# Digital Cinema System Specification: Compliance Test Plan

**Version 1.3**
**(build a140e71)**

Approved for Distribution June 15, 2022
Digital Cinema Initiatives, LLC, Member Representative Committee

Copyright © 2007-2022
Digital Cinema Initiatives, LLC

# Important Notice

This document is a Compliance Test Plan developed by Digital Cinema Initiatives, LLC (DCI). DCI is the owner of this Compliance Test Plan for the purpose of copyright and other laws in all countries throughout the world. The DCI copyright notice must be included in all reproductions, whether in whole or in part, and may not be deleted or attributed to others. DCI hereby grants to its members and their suppliers a limited license to reproduce this Compliance Test Plan for their own use, provided it is not sold. Others must obtain permission to reproduce this Compliance Test Plan from Digital Cinema Initiatives, LLC.

This Compliance Test Plan is intended solely as a guide for companies interested in developing products that can be compatible with other products developed using this document and [DCI-DCSS]. Each DCI member company shall decide independently the extent to which it will utilize, or require adherence to, this Compliance Test Plan. DCI shall not be liable for any exemplary, incidental, proximate or consequential damages or expenses arising from the use of this document. This document defines only one approach to compatibility, and other approaches may be available to the industry. Only DCI has the right and authority to revise or change the material contained in this document, and any revisions by any party other than DCI are unauthorized and prohibited.

Using this document may require the use of one or more features covered by proprietary rights (such as features which are the subject of a patent, patent application, copyright, mask work right or trade secret right). By publication of this document, no position is taken by DCI with respect to the validity or infringement of any patent or other proprietary right. DCI hereby expressly disclaims any liability for infringement of intellectual property rights of others by virtue of the use of this document. DCI has not and does not investigate any notices or allegations of infringement prompted by publication of any DCI document, nor does DCI undertake a duty to advise users or potential users of DCI documents of such notices or allegations. DCI hereby expressly advises all users or potential users of this document to investigate and analyze any potential infringement situation, seek the advice of intellectual property counsel, and, if indicated, obtain a license under any applicable intellectual property right or take the necessary steps to avoid infringement of any intellectual property right. DCI expressly disclaims any intent to promote infringement of any intellectual property right by virtue of the evolution or publication of this document.

DCI gratefully acknowledges the participation and technical contributions of CineCert LLC, 2840 N. Lima St, Suite 110A, Burbank, CA 91504 https://www.cinecert.com/, in the preparation of this document.

DCI gratefully acknowledges the participation and technical contributions of the Fraunhofer Institute for Integrated Circuits, IIS, Am Wolfsmantel 33, 91058 Erlangen, Germany, http://www.iis.fraunhofer.de/, in the preparation of this document.

# Table of Contents


| | | |
|---|---|---|
| **Chapter 1.** | **Introduction** | **8** |
| **1.1.** | **Overview** | **9** |
| **1.2.** | **Normative References** | **12** |
| **1.3.** | **Audience** | **12** |
| **1.4.** | **Conventions and Practices** | **12** |
| **1.5.** | **Digital Cinema System Architecture** | **14** |
| **1.6.** | **Strategies for Successful Testing** | **15** |
| **Part I.** | **Procedural Tests** | **15** |
| **Chapter 2.** | **Digital Cinema Certificates** | **17** |
| **Chapter 3.** | **Key Delivery Messages** | **35** |
| **Chapter 4.** | **Digital Cinema Packaging** | **73** |
| **Chapter 5.** | **Common Security Features** | **99** |
| **Chapter 6.** | **Media Block** | **177** |
| **Chapter 7.** | **Projector** | **263** |
| **Chapter 8.** | **Screen Management System** | **292** |
| **Part II.** | **Design Evaluation Guidelines** | **315** |
| **Chapter 9.** | **FIPS Requirements for a Type 1 SPB** | **317** |
| **Chapter 10.** | **DCI Requirements Review** | **326** |
| **Part III.** | **Consolidated Test Procedures** | **360** |
| **Chapter 11.** | **Testing Overview** | **361** |
| **Chapter 12.** | **Deleted Chapter** | **362** |
| **Chapter 13.** | **Digital Cinema Server Consolidated Test Sequence** | **362** |
| **Chapter 14.** | **Digital Cinema Projector Consolidated Test Sequence** | **370** |
| **Chapter 15.** | **Digital Cinema Projector with MB Consolidated Test Sequence** | **374** |
| **Chapter 16.** | **Link Decryptor/Encryptor Consolidated Test Sequence** | **386** |

| | | |
|---|---|---|
| **Chapter 17.** | **Digital Cinema Server Consolidated Confidence Sequence** | **389** |
| **Chapter 18.** | **Digital Cinema Projector Consolidated Confidence Sequence** | **390** |
| **Chapter 19.** | **Digital Cinema Projector with MB Consolidated Confidence Sequence** | **391** |
| **Chapter 20.** | **OMB Consolidated Test Sequence** | **392** |
| **Chapter 21.** | **Digital Cinema Projector with IMBO Consolidated Test Sequence** | **399** |
| **Chapter 22.** | **OMB Consolidated Confidence Sequence** | **406** |
| **Chapter 23.** | **Digital Cinema Projector with IMBO Consolidated Confidence Sequence** | **407** |
| **Appendix A.** | **Test Materials** | **408** |
| **A.1.** | **Overview** | **409** |
| **A.2.** | **Images** | **409** |
| **A.3.** | **Sound** | **496** |
| **A.4.** | **D-Cinema Packages** | **526** |
| **A.5.** | **Digital Certificates** | **575** |
| **A.6.** | **Key Delivery Messages** | **599** |
| **Appendix B.** | **Equipment List** | **652** |
| **B.1.** | **Hardware** | **653** |
| **B.2.** | **Software** | **654** |
| **Appendix C.** | **Source Code** | **655** |
| **C.1.** | **Overview** | **657** |
| **C.2.** | **dc-thumbprint** | **657** |
| **C.3.** | **schema-check** | **659** |
| **C.4.** | **kdm-decrypt** | **662** |
| **C.5.** | **j2c-scan** | **667** |
| **C.6.** | **eab_calc.py** | **671** |
| **C.7.** | **uuid_check.py** | **673** |
| **C.8.** | **dsig_cert.py** | **674** |
| **C.9.** | **dsig_extract.py** | **677** |
| **Appendix D.** | **ASM Simulator** | **678** |

| | | |
|---|---|---|
| **D.1.** | **ASM Requester and Responder** | **679** |
| **D.2.** | **Example Log Records** | **688** |
| **Appendix E.** | **GPIO Test Fixture** | **702** |
| **Appendix F.** | **Reference Documents** | **704** |
| **Appendix G.** | **Digital Cinema System Specification References to CTP** | **708** |
| **Appendix H.** | **Abbreviations** | **725** |
| **Appendix I.** | **Subtitle Test Evaluation and Pass/Fail Criteria** | **728** |
| **Appendix J.** | **OBAE Test Evaluation Requirements** | **736** |
| **J.1.** | **Overview** | **737** |
| **J.2.** | **Configuration** | **737** |
| **J.3.** | **Requirements** | **737** |
| **J.4.** | **Expectations** | **738** |

# Table of Figures


| | | |
|---|---|---|
| Figure 1.1. | Typical DCI Compliant System Configuration | 14 |
| Figure 6.1. | Standard Frame Panel Designations | 251 |
| Figure 6.2. | Audio Delay Timing | 254 |
| Figure 7.1. | Pixel Structure 16 x 16 Array | 282 |
| Figure 7.2. | Pixel Structure 8 x 8 Array | 282 |
| Figure A.1. | Sync Count | 410 |
| Figure A.2. | "NIST" 2K Test Pattern | 413 |
| Figure A.3. | Black to Gray Step Series | 414 |
| Figure A.4. | Black to White Step Series | 415 |
| Figure A.5. | Color Accuracy Series | 415 |
| Figure A.6. | Intra-Frame Contrast Sequence | 417 |
| Figure A.7. | DCI Numbered Frame Sequence | 419 |
| Figure A.8. | FM Constraints Begin (Encrypted) | 427 |
| Figure A.9. | DCI_gradient_step_s_white_j2c_pt | 432 |
| Figure A.10. | Sync Count with Subtitle Reticles | 493 |
| Figure E.1. | GPIO Test Fixture Schematic | 703 |
| Figure E.2. | GPIO Test Fixture Connector | 703 |
| Figure J.1. | Visual contents of the OBAE Rendering Expectations test material. | 737 |

# Table of Examples


| | | |
|---|---|---|
| Example 2.1. | D-Cinema Certificate | 18 |
| Example 3.1. | Packing List Example (Partial) | 36 |
| Example 3.2. | checksig execution | 37 |
| Example 3.3. | dsig_cert.py execution | 38 |
| Example 3.4. | An X.509 certificate in PEM format | 38 |
| Example 3.5. | dsig_extract.py execution | 39 |
| Example 3.6. | KDM - AuthenticatedPublic area | 40 |
| Example 3.7. | KDM - AuthenticatedPrivate area | 41 |
| Example 3.8. | KDM - Signature area | 42 |
| Example 3.9. | kdm-decrypt Usage and Output | 44 |
| Example 4.1. | Asset Map | 73 |
| Example 4.2. | Volume Index | 74 |
| Example 4.3. | Packing List | 76 |
| Example 4.4. | Composition Playlist | 79 |
| Example 4.5. | MXF Partition Header | 83 |
| Example 4.6. | Source Package structure | 84 |
| Example 4.7. | Cryptographic Framework and Cryptographic Context | 85 |
| Example 4.8. | Essence Descriptor for JPEG 2000 | 85 |
| Example 4.9. | Essence Descriptor for PCM Audio | 86 |
| Example 4.10. | MXF Random Index Pack (RIP) | 87 |
| Example 5.1. | Log Report Example | 124 |
| Example 5.2. | Log Report Record Example | 125 |
| Example 5.3. | Log Report Signature Example | 127 |
| Example C.1. | dc-thumbprint execution | 657 |
| Example C.2. | Using schema-check to check well-formedness | 659 |
| Example C.3. | Using schema-check to check validity | 659 |
| Example C.4. | kdm-decrypt execution | 662 |
| Example C.5. | j2c-scan execution | 667 |
| Example C.6. | eab_calc.py execution | 671 |

Example C.7. uuid_check.py execution 673

Example C.8. dsig_cert.py execution 674

Example C.9. dsig_extract.py execution 677

# Chapter 1. Introduction

Digital Cinema Initiatives, LLC (DCI) is a joint venture of Disney, Fox, Paramount, Sony Pictures Entertainment, Universal, and Warner Bros. Studios. The primary purpose of DCI is to establish uniform specifications for d-cinema. These DCI member companies believe that d-cinema will provide real benefits to theater audiences, theater owners, filmmakers and distributors. DCI was created with the recognition that these benefits could not be fully realized without industry-wide specifications. All parties involved in d-cinema must be confident that their products and services are interoperable and compatible with the products and services of all industry participants. The DCI member companies further believe that d-cinema exhibition will significantly improve the movie-going experience for the public.

Digital cinema is today being used worldwide to show feature motion pictures to thousands of audiences daily, at a level of quality commensurate with (or better than) that of 35mm film release prints. Many of these systems are informed by the *Digital Cinema System Specification, Version 1.0*, published by DCI in 2005. In areas of image and sound encoding, transport security and network services, today's systems offer practical interoperability and an excellent movie-going experience. These systems were designed, however, using de-facto industry practices.

With the publication of the *Digital Cinema System Specification* [DCI-DCSS], and the publication of required standards from SMPTE, ISO, and other bodies, it is possible to design and build d-cinema equipment that meets all DCI requirements. Manufacturers preparing new designs, and theaters planning expensive upgrades are both grappling with the same question: how to know if a d-cinema system is *compliant* with DCI requirements?

Note: This test plan references standards from SMPTE, ISO, and other bodies that have specific publication dates. The specific version of the referenced document to be used in conjunction with this test plan shall be those listed in Appendix F.

## 1.1. Overview

This Compliance Test Plan (CTP) was developed by DCI to provide uniform testing procedures for d-cinema equipment. The CTP details testing procedures, reference files, design evaluation methods, and directed test sequences for content packages and specific types of equipment. These instructions will guide the Test Operator through the testing process and the creation of a standard DCI compliance evaluation report.

This document is presented in three parts and eight appendices.

- Part I. Procedural Tests — contains a library of test procedures for elements of a d-cinema system. Many of the test procedures are applicable to more than one element. The procedure library will be used in Part III. Consolidated Test Procedures to produce complete sequences for testing content and specific types of systems.
    - Chapter 2. Digital Cinema Certificates — describes test objectives and procedures to test d-cinema certificates and devices which use d-cinema certificates for security operations.
    - Chapter 3. Key Delivery Messages — describes test objectives and procedures to test Key Delivery Messages (KDM) and devices which decrypt KDM payloads.
    - Chapter 4. Digital Cinema Packaging — describes test objectives and procedures to test the files in a Digital Cinema Package (DCP).

- Chapter 5. Common Security Features — describes test objectives and procedures to test security requirements that apply to more than one type of d-cinema device (*e.g.*, an SMS or a projector). Security event logging is also addressed in this chapter.

- Chapter 6. Media Block — describes test objectives and procedures to test that Media Block device operations are correct and valid.

- Chapter 7. Projector — describes test objectives and procedures to test that projector operations are correct and valid.

- Chapter 8. Screen Management System — describes test objectives and procedures to test that Screen Management System (SMS) operations are correct and valid.

- Part II. Design Evaluation Guidelines — contains two chapters that describe DCI security requirements for the design and implementation of d-cinema equipment, and methods for verifying those requirements through document analysis. Requirements in this part of the CTP cannot easily be tested by normal system operation. FIPS 140 requirements for deriving random numbers, for example, must be verified by examining the documentation that is the basis of the FIPS certification.

  - Chapter 9. FIPS Requirements for a Type 1 SPB — provides a methodology for evaluating the results of a FIPS 140 security test. Material submitted for testing and the resulting reports are examined for compliance with [DCI-DCSS] requirements.

  - Chapter 10. DCI Requirements Review — provides a methodology for evaluating system documentation to determine whether system aspects that cannot be tested by direct procedural method are compliant with [DCI-DCSS] requirements.

- Part III. Consolidated Test Procedures — contains consolidated test sequences for testing d-cinema equipment and content.

  - Chapter 11. Testing Overview — Provides an overview of the consolidated testing and test reports and a standard form for reporting details of the testing environment.

  - Chapter 13. Digital Cinema Server Consolidated Test Sequence — A directed test sequence for testing a stand-alone Digital Cinema Server comprising a Media Block (MB) and a Screen Management Server (SMS).

  - Chapter 14. Digital Cinema Projector Consolidated Test Sequence — A directed test sequence for testing a stand-alone Digital Cinema Projector with Link Decryptor Block (LDB).

  - Chapter 15. Digital Cinema Projector with MB Consolidated Test Sequence — A directed test sequence for testing a Digital Cinema Projector having an integrated IMB and an integrated or external SMS.

  - Chapter 16. Link Decryptor/Encryptor Consolidated Test Sequence — A directed test sequence for testing an image processing device which is a remote SPB Type 1 with both Link Encryptor and Link Decryptor capabilities.

  - Chapter 17. Digital Cinema Server Consolidated Confidence Sequence — A confidence test sequence for a stand-alone Digital Cinema Server, based on an existing CTP compliance test performed according to Chapter 13. Digital Cinema Server Consolidated Test Sequence.

- Chapter 18. Digital Cinema Projector Consolidated Confidence Sequence — A confidence test sequence for a stand-alone Digital Cinema Projector, based on an existing CTP compliance test performed according to Chapter 14. Digital Cinema Projector Consolidated Test Sequence.

- Chapter 19. Digital Cinema Projector with MB Consolidated Confidence Sequence — A confidence test sequence for a Digital Cinema Projector with MB, based on an existing CTP compliance test performed according to Chapter 15. Digital Cinema Projector with MB Consolidated Test Sequence.

- Chapter 20. OMB Consolidated Test Sequence A directed test sequence for testing an OMB.

- Chapter 21. Digital Cinema Projector with IMBO Consolidated Test Sequence A directed test sequence for testing a Digital Cinema Projector with IMBO.

- Chapter 22. OMB Consolidated Confidence Sequence — A confidence test sequence for an OMB, assuming the existence of an original CTP compliance test performed according to Chapter 20. OMB Consolidated Test Sequence.

- Chapter 23. Digital Cinema Projector with IMBO Consolidated Confidence Sequence — A confidence test sequence for a Digital Cinema Projector with IMBO, assuming the existence of an original CTP compliance test performed according to Chapter 21. Digital Cinema Projector with IMBO Consolidated Test Sequence.

- Appendix A. Test Materials — Provides a complete description of all reference files used in the test procedures including Digital Cinema Packages, KDMs and Certificates.

- Appendix B. Equipment List— Provides a list of test equipment and software used to perform the test procedures. The list is not exclusive and in fact contains many generic entries intended to allow Testing Organizations to exercise some discretion in selecting their tools.

- Appendix C. Source Code — Provides computer programs in source code form. These programs are included here because suitable alternatives were not available at the time this document was prepared.

- Appendix D. ASM Simulator — Provides documentation on **asm-requester** and **asm-responder**, two programs that simulate the behavior of devices that send and receive Auditorium Security Messages.

- Appendix E. GPIO Test Fixture — Provides a schematic for a GPIO test fixture.

- Appendix F. Reference Documents — Provides a complete list of the documents referenced by the test procedures and design requirements.

- Appendix G. Digital Cinema System Specification References to CTP — Provides a cross reference of [DCI-DCSS] sections to the respective CTP sections.

- Appendix H. Abbreviations — Provides explanations of the abbreviations used in this document.

## 1.2. Normative References

The procedures in this document are substantially traceable to the many normative references cited throughout. In some cases, DCI have chosen to express a constraint or required behavior directly in this document. In these cases it will not be possible to trace the requirement directly to an external document. Nonetheless, the requirement is made normative for the purpose of DCI compliance testing by its appearance in this document.

## 1.3. Audience

This document is written to inform readers from many segments of the motion picture industry, including manufacturers, content producers, distributors, and exhibitors. Readers will have specific needs of this text and the following descriptions will help identify the parts that will be most useful to them. Generally though, the reader should have technical experience with d-cinema systems and access to the required specifications. Some experience with general operating system concepts and installation of source code software will be required to run many of the procedures.

**Equipment Manufacturers**
To successfully pass a compliance test, manufacturers must be aware of all requirements and test procedures. In addition to understanding the relevant test sequence and being prepared to provide the Test Operator with information required to complete the tests in the sequence, the manufacturer is also responsible for preparing the documentation called for in Part II. Design Evaluation Guidelines.

**Testing Organizations and Test Operators**
The Testing Organizations and Test Operators are responsible for assembling a complete test laboratory with all required tools and for guiding the manufacturer through the process of compliance testing. Like the manufacturer, Testing Organizations and Test Operators must be aware of all requirements and test procedures at a very high level of detail.

**System Integrators**
Integrators will need to understand the reports issued by Testing Organizations. Comparing systems using reported results will be more accurate if the analyst understands the manner in which individual measurements are made.

## 1.4. Conventions and Practices

### 1.4.1. Typographical Conventions

This document uses the following typographical conventions to convey information in its proper context.

A **Bold Face** style is used to display the names of commands to be run on a computer system.

A `Fixed Width` font is used to express literal data such as string values or element names for XML documents, or command-line arguments and output.

Examples that illustrate command input and output are displayed in a `Fixed Width` font on a shaded background:

```
$ echo "Hello, World!"
Hello, World! 1
```

Less-than (<) and greater-than (>) symbols are used to illustrate generalized input values in command-line examples. They are placed around the generalized input value, *e.g.*, `<input-value>`. These symbols are also used to direct command output in some command-line examples, and are also an integral part of the XML file format.

Callouts (white numerals on a black background, as in the example above) are used to provide reference points for examples that include explanations. Examples with callouts are followed by a list of descriptions explaining each callout.

Square brackets ([ and ]) are used to denote an external document reference, *e.g.*, [SMPTE-377-1].

## 1.4.2. Documentation Format

The test procedures documented in Part I. Procedural Tests will contain the following sub-sections (except as noted)

**Objective —**
Describes what requirements or assertions are to be proven by the test.

**Procedures —**
Defines the steps to be taken to prove the requirements or assertions given in the corresponding objective.

**Material —**
Describes the material (reference files) needed to execute the test. This section may not be present, for example, when the objective can be achieved without reference files.

**Equipment —**
Describes what physical equipment and/or computer programs are needed for executing the test. The equipment list in each procedure is assumed to contain the Test Subject. If the equipment list contains one or more computer programs, the list is also assumed to contain a general purpose computer with a POSIX-like operating system (*e.g.*, Linux). This section may not be present, for example, when the objective can be achieved by observation alone.

**References —**
The set of normative documents that define the requirements or assertions given in the corresponding objective.

The following language is used to identify persons and organizations by role:

**Testing Organization**
An organization which offers testing services based on this document.

**Test Operator**
A member of the Testing Organization that performs testing services.

**Testing Subject**
A device or computer file which is the subject of a test based on this document.

The following language is used for referring to individual components of the system or the system as a whole:

**Media Block and Controlling Devices**
This term refers to the combination of a Media Block (MB), Screen Management System (SMS) or Theater Management System (TMS), content storage and all cabling necessary to interconnect these devices. Depending upon actual system configuration, all of these components may exist in a single chassis or may exist in separate chassis. Some or all components may be integrated into the projector (see below).

**Projector**
The projector is the device responsible for converting the electrical signals from the Media Block to a human visible picture on screen. This includes all necessary power supplies and cabling.

**Projection System**

A complete exhibition system to perform playback of d-cinema content. This includes all cabling, power supplies, content storage devices, controlling terminals, media blocks, projection devices and sound processing devices necessary for a faithful presentation of the content.

**Theater System**

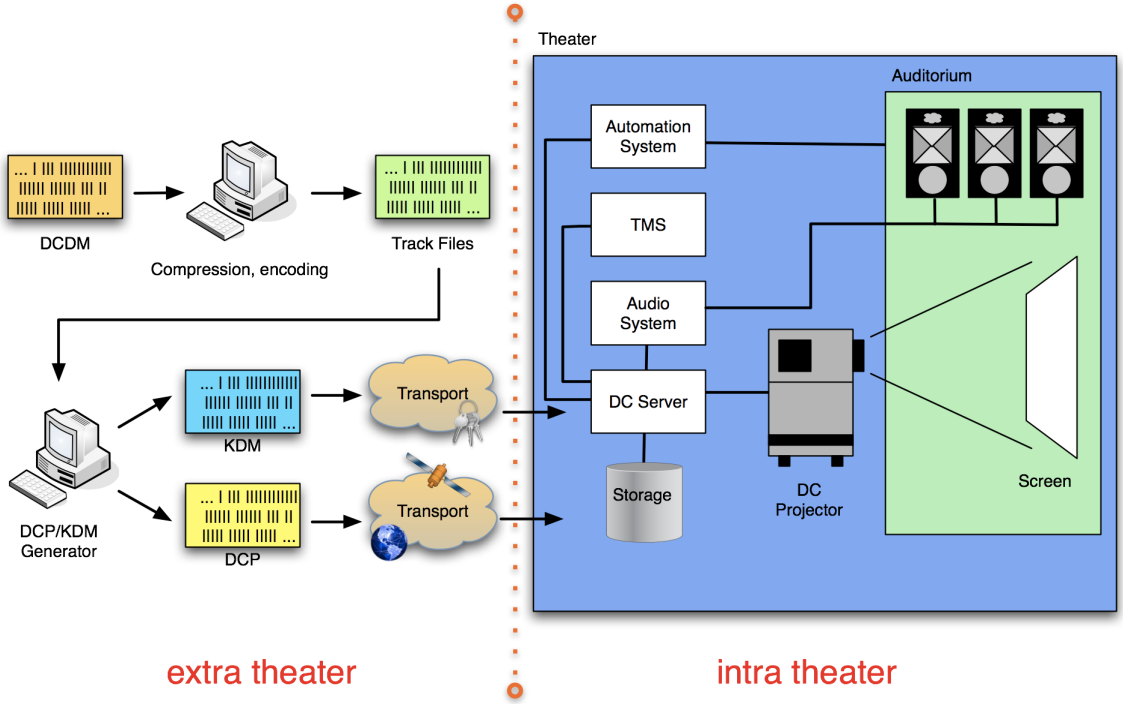
The projection system plus all the surrounding devices needed for full theater operations including theater loudspeakers and electronics (the "B-Chain"), theater automation, a theater network, and management workstations (depending upon implementation), etc.

Note: there may be additional restrictions, depending on implementation. For example, some Media Blocks may refuse to perform even the most basic operations as long as they are not attached to an SMS or Projector. For these environments, additional equipment may be required.

## 1.5. Digital Cinema System Architecture

The [DCI-DCSS] allows different system configurations, meaning different ways of grouping functional modules and equipment together. The following diagram shows what is considered to be a typical configuration allowed by DCI.

### Figure 1.1. Typical DCI Compliant System Configuration




The left side of the diagram shows the *extra-theater* part, which deals with DCP and KDM generation and transport. The right side shows the *intra-theater* part, which shows the individual components of the projection system and how they work together. This test plan will test for proper DCP and KDM formats (*i.e.*, conforming to the Digital Cinema System Specification), for proper transport of the data and for proper processing of valid and malformed DCPs and KDMs. In addition, physical system properties and performance will be tested in order to ensure that the system plays back the data as expected and implements all security measures as required by DCI.

While the above diagram shows what is considered to be a typical configuration allowed by the Digital Cinema System Specification, the [DCI-DCSS] still leaves room for different implementations, for example, some manufacturers may choose to integrate the Media

Decryptor blocks into the projector, or share storage between d-cinema servers.

## 1.6. Strategies for Successful Testing

In order to successfully execute one of the test sequences given in Part III. Consolidated Test Procedures, the Test Operator must understand the details of many documents and must have assembled the necessary tools and equipment to execute the tests. This document provides all the necessary references to standards, tutorials and tools to orient the technical reader.

As an example, Section 7.5.12 requires a calculation to be performed on a set of measured and reference values to determine whether a projector's colorimetry is within tolerance. Section C.6 provides an implementation of this calculation, but the math behind the program and the explanation behind the math are not presented in this document. The Test Operator and system designer must read the reference documents noted in Section 7.5.12 (and any references those documents may make) in order to fully understand the process and create an accurate design or present accurate results on a test report.

Preparing a Test Subject and the required documentation requires the same level of understanding as executing the test. Organizations may even choose to practice executing the test internally in preparation for a test by a Testing Organization. The test procedures have been written to be independent of any proprietary tools. In some cases this policy has led to an inefficient procedure, but the resulting transparency provides a reference measurement that can be used to design new tools, and verify results obtained from any proprietary tools a Testing Organization may use.

[This Page Left Blank Intentionally]

# Part I. Procedural Tests

Many tests in this Part rely on the Security Manager promptly making available log records of events. In order to provide a bound on test durations, failure of a Security Managers to make the record of an event available as part of a log report within 5 minutes of the event being recorded is cause to fail the test being conducted.

## Chapter 2. Digital Cinema Certificates

Authentication of devices in d-cinema is accomplished using *asymmetric cryptography*. Unlike symmetric cryptography, which uses the same key to encrypt and decrypt data, asymmetric cryptography uses a pair of keys that each reverse the other's cryptographic operations: data encrypted with one key in the key pair can only be decrypted by the other key in the key pair. In such a key pair, there is a *public key* that is distributed freely, and a *private key* that is closely held and protected. Public keys are not easily distinguished from one another because they don't carry any identifying information (they're just really long random numbers). To address this, public keys are distributed with metadata that describes the person or device that holds the private key, called the *subject*. This set of metadata and the public key comprise the *digital certificate*. The standard that defines a digital certificate for d-cinema is [SMPTE-430-2] . It is based on the ITU standard for Public Key Infrastructure, called *X.509*, and specifies a number of constraints on the X.509v3 standard, such as the X.509 version that can be used and the size of the RSA keys, among other things.

A digital certificate also contains a *signature*, created by generating a message digest of the certificate and then encrypting that message digest with a (usually different) private key. The signature is then added to the certificate, and is used to verify that the certificate is authentic. The holder of the (private) key used to sign a certificate (encrypt the message digest) is known as the *issuer*, and identifying information about the issuer is in the Issuer field of the certificate, linking the issuer to the subject's certificate. Similarly, identifying information about the subject is in the Subject field. In most cases, the issuer and the subject are different. When the issuer and subject are the same, the certificate is known as being self-*signed*. A self-signed certificate is also self-validating, as its own public key is used to validate its signature. When a self-signed certificate is used to sign other certificates, it becomes the *Certificate Authority* (CA) for those certificates. The collection of certificates, from the top CA certificate to the last certificate (known as a *leaf certificate*) are collectively called the *certificate chain*.

Certificate authentication is recursive: in order to verify that a certificate is valid you have to decrypt the signature using the public key in the issuer's certificate. Once that signature is validated, if the issuer's certificate is not self signed then the signature validation process continues up the chain until a self-signed (CA) certificate is validated. A certificate is trusted only if its entire chain is valid.

The test procedures in this chapter are organized into two groups: tests that evaluate a certificate's compliance to [SMPTE-430-2] and tests that evaluate the behavior of devices that decode certificates. The Certificate Decoder tests are in this section because they are not specific to any particular type of system. All d-cinema devices that decode certificates must behave in the manner described by these tests.

### 2.1. Certificate Structure

The testing procedures that follow make use of the **openssl** cryptographic tools and library. **openssl** is a well known, free, and open source software package available for a number of hardware platforms and operating systems.

Much of the information in a digital certificate can be viewed in a human-readable format using **openssl**'s 'text' option. The information presented in the text output can be used to validate a number of certificate requirements, and to validate certificate-

related KDM requirements by comparing the values present in the text output to the values in the KDM. The following example illustrates the features of a typical d-cinema leaf certificate:

## Example 2.1. D-Cinema Certificate

```
$ openssl x509 -text -noout -in smpte-430-2-leaf-cert.pem 1

Certificate:
    Data:
        Version: 3 (0x2) 2
        Serial Number: 39142 (0x98e6) 3
        Signature Algorithm: sha256WithRSAEncryption 4
        Issuer: O=.ca.example.com, OU=.ra-1b.ra-1a.s430-2.ca.example.com,
                CN=.cc-admin/dnQualifier=0sdCakNi3z6UPCYnogMFITbPMos= 5
    Validity: 6
        Not Before: Mar 9 23:29:52 2007 GMT 7
        Not After : Mar 8 23:29:45 2008 GMT 8
    Subject: O=.ca.example.com, OU=.cc-admin.ra-1b.ra-1a.s430-2.ca.example.com, 9
            CN=SM.ws-1/dnQualifier=H/i8HyVmKEZSFoTeYI2UV9aBiq4= 10
    Subject Public Key Info: 11
        Public Key Algorithm: rsaEncryption 12
        RSA Public Key: (2048 bit) 13
          Modulus (2048 bit): 14
              [hexadecimal values omitted for brevity]
          Exponent: 65537 (0x10001) 15
    X509v3 extensions: 16
        X509v3 Key Usage: 17
          Digital Signature, Key Encipherment, Data Encipherment 18
        X509v3 Basic Constraints: critical 19
          CA:FALSE
        X509v3 Subject Key Identifier: 20
          1F:F8:BC:1F:25:66:28:46:52:16:84:DE:60:8D:94:57:D6:81:8A:AE
        X509v3 Authority Key Identifier: 21
          keyid:D2:C7:42:6A:43:62:DF:3E:94:3C:26:27:A2:03:05:21:36:CF:32:8B
          DirName:/O=.ca.example.com/OU=.ra-1a.s430-2.ca.example.com/
                CN=.ra-1b/dnQualifier=3NMh+Nx9WhnbDcXKK1puOjX4lsY=
          serial:56:CE

Signature Algorithm: sha256WithRSAEncryption 22
           [hexadecimal values omitted for brevity]
```

1 Openssl command line and arguments to view the certificate text

2 The x509 version of the certificate

3 The serial number of the certificate.

4 The algorithm that was used to sign the certificate.

5 Information about the Issuer of the certificate.

6 The validity section of the certificate.

7 The date the certificate validity period begins.

8 The date the certificate validity period ends.

9 The Subject Name of the certificate.

10 Information about the Subject of the certificate

11 Information about the Subject's public key.

12 The algorithm used to create the public key

13 Information about the RSA public key.

14 The modulus value, which is a component of the public key.

15 The exponent value, which is a component of the public key

16 x509 Version 3 Extensions. These extensions provide more information about the private key, the purposes for which it can be used, and how it is identified.

17 Key Usage. These are the actions that the private key can perform.

18 The enumerated list of actions that the private key can perform.

19 x509 Basic Constraints. These declare whether or not the certificate is a CA certificate, and whether or not there is a path length limitation. Basic Constraints must be marked Critical

20 The Subject Key Identifier identifies the public key in the certificate.

21 The Authority Key Identifier identifies the Issuer key used to sign the certificate.

22 The Signature Algorithm used to sign the certificate.

## 2.1.1. Basic Certificate Structure

### Objective

Verify that the certificate uses the ITU X.509, Version 3 standard with ASN.1 DER encoding as described in [ITU-X509]. Also verify that the `Issuer` and `Subject` fields are present inside the signed part of the certificate.

### Procedures

The certificate format and encoding can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -inform PEM -in <certificate>
```

A correctly formatted and encoded certificate will be displayed as text output by **openssl**. An incorrectly formed certificate will cause **openssl** to display an error. A certificate that causes an error to be displayed by the **openssl** command is incorrectly formed and shall be cause to fail this test.

The version of the certificate and the presence of the `Issuer` and `Subject` fields in the signed portion of the certificate can be verified by viewing **openssl's** text output of the certificate. The version number is indicated by 2 in the example certificate, and the issuer and subject fields are indicated by numbers 5 and 10, respectively. An x509 version number other than 3, or the absence of either the Subject field or the Issuer field shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>ITU-X509<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.2. SignatureAlgorithm Fields

### Objective

Verify that the `SignatureAlgorithm` of the signature and the `SignatureAlgorithm` in the signed portion of the certificate both contain the value `"sha256WithRSAEncryption"`.

### Procedures

The signature algorithms of the signature and of the certificate can be verified by using the **openssl** command to display the certificate text as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The signature algorithm of the certificate is indicated by 4 in the example certificate, and the signature algorithm of the signature is indicated by number 22 of the example certificate.

Verify that these fields both contain the value `"sha256WithRSAEncryption"`. If either field contains a different value, this shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.3. SignatureValue Field

### Objective

Verify that the `SignatureValue` field is present outside the signed part of the certificate and contains an ASN.1 Bit String that contains a `PKCS #1SHA256WithRSA` signature block.

### Procedures

The certificate signature value can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

A correct certificate signature will be displayed as colon separated hexadecimal values in the text output by **openssl**. The signature block, omitted from the example certificate, will be present below the signature algorithm at the bottom of the output below callout number 22 of the example certificate. An incorrect certificate signature will cause openssl to display an error. A certificate that causes **openssl** to generate errors is cause to fail this test. A signature value other than sha256WithRSAEncryption is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.4. SerialNumber Field

### Objective

Verify that the `Serial Number` field is present inside the signed part of the certificate and that it contains a nonnegative integer that is no longer than 64 bits (8 bytes).

### Procedures

The certificate serial number can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The serial number field is indicated by 3 in the example certificate. Confirm that the serial number is a non-negative integer that is no longer than 64 bits (8 bytes), and that the parenthetical phrase "neg" is not present. A negative serial number or a number larger than 64 bits shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.5. SubjectPublicKeyInfo Field

### Objective

Verify that the `Subject Public Key Info` field is present inside the signed part of the certificate and that it describes an RSA public key with a modulus length of 2048 bits and a public exponent of 65537.

### Procedures

The subject public key info can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The Subject Public Key Info is indicated by 11 in the example certificate. The modulus length and the public exponent are indicated by 14 and 15, respectively.

Verify that the `Public Key Algorithm` type is `rsaEncryption` and `RSA Public Key` is `(2048 bit)`. Failure to meet both requirements is cause to fail this test.

Verify that the `Modulus` is `(2048 bit)` and that `Exponent` is `65537 (0x10001)`. Any other value for the modulus length or the exponent shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.6. Deleted Section

The section "RSA Key Format" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 2.1.7. Validity Field

### Objective

Verify that the `Validity` field is present inside the signed part of the certificate and contains timestamps in UTC. Timestamps with years up to and including 2049 must use two digits (UTCTime) to represent the year. Timestamps with the year 2050 or later must use four digits (GeneralizedTime) to represent the year.

### Procedures

The presence of the validity field can be verified by using the **openssl** command to display the certificate text as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The validity field is indicated by callout 6 in the example certificate. Confirm that the field is present and that it contains a "Not Before" value as a UTC timestamp as indicated by 7 of the example certificate and a "Not After" value as a UTC timestamp as indicated by 8 of the example certificate. If the validity field is not present, this shall be cause to fail this test.

Verifying the format of the timestamps as either UTCTime or GeneralizedTime can be accomplished by viewing the ASN.1 sequences of the certificate with **openssl**. Additionally, by using the grep command to specify a text string to display, in this case, "TIME", the time formats can be quickly identified:

```
$ openssl asn1parse -in <certificate> |grep TIME
154:d=3 hl=2 l= 13 prim: UTCTIME :070312145212Z
169:d=3 hl=2 l= 13 prim: UTCTIME :270307145212Z
```

Confirm that timestamps up to the year 2049 are in UTCTime format, and that timestamps starting with the year 2050 are in GeneralizedTime format. Timestamps in UTCTime format will be formatted as "YYMMDDhhmmssZ", and Timestamps in GeneralizedTime format will have the year coded as "YYYYMMDDhhmmssZ", where "Y" represents the year, "M" represents the month, "D" represents the day, and "h", "m", "s", and "Z" represent hours, minutes, seconds, and the Universal Coordinated Time zone. A timestamp prior to 2049 that is not in UTC format shall be cause to fail this test. A timestamp starting in 2050 or later that is not in GeneralizedTime format shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.8. AuthorityKeyIdentifier Field

### Objective

Verify that the `Authority Key Identifier` field is present in the `X509v3 Extensions` section inside the signed part of the certificate.

### Procedures

The presence of the `Authority Key Identifier` field can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The Authority Key Identifier of the certificate is indicated by 21 in the example certificate. Confirm that this field exists. The absence of the `Authority Key Identifier` field shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.9. KeyUsage Field

### Objective

Verify that the `Key Usage` field is present in the `X509v3 Extensionssection` inside the signed part of the certificate.

For signer certificates, verify that only the "Certificate Sign" `(keyCertSign)` flag is true, the "CRL Sign" `(cRLSign)` flag may optionally be present.

For the SM role leaf certificate of a dual certificated MB, verify that the "Certificate Sign" `(keyCertSign)`, "CRL Sign" `(cRLSign)`, and the "Digital Signature" `(digitalSignature)` flags are false or not present and that the "Key Encipherment" `(keyEncipherment)` flag is true.

For the LS role leaf certificate of a dual certificated MB, verify that the "Certificate Sign" `(keyCertSign)`, "CRL Sign" `(cRLSign)`, and the "Key Encipherment" `(keyEncipherment)` flags are false or not present, and that the "Digital Signature" `(digitalSignature)` flag is true.

For all leaf certificates not part of a dual certificated MB, verify that the "Certificate Sign" `(keyCertSign)` and "CRL Sign" `(cRLSign)` flags are false or not present, and that the "Digital Signature" `(digitalSignature)`, and "Key Encipherment" `(keyEncipherment)` flags are true.

### Procedures

The presence of the `Key Usage` field can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The `Key Usage` field in the certificate is indicated by 17 in the example certificate.

For all certificates, confirm that this field exists. Absence of the `Key Usage` field shall be cause to fail this test.

For signing certificates, confirm that the key usage listed in the usage list (indicated by 18) has only "Certificate Sign" `(keyCertSign)`, the optional "CRL Sign" `(cRLSign)` flag may be present. Absence of the "Certificate Sign" `(keyCertSign)` flag, or presence of any other flag except for "CRL Sign" `(cRLSign)`, shall be cause to fail this test.

For the SM role leaf certificate of a dual certificated MB, confirm that the key usage lists "Key Encipherment" `(keyEncipherment)`, and that "Digital Signature" `(digitalSignature)` is absent. Absence of "Key Encipherment" `(keyEncipherment)`, or presence of "Digital Signature" `(digitalSignature)`, shall be cause to fail this test. Presence of "Certificate Sign" `(keyCertSign)` or "CRL Sign" `(cRLSign)` shall be cause to fail this test.

For the LS role leaf certificate of a dual certificated MB, confirm that the key usage lists "Digital Signature" `(digitalSignature)`, and that the "Key Encipherment" `(keyEncipherment)` is absent. Absence of "Digital Signature" `(digitalSignature)`, or presence of "Key Encipherment" `(keyEncipherment)`, shall be cause to fail this test. Presence of "Certificate Sign" `(keyCertSign)` or "CRL Sign" `(cRLSign)` shall be cause to fail this test.

For all leaf certificates not part of a dual certificated MB, confirm that the key usage lists "Digital Signature" `(digitalSignature)` and "Key Encipherment" `(keyEncipherment)`. Absence of "Digital Signature" `(digitalSignature)`

and "Key Encipherment" (`keyEncipherment`) shall be cause to fail this test. Presence of "Certificate Sign" (`keyCertSign`) or "CRL Sign" (`cRLSign`) shall be cause to fail this test.

Note that leaf certificates may have other key usages specified, and the presence of other usages not specifically referenced here shall not be a reason to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.5.1.1, 9.5.1.2, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.10. Basic Constraints Field

### Objective

Verify that the `Basic Constraints` field is present in the `X509v3 Extensions` section of the signed portion of the certificate. For signer certificates, verify that the certificate authority attribute is true (CA:TRUE) and the `PathLenConstraint` value is present and either zero or positive. For leaf certificates, verify that the certificate authority attribute is false (CA:FALSE) and the `PathLenConstraintis` absent or zero.

### Procedures

The presence of the `Basic Constraints` field can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The Basic Constraints field in the certificate is indicated by 19 in the example certificate. For signing certificates, confirm that this field exists, that the certificate authority value is true (CA:TRUE), and that the path length is present and is a positive integer. For leaf certificates, confirm that the certificate authority value is false (CA:FALSE) and that the path length is absent or zero. The absence of the Basic Constraints field shall be cause to fail this test. For signer certificates, the absence of the CA:TRUE value, or a negative or missing Path Length value shall be cause to fail this test. For leaf certificates, the presence of the CA:TRUE value or the presence of a path length greater than zero shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.11. Public Key Thumbprint

### Objective

Verify that there is exactly one `DnQualifier` present in the `Subject` field and that the `DnQualifier` value is the Base64 encoded thumbprint of the subject public key in the certificate. Also verify that there is exactly one `DnQualifier` present in the `Issuer` field and that the DnQualifier value is the Base64 encoded thumbprint of the issuer's public key.

### Procedures

The presence of a single instance of the `DnQualifier` field can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The Subject DnQualifier in the certificate is in the Subject information as indicated by 10 in the example certificate, and the Issuer DnQualifier in the certificate is in the Issuer information as indicated by 5. Confirm that each of these fields contain only one DnQualifier. Missing DnQualifier values in either of these fields or the presence of more than one DnQualifier in either field shall be cause to fail this test.

The public key DnQualifier must be recalculated to confirm that the DnQualifier value in each of these fields is correct.

The following steps perform this calculation:

1. Extract the public key from the certificate (using **openssl**)
2. Convert the public key from Base64 to binary (using **openssl**)
3. Skip 24 bytes into the binary form of the public key (using dd)
4. Calculate the SHA-1 digest over the remaining portion of the binary form of the public key (using **openssl**)
5. Convert the SHA-1 digest value to Base64 (using **openssl**)

The steps above can be performed in sequence by redirecting the output from one step to the next, and using **openssl** and the dd command present on most posix compliant operating systems, such as:

```
$ openssl x509 -pubkey -noout -in <certificate> | openssl base64 -d \
| dd bs=1 skip=24 2>/dev/null | openssl sha1 -binary | openssl base64
```

The resulting value is the calculated DnQualifier of the public key in the input certificate. Confirm that when this calculation is performed on the public key in the subject certificate, the calculated value is equal to the DnQualifier present in the Subject field. Confirm that when this calculation is performed on the public key in the issuer certificate, the calculated value is equal to the DnQualifier present in the Issuer field of the subject certificate. A DnQualifier that does not match the calculated value of the corresponding certificate's public key shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.12. Organization Name Field

### Objective

Verify that exactly one instance of the `OrganizationName` field is present in the `Issuer` and `Subject` fields. Verify that the two `OrganizationName` values are identical.

### Procedures

The presence of the `OrganizationName` in the Subject and Issuer fields can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The OrganizationName values are in the Subject and Issuer fields in the certificate as indicated by 5 and 10 in the example certificate. Confirm that the Organization name, the value specified as `" O=<organization-name>"`, is the same in both fields. Non-identical Organizational name values in the Subject and Issuer fields shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.13. OrganizationUnitName Field

### Objective

Verify that exactly one instance of the `OrganizationUnitName` (OU) value is present in the `Issuer` and `Subject` fields.

### Procedures

The presence of the `OrganizationUnitName` in the Subject and Issuer fields can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The OrganizationUnitName values are in the Subject and Issuer fields in the certificate as indicated by 5 and 10 in the example certificate. The absence of an `OrganizationUnitName` in either the Subject or Issuer fields of the certificate shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.14. Entity Name and Roles Field

### Objective

Verify that the `CommonName (CN)` is present exactly once in both the `Subject` and `Issuer` fields. Also verify that the `CommonName` fields contain a physical identification of the entity (*i.e.*, make, model, or serial number, for devices). For leaf certificates (*i.e.*, certificate authority is set to False), verify that at least one role is specified and that it is the role expected for the certificate.

### Procedures

The presence of the `CommonName` in the Subject and Issuer fields can be verified by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

The CommonName values are in the Subject and Issuer fields in the certificate as indicated by 5 and 10 in the example certificate. Confirm that the `CommonName`, the value specified as "CN=<common-name>" is present only once and that it contains information that identifies the entity. For leaf certificates, confirm that the common name specifies at least one role and that it is correct for the certificate. The absence of the `CommonName` value in either the `Subject` or `Issuer` fields shall be cause to fail this test. For leaf certificates, the absence of a role designation shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.15. Unrecognized Extensions

### Objective

Verify that any X.509v3 extensions in the certificate that are not specified in [SMPTE-430-2] (unrecognized extensions) are not marked critical.

### Procedures

The list of X.509v3 extensions in a certificate can be viewed by using the **openssl** command to display the certificate information as described in Example 2.1., *e.g.*:

```
$ openssl x509 -text -noout -in <certificate>
```

For signer certificates (certificates that have CA:TRUE), of the X.509v3 extensions listed in the certificate, "Basic Constraints" (indicated by 19) must be marked critical. "Basic Constraints" may be marked critical for leaf certificates. "Key Usage" and "Authority Key Identifier" (indicated by 17) may be marked critical. No other unrecognized X.509v3 extensions may be marked critical. A signer certificate with a "Basic Constraints" section that is not marked critical shall be cause to fail this test. A Certificate that has any X.509v3 extension marked critical other than "Basic Constraints", "Key Usage" or "Authority Key Identifier" shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.16. Signature Validation

### Objective

Using the issuer's public key, verify that the signature contained in the certificate is valid.

### Procedures

For this operation to be successful, validation must be performed down the certificate chain, from the self-signed root certificate (the CA) to the leaf certificate being validated. Certificate chain validation is recursive, so as each certificate in the chain is validated it is included as part of the validation of the next certificate. With **openssl**, this results in a file that contains the root certificate and, incrementally, each of the signer certificates of certificate chain of the leaf certificate. This file is then used to validate the signature on the leaf certificate. A certificate chain containing three certificates can be validated by following these steps:

1. Verify that the CA certificate signature is valid
2. Verify that the CA's signature on the signer's certificate is valid.
3. Verify that the signer's signature on the leaf certificate is valid.

This example uses **openssl** to validate each certificate, and the unix command 'cat' to append each successive certificate to a single file. This file is specified to **openssl** using the `-CAfile` option.

```
$ openssl verify -CAfile caroot.pem caroot.pem
caroot.pem: OK
$ cp caroot.pem certchain.pem
$ openssl verify -CAfile certchain.pem signer.pem
signer.pem: OK
$ cat signer.pem >> certchain.pem
$ openssl verify -CAfile certchain.pem leaf.pem
leaf.pem: OK
```

Error messages from **openssl** indicate that a certificate in the chain did not validate, and that the chain is not valid. Error messages that indicate that the certificate chain is not valid shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.1.17. Certificate Chains

### Objective

For a given certificate chain:

- Verify that the certificate chain is complete, *i.e.*, for each certificate specified in an `Issuer` field, there is a corresponding certificate whose `Subject` field matches that `Issuer` field.
- Verify that, for each certificate in the chain, the validity period of any child certificate is completely contained within the validity period of the parent certificate.
- Verify that the root certificate (*i.e.*, a self-signed certificate where the CA-flag is true) is a valid root certificate.

### Procedures

A complete certificate chain starts with a leaf certificate and ends with a self-signed (CA root) certificate. Between the leaf certificate and the CA root certificate there should be one or more signer certificates. A leaf certificate is signed by a signer certificate, and the signer certificate is identified by its DnQualifier in the "Issuer" field of the leaf certificate. In a chain of

three certificates, the signer certificate is in turn signed by the CA root certificate, which is similarly identified by its DnQualifier in the Issuer field of the signer's certificate. The CA root certificate is self-signed and has its own DnQualifier in both the Subject and Issuer fields.

To verify that the certificate chain is complete, confirm that the certificates corresponding to the Issuer DnQualifiers of each of the certificates is present, as explained in Section 2.1.11: Public Key Thumbprint. A certificate chain that does not contain all of the certificates matching the DnQualifiers specified in the Issuer fields of the certificates means the chain is not complete and shall be cause to fail this test.

The validity period of a certificate can be viewed using the procedure described in Section 2.1.7: Validity Field. Confirm that for each certificate in the chain, the signer certificate's validity period completely contains the validity period of the signed certificate. A certificate that has a validity period that extends beyond the validity period of its signer (either starting before, or ending after, the validity period of its signer) shall be cause to fail this test.

To confirm that the CA root certificate is a valid root certificate:

1. Verify that the DnQualifier in the Issuer field is the same as the DnQualifier in the Subject field as described in Section 2.1.11: Public Key Thumbprint.

2. Confirm that the Certificate Authority value in the Basic Constraints field is true and the path length value is a number, zero or greater, as described in Section 2.1.10: Basic Constraints Field.

3. Confirm that the X.509v3 Key Usage contains "Certificate Sign" as described in Section 2.1.9: KeyUsage Field.

A CA certificate that does not have a non-negative path length of zero or greater, or that does not have the basic constraints extension marked critical and containing CA:TRUE, shall be cause to fail this test.

A CA Root certificate that is not self-signed shall be cause to fail this test.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Equipment** | **openssl** |

## 2.2. Certificate Decoder Behavior

### 2.2.1. ASN.1 DER Encoding Check

#### Objective

Verify that a certificate is rejected by the decoding device if it contains syntax errors or does not conform to the ASN.1 DER (Distinguished Encoding Rules) format.

#### Procedures

For the malformed certificate below, perform an operation with the device under test using a malformed certificate. Verify that the operation fails. A successful operation using a malformed certificate is cause to fail this test.

1. A certificate encoded as BER (*chain-c3-BER-enc*, *IMB-chain-a3-BER-enc*)

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-430-2 |
| **Test Materials** | *chain-c3-BER-enc*<br>*chain-c1-root*<br>*chain-c3-root*<br>*IMB-chain-a3-BER-enc*<br>*chain-a3-root*<br>*chain-b1-roo* |

## 2.2.2. Missing Required Fields

### Objective

Verify that certificates with missing required fields are rejected by a device under test.

### Procedures

For each of the malformations below, perform an operation on the device with the certificate that contains that malformation. Verify that the operation fails. A successful operation using a malformed certificate is cause to fail this test.

- missing SignatureAlgorithm field (i.e, *chain-c3-no-saf*, *chain-a3-no-saf*) - reject
- missing SignatureValue field (*chain-c3-no-svf*, *chain-a3-no-svf*) - reject
- missing Version field (*chain-c3-no-ver*, *chain-a3-no-ver*) - reject
- missing SerialNumber field (*chain-c3-no-sn*, *chain-a3-no-sn*) - reject
- missing Signature field (*chain-c3-no-sig*, *chain-a3-no-sig*) - reject
- missing Issuer field (*chain-c3-no-issuer*, *chain-a3-no-issuer*) - reject
- missing Subject field (*chain-c3-no-subject*, *chain-a3-no-subject*) - reject
- missing SubjectPublicKeyInfo field (*chain-c3-no-spki*, *chain-a3-no-spki*) - reject
- missing Validity field (*chain-c3-no-val-f*, *chain-a3-no-val-f*) - reject
- missing AuthorityKeyIdentifier field (*chain-c3-no-aki-f*, *chain-a3-no-aki-f*) - reject
- missing KeyUsage field (*chain-c3-no-keyuse*, *chain-a3-no-keyuse*) - reject
- missing BasicConstraint field (*chain-c3-no-basic*, *chain-a3-no-basic*) - reject

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8 |

| SMPTE-430-2 | **Test Materials** |
|---|---|
| *chain-c3-no-saf*<br>*chain-c3-no-svf*<br>*chain-c3-no-ver*<br>*chain-c3-no-sn*<br>*chain-c3-no-sig*<br>*chain-c3-no-issuer*<br>*chain-c3-no-subject*<br>*chain-c3-no-spki*<br>*chain-c3-no-val-f*<br>*chain-c3-no-aki-f*<br>*chain-c3-no-keyuse*<br>*chain-c3-no-basic*<br>*chain-c1-root*<br>*chain-c3-root*<br>*chain-a3-no-aki-f*<br>*chain-a3-no-basic*<br>*chain-a3-no-issuer*<br>*chain-a3-no-keyuse*<br>*chain-a3-no-saf*<br>*chain-a3-no-sig*<br>*chain-a3-no-sn*<br>*chain-a3-no-spki*<br>*chain-a3-no-subject*<br>*chain-a3-no-svf*<br>*chain-a3-no-val-f*<br>*chain-a3-no-ver* | |

## 2.2.3. PathLen Check

### Objective

Verify that, if the Certificate Authority attribute of the `BasicConstraint` field is `True`, the `PathLenConstraint` value is present and is either zero or positive. Verify that if the certificate authority attribute of the `BasicConstraint` field is False, the `PathLenConstraint` field is absent or set to zero.

### Procedures

1. Perform an operation on the device under test using a leaf certificate with a PathLen greater than zero (0). Verify that the operation fails. A successful operation using a certificate with an incorrect Path Length is cause to fail this test.

2. Perform an operation on the device under test using a leaf certificate with a PathLen that is negative. Verify that the operation fails. A successful operation using a certificate with an incorrect Path Length is cause to fail this test.

3. Perform an operation on the device under test using a signer certificate that does not contain a PathLen (PathLen absent). Verify that the operation fails. A successful operation using a certificate with an incorrect Path Length is cause to fail this test.

4. Perform an operation on the device under test using a signer certificate that contains a PathLen that is negative. Verify that the operation fails. A successful operation using a certificate with an incorrect Path Length is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-420-2 |
| **Test Materials** | *chain-c3-path-1*<br>*chain-c3-path-2*<br>*chain-c3-path-3*<br>*chain-c3-path-4*<br>*chain-c3-path-5*<br>*chain-c3-path-6*<br>*chain-c3-path-7*<br>*chain-c3-root*<br>*chain-a3-path-1*<br>*chain-a3-path-2*<br>*chain-a3-path-3*<br>*chain-a3-path-4*<br>*chain-a3-path-5*<br>*chain-a3-path-6*<br>*chain-a3-path-7*<br>*chain-a3-root* |

## 2.2.4. OrganizationName Match Check

### Objective

Verify that the certificate is rejected by the device if the `OrganizationName` in the subject and issuer fields do not match.

### Procedures

Perform an operation on the device with a certificate that has mismatched `OrganizationName` values in the Subject and Issuer fields. Verify that the operation fails. A successful operation using a malformed certificate is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-420-2 |
| **Test Materials** | *chain-c3-org-name*<br>*chain-c3-root*<br>*chain-a3-org-name*<br>*chain-a3-root* |

## 2.2.5. Certificate Role Check

### Objective

Verify that when the validation context includes a desired role, a device under test rejects a leaf certificate with a role that is different than the role expected.

### Procedures

Perform an operation on the device under test using a certificate with a role that is not permitted for the operation. Verify that the operation fails. A successful operation using a certificate with an incorrect role is cause to fail this test.

- Certificate Authority is False and no role specified in CommonName (*chain-c3-role-1*, *chain-a3-role-1*) - reject

- Distribution Root Certificate without a distributor role, remote SPB root Certificate with a role other than SMS role (*chain-c3-role-2*, *chain-a3-role-2*) - reject

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-420-2 |
| **Test Materials** | *chain-c3-role-1*<br>*chain-c3-role-2*<br>*chain-c3-root*<br>*chain-a3-role-1*<br>*chain-a3-role-2*<br>*chain-a3-root* |

## 2.2.6. Validity Date Check

### Objective

Verify that the certificate is rejected if it is not valid at the desired time (according to the validation context, *e.g.*, time of playback).

### Procedures

Perform an operation on the device with a certificate that is not valid. Verify that the operation fails. A successful operation using a certificate at a time outside of its validity period is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-420-2 |
| **Test Materials** | *chain-c3-date-exp*<br>*chain-c3-root*<br>*chain-a3-date-exp*<br>*chain-a3-root* |

## 2.2.7. Signature Algorithm Check

### Objective

Verify that a certificate is rejected by a device under test if the signature algorithms in the certificate body and the signature are not `sha256WithRSAEncryption`.

### Procedures

Perform an operation on the device with a certificate that has mismatched or incorrect signatures for each of the following types of signature errors. Verify that the operation fails. A successful operation using an incorrectly signed certificate is cause

to fail this test.

- Signature algorithm of the signature not sha256WithRSAEncryption (*chain-c3-osig-type*,*chain-a3-iosig-type*) - reject
- Signature algorithm of the certificate not sha256WithRSAEncryption (*chain-c3-isig-type*, *chain-a3-isig-type*) - reject
- Signature algorithms identical, but not sha256WithRSAEncryption (*chain-c3-iosig-type*, *chain-a3-osig-type*) - reject

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-420-2 |
| **Test Materials** | *chain-c3-osig-type*<br>*chain-c3-isig-type*<br>*chain-c3-iosig-type*<br>*chain-c3-root*<br>*chain-a3-iosig-type*<br>*chain-a3-isig-type*<br>*chain-a3-osig-type*<br>*chain-a3-root* |

## 2.2.8. Public Key Type Check

### Objective

Verify that the certificate is rejected if the subject's Public Key is not a 2048 bit RSA key with an exponent of `65537`.

### Procedures

For each of the types of incorrect public keys below, perform an operation on the device with the certificate that has an public key that is not correct. Verify that the operation fails. A successful operation using a certificate with an incorrect public key is cause to fail this test.

- Public Key not an RSA Key (*chain-c3-no-rsa*, *chain-a3-no-rsa*) - reject
- RSA Public Key Length only 1024 bit (*chain-c3-short-rsa*, *chain-a3-short-rsa*) - reject
- Public Key Exponent other then 65537 (*chain-c3-bad-exp*) - reject

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-420-2 |
| **Test Materials** | *chain-c3-no-rsa*<br>*chain-c3-short-rsa*<br>*chain-c3-bad-exp*<br>*chain-c3-root*<br>*chain-a3-no-rsa*<br>*chain-a3-bad-exp*<br>*chain-a3-short-rsa*<br>*chain-a3-root* |

### 2.2.9. Issuer Certificate Presence Check

#### Objective

Verify that the certificate is rejected if the issuer's certificate cannot be located by looking it up using the value of the `AuthorityKeyIdentifier` X.509v3 extension.

#### Procedures

Perform an operation on the device under test using certificates that do not include the certificate's signer specified by the `AuthorityKeyIdentifier`. Verify that the operation fails. A successful operation using a certificate without the certificate signer present is cause to fail this test.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.8<br>SMPTE-420-2 |
| **Test Materials** | *KDM without AuthorityKey certificate* |

# Chapter 3. Key Delivery Messages

This chapter contains tests for Key Delivery Messages (KDM). The test procedures in this chapter are organized into three groups: tests that evaluate a KDM's compliance to [SMPTE-430-1], tests that evaluate a KDM's compliance to [SMPTE-430-3], and tests that evaluate the behavior of devices that decode KDMs. The KDM Decoder tests are in this section because they are not specific to any particular type of system. All d-cinema devices that decode KDMs must behave in the manner described by these tests.

Before diving in to testing KDM files, we will first introduce XML and provide some examples of KDM documents.

## 3.1. eXtensible Markup Language

XML is a file metaformat: a file format for creating file formats. Many of the files that comprise a d-cinema composition (*e.g.*, a feature or trailer), are expressed in XML. While the various d-cinema file formats represent different concepts within the d-cinema system, the arrangement of data within the files is syntactically similar for those files that use XML. This section will provide an overview of XML as used for d-cinema applications. Readers looking for more detailed technical information are referred to the home of XML at http://www.w3.org.

### 3.1.1. XML Documents

The main unit of data storage in an XML document is the XML *element*. XML elements are expressed in a document using *tags*; strings of human-readable text enclosed between less-than (<) and greater-than (>) characters. An XML *document* is an element that is meant to be interpreted as a complete unit. Every XML document consists of a single XML element having zero or more

(usually hundreds more) elements inside. XML documents may be stored as files, transmitted over networks, etc. The following example shows a very simple XML element, rendered as a single tag

```
<Comment/>
```

By itself, this XML element is a complete, though very uninteresting XML document.

To be more useful, our example element needs some data, or *content*. XML content may include unstructured text or additional XML elements. Here we have expanded the element to contain some text:

```
<Comment>The quick brown fox...</Comment>
```

Notice that when an XML element has content, the content is surrounded by two tags, in this case <Comment> and </Comment>. The former is an *opening* tag, the latter a *closing* tag.

We now have some data inside our element. We could help the reader of our example XML document by indicating the language that the text represents (these same characters could of course form words from other languages). The language of the text is *metadata*: in this case, data about the text. In XML, metadata is stored as sets of key/value pairs, or *attributes*, inside the opening tags. We will add an attribute to our example element to show some metadata, in this case we are telling the reader that the text is in English:

```
<Comment language="en">The quick brown fox...</Comment>
```

The following example shows an actual d-cinema data structure (there is no need to understand the contents of this example as this particular structure is covered in more detail in Section 4.2.1.):

### Example 3.1. Packing List Example (Partial)

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<PackingList xmlns="http://www.smpte-ra.org/schemas/429-8/2007/PKL">
  <Id>urn:uuid:59430cd7-882d-48e8-a026-aef4b6253dfc</Id>
  <AnnotationText>Perfect Movie DCP</AnnotationText>
  <IssueDate>2007-07-25T18:21:31-00:00</IssueDate>
  <Issuer>user@host</Issuer>
  <Creator>Packaging Tools v1.0</Creator>
  <AssetList>
    <Asset>
      <Id>urn:uuid:24d73510-3481-4ae5-b8a5-30d9eeced9c1</Id>
      <Hash>AXufMKY7NyZcfSXQ9sCZls5dSyE=</Hash>
      <Size>32239753</Size>
      <Type>application/mxf</Type>
      <AnnotationText>includes M&amp;amp;E</AnnotationText>
    </Asset>
  </AssetList>
</PackingList>
```

## 3.1.2. XML Schema

You may have noticed that the basic structure of XML allows the expression of almost unlimited types and formats of information. Before a device (or a person) can read an XML document and decide whether it is semantically correct, it must be possible for the reader to know what the document is expected to contain.

The XML standard dictates some initial requirements for XML documents. The document shown in Example 3.1. above illustrates some of these requirements:

1. Element tags must be correctly nested: an element must be closed in the same scope in which it was opened. For example, the following XML fragment shows incorrect nesting of the `Element3` element (it should close before `Element2` closes, not after).

```
<Element1>
  <Element2>
  <Element3>
  </Element2>
  </Element3>
</Element1>
```

2. The document may not contain special characters in unexpected places. For example, the &, < and > characters may not appear except in certain cases. Special encodings must be used to use these characters literally within an XML document.

A document which meets these requirements is said to be *well formed*. All XML documents must be well formed. An XML *parser* (a program that reads XML syntax) will complain if you give it XML that is not well-formed. Well-formedness, however, does not help us understand *semantically* what's in an XML document. To know the meaning of a particular XML structure, we have to have a description of that structure.

The structure and permitted values in an XML document can be defined using XML Schema. There are other languages for expressing the content model of an XML document, but XML Schema is the standard used by the SMPTE specifications for d-cinema. XML Schema is a language, expressed in XML, which allows the user to define the names of the elements and attributes that can appear in an XML document. An XML Schema can also describe the acceptable contents of and combinations of the XML elements.

Given an XML Schema and an XML document, a *validating* XML parser will report not only errors in syntax but also errors in the use and contents of the elements defined by the schema. Throughout this document, we will use the **schema-check** program (see Section C.3) to test XML documents. The command takes the instance document and one or more schema documents as arguments

```
$ schema-check <input-file> smpte-430-3.xsd
```

If this command returns without errors, the XML document can be said to be both well-formed and *valid*

Some XML documents are defined using more than one schema. In these cases, you can supply the names of any number of schemas on the command line:

```
$ schema-check <input-file> smpte-430-3.xsd smpte-430-1.xsd
```

### 3.1.3. XML Signature Validation

*XML Signature* is a standard for creating and verifying digital signatures on XML documents. Digital signatures are used to allow recipients of Composition Playlists, Packing Lists and Key Delivery Messages (KDM) to *authenticate* the documents; to prove that the documents were signed by the party identified in the document as the document's signer, and that the documents have not been modified or damaged since being signed.

The **checksig** program (distributed with the XML Security library) can be used to test the signature on an XML document. The program is executed with the name of a file containing a signed XML document:

#### Example 3.2. checksig execution

```
$ checksig test-kdm.xml
Signature verified OK!
```

The program expects that the first certificate in the `<KeyInfo>` element is the signer. This has two implications:

1. The program will fail if the signer is not the first (SMPTE standards allow any order)
2. The program does not check the entire certificate chain

To address the first issue, the **dsig_cert.py** program (see Section C.8) can be used to re-write the XML document with the signer's certificate first in the `<KeyInfo>` element. This is demonstrated in the following example:

## Example 3.3. dsig_cert.py execution

```
$ dsig_cert.py test-kdm.xml > tmp.xml
$ checksig tmp.xml
Signature verified OK!
```

The second issue is addressed by extracting the certificates from the document's XML Signature data and validating them directly with **openssl**. This procedure is the subject of the next section.

### 3.1.3.1. Extracting Certificates from an XML Document

In order to test certificates separately from the XML document in which they are embedded, this procedure will manually extract them into separate PEM files (see [RFC-1421]). A PEM file contains a certificate (more than one if desired, but we're not going to do that just yet) as a DER-encoded binary string which is then encoded using Printable Encoding (see [RFC-1421]). The encoded text is prefixed by the string `-----BEGIN CERTIFICATE-----` followed by a newline. The encoded text is followed by the string `-----END CERTIFICATE-----`. An example of this format can be seen below. Note that the Printable Encoding has newlines after every 64 characters.

## Example 3.4. An X.509 certificate in PEM format

```
-----BEGIN CERTIFICATE-----
MIIEdzCCA1+gAwIBAgICNBowDQYJKoZIhvcNAQELBQAwgYQxGTAXBgNVBAoTEC5j
YS5jaW5lY2VydC5jb20xLDAqBgNVBAsTIy5yYS0xYi5yYS0xYS5zNDMwLTIuY2Eu
Y2luZWNlcnQuY29tMRIwEAYDVQQDEwkuY2MtYWRtaW4xJTAjBgNVBC4THGNwSmxw
NDBCM0hqSG9kOG9JWnpsVi9DU0xmND0wIBcNMDcwMTE1MjI0OTQ0WhgPMjAwODAx
MTUyMjQ5NDJaMIGLMRkwFwYDVQQKExAuY2EuY2luZWNlcnQuY29tMTUwMwYDVQQL
EywuY2MtYWRtaW4ucmEtMWIucmEtMWEuczQzMC0yLmNhLmNpbmVjZXJ0LmNvbTEQ
MA4GA1UEAxMHU00ud3MtMTElMCMGA1UELhMcdC8zQ2xNWjdiQWRGUnhnam1TRTFn
NGY4NUhNPTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOBejWa3Lg+Y
uvTYhCaFy0ET6zH6XrB3rLRrlbeMrrTuUMCX0YSmA7m3ZO1Bd/HQrJxyq6hJmPGu
auxwWiF4w+AajBRp4eSiAt8srACcEmUyqGHwPLoaKVEaHXSOY8gJp1kZwqGwoR40
RQusfAb2/L76+RlMUyACoJuR6k4kOBW3bjEE4E76KKR4k5K580d7uFf5G86GhGfU
AfXHJXboqzHnxQHaMldKNaSskxWrW8GrX43+2ZZUHM2ZKe0Ps/9g2gCRZ6eYaim4
UF+szH0EUY0Mbx4poqn+SZFrUWtEoWcDM6PSTTgCQVOQ1BtzD1lBQoNQGOJcd73N
9f5MfGioWMkCAwEAAaOB5zCB5DALBgNVHQ8EBAMCBLAwDAYDVR0TAQH/BAIwADAd
BgNVHQ4EFgQUt/3ClMZ7bAdFRxgjmSE1g4f85HMwgacGA1UdIwSBnzCBnIAUcpJl
p40B3HjHod8oIZzlV/CSLf6hf6R9MHsxGTAXBgNVBAoTEC5jYS5jaW5lY2VydC5j
b20xJjAkBgNVBAsTHS5yYS0xYS5zNDMwLTIuY2EuY2luZWNlcnQuY29tMQ8wDQYD
VQQDEwYucmEtMWIxJTAjBgNVBC4THEJteVdZV3d0M29FNlJGSTVYdDd3K0hGaEtW
Zz2CAwDpzTANBgkqhkiG9w0BAQsFAAOCAQEAowjAFQsyoKto7+WBeF9HuCRpKkxk
6qMgXzgAfJFRk/pi7CjnfjxvWukJq4HWgWHpXsGFf/RTp08naV1UHNe71sDYV2Fb
MOSFRi2OrRwZExO9SBKQHLZ7ZdLU+6GIHXKjmp9DiofUNOqvZPQnvwG/CmO84CpG
K14ktxtOghczzEiJCk2KISsgOU6NK4cmcFfMjuklTwmD5C6TvaawkvcNJQcldjUw
TWbvd+Edf9wkHNvBERR9lbCGWr16C5BVQZtFBJAU++3guL/4Qn4lkeU/gmR6o99S
```

```
UQ+T344CBSIy06ztiWZiuxoONoXfy12DTSepB+QShmuhsScrfv0Q9bB5hw==
-----END CERTIFICATE-----
```

Within an XML document signed using XML Signature, certificates are stored in `<dsig:X509Certificate>` elements. These elements can be found at the end of the document, within the `</dsig:Signature>` element. The encoding method for storing certificate data in XML Signature is virtually identical to PEM. The Base64 encoding (see [RFC-2045]) uses the same mapping of binary data to text characters, but the line length is not limited as with PEM.

It is a relatively easy task to use a **Text Editor** to copy and paste certificate data from an XML document:

1. Open a new **Text Editor** window, and paste `-----BEGIN CERTIFICATE-----`, then press the Enter key. Note that the number of '-' (dash) characters on either side of the `BEGIN CERTIFICATE` label is five (5).

2. Copy the content of the selected `<dsig:X509Certificate>` element (but not the element tags) from the KDM and paste it into the new editor window. The cursor should now be positioned at the last character of the certificate; press the Enter key.

3. Paste `-----END CERTIFICATE-----` at the end of the new editor window and press the Enter key.

4. Note again that Printable Encoding lines in PEM format files must be no more than 64 characters in length. If the Base64 certificate string copied from the KDM contains long lines, manually break the lines using the cursor and the Enter key.

5. Save the editor's contents to a file, usually with a `.pem` suffix.

In most cases the procedure given above can be automated using the **dsig_extract.py** program (see Section C.9). As shown below, the `-p` option can be used to provide a prefix for the automatically-generated filenames. In this example, the input document contained four certificates.

### Example 3.5. dsig_extract.py execution

```
$ dsig_extract.py -p my_prefix_ test-kdm.xml
$ ls my_prefix_*
my_prefix_1.pem
my_prefix_2.pem
my_prefix_3.pem
my_prefix_4.pem
```

You can test that the certificate has been correctly extracted by using **openssl** to view the contents of the certificate file:

```
$ openssl x509 -text -noout -in <certificate-file.pem>
```

The output from this command should look similar to Example 2.1.

To validate a complete chain of extracted certificates, use the procedure in Section 2.1.16.

## 3.2. Key Delivery Message Example

The Key Delivery Message (KDM) is an XML document that contains cryptographic information necessary to reproduce an encrypted composition. A KDM also contains metadata about the cryptographic information, such as the validity period and the associated Composition Playlist (CPL). The format of the KDM file is specified by [SMPTE-430-1] . A KDM is a type of Extra-Theater Message (ETM), as specified by [SMPTE-430-3] .

The following examples show the elements of the KDM that will be examined during the procedures. Each example is followed by a list of descriptive text that describes the various features of the KDM called out in the examples. These features will be referred to from the test procedures.

## Example 3.6. KDM - AuthenticatedPublic area

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?> 1
<DCinemaSecurityMessage xmlns="http://www.smpte-ra.org/schemas/430-3/2006/ETM" 2
    xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
<AuthenticatedPublic Id="ID_AuthenticatedPublic"> 3
<MessageId>urn:uuid:b80e668c-a175-4bc7-ae48-d3a19c8fce95</MessageId> 4
<MessageType>http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type</MessageType> 5
<AnnotationText>Perfect Movie KDM</AnnotationText> 6
<IssueDate>2007-07-24T17:42:58-00:00</IssueDate> 7
<Signer> 8
  <dsig:X509IssuerName>dnQualifier=wBz3yptkPxbHI/\+LUUeH5R6rQfI=,CN=.cc-admin-x,
      OU=.cc-ra-1a.s430-2.ca.example.com,O=.ca.example.com</dsig:X509IssuerName>
  <dsig:X509SerialNumber>6992</dsig:X509SerialNumber>
</Signer>
<RequiredExtensions>
  <KDMRequiredExtensions xmlns="http://www.smpte-ra.org/schemas/430-1/2006/KDM">
    <Recipient> 9
      <X509IssuerSerial>
        <dsig:X509IssuerName>dnQualifier=wBz3yptkPxbHI/\+LUUeH5R6rQfI=,CN=.cc-admin-x,
          OU=.cc-ra-1a.s430-2.ca.serverco.com,O=.ca.serverco.com</dsig:X509IssuerName>
        <dsig:X509SerialNumber>8992</dsig:X509SerialNumber> 10
      </X509IssuerSerial>
      <X509SubjectName>dnQualifier=83R40icxCejFRR6Ij6iwdf2faTY=,CN=SM.x_Mastering,
        OU=.cc-ra-1a.s430-2.ca.example.com,O=.ca.example.com</X509SubjectName> 11
    </Recipient>
    <CompositionPlaylistId> 12
      urn:uuid:20670ba3-d4c7-4539-ac3e-71e874d4d7d1
    </CompositionPlaylistId>
    <ContentTitleText>Perfect Movie</ContentTitleText> 13
    <ContentKeysNotValidBefore>2007-07-24T17:42:54-00:00</ContentKeysNotValidBefore> 14
    <ContentKeysNotValidAfter>2007-08-23T17:42:54-00:00</ContentKeysNotValidAfter> 15
    <AuthorizedDeviceInfo>
      <DeviceListIdentifier>urn:uuid:d47713b9-cde1-40a9-98fe-22ef172723d0</DeviceListIdentifier>
      <DeviceList> 16
          <CertificateThumbprint>jk4Z8haFhqCGAVbClW65jVSOib4=</CertificateThumbprint> 17
      </DeviceList>
    </AuthorizedDeviceInfo>
    <KeyIdList> 18
      <TypedKeyId>
        <KeyType scope="http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type">MDIK</KeyType> 19
        <KeyId>urn:uuid:15e929b3-1d86-40eb-875e-d21c916fdd3e</KeyId> 20
      </TypedKeyId>
      <TypedKeyId>
          <KeyType scope="http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type">MDAK</KeyType>
          <KeyId>urn:uuid:ca8f7756-8c92-4e84-a8e6-8fab898934f8</KeyId>
      </TypedKeyId>
    [remaining key IDs omitted for brevity]
    </KeyIdList>
    <ForensicMarkFlagList> 21
      <ForensicMarkFlag>
          http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-audio-disable
      </ForensicMarkFlag>
    </ForensicMarkFlagList>
  </KDMRequiredExtensions>
```

```
</RequiredExtensions>
<NonCriticalExtensions/>
</AuthenticatedPublic>
```

1. XML Declaration. This specifies the version of the XML standard to which the document conforms, and the character encoding of the document
2. The root DCinemaSecurityMessage element. This element contains the XML namespace declaration for a KDM as specified in [SMPTE-430-1] .
3. The beginning of the AuthenticatedPublic section of the KDM.
4. The Unique Universal ID (UUID) of the KDM. This is used to uniquely identify the asset map
5. The type of message, in this case a KDM.
6. An annotation text describing the contents or purpose of the KDM.
7. The date the KDM was issued.
8. The portion of the KDM that holds information about the certificate used to sign the KDM.
9. The portion of the KDM that contains information about the recipient (target) certificate.
10. The serial number of the recipient certificate.
11. The Subject Name information from the recipient certificate.
12. The UUID of the CPL used to create the KDM.
13. The ContentTitleText from the CPL used to create the KDM.
14. The starting validity date of the KDM.
15. The ending validity date of the KDM
16. Device list. This list contains the list of certificates thumbprints authorized for use with at least a portion of the KDM.
17. A certificate thumbprint in the device list.
18. The list of KeyIDs and their associated type.
19. The type of key represented by the KeyID.
20. The KeyID.
21. This flag determines whether forensic marking is enabled or disabled. The ForensicMarkFlagList may contain multiple instances of ForensicMarkFlag.

## Example 3.7. KDM - AuthenticatedPrivate area

```
<AuthenticatedPrivate Id="ID_AuthenticatedPrivate"> 1
  <enc:EncryptedKey xmlns:enc="http://www.w3.org/2001/04/xmlenc#"> 2
    <enc:EncryptionMethod
                Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"> 3
      <ds:DigestMethod
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    </enc:EncryptionMethod>
    <enc:CipherData>
    <enc:CipherValue> 4
[256 Byte long encrypted cipherdata block omitted]
</enc:CipherValue>
    </enc:CipherData>
  </enc:EncryptedKey>
  <enc:EncryptedKey xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
    <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
      <ds:DigestMethod
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    </enc:EncryptionMethod>
    <enc:CipherData>
      <enc:CipherValue>
[256 Byte long encrypted cipherdata block omitted]
</enc:CipherValue>
    </enc:CipherData>
```

```
  </enc:EncryptedKey>
  <enc:EncryptedKey xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
    <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
      <ds:DigestMethod
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    </enc:EncryptionMethod>
    <enc:CipherData>
      <enc:CipherValue>
    [ 256 Byte long encrypted cipherdata block omitted]
    </enc:CipherValue>
    </enc:CipherData>
  </enc:EncryptedKey>
  <enc:EncryptedKey xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
    <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
      <ds:DigestMethod
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    </enc:EncryptionMethod>
    <enc:CipherData>
      <enc:CipherValue>
    [ 256 Byte long encrypted cipherdata block omitted]
    </enc:CipherValue>
    </enc:CipherData>
  </enc:EncryptedKey>
  [additional EncryptionKey entries omitted]
</AuthenticatedPrivate>
```

1 The start of the AuthenticatedPrivate section of the KDM

2 The EncryptedKey element indicates there is data encrypted with an RSA public key algorithm.

3 3 The algorithm used to encrypt the data in the CipherData element.

4 A 256 Byte long block of RSA encrypted data.

## Example 3.8. KDM - Signature area

```
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"> 1
<dsig:SignedInfo>
  <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithCom
```

```
2
  <dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /> 3
  <dsig:Reference URI="#ID_AuthenticatedPublic"> 4
    <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /> 5
    <dsig:DigestValue>cnn8M41NR4jQF+9GOZiNJTlfl+C/l8lBFljuCuq9lQE=</dsig:DigestValue> 6
  </dsig:Reference>
  <dsig:Reference URI="#ID_AuthenticatedPrivate"> 7
    <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
    <dsig:DigestValue>TEW7tPwML2iOkIpK2/4rZbJbKgnnXjAtJwe9OJSe8u4=</dsig:DigestValue>
  </dsig:Reference>
</dsig:SignedInfo>
<dsig:SignatureValue>uH41s9odRPXzFz+BF3dJ/myG09cLSE9cLzf2C7f2Fm49P9C53T5RSeEIyqt6p5ll 8
zlH2q3ZJRZcZuV5VA7UkIb4z6U4CGUTU51D8lL/anY1glLFddjUiDU/0nmC4uAsH
rzwQgzOTZmZd2eLo0N70DBtNhTcJZftKUN2O2ybHZaJ7Q/aBxAiCK3h/fRW/b7zM
bcbsD9/VfJFI7VQCOLYwTxq643Exj7sYGKISrjuN+MLAubG50hu74YLOtA/dmGB1
G4VeXkBBR/BEjOEeoxyfFpxbZwkdoI18/Qd1JF32xpE1PlTLrJoRyjrX/6qkm9OJ
X9GyFNd8jVxdYNI4s1JCnQ==</dsig:SignatureValue>
<dsig:KeyInfo> 9
  <dsig:X509Data>
    <dsig:X509IssuerSerial>
      <dsig:X509IssuerName>dnQualifier=wBz3yptkPxbHI/\+LUUeH5R6rQfI=,
CN=.cc-admin-x,OU=.cc-ra-1a.s430-2.ca.example.com,O=.ca.example.com</dsig:X509IssuerName>
      <dsig:X509SerialNumber>6992</dsig:X509SerialNumber>
    </dsig:X509IssuerSerial>
    <dsig:X509Certificate> 10
[PEM encoded certificate omitted]
</dsig:X509Certificate>
  </dsig:X509Data>
  <dsig:X509Data>
    <dsig:X509IssuerSerial>
      <dsig:X509IssuerName>dnQualifier=8O8W8oYHlf97Y8n0kdAgMU7/jUU=,
CN=.s430-2,OU=.ca.example.com,O=.ca.example.com</dsig:X509IssuerName>
      <dsig:X509SerialNumber>50966</dsig:X509SerialNumber>
    </dsig:X509IssuerSerial>
    <dsig:X509Certificate>
[PEM encoded certificate omitted]
</dsig:X509Certificate>
  </dsig:X509Data>
  <dsig:X509Data>
    <dsig:X509IssuerSerial>
      <dsig:X509IssuerName>dnQualifier=8O8W8oYHlf97Y8n0kdAgMU7/jUU=,
CN=.s430-2,OU=.ca.example.com,O=.ca.example.com</dsig:X509IssuerName>
      <dsig:X509SerialNumber>13278513546878383468</dsig:X509SerialNumber>
    </dsig:X509IssuerSerial>
    <dsig:X509Certificate>
[PEM encoded certificate omitted]
</dsig:X509Certificate>
  </dsig:X509Data>
</dsig:KeyInfo>
</dsig:Signature></DCinemaSecurityMessage>
```

1 Start of the signature section of the KDM

2 The canonicalization algorithm of the signature

3 Specifies the signature algorithm (RSA) and the digest algorithm (SHA-256) of the signature.

4 The AuthenticatedPublic reference element

5 The method used to create the digest of the AuthenticatedPublic portion of the KDM

6 The digest of the AuthenticatedPublic portion of the KDM

7 The AuthenticatedPrivate reference element

8 The RSA encrypted form of the two digests

9 The section of the signature portion that contains the singer certificate and its certificate chain

10 The certificate used to sign the KDM

Since the KDM carries encrypted data, a tool that can decrypt the encrypted portions of the KDM has been provided in Section C.1. **kdm-decrypt** takes two arguments, a KDM and the RSA private key that corresponds to the certificate to which the KDM was

targeted, and displays the contents of the encrypted section. Here is an example of **kdm-decrypt** and the resulting output:

### Example 3.9. kdm-decrypt Usage and Output

```
$ kdm-decrypt <kdm-file>
  <rsa-private-key.pem>
    CipherDataID: f1dc124460169a0e85bc300642f866ab (1)
  SignerThumbprint: q5Oqr6GkfG6W2HzcBTee5m0Qjzw= (2)
              CPL Id: 119d8990-2e55-4114-80a2-e53f3403118d (3)
              Key Id: b6276c4b-b832-4984-aab6-250c9e4f9138 (4)
            Key Type: MDIK (5)
          Not Before: 2007-09-20T03:24:53-00:00 (6)
            Not After: 2007-10-20T03:24:53-00:00 (7)
              Key Data: 7f2f711f1b4d44b83e1dd1bf90dc7d8c (8)
```

(1) The CipherData ID. This value is defined in [SMPTE-430-1]
(2) Thumbprint of the certificate that signed the KDM
(3) The UUID of the CPL associated with this KDM
(4) The KeyID that corresponds to the key contained in this EncryptedKey cipherblock
(5) The type of key contained in this EncryptedKey cipherblock
(6) The beginning of validity period of the key
(7) The end of validity period of the key
(8) The encryption key

## 3.3. ETM Features

### 3.3.1. ETM Structure

#### Objective

Verify that the ETM portion of the KDM validates against the ETM schema in [SMPTE-430-3] .

#### Procedures

To verify that the ETM defined elements of the KDM are well formed, validate the KDM against the ETM schema in [SMPTE-430-3], use the procedure described in Section 1.4, *i.e.*,

```
$ schema-check smpte-430-3.xsd <input-file>
schema validation successful
```

If the KDM is not valid or well formed, the program will report an error. A reported error is cause to fail this test.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-3 |
| **Test Equipment** | **schema-check**<br>**Text Editor** |

## 3.3.2. ETM Validity Date Check

### Objective

Verify that the signer's certificate chain was valid at the date specified in the `<IssueDate>` element in the `<AuthenticatedPublic>` area of the KDM.

### Procedures

1. Extract each of the certificates in the signer's certificate chain from the KDM using a **Text Editor**, then, using the process described in Section 2.1.16: Signature Validation, validate the certificate chain. Validation failure of the certificate chain is cause to fail this test.

2. Once the certificate chain has been successfully validated, view the signer certificate in text form using the openssl command as described in Example 2.1.. Locate the `Validity` section of the certificate as indicated by 6 in the example certificate.

3. Using a **Text Editor**, view the contents of the KDM and locate the `<IssueDate>`; element as shown in 7 of Example 3.6..

4. Compare the `Not Before` and `Not After` values of the signer certificate to the date in the <IssueDate> element of the KDM and confirm that it is within the date range. An `<IssueDate>` value outside the date ranges of the certificate is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8 |
| **Test Equipment** | **Text Editor**<br>**openssl** |

## 3.3.3. ETM Signer Element

### Objective

Verify that the certificate chain in the `<Signer>` element of the KDM is valid.

### Procedures

1. Extract each of the certificates in the signer's certificate chain from the KDM using a **Text Editor** as described in Section 1.4.

2. Using the process described in Section 2.1.16: Signature Validation, validate the certificate chain. Validation failure of the certificate chain is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8 |

| | |
|---|---|
| SMPTE-430-1<br>SMPTE-430-2 | **Test Equipment** |
| **Text Editor**<br>**openssl** | |

## 3.3.4. ETM EncryptionMethod Element

### Objective

Verify that the `Algorithm` attribute of the `<EncryptionMethod>` for the encrypted key has the value `"http://www.w3.org/2001/04/xmlenc#rsaoaep-mgf1p"`.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the `Algorithm` attribute of the `<EncryptionMethod>` element in the `<AuthenticatedPrivate>` element for each of the encrypted keys, as indicated by 3 in the example KDM, is `"http://www.w3.org/2001/04/xmlenc#rsaoaep-mgf1p"`. Any other value in this attribute is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.3.5. ETM AnnotationText Language

### Objective

Verify that the content of the `<AnnotationText>` element is in a human-readable language. If the optional `xml:lang` attribute is present, the language must match. If the `xml:lang` attribute is not present, the language must be English.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the `<AnnotationText>` element as indicated by 6 in the Example 3.6. is a human-readable language. The presence of non-human-readable data or text in a language other than English without that language's corresponding `xml:lang` value is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.3.6. ETM ReferenceList Element

### Objective

Verify that the <ReferenceList> element of the <EncryptedKey> element is not present.

### Procedures

Using a **Text Editor**, view the KDM and confirm that, for each instance of the <EncryptedKey> element, the <ReferenceList> element is not present. The presence of the <ReferenceList> element indicates that the KDM is malformed and is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.3.7. ETM SignedInfo CanonicalizationMethod Element

### Objective

Verify that the value of the Algorithm attribute of the <CanonicalizationMethod> element of the <SignedInfo> element in the <Signature> area of the KDM is "http://www.w3.org/TR/2001/RECxml-c14n-20010315#WithComments".

### Procedures

Using a **Text Editor**, view the KDM and confirm that the value of the Algorithm attribute of the <CanonicalizationMethod> of the <SignedInfo> element of the <Signature> element is "http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments", as shown in 2 of Example 3.8.. Any other value in this attribute is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.3.8. ETM Signature Reference Elements

### Objective

Verify that the <SignedInfo> element of the <Signature> area of the KDM contains at least two child <Reference> elements. The value of the URI attribute of each <Reference> element must correspond to the respective ID attribute of the digested element. Verify that the URI attribute of one of the <Reference> element identifies the AuthenticatedPublic portion of the KDM. Verify that the URI attribute of one of the <Reference>; element identifies the AuthenticatedPrivate portion of the KDM.

### Procedures

1. Using a **Text Editor**, view the KDM and confirm that the <SignedInfo> element of the <Signature> area of the KDM has at least two child <Reference> elements as shown in 4 and 7 of Example 3.8. The presence of fewer than two <Reference> elements is cause to fail this test.

2. Confirm that the URI attribute of one of the <Reference> element matches the value of the ID attribute of the AuthenticatedPublic element, as shown by 4 in Example 3.8. and 3 in Example 3.6: KDM - AuthenticatedPublic

area. The absence of this association in the KDM is cause to fail this test.

3. Confirm that the `URI` attribute of one of the `<Reference>` element matches the value of the `ID` attribute of the `AuthenticatedPrivate` element, as shown by 7 in Example 3.8. and 1 in Example 3.7.. The absence of this association in the KDM is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.3.9. ETM SignatureMethod Element

### Objective

Verify that the `<SignatureMethod>` element of the `<SignedInfo>` element of the `<Signature>` area of the KDM contains the URI value `"http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"`.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the `<SignatureMethod>` element of the `<SignedInfo>` element of the `<Signature>` section of the KDM contains the URI value `"http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"`, as shown in 3 of Example 3.8.. Any other value is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.3.10. ETM Signature Transforms Field

### Objective

Verify that `<Reference>` elements of the `<SignedInfo>` element in the `<Signature>` section of the KDM do not contain a `Transforms` attribute.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the `<Reference>` elements of the `<SignedInfo>` element in the `<Signature>` section of the KDM do not contain a `Transforms` attribute. The presence of the `Transforms` attribute is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1<br>SMPTE-430-3 |
| **Test Equipment** | **Text Editor** |

## 3.3.11. ETM Signature DigestMethod Element

### Objective

Verify that the value of the `Algorithm` attribute of the `<DigestMethod>` element of each of the `<Reference>` elements in the `<SignedInfo>` element of the `<Signature>` section of the KDM is `" http:// www.w3.org/2001/04/xmlenc#sha256"`.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the value of the `Algorithm` attribute of the `<DigestMethod>` element of each of the `<Reference>` elements is `"http://www.w3.org/2001/04/xmlenc#sha256"`, as shown in **5** of Example 3.8.. Any other value is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-3 |
| **Test Equipment** | **Text Editor** |

## 3.3.12. ETM Signature Validity

### Objective

Verify that the signature is properly formed, *i.e.*, the `<Signature>` element is properly encoded, all digests are properly formed, the `<SignatureMethod>` and `<CanonicalizationMethod>` in the `<SignedInfo>` element are correct, and the `<Reference>` values are correct. Verify that the signature is valid.

### Procedures

Verifying that the signature is well formed (the XML structure is correct) and that the signature is valid (is properly encoded) can be done by verifying the signature XML against the schema using a validating XML parser, then validating the signature.

1. Using the schema validating tool **schema-check**, validate the KDM against the schema found in [SMPTE-430-3] as described in Section 1.4, *i.e.*,

   ```
   $ schema-check <input-file> smpte-430-3.xsd
   schema validation successful
   ```

   If the KDM is not valid or well formed, the program will report an error. A reported error is reason to fail this test.

2. Using the **checksig** program, verify that there is a signature included in the KDM and that it is valid. A missing or invalid signature is cause to fail this test. Note: Depending on the order of the certificates contained in the log report, the **dsig_cert.py** program may need to be used to re-order the certificates for the **checksig** program.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-3 |
| **Test Equipment** | **Text Editor**<br>**schema-check**<br>**checksig** |

| dsig_cert.py |
|---|

# 3.4. KDM Features

## 3.4.1. KDM MessageType Element

### Objective

Verify that the `<MessageType>` element of the KDM contains the string `"http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type"`

### Procedures

Using a **Text Editor**, view the KDM and confirm that the `<MessageType>` element of the KDM contains the string `"http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type"` as shown in 5 of Example 3.6.. Any other value in this element is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.4.2. KDM SubjectName Element

### Objective

Verify that the Subject Name of the recipient X.509 certificate (target certificate) is identical to the value of the `<SubjectName>` element of the `<Recipient>` element of the `<KDMRequiredExtensions>` element in the KDM.

### Procedures

Comparison of the Subject Name of the certificate against the content of the SubjectName element can be achieved by viewing the text version of the certificate and comparing it to the KDM element to verify they are the same.

1. Using the method described in Example 2.1., view the text information of the certificate and identify the X.509 subject name as shown in 9 .

2. Using a **Text Editor**, view the contents of the KDM and identify the `<SubjectName>` of the `<Recipient>` element as shown in 11 .

3. Confirm that the value of the <SubjectName>element is the same as the Subject Name of the certificate. Differing values are cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1<br>SMPTE-430-2 |
| **Test Equipment** | **Text Editor**<br>**openssl** |

## 3.4.3. KDM ContentAuthenticator Element

### Objective

Verify that, when present, the `<ContentAuthenticator>` element of the `<KDMRequiredExtensions>` element of the KDM contains one of the certificate thumbprints of one of the certificates in the chain of the signer of the CPL.

### Procedures

If the element exists in the KDM:

1. Using **Text Editor**, view value of the `<ContentAuthenticator>` element of the `<KDMRequiredExtensions>` element of the KDM. If the element is not present, this test is considered passed and the remaining procedure steps are not performed.

2. Extract the certificates from the CPL signature. Note: This may be accomplished using the **dsig_extract.py** program.

3. Using **dc-thumbprint**, calculate the thumbprint each of the certificates:

```
$ dc-thumbprint <certificate.pem>
```

4. Confirm that the `<ContentAuthenticator>` value matches one of the thumbprints of the certificate chain of the signer certificate.

Presence of the `<ContentAuthenticator>` with a value that does not match one of the thumbprints is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-429-7<br>SMPTE-430-1 |
| **Test Equipment** | **dc-thumbprint**<br>**Text Editor** |

## 3.4.4. KDM Signer Certificate Presence

### Objective

Verify that the certificate that signed the KDM is present in one of the `<X509Data>` elements of the `<KeyInfo>` elements in the signature portion of the KDM.

### Procedures

Testing that the certificate that signed the KDM is present in an `<X509Data>` element can be achieved by validating the signature. If the validation is successful then the certificate that signed the KDM is present. The signature can be validated using the **dsig_cert.py** and **checksig** commands:

Example:

```
$ dsig_cert.py <kdm-file.kdm.xml> > tmp.xml
$ checksig tmp.xml
```

A KDM that causes **checksig** to display errors indicates that the signature did not validate and shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor**<br>**checksig**<br>**dsig_cert.py** |

## 3.4.5. KDM KeyIdList/TypedKeyId Field

### Objective

Verify that `<TypedKeyId>` element of the `<KeyIdList>` element in the `<KDMRequiredExtensions>` element is well formed. Verify that the element contains one of the following values: `MDIK, MDAK, MDSK, FMIK,` or `FMAK`.

### Procedures

To complete this test, validate the KDM against the schema in [SMPTE-430-1], then verify that one of the required values is present in the element.

1. Validate the KDM against the schema in [SMPTE-430-1] using the procedure described in Section 1.4, *i.e.*,

   ```
   $ schema-check <kdm-file.kdm.xml> smpte-430-1.xsd
   schema validation successful
   ```

   If the KDM is not valid or well formed, the program will report an error. A reported error is cause to fail this test.

2. Using a **Text Editor**, view the value of the `<TypedKeyId>` element, and verify that the element contains one of: `MDIK, MDAK, MDSK, FMIK,` or `FMAK`, as shown in 19 of Example 3.6. Any other value in this element is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor**<br>**schema-check** |

## 3.4.6. KDM ForensicMarkFlagList Element

### Objective

Verify that, if present, the `<ForensicMarkFlagList>` element contains a list of one or both of the following two URIs:

- `http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-picture-disable`
- `http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-audio-disable`

### Procedures

Using a **Text Editor**, view the KDM and confirm the presence of the `<ForensicMarkFlagList>` element. The absence of the element is cause to pass this test and the remainder of this procedure can be skipped. If present, the element must contain one or both of the following URI values:

- `http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-picture-disable`
- `http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-audio-disable`

as shown by 21 of Example 3.6. The presence of the element with any other value, or no value, is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.4.7. KDM EncryptedData Element

### Objective

Verify that element `<EncryptedData>` is not present.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the `<EncryptedData>` element is not present. The presence of the element is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.4.8. KDM KeyInfo Element

### Objective

If present, verify that the values of each <KeyInfo> element of all <EncryptedKey> elements in the <AuthenticatedPrivate> section of the KDM are identical.

### Procedures

Using a **Text Editor**, view the KDM and, if present, confirm that the <KeyInfo> values are identical in all instances of <EncryptedKey> elements. The absence of <KeyInfo> elements is cause to pass this test. The presence of differing <KeyInfo> values in <EncryptedKey> elements is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.4.9. KDM DeviceListDescription Element

### Objective

Verify that when present, the value of the <DeviceListDescription> element is in a human-readable language. If the optional xml:lang attribute is present, the language must match. If the xml:lang attribute is not present, the language must be English.

### Procedures

See Objective.

Using a **Text Editor**, view the KDM and confirm that the <DeviceListDescription> element is either absent or is present and contains human-readable text. The presence of non-human-readable data or text in a language other than English without that language's corresponding xml:lang value is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.4.10. KDM ContentTitleText Language Attribute

### Objective

Verify that value of the <ContentTitleText> element is in a human-readable language. If the optional xml:lang attribute is present, the language must match. If the xml:lang attribute is not present, the language must be English.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the <ContentTitleText> element as indicated by 13 in the Example 3.6. is a human-readable language. The presence of non-human-readable data or text in a language other than English without that language's corresponding xml:lang value is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

## 3.4.11. KDM KeyType Scope Attribute

### Objective

Verify that the optional `scope` attribute of the `<TypedKeyId>` element of the `<KeyIdList>` element is absent or contains the value `http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type`.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the scope attribute of the `<TypedKeyId>` element is either not present or is present and contains the value `http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type`, as shown in 19 of Example 3.6. Presence of the scope attribute with any other value is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1<br>SMPTE-430-3 |
| **Test Equipment** | **Text Editor** |

## 3.4.12. KDM EncryptionMethod

### Objective

Verify that the `Algorithm` attribute of the `<EncryptionMethod>` element of the `<EncryptedKey/>` element has the value `"http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"`.

### Procedures

Using a **Text Editor**, view the KDM and confirm that the `Algorithm` attribute of the `<EncryptionMethod>` of the `<EncryptedKey/>` element contains the value `http://www.w3.org/2001/04/xmlenc#rsa-oaepmgf1p`, as shown in 3 of Example 3.7.. Presence of the `Algorithm` attribute with any other value is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1<br>SMPTE-430-3 |
| **Test Equipment** | **Text Editor**<br>**openssl** |

## 3.4.13. KDM CompositionPlaylistId Element

### Objective

Verify that the value of the <CompositionPlaylistId> element in the KDM matches the value in the RSA protected <EncryptedKey> structure, and that these values match the value of the <Id> element in the respective composition playlist.

### Procedures

The data in the encrypted portion of the KDM can be viewed using the **kdm-decrypt** tool included in Section C.1. To view the data contained in the encrypted section of the KDM, run the command specifying the KDM and the RSA private key corresponding to the certificate to which the KDM was targeted, *i.e.*,

```
$ kdm-decrypt <kdm-file> <rsa-private-key.pem>
```

Verify that the <CompositionPlaylistId> element of the <KDMRequiredExtensions> element in the plaintext portion of the KDM contains the same value as the CPL ID present in the RSA protected <EncryptedKey> structure. Non-identical values shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-429-7<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor**<br>**kdm-decrypt** |

## 3.4.14. KDM Validity Fields

### Objective

Verify that value of the <ContentKeysNotValidBefore> and <ContentKeysNotValidAfter> elements match their counterparts in the RSA protected <EncryptedKey> structure and that the values are in UTC format.

### Procedures

The information in the encrypted portion of the KDM can be viewed using the **kdm-decrypt** tool included in Section C.1. To view the data contained in the encrypted section of the KDM, run the command specifying the KDM and the RSA private key corresponding to the certificate to which the KDM was targeted, *i.e.*,

```
$ kdm-decrypt <kdm-file> <rsa-private-key.pem>
```

Verify that the <ContentKeysNotValidBefore> element of the <KDMRequiredExtensions> element has the same value as the corresponding field inside the RSA protected EncryptedKey structure, and that it is in UTC format as specified in [RFC-3339]. Non-identical values shall be cause to fail this test.

Verify that the <ContentKeysNotValidAfter> element of the <KDMRequiredExtensions> element has the same value as the corresponding field inside the RSA protected EncryptedKey structure, and that it is in UTC format as specified in [RFC-3339]. Non-identical values shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>RFC-3339<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor**<br>**openssl** |

## 3.4.15. KDM KeyIdList Element

### Objective

Verify that each of the KeyID values in the `<KeyIdList>` element of the `<KDMRequiredExtensions>` element matches a KeyID in the RSA protected `<EncryptedKey>` structure and that there are no KeyIDs without corresponding `<EncryptedKey>` structures, nor `<EncryptedKey>` structures with KeyIDs that are not present in the KeyIDList.

### Procedures

The data in the encrypted portion of the KDM can be viewed using the **kdm-decrypt** tool included in Section C.1. To view the data contained in the encrypted section of the KDM, run the command specifying the KDM and the RSA private key corresponding to the certificate to which the KDM was targeted, *i.e.*,

```
$ kdm-decrypt <kdm-file> <rsa-private-key.pem>
```

Compare the list of KeyIDs to the KeyIDs in the RSA protected EncryptedKey structures and verify that each of the KeyIDs in the list correspond to a KeyID in an RSA protected EncryptedKey structure. The presence of KeyIDs in the KeyIDList that do not correspond to a KeyID in an RSA protected EncryptedKey structure shall be cause to fail this test. The presence of a KeyID in an RSA protected EncryptedKey structure that is not also present in the KeyIDList shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **kdm-decrypt**<br>**Text Editor** |

## 3.4.16. KDM CipherData Structure ID

### Objective

Verify that the value of the CipherData Structure ID in the RSA protected `<EncryptedKey>` structure is `f1dc124460169a0e85bc300642f866ab`.

### Procedures

The data in the encrypted portion of the KDM can be viewed using the **kdm-decrypt** tool included in Section C.1. To view the data contained in the encrypted section of the KDM, run the command specifying the KDM and the RSA private key corresponding to the certificate to which the KDM was targeted, *i.e.*,

```
$ kdm-decrypt <kdm-file> <rsa-private-key.pem>
```

Verify that the plaintext value of the CipherData Structure ID is `f1dc124460169a0e85bc300642f866ab`. Any other value shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |

| | |
|---|---|
| **Test Equipment** | **kdm-decrypt** |

## 3.4.17. KDM CipherData Signer Thumbprint

### Objective

Verify that the thumbprint of the signer's certificate in the RSA protected `<EncryptedKey>` element matches the thumbprint of the certificate that signed the KDM.

### Procedures

The data in the encrypted portion of the KDM can be viewed using the **kdm-decrypt** tool included in Section C.1. To view the data contained in the encrypted section of the KDM, run the command specifying the KDM and the RSA private key corresponding to the certificate to which the KDM was targeted, *i.e.*,

```
$ kdm-decrypt <kdm-file> <rsa-private-key.pem>
```

A certificate thumbprint can be calculated using the **dc-thumbprint** tool included in Section C.1. Calculate the thumbprint with **dc-thumbprint**, *i.e.*,

```
$dc-thumbprint <certificate.pem>
```

Identify the certificate used to sign the KDM and calculate its thumbprint. Compare this thumbprint against the thumbprint decrypted from the `<EncryptedKey>` element and confirm that they are the same. Non-identical values shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1<br>SMPTE-430-2 |
| **Test Equipment** | **dc-thumbprint**<br>**kdm-decrypt**<br>**Text Editor** |

## 3.4.18. KDM CipherData Validity

### Objective

Verify that the two CipherData validity fields contain UTC format time values.

### Procedures

The data in the encrypted portion of the KDM can be viewed using the **kdm-decrypt** tool included in Section C.1. To view the data contained in the encrypted section of the KDM, run the command specifying the KDM and the RSA private key corresponding to the certificate to which the KDM was targeted, *i.e.*,

```
$ kdm-decrypt <kdm-file> <rsa-private-key.pem>
```

Verify that the plaintext representation of the `<EncryptedKey>` element contains two validity time stamps in UTC format. Time stamps that are not present or that are not in UTC format shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor**<br>**kdm-decrypt** |

## 3.4.19. KDM CipherData CPL ID

### Objective

Verify that the CipherData Composition Playlist ID is identical to the value of the `<CompositionPlaylistId>` element in the other portions of the KDM.

### Procedures

The data in the encrypted portion of the KDM can be viewed using the **kdm-decrypt** tool included in Section C.1. To view the data contained in the encrypted section of the KDM, run the command specifying the KDM and the RSA private key corresponding to the certificate to which the KDM was targeted, *i.e.*,

```
$ kdm-decrypt <kdm-file> <rsa-private-key.pem>
```

Verify that the decrypted plaintext value of the CompositionPlaylistID the same as the `<CompositionPlaylistId>` element in the AuthenticatedPublic area of the KDM. Mismatching composition playlist IDs shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor**<br>**openssl** |

## 3.4.20. KDM EncryptedKey KeyType

### Objective

Verify that the key types in the `<EncryptedKey>` elements of the KDM use only the allowed key types (`MDIK, MDAK, MDSK, FMIK` and `FMAK`), and that they match the plaintext fields in the `<TypedKeyId>` element values for the KeyIDs in the `<KeyIdList>` element.

### Procedures

The data in the encrypted portion of the KDM can be viewed using the **kdm-decrypt** tool included in Section C.1. To view the data contained in the encrypted section of the KDM, run the command specifying the KDM and the RSA private key corresponding to the certificate to which the KDM was targeted, *i.e.*,

```
$ kdm-decrypt <kdm-file> <rsa-private-key.pem>
```

For each `<EncryptedKey>` element, verify that the plaintext representation contains a key type that is one of `MDIK, MDAK, MDSK, FMIK` or `FMAK`, and that the key type is identical to the key type for the corresponding KeyID in the KeyIDList. A key type that is not either `MDIK, MDAK, MDSK, FMIK` or `FMAK` shall be cause to fail this test. A key type in the `<EncryptedKey>` element that does not match the key type for the corresponding KeyID in the KeyIDList shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | SMPTE-430-1 |
| **Test Equipment** | **Text Editor**<br>**kdm-decrypt** |

## 3.4.21. KDM Recipient X509IssuerName

### Objective

Verify that the Distinguished Name value in the `<X509IssuerName>` element is compliant with [RFC-2253].

### Procedures

Using a **Text Editor**, view the KDM and confirm that the `<X509IssuerName>` element as shown below 8 of Example 3.6.. Verify that any special characters are properly escaped, and the sequence is correct and valid. Improperly escaped characters or sequences that do not conform to [RFC-2253] shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | RFC-2253<br>SMPTE-430-1 |
| **Test Equipment** | **Text Editor** |

# 3.5. KDM Decoder Behavior

The procedures in this section test the behavior of a KDM decoding device, such as a Security Manager (SM) or a KDM authoring device. The procedures use a generic syntax to instruct the test operator to cause the Test Subject to decode a KDM.

In the case of an SM, the text "Perform an operation..." should be interpreted to mean "Assemble and play a show with *DCI 2K StEM (Encrypted)...*".

In the case of a KDM authoring device, the text "Perform an operation..." should be interpreted to mean "Perform a KDM read or ingest operation...".

**Note:**
Some of the procedures in this section require test content that is specifically malformed. In some implementations, these malformations may be caught and reported directly by the SMS without involving the SM. Because the purpose of the procedures is to assure that the SM demonstrates the required behavior, the manufacturer of the Test Subject may need to provide special test programs or special SMS testing modes to allow the malformed content to be applied directly to the SM.

## 3.5.1. KDM NonCriticalExtensions Element

### Objective

Verify that a decoding device does not reject a KDM when the `<NonCriticalExtensions>` element is present and not empty.

### Procedures

Perform an operation on the Test Subject using *KDM with non-empty NonCriticalExtensions*, a KDM that contains the `<NonCriticalExtensions>` element with child content. Verify that the operation is successful. A failed operation shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with non-empty NonCriticalExtensions*<br>*DCI 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 3.5.2. ETM IssueDate Field Check

### Objective

- Verify that the Test Subject verifies that the signer's certificate is valid at the time when the KDM was issued.
- Verify that the Test Subject verifies that the KDM validity does not extend beyond the ending validity period of the certificate.

### Procedures

For each of the malformations below, perform an operation on the Test Subject using the test material that has that malformation. Verify that the operation fails. A successful operation is cause to fail this test.

1. KDM in which the certificate that signed the KDM has an ending validity date prior to the KDM issue date (*KDM with expired Signer certificate*).

2. KDM in which the certificate that signed the KDM has a starting validity date after the KDM issue date (*KDM issued before certificate valid*).

3. KDM in which the validity period extends beyond the end of the signing certificate's validity period (*KDM validity exceeds signer validity*).

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with expired Signer certificate*<br>*KDM issued before certificate valid*<br>*KDM validity exceeds signer validity*<br>*DCI 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 3.5.3. Deleted Section

The section "Maximum Number of DCP Keys" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 3.5.4. Structure ID Check

### Objective

Verify that the Test Subject checks the validity of the CipherData Structure ID as specified in [SMPTE-430-1] and rejects the KDM if the Structure ID is incorrect.

### Procedures

Perform an operation on the Test Subject using *KDM with corrupted CipherData block*, a KDM with an invalid CipherData Structure. Verify that the operation fails. A successful operation is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with corrupted CipherData block* |

| |
|---|
| *DCI 2K StEM*<br>*(Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 3.5.5. Certificate Thumbprint Check

### Objective

Verify that the Test Subject checks that the thumbprint of the signer's certificate matches the signer of the KDM and rejects the KDM if it does not.

### Procedures

Perform an operation on the Test Subject using the KDM with a signer's certificate whose thumbprint does not match the thumbprint of the certificate used to sign the KDM (*KDM with incorrect signer thumbprint*). Verify that the operation fails. A successful operation is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with incorrect signer thumbprint*<br>*DCI 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 3.5.6. Deleted Section

The section "Certificate Presence Check" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 3.5.7. KeyInfo Field Check

### Objective

Verify that when `KeyInfo` elements are present in the `<EncryptedKey>` elements of the `<AuthenticatedPrivate>` area of the KDM, the Test Subject verifies that they all match, and that the Test Subject rejects the KDM if they do not match.

### Procedures

Perform an operation on the Test Subject using the KDM with KeyInfo element values that do not match (*KDM with KeyInfo mismatch*). Verify that the operation fails. A successful operation is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with KeyInfo mismatch*<br>*DCI 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 3.5.8. KDM Malformations

### Objective

Verify that the SM checks that the KDM is well formed and labeled with the correct namespace name.

### Procedures

1. Perform an operation on the Test Subject using *KDM with invalid XML*, which contains XML that is not well-formed. If the operation succeeds this is cause to fail this test.

2. Perform an operation on the Test Subject using *KDM with invalid MessageType*, which contains an incorrect ETM `<MessageType>` value. If the operation succeeds this is cause to fail this test.

3. Perform an operation on the Test Subject using *KDM with expired Signer certificate*, which contains a KDM whose signing certificate has expired. If the operation succeeds this is cause to fail this test.

4. Perform an operation on the Test Subject using *KDM with incorrect namespace name value*, which contains an incorrect ETM namespace name. If the operation succeeds this is cause to fail this test.

5. Perform an operation on the Test Subject using *KDM with empty TDL*, which contains a TDL with no entries. If the operation succeeds this is cause to fail this test.

6. Extract a security log from the Test Subject and using a **Text Editor**, identify the `KDMKeysReceived` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. For the log record produced by the operation using *KDM with invalid MessageType*, verify that the value of the `SignerID` parameter contains the Certificate Thumbprint of the signing certificate of *KDM with invalid MessageType*. Verify that `ReferencedIDs` element contains a `KeyDeliveryMessageID` parameter with a value that is the `MessageId` of *KDM with invalid MessageType*. Failure of any verification shall be cause to fail this test.

    c. For the log record produced by the operation using *KDM with expired Signer certificate*, verify that the `contentId` element contains the `Id` of *DCI 2K StEM (Encrypted)*. Verify that the value of the `SignerID` parameter contains the Certificate Thumbprint of the signing certificate of *KDM with expired Signer certificate*. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of *DCI 2K StEM (Encrypted)* and `KeyDeliveryMessageID` parameter with a value that is the `MessageId` of *KDM with expired Signer certificate*. Failure of any verification shall be cause to fail this test.

    d. Confirm the presence of a `KDMFormatError` exception in each `KDMKeysReceived` log record. Record any additional parameters associated with the exception. A missing `KDMFormatError` exception in any of the associated `KDMKeysReceivedlog` records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.8, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3<br>SMPTE-430-5 |
| **Test Materials** | *KDM with empty TDL*<br>*KDM with expired Signer certificate*<br>*KDM with invalid XML*<br>*KDM with invalid MessageType*<br>*KDM with incorrect namespace name value*<br>*DCI 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 3.5.9. KDM Signature

### Objective

Verify that the Test Subject checks that the KDM signature is valid, including checking that the certificate that signed the KDM is included in the KDM and rejecting the KDM if it is not.

### Procedures

1. Perform an operation on the Test Subject using *KDM with incorrect message digest*. The KDM *KDM with incorrect message digest* is invalid (wrong signature/hash error). If the operation succeeds this is cause to fail this test.

2. Perform an operation on the Test Subject using *KDM with incorrect signer thumbprint*. The KDM *KDM with incorrect signer thumbprint* is invalid (wrong signature identity). If the operation succeeds this is cause to fail this test.

3. Perform an operation on the Test Subject using *KDM without signer certificate*. The KDM *KDM without signer certificate* is invalid (broken certificate chain). If the operation succeeds this is cause to fail this test.

4. Extract a security log from the Test Subject and using a **Text Editor**, identify the `KDMKeysReceived` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of *DCI 2K StEM (Encrypted)*. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of *DCI 2K StEM (Encrypted)* and `KeyDeliveryMessageID` parameter with a value that is the `MessageId` of the KDM used. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. For the log records produced by the operation using *KDM with incorrect message digest* and *KDM with incorrect signer thumbprint*, verify that the value of the `SignerId` parameter contains the Certificate Thumbprint of the signing certificate of the KDM.

    c. Confirm the presence of a `SignatureError` exception in each `KDMKeysReceived` log record. Record any additional parameters associated with the exception. A missing `SignatureError` exception in any of the associated `KDMKeysReceived` log records shall be cause to fail this test.

5. Perform an operation on the Test Subject using *KDM signed with incorrect signer certificate format*. The KDM *KDM signed with incorrect signer certificate format* is invalid (wrong signer certificate format). If the operation succeeds this is cause to fail this test.

6. Extract a security log from the Test Subject and using a **Text Editor**, identify the `KDMKeysReceived` event associated with the above step and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of *DCI 2K StEM (Encrypted)*. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of *DCI 2K StEM (Encrypted)* and `KeyDeliveryMessageID` parameter with a value that is the `MessageId` of the KDM used. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `CertFormatError` exception in the `KDMKeysReceived` log record. Record any additional parameters associated with the exception. A missing `CertFormatError` exception in the associated `KDMKeysReceived` log record shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1 |

| | |
|---|---|
| SMPTE-430-3<br>SMPTE-430-5 | **Test Materials** |
| *KDM with incorrect message digest*<br>*KDM with incorrect signer thumbprint*<br>*KDM without signer certificate*<br>*KDM signed with incorrect signer certificate format*<br>*DCI 2K StEM (Encrypted)* | |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 3.5.10. KDM NonCriticalExtensions Element (OBAE)

### Objective

Verify that a decoding device does not reject a OBAE-capable KDM when the `<NonCriticalExtensions>` element is present and not empty.

### Procedures

Perform an operation on the Test Subject using *KDM with non-empty NonCriticalExtensions (OBAE)*, a KDM that contains the `<NonCriticalExtensions>` element with child content. Verify that the operation is successful. A failed operation shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with non-empty NonCriticalExtensions (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 3.5.11. ETM IssueDate Field Check (OBAE)

### Objective

- Verify that the OBAE-capable Test Subject verifies that the signer's certificate is valid at the time when the KDM was issued.

- Verify that the OBAE-capable Test Subject verifies that the KDM validity does not extend beyond the ending validity period of the certificate.

### Procedures

For each of the malformations below, perform an operation on the Test Subject using the test material that has that malformation. Verify that the operation fails. A successful operation is cause to fail this test.

1. KDM in which the certificate that signed the KDM has an ending validity date prior to the KDM issue date (*KDM with expired Signer certificate (OBAE)*).

2. KDM in which the certificate that signed the KDM has a starting validity date after the KDM issue date (*KDM issued before certificate valid (OBAE)*).

3. KDM in which the validity period extends beyond the end of the signing certificate's validity period (*KDM validity exceeds signer validity (OBAE)*).

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with expired Signer certificate (OBAE)*<br>*KDM issued before certificate valid (OBAE)*<br>*KDM validity exceeds signer validity (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 3.5.12. Structure ID Check (OBAE)

### Objective

Verify that the OBAE-capable Test Subject checks the validity of the CipherData Structure ID as specified in [SMPTE-430-1] and rejects the KDM if the Structure ID is incorrect.

### Procedures

Perform an operation on the Test Subject using *KDM with corrupted CipherData block (OBAE)*, a KDM with an invalid CipherData Structure. Verify that the operation fails. A successful operation is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with corrupted CipherData block (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 3.5.13. Certificate Thumbprint Check (OBAE)

### Objective

Verify that the OBAE-capable Test Subject checks that the thumbprint of the signer's certificate matches the signer of the KDM and rejects the KDM if it does not.

### Procedures

Perform an operation on the Test Subject using the KDM with a signer's certificate whose thumbprint does not match the thumbprint of the certificate used to sign the KDM (*KDM with incorrect signer thumbprint (OBAE)*). Verify that the operation fails. A successful operation is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with incorrect signer thumbprint (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 3.5.14. KeyInfo Field Check (OBAE)

### Objective

Verify that when `KeyInfo` elements are present in the `<EncryptedKey>` elements of the `<AuthenticatedPrivate>` area of the KDM, the OBAE-capable Test Subject verifies that they all match, and that the OBAE-capable Test Subject rejects the KDM if they do not match.

### Procedures

Perform an operation on the Test Subject using the KDM with KeyInfo element values that do not match (*KDM with KeyInfo mismatch (OBAE)*). Verify that the operation fails. A successful operation is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3 |
| **Test Materials** | *KDM with KeyInfo mismatch (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 3.5.15. KDM Malformations (OBAE)

### Objective

Verify that the OBAE-capable SM checks that the KDM is well formed and labeled with the correct namespace name.

### Procedures

1. Perform an operation on the Test Subject using *KDM with invalid XML (OBAE)*, which contains XML that is not well-formed. If the operation succeeds this is cause to fail this test.

2. Perform an operation on the Test Subject using *KDM with invalid MessageType (OBAE)*, which contains an incorrect ETM `<MessageType>` value. If the operation succeeds this is cause to fail this test.

3. Perform an operation on the Test Subject using *KDM with expired Signer certificate (OBAE)*, which contains a KDM whose signing certificate has expired. If the operation succeeds this is cause to fail this test.

4. Perform an operation on the Test Subject using *KDM with incorrect namespace name value (OBAE)*, which contains an incorrect ETM namespace name. If the operation succeeds this is cause to fail this test.

5. Perform an operation on the Test Subject using *KDM with empty TDL (OBAE)*, which contains a TDL with no entries. If the operation succeeds this is cause to fail this test.

6. Extract a security log from the Test Subject and using a **Text Editor**, identify the `KDMKeysReceived` events associated with the above steps and:

a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

b. For the log record produced by the operation using *KDM with invalid MessageType (OBAE)*, verify that the value of the `SignerID` parameter contains the Certificate Thumbprint of the signing certificate of *KDM with invalid MessageType (OBAE)*. Verify that `ReferencedIDs` element contains a `KeyDeliveryMessageID` parameter with a value that is the `MessageId` of *KDM with invalid MessageType (OBAE)*. Failure of any verification shall be cause to fail this test.

c. For the log record produced by the operation using *KDM with expired Signer certificate (OBAE)*, verify that the `contentId` element contains the `Id` of *DCI 2K StEM (OBAE) (Encrypted)*. Verify that the value of the `SignerID` parameter contains the Certificate Thumbprint of the signing certificate of *KDM with expired Signer certificate (OBAE)*. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of *DCI 2K StEM (OBAE) (Encrypted)* and `KeyDeliveryMessageID` parameter with a value that is the `MessageId` of *KDM with expired Signer certificate (OBAE)*. Failure of any verification shall be cause to fail this test.

d. Confirm the presence of a `KDMFormatError` exception in each `KDMKeysReceived` log record. Record any additional parameters associated with the exception. A missing `KDMFormatError` exception in any of the associated `KDMKeysReceivedlog` records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.8, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3<br>SMPTE-430-5 |
| **Test Materials** | *KDM with empty TDL (OBAE)*<br>*KDM with expired Signer certificate (OBAE)*<br>*KDM with invalid XML (OBAE)*<br>*KDM with invalid MessageType (OBAE)*<br>*KDM with incorrect namespace name value (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 3.5.16. KDM Signature (OBAE)

### Objective

Verify that the OBAE-capable Test Subject checks that the KDM signature is valid, including checking that the certificate that signed the KDM is included in the KDM and rejecting the KDM if it is not.

### Procedures

1. Perform an operation on the Test Subject using *KDM with incorrect message digest (OBAE)*. The KDM *KDM with incorrect message digest (OBAE)* is invalid (wrong signature/hash error). If the operation succeeds this is cause to fail

this test.

2. Perform an operation on the Test Subject using *KDM with incorrect signer thumbprint (OBAE)*. The KDM *KDM with incorrect signer thumbprint (OBAE)* is invalid (wrong signature identity). If the operation succeeds this is cause to fail this test.

3. Perform an operation on the Test Subject using *KDM without signer certificate (OBAE)*. The KDM *KDM without signer certificate (OBAE)* is invalid (broken certificate chain). If the operation succeeds this is cause to fail this test.

4. Extract a security log from the Test Subject and using a **Text Editor**, identify the `KDMKeysReceived` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of *DCI 2K StEM (OBAE) (Encrypted)*. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of *DCI 2K StEM (OBAE) (Encrypted)* and `KeyDeliveryMessageID` parameter with a value that is the `MessageId` of the KDM used. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. For the log records produced by the operation using *KDM with incorrect message digest (OBAE)* and *KDM with incorrect signer thumbprint (OBAE)*, verify that the value of the `SignerId` parameter contains the Certificate Thumbprint of the signing certificate of the KDM.

    c. Confirm the presence of a `SignatureError` exception in each `KDMKeysReceived` log record. Record any additional parameters associated with the exception. A missing `SignatureError` exception in any of the associated `KDMKeysReceived` log records shall be cause to fail this test.

5. Perform an operation on the Test Subject using *KDM signed with incorrect signer certificate format (OBAE)*. The KDM *KDM signed with incorrect signer certificate format (OBAE)* is invalid (wrong signer certificate format). If the operation succeeds this is cause to fail this test.

6. Extract a security log from the Test Subject and using a **Text Editor**, identify the `KDMKeysReceived` event associated with the above step and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of *DCI 2K StEM (OBAE) (Encrypted)*. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of *DCI 2K StEM (OBAE) (Encrypted)* and `KeyDeliveryMessageID` parameter with a value that is the `MessageId` of the KDM used. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `CertFormatError` exception in the `KDMKeysReceived` log record. Record any additional parameters associated with the exception. A missing `CertFormatError` exception in the associated `KDMKeysReceived` log record shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3<br>SMPTE-430-5 |
| **Test Materials** | *KDM with incorrect message digest (OBAE)*<br>*KDM with incorrect signer thumbprint (OBAE)*<br>*KDM without signer certificate (OBAE)*<br>*KDM signed with incorrect signer certificate format (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

# Chapter 4. Digital Cinema Packaging

The DCP is the file format for d-cinema content. Entire suites of standards documents from SMPTE define this format, most notably the 428 and 429 multi-part documents. In addition, many IETF documents and some ISO documents are referenced from the SMPTE works. Reading and understanding all of these documents is a substantial task, but it is essential knowledge for accurate and efficient analysis of d-cinema files

In the following procedures, simple tools are used to display the contents of d-cinema files. Example output from these tools is shown with descriptions of the features that will be interesting to the Test Operator. In addition to the tools used in this text, the Test Operator may use more sophisticated methods so long as the results obtained are equivalent to the procedures presented here. The reader should also note that a programmer's **Text Editor** and a binary viewer or editor are essential tools for direct inspection of data.

## 4.1. Asset Map

D-cinema track files and composition playlists are identified by unique, embedded identifiers. These identifiers, called *UUIDs*, are defined by [RFC-4122]. d-cinema XML files use UUIDs to refer to other d-cinema XML files and MXF files (assets). When d-cinema assets are written to a filesystem (*e.g.*, a disk volume), a mechanism is needed to relate the UUID values to filename values in the filesystem. An Asset Map is an XML document that provides a mapping from UUID values to filesystem paths. When a d-cinema package is written to a volume, an Asset Map is created that includes the size and location of every file in the package[1].

[1] Or packages; volumes can contain multiple DCPs.

Along with the Asset Map, each volume has a Volume Index file. The Volume Index file is used to differentiate volumes in a multiple-volume distribution. Both Asset Maps and Volume Indexes are XML files (as described in Section 3.1). The formats of the Asset Map file and the Volume Index file are specified in [SMPTE-429-9]

### Example 4.1. Asset Map

```
<?xml version="1.0" encoding="UTF-8"?> 1
<AssetMap xmlns="http://www.smpte-ra.org/schemas/429-9/2007/AM"> 2
  <Id>urn:uuid:425e93f7-bca2-4255-b8ec-8c7d16fc8881</Id> 3
  <Creator> Packaging Tools v1.0 </Creator> 4
  <VolumeCount>1</VolumeCount> 5
  <IssueDate>2007-07-06T18:25:42-00:00</IssueDate> 6
  <Issuer>user@host</Issuer> 7
  <AssetList> 8
    <Asset> 9
      <Id>urn:uuid:034b95b0-7424-420f-bbff-a875a79465a5</Id> 10
      <PackingList>true</PackingList> 11
      <ChunkList> 12
        <Chunk> 13
          <Path>perfect_movie_domestic_51.pkl.xml</Path> 14
          <VolumeIndex>1</VolumeIndex> 15
```

```
        <Offset>0</Offset> 16
        <Length>14366</Length> 17
      </Chunk>
    </ChunkList>
  </Asset>
  <Asset>
    <Id>urn:uuid:4f89a209-919b-4f21-a1d6-21ad32581115</Id>
    <ChunkList>
      <Chunk>
        <Path>perfect_movie_j2c_r01.mxf</Path>
        <VolumeIndex>1</VolumeIndex>
        <Offset>0</Offset>
        <Length>342162304</Length>
      </Chunk>
    </ChunkList>
  </Asset>
  <Asset>
    <Id>urn:uuid:e522f7b6-6731-4df5-a80e-8cfd74f82219</Id>
    <ChunkList>
      <Chunk>
        <Path>perfect_movie_wav_r01.mxf</Path>
        <VolumeIndex>1</VolumeIndex>
        <Offset>0</Offset>
        <Length>34591246</Length>
      </Chunk>
    </ChunkList>
  </Asset>
  [additional assets omitted for brevity]
  ...
 </AssetList>
</AssetMap>
```

1 XML Declaration. This specifies the version of the XML standard to which the document conforms, and the character encoding of the document.

2 The root Assetmap element. This element contains the XML namespace declaration for an Assetmap as specified in [SMPTE-429-9].

3 The Unique Universal ID (UUID) of the asset map. This is used to uniquely identify the asset map

4 The person, software, or system that generated the asset map.

5 The Volume count indicates the total number of volumes that are referenced by the asset map

6 The date the asset map was issued.

7 The organization or entity that issued the asset map.

8 The AssetList contains all of the assets in the asset map. Each asset is described in an Asset sub-element of the AssetList

9 The Asset element contains all the data about an asset necessary to locate it in the filesystem.

10 The Asset UUID is the unique ID of a particular asset in the asset map

11 The Packinglist element identifies whether or not the asset being described is a Packing List document

12 The Chunklist contains the list of chunks that comprise the complete asset

13 The Chunk element

14 The asset chunk path is the path and filename, in the file system, of the file that contains the asset data

15 The chunk volume index indicates the volume number on which the chunk resides

16 The chunk offset is the number of bytes from the beginning of the complete asset file that this chunk begins. A chunk that is either a complete file or that is the beginning of a file will have an offset of 0.

17 The chunk length is the length, in bytes, of the chunk of the asset

## Example 4.2. Volume Index

```
<?xml version="1.0" encoding="UTF-8"?> 1
<VolumeIndex xmlns="http://www.smpte-ra.org/schemas/429-9/2007/AM"> 2
<Index>1</Index> 3
</VolumeIndex>
```

1 XML Declaration. This specifies the version of the XML standard to which the document conforms, and the character encoding of the document

2 The root Assetmap element. This element contains the XML namespace declaration for an Assetmap as specified in [SMPTE-429-9].

3 The index number of the volume.

## 4.1.1. Asset Map File

### Objective

Verify that the Asset Map file is in the root of the volume, and that it it named `ASSETMAP.xml`. Verify that the Asset Map validates against the schema defined in [SMPTE-429-9].

### Procedures

1. Mount the media that contains the volume with a computer, and obtain a directory listing of the root of the filesystem. The absence of the file `ASSETMAP.xml` is cause to fail this test.

2. Using the **schema-check** software utility, validate the file `ASSETMAP.xml` against the schema in [SMPTE-429-9]. Failure to correctly validate is cause to fail this test. For more information on schema validation see Section 1.4: Conventions and Practices

E.g.:

```
$ cd /
$ ls -F
ASSETMAP.xml
PKL_c2434860-7dab-da2b-c39f-5df000eb2335.xml
J2K_a13c59ec-f720-1d1f-b78f-9bdea4968c7d_video.mxf
WAV_22d190bd-f43b-a420-a12e-2bf29a737521_audio.mxf
...
$
$ schema-check ASSETMAP.xml smpte-429-9.xsd
schema validation successful
$
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.5.2.1<br>SMPTE-429-9 |
| **Test Equipment** | **schema-check** |

## 4.1.2. Volume Index File

### Objective

Verify that the Volume Index file is in the root of the volume and that it it named `VOLINDEX.xml`. Verify that the Volume Index file validates against the schema defined in [SMPTE-429-9].

### Procedures

1. Mount the media that contains the volume with a computer, and obtain a directory listing of the root of the filesystem. The absence of the file `VOLINDEX.xml` is cause to fail this test.

2. Using the **schema-check** software utility, validate the file `VOLINDEX.xml` against the schema in [SMPTE-429-9]. Failure to correctly validate is cause to fail this test. For more information on schema validation see Section 1.4: Conventions and Practices.

E.g.:

```
$ cd /
$ ls -F
VOLINDEX.xml
PKL_c2434860-7dab-da2b-c39f-5df000eb2335.xml
J2K_a13c59ec-f720-1d1f-b78f-9bdea4968c7d_video.mxf
WAV_22d190bd-f43b-a420-a12e-2bf29a737521_audio.mxf
...
$
$ schema-check VOLINDEX.xml smpte-429-9.xsd
schema validation successful
$
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.5.2.1<br>SMPTE-429-9 |
| **Test Equipment** | **schema-check** |

## 4.2. Packing List

The Packing List (PKL) is an XML document (see Section 3.1) that specifies the contents of a d-cinema Package. It contains the UUID, file type (MXF track file, CPL, etc.), and a message digest of each file in the DCP. This information is used to ensure that all of the expected files have been included and have not been modified or corrupted in transit. The format of the Packing List file is specified by [SMPTE-429-8].

### Example 4.3. Packing List

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?> 1
<PackingList xmlns="http://www.smpte-ra.org/schemas/429-8/2007/PKL"> 2
  <Id>urn:uuid:59430cd7-882d-48e8-a026-aef4b6253dfc</Id> 3
  <AnnotationText>Perfect Movie DCP</AnnotationText> 4
  <IssueDate>2007-07-25T18:21:31-00:00</IssueDate> 5
  <Issuer>user@host</Issuer> 6
  <Creator>Packaging Tools v1.0</Creator> 7
  <AssetList> 8
    <Asset> 9
      <Id>urn:uuid:24d73510-3481-4ae5-b8a5-30d9eeced9c1</Id> 10
      <Hash>AXufMKY7NyZcfSXQ9sCZls5dSyE=</Hash> 11
      <Size>32239753</Size> 12
      <Type>application/mxf</Type> 13
```

```
    </Asset>
    <Asset>
      <Id>urn:uuid:456e547d-af92-4abc-baf3-c4d730bbcd65</Id>
      <Hash>kAAo0kXYVDBJUphIID89zauv50w=</Hash>
      <Size>86474446</Size>
      <Type>application/mxf</Type>
    </Asset>
    <Asset>
      <Id>urn:uuid:e4a4e438-63ec-46cb-b9aa-43acee787d79</Id>
      <Hash>kt5bP8y4zmHNAY1qVnujItAb4sY=</Hash>
      <Size>12163</Size>
      <Type>text/xml</Type>
    </Asset>
    <Asset>
      <Id>urn:uuid:3d445456-54d5-42bc-a7cc-a8c00b20ffb7</Id>
      <Hash>AQWMKCxxMv001zTS3Y3Oj8M+d9s=</Hash>
      <Size>62500144</Size>
      <Type>application/mxf</Type>
    </Asset>
    [Remaining assets and signature omitted for brevity]
  </AssetList>
  [Signature omitted for brevity]
</PackingList>
```

1. XML Declaration. This specifies the version of the XML standard to which the document conforms
2. The root packing list element. This element contains the XML namespace declaration for the packing list as specified in[SMPTE-429-8]
3. The Unique Universal ID (UUID) of the packing list
4. The Annotation text is a plain text, human readable language description of the packing list's contents
5. The date the packing list was issued
6. The organization or entity that issued the packing list
7. The person, software, or system that generated the packing lis
8. The assetlist contains all of the assets in the packing list
9. The Asset element contains all the metadata necessary to identify the file
10. The Asset UUID is the unique ID of a particular asset in the packing list
11. The asset hash is a message digest of the asset file
12. The asset size is the size, in bytes, of the asset's file in the filesystem
13. The asset type contains the mime type of the asset, which is a generic description of the file format. It also contains an attribute that specifies the specific kind of type, such as a CPL, Picture, or Sound file

## 4.2.1. Packing List File

### Objective

- Verify that the Packing List is an XML document and that it validates against the schema defined in [SMPTE-429-8].
- Confirm that if the `language` attribute of the `<AnnotationText>` element is not present, or present with a value of "en", that the Annotation text is in human-readable English.
- Verify that the Packing List contains urn:uuid values as specified in [RFC-4122].
- Verify that the listed file sizes match those for each of the referenced assets.

### Procedures

In the following procedures, the callout numbers refer to Example 4.3..

1. Using the **schema-check** software utility, validate the XML file structure against the schema in [SMPTE-429-8]. Failure to correctly validate is cause to fail this test. For more information on schema validation see Section 1.4: Conventions and Practices.

```
$ schema_check.py <input-file> smpte-429-8.xsd
schema validation successful
$
```

2. Open the Packing List file in a **Text Editor** and verify that if the "language" attribute of the `<AnnotationText>` 4 element is not present, or present with a value of "en", that the contents of the `<AnnotationText>` 4 element is human readable English. Failure to meet this requirement is cause to fail this test.

```
$ vi <input-file>
...
<AnnotationText>Perfect Movie Reel #1 Picture</AnnotationText>
...
<AnnotationText language="en">Perfect Movie Reel #1 Sound</AnnotationText>
...
:q
$
```

3. Supply the filename of the Packing List file as an argument to the **uuid_check.py** software utility. Examine the output for error messages that identify expected UUID values that do not conform to the format specified in [RFC-4122]. One or more occurrences is cause to fail this test.

```
$ uuid_check.py <input-file>
all UUIDs conform to RFC-4122
$
```

4. To verify that the real file sizes of the referenced assets are equal to the values of the related XML elements, the path to those assets must be known. The following procedure may be used if the `ASSETMAP.xml` file is available, otherwise the tester will need to devise a method for locating the relevant assets. For each of the `<Asset>` 9 elements contained in the Packing List, compare the contents of the child `<Id>` 10 element with the contents of the `ASSETMAP.xml` file to discover the path to the asset. List the file size of the referenced asset and verify that it is identical to the value of the child `<Size>` 12 element inside the `<Asset>` 9 element. One or more failures to verify the file sizes is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.5.3.1, 5.5.3.2<br>SMPTE-429-8 |
| **Test Equipment** | **schema-check**<br>**uuid_check.py**<br>**Text Editor** |

## 4.2.2. Packing List Signature Validation

### Objective

Verify that the Packing List is signed and that the signature validates.

### Procedures

Using the **checksig** software utility, verify that there is a signature included in the Packing List and that it is valid. If the signature is missing or invalid, this is cause to fail this test. Note: Depending on the order of the certificates contained in the log report, the **dsig_cert.py** program may need to be used to re-order the certificates for the **checksig** program. Example:

```
$ dsig_cert.py <pkl-file.pkl.xml> > tmp.xml
$ checksig tmp.xml
The supplied signature is valid
$
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.5.2.3, 5.5.3.2<br>PKCS-1<br>RFC-3174<br>SMPTE-429-8 |
| **Test Equipment** | **checksig**<br>**dsig_cert.py** |

## 4.3. Composition Playlist

The Composition Playlist (CPL) is an XML document (see Section 3.1) that contains the information necessary to reproduce a composition. It contains metadata about the composition such as the title and the rating, and references to the track files that contain the composition's essence. The format of the Composition Playlist file is specified by [SMPTE-429-7].

### Example 4.4. Composition Playlist

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?> 1
<CompositionPlaylist xmlns="http://www.smpte-ra.org/schemas/429-7/2006/CPL"> 2
  <Id>urn:uuid:20670ba3-d4c7-4539-ac3e-71e874d4d7d1</Id> 3
  <IssueDate>2007-07-25T00:35:03-00:00</IssueDate> 4
  <Issuer>user@host</Issuer> 5
  <Creator> Packaging Tools v1.0 </Creator> 6
  <ContentTitleText>Perfect Movie</ContentTitleText> 7
  <ContentKind>feature</ContentKind> 8
  <ContentVersion> 0
    <Id>urn:uuid:e5a1b4dc-faf3-461b-a5e2-9d33088b1b28</Id> 10
    <LabelText>Perfect Movie - Domestic - US 5.1 </LabelText> 11
  </ContentVersion>
  <RatingList /> 12
  <ReelList> 13
    <Reel> 14
      <Id>urn:uuid:f62cffe9-2da7-4d28-b73e-f21c816ab02f</Id> 15
      <AssetList> 16
        <MainPicture> 17
          <Id>urn:uuid:93270dd0-8675-42fa-9ce8-34b61c963997</Id> 18
          <EditRate>24 1</EditRate> 19
          <IntrinsicDuration>480</IntrinsicDuration> 20
          <EntryPoint>0</EntryPoint> 21
          <Duration>480</Duration> 22
          <FrameRate>24 1</FrameRate> 23
          <ScreenAspectRatio>1998 1080</ScreenAspectRatio> 24
        </MainPicture> 25
```

```
       <MainSound>26
         <Id>urn:uuid:e33b7b37-da90-4429-88af-5c5b63506017</Id>
         <EditRate>24 1</EditRate>
         <IntrinsicDuration>2880</IntrinsicDuration>
         <EntryPoint>120</EntryPoint>
         <Duration>2760</Duration>
       </MainSound>
     </AssetList>
   </Reel>
  </ReelList>
  [Additional reel data and CPL Signature omitted for brevity]
</CompositionPlaylist>
```

1 The XML version of the XML standard to which the document conforms, the character encoding of the document, and whether the document relies on external declarations or parameter entities.

2 The Root Composition Playlist element. This element contains the XML namespace declaration for the Composition Playlist as specified in [SMPTE-429-7].

3 The Unique Universal ID (UUID) of the composition playlist.

4 The date the CPL was issued

5 The organization or entity that issued the CPL

6 The person, software, or system that generated the CPL

7 A descriptive string that describes the composition and is displayed to the user

8 The kind of presentation the CPL represents, such as a feature, trailer, or advertisement

0 The version of the content represented by the composition playlist. This element contains sub-elements that contain a descriptive label and UUID of the content

10 The unique ID of the version of the content represented by the CPL (as opposed to the unique ID of the CPL

11 A text description of the version of the content represented in the CPL

12 The list of ratings applied to the content represented by the CPL. In compositions that contain rating information, the `<RatingList>` element contains at least one instance of the `<Rating>` element, which in turn contains two elements, <Agency>, that contains a URI that represents the agency that issued the rating, and `<Label>`, that contains the rating

13 The list of reels that comprise the composition

14 A reel of the composition

15 The unique ID of the reel

16 The list of assets that comprise the reel

17 The element in the reel that contains the information required to produce images onscreen

18 The unique ID of the MXF track file that contains the picture essence (the picture track file) to be reproduced onscreen

19 The edit rate, or the number of editable units of content, per second, of the picture track file

20 The total number of frames in the track file, inclusive of frames not intended for reproduction onscreen

21 The first frame of the track file to be reproduced onscreen

22 The number of frames of the track file to be reproduced onscreen. When a picture track file is present in a composition, its duration is effectively the duration of the reel

23 The rate, in frames-per-second, at which the essence in the track file will be reproduced

24 The aspect ratio of the essence in the picture track file. This is represented in the CPL as a ratio of two numbers separated by a space

25 The closing tag of the reel's MainPicture element

26 The element in the reel that contains the information required to reproduce sound essence through the primary speaker system. The parameters of a MainSound track file are the same as those of a picture track file

### 4.3.1. Composition Playlist File

### Objective

Verify that the Composition Playlist is an XML document and that it validates against the schema defined in [SMPTE-429-7].

### Procedures

Using the **schema-check** software utility, validate the XML file structure against the schema in [SMPTE-429-7]. Failure to correctly validate is cause to fail this test.

```
$ schema-check <input-file> smpte-429-7.xsd
schema validation successful
$
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.2.3, 5.4.2, 5.4.3, 9.7.7, 5.4.3.2, 5.4.3.3, 5.4.3.4<br>SMPTE-429-7 |
| **Test Equipment** | **schema-check** |

## 4.3.2. Composition Playlist Signature Validation

### Objective

Verify that the Composition Playlist is signed and that the signature validates.

### Procedures

Using the **checksig** software utility, verify that there is a signature included in the Composition Playlist List and that it is valid. If the signature is missing or invalid, this is cause to fail this test. Note: Depending on the order of the certificates contained in the log report, the **dsig_cert.py** program may need to be used to re-order the certificates for the **checksig** program. Example:

```
$ dsig_cert.py <cpl-file.cpl.xml> > tmp.xml
$ checksig tmp.xml
The supplied signature is valid
$
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.2.3, 5.4.3.6, 5.4.4, 9.7.5 |
| **Test Equipment** | **dsig_cert.py**<br>**checksig** |

## 4.3.3. Composition Playlist Key Usage

### Objective

An encrypted Asset is associated with a Decryption Key that is effective for a period of time equal to one Reel. Only one Decryption Key shall be associated with a specific encrypted Asset. Each unique Decryption Key shall be associated with only one encrypted Asset.

- Verify that for each encrypted Asset present in the Composition Playlist, only one `<KeyId>` value is listed. If an Asset Id occurs more than once in the CPL, verify that the same `<KeyId>` is utilized throughout.

- Verify that each `<KeyId>` is associated with only one Asset Id.

#### Procedures

1. Use a **Text Editor** to view the Composition Playlist. For all encrypted Assets (those that have a `<KeyId>` value) make a list of all Asset Id values and the associated `<KeyId>` values.

2. Examine the list to determine that each Asset Id has exactly one `<KeyId>`. If Asset Ids are repeated in the CPL, the same `<KeyId>` should be associated for that Asset every time. Any deviation is cause to fail this test.

3. Examine the list to determine that each `<KeyId>` is associated with exactly one Asset Id (*i.e.* a particular Decryption Key should only be associated with one, unique Asset). Any deviation is cause to fail this test.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.3.1.7 |
| **Test Equipment** | **Text Editor** |

## 4.4. Track Files

A Track File is a container for encoded essence. In the d-cinema system, each Track File contains a single track of a single type of essence. For example, a Track File may contain images or sound or timed text, but never more than one type of essence[2].

[2] Strictly speaking, a Timed Text Track File may contain font and image resources in addition to the XML timed text data, but these resources are considered integral to the timed text essence.

D-cinema Track Files are based on the Material eXchange Format (MXF). MXF is a file metaformat, *i.e.*, a file format for creating file formats. While the various d-cinema Track File formats represent different methods of encoding essence data, the arrangement of metadata within the files is syntactically similar. This section will provide an overview of MXF as used for d-cinema applications. Readers looking for more detailed technical information are referred to [SMPTE-377-1]

### 4.4.1. MXF Internals

#### 4.4.1.1. Overview

Before diving head-first into examining MXF files, it is important to understand the structure of the files. This section will briefly describe the contents of some example MXF files by displaying the files' header metadata using the **klvwalk** software utility from the free ASDCPLib software package.

Briefly, an MXF file [SMPTE-377-1] contains a sequence of Key-Length-Value (KLV) packets. Some packets carry essence and some carry metadata. MXF files are divided into *partitions*. Each partition is comprised of a set of KLV packets. The first KLV packet in each partition is a Partition Pack.

The number of partitions in a digital cinema sound or picture Track File is usually three (Timed Text Track Files may have more than three partitions). The first partition in an MXF file contains the metadata which describe the coding parameters of the essence and the MXF file itself. The second partition contains the essence data as a sequence of KLV-wrapped frames. The final partition contains the index table

To display the metadata in the header partition of an MXF file `testfile.mxf`, use **klvwalk** like so

```
$ klvwalk -r testfile.mxf
...
```

The following sections illustrate the expected output

### 4.4.1.2. MXF Header Partition

As shown in Example 4.5., the first structure to be output is the Partition Pack of the Header Partition. This structure documents the MXF version that the file conforms to and provides a description of the general architecture to be found inside

#### Example 4.5. MXF Partition Header

```
06.0e.2b.34.02.05.01.01.0d.01.02.01.01.02.04.00 len: 120 (ClosedCompleteHeader) 1
  MajorVersion = 1
  MinorVersion = 2
  KAGSize = 1
  ThisPartition = 0
  PreviousPartition = 0
  FooterPartition = 218362864
  HeaderByteCount = 16244
  IndexByteCount = 0
  IndexSID = 0
  BodyOffset = 0
  BodySID = 1
  OperationalPattern = 060e2b34.0401.0101.0d010201.10000000 2
Essence Containers: 3
  060e2b34.0401.0103.0d010301.027f0100
  060e2b34.0401.0107.0d010301.020b0100
```

1 This is an MXF Partition Pack structure. The Universal Label (UL) value indicates that the file is "Closed and Complete".

2 The Operational Pattern UL indicates that the file conforms to OP Atom [SMPTE-390]

3 Essence Container labels indicate the type of essence and the wrapping format. This example shows two container labels: the JPEG 2000 container [SMPTE-422] and the Generic Container [SMPTE-379-1] (the file contains encrypted JPEG 2000 essence)

The following table gives the list of valid Essence Container ULs for d-cinema Track File

**Table 4.1.Essence**

### Container UL Values for D-Cinema

| UL Value | Container Type |
|---|---|
| 060e2b34.0401.0101.0d010301.02060100 | Linear PCM Audio [SMPTE-429-3], [SMPTE-382] |
| 060e2b34.0401.0107.0d010301.020c0100 | JPEG 2000 Images [SMPTE-429-4] |
| 060e2b34.0401.010a.0d010301.02130101 | Timed Text [SMPTE-429-5] |
| 060e2b34.0204.0101.0d010301.027e0100 | Encrypted Essence [SMPTE-429-6] |

## 4.4.1.3. File Package

An MXF file may contain zero or more continuous segments of essence data. Each segment is described by a Source Package structure. Per [SMPTE-429-3], MXF files for digital cinema must contain exactly one top-level Source Package (thus one segment of essence), referred to in MXF jargon as a File Package. Example 4.6. shows a Source Package structure that points to JPEG 2000 essence data.

### Example 4.6.Source Package structure

```
06.0e.2b.34.02.53.01.01.0d.01.01.01.01.01.37.00 len: 294 (SourcePackage) 1
            InstanceUID = 42b5a376-c740-42e2-99f1-4ec782c4837e
            PackageUID = [060a2b34.0101.0105.01010f20],13,00,00,00,
                                  [b4f492cd.b89b.0f65.490c35ec.5f6340b7] 2
                  Name = File Package: SMPTE 429-4 frame wrapping of JPEG 2000 codestreams
       PackageCreationDate = 2007-03-21 07:42:04.000
       PackageModifiedDate = 2007-03-21 07:42:04.000
                  Tracks: 3
  9227a330-7e64-4c90-b4ef-d057ed6ef159
  0de983e3-255b-4d26-bde7-f33c530c077d
  54e13d93-abcf-4869-b008-c59573b8d01d
                  Descriptor = c6a35640-d6d8-433c-82c9-23df2eae9311 4
```

1 This is a Source Package structure [SMPTE-377-1]

2 A Unique Material Identifier (UMID) value which identifies the essence in the file. It has a UUID component which is the value that external entities (*e.g.* Packing Lists and Composition Playlists) use to refer to the essence in the file. See [SMPTE-429-3] for details about how d-cinema UMIDs are formed

3 The list of tracks that appear in the file. There is only one essence track, but it is accompanied by a virtual timecode track and, optionally, a descriptive metadata track that gives cryptographic information (see Section 4.4.1.4 below).

4 This value gives the internal ID of a data set that describes the essence encoding. This set is called an Essence Descriptor. Two examples of essence descriptors are given below in Section 4.4.1.5 and Section 4.4.1.6

## 4.4.1.4. Encrypted Essence

If the MXF file contains encrypted essence, the header metadata will contain one Cryptographic Framework set with a link to a single Cryptographic Context set (defined in [SMPTE-429-6]). These structures are shown in Example 4.7.

## Example 4.7. Cryptographic Framework and Cryptographic Context

```
06.0e.2b.34.02.53.01.01.0d.01.04.01.02.01.00.00 len: 40 (CryptographicFramework) 1
            InstanceUID = b98ca683-2e49-4e6a-88ff-af33910ba334
              ContextSR = 8dcd2f7b-fd0b-4602-bae7-806c82dcfd94

06.0e.2b.34.02.53.01.01.0d.01.04.01.02.02.00.00 len: 120 (CryptographicContext) 2
            InstanceUID = 8dcd2f7b-fd0b-4602-bae7-806c82dcfd94
              ContextID = 3472d593-e9ff-4b2e-84ca-5303b5ce53f7
  SourceEssenceContainer = 060e2b34.0401.0107.0d010301.020c0100 3
         CipherAlgorithm = 060e2b34.0401.0107.02090201.01000000 4
             MICAlgorithm = 060e2b34.0401.0107.02090202.01000000 5
       CryptographicKeyID = c030f37a-bf84-496b-bdc2-81744205a944 6
```

1 This is a Cryptographic Framework structure [SMPTE-429-6]

2 This is a Cryptographic Context structure [SMPTE-429-6]

3 A UL that identifies the type of essence inside the encrypted container. It should be a JPEG 2000 or PCM audio descriptor.

4 A UL that identifies the type of encryption used. This value should always be `060e2b34.0401.0107.02090201.01000000`

5 A UL that identifies the algorithm used to calculate the Message Integrity Check value in each Encrypted KLV (EKLV) packet. When present, this value should always be `060e2b34.0401.0107.02090202.01000000`

6 A UUID value that identifies the 16-byte symmetric key (stored externally) that is required to decrypt the essence data. The key is usually delivered to a system via a Key Delivery Message (see Chapter 3)

### 4.4.1.5. Essence Descriptor for JPEG 2000

If the MXF file contains image essence for DCI-compliant digital cinema, the header metadata will contain an RGBA Essence Descriptor (defined in [SMPTE-377-1], with a strong link to a JPEG 2000 Picture SubDescriptor (defined in [SMPTE-422]. These structures are shown in Example 4.8.

## Example 4.8. Essence Descriptor for JPEG 2000

```
06.0e.2b.34.02.53.01.01.0d.01.01.01.01.01.29.00 len: 169 (RGBAEssenceDescriptor) 1
              InstanceUID = 18a47da5-53d1-4785-a91e-41155753a02f
                  Locators:
             SubDescriptors:
  05f80258-beb2-4769-b99a-af4d6c3895da
             LinkedTrackID = 2
                SampleRate = 24/1 2
         ContainerDuration = 720 3
          EssenceContainer = 060e2b34.0401.0107.0d010301.020c0100
                     Codec = 00000000.0000.0000.00000000.00000000
              FrameLayout = 0
              StoredWidth = 2048 4
             StoredHeight = 1080 5
              AspectRatio = 2048/1080
     PictureEssenceCoding = 060e2b34.0401.0109.04010202.03010103 6
          ComponentMaxRef = 4095
```

```
         ComponentMinRef = 0

         06.0e.2b.34.02.53.01.01.0d.01.01.01.01.01.5a.00 len: 174 (JPEG2000PictureSubDesc
             InstanceUID = 05f80258-beb2-4769-b99a-af4d6c3895da
                   Rsize = 3
                   Xsize = 2048
                   Ysize = 1080
                  XOsize = 0
                  YOsize = 0
                  XTsize = 2048
                  YTsize = 1080
                 XTOsize = 0
                 YTOsize = 0
                   Csize = 3
  PictureComponentSizing = 00000003000000030b01010b01010b0101
      CodingStyleDefault = 0104000101050303000778888888888
     QuantizationDefault = 227f187f007f007ebc76ea76ea76bc6f4c6f4c6f645803580358455fd25fd2
```

1. This is an MXF RGBA Essence Descriptor structure
2. The frame rate of the underlying essence. The essence may be sampled on a finer scale, but this value is the smallest temporal increment than can be accessed in the file
3. The number of frames in the file. Divide this value by the SampleRate to get the duration as a time value in seconds
4. The width of the encoded image as a count of pixels.
5. The height of the encoded image as a count of pixels
6. This UL value indicates the type of compression and the color space of the encoded essence
7. This is an MXF JPEG 2000 Picture SubDescriptor structure. It provides additional metadata associated with the JPEG 2000 encoding

### 4.4.1.6. Essence Descriptor for PCM Audio

If the MXF file contains audio essence for DCI-compliant digital cinema, the header metadata will contain a Wave Audio Descriptor (defined in [SMPTE-382]). This structure is shown in Example 4.9..

## Example 4.9. Essence Descriptor for PCM Audio

```
06.0e.2b.34.02.53.01.01.0d.01.01.01.01.01.48.00 len: 134 (WaveAudioDescriptor) 1
               InstanceUID = 0b7eac6c-85e2-47e4-b0bf-b3e60f6e6cd7
                   Locators:
             SubDescriptors:
             LinkedTrackID = 2
                SampleRate = 24/1 2
          ContainerDuration = 528 3
           EssenceContainer = 060e2b34.0401.0101.0d010301.02060100
          AudioSamplingRate = 48000/1 4
                    Locked = 0
             AudioRefLevel = 0
              ChannelCount = 6 5
           QuantizationBits = 24 6
                  DialNorm = 0
                BlockAlign = 18 7
            SequenceOffset = 0
                    AvgBps = 144000
```

1. This is a Wave Audio Descriptor structure [SMPTE-382]

2 The frame rate of the underlying essence. The essence may be sampled on a finer scale, but this value is the smallest temporal increment than can be accessed in the file.

3 The number of frames in the file. Divide this value by the SampleRate to get the duration as a time value in seconds.

4 The base sample rate of the essence.

5 The number of channels in the file. Each frame of essence will have the same number of channels, multiplexed in the same order

6 The number of bits used to encode a sample of a single channel.

7 The size, in bytes, of a set of samples for all channels in a single sample period. This value should be equal to *(QuantizationBits / 8) * ChannelCount*.

#### 4.4.1.7. Random Index Pack (R.I.P.)

All d-cinema Track Files end with a Random Index Pack (RIP). The RIP provides a lookup table that gives the location of all partitions in the file for easy random access. The number of partitions shown by the RIP should be three if the MXF file is a sound or picture Track File, and may be more than three for a Timed Text Track File.

### Example 4.10. MXF Random Index Pack (RIP)

```
06.0e.2b.34.02.05.01.01.0d.01.02.01.01.11.01.00 len: 40 (RandomIndexMetadata)1 1
  0       : 0
  1       : 16384
  0       : 110688380
```

1 The Random Index Pack (RIP) maps the location of each partition in an MXF file. This example shows three partitions

### 4.4.2. Image and Audio Packaging Standard

#### Objective

- Verify that sound and image essence are wrapped in files conforming to Material Exchange Format (MXF) as defined by [SMPTE-377-1], and further constrained by [SMPTE-379-1], [SMPTE-429-3], and [SMPTE-429-4], [SMPTE-422] for image, or [SMPTE-382] for sound.

- If the Essence Container is encrypted, verify that this conforms to [SMPTE-429-6].

#### Procedures

1. Using the **klvwalk** software utility, produce a listing of the MXF KLV Header Metadata Structure. Error free completion of the command confirms the validity of the MXF structure. Any other result is cause to fail the test.

2. Examine the listing for the MXF Partition Pack structure with a ClosedCompleteHeader Universal Label (UL) value:
`060e2b34.0205.0101.0d010201.01020400`
as shown in Example 4.5. item 1. Absence of this value is cause to fail this test.

3. Examine the listing for the OperationalPattern value:
   `060e2b34.0401.0102.0d010201.10000000`,
   as shown in Example 4.5. item 2 . Absence of this value is cause to fail this test.

4. Examine the listing for the Essence Container values as shown in Example 4.5. item 3 . There are three valid possibilities for the data in this field:

   a. If two values are present, and they are:
      `060e2b34.0401.0103.0d010301.027f0100` and
      `060e2b34.0401.0107.0d010301.020c0100`,
      then the file is an Image file. For more information see Section 4.4.1.5: Essence Descriptor for JPEG 2000.

   b. If two values are present, and they are:
      `060e2b34.0401.0103.0d010301.027f0100` and
      `060e2b34.0401.0101.0d010301.02060100`,
      then the file is an Sound file. For more information see Section 4.4.1.6: Essence Descriptor for PCM Audio.

   c. If two values are present, and they are:
      `060e2b34.0401.0103.0d010301.027f0100` and
      `060e2b34.0401.0107.0d010301.020b0100`,
      the Essence is ciphertext and an additional procedure, listed below, must be carried out.

   Failure to meet exactly one of the valid possibilities is cause to fail this test.

5. Examine the listing and locate the EssenceContainerData set, UL value:
   `060e2b34.0253.0101.0d010101.01012300`.
   This should contain exactly one LinkedPackageUID value. Verify that there is only one SourcePackage set, UL value:
   `060e2b34.0253.0101.0d010101.01013700`
   and that the PackageUID value exactly matches the LinkedPackageUID value of the EssenceContainerData set.
   Failure of any of the above conditions is cause to fail this test.

6. Only for the case of Encrypted Essence, the SourcePackage set, UL value:
   `060e2b34.0253.0101.0d010101.01013700`,
   should contain a third Track UID that matches the InstanceUID value of a single StaticTrack set, UL value:
   `060e2b34.0253.0101.0d010101.01013a00`.
   The StaticTrack set should have a Sequence value that matches the InstanceUID of a Sequence set, UL value:
   `060e2b34.0253.0101.0d010101.01010f00`.
   The found Sequence set should have a StructuralComponents value that matches the InstanceUID of a single DMSegement set, UL value:
   `060e2b34.0253.0101.0d010101.01014100`.
   The DMSegment set should have a DMFramework value that matches a single CryptographicFramework set, UL value:
   `060e2b34.0253.0101.0d010401.02010000`.
   The CryptographicFramework set should have a ContextSR value that matches the InstanceUID of a single CryptographicContext set, UL value:
   `060e2b34.0253.0101.0d010401.02020000`.
   The CryptographicContext set has a SourceEssenceContainer value, which should contain either the UL value:
   `060e2b34.0401.0107.0d010301.020c0100`
   for an Image file, or:
   `060e2b34.0401.0101.0d010301.02060100`
   for a Sound file. For more information see Section 4.4.1.4: Encrypted Essence. Failure of any of the above conditions is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.2.2.2, 5.2.2.3, 5.2.2.4, 5.2.2.5, 5.2.2.6, 5.3.1, 5.3.2<br>SMPTE-377-1<br>SMPTE-379-1<br>SMPTE-382<br>SMPTE-422<br>SMPTE-429-2<br>SMPTE-429-3<br>SMPTE-429-4<br>SMPTE-429-6 |
| **Test Equipment** | **klvwalk** |

## 4.4.3. Timed Text Track File Format

### Objective

- Verify that timed text essence is wrapped in files conforming to Material Exchange Format (MXF) as defined by [SMPTE-377-1] and [SMPTE-410], and further constrained by [SMPTE-379-1] and [SMPTE-429-5].
- Verify that timed text essence is encoded according to {ref-SMPTE-428-7}.
- If the Essence Container is encrypted, verify that this conforms to [SMPTE-429-6].

### Procedures

1. Using the **klvwalk** software utility, produce a listing of the MXF KLV Header Metadata structure. Error free completion of the command confirms the validity of the MXF structure. Any other result is cause to fail the test.
2. Examine the listing for the MXF Partition Pack structure with a ClosedCompleteHeader Universal Label (UL) value:
   `060e2b34.0205.0101.0d010201.01020400`
   as shown in Example 4.5. item 1 . Absence of this value is cause to fail this test.
3. Examine the listing for the OperationalPattern value:
   `060e2b34.0401.0102.0d010201.10000000`,
   as shown in Example 4.5. item 2 . Absence of this value is cause to fail this test.
4. Examine the listing for the Essence Container values as shown in Example 4.5. item 3 . There are two valid possibilities for the data in this field:
   a. If two values are present, and they are:
      `060e2b34.0401.0103.0d010301.027f0100` and
      `060e2b34.0401.010a.0d010301.02130101`,
      then the file is a Timed Text file. For more information see Section 4.4.1.5: Essence Descriptor for JPEG 2000.
   b. If two values are present, and they are:
      `060e2b34.0401.0103.0d010301.027f0100` and
      `060e2b34.0401.0107.0d010301.020b0100`,
      the Essence is ciphertext and an additional procedure, listed below, must be carried out.

   Failure to meet exactly one of the valid possibilities is cause to fail this test.

5. Examine the listing and locate the EssenceContainerData set, UL value:
   `060e2b34.0253.0101.0d010101.01012300`.
   This should contain exactly one LinkedPackageUID value. Verify that there is only one SourcePackage set, UL value:
   `060e2b34.0253.0101.0d010101.01013700`
   and that the PackageUID value exactly matches the LinkedPackageUID value of the EssenceContainerData set.
   Failure of any of the above conditions is cause to fail this test.

6. Only for the case of Encrypted Essence, execute sub-procedure #6 as given in Section 4.4.2. In this case the SourceEssenceContainer value within the CryptographicContext set contain the UL value:
   `060e2b34.0401.010a.0d010301.02130101`
   to indicate a Timed Text file. Failure of any of the above conditions is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 3.3.4<br>SMPTE-428-7<br>SMPTE-429-5<br>SMPTE-429-6 |
| **Test Equipment** | **klvwalk** |

## 4.4.4. Track File Length

### Objective

For each Track File, verify that the minimum duration is a number of frames which is greater or equal to one second of content playback at the specified edit rate. This means that each image Track File needs to contain at least 24 (at 24 fps frame rate) or 48 (at 48 fps frame rate) frames, and that each audio Track File needs to contain at least 48,000 (at 48kHz sampling rate) or 96,000 (at 96 kHz sampling rate) audio samples.

### Procedures

This may be accomplished by using the **asdcp-test** software utility to provide information about the file and confirming that the reported ContainerDuration value is equal or greater than the SampleRate value. Failure to meet the above conditions is cause to fail this test.

E.g.

```
$ asdcp-test -i -v <input-file>
...
SampleRate: 24/1
...
ContainerDuration: 528
...
$
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.3.1.3 |
| **Test Equipment** | **asdcp-test** |

## 4.4.5. Image Track File Frame Boundary

### Objective

- Image Track Files must begin and end with complete frames that allow for splicing. Verify that both the first and the last JPEG2000 image in a sequence are completely contained within the Image Track File, *i.e.*, no other Track Files are needed for complete decoding or displaying of the first and the last frame.

- Each complete Frame of Image Data must be wrapped within the KLV structure according to [SMPTE-336] and [SMPTE-422].

### Procedures

1. Determine the number of frames contained in the Track File. This will be used in the next step to extract the last frame in the file. This can be achieved by using the **asdcp-test** software utility, and subtracting one from the ContainerDuration value, as shown below.

```
$ asdcp-test -i -v PerfectMovie-j2c-pt.mxf
File essence type is JPEG 2000 pictures.
ProductUUID: 43059a1d-0432-4101-b83f-736815acf31d
ProductVersion: Unreleased 1.1.13
CompanyName: DCI
ProductName: asdcplib
EncryptedEssence: No
AssetUUID: 0e676fb1-951b-45c4-8334-ed2c59199815
Label Set Type: SMPTE
AspectRatio: 2048/1080
EditRate: 24/1
StoredWidth: 2048
StoredHeight: 1080
Rsize: 3
Xsize: 2048
Ysize: 1080
XOsize: 0
YOsize: 0
XTsize: 2048
YTsize: 1080
XTOsize: 0
YTOsize: 0
ContainerDuration: 240
Color Components:
11.1.1
11.1.1
11.1.1
Default Coding (16): 0104000101050303000078888888888
Quantization Default (33): 227f187f007f007ebc76ea76ea76bc6f4c6f4c6f645803580358455fd25fd25f61
```

2. Using the **asdcp-test** software utility, extract the first and the last frames of content from the Track File.

```
$ asdcp-test -x first -d 1 -f 0 PerfectMovie-j2c-pt.mxf
$ asdcp-test -x last -d 1 -f 239 PerfectMovie-j2c-pt.mxf
$ ls
first000000.j2c
last000239.j2c
PerfectMovie-j2c-pt.mxf
```

3. Verify that the first and the last frames of content decode completely, and without errors. Failure to correctly decode either frame is cause to fail this test. This can be achieved by using JPEG 2000 decoding software. An example is shown below. (Note that the output of the **j2c-scan** program is long and has been truncated here for brevity. Please see Section C.5 for a detailed example.)

```
$ j2c-scan frame000000.j2c
digital cinema profile: none
rsiz capabilities: standard
pixel offset from top-left corner: (0, 0)
tile width/height in pixels: (2048, 1080)
image width/height in tiles: (1, 1)
tile #1
coding style: 1
progression order: Component-Position-Resolution-Layer
POC marker flag: 0
number of quality layers: 1
rate for layer #1: 0.0
multi-component transform flag: 1
...
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.3.3.2<br>SMPTE-336<br>SMPTE-422 |
| **Test Equipment** | **asdcp-test**<br>**j2c-scan** |

## 4.4.6. Audio Track File Frame Boundary

### Objective

The Audio Track File is required to begin and end with complete frames that are associated with its Image Track File to allow for a clean transition between reels. The audio data within the Track File shall be wrapped using KLV on an image frame boundary.

### Procedures

Verify that exactly the expected number of Audio bytes are embedded within each KLV encoded triplet for each frame of the Audio Track File. This can be achieved by using the software command **`klvwalk`** to display the length of every WAVEssence set (UL value `060e2b34.0102.0101.0d010301.16010101`) and checking that each frame contains the appropriate number of bytes. The expected number of Audio Bytes per frame can be calculated by using the formula len=BPS*Ch*SPF, where BPS is the number of Bytes Per Sample (BPS=3), Ch is the number of Audio Channels in the DCP, and SPF is the number of Samples Per Frame value taken from Table 4.2.

If any frame has an actual `len` that differs from the expected value, calculated from the formula, this is cause to fail this test.

The example below shows eight frames of a composition containing six channels of 48kHz samples at 24fps, completely wrapped in KLV triplets (3 * 6 * 2000 = 36000).

```
$klvwalk PerfectMovie-pcm-pt.mxf
...
060e2b34.0102.0101.0d010301.16010101 len: 36000 (WAVEssence)
060e2b34.0102.0101.0d010301.16010101 len: 36000 (WAVEssence)
060e2b34.0102.0101.0d010301.16010101 len: 36000 (WAVEssence)
```

```
060e2b34.0102.0101.0d010301.16010101 len: 36000 (WAVEssence)
060e2b34.0102.0101.0d010301.16010101 len: 36000 (WAVEssence)
060e2b34.0102.0101.0d010301.16010101 len: 36000 (WAVEssence)
060e2b34.0102.0101.0d010301.16010101 len: 36000 (WAVEssence)
060e2b34.0102.0101.0d010301.16010101 len: 36000 (WAVEssence)
...
```

The possible values for the Samples/Frame are shown in table below.

**Table 4.2.Audio Samples Per Frame**

| FPS | Sample Rate | Samples/Frames |
|---|---|---|
| 24 | 28 kHz | 2000 |
| 24 | 96 kHz | 4000 |
| 48 | 48 kHz | 1000 |
| 48 | 96 kHz | 2000 |

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.3.4.2 |
| **Test Equipment** | **klvwalk** |

# 4.5. Essence

## 4.5.1. Image Structure Container and Image Container Format

### Objective

- Verify that the images contained in the Track Files conform to an Image Structure Container that consists of either 4K (4096x2160) (Operational Level 1) or 2K (2048x1080) (Operational Level 2 and 3). It is expected that the image structure shall use one of the two containers such that either the horizontal or vertical resolution is filled.
- Verify that both the horizontal and vertical dimensions of the image structure container are divisible by four for Level 1, or two for Level 2 and 3 image structures. This ensures that the image can be centered correctly.
- Verify that the bit depth for each code value for a color component shall be 12 bits. This yields 36 bits per pixel.

### Procedures

- Using the software command **klvwalk**, locate the RGBAEssenceDescriptor set and record the StoredWidth, StoredHeight, and AspectRatio values within. The failure to meet any of the following conditions is cause to fail this test:

    a. Verify that the first number (numerator) of the AspectRatio field is the same as the StoredWidth value.

b. Verify that the second number (denominator) of the AspectRatio field is the same as the StoredHeight value.

c. Verify that exactly one of the StoredWidth or StoredHeight values are equal to the Maximum Horizontal Pixels or Maximum Vertical Pixels values from Table 4.3: Image Structure Operational Levels below.

d. Verify that both the StoredWidth and StoredHeight values are equal to, or less than, the Maximum Horizontal Pixels or Maximum Vertical Pixels values, respectively, from Table 4.3 below.

e. Verify that both the StoredWidth and StoredHeight values are exactly divisible by two for a 2K file, and four for a 4K file.

An example of the RGBAEssenceDescriptor set is shown below:

```
$ klvwalk -r PerfectMovie-j2c-pt.mxf
...
060e2b34.0253.0101.0d010101.01012900 len: 169 (RGBAEssenceDescriptor)
InstanceUID = 82141918-ce1b-47a5-ac13-c47cfb2e51a7
GenerationUID = 00000000-0000-0000-0000-000000000000
Locators:
SubDescriptors:
92e96e5e-6bef-4985-8117-7dfa541f96fa
LinkedTrackID = 2
SampleRate = 24/1
ContainerDuration = 240
EssenceContainer = 060e2b34.0401.0107.0d010301.020c0100
Codec = 060e2b34.0401.0109.04010202.03010103
FrameLayout = 0
StoredWidth = 2048
StoredHeight = 1080
AspectRatio = 2048/1080
ComponentMaxRef = 4095
ComponentMinRef = 0
...
```

The valid Image Structure Container values are shown in table below.

### Table 4.3.Image Structure Operational Levels

| Operational level | Maximum Horizontal Pixels | MaximumVertical Pixels | Frames per Second |
|---|---|---|---|
| 1 | 4096 | 2160 | 24 |
| 2 | 2048 | 1080 | 48 |
| 3 | 2048 | 1080 | 24 |

- Using the software commands **asdcp-test** and **j2c-scan**, extract an image frame from the file and verify that the bit depth for each component is 12 bits. A component bit-depth value other than 12 shall be cause to fail this test.
  An example of this operation is shown below:

```
$ asdcp-test -d 1 -x frame j2c/PerfectMovie-j2c-pt.mxf
$ j2c-scan frame_000001.j2c
coding parameters
digital cinema profile: none
rsiz capabilities: standard
pixel offset from top-left corner: (0, 0)
tile width/height in pixels: (2048, 1080)
```

```
image width/height in tiles: (1, 1)
...
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 3.2.1.2, 3.2.1.3, 3.2.1.7<br>SMPTE-428-1 |
| **Test Equipment** | **klvwalk**<br>**asdcp-test**<br>**j2c-scan** |

## 4.5.2. Image Compression Standard & Encoding Parameters

### Objective

Verify that the image encoding parameters in a Picture Track File conform to [SMPTE-429-4].

### Procedures

1. Verify that the UL value in the `PictureEssenceCodingfield` of the MXF `RGBAEssenceDescriptor` (see 6 in Example 4.8) is one of:
   `060e2b34.0401.0109.04010202.03010103` (for 2K images) or
   `060e2b34.0401.0109.04010202.03010104` (for 4K images).
   If the UL value does not match one of those listed above, or is the wrong value for the contained essence, this is cause to fail the test.

2. Using a software command such as **asdcp-test**, extract all the frames in the Track File to a directory. An example is shown below.

```
$ asdcp-test -x frame j2c/PerfectMovie-j2c-pt.mxf
$ ls j2c
frame000000.j2c frame000057.j2c frame000124.j2c frame000191.j2c
frame000001.j2c frame000058.j2c frame000125.j2c frame000192.j2c
frame000002.j2c frame000059.j2c frame000126.j2c frame000192.j2c
frame000003.j2c frame000060.j2c frame000127.j2c frame000194.j2c
...
```

3. Verify that every frame is correctly JPEG 2000 encoded as described in [ISO-15444-1]. Verify that the proper JPEG 2000 encoding parameters as specified in [ISO-15444-1-AMD-1] were used. The Codestream Specifications for 2K and 4K distributions are listed in [DCI-DCSS], section 4.4. This can be achieved by using JPEG 2000 decoding software. An example is shown below. (Note that the output of the **j2c-scan** program is long and has been truncated here for brevity. Please see Section C.5 for a detailed example.) If any frame fails to correctly decode or does not conform to the appropriate Codestream Specifications, this is cause to fail the test.

```
$ j2c-scan frame000000.j2c
digital cinema profile: none
rsiz capabilities: standard
pixel offset from top-left corner: (0, 0)
tile width/height in pixels: (2048, 1080)
image width/height in tiles: (1, 1)
tile #1
coding style: 1
progression order: Component-Position-Resolution-Layer
POC marker flag: 0
number of quality layers: 1
```

```
rate for layer #1: 0.0
multi-component transform flag: 1
...
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 3.2.1.5, 4.2, 4.4<br>ISO-15444-1<br>ISO-15444-1-AMD-1<br>SMPTE-429-4 |
| **Test Equipment** | **asdcp-test**<br>**OpenJPEG** |

## 4.5.3. Audio Characteristics

### Objective

Sound Track Files shall conform to the specifications given in [SMPTE-428-2] and [SMPTE-428-3], and be constrained as specified in [SMPTE-429-2]. A Sound Track File shall contain linear PCM audio sampled at 48000 or 96000 samples per second, 24 bits per sample. The file shall contain no more than 16 channels of audio.

### Procedures

Using the software command **klvwalk**, locate the WaveAudioDescriptor set which starts with the Universal Label (UL) of `060e2b34.0253.0101.0d010101.01014800`. An example is shown below.

```
$ klvwalk -r PerfectMovie-pcm-pt.mxf
...
060e2b34.0253.0101.0d010101.01014800 len: 134 (WaveAudioDescriptor)
InstanceUID = e1c4c755-2c3e-4274-a3bf-581aadd63a4b
GenerationUID = 00000000-0000-0000-0000-000000000000
Locators:
SubDescriptors:
LinkedTrackID = 2
SampleRate = 24/1
ContainerDuration = 480
EssenceContainer = 060e2b34.0401.0101.0d010301.02060100
Codec = 00000000.0000.0000.00000000.00000000
AudioSamplingRate = 48000/1
Locked = 0
AudioRefLevel = 0
ChannelCount = 6
QuantizationBits = 24
DialNorm = 0
BlockAlign = 18
SequenceOffset = 0
AvgBps = 144000
...
```

Verify the following:

1. The EssenceContainer field has a value of `060e2b34.0401.0101.0d010301.02060100`. Any other value is cause to fail this test.

2. The ChannelAssignment field is not present, or, if present, has a value from the set of UL values defined in [SMPTE-429-2], Appendix A, "Audio Channel Assignment Label". Any other value in the ChannelAssignment field is cause to

fail this test.

3. The AudioSamplingRate field has a value of either 48000/1 or 96000/1. Any deviation from these values is cause to fail this test.

4. The ChannelCount field has a value of no fewer than six (6) and no greater than sixteen (16). Any deviation from these values is cause to fail this test.

5. The QuantizationBits field has a value of 24. Any other value is cause to fail this test.

6. The BlockAlign field is exactly the value of `ChannelCount * 3`. Any other value is cause to fail this test.

7. The AvgBps field is exactly the value of the `AudioSamplingRate * ChannelCount * 3`. Any other value is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 3.3.2.2, 3.3.4.1<br>SMPTE-428-2<br>SMPTE-428-3<br>SMPTE-429-2 |
| **Test Equipment** | **klvwalk** |

## 4.5.4. Timed Text Resource Encoding

### Objective

- Verify that timed text descriptions in XML conform to [SMPTE-428-7].
- Verify that font resources conform to [ISO-144496].
- Verify that sub-picture resources conform to [ISO-15948].

### Procedures

1. Extract the Timed Text Resource and any Ancillary Resources from the Track File.

2. Verify that the Timed Text Resource is an XML document that can be validated using the schema from [SMPTE-428-7]. If the XML validation produces errors, this is cause to fail this test.

```
$ schema-check testfile.xml S428-7-2007.xsd
$
```

3. Verify that any font resources are valid according to [ISO-144496]. If the font validation produces errors, this is cause to fail this test.

```
$ ftlint 1 font_file.otf
font_file.otf: OK.
$
```

4. Verify that any subpicture resources are valid according to [ISO-15948]. The subpicture must be of PNG format, decode without errors, and the size (geometry) must be smaller than, or equal to, that of the main picture. If the png file causes **identify** to report errors, or if the geometry of the PNG is greater than that of the main picture, this is cause to fail this test.

```
$ identify -verbose subpicture_0001.png
Image: subpicture_0001.png
Format: PNG (Portable Network Graphics)
Geometry: 120x420
Class: DirectClass
Colorspace: RGB
Type: GrayscaleMatte
Depth: 8 bits
...
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 3.4.2.2, 4.4.3.2, 3.4.3.4<br>ISO-144496<br>ISO-15948<br>SMPTE-428-7 |
| **Test Equipment** | **schema-check**<br>**ftlint**<br>**identify** |

# 4.6. Digital Cinema Package

## 4.6.1. DCP Integrity

### Objective

- Verify that the Volume Asset Map is present, correctly formatted, and correctly located in the filesystem.
- Verify that for all the Packing Lists found in the Asset Map file, all of the assets referenced in each Packing List are present and are valid (*i.e.*, each Referenced Asset's file size and Message Digest are correct).
  File Integrity will be guaranteed by applying the SHA-1 hashing algorithm [RFC-3174] to each asset included in the DCP. The resulting message digest is Base64 encoded and included in the Packing List file.
- Verify that for all the Composition Playlists found in each Packing List, the Referenced Assets exist in the Packing List file.

### Procedures

1. Validate the Format of the Volume Asset Map file by executing the test procedure Section 4.1.1: Asset Map File.
2. Validate the Format of the Volume Index file by executing the test procedure Section 4.1.2: Volume Index File.
3. Validate the Format of each Packing List file by executing the test procedure Section 4.2.1: Packing List File.

4. Validate the Signature of each Packing List file by executing the test procedure Section 4.2.2: Packing List Signature Validation.

5. For each Packing List file (*e.g.* PerfectMovie.pkl.xml) in the Asset Map:

    a. Open the Packing List and for each Asset Id contained within:

        i. Locate the Referenced Asset in the filesystem and compare its file size with the value listed in the `<Size>` element of the `<Asset>` element. Inconsistency is cause to fail this test.

        ii. Calculate the Message Digest of the Referenced Asset and encode the result in Base64. Compare the result with the value listed in the `<Hash>` element of the <Asset>element. Inconsistency is cause to fail this test. The following is an example using the **asdcp-test** software utility:

```
$ asdcp-test -t PerfectMovie-j2c-pt.mxf
t0MirEHOVFF4Mi1IP0iYVjrvb14= PerfectMovie-j2c-pt.mxf
```

6. Validate the Format of each Composition Playlist file by executing the test procedure Section 4.3.1: Composition Playlist File.

7. Validate the Signature of each Composition Playlist file by executing the test procedure Section 4.3.2: Composition Playlist Signature Validation.

8. For each Composition Playlist (*e.g.* PerfectMovie.cpl.xml) in the Asset Map:

    a. Open the Composition Playlist and for each Asset Id contained within:

        i. Locate the Asset Id in the Packing List file. Any missing Asset Ids are cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.2.2.6, 5.3.1.9, 5.5.2.3, 5.5.3.2, 9.7.5<br>PKCS-1<br>RFC-3174<br>SMPTE-429-8 |
| **Test Equipment** | **asdcp-test** |

# Chapter 5. Common Security Features

This chapter contains test procedures of security features that apply to more than one type of device. Procedures are given for Type 1 and Type 2 Secure Processing Block (SPB) physical security requirements, Intra-theater communications, and security log reporting.

## 5.1. SPB Security Features

The test procedures in this section apply to any device or component that is classified as a Type 1 or Type 2 SPB.

## 5.1.1. SPB Digital Certificate

### Objective

*This following applies only if the Test Subject is an SPB*

- Verify that the Test Subject carries the correct number of leaf certificates.
- Verify that the leaf certificates conform to [SMPTE-430-2] and Section 9.5.1 of [DCI-DCSS].
- Verify that the roles contained in the Common Name field of the Test Subject certificate(s) accurately reflect the security functions of the Test Subject.
- Verify that the exterior surface of the device containing the Test Subject is labeled with information traceable to the Common Name of the Test Subject.

### Procedures

If the Test Subject is a Media Block:

1. Obtain the Test Subject leaf certificates from the manufacturer, and using manufacturer-supplied documentation, compile the list of expected role identifiers corresponding to the security functions of the Test Subject -- see [SMPTE-430-2], and Section 9.5.1 of [DCI-DCSS] for lists of roles.
2. Verify that exactly three leaf certificates are presented.
3. Verify that each leaf certificate has a distinct Subject DnQualifier value.
4. Verify that each row of Table 5.1 is matched by exactly one of the leaf certificates.
5. For each leaf certificate, verify that each role listed in the Subject Common Name field corresponds to a security function implemented by the Test Subject.
6. For each leaf certificate, verify that the Subject Common Name field contains the serial number of the Test Subject. Additional identifying information may be present.
7. For each leaf certificate, verify that information identifying the make and model of the Test Subject is carried in the Subject field. Additional identifying information may be present.
8. For each leaf certificate, verify that either the make, model and serial number of the Test Subject, or information that is unambiguously traceable by the manufacturer to the Subject field of all certificates, is clearly placed on the exterior of the device containing the Test Subject.
9. Failure to verify any of the conditions above is cause to fail this test.

**Table 5.1.**
**Media**
**Block**

| Roles listed in the Subject Common Name | DigitalSignature flag | KeyEncipherment flag |
|---|---|---|
| includes the SM and MIC roles, but does not include any of the LS, LE and RES roles | false | true |
| includes the SM, MIC and RES roles, but does not include any of the LS and LE roles | false | true |
| includes LS role, and can additionally include the LE role but not any other role | true | false |

For any other Test Subject:

1. Obtain the Test Subject leaf certificates from the manufacturer, and using manufacturer-supplied documentation, compile the list of expected role identifiers corresponding to the security functions of the Test Subject -- see [SMPTE-430-2], and Section 9.5.1 of [DCI-DCSS] for lists of roles.

2. Verify that exactly one leaf certificate is presented.

3. Verify that the Subject Common Name of the leaf certificate presented includes at least one the role combinations listed in Section 9.5.1.1 of [DCI-DCSS] and does not contain any of the role combination listed in Sections 9.5.1.2 and 9.5.1.3 of [DCI-DCSS].

4. Verify that each role listed in the Subject Common Name field of the leaf certificate corresponds to a security function implemented by the Test Subject.

5. Verify that the Subject Common Name field of the leaf certificate collected contains the serial number of the Test Subject. Additional identifying information may be present.

6. Verify that information identifying the make and model of the Test Subject is carried in the Subject field of the leaf certificate. Additional identifying information may be present.

7. Verify that either the make, model and serial number of the Test Subject, or information that is unambiguously traceable by the manufacturer to the Subject field of the leaf certificate, is clearly placed on the exterior of the device containing the Test Subject.

8. Failure to verify any of the conditions above is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.3<br>SMPTE-430-2 |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 18.2. Projector Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

### 5.1.2. Deleted Section

The section "SPB Type 2 Security Perimeter" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

### 5.1.3. Deleted Section

The section "SPB Type 2 Secure Silicon" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 5.2. Intra-Theater Communication

The procedures in this section apply to devices which can initiate or respond to TLS session requests using TCP port 1173.

**Note:**
The DCSS restricts the use of Link Encryption (LE) to non-MMB configurations and non-OBAE processing devices. Therefore LE related tests are not directed to Procedural Chapters 20 and 21.

### 5.2.1. TLS Session Initiation

#### Objective

- Verify that once started, the Security Manager (SM) establishes a TLS session with all SPB devices it is configured to recognize. Verify that each TLS session is persistent until commanded to terminate.
- Verify that once started, a Remote Type 1 SPB responds to the Security Manager's (SM's) initiatives in establishing a Transport Layer Security (TLS) session. Verify that each TLS session is persistent until commanded to terminate.
- Verify that mutual authentication takes place by exchange of device certificates or complete certificate chains. Verify that the Test Subject successfully connects in both cases.

### Procedures

> **Note:**
> This test can involve the use of more than one **asm-responder** simulator program, each with its own device certificate. This places special emphasis on preparing and selecting the correct KDM for a stage of the test. The KDM's TDL needs to be populated with the appropriate certificate thumbprints for the device or combination of devices intended.

If the Test Subject is a Security Manager device:

1. Configure the Test Subject to recognize as many remote SPBs as the system will allow. Record this value.

2. For each remote SPB included in the Test Subject's configuration, set up and start a corresponding **asm-responder** simulator, providing only a single device certificate for authentication. Use the `--requester-certificate-file-dump` option to capture the certificate(s) supplied by the Test Subject during authentication.

   ```
   $ ls -l /home/asm/pem_dir
   total 16
   -rw-r--r-- 1 root root 1606 2009-04-20 04:20 certificate.pem
   -rw-r--r-- 1 root root 1675 2009-04-20 04:20 privatekey.pem
   $ asm-responder \
   --pem-path /home/asm/pem_dir/ \
   --requester-certificate-file-dump foo.pem
   ```

   There shall be one responder for every remote SPB the Test Subject can be configured to use simultaneously.

3. From an unpowered state, power up the Test Subject. Verify that for each responder, the SM establishes a TLS session after startup.

4. Record whether the connection succeeds. Failure to connect successfully is cause to fail this test.

5. For each remote SPB included in the Test Subject's configuration, set up and start a corresponding **asm-responder** simulator, providing the full certificate chain for authentication. Use the `--requester-certificate-file-dump` option to capture the certificate(s) supplied by the Test Subject during authentication.

   ```
   $ ls -l /home/asm/pem_dir
   total 16
   -rw-r--r-- 1 root root 1606 2009-04-20 04:20 certificate.pem
   -rw-r--r-- 1 root root 6258 2009-04-20 04:20 chain.pem
   -rw-r--r-- 1 root root 1675 2009-04-20 04:20 privatekey.pem
   $ asm-responder \
   --pem-path /home/asm/pem_dir/ \
   --requester-certificate-file-dump foo.pem
   ```

   There shall be one responder for every remote SPB the Test Subject can be configured to use simultaneously.

6. From an unpowered state, power up the Test Subject. Verify that for each responder, the SM establishes a TLS session after startup. Record the time reported as each session is established.

7. Record whether the connection succeeds. Failure to connect successfully is cause to fail this test.

8. Verify that leaf certificates are exchanged by both sides during TLS initialization and that the certificates are valid per [SMPTE-430-2] . Signing certificates may also be present. If a complete certificate chain is not issued by the Test Subject, obtain the remainder of the chain from the manufacturer. Verify that the Test Subject's chain is complete and valid.

a. If the Test Subject is a *MB using dual certificate implementation*, verify that the leaf certificate of the Test Subject is a Log Signer Certificate (LS Cert), as defined in Section 9.5.1 of [DCI-DCSS]. Failure of this verification is cause to fail the test.

9. Set up and play a show using the composition *DCI 2K StEM Test Sequence (Encrypted)* and KDM *KDM for 2K StEM Sequence (Encrypted)*.

10. Verify that for each responder, the TLS session remains connected for the duration of the presentation. Failure to meet this requirement is cause to fail this test.

11. Leave the Test Subject and responder powered up until at least 24 hours have elapsed from the time recorded in Step 6, or until the TLS session is noticed to have ended, whichever happens first.

12. Examine the output from each responder for the first occurrence of the TLS session disconnecting. Record the time reported and calculate the duration of the TLS session by subtracting the value recorded in Step 6. A duration exceeding 24 hours without the TLS session closing is cause to fail this test.

13. Verify that each responder reports re-establishment of a new TLS session after a previous session is terminated. Failure to meet this requirement is cause to fail this test.

14. For each successfully connected responder, disconnect the responder from the test network long enough to cause the SM to close the connection (use manufacturer-supplied documentation to determine the appropriate delay).

15. Reconnect the disconnected responder. Verify that the SM re-establishes a TLS session within the time specified by the manufacturer. Failure to re-establish a TLS session is cause to fail this test.

If the Test Subject is a Remote Type 1 SPB:

1. Configure the Test Subject to accept connections from an **asm-requester** simulator.

2. Command the **asm-requester** to connect to the Test Subject, providing only a single device certificate for authentication. Use the `--responder-certificate-file-dump` option to capture the certificate(s) supplied by the Test Subject during authentication.

```
    $ ls -l /home/asm/pem_dir
    total 16
    -rw-r--r-- 1 root root 1606 2009-04-20 04:20 certificate.pem
    -rw-r--r-- 1 root root 1675 2009-04-20 04:20 privatekey.pem
    $ asm-requester --responder-address 192.168.1.100 \
    --pem-path /home/asm/pem_dir/ \
    --responder-certificate-file-dump foo.pem
```

3. Record whether the connection succeeds. Failure to connect successfully is cause to fail this test.

4. Command the **asm-requester** to connect to the Test Subject, providing the full certificate chain for authentication. Use the `--responder-certificate-file-dump` option to capture the certificate(s) supplied by the Test Subject during authentication.

```
$ ls -l /home/asm/pem_dir
total 16
-rw-r--r-- 1 root root 1606 2009-04-20 04:20 certificate.pem
-rw-r--r-- 1 root root 6258 2009-04-20 04:20 chain.pem
-rw-r--r-- 1 root root 1675 2009-04-20 04:20 privatekey.pem
$ asm-requester --responder-address 192.168.1.100 \
```

```
--pem-path /home/asm/pem_dir/ \
--responder-certificate-file-dump foo.pem
```

5. Record whether the connection succeeds. Failure to connect successfully is cause to fail this test.

6. Verify that leaf certificates are exchanged by both sides during TLS initialization and that the certificates are valid per [SMPTE-430-2] . Signing certificates may also be present. If a complete certificate chain is not issued by the Test Subject, obtain the remainder of the chain from the manufacturer. Verify that the Test Subject's chain is complete and valid.

    a. If the Test Subject is an LDB and is not *permanently married to the Projector SPB*, verify that the Test Subject's chain is that of the LDB and not that of the married Projector SPB (see Section 9.4.3.6.5 in [DCI-DCSS]).
    Failure of this verification is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.3.6.2, 9.4.5.2.3, 9.4.3.6.5, 9.5.1, 9.4.5.3.2<br>SMPTE-430-6 |
| **Test Equipment** | **asm-requester**<br>**asm-responder** |
| **Test Materials** | *DCI 2K StEM Test Sequence (Encrypted)*<br>*KDM for 2K StEM Sequence (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2. Auditorium Security Messages

Auditorium Security Messages (ASM) are used to communicate runtime security information between a Security Manager (SM) and a remote Link Decryptor Block (LDB). The following test procedures apply to any device which can initiate (TLS client) or terminate (TLS server) a TLS session.

To test a device which implements ASM, it will be necessary to use an ASM simulator program or any suitably instrumented peer device. To simplify the descriptions in the procedures below, the language assumes the use of an ASM simulator. A detailed description of a reference ASM simulator is given in Appendix D: ASM Simulator.

## 5.2.2.1. Auditorium Security Message Support

### Objective

Verify that Auditorium Security Messages (ASM) are implemented on TCP port number 1173 per [SMPTE-430-6]. Verify that the ASM QuerySPB message is implemented.

### Procedures

If the Test Subject is a Security Manager device:

1. Set up and start an **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Turn on the Test Subject. Verify that the Test Subject establishes a TLS session with the responder after startup.

3. Verify that the Test Subject issues a TCP `open` request on TCP port 1173.

4. Verify that a leaf certificate for the Test Subject is received by the **asm-responder** simulator during TLS initialization and that the certificate is valid per [SMPTE-430-2] . Signing certificates may also be present. If a complete certificate chain is not issued by the Test Subject, obtain the remainder of the chain from the manufacturer. Verify that the Test Subject's chain is complete and valid.

5. Verify that a `QuerySPB` message is sent by the Test Subject no later than 30 seconds after TLS startup (as reported by the responder).

6. Failure to verify all conditions above is cause to fail this test.

7. Re-start the responder using the **--damage-queryspb** option (causes the program to issue malformed `QuerySPB` responses).

8. Re-start the Test Subject. Verify that the Test Subject establishes a TLS session with the responder after startup. The Test Subject may report ASM errors and may ultimately fail in establishing the session. Failure of the Test Subject to attempt to establish a TLS session is cause to fail this test.

9. Extract a security log from the Test Subject and using a **Text Editor**, identify the ASM `LinkException` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `ASMMessageError` exception in the `LinkException` log record. Record any additional parameters associated with the exception. A missing `ASMMessageError` exception in any of the associated `LinkException` log records shall be cause to fail this test.

If the Test Subject is a remote SPB device:

1. Turn on the Test Subject. Allow the device to come to an idle state. Confirm that there are no conditions present that would cause the device to respond to a `QuerySPB` request with an error or security alert.

2. Set up and start an **asm-requester** simulator. Verify that the requester establishes a TLS session with the Test Subject after startup.

```
$ asm-requester (... standard options ...)
```

3. Verify that the Test Subject accepts the respective TCP `open` request on TCP port 1173.

4. Verify that a leaf certificate for the Test Subject is received by the **asm-requester** simulator during TLS initialization and that the certificate is valid per [SMPTE-430-2] . Signing certificates may also be present. If a complete certificate chain is not issued by the Test Subject, obtain the remainder of the chain from the manufacturer. Verify that the Test Subject's chain is complete and valid.

5. Cause the requester to issue the `QuerySPB` message.

6. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6] with a successful General Response element and a Response Status other than Security Alert.

7. Failure to verify all conditions above is cause to fail this test.

8. Re-start the requester using the **--damage-queryspb** option (causes the program to issue malformed `QuerySPB` requests). Allow the program to run for ten (10) seconds then stop it (using [Ctrl-C]).

9. Extract a security log from the Test Subject and using a **Text Editor**, identify the ASM `LinkException` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `ASMMessageError` exception in the `LinkException` log record. Record any additional parameters associated with the exception. A missing `ASMMessageError` exception in any of the associated `LinkException` log records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | [DCI-DCSS], 9.4.3.5, 9.4.5.2.3, 9.4.5.3<br>[SMPTE-430-2]<br>[SMPTE-430-6] |
| **Test Equipment** | **asm-requester**<br>**asm-responder** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.2. ASM Failure Behavior

### Objective

- Verify that an ASM requester continues to operate normally when it receives a ResponderBusy response.
- Verify that an ASM responder provides a response within the recommended delay interval specified in [SMPTE-430-6].
- Verify that an ASM responder provides appropriate security alert response codes for significant security events.

### Procedures

If the Test Subject is an ASM requester:

1. Set up and configure an **asm-responder** simulator. Command the responder to return all ASM requests (except `QuerySPB`) with `ResponderBusy`.

```
$ asm-responder (... standard options ...) \
--respond-with "Busy"
```

2. Initiate an ASM session between the Test Subject and the responder.
3. Set up and play a show using the DCP and KDM contained in *DCI 2K StEM Test Sequence (Encrypted)* and *KDM for 2K StEM Sequence (Encrypted)* (valid DCP). Start of playout of the show shall be cause to fail this test (theSM has not yet collected logs and loaded link keys).
4. Command the responder to respond normally to all ASM requests. Verify that the Test Subject can begin playout of the show without requiring a system restart. Failure to play the show is cause to fail this test.

If the Test Subject is an ASM responder:

1. Initiate an ASM session between an **asm-requester** and the Test Subject
2. Command the requester to issue an arbitrary sequence of requests (*e.g.* LEKeyLoad, LEKeyQuery, ...) and to monitor `QuerySPB` status.

```
$ asm-requester (... standard options ...) \
--messagetype <message-type>
```

   Verify that for each command, the Test Subject responds within the two (2) second maximum delay period recommended by [SMPTE-430-6]. A response delay greater than two seconds shall be cause to fail this test.

3. For Test Subjects which have field-operable perimeter access, open an access panel and verify that the Subject then responds to all `QuerySPB` requests with the `Security Alert` status value and the `success` General Response

value. Failure to report `Security Alert` status is cause to fail this test.

4. For Test Subjects which can participate in marriage to a companion device and be accessed via ASM in the divorced state, place the device in the "divorced" state and verify that the Subject then responds to all `QuerySPB` requests with the `Security Alert` status value and the `success` General Response value. Failure to report `Security Alert` status is cause to fail this test

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.3.2<br>SMPTE-430-6 |
| **Test Equipment** | **asm-requester**<br>**asm-responder** |
| **Test Materials** | *DCI 2K StEM Test Sequence (Encrypted)*<br>*KDM for 2K StEM Sequence (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.3. ASM "RRP Invalid"

### Objective

Verify that an ASM "RRP Invalid" response is supported.

### Procedures

If the Test Subject is an ASM requester:

1. Configure the Test Subject (a MB) to use the **asm-responder** simulator program instead of a normal projector.

2. Initiate an ASM session between the Test Subject and the responder, configured to respond normally to all commands.

```
$ asm-responder (... standard options ...)
```

3. Set up and begin playing a show using the composition *DCI 2K StEM (Encrypted)*, keyed with *KDM for 2K StEM (Encrypted)*.

4. Before the show finishes playing, command the responder to return all ASM requests with a General Response Element `RRP Invalid`(consult the documentation for the **asm-responder** software for detailed information).

5. The Test Subject is required to terminate and prevent further playback not more than 32 seconds after Step 4 is executed. Failure to verify this requirement is cause to fail the test. Note: 32 seconds is the aggregate of the 30 second maximum time allowed between successive `QuerySPB` requests and the 2 second maximum time for response to an ASM command.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5, 9.4.3.5(9a), 9.4.3.5(15)<br>[SMPTE-430-6] |
| **Test Equipment** | **asm-responder** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 5.2.2.4. ASM "GetTime"

### Objective

Verify that the Test Subject implements the `GetTime` command per [SMPTE-430-6].

### Procedures

If the Test Subject is an ASM requester:

1. Initiate an ASM session between the Test Subject and an **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `GetTime` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the responder without error.

3. Failure of the device to implement the `GetTime` command is cause to fail the test.

If the Test Subject is an ASM responder:

1. Initiate an ASM session between an **asm-requester** simulator and the Test Subject.

```
$ asm-requester (... standard options ...)
```

2. Command the requester to issue a `GetTime` request. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Failure to verify the conditions above is cause to fail the test.

4. Record the difference measured between the time value returned and real time as reported by the reference clock.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5<br>[SMPTE-430-6] |
| **Test Equipment** | **asm-responder**<br>**asm-requester**<br>**Accurate Real-Time Clock** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.5. ASM "GetEventList"

### Objective

Verify that the Test Subject implements the `GetEventList` command per [SMPTE-430-6].

### Procedures

If the Test Subject is an ASM requester:

1. Initiate an ASM session between the Test Subject and an **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `GetEventList` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the responder without error.

3. Failure of the device to implement the `GetEventList` command is cause to fail the test.

If the Test Subject is an ASM responder:

1. Initiate an ASM session between an **asm-requester** simulator and the Test Subject, and command the **asm-requester** simulator to issue a `GetEventList` request.

```
$ asm-requester (... standard options ...)
```

2. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Failure to verify the conditions above is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5<br>[SMPTE-430-6] |
| **Test Equipment** | **asm-requester**<br>**asm-responder** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.6. ASM "GetEventID"

### Objective

Verify that the Test Subject implements the `GetEventID` command per [SMPTE-430-6].

### Procedures

Each `GetEventID` procedure call returns an XML document with a top-level element `LogRecord`. See Example 5.2 for more information about this data type. If the Test Subject is an ASM requester:

1. Initiate an ASM session between the Test Subject and an **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `GetEventID` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the responder without error.

3. Failure of the device to issue the `GetEventID` command is cause to fail the test.

If the Test Subject is an ASM responder:

1. 1. Initiate an ASM session between an **asm-requester** simulator and the Test Subject.

```
$ asm-requester (... standard options ...
```

2. Command the requester to issue a `GetEventID` request. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Failure to verify the conditions above is cause to fail the test.

.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | [DCI-DCSS], 9.4.5<br>[SMPTE-430-4]<br>[SMPTE-430-6] |
| **Test Equipment** | **asm-responder**<br>**asm-requester** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.7. ASM "LEKeyLoad"

### Objective

Verify that the Test Subject implements the `LEKeyLoad` command per [SMPTE-430-6].

### Procedures

If the Test Subject is an ASM requester:

1. Initiate an ASM session between the Test Subject and the **asm-responder** simulator program.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `LEKeyLoad` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the **asm-responder** simulator program without error.

3. Examine the output of the **asm-responder** simulator program and verify the Expire Time for each key loaded is 21600 seconds (6 hours). Any delivered LE Key with an Expire Time other than 21600 shall be cause to fail this test.

4. Failure of the device to issue the `LEKeyLoad` command is cause to fail this test. If the Test Subject is an ASM responder:

If the Test Subject is an ASM responder:

1. Initiate an ASM session between the **asm-requester** simulator program and the Test Subject, specifying the `LEKeyLoad` command.

```
$ asm-requester (... standard options ...) \
--messagetype LEKeyLoad
```

2. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Command the simulator to flood the Test Subject with `LEKeyLoad` messages. Verify that the Subject responds to overflow with an appropriate error.

4. Failure to verify the conditions above is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5<br>[SMPTE-430-6] |
| **Test Equipment** | **asm-responder**<br>**asm-requester** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | | — |

| | | | |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 5.2.2.8. ASM "LEKeyQueryID"

### Objective

Verify that the Test Subject implements the LEKeyQueryID command per [SMPTE-430-6].

### Procedures

If the Test Subject is an ASM requester:

1. Initiate an ASM session between the Test Subject and an **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `LEKeyQueryID` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the responder without error.

3. Failure of the device to implement the `LEKeyQueryID` command is cause to fail the test.

If the Test Subject is an ASM responder:

1. Initiate an ASM session between an **asm-requester** and the Test Subject.

```
$ asm-requester (... standard options ...)
```

2. Command the simulator to issue an `LEKeyLoad` request for a new random key. Verify that the Test Subject responds with success within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Command the simulator to issue an `LEKeyQueryID` request for the key loaded in Step 2. Verify that the Test Subject responds with success within the 2 second maximum delay period recommended by [SMPTE-430-6].

4. Command the simulator to issue an `LEKeyQueryID` request for a known bogus key ID. Verify that the Test Subject responds with failure within the 2 second maximum delay period recommended by [SMPTE-430-6].

5. Failure to verify the conditions above is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5<br>[SMPTE-430-6] |

| | |
|---|---|
| **Test Equipment** | **asm-responder**<br>**asm-requester** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.9. ASM "LEKeyQueryAll"

### Objective

Verify that the Test Subject implements the `LEKeyQueryAll` command per [SMPTE-430-6].

### Procedures

If the Test Subject is an ASM requester:

1. Initiate an ASM session between the Test Subject and a **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `LEKeyQueryAll` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the responder without error.

3. Failure of the device to implement the `LEKeyQueryAll` command is cause to fail the test.

If the Test Subject is an ASM responder:

1. Initiate an ASM session between an **asm-requester** simulator and the Test Subject.

```
$ asm-requester (... standard options ...)
```

2. Command the requester to issue a `LEKeyQueryAll` request. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Failure to verify the conditions above is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5<br>SMPTE-430-6 |
| **Test Equipment** | **asm-requester**<br>**asm-responder** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.10. ASM "LEKeyPurgeID"

### Objective

Verify that the Test Subject implements the `LEKeyPurgeID` command per [SMPTE-430-6].

### Procedures

If the Test Subject is an ASM requester:

1. Initiate an ASM session between the Test Subject and an **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `LEKeyPurgeID` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the responder without error.

3. Failure of the device to implement the `LEKeyPurgeID` command is cause to fail the test.

If the Test Subject is an ASM responder:

1. Initiate an ASM session between an **asm-requester** simulator and the Test Subject.

```
$ asm-requester (... standard options ...)
```

2. Command the requester to issue a `LEKeyPurgeID` request. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Failure to verify the conditions above is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5<br>SMPTE-430-6 |
| **Test Equipment** | **asm-responder**<br>**asm-requester** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.11. ASM "LEKeyPurgeAll"

### Objective

Verify that the Test Subject implements the `LEKeyPurgeAll` command per [SMPTE-430-6].

### Procedures

If the Test Subject is an ASM requester:

1. Initiate an ASM session between the Test Subject and an **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `LEKeyPurgeAll` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the responder without error.

3. Failure of the device to implement the `LEKeyPurgeAll` command is cause to fail the test.

If the Test Subject is an ASM responder:

1. Initiate an ASM session between an **asm-requester** simulator and the Test Subject.

```
$ asm-requester (... standard options ...)
```

2. Command the requester to issue a `LEKeyPurgeAll` request. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Failure to verify the conditions above is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5<br>SMPTE-430-6 |
| **Test Equipment** | **asm-requester**<br>**asm-responder** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.2.12. ASM "GetProjCert"

### Objective

*Only applies to a MB that uses Link Encryption (ASM requester) or an LDB (ASM responder).*

Verify that the Test Subject implements the `GetProjCert` command per [SMPTE-430-6].

### Procedures

If the Test Subject is a MB that uses Link Encryption:

1. Initiate an ASM session between the Test Subject and an **asm-responder** simulator.

```
$ asm-responder (... standard options ...)
```

2. Cause the Test Subject to issue a `GetProjCert` request. This can occur during normal operation of the Test Subject or may require the operator to perform a specific set of instructions. Consult with the system manufacturer to determine requirements. Observe that the request is accepted by the responder without error.

3. Failure of the device to implement the `GetProjCert` command is cause to fail the test.

If the Test Subject is an LDB:

1. Initiate an ASM session between an **asm-requester** simulator and the Test Subject.

```
$ asm-requester (... standard options ...)
```

2. Command the requester to issue a `GetProjCert` request. Verify that the Test Subject responds within the 2 second maximum delay period recommended by [SMPTE-430-6].

3. Failure to verify the conditions above is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.3.6.5, 9.4.5.2.4<br>SMPTE-430-6 |
| **Test Equipment** | **asm-responder**<br>**asm-requester** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.2.3. TLS Exception Logging

### Objective

Verify that a `CertFormatError` exception is recorded in the `LinkOpened` security log record in the case that the signing certificate of the device certificate at the other end of the TLS link is of an incorrect format.

Verify that a `TLSError` exception is recorded in the `LinkOpened` security log record in the case that the link fails to open due to an error in the underlying TLS connection.

Verify that a `TLSError` exception is recorded in the `LinkOpened` security log record in the case that an error is detected in the underlying TLS connection.

### Procedures

**Note:**
This test can involve the use of more than one **asm-responder** simulator program, each with its own device certificate.

This places special emphasis on preparing and selecting the correct KDM for a stage of the test. The KDM's TDL needs to be populated with the appropriate certificate thumbprints for the device or combination of devices intended.

If the Test Subject is a Security Manager device:

1. Configure the Test Subject to recognize as many remote SPBs as the system will allow. Record this value.

2. Perform the following procedures:

    a. For each remote SPB included in the Test Subject's configuration, set up and start a corresponding **asm-responder** simulator using device certificates that do not conform to [SMPTE-430-2] (*e.g.* device certificates with SHA1 signatures). There shall be one responder for every remote SPB the Test Subject can be configured to use simultaneously.

    b. From an unpowered state, power up the Test Subject. Verify that for each responder, the SM does not establish a TLS session after startup. If the SM connects to any responder this is cause to fail this test.

    c. Extract a security log from the Test Subject and using a **Text Editor**, identify the `LinkOpened` event associated with the above steps and:

        i. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

        ii. Confirm the presence of a `CertFormatError` exception in the `LinkOpened` log records. Record any additional parameters associated with the exception. A missing `CertFormatError` exception in any of the associated `LinkOpened` log records shall be cause to fail this test.

3. Perform the following procedures:

    a. For each remote SPB included in the Test Subject's configuration, set up and start a corresponding **asm-responder** simulator set to offer an incorrect cyphersuite type to the Test Subject during negotiation. There shall be one responder for every remote SPB the Test Subject can be configured to use simultaneously.

    b. From an unpowered state, power up the Test Subject. Verify that for each responder, the SM does not establish a TLS session after startup. If the SM connects to any responder this is cause to fail this test.

    c. Extract a security log from the Test Subject and using a **Text Editor**, identify the `LinkOpened` event associated with the above steps and:

        i. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

        ii. Confirm the presence of a `TLSError` exception in the `LinkOpened` log records. Record any additional parameters associated with the exception. A missing `TLSError` exception in any of the associated `LinkOpened` log records shall be cause to fail this test.

4. Perform the following procedures:

    a. For each remote SPB included in the Test Subject's configuration, set up and start a corresponding **asm-responder** simulator. There shall be one responder for every remote SPB the Test Subject can be configured to use simultaneously.

b. From an unpowered state, power up the Test Subject. Verify that for each responder, the SM establishes a TLS session after startup.

c. Command each **asm-responder** to inject random data into the raw TLS stream (consult the documentation for the **asm-responder** software for detailed information).

d. Verify that the Test Subject disconnects from each **asm-responder** after the injection of the random data. Failure to close the TLS connection shall be cause to fail this test.

e. Extract a security log from the Test Subject and using a **Text Editor**, identify the `LinkClosed` event associated with the above steps and:

i. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

ii. Confirm the presence of a `TLSError` exception in the `LinkClosed` log records. Record any additional parameters associated with the exception. A missing `TLSError` exception in any of the associated `LinkClosed` log records shall be cause to fail this test.

If the Test Subject is a Remote Type 1 SPB:

1. Perform the following procedures:

a. Configure the Test Subject to accept connections from an **asm-requester** simulator.

b. Command the **asm-requester** to connect to the Test Subject, using a device certificate that does not conform to [SMPTE-430-2] (*e.g.* device certificate with SHA1 signature).

c. Verify that the **asm-requester** does not successfully connect to the Test Subject. If the connection opens this is cause to fail this test.

d. Extract a security log from the Test Subject and using a **Text Editor**, identify the `LinkOpened` event associated with the above steps and:

i. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

ii. Confirm the presence of a `CertFormatError` exception in the `LinkOpened` log record. Record any additional parameters associated with the exception. A missing `CertFormatError` exception in the associated `LinkOpened` log record shall be cause to fail this test.

2. Perform the following procedures:

a. Command the **asm-requester**, set to offer an incorrect cyphersuite type during negotiation to connect to the Test Subject.

b. Verify that the **asm-requester** does not successfully connect to the Test Subject. If the connection opens this is cause to fail this test.

c. Extract a security log from the Test Subject and using a **Text Editor**, identify the `LinkOpened` event associated with the above steps and:

i. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

ii. Confirm the presence of a `TLSError` exception in the `LinkOpened` log record. Record any additional parameters associated with the exception. A missing `TLSError` exception in the associated `LinkOpened` log record shall be cause to fail this test.

3. Perform the following procedures:

a. Command the **asm-requester** to connect to the Test Subject. If the Test Subject does not successfully open the connection this is cause to fail this test

b. Command each **asm-requester** to inject random data into the raw TLS stream (consult the documentation for the **asm-requester** software for detailed information).

c. Verify that the Test Subject disconnects from each **asm-requester** after the injection of the random data. Failure to close the TLS connection shall be cause to fail this test.

d. Extract a security log from the Test Subject and using a **Text Editor**, identify the `LinkClosed` event associated with the above steps and:

i. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

ii. Confirm the presence of a `TLSError` exception in the `LinkClosed` log records. Record any additional parameters associated with the exception. A missing `TLSError` exception in any of the associated `LinkClosed` log records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.3.6.2, 9.4.5.2.3<br>SMPTE-430-2<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **asm-requester**<br>**asm-responder** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.3. Event Logs

Secure Processing Block (SPB) modules are required to provide event log reports on demand. The log reports are XML documents (see Section 3.1) having a structure defined by [SMPTE-430-4]. This section will describe the report format and present procedures for testing general operational requirements for event logging.

**Note:**
The method of generating a log report will vary between implementations. Consult the manufacturer's documentation for log report generation instructions.

### 5.3.1. Log Report Format

Standard d-cinema log reports are encoded as XML documents per [SMPTE-430-4]. The reports consist of a preamble, which identifies the device that created the report, and a sequence of log records. In log reports which contain security events (Security Event Logs), some of the log records may contain XML Signature elements. The report format includes many unique security features; the reader should study [SMPTE-430-4] in detail to understand how log authentication works.

The following subsections detail the major features of a log report

#### 5.3.1.1. Log Report

A collection of one or more log records is presented as an XML document having a single `LogReport` element as the top-level element. The log report begins with `reportDate` and `reportingDevice` elements. The contents of the elements identify the time the log was created and the device that created the log

**Example 5.1. Log Report Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<LogReport 1
  xmlns="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/" 2
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/">
  <reportDate>2007-05-04T09:30:47-08:00</reportDate> 3
  <reportingDevice> 4
    <dcml:DeviceIdentifier idtype="CertThumbprint">YmVsc3dpY2tAZW50ZXJ0ZWNoLmNvbQ==
    </dcml:DeviceIdentifier>
    <dcml:DeviceTypeID scope="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes#DeviceTyp
    </dcml:DeviceTypeID>
    <dcml:AdditionalID>vnqteTcB2Gji\+1Hl23sxxgOqvwE=</dcml:AdditionalID> 5
    <dcml:DeviceSerial>000000042</dcml:DeviceSerial> 6
    <dcml:ManufacturerCertID>rlpve6MSncWouNIpFcTSIhk6w2A=</dcml:ManufacturerCertID> 7
    <dcml:DeviceCertID>9czqa+0orIADHDIYxAkn/IcmZ3o=</dcml:DeviceCertID>
    <dcml:ManufacturerName>Acme Digital Cinema Inc.</dcml:ManufacturerName>
    <dcml:DeviceName>Mojo Media Block</dcml:DeviceName>
    <dcml:ModelNumber>MB-3000</dcml:ModelNumber>
    <dcml:VersionInfo>
      <dcml:Name>Bootloader</dcml:Name>
```

```
      <dcml:Value>1.0.0.0</dcml:Value>
      <dcml:Name>Security Module</dcml:Name>
      <dcml:Value>3.4.2.1</dcml:Value>
    </dcml:VersionInfo>
  </reportingDevice>
```

1 The `LogReport` element is the root element of a log report document.

2 The `LogRecord` and DCML namespaces are used

3 This value gives the date on which this report document was generated

4 This structure identifies the device that generated this report

5 For log reports generated by an SM that implements dual certificates (see Section 9.5.1.2 at [DCI-DCSS]), the AdditionalID element is present and contains a thumbprint of the SM Log Signer digital certificate

6 The serial number of reporting device

7 The certificate thumbprint (per [SMPTE-430-2]) of the reporting device

### 5.3.1.2. Log Record

Each event contained in the log report is encoded as a `LogRecordElement` element. This element type has three major sub-elements: `LogRecordHeader`, `LogRecordBody`, and `LogRecordSignature`. The first two are shown in the example below, the last is the subject of the next section.

**Note:**
The log record element defined in [SMPTE-430-4] is known by two names. The correct name to use depends on context. Testing a candidate document against the `LogRecord` schema will verify correct use. When a log record (defined as the complex type `logRecordType` in the `LogRecord` schema) appears as a sub-element of a `LogReport` element, the record element name is `LogRecordElement`. When a log record appears as the root element of an XML document, the record element name is `LogRecord`.

`LogRecord` elements are used directly (without a containing `LogReport` parent element) as the return value from an ASM `GetEventID` procedure (see Section 5.2.2.6.) Because ASM procedures are executed exclusively via TLS with a trusted peer, the `LogRecordSignature` element is not required for that particular use.

## Example 5.2. Log Report Record Example

```
<LogRecordElement 1
  xmlns="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/">
  <LogRecordHeader>
    <EventID>urn:uuid:8a221dfc-f5c6-426d-a2b8-9f6ff1cc6e31</EventID> 2
    <TimeStamp>2005-12-17T10:45:00-05:00</TimeStamp> 3
    <EventSequence>1000003</EventSequence> 4
    <DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">kkqiVpDUAggQDHyHz0x9cDcsseU=</dcml:PrimaryID
    </DeviceSourceID>
    <EventClass>http://www.smpte-ra.org/430.5/2007/SecurityLog/</EventClass> 5
    <EventType scope="http://www.smpte-ra.org/430.5/2007/SecurityLog/#EventTypes">Key</Eve
```

```
6
    <contentId>urn:uuid:733365c3-2d44-4f93-accd-43cb39b0cedf</contentId> 7
    <previousHeaderHash>9czqa+0orIADHDIYxAkn/IcmZ3o=</previousHeaderHash> 8
    <recordBodyHash>9czqa+0orIADHDIYxAkn/IcmZ3o=</recordBodyHash> 9
  </LogRecordHeader>
  <LogRecordBody>
    <EventID>urn:uuid:8a221dfc-f5c6-426d-a2b8-9f6ff1cc6e31</EventID>
    <EventSubType scope="http://www.smpte-ra.org/430.5/2007/SecurityLog/#EventSubTypes-key
      KDMKeysReceived
    </EventSubType> 10
    <Parameters> 11
      <dcml:Parameter>
        <dcml:Name>SignerID</dcml:Name>
        <dcml:Value xsi:type="ds:DigestValueType">rlpve6MSncWouNIpFcTSIhk6w2A=</dcml:Value
      </dcml:Parameter>
    </Parameters>
    <Exceptions> 12
      <dcml:Parameter>
        <dcml:Name>KDMFormatError</dcml:Name>
        <dcml:Value xsi:type="xs:string">XML validation failed on line 36</dcml:Value>
      </dcml:Parameter>
    </Exceptions>
    <ReferencedIDs> 13
      <ReferencedID>
        <IDName>CompositionID</IDName>
        <IDValue>urn:uuid:64bb6972-13a0-1348-a5e3-ae45420ea57d</IDValue>
      </ReferencedID>
      <ReferencedID>
        <IDName>KeyDeliveryMessageID</IDName>
        <IDValue>urn:uuid:64bb6972-13a0-1348-a5e3-ae45420ea57d</IDValue>
      </ReferencedID>
    </ReferencedIDs>
  </LogRecordBody>
</LogRecordElement>
```

1 The `LogRecordElement` element contains a single log record, corresponding to a single system event. If the log record is the root element of an XML document, the element name will be `LogRecord`.

2 A UUID value that uniquely identifies this event. This ID must be the same wherever this event appears (*i.e.*, if the event appears in more than one report, the ID will be the same.)

3 The time and date at which the event occurred.

4 The sequence number of this event in the report. This element should not be used in a stand-alone LogRecord element.

5 The event *Class (e.g., Security*.)

6 The event *Type (e.g., Key*.)

7 Gives the UUID most closely associated with the content element that was being handled when the event occurred. This element should not be used in a stand-alone `LogRecord` element

8 The SHA-1 message digest of the `Header` element in the record that preceded this one in the report. This element should not be used in a stand-alone `LogRecord` element

9 The SHA-1 message digest of the `Body` element contained within the same parent `LogRecordElement` or `LogRecord` element

10 Describes the event *Sub-type (e.g., KDMKeysReceived*.)

11 A list of parameters which augment the event sub-type.

12 If an exception (an error) occurred during the procedure that generated the event, this element will contain a list of tokens which describe the error.

13 A list of important identifiers that existed in the procedure context when the event occurred.

### 5.3.1.3. Log Record Signature

An XML Signature is used to create a tamper-proof encoding. The signature is made over the contents of the `RecordAuthData` element as shown in the following example. The `RecordAuthData` element contains the digest of the containing record's `LogRecordHeader` element. Consult [SMPTE-430-4] for details on extending the signature's proof of authenticity to preceding records via the contents of the header's `previousHeaderHash` element.

## Example 5.3. Log Report Signature Example

```
<LogRecordSignature> 1
  <HeaderPlacement>stop</HeaderPlacement>
  <SequenceLength>2</SequenceLength>
  <RecordAuthData Id="ID_RecordAuthData"> 2
    <RecordHeaderHash>SG93IE1hbnkgTW9yZSBSZXZpc2lvbnM/</RecordHeaderHash> 3
    <SignerCertInfo> 4
      <ds:X509IssuerName>CN=DistCo-ca,OU=DistCo-ra,O=DistCo-ra,
        dnQualifier=vnqteTcB2Gji\+1Hl23sxxgOqvwE=</ds:X509IssuerName>
      <ds:X509SerialNumber>16580</ds:X509SerialNumber>
    </SignerCertInfo>
  </RecordAuthData>
  <Signature> 5
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2001031
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha256" />
      <ds:Reference URI="#ID_RecordAuthData">
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>VGhpcyBvbmx5IHRvb2sgdHdvIHllYXJz</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      Vqe6MS0pHovkfqhHlkt/NNEI1GGchCW/EyqxOccSenuzNQc63qL+VIQoIJCcwgnE0i/w/8bIgjfB
      PrsOW5M3zlR0eAZc7tt6f7q50taNmC+O2wfATVXqEE8KC32qO//NQHuOL6bLLH+12oqgR5fS/mlI
      /wpn8s/pAtGA9lAXDRp03EVOvzwq0m9AjzOxIbgzGg6AIY0airJ1gecT1qccb1zGQjB81pr3ctlp
      ECchubtSCqh+frRn4CZc4ZRMLhjnax/zwHIG4ExiMCEKbwaz7DwN8zv1yoPUzut9ik7X0EyfRIlv
      F3piQoLeeFcFrkfNwYyyhTX8iHTO4Cz8YfGNyw==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509IssuerSerial>
          <ds:X509IssuerName>Sample Issuer Name</ds:X509IssuerName>
          <ds:X509SerialNumber>1234567</ds:X509SerialNumber>
        </ds:X509IssuerSerial>
        <!-- X509 certificate value as block of Base64 encoded characters, -->
        <!-- truncated for brevity -->
        <ds:X509Certificate>
          QSBDZXJ0aWZpY2F0ZSB3b3VsZCBiZSBsb25nZXIgdGhhbiB0aGlz</ds:X509Certificate>
      </ds:X509Data>
      <ds:X509Data>
        <ds:X509IssuerSerial>
          <ds:X509IssuerName>Sample Issuer Name 2</ds:X509IssuerName>
        </ds:X509IssuerSerial>
        <!-- X509 certificate value as block of Base64 encoded characters, -->
        <!-- truncated for brevity -->
        <ds:X509Certificate>TG9uZ2VyIHRoYW4gdGhpcyB0b28sIGZvciBzdXJl</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </Signature>
</LogRecordSignature>
```

1. The `LogRecordSignature` contains the signature of a log record.
2. The `RecordAuthData` element is the content that is actually signed for the signature. This element is identified for the signature processor by the Id attribute value
3. A message digest value calculated over the sibling `Header` element.
4. This information identifies the creator of the XML Signature (the document's signer.)
5. A standard XML Signature element.

#### 5.3.1.4. Log Report Signature Validation

XML Signatures on log reports can be checked using the procedure in Section 3.1.3.

#### 5.3.1.5. Log Record Proxy

As specified in Section 9.4.6.3.1 of [DCI-DCSS], the Image Media Block SM collects source log record from all remote SPBs in the suite it enables and includes (proxies) them in log reports it generates. In order to ensure that information is preserved during the proxy process, the following requirements apply:

- The namespace of all elements shall remain identical between source and proxied record, regardless of the presence or absence of default namespace, choice of namespace prefixes and scope of namespace declarations. A namespace declaration in the source record that is not used by any element may be omitted in the proxied record.
- Unless otherwise required, all elements present in the source event shall be present and unaltered in the proxied event. Examples of elements expected to be omitted or altered are `recordBodyHash` (which may change due to changes in namespace declarations), `EventSequence` (as the sequence will necessarily change in the log report), `TimeStamp` (as the compensation of remote SPB time offset by the SM using the ASM `GetTime` request may cause this value to change), `LogRecordSignature` and its children elements (as a new signature will apply to the log report). Elements that are proprietary in nature, *e.g.* an unrecognized "Parameter" name/value pair, shall always be preserved.
- All element attributes that exist in the source events shall be present in the relevant elements in the proxied event.
- The `TimeStamp` local timezone representation in the source events shall not be changed in the proxied events, *i.e.* the requirements of Section 7.1.2 in [SMPTE-430-4] are the responsibility of the remote SPB for that event and shall not be modified further on producing the proxied events in the log report.
- The `EventID` element values shall not be altered.

### 5.3.2. Event Log Operations

#### 5.3.2.1. Log Structure

##### Objective

Verify that that the Log Report retrieved from a security manager (SM):

- is an XML document and that it validates against the XML schemas defined with [SMPTE-430-4] and [SMPTE-433].
- contains urn:uuid values as specified in [RFC-4122].

##### Procedures

1. Set up and play a show using the following composition:

   - *DCI 2K StEM (OBAE) (Encrypted)* keyed with *KDM for 2K StEM (Encrypted) (OBAE)*, if the Test Subject is an OMB; or

   - *DCI 2K StEM (Encrypted)* keyed with *KDM for 2K StEM (Encrypted)*, otherwise.

2. Extract a security log report from the Test Subject that includes the range of time during which the above steps were carried out.

3. Using the **schema-check** software utility, validate the XML file structure against the XML schemas in [SMPTE-430-4] and [SMPTE-433]. Failure to correctly validate is cause to fail this test. For more information on schema validation see Section 3.1.2: XML Schema.

```
$ schema-check <input-file> smpte-433.xsd smpte-430-4.xsd
schema validation successful
```

4. Supply the filename of the Log Report file as an argument to the **uuid_check.py** software utility. Examine the output for error messages that identify expected UUID values that do not conform to the format specified in [RFC-4122]. One or more occurrences is cause to fail this test, unless the non-conforming value is derived from an external source (*i.e.*, a DCP or KDM). Examples of fields that record external values are the parameters "KeyDeliveryMessageID", "CompositionID" and "TrackFileID", and the header element "contentId".

```
$ uuid_check.py <input-file>
all UUIDs conform to RFC-4122
$
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.2<br>RFC-4122<br>SMPTE-430-4<br>SMPTE-433 |
| **Test Equipment** | **schema-check**<br>**uuid_check.py** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)*<br>*DCI 2K StEM (OBAE) (Encrypted)*<br>*KDM for 2K StEM (Encrypted) (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.3.2.2. Log Records for Multiple Remote SPBs

### Objective

*Only applies to an MB Security Manager (SM) which can be configured to use more than one remote SPB.*

Verify that in the case of reports covering the use of multiple remote SPBs, proxied log records are correctly identified with the source SE's identity.

### Procedures

**Note:**
This test involves the use of more than one **asm-responder** simulator program, each with it's own device certificate. This places special emphasis on preparing and selecting the correct KDM for a stage of the test. The KDM's TDL needs to be populated with the appropriate certificate thumbprints for the device or combination of devices intended.

1. Configure the Test Subject to recognize as many remote SPBs as the system will allow. Record this value.

2. For each remote SPB included in the Test Subject's configuration, set up and start a corresponding **asm-responder** simulator. There shall be one responder for every remote SPB the Test Subject can be configured to use simultaneousl.

3. Set up and play a show using the composition *DCI 2K StEM (Encrypted)*, keyed with the KDM *KDM for DCI 2K StEM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation* (KDM containing a TDL listing the certificate thumbprints required by the Test Subject to enable playback of the special auditorium situation identified in Step 1). Failure to play the show completely shall be cause to fail this test

4. Retrieve a log report from the SM covering the time period during which steps 1 - 3 were performed. Verify that the log report contains at least one ASM `LinkOpened` record, with a `DeviceSourceID` element that contains the certificate thumbprint of the respective responder device, for each configured responder. Failure to locate a `LinkOpened` record from each responder shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1 |
| **Test Equipment** | **Text Editor** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for DCI 2K StEM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB | | | |

| | | | |
|---|---|---|---|
| Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 5.3.2.3. Log Sequence Numbers

### Objective

Verify that the security manager (SM) maintains a secure and persistent counter to provide a unique sequential `EventSequence` number to each log record it creates. Verify that this `EventSequence` number appears in the Header node of each log record in a report.

### Procedures

1. Set up and play a show using the composition *DCI 2K StEM (Encrypted)*, keyed with *KDM for 2K StEM (Encrypted)*.

2. Extract a security log report from the Test Subject that includes the range of time during which the above steps were carried out.

3. Examine the log report using a **Text Editor**. Verify that the header in each record contains an `EventSequence` value that is one greater than the value in the previous record.

4. Failure to correctly sequence log records in a report shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1, 9.4.6.3.4<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **Text Editor** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.3.2.4. Log Collection by the SM

### Objective

Verify that the SM collects log information from all remote SPBs in the suite it enables, at the earliest equipment idle time. Verify that TLS sessions are not terminated prior to collection of all remote SPB log data.

### Procedures

1. Configure the Test Subject (a MB) to use the **asm-responder** simulator program.

2. Set up and begin playing a show using the composition *DCI 2K StEM (Encrypted)*, keyed with *KDM for 2K StEM (Encrypted)*.

3. Before the show finishes playing, configure the **asm-responder** to respond to `GetEventList` and `GetEventID` requests with a Busy General Response code.

4. Before the show finishes playing, command the **asm-responder** to create an `SPBClockAdjust` log record with a `TimeStamp` value corresponding to the current time. Note: No actual time adjustment is intended to be made as a result of this step, the value of the `TimeOffset` element in the resulting log record is expected to be zero, or close to zero.

5. After completion of the playback allow 5 minutes to elapse.

6. Confirm that the **asm-responder** is receiving `GetEventList` or `GetEventID` messages from the Test Subject.

7. Configure the **asm-responder** to respond normally to `GetEventList` and `GetEventID` messages

8. Leave the system idle for 5 minutes, then extract a security log report from the Test Subject. Indication from **asm-responder** that the TLS session was terminated anytime between the completion of the playback and the transmission of log records to the Test Subject is cause to fail this test.

9. Using a **Text Editor**, locate the `SPBClockAdjust` record created in step 4 by the **asm-responder** during the playout. Absence of the record is is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **asm-responder**<br>**Text Editor** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 5.3.2.5. General Log System Failure

### Objective

- Verify that the SM requires that the secure logging subsystem is operating as a prerequisite to playback.
- Verify that the SM will not enable for playback any remote SPB for which it has not collected, or cannot collect log records, or where there is any indication that the remote SPB will not record and report log records as required.

### Procedures

1. Configure the Test Subject (a MB) to use the **asm-responder** simulator program.
2. Set up and begin playing a show using the DCP and KDM contained in *DCI 2K StEM (Encrypted)* and *KDM for 2K StEM (Encrypted)* (valid DCP).
3. Before the show finishes playing, configure the ASM responder to respond to `GetEventList` and `GetEventID` requests with a Busy General Response code.
4. After completion of the playback allow 5 minutes to elapse.
5. Attempt to set up and play the show created in step 2.
6. If the SM allows playout, this shall be cause to fail this test.
7. Configure the ASM responder to respond normally to `GetEventList` and `GetEventID` requests.
8. Attempt to set up and play the show created in step 2.
9. If the SM does not allow playout, this shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1 |
| **Test Equipment** | **asm-responder** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 5.3.2.6. Log Report Signature Validity

### Objective

Verify that the Test Subject provides log event information in the form of Log Reports

Verify that all Log Records within a Log Report are properly authenticated as specified in [SMPTE-430-4] and [SMPTE-430-5].

Verify that the Log Report is signed by the SM.

Verify that EventID for a given event is maintained across collections.

### Procedures

> **Note:**
> The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

*If the Test Subject uses a single certificate implementation as defined in Section 9.5.1.1 of [DCI-DCSS]:*

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.

2. Extract a Log Report from the Test Subject covering the time period during which Step 1 was performed.

3. Leave the system idle for no less than 1 minute, then extract a second security Log Report from the Test Subject covering the time period during which Step 1 was performed.

4. Using a **Text Editor**, locate in each of the Log Reports extracted in Steps 2 and 3 the `CPLStart` record. Failure for the records in the two reports to have the same `EventID` value is cause to fail this test. *Note: The following steps shall use the Log Report extracted in Step 2*.

5. Using a **Text Editor**, verify that the root element of the Log Report is `LogReport`. Failure of this verification is cause to fail the test.

6. Using a **Text Editor**, identify all individually signed Log Records and sequences of Log Records, as defined in [SMPTE-430-5]. Failure for any Log Record to either be signed individually or be part of a sequence is cause to fail this test.

7. Authenticate each individually signed Log Record identified in Step 4 as specified in [SMPTE-430-4] and [SMPTE-430-5], including:

    a. Validating the `recordBodyHash` elements as specified in Section 6.1.1.5 of [SMPTE-430-5]; and

    b. Validating the `LogRecordSignature` element as specified in Section 7.3 of [SMPTE-430-4] and Section 6.1.3 of [SMPTE-430-5].

Failure to authenticate any individually signed Log Record is cause to fail the test.

8. Authenticate each sequence of Log Records identified in Step 4 as specified in Section 9 of [SMPTE-430-4], including:

    a. Validating the `previousHeaderHash` (unless the Log Record is the first of a sequence) and `recordBodyHash` elements as specified in Section 6.1.1.5 of [SMPTE-430-5];

    b. Validating the authenticated chain as specified in Section 9 of [SMPTE-430-4]; and

    c. Validating the `LogRecordSignature` element as specified in Section 7.3 of [SMPTE-430-4] and Section 6.1.3 of [SMPTE-430-5].

    Failure to authenticate any sequence of Log Records is cause to fail the test.

9. Using a **Text Editor**, locate one `LogRecordSignature` element. Using its `X509IssuerName` and `X509SerialNumber` from the `SignerCertInfo` element, locate elements that match in one of the `KeyInfo` elements and extract the device certificate from its `X509Certificate` element. Absence of a device certificate or mismatched `X509IssuerName` and `X509SerialNumber` values shall be cause to fail the test.

10. Obtain the SM certificate of the Test Subject.

11. Using **openssl**, compare the certificate obtained in Step 10 to the device certificate obtained in Step 9. Mismatch between the two certificates shall be cause to fail the test.

*If the Test Subject uses a dual certificate implementation as defined in Section 9.5.1.2 of [DCI-DCSS]:*

1. Perform Steps 1-9 above.

2. Obtain the SM and LS certificates of the Test Subject.

3. Using a **Text Editor**, verify that the `LogReport` element contains a single `reportingDevice` child element as defined in [SMPTE-430-4]. Failure of this verification is cause to fail this test.

4. Using a **Text Editor**, verify that the `reportingDevice` element meets the following requirements. Failure to meet any of these requirements is cause to fail this test.

    a. If the `idtype` attribute of the `DeviceIdentifier` element is equal to `"DeviceUID"`, the `DeviceCertID` element shall also be present and shall contain the certificate thumbprint of the SM Certificate.

    b. If the `idtype` attribute of the `DeviceIdentifier` element is equal to `"DeviceUID"`, it shall contain the device UUID of the Test Subject.

    c. If the `idtype` attribute of the `DeviceIdentifier` element is equal to `"CertThumbprint"`, it shall contain the certificate thumbprint of the SM Certificate of the Test Subject.

    d. The `AdditionalID` element shall be present and its value set to the certificate thumbprint of the LS Certificate, encoded as an `ds:DigestValueType` type.

5. Using **openssl**, compare the LS certificate obtained in Step 2 to the device certificate obtained in Step 9 above. Mismatch between the two certificates shall be cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1, 9.4.6.3.3, 9.4.6.3.7, 9.5.1.1, 9.5.1.2<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-433 |
| **Test Equipment** | **Text Editor**<br>**openssl** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.3.2.7. Log Sequence Numbers (OBAE)

### Objective

Verify that the OBAE-capable security manager (SM) maintains a secure and persistent counter to provide a unique sequential `EventSequence` number to each log record it creates. Verify that this `EventSequence` number appears in the Header node of each log record in a report.

### Procedures

1. Set up and play a show using the composition *DCI 2K StEM (OBAE) (Encrypted)*, keyed with *KDM for 2K StEM (Encrypted) (OBAE)*.

2. Extract a security log report from the Test Subject that includes the range of time during which the above steps were carried out.

3. Examine the log report using a **Text Editor**. Verify that the header in each record contains an `EventSequence` value that is one greater than the value in the previous record.

4. Failure to correctly sequence log records in a report shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1, 9.4.6.3.4<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **Text Editor** |
| **Test Materials** | *DCI 2K StEM (OBAE) (Encrypted)*<br>*KDM for 2K StEM (Encrypted) (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 5.3.2.8. Log Report Signature Validity (OBAE)

### Objective

Verify that the OBAE-capable Test Subject provides log event information in the form of Log Reports

Verify that all Log Records within a Log Report are properly authenticated as specified in [SMPTE-430-4] and [SMPTE-430-5].

Verify that the Log Report is signed by the SM.

Verify that EventID for a given event is maintained across collections.

### Procedures

**Note:**
The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

*If the Test Subject uses a single certificate implementation as defined in Section 9.5.1.1 of [DCI-DCSS]:*

1. Set up and play a show using the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*.

2. Extract a Log Report from the Test Subject covering the time period during which Step 1 was performed.

3. Leave the system idle for no less than 1 minute, then extract a second security Log Report from the Test Subject covering the time period during which Step 1 was performed.

4. Using a **Text Editor**, locate in each of the Log Reports extracted in Steps 2 and 3 the `CPLStart` record. Failure for the records in the two reports to have the same `EventID` value is cause to fail this test. *Note: The following steps shall use the Log Report extracted in Step 2.*

5. Using a **Text Editor**, verify that the root element of the Log Report is `LogReport`. Failure of this verification is cause to fail the test.

6. Using a **Text Editor**, identify all individually signed Log Records and sequences of Log Records, as defined in [SMPTE-430-5]. Failure for any Log Record to either be signed individually or be part of a sequence is cause to fail this test.

7. Authenticate each individually signed Log Record identified in Step 4 as specified in [SMPTE-430-4] and [SMPTE-430-5], including:

    a. Validating the `recordBodyHash` elements as specified in Section 6.1.1.5 of [SMPTE-430-5]; and

b. Validating the `LogRecordSignature` element as specified in Section 7.3 of [SMPTE-430-4] and Section 6.1.3 of [SMPTE-430-5].

Failure to authenticate any individually signed Log Record is cause to fail the test.

8. Authenticate each sequence of Log Records identified in Step 4 as specified in Section 9 of [SMPTE-430-4], including:

    a. Validating the `previousHeaderHash` (unless the Log Record is the first of a sequence) and `recordBodyHash` elements as specified in Section 6.1.1.5 of [SMPTE-430-5];

    b. Validating the authenticated chain as specified in Section 9 of [SMPTE-430-4]; and

    c. Validating the `LogRecordSignature` element as specified in Section 7.3 of [SMPTE-430-4] and Section 6.1.3 of [SMPTE-430-5].

    Failure to authenticate any sequence of Log Records is cause to fail the test.

9. Using a **Text Editor**, locate one `LogRecordSignature` element. Using its `X509IssuerName` and `X509SerialNumber` from the `SignerCertInfo` element, locate elements that match in one of the `KeyInfo` elements and extract the device certificate from its `X509Certificate` element. Absence of a device certificate or mismatched `X509IssuerName` and `X509SerialNumber` values shall be cause to fail the test.

10. Obtain the SM certificate of the Test Subject.

11. Using **openssl**, compare the certificate obtained in Step 10 to the device certificate obtained in Step 9. Mismatch between the two certificates shall be cause to fail the test.

*If the Test Subject uses a dual certificate implementation as defined in Section 9.5.1.2 of [DCI-DCSS]:*

1. Perform Steps 1-9 above.

2. Obtain the SM and LS certificates of the Test Subject.

3. Using a **Text Editor**, verify that the `LogReport` element contains a single `reportingDevice` child element as defined in [SMPTE-430-4]. Failure of this verification is cause to fail this test.

4. Using a **Text Editor**, verify that the `reportingDevice` element meets the following requirements. Failure to meet any of these requirements is cause to fail this test.

    a. If the `idtype` attribute of the `DeviceIdentifier` element is equal to `"DeviceUID"`, the `DeviceCertID` element shall also be present and shall contain the certificate thumbprint of the SM Certificate.

    b. If the `idtype` attribute of the `DeviceIdentifier` element is equal to `"DeviceUID"`, it shall contain the device UUID of the Test Subject.

    c. If the `idtype` attribute of the `DeviceIdentifier` element is equal to `"CertThumbprint"`, it shall contain the certificate thumbprint of the SM Certificate of the Test Subject.

    d. The `AdditionalID` element shall be present and its value set to the certificate thumbprint of the LS Certificate, encoded as an `ds:DigestValueType` type.

5. Using **openssl**, compare the LS certificate obtained in Step 2 to the device certificate obtained in Step 9 above. Mismatch between the two certificates shall be cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1, 9.4.6.3.3, 9.4.6.3.7, 9.5.1.1, 9.5.1.2<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-433 |
| **Test Equipment** | **Text Editor**<br>**openssl** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 5.3.3. SM Proxy of Log Events

## 5.3.3.1. SM Proxy of Log Events

### Objective

Verify that an SM can proxy (for a remote SPB) log records which contain an unknown class or type of information.

### Procedures

1. Configure the Test Subject to use the **asm-responder** program as a remote SPB (a virtual LDB). Configure the **asm-responder** to return the set of proprietary test messages. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

```
$ asm-responder (...standard options...) \
--preload-log-event Prop1.xml \
--preload-log-event Prop2.xml \
--preload-log-event Prop3.xml
```

*Note: The "proprietary" test messages are valid [SMPTE-430-4] log records that contain class or type information not defined in a standard document.*

*Note: The timestamp of the preloaded events must be set to a value that will occur after the time the ASM connection is established and before the time that the composition finishes playing. This ensures that the preloaded events are in a time period that is expected to be collected by the SM during the operations of this test.*

2. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.

3. After completion of the playback, wait until the Test Subject collects the security logs (as evidenced by `GetEventList` and `GetEventID` ASM requests).

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record each of Class `Debug`, Type `Info`, Event Subtype `Prop1`, `Prop2`, and `Prop3`.

6. Verify that each event identified in the previous step has correctly formatted parameters as defined in Appendix D and preserves source record information as specified in Section 5.3.1.5.

7. Failure to correctly record each of the proprietary events shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-responder**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 5.3.3.2. SM Proxy of Security Operations Events

### Objective

Verify that an SM can proxy (for a remote SPB) log records which contain correctly coded Security Operations events per [SMPTE-430-5].

### Procedures

1. Configure the Test Subject to use the **asm-responder** program as a remote SPB (a virtual LDB). Configure the **asm-responder** to return the set of Operations test messages. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

```
$ asm-responder (...standard options...) \
--preload-log-event SPBOpen.xml \
--preload-log-event SPBClose.xml \
--preload-log-event SPBMarriage.xml \
--preload-log-event SPBDivorce.xml \
--preload-log-event SPBShutdown.xml \
--preload-log-event SPBStartup.xml \
--preload-log-event SPBClockAdjust.xml \
--preload-log-event SPBSoftware.xml \
--preload-log-event SPBSecurityAlert
```

*Note: The timestamp of the preloaded events must be set to a value that will occur after the time the ASM connection is established and before the time that the composition finishes playing. This ensures that the preloaded events are in a time period that is expected to be collected by the SM during the operations of this test.*

2. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.

3. After completion of the playback, wait until the Test Subject collects the security logs (as evidenced by `GetEventList` and `GetEventID` ASM requests).

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record each of Class `Security`, Type `Operations`, Event Subtypes `SPBOpen`, `SPBClose`, `SPBMarriage`, `SPBDivorce`, `SPBShutdown`, `SPBStartup`, `SPBClockAdjust`, `SPBSoftware`, and`SPBSecurityAlert`.

6. Verify that each event identified in the previous step has correctly formatted parameters as defined in [SMPTE-430-5] and preserves source record information as specified in Section 5.3.1.5.

7. Failure to correctly record each of the Operations events shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-responder**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |

## 5.3.3.3. SM Proxy of Security ASM Events

### Objective

Verify that an SM can proxy (for a remote SPB) log records which contain correctly coded Security ASM events per [SMPTE-430-5].

### Procedures

1. Configure the Test Subject to use the **asm-responder** program as a remote SPB (a virtual LDB). Configure the **asm-responder** to return the set of ASM test messages.. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

```
$ asm-responder (...standard options...) \
--preload-log-event LinkOpened.xml \
--preload-log-event LinkClosed.xml \
--preload-log-event LinkException.xml \
--preload-log-event LogTransfer.xml \
--preload-log-event KeyTransfer.xml \
--preload-log-event BogusLogFormat.xml
```

   *Note: The timestamp of the preloaded events must be set to a value that will occur after the time the ASM connection is established and before the time that the composition finishes playing. This ensures that the preloaded events are in a time period that is expected to be collected by the SM during the operations of this test.*

2. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.

3. After completion of the playback, wait until the Test Subject collects the security logs (as evidenced by `GetEventList` and `GetEventID` ASM requests).

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record each of Class `Security`, Type `ASM`, Event Subtypes `LinkOpened`, `LinkClosed`, `LinkException`, `LogTransfer`, and `KeyTransfer`.

6. Verify that each event identified in the previous step has correctly formatted parameters as defined in [SMPTE-430-5] and preserves source record information as specified in Section 5.3.1.5. Failure to correctly record each of the ASM events shall be cause to fail this test.

7. Verify the presence of one `LogTransfer` event that contains an `ASMLogRequestFailed` exception caused by the `BogusLogFormat.xml` LogRecord. Record any additional parameters associated with the exception. A missing `ASMLogRequestFailed` exception in the associated `LogTransfer` log record shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |

| | |
|---|---|
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-responder**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 5.3.3.4. Remote SPB Time Compensation

### Objective

- Verify that the SM uses the `GetTime` ASM command information to calculate the difference between true time (the SM's time) and time in remote SPBs, and remove the difference in reporting remote SPB event data.
- Verify that the SM tracks the time difference between remote SPB clocks and its internal clock by issuance of the `GetTime` ASM command at least once per day.

### Procedures

1. Configure the Test Subject to recognize as many remote SPBs as the system will allow. Record this value.
2. For each remote SPB included in the Test Subject's configuration:
    a. Advance the system clock of the **Computer with POSIX OS** that will run the **asm-responder** simulator by 15 minutes.
    b. Set up and start a corresponding **asm-responder** simulator. There shall be one responder for every remote SPB the Test Subject can be configured to use simultaneously.
3. Set up a show containing the composition *DCI 2K StEM (Encrypted)*, keyed with *KDM for 2K StEM (Encrypted)* if the number of remote SPBs recorded in Step 1 is one, or *KDM for 2K StEM with Device Specific Special Auditorium TDL* if more than one.
4. Play the show and record the UTC time as provided by an **Accurate Real-Time Clock** at the start of playback.

5. After completion of the playback, wait until the Test Subject collects the security logs (as evidenced by `GetEventList` and `GetEventID` ASM requests).

6. Examine the output from the **asm-responder** for the presence of a `GetTime` ASM request. Absence of a `GetTime` ASM message is cause to fail this test.

7. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

8. Identify the type `<Key>`, subtype `<KeyTransfer>` LogRecords from each remote SPB which were collected in Step 5. This can be accomplished by locating the string "Event recorded by asm-responder" that is recorded as the value of the `<Name>` element of a `<Parameter>` element contained in the `<KeyTransfer>` events from the **asm-responder**.

9. Verify that for each remote SPB, one or more events of type `<Key>`, subtype `<KeyTransfer>` exist that have `<TimeStamp>` elements with values that differ by no more than +/- two seconds from the `<TimeStamp>`s of the corresponding events recorded by the Test Subject. *Note: Use the time recorded in Step 4 to locate the playout of the show in the security log. The Test Subject will record `<KeyTransfer>` events before this time. The corresponding `<KeyTransfer>` events recorded by the remote SPBs will be collected after the show finished playback.* Failure to identify `<TimeStamp>`s corrected to within +/- two seconds shall be cause to fail this test.

10. Allow the Test Subject, in an idle state, to remain connected to the **asm-responder** for 24 hours. Verify that the `GetTime` ASM command is issued at least once every 24 hours. If the `GetTime` command is not received at least once every 24 hours, this shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.5, 9.4.6.3.1<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-responder**<br>**Accurate Real-Time Clock** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)*<br>*KDM for 2K StEM with Device Specific Special Auditorium TDL* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |

## 5.4. Security Log Events

Secure Processing Blocks (SPB) are required to record Security Log Events (defined in [SMPTE-430-5]) upon the occurrence of certain operational states. The procedures in this section should cause the Test Subject to record the respective events.

## 5.4.1. Playout, Validation and Key Events

### 5.4.1.1. FrameSequencePlayed Event

#### Objective

Verify that the SM can produce log records which contain correctly coded `FrameSequencePlayed` events per [SMPTE-430-5].

#### Procedures

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Playout`, Event Subtype `FrameSequencePlayed`.

4. Verify that the `FrameSequencePlayed` record has correctly formatted parameters as defined in [SMPTE-430-5].

5. Failure to correctly record a `FrameSequencePlayed` shall be cause to fail this test.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

#### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.1.2. CPLStart Event

### Objective

Verify that the SM can produce log records which contain correctly coded `CPLStart` events per [SMPTE-430-5].

### Procedures

> **Note:**
> The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Playout`, Event Subtype `CPLStart`.

4. Verify that the `CPLStart` record has correctly formatted parameters as defined in [SMPTE-430-5].

5. Failure to correctly record a `CPLStart` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.1.3. CPLEnd Event

### Objective

Verify that the SM can produce log records which contain correctly coded `CPLEnd` events per [SMPTE-430-5].

### Procedures

**Note:**
The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Playout`, Event Subtype `CPLEnd`.

4. Verify that the `CPLEnd` record has correctly formatted parameters as defined in [SMPTE-430-5].

5. Failure to correctly record a `CPLEnd` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.1.4. PlayoutComplete Event

### Objective

Verify that the SM can produce log records which contain correctly coded `PlayoutComplete` events per [SMPTE-430-5].

### Procedures

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Playout`, Event Subtype `PlayoutComplete`.

4. Verify that the `PlayoutComplete` record has correctly formatted parameters as defined in [SMPTE-430-5].

5. Failure to correctly record a `PlayoutComplete` shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.1.5. CPLCheck Event

### Objective

Verify that the SM can produce log records which contain correctly coded `CPLCheck` events per [SMPTE-430-5].

### Procedures

1. If present, delete the composition *DCI 2K Sync Test (Encrypted)* from the Test Subject.

2. Ingest the composition *DCI 2K Sync Test (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the ingest is started.

3. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 2, less one minute. Verify that the log contains at least one record of Class `Security`, Type `Validation`, Event Subtype `CPLCheck`.

6. Verify that the `CPLCheck` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `CPLCheck` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.1.6. KDMKeysReceived Event

### Objective

Verify that the SM can produce log records which contain correctly coded `KDMKeysReceived` events per [SMPTE-430-5].

### Procedures

1. Delete from the Test Subject any existing KDMs for the composition *DCI 2K Sync Test (Encrypted)*.

2. Ingest the KDM *KDM for DCI 2K Sync Test (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the ingest is started.

3. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events near or after the time recorded in Step 2. Verify that the log contains at least one record of Class `Security`, Type `Key`, Event Subtype `KDMKeysReceived`.

6. Verify that the `KDMKeysReceived` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `KDMKeysReceived` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 5.4.1.7. KDMDeleted Event

### Objective

Verify that the SM can produce log records which contain correctly coded `KDMDeleted` events per [SMPTE-430-5].

### Procedures

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Delete from the Test Subject any KDMs for the composition *DCI 2K Sync Test (Encrypted)*.

3. Attempt to play the composition *DCI 2K Sync Test (Encrypted)*. Successful playback shall be cause to fail this test.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events near or after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Key`, Event Subtype `KDMDeleted`.

6. Verify that the `KDMDeleted` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `KDMDeleted` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.1.8. FrameSequencePlayed Event (OBAE)

### Objective

Verify that the IMBO or OMB can produce, for an OBAE presentation, log records which contain correctly coded `FrameSequencePlayed` events per [SMPTE-430-5].

### Procedures

1. Set up and play a show using the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Extract a security log from the IMBO or OMB that includes the range of time during which the above Steps were carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Playout`, Event Subtype `FrameSequencePlayed` associated with the OBAE essence in *DCI 2K Sync Test (OBAE) (Encrypted)*.

4. Verify that the `FrameSequencePlayed` record has correctly recorded parameters as defined in [SMPTE-430-5].

5. Verify that the `Parameters` list of the `FrameSequencePlayed` record contains a name/value pair whose `Name` element contains the token `OBAEMark`, and whose `Value` element shall contain one of two tokens, either `true` or `false`, indicating that a forensic mark was or was not inserted during playout.

6. Failure to correctly record a `FrameSequencePlayed` as detailed above shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.1.9. CPLStart Event (OBAE)

### Objective

Verify that the OBAE-capable SM can produce log records which contain correctly coded `CPLStart` events per [SMPTE-430-5].

### Procedures

**Note:**
The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by

the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Playout`, Event Subtype `CPLStart`.

4. Verify that the `CPLStart` record has correctly formatted parameters as defined in [SMPTE-430-5].

5. Failure to correctly record a `CPLStart` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 5.4.1.10. CPLEnd Event (OBAE)

### Objective

Verify that the OBAE-capable SM can produce log records which contain correctly coded `CPLEnd` events per [SMPTE-430-5].

### Procedures

**Note:**
The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

1. Set up and play a show using the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Playout`, Event Subtype `CPLEnd`.

4. Verify that the `CPLEnd` record has correctly formatted parameters as defined in [SMPTE-430-5].

5. Failure to correctly record a `CPLEnd` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 5.4.1.11. PlayoutComplete Event (OBAE)

### Objective

Verify that the OBAE-capable SM can produce log records which contain correctly coded `PlayoutComplete` events per [SMPTE-430-5].

### Procedures

1. Set up and play a show using the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Playout`, Event Subtype `PlayoutComplete`.

4. Verify that the `PlayoutComplete` record has correctly formatted parameters as defined in [SMPTE-430-5].

5. Failure to correctly record a `PlayoutComplete` shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 5.4.1.12. CPLCheck Event (OBAE)

### Objective

Verify that the OBAE-capable SM can produce log records which contain correctly coded `CPLCheck` events per [SMPTE-430-5].

### Procedures

1. If present, delete the composition *DCI 2K Sync Test (OBAE) (Encrypted)* from the Test Subject.

2. Ingest the composition *DCI 2K Sync Test (OBAE) (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the ingest is started.

3. Set up and play a show using the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 2, less one minute. Verify that the log contains at least one record of Class `Security`, Type `Validation`, Event Subtype `CPLCheck`.

6. Verify that the `CPLCheck` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `CPLCheck` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 5.4.1.13. KDMKeysReceived Event (OBAE)

### Objective

Verify that the OBAE-capable SM can produce log records which contain correctly coded `KDMKeysReceived` events per [SMPTE-430-5].

### Procedures

1. Delete from the Test Subject any existing KDMs for the composition *DCI 2K Sync Test (OBAE) (Encrypted)*.

2. Ingest the KDM *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the ingest is started.

3. Set up and play a show using the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events near or after the time recorded in Step 2. Verify that the log contains at least one record of Class `Security`, Type `Key`, Event Subtype `KDMKeysReceived`.

6. Verify that the `KDMKeysReceived` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `KDMKeysReceived` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |

| | |
|---|---|
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |

## 5.4.1.14. KDMDeleted Event (OBAE)

### Objective

Verify that the OBAE-capable SM can produce log records which contain correctly coded `KDMDeleted` events per [SMPTE-430-5].

### Procedures

1. Set up and play a show using the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*. With an **Accurate Real-Time Clock**, note the UTC time at the moment the playback is started.

2. Delete from the Test Subject any KDMs for the composition *DCI 2K Sync Test (OBAE) (Encrypted)*.

3. Attempt to play the composition *DCI 2K Sync Test (OBAE) (Encrypted)*. Successful playback shall be cause to fail this test.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events near or after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Key`, Event Subtype `KDMDeleted`.

6. Verify that the `KDMDeleted` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `KDMDeleted` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **DCI Projector**<br>**Accurate Real-Time Clock**<br>**Text Editor** |

| | |
|---|---|
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 5.4.2. ASM and Operations Events

### 5.4.2.1. LinkOpened Event

#### Objective

- Verify that the SM can produce log records which contain correctly coded `LinkOpened` events per [SMPTE-430-5].
- Verify that a remote SPB can produce log records which contain correctly coded `LinkOpened` events per [SMPTE-430-5].

#### Procedures

If the Test Subject is a Media Block that supports ASM:

1. Configure the Test Subject to use the **asm-responder** program as a remote SPB (a virtual LDB). With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

```
$ asm-responder (...standard options...)
```

2. Extract a security log from the Test Subject that includes the range of time during which the above Step was carried out.
3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `ASM`, Event Subtype `LinkOpened`.
4. Verify that the `LinkOpened` record has correctly formatted parameters as defined in [SMPTE-430-5].
5. Failure to correctly record a `LinkOpened` event shall be cause to fail this test.

If the Test Subject is an LDB or LD/LE (remote SPB):

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. With an **Accurate Real-Time Clock**, note the UTC time at the moment the **asm-requester** connects to the Test Subject.

```
$ asm-requester (...standard options...)
```

2. Extract a security log from the Test Subject that includes the range of time during which the above Step was carried out.

3. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1, less 1 minute. Verify that the log contains at least one record of Class `Security`, Type `ASM`, Event Subtype `LinkOpened`.

4. Verify that the `LinkOpened` record has correctly formatted parameters as defined in [SMPTE-430-5].

5. Failure to correctly record a `LinkOpened` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | *Computer with POSIX OS*<br>*asm-responder*<br>*asm-requester*<br>*Accurate Real-Time Clock*<br>*Text Editor* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.4.2.2. LinkClosed Event

### Objective

- Verify that the SM can produce log records which contain correctly coded `LinkClosed` events per [SMPTE-430-5].

- Verify that a remote SPB can produce log records which contain correctly coded `LinkClosed` events per [SMPTE-430-5].

### Procedures

If the Test Subject is a Media Block that supports ASM:

1. Configure the Test Subject to use the **asm-responder** program as a remote SPB (a virtual LDB). Start the **asm-responder**. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

```
$ asm-responder (...standard options...)
```

2. From the idle state, power down the Test Subject using the procedure recommended by the manufacturer.*Note: If the procedure is to interrupt line power, this Step is operationally equivalent to Step 4*.

3. Power up the Test Subject, wait for the system to become idle. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

4. Interrupt line power to the Test Subject. *Note: If applicable, make sure that the projector lamp is off when interrupting power*.

5. Power up the Test Subject, wait for the system to become idle. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

6. Cause the **asm-responder** to disconnect from the Test Subject (*e.g.* quit the program).

7. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

8. Using a **Text Editor**, examine the log report for events corresponding to the Test Subject. Verify that these events include at least one record of Class `Security`, Type `ASM`, Event Subtypes `LinkClosed`, for each period

    a. between the times recorded in Step 1 and Step 3; and

    b. between the times recorded in Step 3 and Step 5; and

    c. after the time recorded in Step 5.

9. Verify that each `LinkClosed` record has correctly formatted parameters as defined in [SMPTE-430-5].

10. Failure to correctly record a `LinkClosed` event shall be cause to fail this test.

If the Test Subject is an LDB or LD/LE (remote SPB):

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. Command **asm-requester** to initiate a TLS session with the Test Subject. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-requester**.

```
$ asm-requester (...standard options...)
```

2. From the idle state, power down the Test Subject using the procedure recommended by the manufacturer. *Note:If the procedure is to interrupt line power, this Step is operationally equivalent to Step 4*.

3. Power up the Test Subject, wait for the system to become idle. Command **asm-requester** to initiate a TLS session with the Test Subject. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-requester**.

4. Interrupt line power to the Test Subject. *Note: If applicable, make sure that the projector lamp is off when interrupting power*.

5. Power up the Test Subject, wait for the system to become idle. Command **asm-requester** to initiate a TLS session with the Test Subject. With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-requester**.

6. Cause the **asm-requester** to disconnect from the Test Subject (*e.g.* quit the program).

7. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

8. Using a **Text Editor**, examine the log report for events corresponding to the Test Subject. Verify that these events include at least one record of Class `Security`, Type `ASM`, Event Subtypes `LinkClosed`, for each period:

    a. between the times recorded in Step 1 and Step 3; and

    b. between the times recorded in Step 3 and Step 5; and

    c. after the time recorded in Step 5.

9. Verify that each `LinkClosed` record has correctly formatted parameters as defined in [SMPTE-430-5].

10. Failure to correctly record a `LinkClosed` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-responder**<br>**asm-requester**<br>**Accurate Real-Time Clock**<br>**Text Editor** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.4.2.3. LinkException Event

### Objective

- Verify that the SM can produce log records which contain correctly coded `LinkException` events per [SMPTE-430-5].

- Verify that a remote SPB can produce log records which contain correctly coded `LinkException` events per [SMPTE-430-5]

### Procedures

If the Test Subject is a Media Block that supports ASM:

1. Configure the Test Subject to use the **asm-responder** program as a remote SPB (a virtual LDB). With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

```
$ asm-responder (...standard options...)
```

2. From the idle state, disconnect the ASM communication channel (*i.e.*, the Ethernet) to the **asm-responder**

3. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*. Playback shall not occur. Successful playback shall be cause to fail this test.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `ASM`, Event Subtype `LinkException`

6. Verify that the `LinkException` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `LinkException` event shall be cause to fail this test.

If the Test Subject is an LDB or LD/LE (remote SPB):

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. With an **Accurate Real-Time Clock**, note the UTC time at the moment the **asm-requester** connects to the Test Subject.

```
$ asm-requester (...standard options...)
```

2. From the idle state, disconnect the ASM communication channel (*i.e.*, the Ethernet) to the **asm-requester**.

3. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried ou

4. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `ASM`, Event Subtype `LinkException`

5. Verify that the `LinkException` record has correctly formatted parameters as defined in [SMPTE-430-5].

6. Failure to correctly record a `LinkException` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-responder**<br>**asm-requester** |

| |
|---|
| **Accurate Real-Time Clock**<br>**Test Materials**<br>**Text Editor**<br><br>*DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.4.2.4. LogTransfer Event

### Objective

- Verify that the SM can produce log records which contain correctly coded `LogTransfer` events per [SMPTE-430-5].
- Verify that a remote SPB can produce log records which contain correctly coded `LogTransfer` events per [SMPTE-430-5].

### Procedures

If the Test Subject is a Media Block that supports ASM:

1. Configure the Test Subject to use the **asm-responder** program as a remote SPB (a virtual LDB). With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

```
$ asm-responder (...standard options...)
```

2. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.
3. After completion of the playback, wait until the Test Subject collects the security logs (as evidenced by `GetEventList` and `GetEventID` ASM requests).
4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.
5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `ASM` and Event Subtype `LogTransfer` generated by the Test Subject. Note: `LogTransfer` records generated by the **asm-responder** can be identified by the presence of a `Parameter` with a `Name` element containing the concatenation of the string "Event recorded by **asm-responder**" and the certificate thumbprint of the **asm-responder**.

6. Verify that the `LogTransfer` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `LogTransfer` event shall be cause to fail this test.

If the Test Subject is an LDB or LD/LE (remote SPB):

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. With an **Accurate Real-Time Clock**, note the UTC time at the moment the **asm-requester** connects to the Test Subject.

```
$ asm-requester (...standard options...)
```

2. Command the **asm-requester** to send a `GetEventList` command to the Test Subject for a date range in which the time recorded in Step 1 is included. E.g:

```
Please enter the desired start and stop times ("YYYY-MM-DDThh:mm:ss/YYYY-MM-DDThh:mm:ss"):
(press 'x' to return to the previous menu).
Press control-C to quit.
2009-01-01T00:00:00/2009-05-01T00:00:00
2009-04-09T18:35:26Z For request no. 0
 Retrieved 2 items from the list: [0, 1]
 General response status: successful
```

3. Command the **asm-requester** to send a `GetEventID` command to the Test Subject for an event ID that was returned from the previous Step. E.g:

```
  Please enter the desired event ID:
(press 'x' to return to the previous menu).
Press control-C to quit.
1
2009-04-09T18:38:30Z For request no. 1
    General response status: successful
[Returned LogRecord omitted for brevity]
```

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `ASM`, Event Subtype `LogTransfer`.

6. Verify that the `LogTransfer` record has correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record a `LogTransfer` shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-responder**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)* |

| |
|---|
| *KDM for DCI 2K*<br>*Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.4.2.5. KeyTransfer Event

### Objective

- Verify that the SM can produce log records which contain correctly coded `KeyTransfer` events per [SMPTE-430-5].
- Verify that a remote SPB can produce log records which contain correctly coded `KeyTransfer` events per [SMPTE-430-5].

### Procedures

If the Test Subject is a Media Block that supports ASM:

1. Configure the Test Subject to use the **asm-responder** program as a remote SPB (a virtual LDB). With an **Accurate Real-Time Clock**, note the UTC time at the moment the Test Subject connects to the **asm-responder**.

```
$ asm-responder (...standard options...)
```

2. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.
3. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.
4. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `ASM`, Event Subtype `KeyTransfer`.
5. Verify that the `KeyTransfer` record has correctly formatted parameters as defined in [SMPTE-430-5].
6. Failure to correctly record a `KeyTransfer` shall be cause to fail this test

If the Test Subject is an LDB or LD/LE (remote SPB):

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. With an **Accurate Real-Time Clock**, note the UTC time at the moment the **asm-requester** connects to the Test Subject.

```
$ asm-requester (...standard options...)
```

2. Command the **asm-requester** to send a `LEKeyLoad` command to the Test Subject. E.g:

```
Please enter the key ID, hexadecimal key, validity period,
          and AES decrypt seed separated by tabs or spaces:
(press 'x' to return to the previous menu).
Press control-C to quit.
          01 9337555bb1121e0d284f3968cbe22fef 36000 42
2009-04-08T18:07:08Z For request no. 0
                     the request fit within the confines of the LDB key buffer
        General response status: successful
```

3. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

4. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `ASM`, Event Subtype `KeyTransfer`.

5. Verify that the `KeyTransfer` record has correctly formatted parameters as defined in [SMPTE-430-5].

6. Failure to correctly record a `KeyTransfer` shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-responder**<br>**asm-requester**<br>**Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 5.4.2.6. SPBStartup and SPBShutdown Events

### Objective

- Verify that the SM can produce log records which contain correctly coded `SPBStartup` and `SPBShutdown` events per [SMPTE-430-5].

- Verify that a remote SPB can produce log records which contain correctly coded `SPBStartup` and `SPBShutdown` events per [SMPTE-430-5].

### Procedures

If the Test Subject is a Media Block:

1. Power up the Test Subject. With an **Accurate Real-Time Clock**, note the UTC time at the moment the power is applied.

2. Wait for the system to become idle.

3. Power down the Test Subject using the procedure recommended by the manufacturer. With an *Accurate Real-Time Clock*, note the UTC time at the moment the shutdown procedure is initiated.

4. Wait for the system to power down completely.

5. Power up the Test Subject. With an **Accurate Real-Time Clock**, note the UTC time at the moment the power is applied.

6. Wait for the system to become idle.

7. Interrupt line power to the Test Subject and associated suite equipment. With an **Accurate Real-Time Clock**, note the UTC time at the moment the power is removed. *Note: If applicable, make sure that the projector lamp is off when interrupting power*.

8. Wait for the system to power down completely.

9. Power up the Test Subject and associated suite equipment, wait for the system to become idle.

10. Extract a security log report from the Test Subject that includes the range of time during which the above steps were carried out.

11. Using a **Text Editor**, examine the log report for events recorded by the Test Subject. Verify that these events include at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBStartup` and `SPBShutdown`, for each of (a) between the times recorded in step 1 and step 5 and (b) after the time recorded in step 5.

12. Verify that the `SPBStartup` and `SPBShutdown` records have correctly formatted parameters as defined in [SMPTE-430-5].

13. Failure to correctly record `SPBStartup` and `SPBShutdown` events shall be cause to fail this test.

If the Test Subject is an LDB or LD/LE (remote SPB):

1. Power up the Test Subject. With an **Accurate Real-Time Clock**, note the UTC time at the moment the power is applied.

2. Wait for the system to become idle.

3. Power down the Test Subject using the procedure recommended by the manufacturer. With an **Accurate Real-Time Clock**, note the UTC time at the moment the shutdown procedure is initiated.

4. Wait for the system to power down completely.

5. Power up the Test Subject. With an **Accurate Real-Time Clock**, note the UTC time at the moment the power is applied.

6. Wait for the system to become idle.

7. Interrupt line power to the Test Subject. With an **Accurate Real-Time Clock**, note the UTC time at the moment the power is removed. *Note: If applicable, make sure that the projector lamp is off when interrupting power*.

8. Wait for the system to power down completely.

9. Power up the Test Subject and associated suite equipment, wait for the system to become idle.

10. Configure the Test Subject to use the **asm-requester** program as a virtual SM.

```
$ asm-requester (...standard options...)
```

11. Extract security log records from the Test Subject that includes the range of time during which the above steps was carried out.

12. Using a **Text Editor**, examine the log records for events recorded by the Test Subject. Verify that these events include at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBStartup` and `SPBShutdown`, for each of (a) between the times recorded in step 1 and step 5 and (b) after the time recorded in step 5.

13. Verify that the `SPBStartup` and `SPBShutdown` records have correctly formatted parameters as defined in [SMPTE-430-5].

14. Failure to correctly record `SPBStartup` and `SPBShutdown` events shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-requester**<br>**Accurate Real-Time Clock**<br>**Text Editor** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.2.7. SPBOpen and SPBClose Events

### Objective

- Verify that the SM of a Media Block, integrated or married to a projector, can produce log records which contain correctly coded `SPBOpen` and `SPBClose` events per [SMPTE-430-5].

- Verify that a remote SPB (LDB), integrated or married to a projector, can produce log records which contain correctly coded `SPBOpen` and `SPBClose` events per [SMPTE-430-5].

### Procedures

If the Test Subject is a Media Block integrated or married with a Projector:

1. Power up the Test Subject and associated suite equipment, with an **Accurate Real-Time Clock**, note the UTC time at the moment the power is applied. Wait for the system to become idle.

2. Open a secure perimeter access door. Wait one minute, close the access door.

3. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

4. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBOpen` and `SPBClose`.

5. Verify that the `SPBOpen` and `SPBClose` records have correctly formatted parameters as defined in [SMPTE-430-5].

6. Failure to correctly record `SPBOpen` and `SPBClose` events shall be cause to fail this test.

If the Test Subject is an LDB (remote SPB) integrated or married with a Projector:

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. With an **Accurate Real-Time Clock**, note the UTC time at the moment the **asm-requester** connects to the Test Subject.

```
$ asm-requester (...standard options...)
```

2. Open a secure perimeter access door. Wait one minute, close the access door.

3. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

4. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBOpen` and `SPBClose`.

5. Verify that the `SPBOpen` and `SPBClose` records have correctly formatted parameters as defined in [SMPTE-430-5].

6. Failure to correctly record `SPBOpen` and `SPBClose` events shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-requester**<br>**Accurate Real-Time Clock**<br>**Text Editor** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.2.8. SPBClockAdjust Event

### Objective

- Verify that the SM can produce log records which contain correctly coded `SPBClockAdjust` events per [SMPTE-430-5].
- Verify that a remote SPB can produce log records which contain correctly coded `SPBClockAdjust` events per [SMPTE-430-5].

### Procedures

If the Test Subject is a Media Block:

1. Power up the Test Subject and associated suite equipment, with an **Accurate Real-Time Clock**, note the UTC time at the moment the power is applied. Wait for the system to become idle.

2. Using the manufacturer's documented procedure, adjust the clock of the Test Subject.

3. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

4. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBClockAdjust`.

5. Verify that the `SPBClockAdjust` records have correctly formatted parameters as defined in [SMPTE-430-5].

6. Failure to correctly record a `SPBClockAdjust` event shall be cause to fail this test.

If the Test Subject is an LDB or LD/LE (remote SPB):

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. With an **Accurate Real-Time Clock**, note the UTC time at the moment the **asm-requester** connects to the Test Subject.

```
$ asm-requester (...standard options...)
```

2. Using the manufacturer's documented procedure, adjust the clock of the Test Subject.

3. Extract a security log from the Test Subject that includes the range of time during which the above Step was carried out.

4. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtype `SPBClockAdjust`.

5. Verify that the `SPBClockAdjust` record has correctly formatted parameters as defined in [SMPTE-430-5].

6. Failure to correctly record a `SPBClockAdjust` event shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-requester**<br>**Accurate Real-Time Clock**<br>**Text Editor** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.2.9. SPBMarriage and SPBDivorce Events

### Objective

- Verify that the SM of a Media Block, married to a projector, can produce log records which contain correctly coded `SPBMarriage` and `SPBDivorce` events per [SMPTE-430-5].

- Verify that a remote SPB (LDB), married to a projector, can produce log records which contain correctly coded `SPBMarriage` and `SPBDivorce` events per [SMPTE-430-5].

### Procedures

If the Test Subject is a Media Block married with a Projector:

1. Power up the Test Subject and associated suite equipment, with an **Accurate Real-Time Clock**, note the UTC time at the moment the power is applied. Wait for the system to become idle.

2. Using the manufacturer's documented procedure, divorce the Media Block from its Projector SPB2.

3. Using the manufacturer's documented procedure, remarry the Media Block to its Projector SPB2.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBMarriage` and `SPBDivorce`.

6. Verify that the `SPBMarriage` and `SPBDivorce` records have correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record `SPBMarriage` and `SPBDivorce` events shall be cause to fail this test.

If the Test Subject is an LDB (remote SPB) married with a Projector:

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. With an **Accurate Real-Time Clock**, note the UTC time at the moment the **asm-requester** connects to the Test Subject.

```
$ asm-requester (...standard options...)
```

2. Using the manufacturer's documented procedure, divorce the LDB from its Projector SPB2.

3. Using the manufacturer's documented procedure, remarry the LDB to its Projector SPB2.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

5. Using a **Text Editor**, examine the log report for events occurring after the time recorded in Step 1. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBMarriage` and `SPBDivorce`.

6. Verify that the `SPBMarriage` and `SPBDivorce` records have correctly formatted parameters as defined in [SMPTE-430-5].

7. Failure to correctly record `SPBMarriage` and `SPBDivorce` events shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-requester**<br>**Accurate Real-Time Clock**<br>**Text Editor** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 5.4.2.10. SPBSoftware Event

### Objective

- Verify that the SM can produce log records which contain correctly coded `SPBSoftware` events per [SMPTE-430-5].
- Verify that a remote SPB can produce log records which contain correctly coded `SPBSoftware` events per [SMPTE-430-5].

### Procedures

If the Test Subject is a Media Block:

1. Power up the Test Subject and associated suite equipment, with an **Accurate Real-Time Clock**, note the UTC time at the moment the power is applied. Wait for the system to become idle.
2. Perform the following procedures:
    a. Using the manufacturer's documented procedure, perform a software installation on the Test Subject.
    b. Return the Test Subject to the idle state (reboot after software installation is acceptable).
    c. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

d. Using a **Text Editor**, examine the log report for events corresponding to the above steps. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBSoftware`.

e. Verify that the `SPBSoftware` records have correctly formatted parameters as defined in [SMPTE-430-5].

f. Failure to correctly record a `SPBSoftware` event shall be cause to fail this test.

3. Perform the following procedures:

a. Attempt a software installation on the Test Subject using a procedure that will cause the update to fail in some fashion (*e.g.* provide wrong signer for the update, incorrect message digest in module, consult with the manufacturer for additional assistance).

b. Return the Test Subject to the idle state.

c. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

d. Using a **Text Editor**, examine the log report for events corresponding to the above steps. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBSoftware`.

e. Verify that the `SPBSoftware` records have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

f. Confirm the presence of a `SoftwareFailure` exception in the `SPBSoftware` log record. Record any additional parameters associated with the exception. A missing `SoftwareFailure` exception in the associated `SPBSoftware` log record shall be cause to fail this test.

If the Test Subject is an LDB or LD/LE (remote SPB):

1. Configure the Test Subject to use the **asm-requester** program as a virtual SM. With an **Accurate Real-Time Clock**, note the UTC time at the moment the **asm-requester** connects to the Test Subject.

```
$ asm-requester (...standard options...)
```

2. Perform the following procedures:

a. Using the manufacturer's documented procedure, perform a software installation on the Test Subject.

b. Return the Test Subject to the idle state (reboot after software installation is acceptable).

c. Extract a security log from the Test Subject that includes the range of time during which the above Step was carried out.

d. Using a **Text Editor**, examine the log report for events corresponding to the above steps. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtype `SPBSoftware`.

e. Verify that the `SPBSoftware` record has correctly formatted parameters as defined in [SMPTE-430-5].

f. Failure to correctly record a `SPBSoftware` event shall be cause to fail this test.

3. Perform the following procedures:

    a. Attempt a software installation on the Test Subject using a procedure that will cause the update to fail in some fashion (*e.g.* provide wrong signer for the update, incorrect message digest in module, consult with the manufacturer for additional assistance).

    b. Return the Test Subject to the idle state.

    c. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

    d. Using a **Text Editor**, examine the log report for events corresponding to the above steps. Verify that the log contains at least one record of Class `Security`, Type `Operations`, Event Subtypes `SPBSoftware`.

    e. Verify that the `SPBSoftware` records have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    f. Confirm the presence of a `SoftwareFailure` exception in the `SPBSoftware` log record. Record any additional parameters associated with the exception. A missing `SoftwareFailure` exception in the associated `SPBSoftware` log record shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5<br>SMPTE-430-6 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-requester**<br>**Accurate Real-Time Clock**<br>**Text Editor** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 5.4.2.11. SPBSecurityAlert Event

### Objective

*The following does not apply to a Test Subject that is a Projector SPB.*

- Verify that, where the SM can produce `SPBSecurityAlert` log events, the respective log records contain correctly coded `SPBSecurityAlert` events per [SMPTE-430-5].

- Verify that, where the remote SPB can produce `SPBSecurityAlert` log events, the respective log records contain correctly coded `SPBSecurityAlert` events per [SMPTE-430-5].

### Procedures

**Note:**
A `SPBSecurityAlert` record indicates an event that is not described by one of the other event record types defined in [SMPTE-430-5]. Each Test Subject must be evaluated to determine what conditions may result in a `SPBSecurityAlert` event being logged. Detailed instructions must be provided by the manufacturer, including any test jigs or applications that may be required to perform the test.

1. Following the manufacturer's documented procedure, for each separately identified condition, configure the Test Subject and perform actions that will result in the logging of a `SPBSecurityAlert` event recording the condition.

2. Extract a security log from the Test Subject that includes the range of time during which the above Step 1 was carried out.

3. Using a **Text Editor**, examine the log report for events corresponding to the above Step 1. Verify that the log contains the expected number of records of Class `Security`, Type `Operations`, Event Subtypes `SPBSecurityAlert`. Verify that the `SPBSecurityAlert` records have correctly formatted parameters as defined in [SMPTE-430-5].

4. For each type of `SPBSecurityAlert` record, provide an explanation of the condition and any parameters that are recorded.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8, 9.4.6.3.8<br>SMPTE-430-4<br>SMPTE-430-5 |
| **Test Equipment** | **Computer with POSIX OS**<br>**asm-requester**<br>**Accurate Real-Time Clock**<br>**Text Editor** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Data only | — | — |

| | | | |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 16.2. LD/LE Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Data only | — | — |

# Chapter 6. Media Block

The Media Block (MB) is a Type 1 SPB comprising a Security Manager (SM) and the Media Decryptors (MD) for all essence types, plus, as required, Forensic Marker (FM) for image or sound, a Link Encryptor (LE) and a Timed Text rendering engine (alpha-channel overlay).

## 6.1. Security Manager (SM)

**Note:**
Some of the procedures in this section require test content that is specifically malformed. In some implementations, these malformations may be caught and reported directly by the SMS without involving the SM. Because the purpose of the procedures is to assure that the SM demonstrates the required behavior, the manufacturer of the Test Subject may need to provide special test programs or special SMS testing modes to allow the malformed content to be applied directly to the SM.

### 6.1.1. Image Integrity Checking

#### Objective

- Verify that the SM detects and logs playback restarts.
- Verify that, for Image Track Files, the SM detects and logs deviations in the:
  - Sequence Number item of the Encrypted Triplet
  - TrackFile ID item of the Encrypted Triplet
  - Check Value of the Encrypted Source Value
  - MIC item of the Encrypted Triplet

#### Procedures

1. Using manufacturer-supplied documentation and by inspection, record a list of means by which playback of a particular composition can be interrupted and restarted. Such means may include command pairs such as pause/play, stop/play, etc. For each of these means:

a. Select for playback the composition *DCI 2K StEM (Encrypted)* keyed with *KDM for 2K StEM (Encrypted)*.

b. Start playback, interrupt playback and restart playback

c. Extract a security log from the Test Subject and using a **Text Editor** and identify the events associated with the playback.

d. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

e. Confirm that there are at least 2 `FrameSequencePlayed` records for each track file included in the composition and that the `FirstFrame` and `LastFrame` parameter values reflect the interrupted playback.

f. Confirm that there is no `PlayoutComplete` event associated with the interrupted playback.

2. Start playback of the composition *DCI 2K StEM (Encrypted)* keyed with *KDM for 2K StEM (Encrypted)* and interrupt line power to the Test Subject before playback of the composition ends. Power up the Test Subject, wait for the system to become idle. Extract a security log from the Test Subject and using a **Text Editor**. Identify the events associated with the playback and:

   a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

   b. Confirm that there are at least 1 `FrameSequencePlayed` record for each track file included in the composition and that the `FirstFrame` and `LastFrame` parameter values reflect the interrupted playback.

   c. Confirm that there is no `PlayoutComplete` event associated with the interrupted playback.

3. Play back the composition *DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)*, keyed with *KDM for DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

   a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

   b. Confirm the presence of a `FrameSequenceError` exception in the `FrameSequencePlayed` log record for the image track file. Record any additional parameters associated with the exception.

4. Play back the composition *DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)*, keyed with *KDM for DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

   a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

   b. Confirm the presence of a `TrackFileIDError` exception in the `FrameSequencePlayed` log record for the image track file. Record any additional parameters associated with the exception.

5. Play back the composition *DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)*, keyed with *KDM with invalid MIC Key (Picture) for DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

b. Confirm the presence of a `FrameMICError` exception in the `FrameSequencePlayed` log record for the image track file. Record any additional parameters associated with the exception.

6. Play back the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM with MIC Key (Picture) for DCI 2K Sync Test (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

   a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

   b. Confirm the presence of a `FrameMICError` exception in the `FrameSequencePlayed` log record for the image track file. Record any additional parameters associated with the exception.

7. Play back the composition *DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted)*, keyed with *KDM for DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

   a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

   b. Confirm that there is no `FrameMICError` exception in the `FrameSequencePlayed` log record for the image track file.

8. Play back the composition *DCI Malformed Test 11: Picture with Check Value error in MXF Track File (Encrypted)*, keyed with *KDM for DCI Malformed Test 11: Picture with Check Value error in MXF Track File (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

   a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

   b. Confirm the presence of a `CheckValueError` exception in the `FrameSequencePlayed` log record for the image track file. Record any additional parameters associated with the exception.

Failure of any of the above conditions is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5<br>SMPTE-429-6<br>SMPTE-429-5 |
| **Test Equipment** | **DCI Projector**<br>**Text Editor** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)*<br>*DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)*<br>*KDM for DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)*<br>*DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)*<br>*KDM for DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)*<br>*DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted)*<br>*KDM for DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted)* |

*DCI Malformed Test 11: Picture with Check Value error in MXF Track File (Encrypted)*
*KDM for DCI Malformed Test 11: Picture with Check Value error in MXF Track File (Encrypted)*
*DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)*
*KDM with invalid MIC Key (Picture) for DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)*
*DCI 2K Sync Test (Encrypted)*
*KDM with MIC Key (Picture) for DCI 2K Sync Test (Encrypted)*

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.2. Sound Integrity Checking

### Objective

Verify that, for Sound Track Files, the SM detects and logs deviations in the:

- Sequence Number item of the Encrypted Triplet
- TrackFile ID item of the Encrypted Triplet
- Check Value of the Encrypted Source Value
- MIC item of the Encrypted Triplet

### Procedures

1. Play back the composition *DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted)*, keyed with *KDM for DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `FrameSequenceError` exception in the `FrameSequencePlayed` log record for the sound track file. Record any additional parameters associated with the exception.

2. Play back the composition *DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)*, keyed with *KDM for DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `TrackFileIDError` exception in the `FrameSequencePlayed` log record for the sound track file. Record any additional parameters associated with the exception.

3. Play back the composition *DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)*, keyed with *KDM with invalid MIC Key (Sound) for DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `FrameMICError` exception in the `FrameSequencePlayed` log record for the sound track file. Record any additional parameters associated with the exception.

4. Play back the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM with MIC Key (Sound) for DCI 2K Sync Test (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `FrameMICError` exception in the `FrameSequencePlayed` log record for the sound track file. Record any additional parameters associated with the exception.

5. Play back the composition *DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)*, keyed with *KDM for DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm that there is no `FrameMICError` exception in the `FrameSequencePlayed` log record for the sound track file.

6. Play back the composition *DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)*, keyed with *KDM for DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

b. Confirm the presence of a `CheckValueError` exception in the `FrameSequencePlayed` log record for the sound track file. Record any additional parameters associated with the exception.

Failure of any of the above conditions is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |
| **Test Equipment** | **Text Editor** |
| **Test Materials** | *DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted)*<br>*KDM for DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted)*<br>*DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)*<br>*KDM for DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)*<br>*DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)*<br>*KDM with invalid MIC Key (Sound) for DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)*<br>*DCI 2K Sync Test (Encrypted)*<br>*KDM with MIC Key (Sound) for DCI 2K Sync Test (Encrypted)*<br>*DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)*<br>*KDM for DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)*<br>*DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)*<br>*KDM for DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.3. Deleted Section

The section "Restriction of Keying to Monitored Link Decryptors" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 6.1.4. Restriction of Keying to MD Type

### Objective

Verify that keys are issued only to a Media Decryptor (MD) matching the key type as specified in the KDM per [SMPTE-430-1].

### Procedures

1. Load the KDM *KDM with mismatched keytype*, which contains a valid decryption key for image, but the Key Type is mismatched.

2. Load and attempt to play the composition *DCI 2K StEM (Encrypted)*. Successful playback shall be cause to fail this test.

3. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of an associated `FrameSequencePlayed` log record that contains a `KeyTypeError` exception. Record any additional parameters associated with the exception. Failure to produce correct log records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-5 |
| **Test Materials** | *KDM with mismatched keytype*<br>*DCI 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.5. Restriction of Keying to Valid CPLs

### Objective

Verify that the SM validates CPLs and logs results as a prerequisite to preparing the suite for the associated composition playback.

### Procedures

1. Supply the CPL *DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)*, keyed with *KDM for DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)*, to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

2. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

3. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of the CPL. Verify that the value of the `SignerID` parameter contains the Certificate Thumbprint of the certificate used to sign the CPL. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `AssetHashError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `AssetHashError` exception shall be cause to fail this test.

4. Supply the CPL *DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)*, keyed with *KDM for DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)* to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

5. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

6. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of the CPL. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `SignatureError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `SignatureError` exception shall be cause to fail this test.

7. Supply the CPL *DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted)*, keyed with *KDM for DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted)* to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

8. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

9. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of the CPL. Verify that the value of the `SignerID` parameter contains the Certificate Thumbprint of the certificate used to sign the CPL. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `AssetMissingError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `AssetMissingError` exception shall be cause to fail this test.

10. Supply the CPL *DCI Malformed Test 14: CPL that does not conform to ST 429-7 (Encrypted)*, keyed with *KDM for DCI Malformed Test 14: CPL that does not conform to ST 429-7 (Encrypted)* to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

11. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

12. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `CPLFormatError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `CPLFormatError` exception shall be cause to fail this test.

13. Supply the CPL *DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted)*, keyed with *KDM for DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted)* to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

14. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

15. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of the CPL. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `CertFormatError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `CertFormatError` exception shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5<br>SMPTE-430-5 |
| **Test Materials** | *DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)*<br>*KDM for DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)*<br>*DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)*<br>*KDM for DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)*<br>*DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted)*<br>*KDM for DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted)*<br>*DCI Malformed Test 14: CPL that does not conform to ST 429-7 (Encrypted)*<br>*KDM for DCI Malformed Test 14: CPL that does not conform to ST 429-7 (Encrypted)*<br>*DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted)*<br>*KDM for DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 6.1.6. Remote SPB Integrity Monitoring

### Objective

The SM must continuously monitor and log the integrity status of all remote SPBs to detect failures during normal operation. The following conditions must be satisfied:

- Verify that the SM issues the QuerySPB command at least once every 30 seconds.
- Verify that the SM creates at least one (1) security log record for each contiguous set of identical QuerySPB responses having a general response value that is not `success`.
- Verify that the SM creates at least one (1) security log record for each contiguous set of identical QuerySPB responses having a status value that is `Security Alert`.
- Verify that the SM continues playout if QuerySPB responses are not received.
- Verify that the SM creates at least one (1) security log record for each contiguous set of unreceived QuerySPB responses.

### Procedures

1. Configure the Test Subject to recognize as many remote SPBs as the system will allow. Record this value.
2. For each remote SPB included in the Test Subject's configuration, set up and start a corresponding **asm-responder** simulator. There shall be one responder for every remote SPB the Test Subject can be configured to use simultaneously.
3. If not already present, load the composition *DCI 2K StEM*.
4. For each remote SPB included in the Test Subject's configuration:
    a. Verify that the Test Subject sends a QuerySPB command to the respective **asm-responder** at least once every thirty (30) seconds.
    b. Play the test content *DCI 2K StEM*.
    c. One minute into playback, disconnect the responder from the Test Subject. Record the UTC time, as provided by an **Accurate Real-Time Clock**, at which this event occurred (Time A). Verify that the show continues to play. Failure to keep playing is cause to fail this test.
    d. Wait 5 minutes, reconnect the responder to the Test Subject. Record the time at which this event occurred (Time *B*). Verify that the show continues to play. Failure to keep playing is cause to fail this test.
    e. Command the responder to answer QuerySPB messages with the `success` general response value and the `Security Alert` status value. Record the time at which this event occurred (Time *C*). Verify (i) that the Test

Subject stops playback and (ii) that, when stopped, playback cannot be restarted. Failure to stop playback or allowing playback to be restarted once stopped are both cause to fail this test.

f. Command the responder to answer QuerySPB messages with `success` general response value and `Not Playing` status value. Observe that the Test Subject returns to normal operation (*i.e.* allows playout). Failure to return to normal operation is cause to fail this test.

g. Play the test content *DCI 2K StEM*.

h. Command the responder to answer QuerySPB messages with the `success` general response value and the `Security Alert` status value. Record the time at which this event occurred (Time *D*). Verify (i) that the Test Subject stops playback and (ii) that, when stopped, playback cannot be restarted. Failure to stop playback or allowing playback to be restarted once stopped are both cause to fail this test.

i. Command the responder to answer QuerySPB messages with `success` general response value and `Playing` status value. Observe that the Test Subject returns to normal operation (*i.e.* allows playout). Failure to return to normal operation is cause to fail this test.

j. For each of the non-zero ASM General Response values (`RRP Failed`, 1), (`RRP Invalid`, 2) and (`Responder Busy`, 3):

    i. Play the test content *DCI 2K StEM*.

    ii. Command the respective responder to answer QuerySPB messages with the General Response value. Verify (i) that the Test Subject stops playback and (ii) that, when stopped, playback cannot be restarted. Record the time at which this event occurred (Time *En*, where *n* is the response value). Failure to stop playback or allowing playback to be restarted once stopped are both cause to fail this test.

    iii. Command the responder to answer QuerySPB messages with `success` General Response value and observe that the Test Subject returns to normal operation. Failure to return to normal operation is cause to fail this test.

k. Retrieve a log report from the SM covering the time period between Time *A* and Time *E3*. Verify the following:

    i. The log report contains at least one ASM `LinkException` record corresponding to the period between Time *A* and Time *B*. The record contains a `QuerySPBError` exception.

    ii. The log report contains at least one ASM `LinkException` record corresponding to Time *C*. The record contains a `QuerySPBAlert` exception.

    iii. The log report contains at least one ASM `LinkException` record corresponding to Time *D*. The record contains a `QuerySPBAlert` exception.

    iv. The log report contains at least one ASM `LinkException` record corresponding to Time *E1*.

    v. The log report contains at least one ASM `LinkException` record corresponding to Time *E2*.

    vi. The log report contains at least one ASM `LinkException` record corresponding to Time *E3*. Failure to verify the presence of each log record listed above shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-6 |
| **Test Equipment** | **asm-responder**<br>**Accurate Real-Time Clock** |
| **Test Materials** | *DCI 2K StEM* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 6.1.7. SPB Integrity Fault Consequences

### Objective

- Verify that, after authentication and/or an ASM QuerySPB Command, the SM responds to SPB substitutions by terminating and re-establishing TLS sessions (and re-authenticating the suite).

- Verify that, after authentication and/or an ASM QuerySPB Command, the SM responds to SPB substitutions by terminating and re-establishing suite playability conditions (KDM prerequisites, SPB queries and key loads).

### Procedures

> **Note:**
> This test involves the use of more than one **asm-responder** simulator program, each with their own device certificate. This places special emphasis on preparing and selecting the correct KDM for a stage of the test. The KDM's TDL needs to be populated with the appropriate cert thumbprints for the device or combination of devices intended.

To complete this test, two KDMs are required to be created and ingested. The Trusted Device List (TDL) must contain the thumbprint of the appropriate Projector/LD device certificate for each of the two responders.

1. Configure two **asm-responder** simulator programs to respond on the same TCP/IP address that the Test Subject is configured to connect to its Projector. Do not connect either ASM responder at this time. Each instance of ASM Responder shall have a different Projector/LD device certificate. The two responders shall be referred to as "Responder A" and "Responder B" respectively.

2. Connect Responder A to the Test Subject. Observe the opening of the TLS session and any commands received. 3. Verify that the QuerySPB request is being issued at least every 30 seconds. Failure of this requirement is cause to fail this test.

3. Ingest *KDM with a TDL including Responder A* for Responder A.

4. Set up and begin playing a show using the composition contained in *DCI 2K StEM (Encrypted)*, keyed with *KDM with a TDL including Responder A.*

5. Record the values of all LE keys that were received up to the time playback started.

6. Two minutes into playback, disconnect Responder A from the Test Subject.

7. Verify that the show continues to play. Failure to keep playing is cause to fail this test.

8. Connect Responder B to the Test Subject.

9. Verify that the show stops playback as soon as TLS authentication is reported on Responder B. Failure to stop playing is cause to fail this test.

10. After TLS completes authentication, observe any commands received. If TLS authentication fails this is cause to fail this test.

11. Attempt to set up and play the show from Step 5. If the show starts playing this is cause to fail this test.

12. Ingest *KDM with a TDL including Responder B* for Responder B.

13. Attempt to set up and play the show from Step 5. If the show does not start playing this is cause to fail this test.

14. Record the values of all LE keys that were received up to the time playback started.

15. Compare the LE key values from Step 6 with those from Step 15. If any value is repeated this is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |
| **Test Equipment** | **asm-responder** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM with a TDL including Responder A*<br>*KDM with a TDL including Responder B* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 6.1.8. Content Key Extension, End of Engagement

### Objective

Verify that to avoid end of engagement issues, composition playout may extend beyond the end of the KDM's playout time window, if started within the KDM playout time window, by a maximum of 6 hours.

### Procedures

**Note:**
This test will require KDMs that contain `ContentKeysNotValidAfter` elements set to a time in the near future. It is recommended that fresh KDMs be generated that will expire 30-60 minutes after beginning the test procedures. Refer to information provided in the relevant step to ensure that the applicable KDM is being used at the appropriate absolute time the step of the test is carried out.

**Note:**
The Test Operator is required to take into account any timezone offsets that may apply to the locality of the Test Subject and the representation of the `ContentKeysNotValidAfter` element of the KDM. For clarity it is recommended that a common representation be used.

**Note:**
The Security Manager's (SM) clock must be accurately set, to the extent possible, for successful execution of this test.

**Note:**
The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

1. Using a **Text Editor**, open the KDM *KDM for Past Time Window Extension (Encrypted)* and note the value of the timestamp contained in the `<ContentKeysNotValidAfter>` element (*i.e.* the KDM's end of validity timestamp). *Note: Steps 2 and 3 must be commenced before the time recorded in this step.*

2. Load the composition *End of Engagement -Past Time Window Extension (Encrypted)*, keyed with *KDM for Past Time Window Extension (Encrypted)*. *End of Engagement -Past Time Window Extension (Encrypted)* is a composition which is 6 hours and 11 minutes in length.

3. Within 5 minutes prior to the timestamp recorded in step 1, attempt to start playing *End of Engagement -Past Time Window Extension (Encrypted)*. Because the complete show extends beyond the 6 hours end of engagement extension window, the composition should not start playback. If the composition starts to playback, this is cause to fail this test.

4. Using a **Text Editor**, open the KDM *KDM for Within Time Window Extension (Encrypted)* and note the value of the timestamp contained in the `<ContentKeysNotValidAfter>` element (*i.e.* the KDM's end of validity timestamp). *Note: Steps 5 and 6 must be commenced before the time recorded in this step.*

5. Load the composition *End of Engagement - Within Time Window Extension (Encrypted)*, keyed with *KDM for Within Time Window Extension (Encrypted)*. *End of Engagement - Within Time Window Extension (Encrypted)* has a duration of 5 hours, 59 minutes and 30 seconds.

6. Within 5 minutes prior to the timestamp recorded in step 4, attempt to start playing *End of Engagement - Within Time Window Extension (Encrypted)*. The composition should start to playback and continue playing in its entirety. If the show fails to start or fails to playout completely, this is cause to fail this test.
   *Note: The test operator does not have to be present for the entire playback. Sufficient proof of successful playback can be observed by examining the security log for complete* `FrameSequencePlayed`, `CPLEnd` *and* `PlayoutComplete` *events.*

.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |
| **Test Equipment** | **Text Editor** |
| **Test Materials** | *End of Engagement - Within Time Window Extension (Encrypted)*<br>*End of Engagement -Past Time Window Extension (Encrypted)*<br>*KDM for Within Time Window Extension (Encrypted)*<br>*KDM for Past Time Window Extension (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 6.1.9. ContentAuthenticator Element Check

### Objective

- Verify that the Test Subject checks that one of the certificates in the certificate chain supplied with the CPL has a certificate thumbprint that matches the value of the KDM `<ContentAuthenticator>` element.

- Verify that the Test Subject checks that such certificate indicates only a "Content Signer (CS) role.

### Procedures

For each of the malformations below, load the indicated CPL and KDM on to the Test Subject. Verify that the the KDM is not used to enable playback. A successful playback is cause to fail this test.

1. Use the composition *DCI 2K StEM (Encrypted)* and supply the KDM *KDM with invalid ContentAuthenticator*. The KDM contains a `<ContentAuthenticator>` element having a certificate thumbprint value that does not match the thumbprint of one of the signer certificates in the certificate chain that signed the associated CPL.

2. Use the composition *DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)* and supply the KDM *KDM for DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)*. The KDM contains a `<ContentAuthenticator>` element having a certificate thumbprint value that matches the thumbprint of one of the signer certificates in the certificate chain that signed the associated CPL but that certificate has no role.

3. Use the composition *DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)* and supply the KDM *KDM for DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)*. The KDM contains a `<ContentAuthenticator>` element having a certificate thumbprint value that matches the thumbprint of one of the signer certificates in the certificate chain that signed the associated CPL but that certificate has a bad role (SM).

4. Use the composition *DCI Malformed Test 18: CPL signed with Extra Role Certificate (Encrypted)* and supply the KDM *KDM for DCI Malformed Test 18: KDM for CPL signed with Extra Role Certificate (Encrypted)*. The KDM contains a `<ContentAuthenticator>` element having a certificate thumbprint value that matches the thumbprint of one of the signer certificates in the certificate chain that signed the associated CPL but that certificate has an extra role.

5. Extract a security log from the Test Subject and using a **Text Editor**, identify the `FrameSequencePlayed` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of `FrameSequencePlayed` log records that contain `ContentAuthenticatorError` exceptions. Record any additional parameters associated with the exception. A missing `ContentAuthenticatorError` exception in any of the associated `FrameSequencePlayed` log records shall be cause to fail this test. Only for the operation associated with step 2, a correctly recorded `CPLCheck` log record with a `CertFormatError` exception is an allowable substitute for a `FrameSequencePlayed` log record to satisfy the requirements of this step of the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5<br>SMPTE-429-7<br>SMPTE-430-1<br>SMPTE-430-2<br>SMPTE-430-5 |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM with invalid ContentAuthenticator*<br>*DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)*<br>*KDM for DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)*<br>*DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)*<br>*KDM for DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)*<br>*DCI Malformed Test 18: CPL signed with Extra Role Certificate (Encrypted)*<br>*KDM for DCI Malformed Test 18: KDM for CPL signed with Extra Role Certificate (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 6.1.10. KDM Date Check

### Objective

Verify that the Test Subject checks that the playout date is within the time period defined by the KDM `ContentKeysNotValidBefore` and `ContentKeysNotValidAfter` elements.

### Procedures

1. Load the composition *DCI 2K StEM (Encrypted)* and KDM *KDM that has expired*, which contains a valid decryption keys, but the KDM has expired.

2. Attempt to play the *DCI 2K StEM (Encrypted)* composition and record the result. Verify that the composition cannot be played. Successful playout is cause to fail this test.

3. Load the composition *DCI 2K StEM (Encrypted)* and the KDM *KDM with future validity period*, which contains a valid decryption keys, but the KDM has is not yet valid.

4. Attempt to play the *DCI 2K StEM (Encrypted)* composition and record the result. Verify that the composition cannot be played. Successful playout is cause to fail this test.

5. Load the composition *DCI 2K StEM (Encrypted)* and KDM *KDM that has recently expired*, which contains a valid decryption keys, but the KDM has expired.

6. Attempt to play the *DCI 2K StEM (Encrypted)* composition and record the result. Verify that the composition cannot be played. Successful playout is cause to fail this test.

7. Load the composition *DCI 2K StEM (Encrypted)* and the KDM *KDM with future validity period*, which contains a valid decryption keys, but the KDM has is not yet valid.

8. Attempt to play the *DCI 2K StEM (Encrypted)* composition and record the result. Verify that the composition cannot be played. Successful playout is cause to fail this test.

9. Extract a security log from the Test Subject and using a **Text Editor**, identify the `FrameSequencePlayed` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `FrameSequencePlayed` log record that contains a `ValidityWindowError` exception. Record any additional parameters associated with the exception. A missing `ValidityWindowError` exception in any of the associated `FrameSequencePlayed` log records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1 |

| SMPTE-430-5 | **Test Materials** |
|---|---|
| *KDM with future validity period*<br>*KDM that has recently expired*<br>*KDM that has expired*<br>*DCI 2K StEM (Encrypted)* | |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.11. KDM TDL Check

### Objective

*The following does not apply if a Special Auditorium Situation is enabled.*

Verify that the Test Subject checks that the set of SPBs configured for playout is consistent with the TDL (`AuthorizedDeviceInfo` element) in the controlling KDM.

### Procedures

If the Test Subject is a *Media Block that is a Companion SPB and is married (physically and electrically) to a Projector SPB*, perform each of the following steps. Before each step, delete all KDMs residing in the Test Subject. After completing the steps, extract a security log from the Test Subject and using a **Text Editor**:

- Identify the `FrameSequencePlayed` record associated with the image track file produced during each step, and confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5].
- If successful playback start is expected, confirm that the `FrameSequencePlayed` record contains a `Parameter` element with a `Name` equal to `DownstreamDevice` and a `Value` equal to the certificate thumbprint of the projector SPB.
- If failed playback start is expected, confirm that the `FrameSequencePlayed` record contains a `TDLError` exception. Record all parameters associated with the exception.

Failure to produce correct log records, including missing required elements or incorrect parameters, shall be cause to fail this test.

1. Load the *KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)*, which is a KDM that carries only the "assume trust" certificate thumbprint. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. If playback does not begin this is cause to fail this test.
2. Load the *KDM with Assume Trust and random TDL entries*, which is KDM with a TDL that carries the "assume trust" certificate thumbprint and a single, randomly generated device list entry. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. Successful start of playback is cause to fail this test.

3. Load the *KDM with random TDL entry*, which contains a single, randomly generated device list entry. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. Successful start of playback is cause to fail this test.

4. Load the *KDM with the SM alone on the TDL*, which is a KDM with a TDL that contains only the certificate thumbprint of the SM Certificate of the Test Subject. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. Successful start of playback is cause to fail the test.

5. Load the *KDM with the projector alone on the TDL*, which is a KDM with a TDL that contains only the certificate thumbprint of the Projector SPB certificate. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. If playback does not begin this is cause to fail this test.

If the Test Subject is a *Media Block that is permanently married to a Projector SPB*, perform each of the following steps. Before each step, delete all KDMs residing in the Test Subject. After completing the steps, extract a security log from the Test Subject and using a **Text Editor**:

- Identify the `FrameSequencePlayed` record associated with the image track file produced during each step, and confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5].

- If successful playback start is expected, confirm that the `FrameSequencePlayed` record does not contain a `Parameter` element with a `Name` equal to `DownstreamDevice`.

- If failed playback start is expected, confirm that the `FrameSequencePlayed` record contains a `TDLError` exception. Record all parameters associated with the exception.

Failure to produce correct log records, including missing required elements or incorrect parameters, shall be cause to fail this test.

1. Load the *KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)*, which is a KDM that carries only the "assume trust" certificate thumbprint. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. If playback does not begin this is cause to fail this test.

2. Load the *KDM with random TDL entry*, which contains a single, randomly generated device list entry. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. If playback does not begin this is cause to fail this test.

3. Load the *KDM with the SM alone on the TDL*, which is a KDM with a TDL that contains only the certificate thumbprint of the SM Certificate of the Test Subject. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. If playback does not begin this is cause to fail this test.

If the Test Subject is a *Media Block that supports Link Encryption*, perform each of the following steps. Before each step, delete all KDMs residing in the Test Subject. After completing the steps, extract a security log from the Test Subject and, using a **Text Editor**:

- Identify the `FrameSequencePlayed` record associated with the image track file produced during each step, and confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5].

- If successful playback start is expected, confirm that the `FrameSequencePlayed` record contains two `Parameter` elements with a `Name` equal to `DownstreamDevice`, the first having a `Value` equal to the certificate thumbprint of the LDB married to the Projector and the second having a `Value` equal to the certificate thumbprint of Projector SPB.

- If failed playback start is expected, confirm that the `FrameSequencePlayed` record contains a `TDLError` exception. Record all parameters associated with the exception.

Failure to produce correct log records, including missing required elements or incorrect parameters, shall be cause to fail this test.

1. Load the *KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)*, which is a KDM that carries only the "assume trust" certificate thumbprint. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. If playback does not begin this is cause to fail this test.

2. Load the *KDM with Assume Trust and random TDL entries*, which is KDM with a TDL that carries the "assume trust" certificate thumbprint and a single, randomly generated device list entry. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. Successful start of playback is cause to fail this test.

3. Load the *KDM with random TDL entry*, which contains a single, randomly generated device list entry. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. Successful start of playback is cause to fail this test.

4. Load the *KDM with the SM alone on the TDL*, which is a KDM with a TDL that contains only the certificate thumbprint of the SM Certificate of the Test Subject. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. Successful start of playback is cause to fail this test.

5. Load the *KDM with the projector alone on the TDL*, which is a KDM with a TDL that contains only the certificate thumbprint of the Projector SPB certificate. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. Successful start of playback is cause to fail the test.

6. Load the *KDM with the LDB alone on the TDL*, which is a KDM with a TDL that contains only the certificate thumbprint of the certificate of the LDB married to the Projector SPB. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. Successful start of playback is cause to fail the test.

7. Load the *KDM with the projector and LDB on the TDL*, which is a KDM with a TDL that contains the certificate thumbprint of the certificates of both the Projector SPB and its married LDB. Attempt to play *DCI 2K StEM (Encrypted)* and record the result. If playback does not begin this is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5, 9.4.3.6.1, 9.4.3.6.5, 9.4.3.6.6<br>SMPTE-430-1<br>SMPTE-430-5 |
| **Test Materials** | *KDM with Assume Trust and random TDL entries*<br>*KDM with the SM alone on the TDL*<br>*KDM with the projector alone on the TDL*<br>*KDM with the LDB alone on the TDL*<br>*KDM with the projector and LDB on the TDL*<br>*KDM with random TDL entry*<br>*KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)*<br>*DCI 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 6.1.12. Maximum Number of DCP Keys

### Objective

Verify that the system supports playback of two compositions with up to 256 different essence encryption keys each

### Procedures

**Note:**
The KDMs specified to be used in this test additionally have one of each type of forensic marking keys FMIK and FMAK. Receiving devices shall process such keys in accordance with the individual implementation, in a manner that will not affect the requirements related to the maximum number of content keys (MDIK and MDAK).

**Note:**
The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

1. Load the compositions *128 Reel Composition, "A" Series* and *128 Reel Composition, "B" Series* on to the Test Subject.

2. Create a show that contains *128 Reel Composition, "A" Series* and *128 Reel Composition, "B" Series*. Each composition contains 128 reels of plaintext picture and sound.

3. Play the show. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback started. Failure to play the complete show shall be cause to fail this test.

4. Extract a security log from the Test Subject that includes the range of time during which Step 3 was carried out

5. Using a **Text Editor**, locate the first `CPLStart` and last `CPLEnd` records that occurred after the time recorded in Step 3. Let *Plaintext Time* be the absolute difference between the `TimeStamp` values of the two records.

6. Load the compositions *128 Reel Composition, "A" Series (Encrypted)* and *128 Reel Composition, "B" Series (Encrypted)* on to the Test Subject.

7. Load the KDMs *KDM for 128 Reel Composition, "A" Series (Encrypted)* and *KDM for 128 Reel Composition, "B" Series (Encrypted)* on to the Test Subject.

8. Create a show that contains *128 Reel Composition, "A" Series (Encrypted)* and *128 Reel Composition, "B" Series (Encrypted)*. Each composition contains 128 reels of encrypted picture and sound.

9. Play the show. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback started. Failure to play the complete show shall be cause to fail this test.

10. The presence of any observable artifacts in the reproduced picture and/or sound shall be cause to fail this test.

11. Extract a security log from the Test Subject that includes the range of time during which Step 9 was carried out.

12. Using a **Text Editor**, locate the first `CPLStart` and last `CPLEnd` records that occurred after the time recorded in Step 9. Let `Ciphertext Time` be the absolute difference between the `TimeStamp` values of the two records.

13. An absolute difference of more than 1 second between `Ciphertext Time` and `Plaintext Time` is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.7.7<br>SMPTE-430-1 |
| **Test Materials** | *128 Reel Composition, "A" Series*<br>*128 Reel Composition, "B" Series*<br>*128 Reel Composition, "A" Series (Encrypted)*<br>*128 Reel Composition, "B" Series (Encrypted)*<br>*KDM for 128 Reel Composition, "A" Series (Encrypted)*<br>*KDM for 128 Reel Composition, "B" Series (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.13. CPL Id Check

### Objective

Verify that the Test Subject checks that the KDM `<CompositionPlaylistId>` element matches the value of the CompositionPlaylistID field of KDM CipherData structure as specified in [SMPTE-430-1]

### Procedures

1. Load *DCI 2K StEM (Encrypted)*.

2. load *KDM with bad CipherData CompositionPlaylistId value*, a KDM in which (i) the value of the CompositionPlaylistID field of the CipherData structure does not match the value of the `<Id>` element of *DCI 2K StEM (Encrypted)* and (ii) the value of the `<CompositionPlaylistId>` element matches the value of the CompositionPlaylist `<Id>` element of *DCI 2K StEM (Encrypted)*. Attempt to play *DCI 2K StEM (Encrypted)*. Successful playback is cause to fail this test.

3. Delete *KDM with bad CipherData CompositionPlaylistId value*.

4. Load *KDM with bad CompositionPlaylistId value*, a KDM in which (i) the value of the CompositionPlaylistID field of the CipherData structure matches the value of the `<Id>` element of *DCI 2K StEM (Encrypted)* and (ii) the value of the

`<CompositionPlaylistId>` element does not match the value of the CompositionPlaylist `<Id>` element in *DCI 2K StEM (Encrypted)*. Attempt to play *DCI 2K StEM (Encrypted)*. Successful playback is cause to fail this test.

5. Extract a security log from the Test Subject and using a **Text Editor**, identify the `KDMKeysReceived` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `KDMFormatError` exception in the `KDMKeysReceived` log record. Record any additional parameters associated with the exception. A missing `KDMFormatError` exception in any of the associated `KDMKeysReceived` log records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>SMPTE-430-1<br>SMPTE-430-3<br>SMPTE-430-5 |
| **Test Materials** | *KDM with bad CipherData CompositionPlaylistId value*<br>*KDM with bad CompositionPlaylistId value*<br>*DCI 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.14. CPL Id Check (OBAE)

### Objective

Verify that the Test Subject checks that the KDM `<CompositionPlaylistId>` element matches the value of the `CompositionPlaylistId` field of KDM CipherData structure as specified in [SMPTE-430-1] .

### Procedures

**Note:**
If the Test Subject is an OMB, the KDM targeting the associated IMB is valid, i.e. it is an instance of *KDM for 2K StEM (Encrypted) (OBAE)*.

1. Load *DCI 2K StEM (OBAE) (Encrypted)*.

2. Load *KDM with bad CipherData CompositionPlaylistId value (OBAE)*, a KDM in which (i) the value of the `CompositionPlaylistId` field of the `CipherData` structure does not match the value of the `<Id>` element of *DCI 2K*

*StEM (OBAE) (Encrypted)* and (ii) the value of the `<CompositionPlaylistId>` element matches the value of the CompositionPlaylist `<Id>` element of *DCI 2K StEM (OBAE) (Encrypted)*. Attempt to play *DCI 2K StEM (OBAE) (Encrypted)*. Successful playback is cause to fail this test.

3. Delete *KDM with bad CipherData CompositionPlaylistId value (OBAE)*.

4. Load *KDM with bad CompositionPlaylistId value (OBAE)*, a KDM in which (i) the value of the `CompositionPlaylistId` field of the `CipherData` structure matches the value of the `<Id>` element of *DCI 2K StEM (OBAE) (Encrypted)* and (ii) the value of the `<CompositionPlaylistId>` element does not match the value of the CompositionPlaylist `<Id>` element in *DCI 2K StEM (OBAE) (Encrypted)*. Attempt to play *DCI 2K StEM (OBAE) (Encrypted)*. Successful playback is cause to fail this test.

5. Extract a security log from the Test Subject and using a **Text Editor**, identify the `KDMKeysReceived` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `KDMFormatError` exception in the `KDMKeysReceived` log record. Record any additional parameters associated with the exception. A missing `KDMFormatError` exception in any of the associated `KDMKeysReceived` log records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8, 9.4.3.5<br>OBAE-ADD, 3.3<br>SMPTE-430-1<br>SMPTE-430-3<br>SMPTE-430-5 |
| **Test Materials** | *KDM with bad CipherData CompositionPlaylistId value (OBAE)*<br>*KDM with bad CompositionPlaylistId value (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.15. Restriction of Playback in Absence of Integrity Pack Metadata

### Objective

Verify that playback of encrypted content is disallowed or terminated when integrity pack metadata is missing.

### Procedures

For each of the rows of Table 6.1, perform the following steps in order:

1. If the Test Subject is not one of the *Target Test Subject(s)*, skip the row.

2. Attempt playback of the *Malformed Composition* from its start using the associated *KDM*, and, with an **Accurate Real-Time Clock**, note the UTC time of the attempt.

3. Confirm that either:

    a. no part of the *Malformed Composition* is played; or

    b. playback of the *Malformed Composition* stops no later than 61 seconds after playback starts.

4. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out and, using a **Text Editor**, confirm that:

    a. all required elements of the security log have correctly formatted parameters as defined in [SMPTE-430-5].

    b. there is exactly one `FrameSequencePlayed` log record for the associated *Malformed Track File* and that the record contains a single instance of the specified *Exception Token*.

    c. there is no `PlayoutComplete` event associated with the playback.

Failure of any part of any of the steps above shall be cause to fail this test.

### Table 6.1. List of Compositions with missing integrity pack items

| Malformed Composition, Malformed Composition KDM and Malformed Track File | Exception Token | Target Test Subject(s) |
|---|---|---|
| m25_integrity_pict_mic_ct.cpl.xml<br>m25_integrity_pict_mic_ct.kdm.xml<br>m25_integrity_pict_mic_j2c_ct.mxf | `FrameMICError` | IMB, IMBO |
| m27_integrity_pict_tfid_ct.cpl.xml<br>m27_integrity_pict_tfid_ct.cpl.xml<br>m27_integrity_pict_tfid_j2c_ct.mxf | `TrackFileIDError` | IMB, IMBO |
| m26_integrity_pict_snum_ct.cpl.xml<br>m26_integrity_pict_snum_ct.kdm.xml<br>m26_integrity_pict_snum_j2c_ct.mxf | `FrameSequenceError` | IMB, IMBO |
| m28_integrity_snd_mic_ct.cpl.xml<br>m28_integrity_snd_mic_ct.kdm.xml<br>m28_integrity_snd_mic_pcm_ct.mxf | `FrameMICError` | IMB, IMBO |
| m30_integrity_snd_tfid_ct.cpl.xml<br>m30_integrity_snd_tfid_ct.kdm.xml<br>m30_integrity_snd_tfid_pcm_ct.mxf | `TrackFileIDError` | IMB, IMBO |
| m29_integrity_snd_snum_ct.cpl.xml<br>m29_integrity_snd_snum_ct.kdm.xml<br>m29_integrity_snd_snum_pcm_ct.mxf | `FrameSequenceError` | IMB, IMBO |
| m20_integrity_obae_ms_mic_ct.cpl.xml<br>m20_integrity_obae_ms_mic_ct.kdm.xml<br>m20_integrity_obae_ms_mic_pcm_ct.mxf | `FrameMICError` | IMB, IMBO |
| m22_integrity_obae_ms_tfid_ct.cpl.xml | | |

| | | |
|---|---|---|
| m22_integrity_obae_ms_tfid_ct.kdm.xml<br>m22_integrity_obae_ms_tfid_pcm_ct.mxf | `TrackFileIDError` | IMB, IMBO |
| m21_integrity_obae_ms_snum_ct.cpl.xml<br>m21_integrity_obae_ms_snum_ct.kdm.xml<br>m21_integrity_obae_ms_snum_pcm_ct.mxf | `FrameSequenceError` | IMB, IMBO |
| m19_integrity_obae_mic_ct.cpl.xml<br>m19_integrity_obae_mic_ct.kdm.xml<br>m19_integrity_obae_mic_obae_ct.mxf | `FrameMICError` | OMB, IMBO |
| m24_integrity_obae_tfid_ct.cpl.xml<br>m24_integrity_obae_tfid_ct.kdm.xml<br>m24_integrity_obae_tfid_obae_ct.mxf | `TrackFileIDError` | OMB, IMBO |
| m23_integrity_obae_snum_ct.cpl.xml<br>m23_integrity_obae_snum_ct.kdm.xml<br>m23_integrity_obae_snum_obae_ct.mxf | `FrameSequenceError` | OMB, IMBO |

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.3.6.4<br>SMPTE-429-6<br>SMPTE-430-5 |
| **Test Equipment** | **Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *M25 Composition with Malformed Integrity Pack: Missing MIC item (Picture) (Encrypted)*<br>*KDM for M25 Composition with Malformed Integrity Pack: Missing MIC item (Picture) (Encrypted)*<br>*M25 Picture Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)*<br>*M27 Composition with Malformed Integrity Pack: Missing TrackFileID item (Picture) (Encrypted)*<br>*KDM for M27 Composition with Malformed Integrity Pack: Missing TrackFileID item (Picture) (Encrypted)*<br>*M27 Picture Track File with Malformed Integrity Pack: Missing TrackFileID item (Encrypted)*<br>*M26 Composition with Malformed Integrity Pack: Missing SequenceNumber item (Picture) (Encrypted)*<br>*KDM for M26 Composition with Malformed Integrity Pack: Missing SequenceNumber item (Picture) (Encrypted)*<br>*M26 Picture Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)*<br>*M28 Composition with Malformed Integrity Pack: Missing MIC item (PCM) (Encrypted)*<br>*KDM for M28 Composition with Malformed Integrity Pack: Missing MIC item (PCM) (Encrypted)*<br>*M28 Sound Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)*<br>*M30 Composition with Malformed Integrity Pack: Missing TrackFileID item (PCM) (Encrypted)*<br>*KDM for M30 Composition with Malformed Integrity Pack: Missing TrackFileID item (PCM) (Encrypted)*<br>*M30 Sound Track File with Malformed Integrity Pack: Missing TrackFileID item (Encrypted)*<br>*M29 Composition with Malformed Integrity Pack: Missing SequenceNumber item (PCM) (Encrypted)*<br>*KDM for M29 Composition with Malformed Integrity Pack: Missing SequenceNumber item (PCM) (Encrypted)*<br>*M29 Sound Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)*<br>*M20 Composition with Malformed Integrity Pack: Missing MIC item (OBAE Main Sound) (Encrypted)*<br>*KDM for M20 Composition with Malformed Integrity Pack: Missing MIC item (OBAE Main* |

*Sound) (Encrypted)*
*M20 Sound Track File with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted)*
*M22 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE Main Sound) (Encrypted)*
*KDM for M22 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE Main Sound) (Encrypted)*
*M22 Sound Track File with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)*
*M21 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE Main Sound) (Encrypted)*
*KDM for M21 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE Main Sound) (Encrypted)*
*M21 Sound Track File with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted)*
*M19 Composition with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted)*
*KDM for M19 Composition with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted)*
*M19 OBAE Track File with Malformed Integrity Pack:*

*Missing MIC item (Encrypted)*
*M24 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)*
*KDM for M24 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)*
*M24 OBAE Track File with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)*
*M23 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted)*
*KDM for M23 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted)*
*M23 OBAE Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)*

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.16. Restriction of Keying to MDEK Type (OBAE)

### Objective

Verify that a key is not issued to an OBAE media decryptor if the `KeyType` of the key is not equal to `"MDEK"`.

### Procedures

1. Load *KDM with mismatched KeyType value (OBAE)*.

2. Load and attempt to play the composition *DCI 2K StEM (OBAE) (Encrypted)*. Successful playback shall be cause to fail this test.

3. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of an associated `FrameSequencePlayed` log record that contains a `KeyTypeError` exception. Record any additional parameters associated with the exception. Failure to produce correct log records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.3.6.4<br>SMPTE-430-1<br>SMPTE-430-5 |
| **Test Equipment** | **Text Editor** |
| **Test Materials** | *KDM with mismatched KeyType value (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.17. OBAE Integrity Checking

### Objective

Verify that, for OBAE Track Files, the SM detects and logs deviations in the:

- Sequence Number item of the Encrypted Triplet
- TrackFile ID item of the Encrypted Triplet
- Check Value of the Encrypted Source Value
- MIC item of the Encrypted Triplet

### Procedures

1. Play back the composition *M40 OBAE DCP with Frame-out-of-order error (Encrypted)*, keyed with *KDM for M40 OBAE DCP with Frame-out-of-order error (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `FrameSequenceError` exception in the `FrameSequencePlayed` log record for the OBAE track file. Record any additional parameters associated with the exception.

2. Play back the composition *M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)*, keyed with *KDM for M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `TrackFileIDError` exception in the `FrameSequencePlayed` log record for the OBAE track file. Record any additional parameters associated with the exception.

3. Play back the composition *DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)*, keyed with *KDM with invalid MIC Key for DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `FrameMICError` exception in the `FrameSequencePlayed` log record for the OBAE track file. Record any additional parameters associated with the exception.

4. Play back the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM with MIC Key for DCI 2K Sync Test (OBAE) (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `FrameMICError` exception in the `FrameSequencePlayed` log record for the OBAE track file. Record any additional parameters associated with the exception.

5. Play back the composition *M44 OBAE DCP with HMAC error in MXF Track File (Encrypted)*, keyed with *KDM for M44 OBAE DCP with HMAC error in MXF Track File (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm that there is no `FrameMICError` exception in the `FrameSequencePlayed` log record for the OBAE track file.

6. Play back the composition *M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)*, keyed with *KDM for M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)*. Extract a security log from the Test Subject and using a **Text Editor**, identify the events associated with the playback and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `CheckValueError` exception in the `FrameSequencePlayed` log record for the OBAE track file. Record any additional parameters associated with the exception.

Failure of any of the above conditions is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.3.6.4 |
| **Test Equipment** | **Text Editor** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*M40 OBAE DCP with Frame-out-of-order error (Encrypted)*<br>*M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)*<br>*DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)*<br>*M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)*<br>*M44 OBAE DCP with HMAC value error in MXF Track File (Encrypted)*<br>*KDM for M40 OBAE DCP with Frame-out-of-order error (Encrypted)*<br>*KDM for M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)*<br>*KDM for M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)*<br>*KDM with invalid MIC Key for DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)*<br>*KDM with MIC Key for DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for M44 OBAE DCP with HMAC Value error in MXF Track File (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.18. Content Key Extension, End of Engagement (OBAE)

### Objective

Verify that, to avoid end of engagement issues, OBAE composition playout can extend beyond the end of the KDM's playout time window by a maximum of 6 hours as long as playback is started within the KDM playout time window.

### Procedures

**Note:**
This test requires KDMs that contain `ContentKeysNotValidAfter` elements set to a time in the near future. It is recommended that fresh KDMs be generated that will expire 30-60 minutes after beginning the test procedures. Refer to information provided in the relevant step to ensure that the applicable KDM is being used at the appropriate absolute time the step of the test is carried out.

**Note:**
The Test Operator is required to take into account any timezone offsets that may apply to the locality of the Test Subject and the representation of the `ContentKeysNotValidAfter` element of the KDM. For clarity it is recommended that a common representation be used.

**Note:**
The Security Manager's (SM) clock must be accurately set, to the extent possible, for successful execution of this test.

**Note:**
The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

1. Using a **Text Editor**, open the KDM *KDM for Past Time Window Extension (OBAE) (Encrypted)* and note the value of the timestamp contained in the `<ContentKeysNotValidAfter>` element (*i.e.* the KDM's end of validity timestamp).

   *Note: Steps 2 and 3 must be commenced before the time recorded in this step.*

2. Load the composition *End of Engagement - Past Time Window Extension (OBAE) (Encrypted)*, keyed with *KDM for Past Time Window Extension (OBAE) (Encrypted)*. The composition is 6 hours and 11 minutes in length.

3. Within 5 minutes prior to the timestamp recorded in step 1, attempt to start playing *End of Engagement - Past Time Window Extension (OBAE) (Encrypted)*. Because the complete show extends beyond the 6 hours end of engagement extension window, the composition should not start playback. If the composition starts to playback, this is cause to fail this test.

4. Using a **Text Editor**, open the KDM *KDM for Within Time Window Extension (OBAE) (Encrypted)* and note the value of the timestamp contained in the `<ContentKeysNotValidAfter>` element (*i.e.* the KDM's end of validity timestamp). *Note: Steps 5 and 6 must be commenced before the time recorded in this step.*

5. Load the composition *End of Engagement - Within Time Window Extension (OBAE) (Encrypted)*, keyed with *KDM for Within Time Window Extension (OBAE) (Encrypted)*. The composition has a duration of 5 hours, 59 minutes and 30 seconds.

6. Within 5 minutes prior to the timestamp recorded in step 4, attempt to start playing *End of Engagement - Within Time Window Extension (OBAE) (Encrypted)*. The composition should start to playback and continue playing in its entirety. If the show fails to start or fails to playout completely, this is cause to fail this test.

   *Note: The test operator does not have to be present for the entire playback. Sufficient proof of successful playback can be observed by examining the security log for complete `FrameSequencePlayed`, `CPLEnd` and `PlayoutComplete` events.*

.

## Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |
| **Test Equipment** | **Text Editor** |
| **Test Materials** | *End of Engagement - Past Time Window Extension (OBAE) (Encrypted)*<br>*End of Engagement - Within Time Window Extension (OBAE) (Encrypted)*<br>*KDM for Past Time Window Extension (OBAE) (Encrypted)*<br>*KDM for Within Time Window Extension (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 6.1.19. Plurality of Media Block Identity Certificates

### Objective

Verify that the Media Block supports one published identity certificate and one reserved identity certificate.

### Procedures

**Note:**
For simplicty, this test procedure uses same OBAE content for all Media Blocks (IMB, integrated IMB, IMBO and OMB) since the objective is to merely to determine whether playback occurs, and not whether a complete presentation occurred.

1. Obtain, from the manufacturer, the published and reserved identity certificates of the Test Subject, as defined in Section 9.5.1.3 of [DCI-DCSS].
2. Verify that the roles listed in the published identity certificate obtained in step 1 include SM but not RES ([SMPTE-430-2] specifies roles found in certificates). Failure of this verification is cause to fail the test.
3. Verify that the roles listed in the reserved identity certificate obtained in step 1 includes SM and RES. Failure of this verification is cause to fail the test.
4. Load *DCI 2K StEM (OBAE) (Encrypted)*.
5. Load *KDM for 2K StEM (Encrypted) (OBAE)* targeted at the published identity certificate obtained in step 1.
6. Playback *DCI 2K StEM (OBAE) (Encrypted)*. Failure to playback is cause to fail this test.
7. Delete *KDM for 2K StEM (Encrypted) (OBAE)* loaded in step 5.
8. Load *KDM for 2K StEM (Encrypted) (OBAE)* targeted at the reserved identity certificate obtained in step 1.
9. Playback *DCI 2K StEM (OBAE) (Encrypted)*. Failure to playback is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1.3<br>SMPTE-430-2 |
| **Test Materials** | *KDM for 2K StEM (Encrypted) (OBAE)* |

| |
|---|
| *DCI 2K StEM*<br>*(OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.20. Validity of Media Block Certificates

### Objective

Verify that the Media Block certificates are valid.

### Procedures

For each Media Block of the Test Subject:

1. Obtain, from the manufacturer, (i) the one or more X.509 digital leaf certificates associated with the Media Block and (ii) the complete chain of signer certificates for each of the one or two leaf certificate, up to and including the manufacturer's self-signed root certificate.

2. For each certificate, perform the following tests:

    - 2.1.1. Basic Certificate Structure
    - 2.1.2. SignatureAlgorithm Fields
    - 2.1.3. SignatureValue Field
    - 2.1.4. SerialNumber Field
    - 2.1.5. SubjectPublicKeyInfo Field
    - 2.1.6. Deleted Section
    - 2.1.7. Validity Field
    - 2.1.8. AuthorityKeyIdentifier Field
    - 2.1.9. KeyUsage Field
    - 2.1.10. Basic Constraints Field

- 2.1.11. Public Key Thumbprint
- 2.1.12. Organization Name Field
- 2.1.13. OrganizationUnitName Field
- 2.1.14. Entity Name and Roles Field
- 2.1.15. Unrecognized Extensions
- 2.1.16. Signature Validation

3. For the complete chain of signer certificates, perform 2.1.17. Certificate Chains

Failure of any of these above conditions is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1<br>SMPTE-430-2 |
| **Test Equipment** | **Network Analyzer**<br>**openssl** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 18.2. Projector Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 6.1.21. Maximum Number of DCP Keys (OBAE)

### Objective

Verify that the system supports playback of two compositions with up to 256 different essence encryption keys each

### Procedures

> **Note:**
> The KDMs specified to be used in this test additionally have one of each type of forensic marking keys FMIK and FMAK. Receiving devices shall process such keys in accordance with the individual implementation, in a manner that will not affect the requirements related to the maximum number of content keys (MDIK and MDAK).

> **Note:**
> The `CPLStart` and `CPLEnd` records are triggered by the first and last edit unit, respectively, of the CPL reproduced by the Test Subject. For example, in the case of an OMB with OBAE capability, the first and last edit units of the CPL are OBAE edit units, since picture edit units are not reproduced despite Main Picture assets being present in the CPL received by the OMB.

1. Load the compositions *128 Reel Composition, "A" Series (OBAE)* and *128 Reel Composition, "B" Series (OBAE)* on to the Test Subject.

2. Create a show that contains *128 Reel Composition, "A" Series (OBAE)* and *128 Reel Composition, "B" Series (OBAE)*. Each composition contains 128 reels of plaintext content.

3. Play the show. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback started. Failure to play the complete show shall be cause to fail this test.

4. Extract a security log from the Test Subject that includes the range of time during which Step 3 was carried out

5. Using a **Text Editor**, locate the first `CPLStart` and last `CPLEnd` records that occurred after the time recorded in Step 3. Let *Plaintext Time* be the absolute difference between the `TimeStamp` values of the two records.

6. Load the compositions *128 Reel Composition, "A" Series (OBAE) (Encrypted)* and *128 Reel Composition, "B" Series (OBAE) (Encrypted)* on to the Test Subject.

7. Load the KDMs *KDM for 128 Reel Composition, "A" Series (OBAE) (Encrypted)* and *KDM for 128 Reel Composition, "B" Series (OBAE) (Encrypted)* on to the Test Subject.

8. Create a show that contains *128 Reel Composition, "A" Series (OBAE) (Encrypted)* and *128 Reel Composition, "B" Series (OBAE) (Encrypted)*. Each composition contains 128 reels of encrypted content where 256 distinct cryptographic keys are used.

9. Play the show. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback started. Failure to play the complete show shall be cause to fail this test.

10. The presence of any observable artifacts in the reproduced picture and/or sound shall be cause to fail this test.

11. Extract a security log from the Test Subject that includes the range of time during which Step 9 was carried out.

12. Using a **Text Editor**, locate the first `CPLStart` and last `CPLEnd` records that occurred after the time recorded in Step 9. Let `Ciphertext Time` be the absolute difference between the `TimeStamp` values of the two records.

13. An absolute difference of more than 1 second between `Ciphertext Time` and `Plaintext Time` is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.7.7<br>[OBAE-ADD]<br>SMPTE-430-1 |
| **Test Materials** | *128 Reel Composition, "A" Series (OBAE)*<br>*128 Reel Composition, "B" Series (OBAE)*<br>*128 Reel Composition, "A" Series (OBAE) (Encrypted)*<br>*128 Reel Composition, "B" Series (OBAE) (Encrypted)*<br>*KDM for 128 Reel Composition, "A" Series (OBAE) (Encrypted)*<br>*KDM for 128 Reel Composition, "B" Series (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.1.22. Restriction of Keying to Valid CPLs (OBAE)

### Objective

Verify that the OBAE-capable SM validates CPLs and logs results as a prerequisite to preparing the suite for the associated composition playback.

### Procedures

1. Supply the CPL *DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)*, keyed with *KDM for DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)*, to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

2. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

3. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of the CPL. Verify that the value of the `SignerID` parameter contains the Certificate Thumbprint of the certificate used to sign the CPL. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `AssetHashError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `AssetHashError` exception shall be cause to fail this test.

4. Supply the CPL *DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)*, keyed with *KDM for DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)* to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

5. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

6. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of the CPL. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `SignatureError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `SignatureError` exception shall be cause to fail this test.

7. Supply the CPL *DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)*, keyed with *KDM for DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)* to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

8. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

9. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of the CPL. Verify that the value of the `SignerID` parameter contains the Certificate Thumbprint of the certificate used to sign the CPL. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `AssetMissingError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `AssetMissingError` exception shall be cause to fail this test.

10. Supply the CPL *DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)*, keyed with *KDM for DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)* to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

11. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

12. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `CPLFormatError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `CPLFormatError` exception shall be cause to fail this test.

13. Supply the CPL *DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)*, keyed with *KDM for DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)* to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.

14. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

15. Extract a security log from the Test Subject and using a **Text Editor**, identify the `CPLCheck` event associated with the above operation and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the `contentId` element contains the `Id` of the CPL. Verify that `ReferencedIDs` element contains a `CompositionID` parameter with a value that is the `Id` of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `CertFormatError` exception in the `CPLCheck` log record. Record any additional parameters associated with the exception. A missing `CertFormatError` exception shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5<br>SMPTE-430-5 |
| **Test Materials** | *DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)*<br>*KDM for DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)*<br>*DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)*<br>*KDM for DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)*<br>*DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)*<br>*KDM for DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)*<br>*DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)*<br>*KDM for DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)*<br>*DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)*<br>*KDM for DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |

## 6.1.23. ContentAuthenticator Element Check (OBAE)

### Objective

- Verify that the OBAE-capable Test Subject checks that one of the certificates in the certificate chain supplied with the CPL has a certificate thumbprint that matches the value of the KDM `<ContentAuthenticator>` element.

- Verify that the OBAE-capable Test Subject checks that such certificate indicates only a "Content Signer (CS) role.

### Procedures

For each of the malformations below, load the indicated CPL and KDM on to the Test Subject. Verify that the the KDM is not used to enable playback. A successful playback is cause to fail this test.

1. Use the composition *DCI 2K StEM (OBAE) (Encrypted)* and supply the KDM *KDM with invalid ContentAuthenticator (OBAE)*. The KDM contains a `<ContentAuthenticator>` element having a certificate thumbprint value that does not match the thumbprint of one of the signer certificates in the certificate chain that signed the associated CPL.

2. Use the composition *DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)* and supply the KDM *KDM for DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)*. The KDM contains a `<ContentAuthenticator>` element having a certificate thumbprint value that matches the thumbprint of one of the signer certificates in the certificate chain that signed the associated CPL but that certificate has no role.

3. Use the composition *DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)* and supply the KDM *KDM for DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)*. The KDM contains a `<ContentAuthenticator>` element having a certificate thumbprint value that matches the thumbprint of one of the signer certificates in the certificate chain that signed the associated CPL but that certificate has a bad role (SM).

4. Use the composition *DCI Malformed Test 18b: CPL signed with Extra Role Certificate (OBAE) (Encrypted)* and supply the KDM *KDM for DCI Malformed Test 18b: KDM for CPL signed with Extra Role Certificate (OBAE) (Encrypted)*. The KDM contains a `<ContentAuthenticator>` element having a certificate thumbprint value that matches the thumbprint of one of the signer certificates in the certificate chain that signed the associated CPL but that certificate has an extra role.

5. Extract a security log from the Test Subject and using a **Text Editor**, identify the `FrameSequencePlayed` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of `FrameSequencePlayed` log records that contain `ContentAuthenticatorError` exceptions. Record any additional parameters associated with the exception. A missing `ContentAuthenticatorError` exception in any of the associated `FrameSequencePlayed` log records shall be cause to fail this test. Only for the operation associated with step 2, a correctly recorded `CPLCheck` log record with a `CertFormatError` exception is an allowable substitute for a `FrameSequencePlayed` log record to satisfy the requirements of this step of the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5<br>SMPTE-429-7<br>SMPTE-430-1<br>SMPTE-430-2<br>SMPTE-430-5 |
| **Test Materials** | *DCI 2K StEM (OBAE) (Encrypted)*<br>*KDM with invalid ContentAuthenticator (OBAE)*<br>*DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)*<br>*KDM for DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)*<br>*DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)*<br>*KDM for DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)*<br>*DCI Malformed Test 18b: CPL signed with Extra Role Certificate (OBAE) (Encrypted)*<br>*KDM for DCI Malformed Test 18b: KDM for CPL signed with Extra Role Certificate (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |

## 6.1.24. KDM Date Check (OBAE)

### Objective

Verify that the OBAE-capable Test Subject checks that the playout date is within the time period defined by the KDM `ContentKeysNotValidBefore` and `ContentKeysNotValidAfter` elements.

### Procedures

1. Load the composition *DCI 2K StEM (OBAE) (Encrypted)* and KDM *KDM that has expired (OBAE)*, which contains a valid decryption keys, but the KDM has expired.

2. Attempt to play the *DCI 2K StEM (OBAE) (Encrypted)* composition and record the result. Verify that the composition cannot be played. Successful playout is cause to fail this test.

3. Load the composition *DCI 2K StEM (OBAE) (Encrypted)* and the KDM *KDM with future validity period (OBAE)*, which contains a valid decryption keys, but the KDM has is not yet valid.

4. Attempt to play the *DCI 2K StEM (OBAE) (Encrypted)* composition and record the result. Verify that the composition cannot be played. Successful playout is cause to fail this test.

5. Load the composition *DCI 2K StEM (OBAE) (Encrypted)* and KDM *KDM that has recently expired (OBAE)*, which contains a valid decryption keys, but the KDM has expired.

6. Attempt to play the *DCI 2K StEM (OBAE) (Encrypted)* composition and record the result. Verify that the composition cannot be played. Successful playout is cause to fail this test.

7. Load the composition *DCI 2K StEM (OBAE) (Encrypted)* and the KDM *KDM with future validity period (OBAE)*, which contains a valid decryption keys, but the KDM has is not yet valid.

8. Attempt to play the *DCI 2K StEM (OBAE) (Encrypted)* composition and record the result. Verify that the composition cannot be played. Successful playout is cause to fail this test.

9. Extract a security log from the Test Subject and using a **Text Editor**, identify the `FrameSequencePlayed` events associated with the above steps and:

    a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Missing required elements or incorrect parameters shall be cause to fail this test.

    b. Confirm the presence of a `FrameSequencePlayed` log record that contains a `ValidityWindowError` exception. Record any additional parameters associated with the exception. A missing `ValidityWindowError` exception in any of the associated `FrameSequencePlayed` log records shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.8<br>SMPTE-430-1<br>SMPTE-430-5 |
| **Test Materials** | *KDM with future validity period (OBAE)*<br>*KDM that has recently expired (OBAE)*<br>*KDM that has expired (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

# 6.2. Link Encryption (LE)

*This section is only applicable to systems that use Link Encryption.*

**Note:**
The DCSS restricts the use of Link Encryption (LE) to non-MMB configurations and non-OBAE processing devices. Therefore LE related tests are not directed to Procedural Chapters 20 and 21.

## 6.2.1. Deleted Section

The section "LDB Trust" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 6.2.2. Special Auditorium Situation Operations

### Objective

*The following applies only to a Test Subject that supports Special Auditorium Situations.*

- Verify that the SM enables Special Auditorium Situations only when the SM receives a KDM whose TDL contains only the identities of the remote SPBs identified during TLS authentication.
- Verify that the SM shall not support the use of more than one image processor remote SPB (LD/LE) for any LDB/ projector configuration.
- Verify that the SM authenticates each remote SPB against the TDL using a dedicated TLS session.
- Verify that the SM keys each remote SPB for Link Encryption operation using standardized Intra-Theater Security (ASM) Messaging.

### Procedures

**Note:**
This test involves the use of more than one **asm-responder** simulator program, each with its own device certificate TDL needs to be populated with the appropriate certificate thumbprints for the device or combination of devices intended.

1. If not already on the system, ingest the composition *DCI 2K Sync Test (Encrypted)*.

2. Using supplied documentation (system manuals) and/or with the assistance of the manufacturer, list the possible Special Auditorium Situations that the Test Subject can support (*e.g.* 2 LDB/projectors, 1 LD/LE 1 LDB/projector, 2 LD/LE 2 LDB/projectors, 1 MB/projector 1 LDB/projector).

3. For each of the Special Auditorium Situations recorded in Step 2, set up and start corresponding **asm-responder** simulators using device certificates that are appropriate for each **asm-responder** role in the Special Auditorium Situation (*e.g.* LD and PR (projector that utilizes electronic marriage), LD/PR (permanently married projector) or LD/LE (image processor) and perform the following Steps:

    a. Power up the part of the system that contains the MB and observe that all the TLS connections become established.

    b. Create the KDM *KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and an additional device certificate*.

    c. Create the KDM *KDM with a TDL that contains all but one of the certificate thumbprints for the devices in the special auditorium situation*.

    d. Create the KDM *KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and the "assume trust" thumbprint*.

    e. Create the KDM *KDM with a TDL that contains one more LD/LE device thumbprints than there are LD/projector thumbprints in the special auditorium situation*.

    f. Create the KDM *KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation*.

    g. Delete any KDMs already existing in the Test Subject. Ingest the KDM *KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and an additional device certificate*. Attempt to play the composition *DCI 2K Sync Test (Encrypted)*, the system should prevent playback. If the system plays the content, this shall be cause to fail this test.

    h. Delete any KDMs already existing in the Test Subject. Ingest the KDM *KDM with a TDL that contains all but one of the certificate thumbprints for the devices in the special auditorium situation*. Attempt to play the composition *DCI 2K Sync Test (Encrypted)*, the system should prevent playback. If the system plays the content, this shall be cause to fail this test.

    i. Delete any KDMs already existing in the Test Subject. Ingest the KDM *KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and the "assume trust" thumbprint*. Attempt to play the composition *DCI 2K Sync Test (Encrypted)*, the system should prevent playback. If the system plays the content, this shall be cause to fail this test.

    j. Delete any KDMs already existing in the Test Subject. Ingest the KDM *KDM with a TDL that contains one more LD/LE device thumbprints than there are LD/projector thumbprints in the special auditorium situation*. Attempt to play the composition *DCI 2K Sync Test (Encrypted)*, the system should prevent playback. If the system plays the content, this shall be cause to fail this test.

k. Delete any KDMs already existing in the Test Subject. Ingest the KDM *KDM with Assume Trust TDL Entry for DCI 2K Sync Test (Encrypted)*. Attempt to play the composition *DCI 2K Sync Test (Encrypted)*, the system should prevent playback. If the system plays the content, this shall be cause to fail this test.

l. Delete any KDMs already existing in the Test Subject. Ingest the KDM *KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation*. Attempt to play the composition *DCI 2K Sync Test (Encrypted)*, the system should successfully complete playback. If the system does not successfully play the content, this shall be cause to fail this test.

m. Examine the output from the **asm-responder** simulators with an LD role. Failure for any simulator with an LD role to have received at least one LE key from the Test Subject using Auditorium Security Messages shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.4.1, 9.4.3.5 |
| **Test Equipment** | **asm-responder** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and an additional device certificate*<br>*KDM with a TDL that contains all but one of the certificate thumbprints for the devices in the special auditorium situation*<br>*KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and the "assume trust" thumbprint*<br>*KDM with a TDL that contains one more LD/LE device thumbprints than there are LD/projector thumbprints in the special auditorium situation*<br>*KDM with Assume Trust TDL Entry for DCI 2K Sync Test (Encrypted)*<br>*KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 6.2.3. LE Key Usage

### Objective

Verify that a fresh Link Encryption key is used for each movie showing.

### Procedures

Using a suitable utility (*e.g.* a diagnostic program for the link decrypting device) to display the unique identifier (LE KeyID or other suitable identifier) of the LE session key that is currently in use by the LDB, perform the following procedures:

1. Setup and play the composition *DCI 2K StEM (Encrypted)*.

2. Record the LE key identifier reported by the utility to be in use during the playback.

3. Repeat Step 1.

4. Record the LE key identifier reported by the utility to be in use during the playback. If a new session key is not selected this is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.4<br>SMPTE-430-6 |
| **Test Equipment** | **LDB Monitor** |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 6.2.4. MB Link Encryption

### Objective

*The following applies to a Test Subject that is a MB that provides one or more link encrypted image interfaces.*

Verify that Link Encryption is applied to every image output that is capable of delivering d-cinema content to a remote SPB (link decryptor).

Verify that Link Encryption is applied for both plaintext and ciphertext compositions.

Verify that for playback of content that is not encrypted (therefore no KDM or TDL for this content exists) the SM automatically assumes "trust" in the LDB and projector SPBs for purposes of keying the LDB and enabling playback.

### Procedures

**Note:**
This test can involve the use of more than one **DCI Projector** or **asm-responder** simulator programs, each with its own device certificate. This places special emphasis on preparing and selecting the correct KDM for a stage of the test. The KDM's TDL needs to be populated with the appropriate certificate thumbprints for the device or combination of devices intended.

**Note:**
Steps 2d and 2g of this test require verification that the link encryption applied to every interface can be correctly decoded. If the Test Subject uses identical LE keys on all image interfaces, and does not require a "Special Auditorium Situation" for more than one image interface to be active, a single **DCI Projector** may be used to check each interface in turn. If the Test Subject keys the interfaces with different LE keys, or requires a "Special Auditorium Situation", one of the following strategies may be employed to allow the objective to be confirmed:

i. If the Testing Organization has access to as many **DCI Projectors** as there are image interfaces, the test may be carried out with multiple projectors.

ii. If there are less **DCI Projectors** available than image interfaces, an **asm-responder**, with unique LD (and PR if appropriate) device certificates, shall be substituted for each **DCI Projector** required by the configuration. Each **asm-responder** shall be responsible for capturing the LE key(s) delivered for each respective of the image interface configured in the Special Auditorium Situation. A single **DCI Projector** is used to verify that each of the image outputs is delivering a valid link encrypted signal, by connecting to the respective image interface and using an **asm-requester** configured to connect to the **DCI Projector** to send the LE key(s) captured by the **asm-responder** corresponding to that image interface.

1. With the assistance of the manufacturer, list the image interfaces present on the Test Subject that are capable of delivering d-cinema content to a remote SPB (link decryptor).

2. For each of the interfaces identified in the previous step, perform the following procedures:

    a. Attach a suitable monitor to the interface that connects the LD and the Media Block (MB) without disrupting the LE to LD connection (*i.e.*, "tap" the connection; this may require soldering a special test adapter).

    b. Remove and restore power to the equipment containing the MB. This forces fresh TLS sessions to the remote SPBs and ensures that fresh LE keys are generated.

    c. Setup and play a show using *DCI 2K StEM* This test material contains a plaintext composition.

    d. Verify that the image is displayed properly on the projection screen. Failure to observe a correctly displayed image is cause to fail this test

    e. Verify that only a scrambled signal is seen on the monitor. A non-scrambled image on the monitor is cause to fail this test.

    f. Setup and play a show using *DCI 2K StEM (Encrypted)*, keyed with *KDM for 2K StEM (Encrypted)*, or if the Test Subject requires use of a "Special Auditorium Situation" type TDL to enable playback, *KDM for 2K StEM with Device Specific Special Auditorium TDL*. This test material contains an encrypted composition.

    g. Verify that the image is displayed properly on the projection screen. Failure to observe a correctly displayed image is cause to fail this test

    h. Verify that only a scrambled signal is seen on the monitor. A non-scrambled image on the monitor is cause to fail this test.

## Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.2.2.10, 8.4.2, 8.4.3.1, 9.4.4 |
| **Test Equipment** | **Dual-Link Monitor**<br>**Bridge Tap Connector**<br>**DCI Projector** |

| | |
|---|---|
| **asm-responder**<br>**asm-requester** | **Test Materials** |
| *DCI 2K StEM*<br>*DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)*<br>*KDM for 2K StEM with Device Specific Special Auditorium*<br>*TDL* | |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

## 6.3. Clocks and Time

This section describes general requirements concerning the time awareness of the projection system and its individual components. All procedures are applicable to the Security Manager, with the notable exception of section 6.3.2, which is applicable to all SPBs of Type 1.

### 6.3.1. Clock Adjustment

#### Objective

- Verify that in order to maintain synchronization between auditoriums, exhibitors are able to adjust a SM's time by a maximum of +/- 6 minutes within any calendar year.
- Verify that the SM time adjustments are logged events.

#### Procedures

**Note:**
The following procedures are likely to fail if the Test Subject has had its time adjusted since manufacture. The current time may not be centered on the adjustment range zero point. Any such adjustments, however, will be evidenced in the security log and by examining the relevant `TimeOffset` elements, the zero point can be derived and the time set accordingly. If

necessary, contact the manufacturer for assistance in determining and setting the time to the center of the range of adjustment for the current calendar year.

1. Select for playback the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.

2. Play back the composition and at the moment the last frame of picture is reproduced, record the UTC time as provided by an **Accurate Real-Time Clock**.

3. Attempt to advance the time of the SM by 6 minutes. Record whether the adjustment was successful and the UTC time at the moment of adjustment. Failure to successfully adjust the time is cause to fail this test.

4. Repeat Steps 1 and 2.

5. Attempt to advance the time of the SM by 5 seconds. Record whether the adjustment was successful and the UTC time at the moment of adjustment. If the time can be successfully adjusted, this is cause to fail this test.

6. Return the time to the zero point, *i.e.* retard by the total amount successfully advanced in Steps 3 and 5.

7. Attempt to retard the time of the SM by 6 minutes. Record whether the adjustment was successful and the UTC time at the moment of adjustment. Failure to successfully adjust the time is cause to fail this test.

8. Repeat Steps 1 and 2.

9. Attempt to retard the time of the SM by 5 seconds. Record whether the adjustment was successful and the UTC time at the moment of adjustment. If the time can be successfully adjusted, this is cause to fail this test.

10. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

11. Locate a `FrameSequencePlayed` event caused by Step 2. Subtract the value of the time recorded in Step 2 (UTC time) from the `TimeStamp` from the `LogRecord` (System time). Record this time as the delta of System time to UTC time for the unadjusted state.

12. Locate the `SPBClockAdjust` event from Step 3 and confirm that the `TimeStamp` contains a value which is the time recorded in Step 3 (UTC time) + the delta from Step 11 + 6 minutes.

13. Locate the `SPBClockAdjust` event from Step 7 and confirm that the `TimeStamp` contains a value which is the time recorded in Step 7 (UTC time) + the delta from Step 11 - 6 minutes.

14. Locate the `SPBClockAdjust` event from Step 5 and confirm the presence of an Exception with a name of `AdjustmentRangeError`. Confirm that the `TimeStamp` contains a value as follows:
    $T_{log} = T_{step5} + T_{step11} + T_{offset}$
    where:
    $T_{log}$ is the Timestampof the log event
    $T_{step5}$ is the time record in Step 5 (UTC time)
    $T_{step11}$ is the delta from Step 11
    $T_{offset}$ is 6 minutes
    The value of the `TimeOffset` parameter shall be ignored.

15. Locate the `SPBClockAdjust` event from Step 9 and confirm the presence of an Exception with a name of `AdjustmentRangeError`. Confirm that the `TimeStamp` contains a value as follows:
    $T_{log} = T_{step9} + T_{step11} - T_{offset}$

where:
$T_{log}$ is the Timestampof the log event
$T_{step9}$ is the time record in Step 9 (UTC time)
$T_{step11}$ is the delta from Step 11
$T_{offset}$ is 6 minutes
The value of the `TimeOffset` parameter shall be ignored.

16. Locate a `FrameSequencePlayed` event caused by Step 4. Confirm that the `TimeStamp` contains a value which is the time recorded in Step 4 (UTC time) + the delta from Step 11 + 6 minutes.

17. Locate a `FrameSequencePlayed` event caused by Step 8. Confirm that the `TimeStamp` contains a value which is the time recorded in Step 8 (UTC time) + the delta from Step 11 - 6 minutes.

18. Incorrect or missing `LogRecord` elements for Steps 11 through 17 shall be cause to fail this test. *Note: The `TimeStamp` values will have an accuracy that depends on various factors such as system responsiveness, test operator acuity, etc, and are essentially approximate. The intent is to verify that the `TimeStamp` values indeed reflect the time adjustments*.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |
| **Test Equipment** | **Accurate Real-Time Clock** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 6.3.2. SPB Type 1 Clock Battery

### Objective

Verify that the Type 1 SPB clock's battery is changeable without losing track of proper time.

### Procedures

In the case where the Test Subject must be returned to the manufacturer for battery replacement (*i.e.* field replacement of the battery is not possible), the remainder of this procedure shall be ignored and the reported result of this procedure shall be "N/A".

The phrase "record synchronized accurate time" used below means that the Test Operator records the value of the **Accurate Real-Time Clock** so as to determine a range of predictable deltas between the value of the **Accurate Real-Time Clock** and the timestamp in the log record that corresponds to an event. It is not important that the two times be equal, but that the difference be predictable to within a range that accommodates both variances in the responsiveness of the Test Subject for time stamping the logged operation and the accuracy of the Test Operator. Note: Each end of the range of the deltas is extended by an additional 2 seconds to allow for minor resolution inaccuracies of the testing methodology.

1. Perform the following actions:

    a. Adjust the clock of the Test Subject +2 seconds, record synchronized accurate time.

    b. Adjust the clock -2 seconds, record synchronized accurate time.

2. Repeat step 1 four times.

3. Perform the battery replacement procedure per the manufacturer's instructions.

4. Perform the following actions:

    a. Adjust the clock +2 seconds, record synchronized accurate time.

    b. Adjust the clock -2 seconds, record synchronized accurate time.

5. Extract a log report, or transfer the log records over ASM, for a time period that includes the times during which steps 1-4 were performed.

6. The absence of a log record for any of the clock adjustments made by the above steps shall be cause to fail this test.

7. For each of the five repetitions of step 1a, subtract 2 seconds from the event timestamp to compensate for the 2 seconds added to the SM clock. Compute the delta, in seconds, between the recorded synchronized accurate time and the logged time for the event. Assign the label of $1a_{min}$ to the minimum delta in the set. Assign the label of $1a_{max}$ to the maximum delta in the set.

8. For each of the five repetitions of step 1b, compute the delta, in seconds, between the recorded synchronized accurate time and the logged time for the event. No adjustment to the event timestamps is required as the clock has been returned to its original setting. Assign the label of $1b_{min}$ to the minimum delta in the set. Assign the label of $1b_{max}$ to the maximum delta in the set.

9. For the event in step 4a, subtract 2 seconds from the event timestamp to compensate for the 2 seconds added to the SM clock. Compute the delta, in seconds, between the recorded synchronized accurate time and the logged time for the event and record the value as *4a*. A value of *4a* that is less than $1a_{min} - 2$ seconds is cause to fail the test. A value of 4a that is greater than $1a_{max} + 2$ seconds is cause to fail the test.

10. For the event in step 4b, compute the delta, in seconds, between the recorded synchronized accurate time and the logged time for the event and record the value as *4b*. A value of *4b* that is less than $1b_{min}$ - 2 seconds is cause to fail the test. A value of *4b* that is greater than $1b_{max} + 2$ seconds is cause to fail the test.

## Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |
| **Test Equipment** | **Accurate Real-Time Clock** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.3.3. Clock Resolution

### Objective

Verify that the SM clock has a resolution to one second.

### Procedures

1. Setup and play back a show containing the composition *64 Reel Composition, 1 Second Reels (Encrypted)*, keyed with *KDM for 64 1 second reel Composition (Encrypted)*. This composition contains 64 reels of encrypted essence, each with a duration of one (1) second.

2. Examine the log records produced by the above playback. If the time stamps of the log entries are recorded to one (1) second resolution, it can be deduced that the SM clock has a resolution of at least one second. Failure to meet this requirement is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |
| **Test Materials** | *64 Reel Composition, 1 Second Reels (Encrypted)*<br>*KDM for 64 1 second reel Composition (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.3.4. Clock Resolution (OMB)

### Objective

Verify that the OMB clock has a resolution to one second.

### Procedures

1. Setup and play back a show containing the composition *64 Reel Composition, 1 Second Reels (OBAE) (Encrypted)*, keyed with *KDM for 64 1 second reel Composition (OBAE) (Encrypted)*. This composition contains 64 reels of encrypted essence, each with a duration of one (1) second.

2. Examine the log records produced by the above playback. If the time stamps of the log entries are recorded to one (1) second resolution, it can be deduced that the OMB clock has a resolution of at least one second. Failure to meet this requirement is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |
| **Test Materials** | *64 Reel Composition, 1 Second Reels (OBAE) (Encrypted)*<br>*KDM for 64 1 second reel Composition (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 6.3.5. Clock Adjustment (OMB)

### Objective

- Verify that in order to maintain synchronization between auditoriums, exhibitors are able to adjust an OMB's time by a maximum of +/- 6 minutes within any calendar year.

- Verify that the OMB time adjustments are logged events.

### Procedures

> **Note:**
> The following procedures are likely to fail if the Test Subject has had its time adjusted since manufacture. The current time may not be centered on the adjustment range zero point. Any such adjustments, however, will be evidenced in the security log and by examining the relevant `TimeOffset` elements, the zero point can be derived and the time set accordingly. If necessary, contact the manufacturer for assistance in determining and setting the time to the center of the range of adjustment for the current calendar year.

1. Select for playback the composition *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*.

2. Play back the composition and at the moment the last frame of picture is reproduced, record the UTC time as provided by an **Accurate Real-Time Clock**.

3. Attempt to advance the time of the OMB by 6 minutes. Record whether the adjustment was successful and the UTC time at the moment of adjustment. Failure to successfully adjust the time is cause to fail this test.

4. Repeat Steps 1 and 2.

5. Attempt to advance the time of the OMB by 5 seconds. Record whether the adjustment was successful and the UTC time at the moment of adjustment. If the time can be successfully adjusted, this is cause to fail this test.

6. Return the time to the zero point, *i.e.* retard by the total amount successfully advanced in Steps 3 and 5.

7. Attempt to retard the time of the OMB by 6 minutes. Record whether the adjustment was successful and the UTC time at the moment of adjustment. Failure to successfully adjust the time is cause to fail this test.

8. Repeat Steps 1 and 2.

9. Attempt to retard the time of the OMB by 5 seconds. Record whether the adjustment was successful and the UTC time at the moment of adjustment. If the time can be successfully adjusted, this is cause to fail this test.

10. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

11. Locate a `FrameSequencePlayed` event caused by Step 2. Subtract the value of the time recorded in Step 2 (UTC time) from the `TimeStamp` from the `LogRecord` (System time). Record this time as the delta of System time to UTC time for the unadjusted state.

12. Locate the `SPBClockAdjust` event from Step 3 and confirm that the `TimeStamp` contains a value which is the time recorded in Step 3 (UTC time) + the delta from Step 11 + 6 minutes.

13. Locate the `SPBClockAdjust` event from Step 7 and confirm that the `TimeStamp` contains a value which is the time recorded in Step 7 (UTC time) + the delta from Step 11 - 6 minutes.

14. Locate the `SPBClockAdjust` event from Step 5 and confirm the presence of an Exception with a name of `AdjustmentRangeError`. Confirm that the `TimeStamp` contains a value as follows:
    $T_{log} = T_{step5} + T_{step11} + T_{offset}$
    where:
    $T_{log}$ is the Timestampof the log event
    $T_{step5}$ is the time record in Step 5 (UTC time)
    $T_{step11}$ is the delta from Step 11
    $T_{offset}$ is 6 minutes
    The value of the `TimeOffset` parameter shall be ignored.

15. Locate the `SPBClockAdjust` event from Step 9 and confirm the presence of an Exception with a name of `AdjustmentRangeError`. Confirm that the `TimeStamp` contains a value as follows:
    $T_{log} = T_{step9} + T_{step11} - T_{offset}$
    where:
    $T_{log}$ is the Timestampof the log event
    $T_{step9}$ is the time record in Step 9 (UTC time)
    $T_{step11}$ is the delta from Step 11
    $T_{offset}$ is 6 minutes
    The value of the `TimeOffset` parameter shall be ignored.

16. Locate a `FrameSequencePlayed` event caused by Step 4. Confirm that the `TimeStamp` contains a value which is the time recorded in Step 4 (UTC time) + the delta from Step 11 + 6 minutes.

17. Locate a `FrameSequencePlayed` event caused by Step 8. Confirm that the `TimeStamp` contains a value which is the time recorded in Step 8 (UTC time) + the delta from Step 11 - 6 minutes.

18. Incorrect or missing `LogRecord` elements for Steps 11 through 17 shall be cause to fail this test. *Note: The `TimeStamp` values will have an accuracy that depends on various factors such as system responsiveness, test operator acuity, etc, and are essentially approximate. The intent is to verify that the `TimeStamp` values indeed reflect the time adjustments*.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |
| **Test Equipment** | **Accurate Real-Time Clock** |
| **Test Materials** | *DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)* |

#### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |

## 6.4. Forensic Marking (FM)

### 6.4.1. FM Application Constraints

#### Objective

- Verify that FM is not applied to non-encrypted audio or image content.
- Verify that FM is not applied to Track Files that are not encrypted in case portions of a composition are encrypted and other portions are not.
- Verify that event log records reflect the FM state.

#### Procedures

1. Play back the DCP *2K FM Application Constraints (Encrypted)*, keyed with *KDM for 2K FM Application Constraints (Encrypted)* and present the reproduced image and each of the 16 channels of sound to the appropriate Forensic Marking (FM) detector. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback is started. This package has a CPL that selects between encrypted and plaintext, image and sound track files in a specific order.

2. Verify that the FM detectors report the following status for the presentation: Note: Each segment of the presentation is approximately 35 minutes long and contains slates at the head and tail.

    a. The first segment of the presentation should indicate both image FM and sound FM are absent.

    b. The second segment of the presentation should indicate image FM is present and sound FM is absent.

    c. The third segment of the presentation should indicate image FM is absent and sound FM is present.

    d. The last segment of the presentation should indicate both image FM and sound FM are present.

    Any discrepancy between the expected and reported FM states is cause to fail this test.

3. Extract a security log from the Test Subject that includes the range of time during which step 1 was carried out.

4. Using a **Text Editor**, locate the FrameSequencePlayed records that correspond to the encrypted track files played during the presentation segments and:

    a. Verify there are no FrameSequencePlayed records corresponding to the first segment of the presentation (plaintext track files do not generate these records).

    b. Verify that FrameSequencePlayed records corresponding to the second segment of the presentation contain values of the ImageMark parameter equal to "true" and do not contain an AudioMark parameter.

    c. Verify that FrameSequencePlayed records corresponding to the third segment of the presentation contain values of the AudioMark parameter equal to "true" and do not contain an ImageMark parameter.

    d. For the FrameSequencePlayed records corresponding to the last segment of the presentation:

        i. Verify that records associated with image track files contain one ImageMark parameter with value "true" and do not contain an AudioMark parameter; and

        ii. verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter

    Failure of any these verifications is cause to fail this test.

Note: the equipment manufacturer is required to provide a suitable FM decoder (*i.e.*, software and hardware).

## Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.2 |
| **Test Equipment** | **FM Detector**<br>**Accurate Real-Time Clock** |
| **Test Materials** | *2K FM Application Constraints (Encrypted)*<br>*KDM for 2K FM Application Constraints (Encrypted)* |

## Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| | | | |

| | | | |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.4.2. Granularity of FM Control

### Objective

- Verify that "No FM mark" states are capable of being independently controlled, for audio and image, via appropriate use of the `ForensicMarkFlagList` element of the KDM for audio and image Track Files.
- Verify that the `ForensicMarkFlagList` element of the KDM and thus the "no FM mark" state applies to the entire CPL/composition, according to the associated KDM.
- Verify that the "no FM mark" state does not apply to any other composition, even if the other composition is part of the same showing (*i.e.*, same Show Playlist).
- Verify that event log records reflect the FM state.

### Procedures

1. Build a show playlist out of the following four compositions, in the order listed:
    1. *2K FM Control Granularity - No FM (Encrypted)*, keyed with *KDM for 2K FM Control Granularity - No FM (Encrypted)*.
    2. *2K FM Control Granularity - Image Only FM (Encrypted)*, keyed with *KDM for 2K FM Control Granularity - Image Only FM (Encrypted)*.
    3. *2K FM Control Granularity - Sound Only FM (Encrypted)*, keyed with *KDM for 2K FM Control Granularity - Sound Only FM (Encrypted)*.
    4. *2K FM Control Granularity - Image and Sound FM (Encrypted)*, keyed with *KDM for 2K FM Control Granularity - Image and Sound FM (Encrypted)*.
2. Play back the show, and present the reproduced image and each of the 16 channels of sound to the appropriate Forensic Marking (FM) detector. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback is started.
3. Verify that the FM detectors report the following status for the presentation:
    a. *2K FM Control Granularity - No FM (Encrypted)*: No image FM and no audio FM for the whole composition.
    b. *2K FM Control Granularity - Image Only FM (Encrypted)*: Image FM present, but no audio FM, for the whole composition.

c. *2K FM Control Granularity - Sound Only FM (Encrypted)*: No image FM, but audio FM present, for the whole composition.

d. *2K FM Control Granularity - Image and Sound FM (Encrypted)*: Image FM and audio FM present for the whole composition.

Any discrepancy between the expected and reported FM states is cause to fail this test.

4. Extract a security log from the Test Subject that includes the range of time during which step 2 was carried out.

5. Using a **Text Editor**, locate FrameSequencePlayed records corresponding to the playback and:

a. For the FrameSequencePlayed records corresponding to the playback of *2K FM Control Granularity - No FM (Encrypted)*:

i. Verify that records associated with image track files contain one ImageMark parameter with value "false" and do not contain an AudioMark parameter; and

ii. verify that records associated with audio track files contain one AudioMark parameter with value "false" and do not contain an ImageMark parameter.

b. For the FrameSequencePlayed records corresponding to the playback of *2K FM Control Granularity - Image Only FM (Encrypted)*:

i. Verify that records associated with image track files contain one ImageMark parameter with value "true" and do not contain an AudioMark parameter; and

ii. verify that records associated with audio track files contain one AudioMark parameter with value "false" and do not contain an ImageMark parameter.

c. For the FrameSequencePlayed records corresponding to the playback of *2K FM Control Granularity - Sound Only FM (Encrypted)*:

i. Verify that records associated with image track files contain one ImageMark parameter with value "false" and do not contain an AudioMark parameter; and

ii. verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter.

d. For the FrameSequencePlayed records corresponding to the playback of *2K FM Control Granularity - Image and Sound FM (Encrypted)*:

i. Verify that records associated with image track files contain one ImageMark parameter with value "true" and do not contain an AudioMark parameter; and

ii. verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter.

Failure of any these verifications is cause to fail this test.

Note: the equipment manufacturer is required to provide a suitable FM decoder (*i.e.*, software and hardware).

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.2<br>SMPTE-430-1 |
| **Test Equipment** | **FM Detector**<br>**Accurate Real-Time Clock** |
| **Test Materials** | *2K FM Control Granularity - No FM (Encrypted)*<br>*2K FM Control Granularity - Image Only FM (Encrypted)*<br>*2K FM Control Granularity - Sound Only FM (Encrypted)*<br>*2K FM Control Granularity - Image and Sound FM (Encrypted)*<br>*KDM for 2K FM Control Granularity - No FM (Encrypted)*<br>*KDM for 2K FM Control Granularity - Image Only FM (Encrypted)*<br>*KDM for 2K FM Control Granularity - Sound Only FM (Encrypted)*<br>*KDM for 2K FM Control Granularity - Image and Sound FM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.4.3. FM Payload

### Objective

- Verify that the Forensic Marking data payload is a minimum of 35 bits, and contains both time stamp and location data.
- Verify that every 15 minutes, 24 hours per day, 366 days/year are time stamped (will repeat annually).
- Verify that 16 bits (enough values for all the possible 35,136 time stamps) are allocated for the time stamp.
- Verify that 19 bits (524,288 possible locations/serial numbers) are allocated for location (serial number) information.
- Verify that all 35 bits are included in each five minute segment.
- Verify that recovery is possible with a 30-minute content sample for positive identification.

### Procedures

1. Setup and play a show using the composition *2K FM Payload (Encrypted)*, keyed with *KDM for KDM for 2K FM Payload (Encrypted)*.
2. Play a section 30 minutes in length and use appropriate image and audio FM detectors to extract the data payload of the Forensic Marking.
3. Verify that the Forensic Marking decoder indicates that a "positive identification" has been made.

4. Verify that at least the following data is contained within both image and each of the 16 audio channels:

    a. 16 bit time stamp.

    b. 19 bit location ID.

5. Verify that two or three sequential time stamps have been recovered during the 30 minute content sample.

Failure to verify any of the above conditions shall be cause to fail this test.

To verify that all possible time stamps are generated would prove impractical, as testing would need to continue for a full calendar year. Design review is necessary to verify this assertion.

An assessment of whether all 35 bits are included in each 5 minute segments may be made if the Forensic Marking decoder is capable of providing data before "positive identification" is confirmed. This does not fully cover the objective, however, which can only be verified by design review.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.1 |
| **Test Equipment** | **FM Decoder** |
| **Test Materials** | *2K FM Payload (Encrypted)*<br>*KDM for 2K FM Payload (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 6.4.4. FM Audio Bypass

### Objective

- Verify that the Media Block does not alter the audio content essence when forensic marking is disabled using the KDM `ForensicMarkFlagList` "no FM mark" or "selective audio FM mark" commands.

### Procedures

1. Load and playback in their entirety the following CPLs using the associated KDM. For each, capture all 16 audio channels output from the Media Block using a **Digital Audio Recorder** in such a way that the captured audio signal is

bit-for-bit identical to the output audio signal.

a. *Binary Audio Forensic Marking Bypass Test (Encrypted)* and *KDM for Binary Audio Forensic Marking Test (Encrypted)*

b. *Binary Audio Forensic Marking Bypass Test (Encrypted)* and *KDM for Binary Selective Audio Forensic Marking Test (Encrypted)*

2. Using **Sound Editor** or equivalent software, verify that, for each audio channel captured in Step 1.a, the sequence of captured audio samples is bit-for-bit identical to a continuous sequence of an equal number of audio samples from the corresponding audio channel from the source sound track file. Any discrepancy is cause to fail this test.

3. Using **Sound Editor** or equivalent software, verify that, for each of audio channels 7-16 captured in Step 1.b, the sequence of captured audio samples is bit-for-bit identical to a continuous sequence of an equal number of audio samples from the corresponding audio channel from the source sound track file. Any discrepancy is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.2 |
| **Test Equipment** | **Digital Audio Recorder** |
| **Test Materials** | *Binary Audio Forensic Marking Bypass Test (Encrypted)*<br>*KDM for Binary Audio Forensic Marking Test (Encrypted)*<br>*KDM for Binary Selective Audio Forensic Marking Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.4.5. Selective Audio FM Control

### Objective

- Verify that the forensic marking "selective audio FM mark" and "no FM mark" states can be commanded by the `ForensicMarkFlagList` element of the KDM that enables playout.

- Verify that when commanded, the "no FM mark" state shall apply to the entire encrypted DCP. The "no FM mark" state shall not apply to any other DCP, even if the other DCP is part of the same showing (*i.e.*, same Show Playlist).

- Verify that if both the "no FM mark" and "selective audio FM mark" are present in the KDM used to enable the selective audio FM mark command, the "selective audio FM mark" will override the "no FM mark" command.

- Verify that only one `ForensicMarkFlagList` URI of the form `http://www.dcimovies.com/430-1/2006/KDM#mrkflg-audio-disable-above-channel-XX` (where XX is a value in the set {01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15, 16 ... 99}) is allowed in the KDM used to enable the selective audio FM mark command.

### Procedures

1. Build a show playlist out of the following four compositions, keyed with their KDMs, in the order listed

   - *Selective Audio FM - No FM (Encrypted)*, keyed with *KDM for Selective Audio FM - No FM (Encrypted)*
   - *Selective Audio FM - Not Above Channel 6 (Encrypted)*, keyed with *KDM for Selective Audio FM - Not Above Channel 6 (Encrypted)*
   - *Selective Audio FM - Not Above Channel 8 (Encrypted)*, keyed with *KDM for Selective Audio FM - Not Above Channel 8 (Encrypted)*
   - *Selective Audio FM - All FM (Encrypted)*, keyed with *KDM for Selective Audio FM - All FM (Encrypted)*

   Note: The KDM *KDM for Selective Audio FM - Not Above Channel 6 (Encrypted)* contains both a "selective audio FM mark" and a "no FM mark" URI in the `ForensicMarkFlagList`.

2. Play back the show, and present the reproduced sound to the appropriate Forensic Marking (FM) detector. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback is started.

3. Verify that the FM detectors report the following status for the presentation:

   a. *Selective Audio FM - No FM (Encrypted)*: No audio FM for any of the 16 audio channels, for the whole composition.

   b. *Selective Audio FM - Not Above Channel 6 (Encrypted)*: Audio FM present on channels 1 through 6 inclusive, and absent on channels 7 through 16 inclusive, for the whole composition.

   c. *Selective Audio FM - Not Above Channel 8 (Encrypted)*: Audio FM present on channels 1 through 8 inclusive, and absent on channels 9 through 16 inclusive, for the whole composition.

   d. *Selective Audio FM - All FM (Encrypted)*: Audio FM present, on all 16 channels, for the whole composition.

   Any discrepancy between the expected and reported FM states is cause to fail this test.

4. Extract a security log from the Test Subject that includes the range of time during which step 2 was carried out.

5. Using a**Text Editor**, locate FrameSequencePlayed records corresponding to the playback and:

   a. For the FrameSequencePlayed records corresponding to the playback of *Selective Audio FM - No FM (Encrypted)*: Verify that records associated with audio track files contain one AudioMark parameter with value "false" and do not contain an ImageMark parameter.

   b. For the FrameSequencePlayed records corresponding to the playback of *Selective Audio FM - Not Above Channel 6 (Encrypted)*: Verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter.

   c. For the FrameSequencePlayed records corresponding to the playback of *Selective Audio FM - Not Above Channel 8 (Encrypted)*: Verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter.

d. For the FrameSequencePlayed records corresponding to the playback of *Selective Audio FM - All FM (Encrypted)*: Verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter.

Failure of any these verifications is cause to fail this test.

6. Build a show playlist out of the following four compositions, keyed with their KDMs, in the order listed

- *Selective Audio FM - All FM (Encrypted)*, keyed with *KDM for Selective Audio FM - All FM (Encrypted)*
- *Selective Audio FM - Not Above Channel 10 (Encrypted)*, keyed with *KDM for Selective Audio FM - Not Above Channel 10 (Encrypted)*
- *Selective Audio FM - Not Above Channel 17 (Encrypted)*, keyed with *KDM for Selective Audio FM - Not Above Channel 17 (Encrypted)*
- *Selective Audio FM - No FM (Encrypted)*, keyed with *KDM for Selective Audio FM - No FM (Encrypted)*

Note: The KDM *KDM for Selective Audio FM - Not Above Channel 17 (Encrypted)* contains both a "selective audio FM mark" and a "no FM mark" URI in the `ForensicMarkFlagList`.

7. Play back the show, and present the reproduced sound to the appropriate Forensic Marking (FM) detector. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback is started.

8. Verify that the FM detectors report the following status for the presentation:

a. *Selective Audio FM - All FM (Encrypted)*: Audio FM present, on all 16 channels, for the whole composition.

b. *Selective Audio FM - Not Above Channel 10 (Encrypted)*: Audio FM present on channels 1 through 10 inclusive, and absent on channels 11 through 16 inclusive, for the whole composition.

c. *Selective Audio FM - Not Above Channel 17 (Encrypted)*: Audio FM present, on all 16 channels, for the whole composition.

d. *Selective Audio FM - No FM (Encrypted)*: No audio FM for any of the 16 audio channels, for the whole composition.

Any discrepancy between the expected and reported FM states is cause to fail this test.

9. Extract a security log from the Test Subject that includes the range of time during which step 7 was carried out.

10. Using a **Text Editor**, locate FrameSequencePlayed records corresponding to the playback and:

a. For the FrameSequencePlayed records corresponding to the playback of *Selective Audio FM - All FM (Encrypted)*: Verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter.

b. For the FrameSequencePlayed records corresponding to the playback of *Selective Audio FM - Not Above Channel 10 (Encrypted)*: Verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter.

c. For the FrameSequencePlayed records corresponding to the playback of *Selective Audio FM - Not Above Channel 17 (Encrypted)*: Verify that records associated with audio track files contain one AudioMark parameter with value "true" and do not contain an ImageMark parameter.

d. For the FrameSequencePlayed records corresponding to the playback of *Selective Audio FM - No FM (Encrypted)*: Verify that records associated with audio track files contain one AudioMark parameter with value "false" and do not contain an ImageMark parameter.

Failure of any these verifications is cause to fail this test.

11. Set up a show using the composition *DCI 2K StEM (Encrypted)*, keyed with the KDM *KDM with two selective audio FM mark URIs*.

12. Attempt to start playback and record the result. Successful start of playback is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.2 |
| **Test Equipment** | **FM Decoder** |
| **Test Materials** | *Selective Audio FM - No FM (Encrypted)*<br>*Selective Audio FM - All FM (Encrypted)*<br>*Selective Audio FM - Not Above Channel 6 (Encrypted)*<br>*Selective Audio FM - Not Above Channel 8 (Encrypted)*<br>*Selective Audio FM - Not Above Channel 10 (Encrypted)*<br>*Selective Audio FM - Not Above Channel 17 (Encrypted)*<br>*DCI 2K StEM (Encrypted)*<br>*KDM for Selective Audio FM - No FM (Encrypted)*<br>*KDM for Selective Audio FM - All FM (Encrypted)*<br>*KDM for Selective Audio FM - Not Above Channel 6 (Encrypted)*<br>*KDM for Selective Audio FM - Not Above Channel 8 (Encrypted)*<br>*KDM for Selective Audio FM - Not Above Channel 10 (Encrypted)*<br>*KDM for Selective Audio FM - Not Above Channel 17 (Encrypted)*<br>*KDM with two selective audio FM mark URIs* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.4.6. FM Application Constraints (OBAE)

### Objective

- Verify that FM is not applied to non-encrypted OBAE or image content.

- Verify that FM is not applied to Track Files that are not encrypted in case portions of a composition are encrypted and other portions are not.

- Verify that event log records reflect the FM state.

### Procedures

1. Play back the DCP *2K FM Application Constraints (OBAE) (Encrypted)*, keyed with *KDM for 2K FM Application Constraints (OBAE)* and present the reproduced image and OBAE-rendered audio channels to the appropriate Forensic Marking (FM) detector. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback is started. This package has a CPL that selects between encrypted and plaintext, image and OBAE track files in a specific order.

2. Verify that the FM detectors report the following status for the presentation: Note: Each segment of the presentation is approximately 35 minutes long and contains slates at the head and tail.

    a. The first segment of the presentation should indicate both image FM and OBAE FM are absent.

    b. The second segment of the presentation should indicate image FM is present and OBAE FM is absent.

    c. The third segment of the presentation should indicate image FM is absent and OBAE FM is present.

    d. The last segment of the presentation should indicate both image FM and OBAE FM are present.

    Any discrepancy between the expected and reported FM states is cause to fail this test.

3. Extract a security log from the Test Subject that includes the range of time during which step 1 was carried out.

4. Using a **Text Editor**, locate the `FrameSequencePlayed` records that correspond to the encrypted track files played during the presentation segments and:

    a. Verify there are no `FrameSequencePlayed` records corresponding to the first segment of the presentation (plaintext track files do not generate these records).

    b. Verify that `FrameSequencePlayed` records corresponding to the second segment of the presentation contain values of the `ImageMark` parameter equal to `"true"` and do not contain an `OBAEMark` parameter.

    c. Verify that `FrameSequencePlayed` records corresponding to the third segment of the presentation contain values of the `OBAEMark` parameter equal to `"true"` and do not contain an `ImageMark` parameter.

    d. For the `FrameSequencePlayed` records corresponding to the last segment of the presentation:

        i. Verify that records associated with image track files contain one `ImageMark` parameter with value `"true"` and do not contain an `OBAEMark` parameter; and

        ii. verify that records associated with OBAE track files contain one `OBAEMark` parameter with value `"true"` and do not contain an `ImageMark` parameter

    Failure of any these verifications is cause to fail this test.

Note: the equipment manufacturer is required to provide a suitable FM decoder (*i.e.*, software and hardware).

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.2, 9.4.6.3.8<br>[OBAE-ADD] |
| **Test Equipment** | **FM Detector**<br>**Accurate Real-Time Clock** |
| **Test Materials** | *2K FM Application Constraints (OBAE) (Encrypted)*<br>*KDM for 2K FM Application Constraints (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.4.7. Granularity of FM Control (OBAE)

### Objective

- Verify that the `ForensicMarkFlagList` element of the KDM:
  - controls the application of forensic marking independently for OBAE and image essence kinds;
  - applies to the entire composition; and
  - applies exclusively to the Composition targeted by the KDM and no other composition, even if the other composition is part of the same show (*i.e.*, same Show Playlist).
- Verify that event log records reflect the application of the `ForensicMarkFlagList` element of the KDM.

### Procedures

1. Build a show playlist out of the following four compositions, in the order listed:
    1. *2K FM Control Granularity - No FM (OBAE) (Encrypted)*, keyed with *KDM for 2K FM Control Granularity - No FM (OBAE)*.
    2. *2K FM Control Granularity - Image Only FM (OBAE) (Encrypted)*, keyed with *KDM for 2K FM Control Granularity - Image Only FM (OBAE)*.
    3. *2K FM Control Granularity - OBAE Only FM (OBAE) (Encrypted)*, keyed with *KDM for 2K FM Control Granularity - OBAE Only FM (OBAE)*.
    4. *2K FM Control Granularity - Image and OBAE FM (OBAE) (Encrypted)*, keyed with *KDM for 2K FM Control Granularity - Image and OBAE FM (OBAE)*.

2. Play back the show, and present the reproduced image and all OBAE-rendered audio channels to the appropriate Forensic Marking (FM) detector. With an **Accurate Real-Time Clock**, note the UTC time at the moment playback is started.

3. Verify that the FM detectors report the following status for the presentation:

    a. *2K FM Control Granularity - No FM (OBAE) (Encrypted)*: No image FM and no OBAE FM for the whole composition.

    b. *2K FM Control Granularity - Image Only FM (OBAE) (Encrypted)*: Image FM present, but no OBAE FM, for the whole composition.

    c. *2K FM Control Granularity - OBAE Only FM (OBAE) (Encrypted)*: No image FM, but OBAE FM present, for the whole composition.

    d. *2K FM Control Granularity - Image and OBAE FM (OBAE) (Encrypted)*: Image FM and OBAE FM present for the whole composition.

    Any discrepancy between the expected and reported FM states is cause to fail this test.

4. Extract a security log from the Test Subject that includes the range of time during which step 2 was carried out.

5. Using a **Text Editor**, locate `FrameSequencePlayed` records corresponding to the playback and:

    a. For the `FrameSequencePlayed` records corresponding to the playback of *2K FM Control Granularity - No FM (OBAE) (Encrypted)*:

        i. Verify that records associated with image track files contain one `ImageMark` parameter with value `"false"` and do not contain an `OBAEMark` parameter; and

        ii. verify that records associated with OBAE track files contain one `OBAEMark` parameter with value `"false"` and do not contain an `ImageMark` parameter.

    b. For the `FrameSequencePlayed` records corresponding to the playback of *2K FM Control Granularity - Image Only FM (OBAE) (Encrypted)*:

        i. Verify that records associated with image track files contain one `ImageMark` parameter with value `"true"` and do not contain an `OBAEMark` parameter; and

        ii. verify that records associated with OBAE track files contain one `OBAEMark` parameter with value `"false"` and do not contain an `ImageMark` parameter.

    c. For the `FrameSequencePlayed` records corresponding to the playback of *2K FM Control Granularity - OBAE Only FM (OBAE) (Encrypted)*:

        i. Verify that records associated with image track files contain one `ImageMark` parameter with value `"false"` and do not contain an `OBAEMark` parameter; and

        ii. verify that records associated with OBAE track files contain one `OBAEMark` parameter with value `"true"` and do not contain an `ImageMark` parameter.

d. For the `FrameSequencePlayed` records corresponding to the playback of *2K FM Control Granularity - Image and OBAE FM (OBAE) (Encrypted)*:

i. Verify that records associated with image track files contain one `ImageMark` parameter with value `"true"` and do not contain an `OBAEMark` parameter; and

ii. verify that records associated with OBAE track files contain one `OBAEMark` parameter with value `"true"` and do not contain an `ImageMark` parameter.

Failure of any these verifications is cause to fail this test.

Note: the equipment manufacturer is required to provide a suitable FM decoder (*i.e.*, software and hardware).

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.2, 9.4.6.3.8<br>SMPTE-430-1<br>[OBAE-ADD] |
| **Test Equipment** | **FM Detector**<br>**Accurate Real-Time Clock** |
| **Test Materials** | *2K FM Control Granularity - No FM (OBAE) (Encrypted)*<br>*2K FM Control Granularity - Image Only FM (OBAE) (Encrypted)*<br>*2K FM Control Granularity - OBAE Only FM (OBAE) (Encrypted)*<br>*2K FM Control Granularity - Image and OBAE FM (OBAE) (Encrypted)*<br>*KDM for 2K FM Control Granularity - No FM (OBAE)*<br>*KDM for 2K FM Control Granularity - Image Only FM (OBAE)*<br>*KDM for 2K FM Control Granularity - OBAE Only FM (OBAE)*<br>*KDM for 2K FM Control Granularity - Image and OBAE FM (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.4.8. FM Payload (OBAE)

### Objective

- Verify that the Forensic Marking data payload for OBAE essence is a minimum of 35 bits, and contains both time stamp and location data.
- Verify that every 15 minutes, 24 hours per day, 366 days/year are time stamped (will repeat annually).
- Verify that 16 bits (enough values for all the possible 35,136 time stamps) are allocated for the time stamp.
- Verify that 19 bits (524,288 possible locations/serial numbers) are allocated for location (serial number) information.

- Verify that all 35 bits are included in each five minute segment.
- Verify that recovery is possible with a 30-minute content sample for positive identification.
- Verify that recovery is possible with a range of OBAE rendering configurations.

### Procedures

Perform the following steps:

1. Setup a show using the composition *2K FM Payload (OBAE) (Encrypted)*, keyed with *KDM for 2K FM Payload (OBAE) (Encrypted)*.
2. Setup the Test Subject with the maximum number of rendered channels supported by the system.
3. Perform the following steps:
    a. Play a section 30 minutes in length and use appropriate OBAE FM detectors to extract the data payload of the Forensic Marking.
    b. Verify that the Forensic Marking decoder indicates that a "positive identification" has been made.
    c. Verify that at least the following data is contained within each of the rendered audio channels:
        - 16 bit time stamp.
        - 19 bit location ID.
    d. Verify that two or three sequential time stamps have been recovered during the 30 minute content sample.

Failure to verify any of the above conditions shall be cause to fail this test.

**Note:**
To verify that all possible time stamps are generated would prove impractical, as testing would need to continue for a full calendar year. Design review is necessary to verify this assertion.

**Note:**
An assessment of whether all 35 bits are included in each 5 minute segments may be made if the Forensic Marking decoder is capable of providing data before "positive identification" is confirmed. This does not fully cover the objective, however, which can only be verified by design review.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.1<br>[OBAE-ADD] |
| **Test Equipment** | **FM Decoder** |
| **Test Materials** | *2K FM Payload (OBAE) (Encrypted)*<br>*KDM for 2K FM Payload (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |

## 6.4.9. FM Audio Bypass (OBAE)

### Objective

Verify that the Media Block does not alter the OBAE content essence when forensic marking is disabled using the KDM `ForensicMarkFlagList` "no FM mark" commands.

### Procedures

1. Setup the Test Subject with the maximum number of rendered channels supported by the system.

2. Load and playback in their entirety the following CPLs using the associated KDM. For each, capture all rendered channels output from the Media Block using a **Digital Audio Recorder** in such a way that the captured audio signal is bit-for-bit identical to the output audio signal.

    a. *2K FM Payload (OBAE) (Encrypted)* and *KDM for 2K FM Payload (OBAE) with FM Bypass (Encrypted)*, where forensic marking application to the OBAE essence is disabled using the "no FM mark" flag; and

    b. *2K FM Payload (plaintext OBAE) (Encrypted)* and *KDM for 2K FM Payload (plaintext OBAE) (Encrypted)*, where forensic marking is not applied to the OBAE essence since it is plaintext.

3. Using **Sound Editor** or equivalent software, verify that, for each audio channel captured in Step 2, the sequence of captured audio samples is bit-for-bit identical between Steps 2.a and 2.b. Any discrepancy is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.2<br>[OBAE-ADD] |
| **Test Equipment** | **Digital Audio Recorder**<br>**Sound Editor** |
| **Test Materials** | *2K FM Payload (OBAE) (Encrypted)*<br>*KDM for 2K FM Payload (OBAE) with FM Bypass (Encrypted)*<br>*2K FM Payload (plaintext OBAE) (Encrypted)*<br>*KDM for 2K FM Payload (plaintext OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

# 6.5. Image Reproduction

## 6.5.1. Playback of Image Only Material

### Objective

Verify that all projection systems are capable of playing back content that consists of image only, *i.e.*, has no corresponding audio or other track.

### Procedures

Play back the DCP *DCI NIST Frame no sound files*. This package comprises image only. Verify that the image is displayed correctly. Failure to display the image is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.3.1.3 |
| **Test Materials** | *DCI NIST Frame no sound files* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.5.2. Decoder Requirements

### Objective

- Verify that the image decoder meets all requirements for JPEG 2000 image decoder presented in [DCI-DCSS], Section 4.3.2
- Verify that the decoder decodes each color component at 12 bits per sample, with equal color/component bandwidth, and does not subsample chroma (*i.e.*, does not generate any 4:2:2 signal or similar), except as permitted by [DCI-DCSS], Section 2.1.1.4
- For 2K decoders, verify that it shall decode 2K data for every frame in a 4K distribution.
- For 4K decoders, verify that it shall decode 4K data for every frame in a 4K distribution.

### Procedures

1. Verify that the decoder output conforms to the following image specifications:

    a. 2K = 2048 x 1080 at 24 fps

    b. 2K = 2048 x 1080 at 48 fps

    c. 4K = 4096 x 2160 at 24 fps

    To verify this, build and play a single show containing the compositions *DCI 2K Sync Test* (2K@24fps), *DCI 2K Sync Test (48fps)* (2K@48fps) and *4K Sync Test* (4K@24fps). Verify that playback is successful and that image and audio are properly reproduced as described below.
    The test images used in the referenced compositions are similar for each of the 2K and 4K variants. In many cases, the features as they appear in the 2K image are simply scaled to create the 4K image. The description of the features of the 2k variant follows. Note that failure language declared in the 2k variant description will be modified later in this procedure to describe compliant display of the image on 24 fps 4K and 48 fps 2K displays.
    In the image descriptions that follow, the term "source pixel" is used to define the respective image feature in terms of the input signal. The display may have a different resolution than the image, in which case a given input -- the source pixel -- may be mapped to some number of display pixels other than one, and may also contribute to shading on adjacent pixels. For example, a line that is one source pixel in width in the 2K image should appear two pixels in witdh on a 4K display. Similarly, a line that is one source pixel in width in the 4K image will likely appear diminished -- perhaps significantly -- on a 2K display, and will perhaps not be centered on a particular line of the display's pixels.

        i. For the *DCI 2K Sync Test* composition (2K@24fps), locate and confirm the appearance of the following features of the test image:

            A. A yellow reticle defines the area of the 1:1.85 aspect ratio (1998 x 1080). The lines comprising the reticle are one source pixel in width. Small, outward facing arrows of matching color indicate the reticle position for the case where some occlusion prevents display of the horizontal lines (*i.e.*, the top-most or bottommost lines of the image.) Failure to display the full reticle shall be cause to fail the test.

            B. A green reticle defines the area of the 1:2.39 aspect ratio (2048 x 858). The lines comprising the reticle are one source pixel in width. Small, outward facing arrows of matching color indicate the reticle position for the case where some occlusion prevents display of the vertical lines (*i.e.*, the left-most or right-most lines of the image.) Failure to display the full reticle shall be cause to fail the test.

            C. A non-antialiased circle is placed in the center of the image. The source pixels comprising the circle are either ref-white or background-gray. The circle should appear to have equal height and width. Distortion of the circle geometry shall be cause to fail the test.

            D. To the left of the circle are six patches, in two rows of three. From left to right, top to bottom, the patches are designated P1, P2, P3, P4, P5, P6. (See Figure 6.1. below for a graphical definition of the panel designations.)

                a. Pattern P1 is a pair of grayscale concentric squares having two different luminances. The outer square is dark gray (12-bit X'Y'Z' code values 122,128,125). The inner square is absolute black (12-bit X'Y'Z' code values 0,0,0).

                b. Pattern P2 is a set of sixty (60) horizontal lines, each line being one source pixel in height, alternating red-green-blue, from top to bottom. Failure to display the correct colors and number of lines shall be cause to fail the test.

c. Pattern P3 is a set of thirty (30) horizontal lines, each line being two source pixels in height, alternating red-green-blue, from top to bottom. Failure to display the correct colors and number of lines shall be cause to fail the test.

d. Pattern P4 is a 60 x 60 "checkerboard" array of black and white areas. The size of each black or white area is one source pixel. Failure to display the pattern with uniform color, contrast and area size shall be cause to fail the test.

e. Pattern P5 is a set of sixty (60) vertical lines, each line being one source pixel in width, alternating red-green-blue, from left to right. Failure to display the correct colors and number of lines shall be cause to fail the test.

f. Pattern P6 is a set of thirty (30) vertical lines, each line being two source pixels in width, alternating red-green-blue, from left to right. Failure to display the correct colors and number of lines shall be cause to fail the test.

E. To the right of the circle are six patches, in two rows of three. From left to right, top to bottom, the patches are designated P7, P8, P9, P10, P11, P12.

a. Pattern P7 is a set of thirty (30) horizontal lines, each line being two source pixels in height, alternating black-white, from top to bottom. Failure to display the correct colors and number of lines shall be cause to fail the test.

b. Pattern P8 is a set of sixty (60) horizontal lines, each line being one source pixel in height, alternating black-white, from top to bottom. Failure to display the correct colors and number of lines shall be cause to fail the test.

c. Pattern P9 is a pair of grayscale concentric squares having two different luminances. The outer square is reference white (12-bit X'Y'Z' code values (3794, 3960, 3890)). The inner square is absolute white (12-bit X'Y'Z' code values (4095,4095,4095)). Note that the square having absolute white color will have red hue.

d. Pattern P10 is a set of thirty (30) vertical lines, each line being two source pixels in width, alternating black-white, from left to right. Failure to display the correct colors and number of lines shall be cause to fail the test.

e. Pattern P11 is a set of sixty (60) vertical lines, each line being one source pixel in width, alternating black-white, from left to right. Failure to display the correct colors and number of lines shall be cause to fail the test.

f. Pattern P12 is a 30 x 30 "checkerboard" array of black and white areas. The size of each black or white area is two source pixels square. Failure to display the pattern with uniform color and area size shall be cause to fail the test.

F. Below the circle is a set of twenty (20) rectangular grayscale patches, in two centered horizontal rows of ten (10) patches each. Each patch has a distinct luminance, which are defined in [SMPTE-431-2]. No two adjacent patches should appear to have the same luminance. Failure to display twenty distinct patches shall be cause to fail the test.

ii. For the *4K Sync Test* composition (4K@24fps), locate and confirm the appearance of the features of the test image as described for the *DCI 2K Sync Test* composition, with the following exceptions:

A. Pattern P2 is a set of one hundred twenty (120) horizontal lines, each line being one source pixel in height, alternating red-green-blue, From top to bottom. When displayed on a 2K display, no pass/fail criteria shall be applied. Failure to display the correct colors and number of lines shall be cause to fail the test.

B. Pattern P3 is a set of sixty (60) horizontal lines, each line being two source pixels in height, alternating red-green-blue, From top to bottom. When displayed on a 2K display, this feature will appear as pattern P2 in the 2K test frame. Failure to display the correct colors and number of lines shall be cause to fail the test.

C. Pattern P4 is a 120 x 120 "checkerboard" array of black and white areas. The size of each black or white area is one source pixel. When displayed on a 2K display, this feature will appear as a unform (but perhaps variegated) gray field. Failure to display the pattern with uniform color, contrast and area size shall be cause to fail the test.

D. Pattern P5 is a set of one hundred twenty (120) vertical lines, each line being one source pixel in width, alternating red-green-blue, From left to right. When displayed on a 2K display, no pass/fail criteria shall be applied. Failure to display the correct colors and number of lines shall be cause to fail the test.

E. Pattern P6 is a set of sixty (60) vertical lines, each line being two source pixels in width, alternating redgreen- blue, from left to right. When displayed on a 2K display, this feature will appear as pattern P5 in the 2K test frame. Failure to display the correct colors and number of lines shall be cause to fail the test.

F. Pattern P7 is a set of sixty (60) horizontal lines, each line being two source pixels in height, alternating black-white, from top to bottom. When displayed on a 2K display, this feature will appear as pattern P8 in the 2K test frame. Failure to display the correct colors and number of lines shall be cause to fail the test.

G. Pattern P8 is a set of one hundred twenty (120) horizontal lines, each line being one source pixel in height, alternating black-white, from top to bottom. When displayed on a 2K display, no pass/fail criteria shall be applied. Failure to display the correct colors and number of lines shall be cause to fail the test.

H. Pattern P10 is a set of sixty (60) vertical lines, each line being two source pixels in width, alternating black- white, from left to right. When displayed on a 2K display, this feature will appear as pattern P11 in the 2K test frame. Failure to display the correct colors and number of lines shall be cause to fail the test.

I. Pattern P11 is a set of one hundred twenty (120) vertical lines, each line being one source pixel in width, alternating black-white, from left to right. When displayed on a 2K display, no pass/fail criteria shall be applied. Failure to display the correct colors and number of lines shall be cause to fail the test.

J. Pattern P12 is a 60 x 60 "checkerboard" array of black and white areas. The size of each black or white area is two source pixels square. Failure to display the pattern with uniform color and area size shall be cause to fail the test.

iii. For the *DCI 2K Sync Test* (48fps) composition (2K@48fps), locate and confirm the appearance of the features of the test image as described for the *DCI 2K Sync Test* composition, with the following exceptions:

A. In the case where the MB provides image data to the projector via dual 1.5 Gb/s (or single 3 Gb/s) SDI link, [DCI-DCSS], Section 2.1.1.4 allows chroma subsampling on 48 fps images (*i.e.* 4:2:2). In

this case, patch P5 of the 2K test image is expected to be displayed with chroma blending. Patch P3 may display chroma blending, depending on the coincidence of the 2X horizontal source pixels and the subsampling algorithm. Patch P6 is expected to be reproduced discretely, with no visible chroma blending. No blending shall be visible for any of the patches P7, P8, P10 and P11. The number of lines displayed in patterns P7 and P10 shall be thirty (30). The number of lines displayed in patterns P8 and P11 shall be sixty (60). Failure to display the correct number of lines in each of the panels P7, P8, P10 and P11 shall be cause to fail the test. Appearance of chroma blending deviating from the above shall be cause to fail the test.

2. Verify that the decoder outputs 12-bit X'Y'Z' color:

    a. To test for 12 bit color reproduction play back the composition *DCI 2K Moving Gradient*. This clip contains a special moving pattern to reveal usage of all 12 bits. The pattern contains three vertical bands, each 250 horizontal pixels in width, corresponding to 12, 11 and 10 bit representations of a sine wave that advances in value by 1 degree per pixel. The bands are labeled with the 12 bit region on the left, 11 bit region in the center and 10 bit region on the right of the screen. Examine the image for artifacts such as contouring or vertical striations. Any such noticeable artifacts in the 12 bit region of the pattern is cause to fail this test. The 11 and 10 bit regions are provided for reference.

3. To test for X'Y'Z' color reproduction: Using a **DCI Projector**, properly calibrated for Luminance and Color Calibration and a **Spectroradiometer**, perform the following steps:

    a. For each of the 12 Color Accuracy color patch code values referenced in [SMPTE-431-2], Table A.4, display the given X'Y'Z' code values. This may be achieved by displaying a suitable test file or by delivering the appropriate signal to an external interface (*e.g.* Dual-Link HD-SDI). Measure and record the displayed Luminance and Color Coordinates for each of the Color Accuracy patches.

    b. Play back the composition *Color Accuracy Series* and measure and record the displayed Luminance and Color Coordinates for each of the Color Accuracy patches.

    c. For each of the the corresponding reference and decoded values recorded in steps i and ii, calculate the x and y delta values and record them.

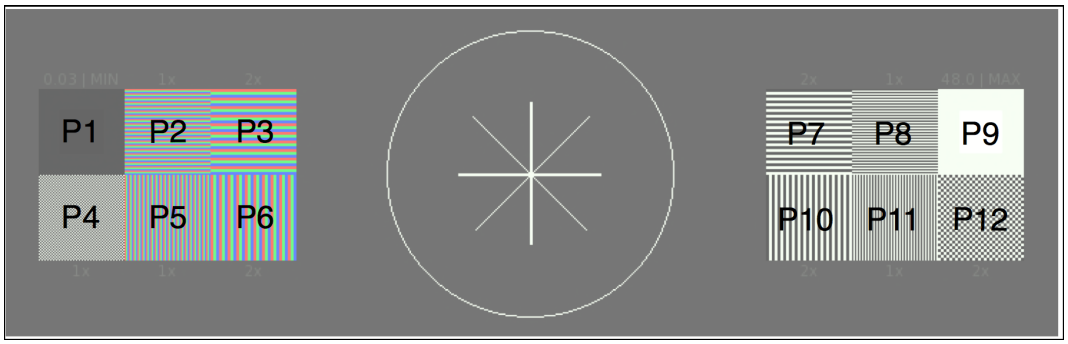
    If any of the values recorded in step iii exceed the tolerances defined in [SMPTE-431-2], Table A, Section 7.9 this is cause to fail this test.

4. For 4K decoders, verify that it shall decode 4K data for every frame in a 4K distribution, or for 2K decoders, verify that it shall decode 2K data for every frame in a 4K distribution. To test this perform the following procedure:

    a. Play back the composition *2K DCI Maximum Bitrate Composition (Encrypted)*, keyed with *KDM for 2K Maximum Bitrate Composition (Encrypted)*. This composition contains a codestream at the maximum allowable bitrate of an image with a burned in counter, incremented by one with every frame. The projected image must be filmed with a suitable camera and then be viewed in slow motion to verify that no counter numbers are skipped. Failure to observe all the numbered frames shall be cause to fail this test. Verify that the projected image contains a clearly visible, regular pattern that does not change over time (except for the burned in counter). If any other artifacts are noted (*e.g.* flickering or similar) this is cause to fail this test.

    b. Play back the composition *4K DCI Maximum Bitrate Composition (Encrypted)*, keyed with *KDM for 4K Maximum Bitrate Composition (Encrypted)*. This composition contains a codestream at the maximum allowable bitrate of an image with a burned in counter, incremented by one with every frame. The projected image must be filmed with a suitable camera and then be viewed in slow motion to verify that no counter numbers are skipped. Failure to observe all the numbered frames shall be cause to fail this test. Verify that the projected image contains a clearly visible, regular pattern that does not change over time (except for the burned in counter). If any other artifacts are noted (*e.g.* flickering or similar) this is cause to fail this test.

### Figure 6.1. Standard Frame Panel Designations




#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 4.3.2, 2.1.1.4<br>SMPTE-428-1<br>SMPTE-430-2 |
| **Test Equipment** | **48 fps Camera** |
| **Test Materials** | *DCI 2K Sync Test*<br>*DCI 2K Sync Test (48fps)*<br>*4K Sync Test*<br>*DCI 2K Moving Gradient*<br>*Color Accuracy Series*<br>*2K DCI Maximum Bitrate Composition (Encrypted)*<br>*4K DCI Maximum Bitrate Composition (Encrypted)*<br>*KDM for 2K Maximum Bitrate Composition (Encrypted)*<br>*KDM for 4K Maximum Bitrate Composition (Encrypted)* |

#### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.6. Audio Reproduction

### 6.6.1. Digital Audio Interfaces

#### Objective

Verify that the Media Block has a digital audio output interface with the capacity for delivering 16 channels of digital audio at 24-bit 48 kHz or (optionally) 96 kHz, and follows the [AES3-2003] recommended practice for serial transmission format for

two-channel linearly represented digital audio data.

### Procedures

1. Play the composition *DCI 1-16 Numbered Channel Identification* which contains spoken identification for each of the 16 audio channels and verify correct output. Failure to confirm correct reproduction on any channel is cause to fail this test.

2. Play the composition *DCI NIST Frame with Pink Noise* which contains 16 channels of Pink Noise at 48kHz sample rate and verify:

    a. 48kHz AES3 signal at all outputs.

    b. Pink noise bandwidth to 22kHz.

    c. 24 active bits on analyzer.
    Failure to confirm above conditions a, b and c, is cause to fail this test.

3. If the Test Subject supports playback of 96 kHz audio, play the composition *DCI NIST Frame with Pink Noise (96 kHz)* which contains 16 channels of Pink Noise at 96kHz sample rate and verify:

    a. 96kHz AES3 signal at all outputs.

    b. Pink noise bandwidth to 44kHz.

    c. 24 active bits on analyzer.

    Failure to confirm above conditions a, b and c, is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | AES3-2003<br>DCI-DCSS, 7.5.4.3, 7.5.6.1, 7.5.6.2 |
| **Test Equipment** | **AES3 Audio Analyzer** |
| **Test Materials** | *DCI 1-16 Numbered Channel Identification*<br>*DCI NIST Frame with Pink Noise*<br>*DCI NIST Frame with Pink Noise (96 kHz)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.6.2. Audio Sample Rate Conversion

### Objective

If it supports playback of 96 kHz audio, verify that the Test Subject has the capability of performing Sample Rate Conversion (SRC) when needed.

### Procedures

*Only applies to a Test Subject that supports playback of 96 kHz audio.*

1. Play back the DCP *DCI NIST Frame with 1 kHz tone (-20 dB fs, 96kHz)*. Enable SRC on the system, select an output rate of 48kHz. With an AES analyzer, confirm that each of the AES-3 outputs are producing an AES signal with a 48kHz sample rate. Any other measured output sample rate is cause to fail this test.

2. Play back the DCP *DCI NIST Frame with 1 kHz tone (-20 dB fs)*. Enable SRC on the system, select an output rate of 96kHz. With an AES analyzer, confirm that each of the AES-3 outputs are producing an AES signal with a 96kHz sample rate. Any other measured output sample rate is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 3.3.2.1 |
| **Test Equipment** | **AES3 Audio Analyzer** |
| **Test Materials** | *DCI NIST Frame with 1 kHz tone (-20 dB fs)*<br>*DCI NIST Frame with 1 kHz tone (-20 dB fs, 96kHz)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.6.3. Audio Delay Setup

### Objective

Verify that the system provides a method for adjusting the delay of the audio signal relative to the image. It must be possible to offset audio +/-200 ms in 10 ms increments.

### Procedures

1. Connect channel 1 of the oscilloscope to the analog center channel output of the sound equipment.

2. Connect channel 2 of the oscilloscope to a photodiode that is placed in front of the projection screen, where the flashing rectangle is located.

3. Perform the following steps:

a. Play back the composition *DCI 2K Sync Test*. This composition contains short beeps (one frame in length) and a white flashing rectangle at the bottom of the screen, synchronized to the beeps.

b. Measure the delay between the light pulse and the audio pulse. This will depend on a combination of many factors such as the image processing delay of the display device, sound processing delay in the sound equipment, and digital signal transmission delays (buffering of data). Record the timing with zero offset applied to the unit under test. Use this nominal figure as the reference point for the following steps.

c. Set the offset to -200 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure minus 200 ms. Failure to meet this requirement is cause to fail this test.

d. Set the offset to +200 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure plus 200 ms. Failure to meet this requirement is cause to fail this test.

e. Set the offset to -190 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure minus 190 ms. Failure to meet this requirement is cause to fail this test.

f. Set the offset to +190 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure plus 190 ms. Failure to meet this requirement is cause to fail this test.

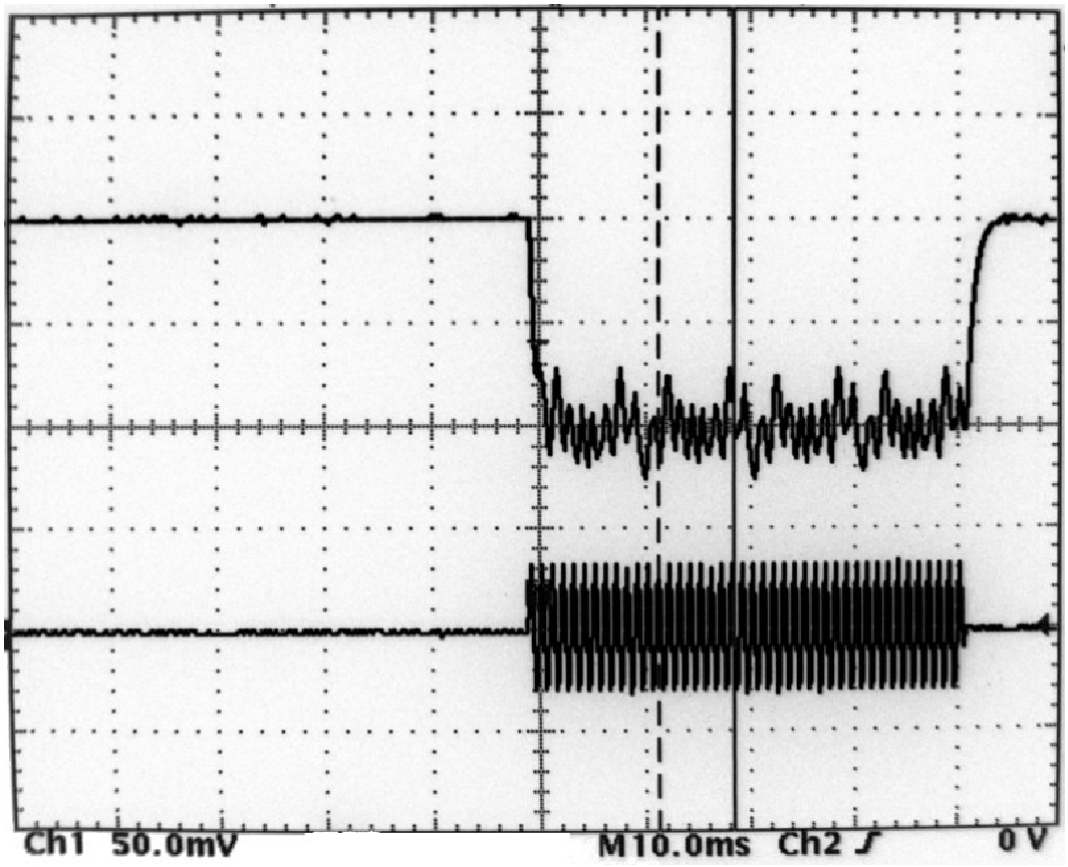
g. Set the offset to -10 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure minus 10 ms. Failure to meet this requirement is cause to fail this test.

h. Set the offset to +10 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure plus 10 ms. Failure to meet this requirement is cause to fail this test.

4. Repeat the above test, but this time for 48 fps (use the composition *DCI 2K Sync Test (48fps)*). Record the results obtained.

The image below shows what a typical measurement is expected to look like. The upper trace shows the light output of the projector, measured by means of the photo diode. The photo diode signal is shown inverted, *i.e.*, low means high light output. The lower trace shows the analog center channel output of the Media Block after D/A conversion from the AES-EBU signal.

## Figure 6.2. Audio Delay Timing




Warning: the optical flashes generated during this test can cause physiological reactions in some people. People who are sensitive to such optical stimuli should not view the test material.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.4.1.8 |
| **Test Equipment** | **Oscilloscope**<br>**Photodiode** |
| **Test Materials** | *DCI 2K Sync Test*<br>*DCI 2K Sync Test (48fps)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.6.4. Click Free Splicing of Audio Track Files

### Objective

Verify that the playback system allows click free splicing of the audio track files.

> **Note:**
> Note: Playback of this test must be done in a properly equipped and set up movie theater, at reference level, *i.e.*, fader setting 7.0 for Dolby and compatibles or fader setting 0 dB for Sony and compatibles. A single channel of pink noise at -20dBFS should produce a Sound Pressure Level (SPL) of 85dBc, from any of the front loudspeakers, at the monitoring position. Monitoring by means of smaller monitor boxes or headphones is not sufficient.

### Procedures

Play back *DCP for Audio Tone Multi-Reel (Encrypted)*, which contains a sequence of audio track files arranged such that no discontinuity exists at the splice points.

Any audible snap, crackle, pop or other unpleasant artifact at any splice point shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.3.1.6 |
| **Test Equipment** | **Sound System** |
| **Test Materials** | *DCP for Audio Tone Multi-Reel (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

# 6.7. Timed Text Reproduction

## 6.7.1. Media Block Overlay

### Objective

In the case that the Media Block implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel), verify that assets are rendered and displayed correctly by the system.

### Procedures

1. Using a digital cinema projector that does not provide an internal subtitle rendering capability (or one in which subtitle rendering capability is disabled), load and play back each of the compositions:

a. *2K Scope Subtitle Test (Encrypted)*, keyed with *KDM for 2K Scope Subtitle Test (Encrypted)*.

b. *2K Flat Subtitle Test (Encrypted)*, keyed with *KDM for 2K Flat Subtitle Test (Encrypted)*.

c. *2K Full Subtitle Test (Encrypted)*, keyed with *KDM for 2K Full Subtitle Test (Encrypted)*.

d. *4K Scope Subtitle Test (Encrypted)*, keyed with *KDM for 4K Scope Subtitle Test (Encrypted)*.

e. *4K Flat Subtitle Test (Encrypted)*, keyed with *KDM for 4K Flat Subtitle Test (Encrypted)*.

f. *4K Full Subtitle Test (Encrypted)*, keyed with *KDM for 4K Full Subtitle Test (Encrypted)*.

g. *2K 48fps Scope Subtitle Test (Encrypted)*, keyed with *KDM for 2K 48fps Scope Subtitle Test (Encrypted)*.

h. *2K 48fps Flat Subtitle Test (Encrypted)*, keyed with *KDM for 2K 48fps Flat Subtitle Test (Encrypted)*.

i. *2K 48fps Full Subtitle Test (Encrypted)*, keyed with *KDM for 2K 48fps Full Subtitle Test (Encrypted)*.

2. Refer to Appendix I and for each scene in each composition, record the state of compliance with the basic and specific pass/fail criteria listed therein. Failure of any compliance criterion is cause to fail this test.

## Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.5.4.2.5, 7.5.4.2.6, 7.5.4.2.7<br>SMPTE-429-2 |
| **Test Equipment** | **DCI Projector** |
| **Test Materials** | *2K Scope Subtitle Test (Encrypted)*<br>*2K Flat Subtitle Test (Encrypted)*<br>*2K Full Subtitle Test (Encrypted)*<br>*4K Scope Subtitle Test (Encrypted)*<br>*4K Flat Subtitle Test (Encrypted)*<br>*4K Full Subtitle Test (Encrypted)*<br>*2K 48fps Scope Subtitle Test (Encrypted)*<br>*2K 48fps Flat Subtitle Test (Encrypted)*<br>*2K 48fps Full Subtitle Test (Encrypted)*<br>*KDM for 2K Scope Subtitle Test (Encrypted)*<br>*KDM for 2K Flat Subtitle Test (Encrypted)*<br>*KDM for 2K Full Subtitle Test (Encrypted)*<br>*KDM for 4K Scope Subtitle Test (Encrypted)*<br>*KDM for 4K Flat Subtitle Test (Encrypted)*<br>*KDM for 4K Full Subtitle Test (Encrypted)*<br>*KDM for 2K 48fps Scope Subtitle Test (Encrypted)*<br>*KDM for 2K 48fps Flat Subtitle Test (Encrypted)*<br>*KDM for 2K 48fps Full Subtitle Test (Encrypted)* |

## Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband | |

| | | | |
|---|---|---|---|
| image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — | | |
| 15.2. Projector with MB Test Sequence | Pass/Fail | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |

## 6.7.2. Deleted Section

The section "Timed Text Synchronization" was deleted. The section number is maintained here to preserve the numbering of subsequent sections

## 6.7.3. Deleted Section

The section "Support for Multiple Captions" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 6.7.4. Default Timed Text Font

### Objective

Verify that a timed-text rendering system provides a default font to be used in the case where no font files are supplied with the DCP.

### Procedures

1. Load and play the composition *DCI Malformed Test 8: DCP with timed text and a missing font*.

2. Verify that the timed text instances contain multiple lines of text.

3. Failure to correctly display multiple lines of text shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 3.4.3<br>SMPTE-428-7 |

| | |
|---|---|
| SMPTE-429-5 | **Test Materials** |
| *DCI Malformed Test 8: DCP with timed text and a missing font* | |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |
| 14.2. Projector Test Sequence | Pass/Fail | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.7.5. Deleted Section

The section "Support for Subpicture Display" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 6.7.6. Timed Text Decryption

### Objective

Verify that an SM can play a composition that contains encrypted timed text essence.

### Procedures

1. Load the composition *DCI 2K Sync test with Subtitles (Encrypted)* and KDM *KDM for DCI 2K Sync Test with Subtitles (Encrypted)*.

2. Play the composition *DCI 2K Sync test with Subtitles (Encrypted)*.

3. Verify that the timed text appears on screen as indicated by the main picture.

4. Failure to correctly display multiple lines of text shall be cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.7.2, 9.4.3.6.3, 9.4.3.5<br>SMPTE-428-7<br>SMPTE-429-5 |
| **Test Materials** | *DCI 2K Sync test with Subtitles (Encrypted)*<br>*KDM for DCI 2K Sync Test with Subtitles (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

# 6.8. OBAE Reproduction

## 6.8.1. Click Free Splicing of OBAE Track Files

### Objective

Verify that the playback system allows click free splicing of OBAE track files.

> **Note:**
> Playback of this test must be done in a theatrical environment calibrated and setup for OBAE reproduction. Monitoring by means of smaller monitor boxes or headphones is not sufficient.

### Procedures

1. Setup the **OBAE Sound System** with the maximum number of rendered channels supported by the system.

2. Play back *DCP for OBAE Tone Multi-Reel (Encrypted)*, which contains a sequence of OBAE Track Files arranged such that no discontinuity exists at the splice points.

Any audible snap, crackle, pop or other unpleasant artifact at any splice point shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 5.3.1.6<br>[OBAE-ADD] |
| **Test Equipment** | **OBAE Sound System** |
| **Test Materials** | *DCP for OBAE Tone Multi-Reel (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.8.2. OBAE Delay Setup

### Objective

Verify that the system provides a method for adjusting the delay of rendered OBAE essence relative to the image. It must be possible to offset audio +/-200 ms in 10 ms increments.

### Procedures

1. Connect channel 1 of the oscilloscope to the analog center channel output of the sound equipment.

2. Connect channel 2 of the oscilloscope to a photodiode that is placed in front of the projection screen, where the flashing rectangle is located.

3. Perform the following steps:

    a. Play back the composition *DCI 2K Sync Test (OBAE)*. This composition contains short beeps (one frame in length) and a white flashing rectangle at the bottom of the screen, synchronized to the beeps.

    b. Measure the delay between the light pulse and the audio pulse. This will depend on a combination of many factors such as the image processing delay of the display device, sound processing delay in the sound equipment, and digital signal transmission delays (buffering of data). Record the timing with zero offset applied to the unit under test. Use this nominal figure as the reference point for the following steps.

    c. Set the offset to -200 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure minus 200 ms. Failure to meet this requirement is cause to fail this test.

    d. Set the offset to +200 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure plus 200 ms. Failure to meet this requirement is cause to fail this test.

    e. Set the offset to -190 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure minus 190 ms. Failure to meet this requirement is cause to fail this test.

    f. Set the offset to +190 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure plus 190 ms. Failure to meet this requirement is cause to fail this test.

    g. Set the offset to -10 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure minus 10 ms. Failure to meet this requirement is cause to fail this test.

    h. Set the offset to +10 ms and verify that the delay observed at the oscilloscope corresponds is consistent with the nominal figure plus 10 ms. Failure to meet this requirement is cause to fail this test.

4. Repeat the above test, but this time for 48 fps (use the composition *DCI 2K Sync Test (48fps)*). Record the results obtained.

Figure 6.2. shows what a typical measurement is expected to look like. The upper trace shows the light output of the projector, measured by means of the photo diode. The photo diode signal is shown inverted, *i.e.*, low means high light output. The lower trace shows the analog center channel output.

> **Note:**
> The optical flashes generated during this test can cause physiological reactions in some people. People who are sensitive to such optical stimuli should not view the test material.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.4.1.8<br>[OBAE-ADD] |
| **Test Equipment** | **Oscilloscope**<br>**Photodiode** |
| **Test Materials** | *DCI 2K Sync Test (OBAE)*<br>*DCI 2K Sync Test (48fps) (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.8.3. Maximum Bitrate OBAE

### Objective

Verify that the playback system supports playback of OBAE content that consists of maximum size frames, as defined in [SMPTE-429-18].

### Procedures

Perform the following steps:

1. Select and play *Maximum Bitrate OBAE (Encrypted)* keyed with *KDM for Maximum Bitrate OBAE (Encrypted)*.

2. Select and play *Maximum Bitrate OBAE 48 fps (Encrypted)* keyed with *KDM for Maximum Bitrate OBAE 48 fps (Encrypted)*.

Any audible artifact, interruption in playback or inability to start playback is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | [OBAE-ADD]<br>[SMPTE-429-18] |

| | |
|---|---|
| **Test Equipment** | **OBAE Sound System** |
| **Test Materials** | *Maximum Bitrate OBAE (Encrypted)*<br>*KDM for Maximum Bitrate OBAE (Encrypted)*<br>*Maximum Bitrate OBAE 48 fps (Encrypted)*<br>*KDM for Maximum Bitrate OBAE 48 fps (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 6.8.4. OBAE Rendering Expectations

### Objective

Verify that the **OBAE Sound System** meets acoustic rendering expectations.

### Procedures

Perform the following steps:

1. Configure the **OBAE Sound System** according to J.2. Configuration.

2. Playback *OBAE Rendering Expectations* in its entirety, subject to the requirements specified at J.3. Requirements. Deviation from any of these requirements is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | [OBAE-ADD]<br>[SMPTE-2098-3] |
| **Test Equipment** | **OBAE Sound System** |
| **Test Materials** | *OBAE Rendering Expectations* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

# Chapter 7. Projector

The Projector is a Type 2 SPB comprising a light processing system, including electronic and optical components, and a companion SPB. The projector may be stand-alone, in which case the companion SPB will be a Link Decryptor (LD), or else the companion SPB will be a

Media Block (MB). The projector may include a Timed Text rendering engine (alpha-channel overlay).

# 7.1. Projector Test Environment for Image Measurements

When making image measurements on a Test Subject, the following environmental conditions must exist:

The Test Subject (projector) must be turned on (including the lamp) and allowed to thermally stabilize for 20 to 30 minutes prior to all measurements. All required setup and calibration procedures, as recommended by the manufacturer, shall be carried out or verified prior to all measurements. The projector's color management system must be configured such that incoming code values are interpreted in accordance with [SMPTE-428-1].

Stray light on the screen must be minimized. The room lights in screening rooms must be turned off, with the exception of the minimal lighting provided for working or safety reasons. For a theatrical environment room, the room lights must be the normal theatrical lighting environment. The ambient light level of a mastering environment reflected by the screen must be less than 0.01 $Cd/m^2$(.0029 ft-L), that of a theatrical environment less than 0.03 $Cd/m^2$ (.01 ft-L). The use of black nonreflective surfaces with recessed lighting is encouraged. Safety regulations and the placement of exit lights or access lights can result in a higher ambient light level.

The screen must be non-specular and equally reflective over the entire visible spectrum. The screen should have variable black masking, adjustable to tightly frame the projected image (at a minimum, this should include the 1.85:1 and 2.39:1 image formats).

All image parameters must be measured off of the screen from the center of the normal seating area in an exhibition theater. All measurements must be done according to [SMPTE-431-1], [SMPTE-431-2].

Section 7.5.13 describes measuring the test environment. Measurements recorded from Section 7.5.5 through Section 7.5.12 should be interpreted in consideration of the measured test environment.

# 7.2. SPB Type 2

## 7.2.1. Projector and Direct View Display Physical Protection

### Objective

- Verify that the projector's or direct view display's companion SPB (LDB or MB) and its plaintext image interfaces are physically inside of, or otherwise mechanically connected to, the type 2 SPB.
- Verify that SPB type 2 protection requirements are provided by the Projector or Direct View SPB.

### Procedures

- If the Test Subject is a Projector:

    1. By physical examination and using documentation provided by the manufacturer, determine the physical perimeter that provides the type 2 SPB protection for the Projector. Verify that the type 2 SPB provides a hard, opaque physical security perimeter that surrounds the electronics and prevents access to internal circuitry.
    Failure of this verification is cause to fail this test.

- If the Test Subject is a Projector or a Direct View Display:
  By physical examination and using documentation provided by the manufacturer:

    2. Locate, and for each of any removable access covers and/or doors of the type 2 SPB intended for Security Servicing (*i.e.*, openings that enable access to Security-Sensitive Signals), record whether they are protected by either (1) mechanical locks employing physical or logical keys and tamper-evident seals (*e.g.*, evidence tape or holographic seals), or (2) pick resistant locks employing physical or logical keys.
       The absence of protection as required on any of these security access covers or doors is cause to fail this test.

    3. Locate the companion SPB's and type 2 SPB's Security Sensitive Signals. Verify that:

        a. Security Sensitive Signals are not accessible via (i) any removable access covers and/or doors other than those located in step 2, (ii) any ventilation holes or other openings; and

        b. Access to Security Sensitive Signals and circuits would cause permanent and easily visible damage. Failure of either of these verifications is cause to fail this test.

    4. Locate the Companion SPB (MB or LDB). Verify that the Companion SPB is entirely enclosed within, or mechanically connected to, the SPB type 2 enclosure.
       Failure to meet this requirement is cause to fail this test.

- If the Test Subject is a Direct View Display:

    5. By physical examination and using documentation provided by the manufacturer, verify that:

        a. The physical intrusion barrier presented by the light emitting front surface of the display's Cabinets or Modules is not penetrate-able without permanently destroying the proper operation of a Cabinet and/or Module penetrated, and leaving permanent and easily visible damage.

        b. Cabinets and/or Modules are mechanically interlocked to each other directly and/or via the supporting frame structure such that any separation that would enable access to internal signals causes permanent and easily visible damage.

        c. Access to light emitting (pixel generating) component electrical signals from the surface of the display screen is limited to individual component pins, and there is no access to signals that would constitute a portion of the picture image beyond the pixel by pixel level.

  Failure to meet any of these requirements is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.2.2, 9.4.3.6.1, 9.5.2.2, 9.5.2.4, 9.5.2.4.1 |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.2.2. Projector and Direct View Display Security Servicing

### Objective

- Verify that the projector or direct view display SPB implements a "security access opening" event signal to the companion SPB.

- Verify that playback terminates and/or is not permitted if the security access opening event is active, or a front removable module has been removed.

### Procedures

- If the Test Subject is a Projector or Direct View Display:
  By physical examination and using documentation provided by the manufacturer, locate each of the type 2 SPB access door and/or panel openings intended for Security Servicing (*i.e.*, openings that enable access to Security- Sensitive Signals). Execute the following tests 1-4 for each opening found, and record the results.

    1. Play back the DCP *DCI 2K StEM*.

    2. Open the SPB access door/panel and observe that playback terminates. If playback does not terminate, this is cause to fail this test.

    3. Attempt to start playback with the door/panel open. If playback starts, this is cause to fail this test.

    4. Close the opening and examine the logs from the SPB's companion SPB and verify that an "SPBOpen" event was created for each time a door/panel was opened, and an "SPBClose" event was created for each closure. If any log record is missing, this is cause to fail this test.

- If the Test Subject is a Direct View Display:
  With the exception of step 6(c), the following tests may be verified by physical examination of the direct view display's type 2 SPB and using documentation provided by the manufacturer:

    5. Noting the servicing method exception defined for step 6 below: Identify and document each distinct method that can be used for replacing (disassembly and reassembly, etc.) a Cabinet or Module. For each method that exposes Security-Sensitive Signals, verify that:

        a. a security access opening event is triggered, and

        b. playback is prevented while the security access opening event is active.
        Failure of either of the above requirements is cause to fail this test. (It is allowed for one security access opening event to be triggered in the course of simultaneously replacing multiple Cabinets and/or Modules as part of a single servicing event.)

    6. For Cabinets having *front removable Modules* designed for non-security servicing (*i.e.*, designed for Module replacement without triggering a security access opening event), verify that the removal of any front-serviceable Module:

        a. exposes only those pixel signals accessible via the electrical connection(s) associated with the Module removed and does not otherwise expose Security-Sensitive Signals or compromise the SPB type 2 perimeter. Note that signaling multiplexing may have a multiplier effect that exposes signals associated

with other Modules via the connection(s); this is allowed, but must be considered in step (c) below. Display Security Servicing
Failure to meet this requirement is cause to fail this test.

b. is detected and prevents playback of an encrypted composition.
Failure to meet this requirement is cause to fail this test.

c. Quantity over 15 (*i.e.*, removal of more than 15 modules), or a quantity that exposes pixel signals constituting more than 5% of the display screen area, whichever is less within any 8 hour period, shall trigger a security access opening event.
To execute this step:

i. calculate the minimum number of Modules required to expose pixel signals constituting more than 5% of the screen area, considering the multiplier effect noted in (a). If the number is less than 16, record this number as MaxNumber, otherwise set MaxNumber to 16.

ii. determine a Module removal selection sequence for removing a quantity of (MaxNumber + 1) of Modules which are most likely to stress the display opening detection design.

iii. Recording a test start time as "T0", begin removing and replacing Modules in the sequence order determined in step (ii) until an access opening event has been triggered, or 16 Modules have been removed and replaced. Record this quantity.

iv. Following the manufacturers requirements, clear (reset) the access opening event. After 7 hours and 55 minutes from T0 of step (iii), remove and replace the next Module in sequence. Verify that a security access opening event has been triggered.

A quantity recorded in step (iii) of not less than MaxNumber is cause to fail this test. Failure of a security access opening event to trigger for step (iv) is cause to fail this test.

7. For each occurrence of a security access opening event of tests 4, 5 and 6, verify that:

a. clearing (resetting) of the alarm event requires the use of a physical key or entry of a code,

b. SPBOpen and SPBClose events are logged for each occurrence.

Failure of either of the above requirements is cause to fail this test.

## Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.1, 9.5.2.4, 9.5.2.4.1 |
| **Test Materials** | *DCI 2K StEM* |

## Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 18.2. Projector Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 7.2.3. Deleted Section

The section "SPB2 Requirements" was deleted. The section number is maintained here to preserve the numbering of subsequent sections

## 7.2.4. Deleted Section

The section "SPB2 Secure Silicon Requirements" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 7.2.5. Deleted Section

The section "SPB2 Tamper Evidence" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 7.2.6. SPB2 Secure Silicon Field Replacement

### Objective

Verify that the secure silicon device, contained within a SPB Type 2, is not field serviceable (though it may be field replaceable). Verify that it is not accessible during normal SPB Type 2 operation or non-security-related servicing.

### Procedures

By careful optical and physical examination, verify that the secure silicon device contained within a SPB Type 2

1. is not field serviceable (but may be field replaceable), *i.e.*, there are no provisions for direct access to the SPB Type 2 secure silicon circuitry.

2. is not accessible during normal SPB Type 2 operation or non-security-related servicing, *i.e.*, is mounted in a special compartment separated from areas accessible during operations or normal servicing. If the SPB2 secure silicon device is accessible during non-security servicing or normal operations, this shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.3 |

### Consolidated Test Sequences

—

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.2.7. Systems without Electronic Marriage

### Objective

Verify that in the configuration of a permanently married companion SPB (MB or LDB), the companion SPB is not field replaceable and requires the projector SPB and companion SPB system to both be replaced in the event of an SPB failure.

### Procedures

Verify that the companion SPB Type 1 (MB if no link encryption is used or LDB if link encryption is used) is not field-replaceable. Careful optical and physical inspection is necessary for this. Any deviation from these requirements is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.6 |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.2.8. Electronic Marriage Break Key Retaining

### Objective

Verify that breaking the marriage between the projector and its companion SPB (LDB or MB) does not zeroize the projector SPB type 2 long term identity keys (RSA private keys).

### Procedures

(Only applies to systems that implement an Electronic Marriage, *i.e.*, those that have field replaceable LDBs or MBs.)

1. Using procedures and tools provided by the manufacturer of the Projector, obtain the device certificate representing the identity of the SPB type 2 in PEM encoded format.

2. Using the procedure illustrated in Section 2.1.11, record the public key thumbprint of the certificate obtained in the above step.

3. Intentionally break the marriage and remarry the systems (this may require support by the manufacturer).

4. Using the same procedure as described in steps 1 and 2, verify that the public key in the certificate supplied by the projector is the same as before the remarriage. Mismatching public key thumbprints are cause to fail this test.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.1 |

#### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.3. Companion SPB Type 1

### 7.3.1. Deleted Section

The section "Projector Companion SPB Location" was deleted. The section number is maintained here to preserve the numbering of subsequent sections

### 7.3.2. Companion SPBs with Electronic Marriage

#### Objective

This test only applies to field replaceable companion SPBs (MB or LDB) that implement electronic marriage functions.

- Verify that as part of the installation, or reinstallation, (*i.e.*, mechanical connection to the projector and electrical initiation) an electrical and logical marriage of the companion SPB (MB or LDB) with the projector SPB is performed.

- Verify that upon initiation of the marriage a "SPBMarriage" log record is written (per [SMPTE-430-5]) and that the record contains all required data.

- Verify that upon break of the marriage a "SPBDivorce" log record is written (per [SMPTE-430-5]) and that the record contains all required data.

#### Procedures

1. Verify system is functional prior to breaking the marriage. This can be achieved by loading and successfully playing the composition *DCI 2K Sync Test*.

2. Power down the system, locate the field-replaceable companion SPB (MB or LDB), break the marriage by disconnecting and/or removing the SPB.

3. Replace and reconnect the companion SPB, power up the system, examine the logs and verify that a "SPBDivorce" log record has been written. Absence of this entry is cause to fail this test.

4. Verify the following are contained in the SPBDivorce record:

    a. The `DeviceSourceID` element contains the Certificate Thumbprint of the companion SPB.

    b. The `DeviceConnectedID` element contains the Certificate Thumbprint of the projector SPB2.

    c. The log entry contains an `AuthId` record.

    Failure to meet requirements a, b and c above is cause to fail this test.

5. Setup a show with composition from Step 1. Verify that the system does not play the composition. Failure to meet this requirement is cause to fail this test.

6. Perform the marriage installation procedure and repeat Step 1 to verify that the system is now capable of playout. Failure to meet this requirement is cause to fail this test.

7. Examine the logs and verify that a "SPBMarriage" log entry has been written. Absence of this entry is cause to fail this test.

8. Verify the following are contained in the SPBMarriage record:

    a. The `DeviceSourceID` element contains the Certificate Thumbprint of the companion SPB.

    b. The `DeviceConnectedID` element contains the Certificate Thumbprint of the projector SPB2.

    c. The log entry contains an `AuthId` record.
    Failure to meet requirements a, b and c above is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.1, 9.4.3.6.2, 9.4.3.6.3<br>SMPTE-430-5 |
| **Test Materials** | *DCI 2K Sync Test* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 18.2. Projector Confidence Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 7.3.3. Companion SPB Marriage Break Key Retaining

### Objective

- Verify that breaking the marriage between the Media Block (MB) companion SPB (Type 1) and the projector SPB (type 2) does not zeroize the MB's long term identity keys (RSA private keys).
- Verify that breaking the marriage between the Link Decryptor Block (LDB) companion SPB (Type 1) and the projector SPB (type 2) does not zeroize the LDB's long term identity keys (RSA private keys).

### Procedures

> **Note:**
> This section only applies to systems that implement an Electronic Marriage, *i.e.*, those that have field replaceable companion SPBs (MBs or LDBs).

In the case of an MB that is married to a Projector SPB and *implements dual certificates* as defined in Section 9.5.1.2 of [DCI-DCSS]:

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.
2. Extract a signed [SMPTE-430-5] security log report from the Test Subject that includes the range of time during which the above step was carried out.
3. Using the procedures illustrated in Section 3.1.3, use the **checksig** program to verify the signature of the log report collected in step 2. Note: Depending on the order of the certificates contained in the log report, the **dsig_cert.py** program may need to be used to re-order the certificates for the **checksig** program.
4. Using the procedures illustrated in Section 3.1.3.1, extract the certificates in the signing chain of the log report collected in step 2. Note: This may be accomplished using the **dsig_extract.py** program.
5. Using the procedures illustrated in Section C.2, use the **dc-thumbprint** program to calculate the thumbprint of the Log Signer Certificate that signed the log report collected in step 2. Record the value of the calculated thumbprint.
6. Intentionally break the marriage and remarry the companion SPB and the projector SPB (this may require support by the manufacturer).
7. Repeat steps 1 and 2 using the same composition and KDM as before. Failure to successfully play content or retrieve a log report after remarriage is cause to fail this test.
8. Repeat step 3 using the log report collected after remarriage. Failure to successfully verify the signature is cause to fail this test.

9. Repeat steps 4 and 5 using the log report collected after remarriage. Confirm that the Log Signer Certificate public key thumbprint calculated after remarriage matches the one from step 5. Mismatching Log Signer Certificate public key thumbprints are cause to fail this test.

In the case of an MB that is married to a Projector SPB and *implements a single certificate* as defined in Section 9.5.1.1 of [DCI-DCSS]:

1. Set up and play a show using the composition *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)*.

2. Extract a signed [SMPTE-430-5] security log report from the Test Subject that includes the range of time during which the above step was carried out.

3. Using the procedures illustrated in Section 3.1.3, use the **checksig** program to verify the signature of the log report collected in step 2. Note: Depending on the order of the certificates contained in the log report, the **dsig_cert.py** program may need to be used to re-order the certificates for the **checksig** program.

4. Using the procedures illustrated in Section 3.1.3.1, extract the certificates in the signing chain of the log report collected in step 2. Note: This may be accomplished using the **dsig_extract.py** program.

5. Using the procedures illustrated in Section C.2, use the **dc-thumbprint** program to calculate the thumbprint of the certificate that signed the log report collected in step 2. Record the value of the calculated thumbprint.

6. Intentionally break the marriage and remarry the companion SPB and the projector SPB (this may require support by the manufacturer).

7. Repeat steps 1 and 2 using the same composition and KDM as before. Failure to successfully play content or retrieve a log report after remarriage is cause to fail this test.

8. Repeat step 3 using the log report collected after remarriage. Failure to successfully verify the signature is cause to fail this test.

9. Repeat steps 4 and 5 using the log report collected after remarriage. Confirm that the certificate thumbprint calculated after remarriage matches the one from step 5. Mismatching public key thumbprints are cause to fail this test.

In the case of an LDB married to a Projector SPB:

1. Using an ASM requester simulator, initiate a TLS session with the companion SPB (LDB) and capture the certificate supplied by the companion SPB in PEM encoded format.

2. Using the procedure illustrated in Section 2.1.11, record the public key thumbprint of the certificate captured in the above step.

3. Intentionally break the marriage and remarry the systems (this may require support by the manufacturer).

4. Verify that, after remarriage, the system is able to re-establish a TLS session. Failure to establish a TLS session after remarriage is cause to fail this test.

5. Using the same procedure as described in steps 1 and 2, verify that the public key in the certificate supplied by the companion SPB upon initialization is the same as before the remarriage. Mismatching public key thumbprints are cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.2, 9.4.3.6.3, 9.5.1.2 |
| **Test Equipment** | **asm-requester** |
| **Test Materials** | *DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 18.2. Projector Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.3.4. Remote SPB Clock Adjustment

### Objective

1. Verify that in order to maintain synchronization between auditoriums, exhibitors are able to adjust a remote SPB's clock offset a maximum of +/- 15 minutes within any calendar year.

2. Verify that the remote SPB clock offset time adjustments are logged events.

### Procedures

> **Note:**
> The following procedures are likely to fail if the Test Subject has had its time adjusted since manufacture. The current time may not be centered on the adjustment range zero point. Any such adjustments, however, will be evidenced in the security log and by examining the relevant `<TimeOffset>` elements, the zero point can be derived and the time set accordingly. If necessary, contact the manufacturer for assistance in determining and setting the time to the center of the range of adjustment for the current calendar year.

1. Configure an **asm-requester** to communicate with the Test Subject and initialize the connection.

2. Issue a `LEKeyLoad` ASM command and record the UTC time as provided by an **Accurate Real-Time Clock** at the moment the command is sent.

3. Attempt to advance the time of the remote SPB by 15 minutes. Record whether the adjustment was successful and the UTC time at the moment of adjustment. Failure to successfully adjust the time is cause to fail this test.

4. Repeat Step 2.

5. Return the time to the zero point (retard 15 minutes).

6. Attempt to retard the time of the remote SPB by 15 minutes. Record whether the adjustment was successful and the UTC time at the moment of adjustment. Failure to successfully adjust the time is cause to fail this test.

7. Repeat Step 2.

8. Return the time to the zero point (advance 15 minutes).

9. Attempt to adjust the time more than + 15 minutes. Record whether the adjustment was successful and the UTC time at the moment of adjustment. If the time can be successfully adjusted more than 15 minutes this is cause to fail this test.

10. Attempt to adjust the time more than -15 minutes. Record whether the adjustment was successful and the UTC time at the moment of adjustment. If the time can be successfully adjusted more than 15 minutes this is cause to fail this test.

11. Extract a security log from the Test Subject that includes the range of time during which the above Steps were carried out.

12. Locate a `LEKeyLoad` event caused by Step 2. Subtract the value of the time recorded in Step 2 (UTC time) from the TimeStamp from the LogRecord (System time). Record this time as the delta of System time to UTC time for the unadjusted state.

13. Locate the `SPBClockAdjust` event from Step 3 and confirm that the TimeStamp contains a value which is the time recorded in Step 3 (UTC time) + the delta from Step 12 + 15 minutes.

14. Locate the `SPBClockAdjust` event from Step 6 and confirm that the TimeStamp contains a value which is the time recorded in Step 6 (UTC time) + the delta from Step 12 - 15 minutes.

15. Locate the `SPBClockAdjust` event from Step 9 and confirm the presence of an Exception with a name of "AdjustmentRangeError".

16. Locate the `SPBClockAdjust` event from Step 10 and confirm the presence of an Exception with a name of "AdjustmentRangeError".

17. Locate a `LEKeyLoad` event caused by Step 4. Confirm that the TimeStamp contains a value which is the time recorded in Step 4 (UTC time) + the delta from Step 12 + 15 minutes.

18. Locate a `LEKeyLoad` event caused by Step 7. Confirm that the TimeStamp contains a value which is the time recorded in Step 6 (UTC time) + the delta from Step 12 - 15 minutes.

19. Incorrect or missing LogRecords for Steps 12 through 18 shall be cause to fail this test. *Note: The TimeStamp values will have an accuracy that depends on various factors such as system responsiveness, test operator acuity, etc, and are essentially approximate. The intent is to verify that the TimeStamps indeed reflect the +/- 15 minute adjustments.*

*Note: If the Test Subject's method of adjusting the time constrains the adjustment before passing the request to the remote SPB, the required security log entries from Steps 15 and 16 will not be produced. In this case, the manufacturer will need to provide a method or software tool which allows the remote SPB to receive out-of-range adjustment commands.*

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |
| **Test Equipment** | **asm-requester**<br>**Accurate Real-Time Clock** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 7.4. Link Decryptor Block

The Link Decryptor Block (LDB) is a Type 1 SPB that is used to receive encrypted signals into a Type 2 SPB companion device (such as a projector).

### 7.4.1. Deleted Section

The section "LDB without Electronic Marriage" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

### 7.4.2. LDB TLS Session Constraints

#### Objective

Verify that LDBs do not establish security communications with more than one SM at a time.

#### Procedures

1. Configure a system comprising the Test Subject and two (2) **asm-requester**. The requesters shall have unique device certificates and IP addresses and shall be on the same subnet as the Test Subject. The two requesters shall be referred to as "Requester A" and "Requester B" respectively.

2. Using Requester A, start a TLS session to the Test Subject . Observe that the Test Subject accepts the connection. Failure to successfully connect is cause to fail this test.

3. Using Requester B, attempt to open a second TLS session with the Test Subject, confirm that the Test Subject does not accept connections. Deviation from this behavior is cause to fail this test.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.2 |
| **Test Equipment** | **asm-requester** |

#### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 7.4.3. LDB Time-Awareness

### Objective

Verify that the LDB contains a UTC reference clock which is backed up by battery and operative for time stamping log events under powered and unpowered conditions.

### Procedures

1. Make sure the system has been fully operational (*i.e.*, initialized) at least once before this test.
2. Note down the system clock relative to an external digital reference clock, thus making calculation of the relative clock offset possible.
3. Power off the system.
4. Open the projector SPB 2 door and note down the external reference clock time at which this happened.
5. Power up the system again.
6. Examine the log records and verify that the opened SPB door has been logged at the right time. This can be verified because the offset of the internal clock relative to the external reference clock is known, so the expected internal clock time of the open door event can be calculated. An incorrect time stamp is cause to fail this test.
7. While powered, open the projector door and verify that an according log entry is written with the correct time. An incorrect time stamp is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.2.6 |
| **Test Equipment** | **Accurate Real-Time Clock** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |

## 7.4.4. Deleted Section

The section "LDB ASM Conformity" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 7.4.5. LDB Key Storage

### Objective

Verify that the LDB accepts and stores LD keys and associated parameters provided by the SM. Verify that the LDB has the capacity to store at least 16 key/parameter sets.

### Procedures

1. Using an **asm-requester** simulator, initiate a TLS session with the LDB and issue an `LEKeyPurgeAll` command.

```
$ asm-requester (... standard options ...) --messagetype LEKeyPurgeAll
```

2. Using an **asm-requester** simulator, issue an `LEKeyQueryAll` command. The response should indicate an empty LE key list. A non-empty list shall be cause to fail this test.

```
$ asm-requester (... standard options ...) --messagetype LEKeyQueryAll
list size: 0
```

3. Using an **asm-requester** simulator, issue sixteen (16) `LEKeyLoad` commands. Verify that the LE key list contains sixteen keys by executing an `LEKeyQueryAll` command. An LE key list size other than sixteen shall be cause to fail this test.

```
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 1
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 2
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 3
...
$ asm-requester (... standard options ...) --messagetype LEKeyQueryAll
list size: 16
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.2 |
| **Test Equipment** | **asm-requester** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 7.4.6. LDB Key Purging

### Objective

- Verify that the LDB purges LD keys upon expiration of the SM-designated validity period.

- Verify that the LDB purges LD keys upon receipt of a `LEKeyPurgeAll` command from the SM.

### Procedures

1. Using an **asm-requester** simulator, initiate a TLS session with the LDB and issue an `LEKeyPurgeAll` command.

```
$ asm-requester (... standard options ...) --messagetype LEKeyPurgeAll
```

2. Using an **asm-requester** simulator, issue an `LEKeyQueryAll` command. The response should indicate an empty LE key list. A non-empty list shall be cause to fail this test.

```
$ asm-requester (... standard options ...) --messagetype LEKeyQueryAll
list size: 0
```

3. Using an **asm-requester** simulator, issue an `LEKeyLoad` command with a validity period of one minute. Verify that the LE key list contains one (1) key by executing an `LEKeyQueryAll` command. An LE key list size other than one shall be cause to fail this test.

```
$ asm-requester (... standard options ...) --messagetype LEKeyLoad \
--messagetype-id 4
$ asm-requester (... standard options ...) --messagetype LEKeyQueryAll
list size: 1
```

4. Wait one minute. Using an **asm-requester** simulator, issue an `LEKeyQueryAll` command. The response should indicate an LE key list with zero (0) keys. An LE key list or a size greater than zero (0) shall be cause to fail this test.

```
$ asm-requester (... standard options ...) --messagetype LEKeyQueryAll
list size: 0
```

5. Using an **asm-requester** simulator, issue six (6) `LEKeyLoad` commands. Verify that the LE key list contains six keys by executing an `LEKeyQueryAll` command. An LE key list size other than six (6) shall be cause to fail this test.

```
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 1
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 2
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 3
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 4
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 5
$ asm-requester (... standard options ...) --messagetype LEKeyLoad --messagetype-id 6
$ asm-requester (... standard options ...) --messagetype LEKeyQueryAll
list size: 6
```

6. Using an **asm-requester** simulator, execute an `LEKeyPurgeAll` command.

```
$ asm-requester (... standard options ...) --messagetype LEKeyPurgeAll
```

7. Using an **asm-requester** simulator, issue an `LEKeyQueryAll` command. The response should indicate an LE key list with zero (0) keys. An LE key list or a size greater than zero (0) shall be cause to fail this test.

```
$ asm-requester (... standard options ...) --messagetype LEKeyQueryAll
list size: 0
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.2 |

| Test Equipment | asm-requester |
|---|---|

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 16.2. LD/LE Test Sequence | Pass/Fail | — | — |

## 7.4.7. Deleted Section

The section "LDB Logging" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

# 7.5. Projector Image Reproduction

## 7.5.1. Projector Overlay

### Objective

In the case that the Projector implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel), verify that assets are rendered and displayed correctly by the system.

### Procedures

1. Using a digital cinema server that does not provide an internal subtitle rendering capability (or one in which subtitle rendering capability is disabled), load and play each of the compositions:

    a. *2K Scope Subtitle Test (Encrypted)*, keyed with *KDM for 2K Scope Subtitle Test (Encrypted)*.

    b. *2K Flat Subtitle Test (Encrypted)*, keyed with *KDM for 2K Flat Subtitle Test (Encrypted)*.

    c. *2K Full Subtitle Test (Encrypted)*, keyed with *KDM for 2K Full Subtitle Test (Encrypted)*.

    d. *4K Scope Subtitle Test (Encrypted)*, keyed with *KDM for 4K Scope Subtitle Test (Encrypted)*.

    e. *4K Flat Subtitle Test (Encrypted)*, keyed with *KDM for 4K Flat Subtitle Test (Encrypted)*.

    f. *4K Full Subtitle Test (Encrypted)*, keyed with *KDM for 4K Full Subtitle Test (Encrypted)*.

    g. *2K 48fps Scope Subtitle Test (Encrypted)*, keyed with *KDM for 2K 48fps Scope Subtitle Test (Encrypted)*.

h. *2K 48fps Flat Subtitle Test (Encrypted)*, keyed with *KDM for 2K 48fps Flat Subtitle Test (Encrypted)*.

i. *2K 48fps Full Subtitle Test (Encrypted)*, keyed with *KDM for 2K 48fps Full Subtitle Test (Encrypted)*.

2. Refer to Appendix I and for each scene in each composition, record the state of compliance with the basic and specific pass/fail criteria listed therein. Failure of any compliance criterion is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.4.4.2.5, 7.5.4.2.6, 7.5.4.2.7<br>SMPTE-429-2 |
| **Test Equipment** | **DCI Server** |
| **Test Materials** | *2K Scope Subtitle Test (Encrypted)*<br>*2K Flat Subtitle Test (Encrypted)*<br>*2K Full Subtitle Test (Encrypted)*<br>*4K Scope Subtitle Test (Encrypted)*<br>*4K Flat Subtitle Test (Encrypted)*<br>*4K Full Subtitle Test (Encrypted)*<br>*2K 48fps Scope Subtitle Test (Encrypted)*<br>*2K 48fps Flat Subtitle Test (Encrypted)*<br>*2K 48fps Full Subtitle Test (Encrypted)*<br>*KDM for 2K Scope Subtitle Test (Encrypted)*<br>*KDM for 2K Flat Subtitle Test (Encrypted)*<br>*KDM for 2K Full Subtitle Test (Encrypted)*<br>*KDM for 4K Scope Subtitle Test (Encrypted)*<br>*KDM for 4K Flat Subtitle Test (Encrypted)*<br>*KDM for 4K Full Subtitle Test (Encrypted)*<br>*KDM for 2K 48fps Scope Subtitle Test (Encrypted)*<br>*KDM for 2K 48fps Flat Subtitle Test (Encrypted)*<br>*KDM for 2K 48fps Full Subtitle Test (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.2. Deleted Section

The section "Projector Lens" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 7.5.3. Projector Pixel Count/Structure

### Objective

Verify that the sampling structure of the displayed picture array (pixel count of the projector) is equal that of the respective specified image containers (either 4096 x 2160 or 2048 x 1080).

### Procedures

Note: Prior to performing the following procedures, it is necessary to verify that any electronic rescaling of the image is fully disabled. This may include turning off resizing, keystone correction, filters and/or other related processes.

- For 2K Projectors: Display the test composition *Pixel Structure Pattern S 2k* Verify that the complete set of 16x16 and 8x8 pixel blocks is displayed.

- For 4K Projectors: Display the test pattern *Pixel Structure Pattern S 4k*. Verify that the complete set of 16x16 pixel blocks is displayed.

Deviation from the expected image is cause to fail this test. The figures below illustrate the features of the pixel array test pattern. The 2k pattern consists of a 128 x 67 grid of 16 x 16 pixel blocks as illustrated in Figure 7.1.. A single-pixel white border surrounds the pattern. Each 16 x 16 block contains a horizontal and vertical location index encoded as a 8-bit binary ladder, with the MSb being at the top or left side of the vertical and horizontal ladders, respectively. The example below shows a block with index *X =81, Y = 37*. The pixel at location 0,0 in the block is located at pixel *x = 1296 = X * 16, y = 592 = Y * 16* on the display. The bottom 8 pixels of the 2k pattern consist of similar, un-indexed 8 x 8 patterns as illustrated in Figure 7.2. .

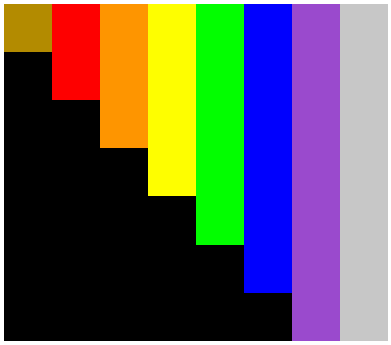
The 4k pattern consists of a 256 x 135 grid of 16 x 16 pixel arrays.A single-pixel white border surrounds the pattern.

Within each block, color-coded bands mark pixel positions. The bands may have North, South, East or West orientation (the example blocks have South orientation). Pixel positions are coded left to right (top to bottom for East and West orientations) with the following color sequence: brown, red, orange, yellow, green, blue, violet, gray.

Note: North, South, East and West orientations are provided in the test materials set to support investigation of anomalies.

## Figure 7.1. Pixel Structure 16 x 16 Array

## Figure 7.2. Pixel Structure 8 x 8 Array



Warning: the patterns displayed during this test can cause vertigo in some people. People who are sensitive to such optical stimuli should not view the test material.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.2.2.6, 8.2.2.7 |
| **Test Materials** | *Pixel Structure Pattern N 2k*<br>*Pixel Structure Pattern S 2k*<br>*Pixel Structure Pattern E 2k*<br>*Pixel Structure Pattern W 2k*<br>*Pixel Structure Pattern N 4k*<br>*Pixel Structure Pattern S 4k*<br>*Pixel Structure Pattern E 4k*<br>*Pixel Structure Pattern W 4k* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 18.2. Projector Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 7.5.4. Projector Spatial Resolution and Frame Rate Conversion

### Objective

Verify that the native display resolution, spatial conversions (where necessary), scaling and frame rates are according to the DCI Specification.

### Procedures

1. Verify that the display has a native resolution of either 4096 x 2160 or 2048 x 1080.

2. In case the native resolution is 4096 x 2160, verify that the projector performs up-conversion of 2048 x 1080 signals, *i.e.*, that the screen is filled as it would be with a 4K image.

3. Verify that all spatial conversions are done at an exact ratio of 2:1 in each axis.

4. In case scaling is used for supporting constant height or constant width projection, visually verify that this scaling does not introduce any visible image artifacts.

5. Verify that image material with frame rates different from the projection system's native refresh rate is converted by the Projector to the Projector's native refresh rate, *i.e.*, the image is displayed properly.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.2.2.7, 8.2.2.8 |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.5. White Point Luminance and Uniformity

### Objective

- Verify that the peak white luminance measured at the screen center is 48 cd/m^2 as specified according to [SMPTE-431-1].
- Verify that luminance uniformity is as specified according to [SMPTE-431-1].

### Procedures

*Note: Prior to taking measurements, ensure that the projector setup and test environment requirements detailed in Section 7.1 have been performed.*

Display the "full white" test pattern (X'= 3794, Y'=3960, Z'=3890) contained in the DCP *Sequential Contrast and Uniformity Sequence*. Align the light source to minimize luminance fall-off from center to corners. The test pattern may already be stored in the Projector for easy setup. In case it is not stored internally it must be provided by means of an external signal source.

1. Adjust the lamp focus or lamp current to a light level of 48 cd/$m^2$ measured at the screen center. Record the measured light level and any quantitative values of adjustable parameters from the projection system (*e.g.* lamp power, x/y/x lamp position etc).

2. Measure the luminance at the four sides. Record the measured light levels.

3. In the case of review rooms, measure the luminance at the four corners. Record the measured light levels.

Note: All measurements shall be done as described in [SMPTE-431-1]. Measurement criteria like Projector conditions, measurement locations on the screen, and measurement locations in the auditorium are given in [SMPTE-431-1].

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.3.4.3, 8.3.4.4<br>SMPTE-431-1 |
| **Test Equipment** | **Photometer** |
| **Test Materials** | *Sequential Contrast and Uniformity Sequence* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.6. White Point Chromaticity and Uniformity

### Objective

- Verify that white point chromaticity is as specified according to [SMPTE-431-1].
- Verify that chromaticity uniformity of the Projection System is as specified according to [SMPTE-431-1].

### Procedures

*Note: Prior to taking measurements, ensure that the projector setup and test environment requirements detailed in Section 7.1 have been performed.*

Display the "full white" test pattern (X'=3794, Y'=3960, Z'=3890) contained in the DCP *Sequential Contrast and Uniformity Sequence*. The test pattern may already be stored in the projector for easy setup. In case it is not stored internally it must be provided by means of an external signal source.

1. Measure the white point chromaticity coordinates at the center of the screen with a **Spectroradiometer**. Record the measured chromaticity values.
2. Measure white point chromaticity uniformity by measuring the chromaticity coordinates at the four corners with a **Spectroradiometer**. Record the measured chromaticity values.

Note: All measurements shall be done as described in [SMPTE-431-1]. Measurement criteria like Projector conditions, measurement locations on the screen, and measurement locations in the auditorium are given in [SMPTE-431-1].

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.3.4.5, 8.3.4.6 |

| | |
|---|---|
| SMPTE-431-1 | **Test Equipment** |
| **Spectroradiometer** | **Test Materials** |
| *Sequential Contrast and Uniformity Sequence* | |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.7. Sequential Contrast

### Objective

Measure the sequential contrast ratio of the Projector.

### Procedures

*Note: Prior to taking measurements, ensure that the projector setup and test environment requirements detailed in Section 7.1 have been performed.*

1. Measure the luminance at the center of the screen for the "full black" test pattern contained in the DCP *Sequential Contrast and Uniformity Sequence*.
2. Measure the luminance at the center of the screen for the "full white" test pattern contained in the DCP *Sequential Contrast and Uniformity Sequence*.
3. Compute the sequential contrast ratio by dividing the white luminance value by the black luminance value.
4. Record the calculated value.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.3.4.7 |
| **Test Equipment** | **Photometer** |
| **Test Materials** | *Sequential Contrast and Uniformity Sequence* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |

## 7.5.8. Intra-frame Contrast

### Objective

Measure the intra-frame contrast ratio of the Projector.

### Procedures

*Note: Prior to taking measurements, ensure that the projector setup and test environment requirements detailed in Section 7.1 have been performed.*

1. Display the checkerboard test pattern *Intra-Frame Contrast Sequence*.
2. Measure the luminance level at each of the patches in the checkerboard test pattern.
3. Calculate the average value of the luminance of the white patches and divide by the average value of the luminance of the black patches.
4. Record the calculated value.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.3.4.8<br>SMPTE-431-2 |
| **Test Equipment** | **Photometer** |
| **Test Materials** | *Intra-Frame Contrast Sequence* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.9. Grayscale Tracking

### Objective

Using the black-to-white gray and the black-to-dark gray step-scale test patterns, verify that the entire step-scale appears neutral without any visible color non-uniformity or non-monotonic luminance steps in the test pattern.

### Procedures

*Note: Prior to taking measurements, ensure that the projector setup and test environment requirements detailed in Section 7.1 have been performed.*

1. With the Projector powered down or douser closed, use a **Spectroradiometer** to measure and record the Luminance of the ambient light reflected from the screen.

2. With the Projector powered up, douser open and displaying no image or black code values, use a **Spectroradiometer** to measure and record the Luminance of the light reflected from the screen.

3. Play back the DCP *DCI White Steps* (black-to-white gray step-scale test pattern).

4. For each of the ten steps of the pattern listed in Table A-2 of [SMPTE-431-2], measure and record the Output Luminance and Chromaticity Coordinates with a **Spectroradiometer**.

5. The entire step-scale should appear neutral without any visible color non-uniformity or non-monotonic luminance steps in the test pattern. Record the presence of any perceived deviation from a neutral scale.

6. Play back the DCP *DCI Gray Steps* (black-to-dark gray step-scale test pattern).

7. For each of the ten steps of the pattern listed in Table A-3 of [SMPTE-431-2], measure and record the Luminance and Chromaticity Coordinates with a **Spectroradiometer**.

8. The entire step-scale should appear neutral without any visible color non-uniformity or non-monotonic luminance steps in the test pattern. Record the presence of any perceived deviation from a neutral scale.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.3.4.9<br>SMPTE-431-2 |
| **Test Equipment** | **Spectroradiometer** |
| **Test Materials** | *DCI White Steps*<br>*DCI Gray Steps* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.10. Contouring

### Objective

Verify that no contouring can be observed.

### Procedures

1. Play back the composition *DCI 2K Moving Gradient*. This clip contains a special moving pattern to reveal usage of all 12 bits. The pattern contains three vertical bands, each 250 horizontal pixels in width, corresponding to 12, 11 and 10

bit representations of a sine wave that advances in value by 1 degree per pixel. The bands are labeled with the 12 bit region on the left, 11 bit region in the center and 10 bit region on the right of the screen. Examine the image for artifacts such as contouring or vertical striations. Record the presence of any such noticeable artifacts in the 12 bit region of the pattern. The 11 and 10 bit regions are provided for reference.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.3.3<br>SMPTE-431-2 |
| **Test Materials** | *DCI 2K Moving Gradient* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.11. Transfer Function

### Objective

Verify that the correct encoding transfer function is being used by the projector.

### Procedures

*Note: Prior to taking measurements, ensure that the projector setup and test environment requirements detailed in Section 7.1 have been performed.*

1. With the projector powered down or douser closed, use a **Spectroradiometer** to measure and record the luminance of the ambient light reflected from the screen.

2. With the projector powered up, douser open and displaying no image or black code values, use a **Spectroradiometer** to measure and record the luminance of the light reflected from the screen.

3. Play back the DCP *DCI White Steps* (black-to-white gray step-scale test pattern).

4. For each of the ten steps of the pattern listed in Table A-2 of [SMPTE-431-2], measure and record the output luminance and chromaticity coordinates with a **Spectroradiometer**.

5. For each of the measured Output luminance values, calculate the percentage deviation from the target value and record those results.

6. Play back the DCP *DCI Gray Steps* (black-to-dark gray step-scale test pattern).

7. For each of the ten steps of the pattern listed in Table A-3 of [SMPTE-431-2], measure and record the Output luminance and chromaticity coordinates with a **Spectroradiometer**.

8. For each of the measured Output luminance values, calculate the percentage deviation from the target value and record those results.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.3.4.11<br>SMPTE-431-2 |
| **Test Materials** | *DCI White Steps*<br>*DCI Gray Steps* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.12. Color Accuracy

### Objective

Verify that all colors are accurately reproduced within the tolerances as specified in [SMPTE-432-1].

### Procedures

*Note: Prior to taking measurements, ensure that the projector setup and test environment requirements detailed in Section 7.1 have been performed.*

1. With the Projector powered down or douser closed, use a **Spectroradiometer** to measure and record the Luminance of the ambient light reflected from the screen.

2. With the Projector powered up, douser open and displaying no image or black code values, use a **Spectroradiometer** to measure and record the Luminance of the light reflected from the screen.

3. Play back the DCP *Color Accuracy Series*.

4. For each of the twelve color patches listed in Table A-4 of [SMPTE-432-2], measure and record the Output Luminance and Chromaticity Coordinates with a **Spectroradiometer**.

5. For each of the measured sets of Color Coordinates and Output Luminance values, derive the L*a*b* equivalent values and record them.

6. Using the formula $deltaE^*_{ab}=[(\Delta L^*)^2 + (\Delta a^*)^2 + (\Delta b^*)^2]^{1/2}$, for each pair of values from steps 5 and 6, calculate the $deltaE^*_{ab}$ value. Record each such value and indicate whether it is less than or equal to 4.0. **eab_calc.py**, a tool to perform this calculation, is available in Section C.6.

Note: See Annex L of [SMPTE-432-1] for an example of how to convert xyY values to L*a*b* values.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 8.3.4.13<br>SMPTE-431-2<br>SMPTE-432-1 |
| **Test Equipment** | **Spectroradiometer**<br>**eab_calc.py** |
| **Test Materials** | *Color Accuracy Series* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 7.5.13. Projector Test Environment

### Objective

Record information about the test environment in which the reported projector measurements were made.

### Procedures

1. Record the distance between the front of the projector lens and the center of the screen.
2. Record the approximate vertical angle of incidence of the front of the projector lens to the center of the screen.
3. Record the approximate horizontal angle of incidence of the front of the projector lens to the center of the screen.
4. Record the distance between the front of the colorimeter lens and the center of the screen.
5. Record the approximate vertical angle of incidence of the front of the colorimeter lens to the center of the screen.
6. Record the approximate horizontal angle of incidence of the front of the colorimeter lens to the center of the screen.
7. Record the size of the screen.
8. Record the approximate gain of the screen.
9. Record the perforation configuration of the screen.
10. With the projector lamp switched off (or doused), record the luminance at the center of the screen in units of Cd/m 2.

### Consolidated Test Sequences

☐

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 14.2. Projector Test Sequence | Data only | — | — |

# Chapter 8. Screen Management System

A Screen Management System (SMS) (or Theater Management System (TMS)) is responsible for providing the operator's interface for ingest, scheduling, reporting, etc. In this document the term SMS will be used exclusively, although the same test procedures can apply to a TMS that is able to directly manage a suite of equipment for a screen.

The SMS is not hosted on secure hardware (*i.e.*, it is not required to be within an SPB).

## 8.1. Ingest and Storage

### 8.1.1. Storage System Ingest Interface

#### Objective

Verify that the system provides an interface to the storage system, for DCP ingest, that is Ethernet, 1Gb/s or better, over copper (1000Base-T) or fiber (1000Base-FX), as described in [IEEE-802-3], running the TCP/IP protocol.

#### Procedures

1. Use a computer with the appropriate interface cards, *e.g.*, 1000Base-T copper Ethernet and network analysis tools such as Wireshark installed, to tap the ingest interface.

2. Ingest *DCI 2K StEM Test Sequence (Encrypted)* and verify that the packets can be read by the computer that runs the network analysis tools. Failure to observe the packets contained in the DCP is cause to fail this test.

3. Verify that the data packets read are valid TCP/IP data packets. Use of any other protocol to ingest the DCP is cause to fail this test.

#### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 6.2.3<br>IEEE-802-3 |
| **Test Equipment** | **Network Analyzer** |
| **Test Materials** | *DCI 2K StEM Test Sequence (Encrypted)* |

#### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.1.2. Storage System Capacity

### Objective

Verify that the storage system available to the SMS has a capacity of at least 1TByte of content.

### Procedures

Verify that the storage system has the capacity to hold at least 1TByte of content. This can be done in three ways:

1. Verify by using the specification of the manufacturer.

2. Examine the capacity of the file system representing the storage system, and verify that there is enough available storage to hold 1 TByte of content data. Use appropriate file system tools to perform this task.

3. Measure the storage capacity by copying 1TByte of content to the storage and verifying that no content has been purged by playing back all content.

If the capacity of the storage system is less than 1TByte, this is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.2.3.11 |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.1.3. Storage System Redundancy

### Objective

Verify that the storage system available to the SMS provides redundancy in the case of hard disk failure.

### Procedures

Verify the existence and functionality of an appropriate RAID configuration by performing the following:

1. Ingest the composition *DCI 2K StEM (Encrypted) i.e.*, load it into the storage system.
2. Power down the system.
3. Disconnect one hard drive of the RAID configuration.
4. Re-power the system.
5. Set up and play a show that contains the composition *DCI 2K StEM (Encrypted)*, keyed with *KDM for 2K StEM (Encrypted)* and verify that playback is successful, *i.e.*, playback can be started, is not interrupted and does not show any picture or sound artifacts. Unsuccessful playback is cause to fail this test.
6. Power down the system and reconnect the hard drive that was disconnected in step 3.
7. Repower the system and perform any necessary manufacturer-specified procedures to restore the RAID configuration to normal.
8. Repeat steps 2 through 7 for all other drives contained in the storage system.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.5.3.2 |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.1.4. Storage System Performance

### Objective

Verify that the storage system available to the SMS is able to sustain a minimum peak data rate of 307 MBit/sec to allow for uninterrupted digital cinema playback.

### Procedures

1. Setup and play the composition *2K DCI Maximum Bitrate Composition (Encrypted)*, keyed with *KDM for 2K Maximum Bitrate Composition (Encrypted)*. This composition starts with a count to check synchronization between picture and sound. 10 minutes of an image with minimal compression and 16 audio channels (each 24 bit per sample, 96 kHz) follows, then a second synchronization count. The content between the synchronization counts will require the maximum allowable data rate for successful reproduction.

2. Verify that playback is successful, *i.e.*, playback can be started, is not interrupted and does not show any picture or sound artifacts. Unsuccessful playback is cause to fail this test.

3. Extract the logs from the Test Subject and examine the associated `FrameSequencePlayed` and `PlayoutComplete` events recorded during the playback for complete and successful reproduction. Any exceptions or missing `FrameSequencePlayed` or `PlayoutComplete` events are cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.5.3.3, 7.5.3.4, 7.5.3.6 |
| **Test Materials** | *2K DCI Maximum Bitrate Composition (Encrypted)*<br>*KDM for 2K Maximum Bitrate Composition (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.1.5. Storage System Redundancy (OBAE)

### Objective

Verify that the storage system available to the OBAE-capable SMS provides redundancy in the case of hard disk failure.

### Procedures

Verify the existence and functionality of an appropriate RAID configuration by performing the following:

1. Ingest the composition *DCI 2K StEM (OBAE) (Encrypted) i.e.*, load it into the storage system.

2. Power down the system.

3. Disconnect one hard drive of the RAID configuration.

4. Re-power the system.

5. Set up and play a show that contains the composition *DCI 2K StEM (OBAE) (Encrypted)*, keyed with *KDM for 2K StEM (Encrypted) (OBAE)* and verify that playback is successful, *i.e.*, playback can be started, is not interrupted and does not show any picture or sound artifacts. Unsuccessful playback is cause to fail this test.

6. Power down the system and reconnect the hard drive that was disconnected in step 3.

7. Repower the system and perform any necessary manufacturer-specified procedures to restore the RAID configuration to normal.

8. Repeat steps 2 through 7 for all other drives contained in the storage system.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.5.3.2<br>OBAE-ADD |
| **Test Materials** | *DCI 2K StEM (OBAE) (Encrypted)*<br>*KDM for 2K StEM (Encrypted) (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 8.1.6. Storage System Performance (OBAE)

### Objective

Verify that the storage system available to the OBAE-capable SMS allows uninterrupted playback of maximum bitrate content.

### Procedures

1. Setup and play the composition *2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)*, keyed with *KDM for 2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)*. This composition requires the maximum allowable data rate for successful reproduction.

2. Verify that playback is successful, *i.e.*, playback can be started, is not interrupted and does not show any picture or sound artifacts. Unsuccessful playback is cause to fail this test.

3. Extract the logs from the Test Subject and examine the associated `FrameSequencePlayed` and `PlayoutComplete` events recorded during the playback for complete and successful reproduction. Any exceptions or missing `FrameSequencePlayed` or `PlayoutComplete` events are cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.5.3.3, 7.5.3.4, 7.5.3.6<br>OBAE-ADD |
| **Test Materials** | *2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)*<br>*KDM for 2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

# 8.2. Screen Management System

## 8.2.1. Deleted Section

The section "Screen Management System" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 8.2.2. Show Playlist Creation

### Objective

- Verify that the SMS provides the necessary functions for managing Composition Play Lists (CPLs) and for assembling them into shows (SPL creation).
- Verify that the SMS allows only authorized persons to build a Show Playlist (SPL).

### Procedures

1. Ingest the composition *DCI 2K StEM* into the system.
2. Using the system, locate the composition *DCI 2K StEM*.
3. Create a new Show Play List (SPL) and add *DCI 2K StEM* twice to the show. The two instances of *DCI 2K StEM* are herein referred to as *DCI 2K StEM* X and *DCI 2K StEM* Y.
4. Ingest the composition *DCI 2K StEM (Encrypted)* and the KDM *KDM for 2K StEM (Encrypted)* into the system.
5. Using the system, locate the composition *DCI 2K StEM (Encrypted)*.
6. Append the composition *DCI 2K StEM (Encrypted)* to the end of the show.
7. In the show, move the composition *DCI 2K StEM (Encrypted)* in between *DCI 2K StEM* X and *DCI 2K StEM* Y.
8. Ingest *DCI Black Spacer - 5 seconds* and insert it between each of the compositions in the show.
9. Start playback and verify that the presentation proceeds as expected and the inserted black frames and silence are presented correctly.
10. Attempt to delete each of the compositions *DCI 2K StEM*, *DCI 2K StEM (Encrypted)* and *DCI Black Spacer - 5 seconds* from system storage. The system is required to warn that the content is part of a current show and not allow deletion.
11. Wait until playback is completed.

12. Remove *DCI 2K StEM* X from the show.

13. Attempt to delete *DCI 2K StEM* from storage. It is expected that the SMS warns the user that this composition is part of an SPL.

14. Delete the show then delete *DCI 2K StEM* and *DCI 2K StEM (Encrypted)*. It is expected that this operation succeeds.

15. Verify that the aforementioned compositions have been removed.

16. Verify that the above functions for assembling content into an SPL are executable with an easy to use graphical user interface.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.2.3.5, 7.2.3.7, 7.3.4, 7.4.1.1, 7.4.1.2, 7.4.1.3, 7.4.1.4, 7.4.1.5, 7.4.1.6 |
| **Test Materials** | *DCI 2K StEM*<br>*DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)*<br>*DCI Black Spacer - 5 seconds* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Data only | — | — |
| 15.2. Projector with MB Test Sequence | Data only | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.2.3. Show Playlist Format

### Objective

Verify that the SMS supports the required Show Playlist Format.

### Procedures

1. Export the Show Playlist (SPL) to external media.

2. Use the software command **schema-check** to verify that the SPL exported in the above step is well formed XML. XML format errors are cause to fail this test. An example is shown below.

```
$ schema-check <input-file>
schema validation successful
```

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.3, 7.4.1.6 |
| **Test Equipment** | **schema-check** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.2.4. Deleted Section

The section "KDM Validity Checks" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 8.2.5. Automation Control and Interfaces

### Objective

Verify that the SMS supports theater automation interface via any one or more of:

- contact closures (general purpose I/O)
- serial data interface
- network (*e.g.*, Ethernet)

### Procedures

1. Configure an automation test setup that allows the Test Subject to signal an event using a visible state change (*e.g.* an L.E.D.), and allows the Test Subject to be signalled via external stimulus (*e.g.*, an SPST switch).
2. Verify that the Test Subject can change the state of the event indicator at pre-determined times using the playlist. Failure to meet this requirement shall be cause to fail this test.
3. Verify that playback of a playlist on the Test Subject can be started by external stimulus. Failure to meet this requirement shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.3.4, 7.4.1.6, 7.4.1.7, 7.5.7.2 |
| **Test Equipment** | **DCI Projector**<br>**GPIO Test Fixture** |
| **Test Materials** | *DCI 2K StEM Test Sequence* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.2.6. Interrupt Free Playback

### Objective

Verify that the system can play a sequence of CPLs (a Show Playlist) without noticeable interruptions such as unexpected pauses or visual or audible artifacts.

### Procedures

To verify that playback is possible without any interruptions:

1. Assemble a show containing the compositions *4K DCI NIST Frame with silence*, *DCI 5.1 Channel Identification DCI 2K Sync test with Subtitles (Encrypted)* and *DCI 2K StEM (Encrypted)*, keyed with *KDM for DCI 2K Sync Test with Subtitles (Encrypted)* and *KDM for 2K StEM (Encrypted)*

2. Play back the show. Verify that playback succeeds and is completed without any image or sound distortions and without any interruption. Incomplete or interrupted playback or the presence of distortions or artifacts shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.4.1.8 |
| **Test Materials** | *4K DCI NIST Frame with silence*<br>*DCI 5.1 Channel Identification*<br>*DCI 2K Sync test with Subtitles (Encrypted)*<br>*DCI 2K StEM (Encrypted)*<br>*KDM for DCI 2K Sync Test with Subtitles (Encrypted)*<br>*KDM for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.2.7. Artifact Free Transition of Image Format

### Objective

Verify artifact free transition between differing pixel array sizes.

### Procedures

To verify that mode transitions do not cause any artifacts:

1. Assemble a Show that contains 3 repetitions of the following 2 compositions *DCI 2K Image with Frame Number Burn In (Flat)*, which contains two reels of 1.85:1 content, followed by *DCI 2K Image with Frame Number Burn In (Scope)*, which contains two reels of 2.39:1 content.

2. Start playback and observe the projected image. Transitions between reels and compositions are announced visually by means of a burned-in counter. Verify that for all transitions, no visible artifacts, *e.g.*, rolling, flashes, distorted images etc, are visible, and that every frame is displayed correctly on each outgoing and incoming transition. If any visible artifact is present or any incoming or outgoing frame is not displayed, this is cause to fail the test. *Note: Use of a camera to shoot the display off screen to confirm display of all frames can be helpful in this test*.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.4.1.6 |
| **Test Materials** | *DCI 2K Image with Frame Number Burn In (Flat)*<br>*DCI 2K Image with Frame Number Burn In (Scope)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 8.2.8. Restarting Playback

### Objective

Verify that power failures cause the system to enter a stable stop/idle condition and that the system provides the ability to restart playback at a point prior to a power interruption.

### Procedures

1. Load *DCI 2K Image with Frame Number Burn In (Encrypted)* and *KDM for DCI 2K Image with Frame Number Burn In (Encrypted)*, then assemble and start a show.

2. Interrupt the presentation by interrupting the Test Subject's power supply. If possible, the projector power supply should not be interrupted as this may cause overheating and damage the projector.

3. Re-establish power and verify that the system enters a stable stop/idle state. Failure to meet this requirement is cause to fail this test.

4. Verify that the system notifies the user that the last playback was abnormally interrupted, and offers the possibility of restarting the show. Failure to meet this requirement is cause to fail this test.

5. Attempt to restart the presentation at a point prior to the power interruption and verify that the restart was successful. Failure to meet this requirement is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.2.3.13, 7.4.1.2, 7.4.1.8 |
| **Test Materials** | *KDM for DCI 2K Image with Frame Number Burn In (Encrypted)*<br>*DCI 2K Image with Frame Number Burn In (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.2.9. SMS User Accounts

### Objective

Verify that the SMS supports multiple levels of user accounts.

### Procedures

1. Study the user manual to discover factory-created account names and passwords.

2. If required by the system, create the necessary operating accounts.

3. Return the system to the "logged out" state.

4. For each account, log on to the system using the account information and note the privileges available to the account user (*e.g.*, run show, load content, create account, etc.). Failure of the system to provide privilege separation using distinct user accounts is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.4.1.3 |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | Record the available operator roles (names) and whether locally-defined accounts can be created. |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | Record the available operator roles (names) and whether locally-defined accounts can be created. |
| 20.2. OMB Test Sequence | Pass/Fail | — | Record the available operator roles (names) and whether locally-defined accounts can be created. |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.2.10. SMS Operator Identification

### Objective

Verify that the security system requires the SMS and SMS operator to be identified to the Security Manager.

### Procedures

1. List all the methods available to the Test Subject that can cause playback of a composition or show. This could include any preset or created user accounts/logins to the SMS/TMS, direct command, *e.g.*, by front panel controls or automation inputs and events initiated by an automatic scheduler. Manufacturer-supplied documentation, including manuals, may be consulted to assist with this step.

2. For each of the cases from the list created in Step 1, cause the composition *DCI 2K StEM (Encrypted)*, or a show that contains it, to play back. Record the time of day at the end of each playback.

3. Retrieve the audit logs from the system.

4. By using the time values recorded in Step 2, for each of the cases from the list created in Step 1:

    a. Locate the corresponding `FrameSequencePlayed` playout events.

    b. Verify that there is a `FrameSequencePlayed` event for both audio and image and that they each contain a parameter named `AuthId` with a value that is not absent.

    c. Record each `AuthId` value. Any missing `AuthId` parameter or any `AuthId` parameter that has a value that is unpopulated is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.1.1 |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*KDM for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.2.11. SMS Identity and Certificate

### Objective

Verify that the SMS carries a [SMPTE-430-2] compliant digital certificate to identify the SMS entity to the SM. Verify that the SMS certificate indicates either the `SMS` role, or the `TMS` role, unless the SMS is contained within an SPB meeting the protection requirements for any other designated roles.

### Procedures

1. Obtain the SMS certificate (and chain if available):
    - If the SMS communicates with the SM via a network accessible to test equipment, use network analysis tools (*e.g.*, Wireshark) to monitor the packets exchanged between the SMS and SM and extract the leaf certificate and, if present, the associated signing certificate(s). If signing certificates are not present, obtain them from the manufacturer.
    - If network monitoring is not possible, obtain the complete certificate chain from the manufacturer.
2. Extract the Subject Common Name field from the leaf certificate collected in step 1. Failure for the Common Name to include either the `SMS` role, or the `TMS` role, is cause to fail the test.
3. Verify that the Subject Common Name field of the leaf certificate collected in step 1 contains the serial number of the Test Subject. Additional identifying information may be present. Failure of this verification is cause to fail the test.
4. Verify that information identifying the make and model of the Test Subject is carried in the Subject field of the certificate collected in step 1. Additional identifying information may be present. Failure of this verification is cause to fail the test.
5. Verify that either the make, model and serial number of the Test Subject, or information that is unambiguously traceable by the manufacturer to the Subject field from the leaf certificate obtained in step 1, is clearly placed on the exterior of the device containing the Test Subject. Failure of this verification is cause to fail the test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.2.5, 9.5.1 |
| **Test Equipment** | **Network Analyzer**<br>**openssl** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 8.2.12. Content Keys and TDL check

### Objective

1. Verify that the SMS, working with the security infrastructure, checks that, prior to initiating playback of a Show Playlist (scheduled exhibition), (i) all content keys required for the playback of the Show Playlist are available and valid, and (ii) the suite equipment to be used or the playback of the Show Playlist is included on the TDL.

2. Verify that the SMS does this check for every composition individually.

### Procedures

With the test materials specified below, perform the following procedures:

1. Try to assemble and play a show using *DCI 2K StEM (Encrypted)* without providing a KDM. If playback begins this is cause to fail this test.

2. Try to assemble and play a show using *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)* and *DCI 2K StEM (Encrypted)*, keyed with *KDM with incorrect message digest* in that order. The KDM *KDM with incorrect message digest* is invalid (wrong signature/hash error). If playback begins this is cause to fail this test.

3. Try to assemble and play a show using *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)* and *DCI 2K StEM (Encrypted)*, keyed with *KDM that has expired* which contains an expired time window. If playback begins this is cause to fail this test.

4. Try to assemble and play a show using *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)* and *DCI 2K StEM (Encrypted)*, keyed with *KDM with future validity period* which contains a time window in the future. If playback begins this is cause to fail this test.

5. Try to assemble and play a show using *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)* and *DCI 2K StEM (Encrypted)*, keyed with *KDM with invalid XML* which contains an XML malformation. If playback begins this is cause to fail this test.

6. Try to assemble and play a show using *DCI 2K Sync Test (Encrypted)*, with *KDM for DCI 2K Sync Test (Encrypted)* and *DCI 2K StEM (Encrypted)*, keyed with *KDM with empty TDL*, which is a KDM that does not list any trusted devices in its TDL. If playback begins this is cause to fail this test.

7. Try to assemble and play a show using *DCI 2K Sync Test (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (Encrypted)* and *DCI 2K StEM (Encrypted)*, keyed with *KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)*, which is a KDM that carries only the "assume trust" empty-string thumbprint. Attempt to play the composition and record the result. If playback does not begin this is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.2<br>SMPTE-430-1 |
| **Test Materials** | *DCI 2K StEM (Encrypted)*<br>*DCI 2K Sync Test (Encrypted)*<br>*KDM for DCI 2K Sync Test (Encrypted)*<br>*KDM with incorrect message digest*<br>*KDM that has expired*<br>*KDM with future validity period*<br>*KDM with invalid XML*<br>*KDM with empty TDL*<br>*KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 8.2.13. Content Keys and TDL check (OBAE)

### Objective

1. Verify that the SMS checks that, prior to initiating playback of a Show Playlist that contains OBAE content, (i) all content keys required for the playback of the Show Playlist are available and valid, and (ii) the suite equipment to be used for the playback of the Show Playlist is included on the TDL.

2. Verify that the SMS does this check for every composition individually.

**Note:**
Two instances of each KDM listed below are needed if the Test Subject includes an OMB: one instance of each KDM for the IMB and one instance of each KDM for the OMB.

### Procedures

With the test materials specified below, perform the following procedures:

1. Try to assemble and play a show using *DCI 2K StEM (OBAE) (Encrypted)* without providing a KDM. If playback begins this is cause to fail this test.

2. Try to assemble and play a show using *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)* and *DCI 2K StEM (OBAE) (Encrypted)*, keyed with *KDM with incorrect message digest (OBAE)* in that order. If playback begins this is cause to fail this test.

3. Try to assemble and play a show using *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)* and *DCI 2K StEM (OBAE) (Encrypted)*, keyed with *KDM that has expired (OBAE)*. If playback begins this is cause to fail this test.

4. Try to assemble and play a show using *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)* and *DCI 2K StEM (OBAE) (Encrypted)*, keyed with *KDM with future validity period (OBAE)*. If playback begins this is cause to fail this test.

5. Try to assemble and play a show using *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)* and *DCI 2K StEM (OBAE) (Encrypted)*, keyed with *KDM with invalid XML (OBAE)*. If playback begins this is cause to fail this test.

6. Try to assemble and play a show using *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)* and *DCI 2K StEM (OBAE) (Encrypted)*, keyed with *KDM with empty TDL (OBAE)*. If playback begins this is cause to fail this test.

7. Try to assemble and play a show using *DCI 2K Sync Test (OBAE) (Encrypted)*, keyed with *KDM for DCI 2K Sync Test (OBAE) (Encrypted)* and *DCI 2K StEM (OBAE) (Encrypted)*, keyed with *KDM with Assume Trust TDL Entry (OBAE)*. If playback does not begin this is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.2<br>SMPTE-430-1 |
| **Test Materials** | *DCI 2K StEM (OBAE) (Encrypted)*<br>*DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test (OBAE) (Encrypted)*<br>*KDM with incorrect message digest (OBAE)*<br>*KDM that has expired (OBAE)*<br>*KDM with future validity period (OBAE)*<br>*KDM with invalid XML (OBAE)*<br>*KDM with empty TDL (OBAE)*<br>*KDM with Assume Trust TDL Entry (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 8.2.14. KDM Content Keys Check

### Objective

Verify that the SMS checks that, prior to initiating playback of a Show Playlist, content keys carried in the KDM associated with a CPL included in the Show Playlist match exactly those content keys used by the CPL.

### Procedures

For each of the rows of Table 8.1, create a Show Playlist with the *Composition* and attempt to play it using the *Malformed KDM*. If playback begins this is cause to fail this test.

### Table 8.1.List of Compositions and associated KDMs with mismatched content keys

| Composition | Malformed KDM |
|---|---|
| sync_test_with_subs_ct.cpl.xml | m0100_missing_key_pict.kdm.xml |
| sync_test_with_subs_ct.cpl.xml | m0102_missing_key_snd.kdm.xml |
| sync_test_with_subs_ct.cpl.xml | m0104_missing_key_sub.kdm.xml |
| 2K_sync_test_with_subs_obae_ct.cpl.xml | m0106_missing_key_pict_obae.kdm.xml |
| 2K_sync_test_with_subs_obae_ct.cpl.xml | m0108_missing_key_snd_obae.kdm.xml |
| 2K_sync_test_with_subs_obae_ct.cpl.xml | m0110_missing_key_sub_obae.kdm.xml |
| 2K_sync_test_with_subs_obae_ct.cpl.xml | m0112_missing_key_obae_obae.kdm.xml |

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.3.6.4<br>SMPTE-430-1 |
| **Test Equipment** | **Accurate Real-Time Clock**<br>**Text Editor** |
| **Test Materials** | *DCI 2K Sync test with Subtitles (Encrypted)*<br>*DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync test with Subtitles (Encrypted): missing picture essence key*<br>*KDM for DCI 2K Sync test with Subtitles (Encrypted): missing sound essence key*<br>*KDM for DCI 2K Sync test with Subtitles (Encrypted): missing subtitle essence key*<br>*KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing picture essence key*<br>*KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing sound essence key*<br>*KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing picture subtitle key*<br>*KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing OBAE key* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |

| | | | |
|---|---|---|---|
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |

## 8.2.15. Validity of SMS Certificates

### Objective

Verify that the SMS certificates are valid.

### Procedures

1. Obtain the SMS certificate (and chain if available):
    - If the SMS communicates with the SM via a network accessible to test equipment, use network analysis tools (*e.g.*, Wireshark) to monitor the packets exchanged between the SMS and SM and extract the leaf certificate and, if present, the associated signing certificate(s). If signing certificates are not present, obtain them from the manufacturer.
    - If network monitoring is not possible, obtain the complete certificate chain from the manufacturer.
2. For each certificate, perform the following tests:
    - 2.1.1. Basic Certificate Structure
    - 2.1.2. SignatureAlgorithm Fields
    - 2.1.3. SignatureValue Field
    - 2.1.4. SerialNumber Field
    - 2.1.5. SubjectPublicKeyInfo Field
    - 2.1.6. Deleted Section
    - 2.1.7. Validity Field
    - 2.1.8. AuthorityKeyIdentifier Field
    - 2.1.9. KeyUsage Field
    - 2.1.10. Basic Constraints Field
    - 2.1.11. Public Key Thumbprint
    - 2.1.12. Organization Name Field
    - 2.1.13. OrganizationUnitName Field

- 2.1.14. Entity Name and Roles Field
- 2.1.15. Unrecognized Extensions
- 2.1.16. Signature Validation

3. For the complete chain of signer certificates, perform 2.1.17. Certificate Chains

Failure of any of these above conditions is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.2.5, 9.5.1<br>SMPTE-430-2 |
| **Test Equipment** | **Network Analyzer**<br>**openssl** |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 13.2. Server Test Sequence | Pass/Fail | — | — |
| 15.2. Projector with MB Test Sequence | Pass/Fail | — | — |
| 17.2. Server Confidence Sequence | Pass/Fail | — | — |
| 19.2. Projector with MB Confidence Sequence | Pass/Fail | — | — |
| 20.2. OMB Test Sequence | Pass/Fail | — | — |
| 21.2. Digital Cinema Projector with IMBO Test Sequence | Pass/Fail | — | — |
| 22.2. OMB Confidence Sequence | Pass/Fail | — | — |
| 23.2. Digital Cinema Projector with IMBO Confidence Sequence | Pass/Fail | — | — |

## 8.2.16. Interrupt Free Playback (OBAE)

### Objective

Verify that the OBAE-capable system can play a sequence of CPLs (a Show Playlist) without noticeable interruptions such as unexpected pauses or visual or audible artifacts.

### Procedures

To verify that playback is possible without any interruptions:

1. Assemble a show containing the compositions:
   - *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* keyed with *KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*

- *OBAE Rendering Expectations (Clip)*
- *DCI 2K StEM (OBAE) (Encrypted)* keyed with *KDM for 2K StEM (Encrypted) (OBAE)*

2. Play back the show. Verify that playback succeeds and is completed without any image or sound distortions and without any interruption. Incomplete or interrupted playback or the presence of distortions or artifacts shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.4.1.8<br>OBAE-ADD |
| **Test Materials** | *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*<br>*KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*<br>*OBAE Rendering Expectations (Clip)*<br>*DCI 2K StEM (OBAE) (Encrypted)*<br>*KDM for 2K StEM (Encrypted) (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 8.2.17. Restarting Playback (OBAE)

### Objective

Verify that power failures cause the system to enter a stable stop/idle condition and that the OBAE-capable system provides the ability to restart playback at a point prior to a power interruption.

### Procedures

1. Load *DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)* and *KDM for DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)*, then assemble and start a show.

2. Interrupt the presentation by interrupting the Test Subject's power supply. If possible, the projector power supply should not be interrupted as this may cause overheating and damage the projector.

3. Re-establish power and verify that the system enters a stable stop/idle state. Failure to meet this requirement is cause to fail this test.

4. Verify that the system notifies the user that the last playback was abnormally interrupted, and offers the possibility of restarting the show. Failure to meet this requirement is cause to fail this test.

5. Attempt to restart the presentation at a point prior to the power interruption and verify that the restart was successful. Failure to meet this requirement is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.2.3.13, 7.4.1.2, 7.4.1.8<br>OBAE-ADD |
| **Test Materials** | *KDM for DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)*<br>*DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 8.2.18. Show Playlist Creation (OBAE)

### Objective

- Verify that the OBAE-capable SMS provides the necessary functions for managing Composition Play Lists (CPLs) and for assembling them into shows (SPL creation).
- Verify that the OBAE-capable SMS allows only authorized persons to build a Show Playlist (SPL).

### Procedures

1. Ingest the composition *DCI 2K StEM (OBAE)* into the system.
2. Using the system, locate the composition *DCI 2K StEM (OBAE)*.
3. Create a new Show Play List (SPL) and add *DCI 2K StEM (OBAE)* twice to the show. The two instances of *DCI 2K StEM (OBAE)* are herein referred to as *DCI 2K StEM (OBAE)* X and *DCI 2K StEM (OBAE)* Y.
4. Ingest the composition *DCI 2K StEM (OBAE) (Encrypted)* and the KDM *KDM for 2K StEM (Encrypted) (OBAE)* into the system.
5. Using the system, locate the composition *DCI 2K StEM (OBAE) (Encrypted)*.
6. Append the composition *DCI 2K StEM (OBAE) (Encrypted)* to the end of the show.
7. In the show, move the composition *DCI 2K StEM (OBAE) (Encrypted)* in between *DCI 2K StEM (OBAE)* X and *DCI 2K StEM (OBAE)* Y.
8. Ingest *DCI Black Spacer - 5 seconds* and insert it between each of the compositions in the show.
9. Start playback and verify that the presentation proceeds as expected and the inserted black frames and silence are presented correctly.
10. Attempt to delete each of the compositions *DCI 2K StEM (OBAE)*, *DCI 2K StEM (Encrypted)* and *DCI Black Spacer - 5 seconds* from system storage. The system is required to warn that the content is part of a current show and not allow deletion.
11. Wait until playback is completed.

12. Remove *DCI 2K StEM (OBAE)* X from the show.

13. Attempt to delete *DCI 2K StEM (OBAE)* from storage. It is expected that the SMS warns the user that this composition is part of an SPL.

14. Delete the show then delete *DCI 2K StEM (OBAE)* and *DCI 2K StEM (OBAE) (Encrypted)*. It is expected that this operation succeeds.

15. Verify that the aforementioned compositions have been removed.

16. Verify that the above functions for assembling content into an SPL are executable with an easy to use graphical user interface.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.2.3.5, 7.2.3.7, 7.3.4, 7.4.1.1, 7.4.1.2, 7.4.1.3, 7.4.1.4, 7.4.1.5, 7.4.1.6<br>OBAE-ADD |
| **Test Materials** | *DCI 2K StEM (OBAE)*<br>*DCI 2K StEM (OBAE) (Encrypted)*<br>*KDM for 2K StEM (Encrypted) (OBAE)*<br>*DCI Black Spacer - 5 seconds* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Data only | — | — |

## 8.2.19. Automation Control and Interfaces (OBAE)

### Objective

Verify that the OBAE-capable SMS supports theater automation interface via any one or more of:

- contact closures (general purpose I/O)
- serial data interface
- network (*e.g.*, Ethernet)

### Procedures

1. Configure an automation test setup that allows the Test Subject to signal an event using a visible state change (*e.g.* an L.E.D.), and allows the Test Subject to be signalled via external stimulus (*e.g.*, an SPST switch).

2. Verify that the Test Subject can change the state of the event indicator at pre-determined times using the playlist. Failure to meet this requirement shall be cause to fail this test.

3. Verify that playback of a playlist on the Test Subject can be started by external stimulus. Failure to meet this requirement shall be cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.3.4, 7.4.1.6, 7.4.1.7, 7.5.7.2<br>OBAE-ADD |
| **Test Equipment** | **DCI Projector**<br>**GPIO Test Fixture** |
| **Test Materials** | *DCI 2K StEM (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

## 8.2.20. SMS Operator Identification (OBAE)

### Objective

Verify that the security system requires the SMS and SMS operator to be identified to the OBAE-capable Security Manager.

### Procedures

1. List all the methods available to the Test Subject that can cause playback of a composition or show. This could include any preset or created user accounts/logins to the SMS/TMS, direct command, *e.g.*, by front panel controls or automation inputs and events initiated by an automatic scheduler. Manufacturer-supplied documentation, including manuals, may be consulted to assist with this step.

2. For each of the cases from the list created in Step 1, cause the composition *DCI 2K StEM (OBAE) (Encrypted)*, or a show that contains it, to play back. Record the time of day at the end of each playback.

3. Retrieve the audit logs from the system.

4. By using the time values recorded in Step 2, for each of the cases from the list created in Step 1:

    a. Locate the corresponding `FrameSequencePlayed` playout events.

    b. Verify that there is a `FrameSequencePlayed` event for both audio and image and that they each contain a parameter named `AuthId` with a value that is not absent.

    c. Record each `AuthId` value. Any missing `AuthId` parameter or any `AuthId` parameter that has a value that is unpopulated is cause to fail this test.

### Supporting Materials

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.1.1<br>OBAE-ADD |

| | |
|---|---|
| **Test Materials** | *DCI 2K StEM (OBAE) (Encrypted)*<br>*KDM for 2K StEM (Encrypted) (OBAE)* |

### Consolidated Test Sequences

| Sequence | Type | Conditions | Measured Data |
|---|---|---|---|
| 20.2. OMB Test Sequence | Pass/Fail | — | — |

[This Page Left Blank Intentionally]

# Part II. Design Evaluation Guidelines

## Chapter 9. FIPS Requirements for a Type 1 SPB

Type 1 Secure Processing Blocks (SPB) are required by DCI to conform to a U.S. National Institute of Standards and Technology (NIST) FIPS 140 version in effect at the time of DCI compliance testing. Testing for compliance with FIPS 140 is performed by independent laboratories accredited by NIST NVLAP.

In May 2019, NIST announced the plan and schedule to migrate the security requirements for cryptographic modules from FIPS 140-2 to FIPS 140-3. In order to simplify accommodation of this Chapter 9. FIPS Requirements for a Type 1 SPB for FIPS 140-2 and FIPS 140-3 (and references to these documents throughout the CTP), FIPS 140-2 and FIPS 140-3 references have been revised to refer generically to *FIPS 140*, unless otherwise noted.

The testing program, known as the Cryptographic Module Validation Program (CMVP), is a joint effort of NIST's Computer Systems Laboratory (CSL) and the Communications Security Establishment (CSE) of the Government of Canada. More information about CMVP can be found on the NIST web site at http://csrc.nist.gov/groups/STM/. To be compliant with the DCI System Specification, a Type 1 SPB device must be tested by an accredited laboratory, the resulting documentation must be submitted to NIST/CSE for examination, and a validation certificate must be issued by NIST/CSE. Throughout this document, the term "FIPS 140-2 testing" will refer to this entire process.

FIPS 140 testing is very thorough but also very selective. To determine whether Type 1 SPB meets the DCI requirements, the documents prepared for and presented to the FIPS testing lab by the manufacturer must be reviewed by an examiner as guided by the requirements presented in this chapter. This chapter will briefly explain the FIPS testing process and the documentation that is produced. A procedure will be presented that will guide the examiner through the task of evaluating a FIPS 140 test report and determining the DCI compliance status of the respective Test Subject.

### 9.1. FIPS Testing Procedures

This section will explain the process of obtaining a FIPS 140 validation certificate from NIST/CSE. This information is intended to guide the examiner in understanding the documentation that will be produced in that process. This information is not exhaustive and is not intended to guide a manufacturer in obtaining a validation certificate. The following sub-sections illustrate the tasks in a typical validation process.

**Accredited Laboratory**

FIPS 140 testing is performed by an accredited laboratory. This Cryptographic Modules Testing (CMT) laboratory will assist the manufacturer in preparing the required documentation and will test sample devices for conformance to the documentation. The CMT laboratory may help the manufacturer resolve compliance issues in the design, but this help is limited to comments on proposed designs, actual design participation may not occur. The documentation and test reports may be submitted to NIST/CSE by the CMT laboratory or the manufacturer.

NIST makes available the list of accredited CMT laboratories on the agency web site (see http://csrc.nist.gov/groups/STM/testing_labs/index.html). Any of the laboratories can be used, but some restrictions may apply. For example, a laboratory that is owned by the Test Subject manufacturer or one that contributed to the design of the Test Subject will be disqualified from testing that Test Subject. More information about CMT laboratories and laboratory selection can be found in *Frequently Asked Questions for the Cryptographic Module Validation Program* (http://csrc.nist.gov/groups/STM/cmvp/documents/ CMVPFAQ.pdf).

**Note:**
The FIPS 140 validation test report prepared by the CMT laboratory is a proprietary and closely controlled document. The manufacturer must ensure that it has permission to disclose the test report to the DCI Testing Organization.

**Standards and Supporting Documentation**

The manufacturer must obtain and understand all of the NIST documentation that is relevant to the FIPS 140 testing process. In addition to the documentation about the validation process itself, the manufacturer will also need documentation which addresses the requirements for particular algorithms implemented in the device.

**Security Element Documentation**

All design elements which are addressed by FIPS 140, *e.g.*, cryptographic algorithms and Critical Security Parameters (CSP), must be documented and tested according to CMT procedures. The manufacturer must work with the testing lab to identify all such design features and prepare the required documentation.

**Design Modification**

The Cryptographic Algorithm Validation Program (CAVP) and CMVP validation testing processes may require design modifications to the cryptographic module hardware, software, firmware, or documentation. The CMT laboratory performing the validation testing identifies the compliance issues, but does not design or redesign the cryptographic module with the manufacturer, or for the manufacturer.

**Note:**
The manufacturer is responsible for implementing a compliant design, and submitting required testing evidence to the CMT laboratory for review and testing

**Test Subject Instrumentation**

Where it is not possible to test a particular subsystem from outside the module (*e.g.*, the seed method for a random number generator), the manufacturer must provide the instrumentation necessary to allow the laboratory to test the subsystem. A simulator may be used, for example, to prove the correct functioning of microcode for an ASIC or FPGA.

Additionally, the manufacturer may be required to develop test jigs to facilitate the error injection process; for example, to simulate tamper events and other hardware failures.

**Operational Testing**

The CMT lab exercises the cryptographic module through all major states, including error states, while monitoring all external ports and interfaces using manufacturer testing tools and equipment. This may require the ability to manipulate program execution and record the contents of memory, thus requiring instrumentation as described above.

**Report Submission**

Upon successful completion of the validation testing (no failed test assertions exist), the CMT laboratory submits a FIPS 140-2 validation report to the CMVP for certification. CMVP personnel examine the submission for correctness, sending any necessary requests for clarification to the CMT laboratory. The submission may be rejected, in which case the manufacturer and laboratory must work to resolve the issue(s) raised and re-submit the validation report. Once the submission is accepted by CMVP, a certificate is issued for the cryptographic module.

The CMVP maintains a list of all cryptographic modules validated to FIPS 140 requirements. This list is published online at http://csrc.nist.gov/groups/STM/cmvp/validation.html. The CMVP also maintains a list of cryptographic modules currently undergoing FIPS 140 testing (a listing on the CMVP pre-validation website does not equate to having a FIPS 140-2 validation). The pre-validation list is at http://csrc.nist.gov/groups/STM/cmvp/inprocess.html.

**Maintenance**

Changes to the module design require re-validation. The effort required to validate an updated design may be small if the design changes are minor.

## 9.2. Submitted Materials

The CMT laboratory will review and analyze design materials during the validation testing process. The following list shows the documents generally expected to be submitted.

- Master Components List (bill of materials); All items submitted as test evidence to the CMT laboratory (*e.g.*, software, firmware, hardware, source code, documentation, etc.) must be specified on the Master Components List, along with a unique identifier and version
- Production grade samples of the cryptographic module (minimum of five for Level 3)
- Security policy
- Data sheets for hardware components
- Listing of all significant information flows
- Finite state model
- Clearly annotated source code
- Functional specifications
- Block diagrams
- Schematics
- VHDL for custom components
- Software design documentation (such as an API or developers guide)
- Mechanical drawings & assembly drawings (approximately to scale)
- Printed circuit board layout drawings
- Cryptographic Key and Critical Security Parameter documentation
- Delivery and operations procedures
- Cryptographic Officer & User guidance
- Configuration management specification
- Operational testing plan(s), and associated testing equipment
- Rationale for exclusion of any components from the security requirements of FIPS 140
- Proof of conformance to FCC Part 15, Subpart B Class A requirements
- CAVP Algorithm validation certificates for all implemented Approved cryptographic algorithms
- Documentation detailing the correspondence of all security rules to the implementation

## 9.3. Test Lab Reports

A FIPS 140 validation test report is created by CMT laboratory engineers for submission to CMVP. The report details the documentation received and the test engineer's evaluation of the implementation's fidelity to the documentation and FIPS 140 requirements. The module tested receives a FIPS 140 validation certificate (i.e., either [FIPS-140-2] or [FIPS-140-3]) once the CMVP reviews and approves the test report.

## 9.4. Interpreting FIPS Test Reports

The CMT laboratory assessments contained within a FIPS 140 validation test report address each of the applicable "TE" requirements corresponding to the eleven areas specified in the FIPS 140 Derived Test Requirements (DTR). These requirements instruct the tester as to what he or she must do in order to test the cryptographic module with respect to the given assertion (which is a statement that must be true for the module to satisfy the requirement of a given area at a given level).

For each applicable FIPS 140 "TE", the tester's assessment includes:

- A statement that the tester verified the requirement was satisfied, or that the requirement is not applicable
- Details on how the tester verified the requirement (*e.g.* through documentation review, source code analysis, physical attack, operational testing, etc.).
- References to supporting design documentation and other test evidence
- References to algorithm standards and CAVP validation certificates as applicable

The DCI Testing Organization must obtain an official copy of the FIPS 140 validation test report directly from the CMT lab that performed the testing. The Test Operator must verify that the name of the cryptographic module and version (software, hardware, firmware) under review are identical to the versions reviewed for the FIPS 140 validation certificate, and supporting CAVP algorithm validation certificate(s).

To confirm whether the cryptographic module satisfies the DCI requirements, the Test Operator must review the "TE" assessments (and associated references as needed) that are relevant to corresponding DCI requirements (the specific assessments are located below with the respective DCI requirements. The functionality described must be consistent with the observed implementation.

## 9.5. DCI Requirements for FIPS Modules

Each of the subsections below describes a DCI requirement that must be proven by examining the FIPS 140 validation report. For each requirement, observe the design of the respective system element (with the aid of the Test Subject Representative) and record whether or not the design meets the requirement.

### 9.5.1. SM Operating Environment

Verify that the Security Manager (SM) operating environment is limited to the FIPS 140 "limited operational" or "non-modifiable operational" environment category.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.2.4, 9.5.2.5, 9.5.2.7<br>FIPS-140-2<br>FIPS-140-3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

| | | |
|---|---|---|
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 9.5.2. LE Key Generation

Verify the following:

1. That, for a Test Subject implementing a Link Encryptor (LE), the Test Subject supports keying of the Link Encryptor (LE) by generating unpredictable keys and having a controlled usage validity period.
2. That, for a Test Subject implementing a Link Encryptor (LE) or Link Decryptor (LD) SE,
    1. Link Encryptor (LE) keys are 112 bits in length for TDES or 128 bits in length for AES, and that those keys are generated according to the requirements of the [DCI-DCSS], Sections 9.7.6 and 9.5.2.5.
    2. Link Encryption is implemented according to [SMPTE-rdd-20]
    3. Link Encryption keys are distributed using the appropriate Standardized Security Messages of [DCI-DCSS], Section 9.4.5.2.4 and, specifically, not distributed using in-band techniques

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.4, 9.5.2.5, 9.7.6<br>FIPS-140-2<br>FIPS-140-3<br>SMPTE-rdd-20 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |

## 9.5.3. SPB Type 1 Tamper Responsiveness

For components of the system designated *Type 1 SPB*, verify the following:

1. That SPBs with access doors or removable covers are monitored 24/7 to assure that in the event of intrusion via such openings the SPB terminates all activity and zeroizes all Critical Security Parameters (CSPs) (see [DCI-DCSS], Section 9.5.2.6).
2. That if the SPB requires a power source to accomplish tamper detection and response, it must zeroize its CSPs prior to any situation arising where such power source may not be available.
3. That log records are not purged in the event of intrusion or other tamper detection

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.2, 9.4.3.6.2.1, 9.4.3.6.3, 9.5.2.2, 9.5.2.5, 9.5.2.6<br>FIPS-140-2<br>FIPS-140-3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 9.5.4. Security Design Description Requirements

For components of the system designated *Type 1 SPB*, verify that equipment suppliers define and describe their respective security designs surrounding the use of port 1173 per the requirements of FIPS 140 "Cryptographic Module Ports and Interfaces" and [DCI-DCSS], Section 9.5.2.5.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.3, 9.5.2.5<br>FIPS-140-2<br>FIPS-140-3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 9.5.5. Deleted Section

The section "SPB1 Tamper Resistance" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 9.5.6. SPB Type 1 FIPS Requirements

For components of the system designated *Type 1 SPB*, verify the following: the component meets and is certified for the requirements of FIPS 140 Level 3 in all areas except those subject to the exceptions or additional notes as specified in [DCI-DCSS], Section 9.5.2.5.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5 |

| |
|---|
| FIPS-140-2<br>FIPS-140-3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 9.5.7. Deleted Section

The section "SPB1 Secure Silicon FIPS Requirements" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 9.5.8. Asymmetric Key Generation

For components of the system designated *Type 1 SPB*, verify that keys are generated as specified in [RFC-3447] and per the requirements of FIPS 140 "Cryptographic Key Management" and the [DCI-DCSS], Section 9.5.2.5.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5, 9.7.6<br>RFC-3447<br>FIPS-140-2<br>FIPS-140-3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 9.5.9. Critical Security Parameter Protection

Verify that the following Critical Security Parameters (CSPs) receive Secure Processing Block (SPB) Type 1 protection, whenever they exist outside of their originally encrypted state, in accordance with IPS-140 and the requirements of [DCI-DCSS], Section 9.5.2.5:

1. Device Private Keys - RSA private key that devices use to prove their identity and facilitate secure Transport Layer Security (TLS) communications.
2. Content Encryption Keys - Key Delivery Message (KDM) AES keys that protect content.
3. Content Integrity Keys - HMAC-SHA-1 keys that protect the integrity of compressed content (integrity pack check parameters).
4. *This step has been deleted*
5. Link Encryption Keys - Keys that protect the privacy and integrity of uncompressed content for link encryption.
6. TLS secrets - These are transient keys/parameters used or generated in support of TLS and Auditorium Security Messaging (ASM).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5, 9.5.2.6<br>FIPS-140-2<br>FIPS-140-3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 9.5.10. Deleted Section

The section "SPB 1 Firmware Modifications" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 9.5.11. Degraded mode(s) of operation prohibited

*This procedure is applicable only to FIPS-140-3 certification.*

Verify that degraded mode(s) of operation, as defined in FIPS-140-3, are not implemented.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5.1<br>FIPS-140-3 |

## 9.5.12. Control output inhibition

*This procedure is applicable only to FIPS-140-3 certification.*

Verify that the SPB Type 1 inhibits its control output interface during each error state, as specified in FIPS-140-3.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5.1<br>FIPS-140-3 |

## 9.5.13. Maintenance role/interface prohibited

*This procedure is applicable only to FIPS-140-3 certification.*

Verify that a maintenance role/interface, as defined in FIPS-140-3, is not implemented.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5.1<br>FIPS-140-3 |

## 9.5.14. Self-initiated cryptographic output capability

*This procedure is applicable only to FIPS-140-3 certification.*

Verify that, if the SPB Type 1 supports "self-initiated cryptographic output capability," that a User Role and/or Crypto Officer Role is required to support the AuthorityID requirements of DCI-DCSS, 9.4.2.5.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5.1, 9.4.2.5<br>FIPS-140-3 |

## 9.5.15. Self-initiated cryptographic output capability

*This procedure is applicable only to FIPS-140-3 certification.*

Verify the strength and hardness of SPB Type 1 physical security enclosure material(s) are sustained over the SPB Type 1's range of operation, storage, and distribution by review of design documentation. Verify that destructive physical attacks performed on SPB-1 at nominal temperature(s) verified the strength and hardness of SPB Type 1 physical security enclosure material(s).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5.1<br>FIPS-140-3 |

### 9.5.16. Periodic self-tests

*This procedure is applicable only to FIPS-140-3 certification.*

Verify that the specified Security Policy maximum time between periodic self-tests, as defined in FIPS-140-3, is not more than one week.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5.1<br>FIPS-140-3 |

# Chapter 10. DCI Requirements Review

Like the previous chapter, this chapter contains procedures for evaluating system design for fidelity to DCI requirements that cannot be tested by direct examination of a finished product. These requirements are different though, because they are not proven by the FIPS 140 certification process. The process of proving these requirements is the same, however. Documentation must be produced and Test Subjects must be instrumented to give the examiner all necessary information to evaluate the design. Manufacturers must produce proof in the form of design documentation for each of the relevant Requirements listed in Section 10.4. (To see which requirements are relevant to a particular type of device, consult the Design Review sections of Part III. Consolidated Test Procedures.)

To complete a compliance evaluation using the requirements in this section, the examiner must be presented with the documentation detailed below. The examiner must also have access to a Test Sample (a production-grade sample of the system, conforming to the operational capabilities of the Design Review sequence being used). Wherever possible, the examiner should confirm that the documentation matches the Test Sample.

## 10.1. Type 1 SPB Documentation

For a Type 1 SPB, it should be possible to validate the requirements in this chapter using much of the test material produced for the FIPS 140 test. It may be necessary for the manufacturer to provide additional information in the case where a requirement is not provable using documentation prepared with only the FIPS 140 test in mind. Manufacturers are encouraged to consider the objectives of this chapter when preparing material for the FIPS 140 test of a Type 1 SPB.

The following documents (repeated from Chapter 9) are examples of the types of documentation that will be useful when proving compliance with the requirements presented in this chapter:

- Master Components List (bill of materials); All items submitted as test evidence to the Testing Organization (*e.g.*, software, firmware, hardware, source code, documentation, etc.) must be specified on the Master Components List, along with a unique identifier and version
- Security policy
- Data sheets for hardware components
- Listing of all significant information flows
- Finite state model
- Clearly annotated source code

- Functional specifications
- Block diagrams
- Schematics
- Software design documentation (such as an API or developers guide)
- Mechanical drawings & assembly drawings (approximately to scale)
- Printed circuit board layout drawings
- Cryptographic Key and Critical Security Parameter documentation
- Delivery and operations procedures
- Cryptographic Officer & User guidance
- Configuration management specification
- Operational testing plan(s), and associated testing equipment
- Documentation detailing the correspondence of all security rules to the implementation

## 10.2. Type 2 SPB Documentation

For a Type 2 SPB, it is necessary to produce documentation to validate the requirements in this chapter. Because a Type 2 SPB is not required to undergo FIPS 140 testing, this documentation will be produced only for the purpose of this DCI compliance test. Note that the documentation need not cover aspects of the design that are not the subject of the requirements.

The following documentation must be supplied:

- Block diagrams showing chassis partitions, major components, locations of security components, security parameters and security related information flows.
- Descriptions and functions of all electronic interfaces and user interfaces, for both security and non-security operations. (Proprietary details of non-security related interfaces are not required, however enough information must be supplied to allow the examiner to prove that all security-related interfaces have been fully documented).
- User and maintenance manual information relating to security, *i.e.* installation and operation details including user and maintenance roles for electronic access and detailed declarations of capabilities for each role. Also include check lists or instructions from user or maintenance documentation that contain information suggesting security-related instructions, recommended practices, etc. for users and maintenance personel.
- Analysis of user and maintenance role capabilities reconciled against DCI requirements for "non-security" vs. "security" related access and maintenance.
- Finite state model, limited to SPB-2 security functional operation (including interaction with the companion type-1 SPB, as applicable).

In addition to the above, any documentation that can be used to prove that the design meets a particular requirement should be provided.

## 10.3. Forensic Mark IP Disclosure

For a Test Subject which implements Forensic Marking (FM), it will be necessary to provide, in addition to the documentation listed above, an intellectual property disclosure statement which describes any claims on intellectual property that the manufacturer intends to make on the FM algorithm.

## 10.4. DCI Requirements for Security Modules

Each of the subsections below describes a DCI requirement that must be proven by examining the manufacturer's documentation.

### 10.4.1. Theater System Reliability

- Record the calculated Mean Time Between Failure (MTBF) for the design. There are no Pass/Fail criteria for this value.
- Record the calculated Mean Time Between Failure (MTBF) for the design. There are no Pass/Fail criteria for this value.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.2.3.1, 7.2.3.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

### 10.4.2. Theater System Storage Security

- Verify that image and audio essence on storage devices retains its original AES encryption, if present during ingest.
- Verify that decrypted plaintext (image or audio) essence is never stored on the storage system.
- Verify that with the exception of subtitle essence, encrypted essence files are decrypted only in real-time during playback.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 7.5.3.8, 9.4.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |

| | | |
|---|---|---|
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.3. Security Devices Self-Test Capabilities

Verify that (to the extent possible) all security devices are designed with self-test capability to announce failures and take themselves out of service.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.4. Security Entity Physical Protection

Verify that the following Security Entities (SE) are contained within Type 1 SPBs:

- Security Manager (SM)
- Media Decryptor (MD)
- Link Encryptor (LE)
- Link Decryptor (LD)
- Forensic Marker (FM)

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.1.1, 9.3.3.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.5. Secure SMS-SM Communication

*Does not apply to an SMS that is permanently integrated.*

Verify that the SMS communicates with the SM under its control using:

- TLS 1.0, 1.2 or 1.3; and
- a TCP port other than 1173.

| | |
|---|---|
| **Reference Documents** | [RFC-2246]<br>[RFC-2246]<br>[RFC-8446]<br>DCI-DCSS, 9.4.1.1, 9.4.2.5, 9.4.5.1, 9.4.5.2.3.(9) |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.6. Location of Security Manager

Using the definition of a Security Manager (SM) and its functions specified in Sections 9.4.2.4, 9.4.3.5, 9.6.1 and 9.6.1.2 of [DCI-DCSS]:

- Verify that each Media Block (MB) contains all the functions of exactly one SM.
- Verify that no SM function is implemented outside the Secure Processing Block Type 1 (SPB Type 1) boundaries of an MB.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.2.4, 9.4.3.5, 9.6.1, 9.6.1.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.7. Deleted Section

The section "SM Usage of OS Security Features" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 10.4.8. Secure Remote SPB-SM Communications

Verify that security communications between the Security Manager (SM) and remote SPBs only use:

- TLS 1.0 as specified in [RFC-2246] and constrained by [SMPTE-430-6];
- Standardized security messages, as defined by [DCI-DCSS], Table 15; and
- TCP port 1173.

| | |
|---|---|
| **Reference Documents** | [RFC-2246]<br>[SMPTE-430-6]<br>DCI-DCSS, 9.4.2.4, 9.4.5.1, 9.4.5.2.3(9), 9.4.5.3.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

## 10.4.9. Playback Preparation

Verify that the SM prepares the security system for playout within 30 minutes prior to showtime.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.10. Special Auditorium Situation Detection

*The following applies only to a Test Subject that is a Media Block.*

If the Test Subject supports Special Auditorium Situations, verify that the Test Subject enables Special Auditorium Situation during the auditorium security network TLS session establishment and if and only if one or two of the following conditions are met:

a. The use of (i) more than one remote LDB/projector pair with a single MB, or (ii) an LD/LE image processor SPB inserted between the MB and one or more remote LDB/projector pair(s); or

b. The use of an integrated and married MB/projector pair, where the MB also outputs a Link Encrypted image signal to one or more remote LDB/projector pair(s). The MB shall simultaneously meet all requirements for both integrated and non-integrated projector system implementations.

Unless a Special Auditorium Situations is enabled, verify that the Test Subject supports suite playback for exactly one projector.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.4.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | Applies only to a Type 1 SPB device or module which implements features that allow it to supply keys or content to a remote SPB. |

## 10.4.11. Prevention of Keying of Compromised SPBs

Verify that the SM precludes delivery of keys or content to, or play back on, devices reporting a Security Alert or remote SPBs not listed on the KDM TDL.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

## 10.4.12. SPB Authentication

Verify that the Security Manager (SM) performs remote Secure Processing Block (SPB) authentication through Transport Layer Security (TLS) session establishment, and maintain the certificate lists collected.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

## 10.4.13. TLS Session Key Refreshes

Verify that the Security Manager (SM) maintains open Transport Layer Security (TLS) sessions with remote SPBs for not more than 24 hours between complete restarts (*i.e.*, forces periodic fresh TLS keys).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

## 10.4.14. LE Key Issuance

Verify that the SM supports keying of the Link Encryptor (LE) by transferring LE keys only to an authenticated and trusted Link Decryptor Block (LDB) and companion SPB (*i.e.*, the projector). Verify that LE keys are not issued to the LDB unless the LDB certificate and, where applicable, companion SPB certificate, are listed on the TDL of the enabling KDM.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

## 10.4.15. Maximum Key Validity Period

Note: Only applicable where external MDs or FMs are used.

Verify that the key usage validity period is six (6) hours. Verify that the six hour period does not extend beyond the playback time window specified in the KDM. An exception to this requirement may be made when playout is started within the KDM playout time window, but the playout time window expires before the end of playout. In this case the show may playout beyond the playout time window by a maximum of six (6) hours.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5, 9.4.5.3.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

## 10.4.16. KDM Purge upon Expiry

Verify that the Security Manager (SM) deletes from its storage a Key Delivery Message (KDM) (and associated keys) no later than 10 minutes after its playout time window has expired (passed), unless playout is started within the KDM playout time window but the playout time window expires before the end of playout. In the latter case, verify that the SM deletes from its storage the KDM (and associated keys) no later than 10 minutes after (i) the end of the show or (ii) the end of the six (6) hour period following the end of the KDM playout time window, whichever comes first.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.17. Key Usage Time Window

Verify that the Security Manager (SM) enforces the playback time window specified in the Key Delivery Message (KDM) by delivering content keys to Media Decryptors (MD) along with usage periods fully contained within the KDM validity time window. An exception to this requirement may be made when playout is started within the KDM playout time window, but the playout time window expires before the end of playout. In this case the show may playout beyond the playout time window by a maximum of six (6) hours.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.18. Projector Secure Silicon Device

Verify that the projector SPB includes a secure silicon host device (see Section 9.4.3.6.1 of [DCI-DCSS]) that contains the SPB's digital certificate.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

| | | |
|---|---|---|
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.19. Access to Projector Image Signals

Verify that the Projector SPB design does not allow physical access to signals running between the companion SPB and the projector SPB without breaking the marriage.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.20. Systems with Electronic Marriage

Verify that an electronic marriage is planned upon installation of a MB or LDB projector pair. Verify that this physical/ electrical connection is battery-backed and monitored 24/7 by the companion SPB and, if broken, shall require a reinstallation (re-marriage) process.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.21. Systems Without Electronic Marriage

Verify that in the configuration of a permanently married companion SPB (MB or LDB) the companion SPB is not field replaceable and require the projector SPB and companion SPB system to both be replaced in the event of an SPB failure.

If the companion SPB is an LDB or the companion SPB is a *MB with single certificate implementation* as defined in Section 9.5.1.1 of [DCI-DCSS], verify that the system contains exactly one leaf certificate.

If the companion SPB is a *MB with dual certificate implementation* as defined in Section 9.5.1.2 of [DCI-DCSS], verify that the system contains exactly two leaf certificates.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.6, 9.5.1.1, 9.5.1.2 |

☐

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.22. Clock Date-Time-Range

Verify that the MB clock has a Date-Time range of at least 20 years.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.23. Clock Setup

Verify that the SM clock is set by the manufacturer to within one second of UTC by means of a national time standard (such as WWV).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.24. Clock Stability

If the device is an SM, verify that the clock stability requirement of +/- 30 seconds per month is met. If the device is a remote SPB, verify that the clock stability requirement of +/- 60 seconds per month is met.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.25. Repair and Renewal of SPBs

Verify that an SPB cannot be repaired or renewed without direct manufacturer action.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.26. SPB2 Protected Devices

Verify that Type 2 SPB surrounds the following sub-systems:

a. security environment consisting of a secure silicon chip; input/output signals to the secure silicon chip and the projector SPB; perimeter access panel monitoring

b. the projector image signal processing environment

Verify through physical inspection that a sample device contains the above listed sub-systems in a manner consistent with the documentation.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.4 |

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

| | | |
|---|---|---|
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.27. Clock Continuity

Verify that the clock is tamper-proof and thereafter may not be reset.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.28. TLS Endpoints

Verify that all TLS end points are within the physical protection perimeter of the associated SPB.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |

## 10.4.29. Deleted Section

The section "Implementation of RRPs" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 10.4.30. SMS and SPB Authentication and ITM Transport Layer

*Does not apply to an SMS that is permanently integrated.*

Verify that the authentication of the TLS sessions between the SM and remote SPB or SMS utilizes digital certificates as defined by [SMPTE-430-2], which facilitate a cryptographic process that identifies each SPB device to the SM.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.1, 9.4.2.5<br>REF-2246<br>SMPTE-430-2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.31. Idempotency of ITM RRPs

Verify that transactions are "idempotent" (such a transaction may be repeated without changing its outcome).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.32. RRP Synchronism

Verify that RRP protocols are synchronous: each pairing must opened and closed before a new RRP is opened between any two devices. Nested transactions (in which one end point must communicate with another end point while the first waits) are allowed.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.3 |

| Sequence | Type | Conditions |
|---|---|---|

| | | |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.33. TLS Mode Bypass Prohibition

Verify that except where noted in the [DCI-DCSS], non-TLS security communications are not used, and that production Digital Cinema security equipment has no provisions for performing security functions in a TLS "bypass" mode.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.34. RRP Broadcast Prohibition

Verify that no broadcast RRP commands are used or required.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.35. Implementation of Proprietary ITMs

Verify that any proprietary ITM implemented by equipment suppliers do not communicate over TCP or UDP port 1173, and that such ITMs do not communicate information that is the subject of any [SMPTE-430-6] commands.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.3<br>SMPTE-430-6 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.36. RRP Initiator

Verify that, except where noted, only the SMS or SM initiate RRPs.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.37. Deleted Section

The section "SPB TLS Session Partners" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 10.4.38. Deleted Section

The section "SM TLS Session Partners" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 10.4.39. RRP "Busy" and Unsupported Types

Verify that unless otherwise noted, an RRP response is allowed to be busy or an unsupported message type and that such a response is not an error event.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.40. RRP Operational Messages

Verify that Intra-theater Message (ITM) Request-Response Pairs (RRP) category 1 operational messages are transported using:

- TLS 1.0, 1.2 or 1.3; and
- a TCP port other than 1173.

| | |
|---|---|
| **Reference Documents** | [RFC-2246]<br>[RFC-2246]<br>[RFC-8446]<br>DCI-DCSS, 9.4.2.5, 9.4.5.2.4, 9.4.5.2.3.(9) |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.41. Deleted Section

The section "FM Generic Inserter Requirements" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 10.4.42. FM Algorithm General Requirements

For a Forensic Marking (FM) embedder:

1. Verify that single distribution inventory is supported by the FM algorithm.
2. Verify by examination of the FM embedder intellectual property disclosure that the terms and conditions of use for the FM algorithm are reasonable and non-discriminatory (RAND).
3. Verify that detection can be performed by the manufacturer or the Rights Owner at the Rights Owner's premises.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.43. FM Insertion Requirements

- Verify that audio (main sound and OBAE, as applicable) and image FM insertion is a real-time (*i.e.*, show playback time), in-line process performed in the associated MB, and has a reasonable computational process.
- Verify that audio (main sound and OBAE, as applicable) and image FM is applied at the earliest point after decryption and prior to the essence being present on any data bus outside the MB.
- Verify that all FM inserters insert a unique 19-bit minimum "location" Forensic Marking Identification (FMID) that is permanently associated with the associated MB.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.1, 9.4.6.2(9)<br>OBAE-ADD, 3.4 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |

| | | |
|---|---|---|
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.44. IFM Visual Transparency

Verify that IFM is visually transparent to the critical viewer in butterfly tests for motion image content.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.45. IFM Robustness

Verify that IFM resists/survives video processing attacks (such as digital-to-analog conversions, including multiple D-A/A-D conversions), re-sampling and re-quantization (including dithering and recompression), common signal enhancements to image contrast and color, resizing, letterboxing, aperture control, low-pass filtering, anti-aliasing, brick wall filtering, digital video noise reduction filtering, frame-swapping, compression, arbitrary scaling (aspect ratio is not necessarily constant), cropping, overwriting, addition of noise and other transformations. Verify that IFM survives collusion (the combining of multiple videos in the attempt to make a different fingerprint or to remove it), format conversion, the changing of frequencies and spatial resolution (among, for example, NTSC, PAL and SECAM, into another and vice versa), horizontal and vertical shifting and camcorder capture and low bit rate compression (*e.g.*, 500 Kbps H264, 1.1 Mbps MPEG-1).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.46. AFM Inaudibility

Verify that AFM is inaudible in critical listening A/B tests

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.47. AFM Robustness

Verify that AFM resists/survives multiple D/A and A/D conversions, radio frequency or infrared transmissions within the theater, any combination and down conversion of captured channels, re-sampling of channels, time compression/ expansion with pitch shift and pitch preserved, linear speed changes within 10% and pitch-invariant time scaling within 4%. Verify that AFM resists/survives data reduction coding, nonlinear amplitude compression, additive or multiplicative noise frequency response distortion such as equalization, addition of echo, band-pass filtering, flutter and wow and overdubbing.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.48. FM Control Instance

Verify that the SM is solely responsible for control of FM marking processes (*i.e.*, "on/off") for the auditorium it is installed in and command and control of this function is only via the KDM indicator per [SMPTE-430-1] .

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.2<br>SMPTE-430-1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.49. Deleted Section

The section "SE Time Stamping" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 10.4.50. SE Log Authoring

Verify that an SE authors its own log records, or utilizes the services of a proxy within the same secure SPB

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.51. SPB Log Storage Requirements

Verify that log records stored in SPBs are stored in non-volatile memory and are not purge-able. Verify that data is overwritten beginning with the oldest data as new log data is accumulated. Verify that no log records are overwritten unless collected by the SM..

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.52. Remote SPB Log Storage Requirements

Verify that remote SPBs have sufficient secure storage to hold log data to accommodate at least two days worth of typical operation.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |

## 10.4.53. MB Log Storage Capabilities

Verify that the SM is capable of storing at least 12 months of typical log data accumulation for the auditorium in which it is installed, including log data collected from the associated remote SPBs.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.54. Logging for Standalone Systems

Verify that the logging subsystem implementations do not affect the ability of Exhibition to operate their projection systems in a standalone fashion.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.1 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |

| | | |
|---|---|---|
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.55. Logging of Failed Procedures

Verify that failure or refusal of logged events is also a logged event (as applicable).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8, 9.4.6.3.10 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.56. SPB Log Failure

Verify that behavior of security devices (SPB or SE) is specified and designed to immediately terminate operation, and requires replacement, upon any failure of its secure logging operation.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.10 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.57. Log Purging in Failed SPBs

Verify that resident log records in failed SPBs (and their contained SEs) are not purge-able except by authorized repair centers, which are capable of securely recovering such log records.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.3.10 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.58. MB Tasks

- Verify that, if included as part of the MB design, decryption and forensic marking of image essence is performed within the SPB boundary of the MB, and that the resulting image signal is passed to the projector SPB or LDB, as appropriate.
- Verify that, if included as part of the MB design, decryption and forensic marking of audio essence is performed within the SPB boundary of the MB, and that the resulting audio signal is passed to external components.
- Verify that, if included as part of the MB design, decryption, rendering and forensic marking of OBAE essence is performed within the SPB boundary of the MB, and that the resulting audio signal is passed to external components.
- Verify that, if included as part of the MB design, decryption of subtitle essence is performed within the SPB boundary of the MB, and that the resulting plaintext essence is passed to external components.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.3, 9.4.3.6.4<br>OBAE-ADD, 3.3, 3.4, 3.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.59. Type 1 SPB RSA Private Keys

- Verify that RSA private keys in a Type 1 SPB which constitute the subject of any certificate having an SM or LS role are (1) generated within the secure silicon device, (2) whether encrypted or not do not exist outside of the secure silicon device and (3) are not accessible to any process external to the secure silicon device.

- Verify that the entropy source (seed) used in the generation of the above RSA keys (1) is fully contained within the MB's SPB Type 1 and is not dependent on or influenced by any parameter or value external to the SPB, (2) does not enable the export of any information about the seed from the SPB.
- Verify that the CipherValue elements of the KDM's AuthenticatedPrivate element are decrypted by and within the secure silicon device.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.5.2.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.60. Content Keys Outside Secure Silicon

Verify that once decrypted from the KDM (and except when being used during playback) content keys are either cached within the secure silicon IC, or protected by AES key wrapping per [NIST-800-38F] when cached externally to secure silicon within the Media Block.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.1, 9.5.2.2, 9.7.4<br>NIST-800-38F |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.61. Prohibition of SPB Type 1 Field Serviceability

Verify that SPBs of Type 1 are not field serviceable (*e.g.*, SPB Type 1 maintenance access doors shall not be open-able in the field).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.3 |

| Sequence | Type | Conditions |
|---|---|---|
| | | |

| | | |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.62. Use of Software Protection Methods

Verify that software protection methods are not used to protect CSPs or content essence

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.63. TMS Role

Verify that in the event that Exhibition command and control designs include the TMS as a device that interfaces with the SMs, such a TMS is viewed by the security system as an SMS, and carries a digital certificate and follows all other SMS behavior, TLS and ITM communications requirements.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.64. D-Cinema Security Parameter Protection

Verify that the following Digital Cinema Security Parameters (DCSPs) receive SPB Type 1 protection, whenever they exist outside of their originally encrypted state:

1. Watermarking or Fingerprinting command and control - Any of the parameters or keys used in a particular Forensic Marking process.

2. Logged Data - All log event data and associated parameters constituting a log record or report.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.6 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.65. RSA Key Entropy

Verify that the mechanism used to generate RSA key pairs must have at least 128-bits of entropy (unpredictability).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.7.6 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.66. Preloaded Symmetric Key Entropy

Verify that AES or TDES symmetric keys pre-loaded into a device are generated with a high quality random number generator with at least 128 bits of entropy (112 bits for TDES).

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.7.6 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.67. MD Caching of Keys

Verify that the Media Decryptor is capable of securely caching at least 512 keys

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.7.7 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.68. SPB Type 1 Firmware Modifications

Verify the following:

1. The device is designed such that the firmware cannot be modified without the knowledge and permission of the original manufacturer.
2. The device's firmware modification procedure requires a digital certificate per [SMPTE-430-2] that identifies the authority figure responsible for making the firmware change.
3. The device logs firmware change information including timestamp, version and operator identity

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.7 |

| Sequence | Type | Conditions |
|---|---|---|
| | | |

| | | |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.69. SPB Type 1 Log Retention

Verify that log records are not purged from a Type 1 SPB in the event of intrusion or other tamper detection.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.2.1, 9.4.3.6.3, 9.4.6.3.10 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.70. ASM Get Time Frequency

Verify that the SM executes the ASM GetTime command immediately after power-up initialization and at least once every 24 hours of operation.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | Applies only to a Type 1 SPB device or module which implements features that allow it to supply keys or content to a remote SPB. |

## 10.4.71. Deleted Section

The section "SPB2 Log Memory Availability" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## 10.4.72. SPB Secure Silicon Requirements

Verify that the SPB's Secure Silicon device meets FIPS 140 level 3 "Physical Security" area requirements as defined for "single-chip cryptographic modules". Failure of this verification is cause to fail this test.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.5.2.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.73. SPB Type 1 Battery Life

- Verify that the Type 1 SPB clock's battery has a life of at least 5 years under normal operating conditions

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.7 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.74. Companion SPB Retrieve Projector Cert

*Only applies to a Test Subject that is a Companion SPB (LDB or SM).*

Verify that the Test Subject retrieves the Projector SPB certificate over the marriage connection.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.75. Log Collection for Married MB

Verify that, when integrated within a projector as the projector's companion SPB, or permanently married to the projector, the MB provides 24/7 log recording support, and storage of all log records associated with the projector SPB.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.76. Companion SPB Single Purpose Requirement

*The following applies only to Test Subjects that are Companion SPBs, i.e. MB or LDB designed to operate with an integrated projection system.*

Verify that the Test Subject does not operate unless integrated with a projector SPB. In particular,

- if the Test Subject is an LDB, verify that the Test Subject cannot perform link decryption functions unless integrated within a projector SPB; or
- if the Test Subject is a MB, verify that the Test Subject cannot perform any composition decryption function unless integrated within and married to a projector SPB.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.3, 9.4.3.6.2 |

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.77. Standalone MB Single Purpose Requirement

*The following applies only to a MB that is not designed to operate with an integrated projection system, i.e. not designed as a Companion SPB.*

Verify that the Test Subject cannot operate, or be reconfigured to operate with an integrated projection system, *i.e.* as a Companion SPB.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.3 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |

## 10.4.78. Projector SPB Log Reporting Requirements

Verify that the Projector SPB sends log event data across the marriage electrical interface for retention by the companion SPB, as specified in Table 19 of [DCI-DCSS].

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.1, 9.4.6.3.8 |

| Sequence | Type | Conditions |
|---|---|---|
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.79. TLS RSA Requirement

Verify that the Test Subject, for the purpose of ASM communications, only supports the TLS CipherSuite "TLS_RSA_WITH_AES_128_CBC_SHA" as specified in [SMPTE-430-6].

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.2.4 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 14.3. Projector Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 16.3. LD/LE Design Review | Pass/Fail | — |

## 10.4.80. Dual Certificate SMS Authentication

*Only applies if the SM uses dual certificates and the SMS is not permanently integrated.*

- Verify that if the Test Subject's SMS establishes the TLS session with the SM (SM is the TLS server) the SM Certificate (SM Cert) shall be presented by the SM.
- Verify that if the Test Subject's SM establishes the TLS session with SMS (SMS is the TLS server) the Log Signer Certificate (LS Cert) shall be presented by the SM.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.5.3.2, 9.5.1, 9.5.1.2, 9.4.2.5 |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.81. Constrained OMB Processing Capability

Verify that an OMB does *not*:

- Process or generate any Auditorium Security Messages (ASM) or use "port 1173";
- Support link encryption;
- Attempt to authenticate other SPBs;
- Attempt to interface or communicate with any other SPB (projector, LDB, LD/LE or other MB), except to accept non-security messaging; and
- Process essence other than the following:
  - Object-Based Audio Essence (OBAE) as defined in [OBAE-ADD]; or
  - Auxiliary Data (AD) essence as defined in [SMPTE-429-14], subject to the constraints of Section 9.4.2.7 at [DCI-DCSS].

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.6.3(5), 9.4.3.6.4, 9.4.2.7, 9.4.5<br>OBAE-ADD<br>SMPTE-429-14 |

| Sequence | Type | Conditions |
|---|---|---|
| 20.3. OMB Design Review | Pass/Fail | — |

## 10.4.82. Export of KDM-Borne Keys

Verify that under no circumstances does the SM export any KDM-borne key from the SM's SPB.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.3.5(9d) |

| Sequence | Type | Conditions |
|---|---|---|
| 13.3. Server Design Review | Pass/Fail | — |
| 15.3. Projector with MB Design Review | Pass/Fail | — |
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.83. Encrypted Auxiliary Data Processing

If the MB under test can decrypt Auxiliary Data as defined by [SMPTE-429-14]:

- Verify that each such decryption takes place only within the MB, and uses only an MDX1 KeyType that is delivered within a KDM.
- Verify that the MB does not process the MDX2 KeyType.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.2.7, 9.4.3.6.4<br>SMPTE-429-14 |

## 10.4.84. OBAE Addendum

- Verify that Media Block OBAE essence format processing is as represented by [SMPTE-2098-2], per the requirements of the [OBAE-ADD] Section 3.1 "Essence Format."
- Verify that Media Block OBAE essence processing is per [SMPTE-429-18] and consistent with all provisions of [SMPTE-429-19], per the requirements of the [OBAE-ADD] Section 3.2 "Packaging."
- Verify that Media Block OBAE essence decryption processing decrypts OBAE essence within the MB using only the MDEK KeyType delivered by a KDM per [SMPTE-430-1], per the requirements of the [OBAE-ADD] Section 3.3 "Security." See also Section 6.1.4: Restriction of Keying to MD Type.
- Verify that OBAE essence forensic marking adheres to the same requirements as non-OBAE audio (all audio channels are marked prior to essence leaving the MB and all FM marks are recoverable). Verify that all OBAE forensic marking is enabled/disabled (all marked/none marked) pursuant to the presence/absence respectively of the MDEK flag defined in [SMPTE-430-1], per the requirements of the [OBAE-ADD], Section 3.4 "Forensic Marking." See also Section 6.4.2: Granularity of FM Control, Section 6.4.3: FM Payload and Section 10.4.43: FM Insertion Requirements.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 3.1, 3.2, 3.3, 3.4<br>SMPTE-2098-2 |

| | |
|---|---|
| | SMPTE-429-18<br>SMPTE-429-19<br>SMPTE-430-1 |

| Sequence | Type | Conditions |
|---|---|---|
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.85. OBAE FM Robustness

- Verify that forensic marking applied to OBAE essence resists/survives multiple D/A and A/D conversions, radio frequency or infrared transmissions within the theater, any combination and down conversion of captured channels, resampling of channels, time compression/expansion with pitch shift and pitch preserved, linear speed changes within 10% and pitch-invariant time scaling within 4%.
- Verify that forensic marking applied to OBAE essence resists/survives data reduction coding, nonlinear amplitude compression, additive or multiplicative noise frequency response distortion such as equalization, addition of echo, band-pass filtering, flutter and wow and overdubbing.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.3<br>OBAE-ADD, 3.4 |

| Sequence | Type | Conditions |
|---|---|---|
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

## 10.4.86. OBAE FM Inaudibility

Verify that forensic marking applied to OBAE essence is inaudible in critical listening A/B tests.

| | |
|---|---|
| **Reference Documents** | DCI-DCSS, 9.4.6.1.3<br>OBAE-ADD, 3.4 |

| Sequence | Type | Conditions |
|---|---|---|
| 20.3. OMB Design Review | Pass/Fail | — |
| 21.3. Digital Cinema Projector with IMBO Design Review | Pass/Fail | — |

# Part III. Consolidated Test Procedures

The chapters in this part contain consolidated procedures and standardized test reports for testing Digital Cinema equipment and content. These consolidated procedures refer to the elemental procedures in Part I. Procedural Tests and Part II. Design Evaluation Guidelines, building on those procedures to present a complete, ordered sequence for testing the Test Subject.

The Test Subject of each consolidated procedure is the device under test. This Test Subject is part of a d-cinema system comprised of one or more *certificated devices*. Certificated devices are the Image Media Block (IMB), Outboard Media Block (OMB), Image Media Block with OMB functions (IMBO), Link Decryptor Block (LDB), Projector, Screen Management System/Server (SMS) and Link Decryptor/Encryptor (LD/LE). The Test Subject and other certificated devices to be tested are designated at the opening of each consolidated test procedure chapter. All designated certificated devices shall be included in the testing for each chapter and be specifically listed in the test report.

**Note:**
The DCSS restricts the use of Link Encryption (LE) to non-MMB configurations and non-OBAE processing devices. Therefore LE related tests are not directed to or included in Procedural Chapters 20 and 21.

# Chapter 11. Testing Overview

## 11.1. Test Reports

To prepare a test report, select the test sequence for the Test Subject and perform the tests in the order presented, recording the results of each test as you progress.

Information about the testing session itself is recorded in the following Table 11.1: Test Session Data for the test sequence performed. All fields must be filled in. To assure a standardized presentation of the information, lines 1-11 of the table shall be present in the report as shown, with the appropriate information filled in according to the test procedure performed. The certificated devices that comprise the Test Subject for each chapter are designated in parenthesis in line 10, and each designated device must be uniquely identified by manufacturer and product name and model/version number, etc. in line 9.

Each certificated device must be singularly compliant with the tests specified in the given chapter to be listed in line 9, either by passing all applicable consolidated test requirements as part of the current procedure, or as part of a previous CTP report, or as enabled by a family grouping or confidence retest. The Test Subject shall not indicate a line 11 "pass" unless all designated certificated devices are compliant.

Per [DCI-DCSS], Section 9.4.3.6.6 if the Projector and SPB (IMB, IMBO or LDB) are permanently married the pair shall be identified by a single certificate and treated as a single certificated device. Per [DCI-DCSS], Section 9.4.2.5 if the SMS is permanently integrated within a SPB (IMB, IMBO or LDB), the pair shall be identified by a single certificate and treated as a single certificated device

**Table**
**11.1.Test**

### Session Data

| | |
|---|---|
| 1. Reporting date | |
| 2. Name of Testing Organization | |
| 3. Address of Testing Organization | |
| 4. Name of Test Operator | |
| 5. Test location (if not at testing org's site) | |
| 6. Name of Test Subject Representative | |
| 7. Address of Test Subject Representative | |
| 8. Make and model of Test Subject (to be included on the DCI listing hot link) | |
| 9. Serial and model numbers identifying each of the participating certificated devices, including software and/or firmware version numbers as applicable[a]. | |
| 10. Test procedure performed (select one) | ☐ Chapter 13: Standalone IMB Server (IMB + SMS)<br>☐ Chapter 14: Standalone Projector (Proj + LDB)<br>☐ Chapter 15: Projector w/IMB (Proj + IMB + SMS)<br>☐ Chapter 16: Link Decryptor/Encryptor (LD/LE)<br>☐ Chapter 20: OMB (OMB + IMB + SMS)<br>☐ Chapter 21: Projector w/IMBO (Proj + IMBO + SMS) |
| 11. Test status (select one) | ☐ Pass<br>☐ Fail |

[a] For a permanently married projector, single line 9 item shall identify the projector and companion device (per [DCI-DCSS], Section 9.4.3.6.6). For an integrated SMS, a single line 9 item shall identify the SMS and IMB (per [DCI-DCSS], Section 9.4.2.5, first bullet). To assure clarity, line 9 information shall include the text "permanently married" or "permanently integrated" as applicable.

# Chapter 12. Deleted Chapter

The chapter "Digital Cinema Package (DCP) Consolidated Test Sequence" was deleted. The chapter number is maintained here to preserve the numbering of subsequent sections.

# Chapter 13. Digital Cinema Server Consolidated Test Sequence

## 13.1. Overview

The test sequence defined in this chapter is intended to be used to test a stand-alone d-cinema *server* as the Test Subject. The configuration and architecture of the Test Subject may vary, but the test sequence requires that the system consists of at least an Image Media Block (IMB, containing a Security Manager, Media Decryptor, Link Encryptor, etc.) and a Screen Management Server

(SMS). For the purpose of this test, the Test Operator may substitute a Theater Management Server (TMS) for the SMS if it implements the required functionality. Wherever a test procedure refers to an SMS, the equivalent TMS may also be used.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 13.2. Server Test Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 3.5.1. KDM NonCriticalExtensions Element | | | — | — |
| 2 | 3.5.2. ETM IssueDate Field Check | | | — | — |
| 3 | 3.5.4. Structure ID Check | | | — | — |
| 4 | 3.5.5. Certificate Thumbprint Check | | | — | — |
| 5 | 3.5.7. KeyInfo Field Check | | | — | — |
| 6 | 3.5.8. KDM Malformations | | | — | — |
| 7 | 3.5.9. KDM Signature | | | — | — |
| 8 | 5.1.1. SPB Digital Certificate | | | — | — |
| 9 | 5.2.1. TLS Session Initiation | | | — | — |
| 10 | 5.2.2.1. Auditorium Security Message Support | | | — | — |
| 11 | 5.2.2.2. ASM Failure Behavior | | | — | — |
| 12 | 5.2.2.3. ASM "RRP Invalid" | | | — | — |
| 13 | 5.2.2.4. ASM "GetTime" | | | — | — |
| 14 | 5.2.2.5. ASM "GetEventList" | | | — | — |
| 15 | 5.2.2.6. ASM "GetEventID" | | | — | — |
| 16 | 5.2.2.7. ASM "LEKeyLoad" | | | | — |
| 17 | 5.2.2.8. ASM "LEKeyQueryID" | | | — | — |
| 18 | 5.2.2.9. ASM "LEKeyQueryAll" | | | — | — |
| 19 | 5.2.2.10. ASM "LEKeyPurgeID" | | | — | — |
| 20 | 5.2.2.11. ASM "LEKeyPurgeAll" | | | — | — |
| 21 | 5.2.2.12. ASM "GetProjCert" | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 23 | 5.3.2.1. Log Structure | | | — | — |
| 24 | 5.3.2.2. Log Records for Multiple Remote SPBs | | | — | — |
| 25 | 5.3.2.3. Log Sequence Numbers | | | — | — |
| 26 | 5.3.2.4. Log Collection by the SM | | | — | — |
| 27 | 5.3.2.5. General Log System Failure | | | — | — |
| 28 | 5.3.2.6. Log Report Signature Validity | | | — | — |
| 29 | 5.3.3.1. SM Proxy of Log Events | | | — | — |
| 30 | 5.3.3.2. SM Proxy of Security Operations Events | | | — | — |
| 31 | 5.3.3.3. SM Proxy of Security ASM Events | | | — | — |
| 32 | 5.3.3.4. Remote SPB Time Compensation | | | — | — |
| 33 | 5.4.1.1. FrameSequencePlayed Event | | | — | — |
| 34 | 5.4.1.2. CPLStart Event | | | — | — |
| 35 | 5.4.1.3. CPLEnd Event | | | — | — |
| 36 | 5.4.1.4. PlayoutComplete Event | | | — | — |
| 37 | 5.4.1.5. CPLCheck Event | | | — | — |
| 38 | 5.4.1.6. KDMKeysReceived Event | | | — | — |
| 39 | 5.4.1.7. KDMDeleted Event | | | — | — |
| 40 | 5.4.2.1. LinkOpened Event | | | — | — |
| 41 | 5.4.2.2. LinkClosed Event | | | — | — |
| 42 | 5.4.2.3. LinkException Event | | | — | — |
| 43 | 5.4.2.4. LogTransfer Event | | | — | — |
| 44 | 5.4.2.5. KeyTransfer Event | | | — | — |
| 45 | 5.4.2.6. SPBStartup and SPBShutdown Events | | | — | — |
| 46 | 5.4.2.8. SPBClockAdjust Event | | | — | — |
| 47 | 5.4.2.10. SPBSoftware Event | | | — | — |
| 48 | 5.4.2.11. SPBSecurityAlert Event | (data only) | | — | — |
| 49 | 6.1.1. Image Integrity Checking | | | — | — |
| 50 | 6.1.2. Sound Integrity Checking | | | — | — |
| 51 | 6.1.4. Restriction of Keying to MD Type | | | — | — |
| 52 | 6.1.5. Restriction of Keying to Valid CPLs | | | — | — |
| 53 | 6.1.6. Remote SPB Integrity Monitoring | | | — | — |
| 54 | 6.1.7. SPB Integrity Fault Consequences | | | — | — |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 55 | 6.1.8. Content Key Extension, End of Engagement | | | — | — |
| 56 | 6.1.9. ContentAuthenticator Element Check | | | — | — |
| 57 | 6.1.10. KDM Date Check | | | — | — |
| 58 | 6.1.11. KDM TDL Check | | | — | — |
| 59 | 6.1.12. Maximum Number of DCP Keys | | | — | — |
| 60 | 6.1.13. CPL Id Check | | | — | — |
| 61 | 6.1.15. Restriction of Playback in Absence of Integrity Pack Metadata | | | — | — |
| 62 | 6.1.19. Plurality of Media Block Identity Certificates | | | — | — |
| 63 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 64 | 6.2.2. Special Auditorium Situation Operations | | | — | — |
| 65 | 6.2.3. LE Key Usage | | | — | — |
| 66 | 6.2.4. MB Link Encryption | | | — | — |
| 67 | 6.3.1. Clock Adjustment | | | — | — |
| 68 | 6.3.2. SPB Type 1 Clock Battery | | | — | — |
| 69 | 6.3.3. Clock Resolution | | | — | — |
| 70 | 6.4.1. FM Application Constraints | | | — | — |
| 71 | 6.4.2. Granularity of FM Control | | | — | — |
| 72 | 6.4.3. FM Payload | | | — | — |
| 73 | 6.4.4. FM Audio Bypass | | | — | — |
| 74 | 6.4.5. Selective Audio FM Control | | | — | — |
| 75 | 6.5.1. Playback of Image Only Material | | | — | — |
| 76 | 6.5.2. Decoder Requirements | | | — | — |
| 77 | 6.6.1. Digital Audio Interfaces | | | — | — |
| 78 | 6.6.2. Audio Sample Rate Conversion | | | — | — |
| 79 | 6.6.3. Audio Delay Setup | | | — | — |
| 80 | 6.6.4. Click Free Splicing of Audio Track Files | | | — | — |
| 81 | 6.7.1. Media Block Overlay | | | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |
| 82 | 6.7.4. Default Timed Text Font | | | Applies to a Media Block that implements an alpha channel overlay | |

| | | | | | |
|---|---|---|---|---|---|
| 82 | 6.7.4. Default Timed Text Font | | | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |
| 83 | 6.7.6. Timed Text Decryption | | | — | — |
| 84 | 8.1.1. Storage System Ingest Interface | | | — | — |
| 85 | 8.1.2. Storage System Capacity | | | — | — |
| 86 | 8.1.3. Storage System Redundancy | | | — | — |
| 87 | 8.1.4. Storage System Performance | | | — | — |
| 88 | 8.2.2. Show Playlist Creation | (data only) | | — | — |
| 89 | 8.2.3. Show Playlist Format | | | — | — |
| 90 | 8.2.5. Automation Control and Interfaces | | | — | — |
| 91 | 8.2.6. Interrupt Free Playback | | | — | — |
| 92 | 8.2.7. Artifact Free Transition of Image Format | | | — | — |
| 93 | 8.2.8. Restarting Playback | | | — | — |
| 94 | 8.2.9. SMS User Accounts | | | — | Record the available operator roles (names) and whether locally-defined accounts can be created. |
| 95 | 8.2.10. SMS Operator Identification | | | — | — |
| 96 | 8.2.11. SMS Identity and Certificate | | | — | — |
| 97 | 8.2.12. Content Keys and TDL check | | | — | — |
| 98 | 8.2.14. KDM Content Keys Check | | | — | — |
| 99 | 8.2.15. Validity of SMS Certificates | | | — | — |

## 13.3. Server Design Review

For each requirement listed in the table below, prove that the system design meets the requirement by identifying the software or hardware mechanism that implements the requirement and analyzing the design to assure that the requirement has been met, subject to stipulated conditions. If a proof cannot be made, the design will be considered non-compliant with regard to the requirement. To perform this analysis the examiner will require access to exhibit documents (system design artifacts) such as schematic diagrams, implementation source code, unit test source code, state diagrams, design notes, etc. See Chapter 9: FIPS Requirements for a Type 1 SPB and Chapter 10: DCI Requirements Review for more information.

For each requirement, the examiner must record the identifiers of the exhibits consulted in proving the requirement, including applicable version identifiers, section or sheet numbers, grid identifiers, etc., and the examiner must record Pass or Fail to indicate whether or not the requirement has been met by the design. The examiner may also record any notes relevant to interpreting the exhibits and to the determination of the compliance status.

| Step | Procedure | Pass | Fail | Conditions | Exhibit Identifiers |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 1 | 9.5.1. SM Operating Environment | | | — | |
| 2 | 9.5.2. LE Key Generation | | | — | |
| 3 | 9.5.3. SPB Type 1 Tamper Responsiveness | | | — | |
| 4 | 9.5.4. Security Design Description Requirements | | | — | |
| 5 | 9.5.6. SPB Type 1 FIPS Requirements | | | — | |
| 6 | 9.5.8. Asymmetric Key Generation | | | — | |
| 7 | 9.5.9. Critical Security Parameter Protection | | | — | |
| 8 | 10.4.1. Theater System Reliability | | | — | |
| 9 | 10.4.2. Theater System Storage Security | | | — | |
| 10 | 10.4.3. Security Devices Self-Test Capabilities | | | — | |
| 11 | 10.4.4. Security Entity Physical Protection | | | — | |
| 12 | 10.4.5. Secure SMS-SM Communication | | | — | |
| 13 | 10.4.6. Location of Security Manager | | | — | |
| 14 | 10.4.8. Secure Remote SPB-SM Communications | | | — | |
| 15 | 10.4.9. Playback Preparation | | | — | |
| 16 | 10.4.10. Special Auditorium Situation Detection | | | — | |
| 17 | 10.4.11. Prevention of Keying of Compromised SPBs | | | — | |
| 18 | 10.4.12. SPB Authentication | | | — | |
| 19 | 10.4.13. TLS Session Key Refreshes | | | — | |
| 20 | 10.4.14. LE Key Issuance | | | — | |
| 21 | 10.4.15. Maximum Key Validity Period | | | — | |
| 22 | 10.4.16. KDM Purge upon Expiry | | | — | |
| 23 | 10.4.17. Key Usage Time Window | | | — | |
| 24 | 10.4.22. Clock Date-Time-Range | | | — | |
| 25 | 10.4.23. Clock Setup | | | — | |
| 26 | 10.4.24. Clock Stability | | | — | |
| 27 | 10.4.25. Repair and Renewal of SPBs | | | — | |
| 28 | 10.4.27. Clock Continuity | | | — | |
| 29 | 10.4.28. TLS Endpoints | | | — | |
| 30 | 10.4.30. SMS and SPB Authentication and ITM Transport Layer | | | — | |
| 31 | 10.4.31. Idempotency of ITM RRPs | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 32 | 10.4.32. RRP Synchronism | | | — | |
| 33 | 10.4.33. TLS Mode Bypass Prohibition | | | — | |
| 34 | 10.4.34. RRP Broadcast Prohibition | | | — | |
| 35 | 10.4.35. Implementation of Proprietary ITMs | | | — | |
| 36 | 10.4.36. RRP Initiator | | | — | |
| 37 | 10.4.39. RRP "Busy" and Unsupported Types | | | — | |
| 38 | 10.4.40. RRP Operational Messages | | | — | |
| 39 | 10.4.42. FM Algorithm General Requirements | | | — | |
| 40 | 10.4.43. FM Insertion Requirements | | | — | |
| 41 | 10.4.44. IFM Visual Transparency | | | — | |
| 42 | 10.4.45. IFM Robustness | | | — | |
| 43 | 10.4.46. AFM Inaudibility | | | — | |
| 44 | 10.4.47. AFM Robustness | | | — | |
| 45 | 10.4.48. FM Control Instance | | | — | |
| 46 | 10.4.50. SE Log Authoring | | | — | |
| 47 | 10.4.51. SPB Log Storage Requirements | | | — | |
| 48 | 10.4.53. MB Log Storage Capabilities | | | — | |
| 49 | 10.4.54. Logging for Standalone Systems | | | — | |
| 50 | 10.4.55. Logging of Failed Procedures | | | — | |
| 51 | 10.4.56. SPB Log Failure | | | — | |
| 52 | 10.4.57. Log Purging in Failed SPBs | | | — | |
| 53 | 10.4.58. MB Tasks | | | — | |
| 54 | 10.4.59. Type 1 SPB RSA Private Keys | | | — | |
| 55 | 10.4.60. Content Keys Outside Secure Silicon | | | — | |
| 56 | 10.4.61. Prohibition of SPB Type 1 Field Serviceability | | | — | |
| 57 | 10.4.62. Use of Software Protection Methods | | | — | |
| 58 | 10.4.63. TMS Role | | | — | |
| 59 | 10.4.64. D-Cinema Security Parameter Protection | | | — | |
| 60 | 10.4.65. RSA Key Entropy | | | — | |
| 61 | 10.4.66. Preloaded Symmetric Key Entropy | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 62 | 10.4.67. MD Caching of Keys | | | — | |
| 63 | 10.4.68. SPB Type 1 Firmware Modifications | | | — | |
| 64 | 10.4.69. SPB Type 1 Log Retention | | | — | |
| 65 | 10.4.70. ASM Get Time Frequency | | | — | |
| 66 | 10.4.72. SPB Secure Silicon Requirements | | | — | |
| 67 | 10.4.73. SPB Type 1 Battery Life | | | — | |
| 68 | 10.4.77. Standalone MB Single Purpose Requirement | | | — | |
| 69 | 10.4.79. TLS RSA Requirement | | | — | |
| 70 | 10.4.80. Dual Certificate SMS Authentication | | | — | |
| 71 | 10.4.82. Export of KDM-Borne Keys | | | — | |

# Chapter 14. Digital Cinema Projector Consolidated Test Sequence

## 14.1. Overview

The test sequence defined in this chapter is intended to be used to test a stand-alone d-cinema projector as the Test Subject. The configuration and architecture of the projector may vary, but the test sequence requires that the system consists of at least a Link Decryptor Block (LDB) and a light processing system including electronic and optical components (Projector).

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 14.2. Projector Test Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 5.1.1. SPB Digital Certificate | | | — | — |
| 2 | 5.2.1. TLS Session Initiation | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 3 | 5.2.2.1. Auditorium Security Message Support | | | — | — |
| 4 | 5.2.2.2. ASM Failure Behavior | | | — | — |
| 5 | 5.2.2.4. ASM "GetTime" | | | — | — |
| 6 | 5.2.2.5. ASM "GetEventList" | | | — | — |
| 7 | 5.2.2.6. ASM "GetEventID" | | | — | — |
| 8 | 5.2.2.7. ASM "LEKeyLoad" | | | | — |
| 9 | 5.2.2.8. ASM "LEKeyQueryID" | | | — | — |
| 10 | 5.2.2.9. ASM "LEKeyQueryAll" | | | — | — |
| 11 | 5.2.2.10. ASM "LEKeyPurgeID" | | | — | — |
| 12 | 5.2.2.11. ASM "LEKeyPurgeAll" | | | — | — |
| 13 | 5.2.2.12. ASM "GetProjCert" | | | — | — |
| 14 | 5.2.3. TLS Exception Logging | | | — | — |
| 15 | 5.3.2.1. Log Structure | | | — | — |
| 16 | 5.4.2.1. LinkOpened Event | | | — | — |
| 17 | 5.4.2.2. LinkClosed Event | | | — | — |
| 18 | 5.4.2.3. LinkException Event | | | — | — |
| 19 | 5.4.2.4. LogTransfer Event | | | — | — |
| 20 | 5.4.2.5. KeyTransfer Event | | | — | — |
| 21 | 5.4.2.6. SPBStartup and SPBShutdown Events | | | — | — |
| 22 | 5.4.2.7. SPBOpen and SPBClose Events | | | — | — |
| 23 | 5.4.2.8. SPBClockAdjust Event | | | — | — |
| 24 | 5.4.2.9. SPBMarriage and SPBDivorce Events | | | — | — |
| 25 | 5.4.2.10. SPBSoftware Event | | | — | — |
| 26 | 5.4.2.11. SPBSecurityAlert Event | (data only) | | — | — |
| 27 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 28 | 6.3.2. SPB Type 1 Clock Battery | | | — | — |
| 29 | 6.7.4. Default Timed Text Font | | | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |
| 30 | 7.2.1. Projector and Direct View Display Physical Protection | | | — | — |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 31 | 7.2.2. Projector and Direct View Display Security Servicing | | | — | — |
| 32 | 7.2.6. SPB2 Secure Silicon Field Replacement | | | — | — |
| 33 | 7.2.7. Systems without Electronic Marriage | | | — | — |
| 34 | 7.3.2. Companion SPBs with Electronic Marriage | | | — | — |
| 35 | 7.3.3. Companion SPB Marriage Break Key Retaining | | | — | — |
| 36 | 7.3.4. Remote SPB Clock Adjustment | | | — | — |
| 37 | 7.4.2. LDB TLS Session Constraints | | | — | — |
| 38 | 7.4.3. LDB Time-Awareness | | | — | — |
| 39 | 7.4.5. LDB Key Storage | | | — | — |
| 40 | 7.4.6. LDB Key Purging | | | — | — |
| 41 | 7.5.1. Projector Overlay | | | — | — |
| 42 | 7.5.3. Projector Pixel Count/Structure | | | — | — |
| 43 | 7.5.4. Projector Spatial Resolution and Frame Rate Conversion | (data only) | | — | — |
| 44 | 7.5.5. White Point Luminance and Uniformity | (data only) | | — | — |
| 45 | 7.5.6. White Point Chromaticity and Uniformity | (data only) | | — | — |
| 46 | 7.5.7. Sequential Contrast | (data only) | | — | — |
| 47 | 7.5.8. Intra-frame Contrast | (data only) | | — | — |
| 48 | 7.5.9. Grayscale Tracking | (data only) | | — | — |
| 49 | 7.5.10. Contouring | (data only) | | — | — |
| 50 | 7.5.11. Transfer Function | (data only) | | — | — |
| 51 | 7.5.12. Color Accuracy | (data only) | | — | — |
| 52 | 7.5.13. Projector Test Environment | (data only) | | — | — |

## 14.3. Projector Design Review

For each requirement listed in the table below, prove that the system design meets the requirement by identifying the software or hardware mechanism that implements the requirement and analyzing the design to assure that the requirement has been met, subject to stipulated conditions. If a proof cannot be made, the design will be considered non-compliant with regard to the requirement. To perform this analysis the examiner will require access to exhibit documents (system design artifacts) such as schematic diagrams, implementation source code, unit test source code, state diagrams, design notes, etc. See Chapter 9: FIPS Requirements fora Type 1 SPB and Chapter 10: DCI Requirements Review for more information.

For each requirement, the examiner must record the identifiers of the exhibits consulted in proving the requirement, including applicable version identifiers, section or sheet numbers, grid identifiers, etc., and the examiner must record *Pass* or *Fail* to indicate whether or not the requirement has been met by the design. The examiner may also record any notes relevant to interpreting the exhibits and to the determination of the compliance status.

| Step | Procedure | Pass | Fail | Conditions | Exhibit Identifiers |
|---|---|---|---|---|---|
| 1 | 9.5.2. LE Key Generation | | | — | |
| 2 | 9.5.3. SPB Type 1 Tamper Responsiveness | | | — | |
| 3 | 9.5.4. Security Design Description Requirements | | | — | |
| 4 | 9.5.6. SPB Type 1 FIPS Requirements | | | — | |
| 5 | 9.5.8. Asymmetric Key Generation | | | — | |
| 6 | 9.5.9. Critical Security Parameter Protection | | | — | |
| 7 | 10.4.1. Theater System Reliability | | | — | |
| 8 | 10.4.3. Security Devices Self-Test Capabilities | | | — | |
| 9 | 10.4.4. Security Entity Physical Protection | | | — | |
| 10 | 10.4.18. Projector Secure Silicon Device | | | — | |
| 11 | 10.4.19. Access to Projector Image Signals | | | — | |
| 12 | 10.4.20. Systems with Electronic Marriage | | | — | |
| 13 | 10.4.21. Systems Without Electronic Marriage | | | — | |
| 14 | 10.4.24. Clock Stability | | | — | |
| 15 | 10.4.25. Repair and Renewal of SPBs | | | — | |
| 16 | 10.4.26. SPB2 Protected Devices | | | — | |
| 17 | 10.4.27. Clock Continuity | | | — | |
| 18 | 10.4.28. TLS Endpoints | | | — | |
| 19 | 10.4.30. SMS and SPB Authentication and ITM Transport Layer | | | — | |
| 20 | 10.4.31. Idempotency of ITM RRPs | | | — | |
| 21 | 10.4.32. RRP Synchronism | | | — | |
| 22 | 10.4.33. TLS Mode Bypass Prohibition | | | — | |
| 23 | 10.4.34. RRP Broadcast Prohibition | | | — | |
| 24 | 10.4.35. Implementation of Proprietary ITMs | | | — | |
| 25 | 10.4.36. RRP Initiator | | | — | |
| 26 | 10.4.40. RRP Operational Messages | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 27 | 10.4.50. SE Log Authoring | | | — | |
| 28 | 10.4.51. SPB Log Storage Requirements | | | — | |
| 29 | 10.4.52. Remote SPB Log Storage Requirements | | | — | |
| 30 | 10.4.54. Logging for Standalone Systems | | | — | |
| 31 | 10.4.55. Logging of Failed Procedures | | | — | |
| 32 | 10.4.56. SPB Log Failure | | | — | |
| 33 | 10.4.57. Log Purging in Failed SPBs | | | — | |
| 34 | 10.4.59. Type 1 SPB RSA Private Keys | | | — | |
| 35 | 10.4.61. Prohibition of SPB Type 1 Field Serviceability | | | — | |
| 36 | 10.4.62. Use of Software Protection Methods | | | — | |
| 37 | 10.4.64. D-Cinema Security Parameter Protection | | | — | |
| 38 | 10.4.65. RSA Key Entropy | | | — | |
| 39 | 10.4.66. Preloaded Symmetric Key Entropy | | | — | |
| 40 | 10.4.68. SPB Type 1 Firmware Modifications | | | — | |
| 41 | 10.4.69. SPB Type 1 Log Retention | | | — | |
| 42 | 10.4.72. SPB Secure Silicon Requirements | | | — | |
| 43 | 10.4.73. SPB Type 1 Battery Life | | | — | |
| 44 | 10.4.74. Companion SPB Retrieve Projector Cert | | | — | |
| 45 | 10.4.76. Companion SPB Single Purpose Requirement | | | — | |
| 46 | 10.4.78. Projector SPB Log Reporting Requirements | | | — | |
| 47 | 10.4.79. TLS RSA Requirement | | | — | |

# Chapter 15. Digital Cinema Projector with MB Consolidated Test Sequence

## 15.1. Overview

The test sequence defined in this chapter is intended to be used to test a d-cinema projector with an integrated Image Media Block (IMB) as the Test Subject. The configuration and architecture of the system may vary, but the test sequence requires that the system consists of at least a light processing system including electronic and optical components (Projector), an Image Media Block (containing a Security Manager, Media Decryptor, etc.), and a Screen Management Server (SMS). For the purpose of this test, the Test Operator may substitute a Theater Management Server (TMS) for the SMS if it implements the required functionality. Wherever a test procedure refers to an SMS, the equivalent TMS may also be used.

For the purpose of compliance testing as defined in this Chapter, the spatial resolution of the projector shall be no less than that of the Media Block.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 15.2. Projector with MB Test Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 3.5.1. KDM NonCriticalExtensions Element | | | — | — |
| 2 | 3.5.2. ETM IssueDate Field Check | | | — | — |
| 3 | 3.5.4. Structure ID Check | | | — | — |
| 4 | 3.5.5. Certificate Thumbprint Check | | | — | — |
| 5 | 3.5.7. KeyInfo Field Check | | | — | — |
| 6 | 3.5.8. KDM Malformations | | | — | — |
| 7 | 3.5.9. KDM Signature | | | — | — |
| 8 | 5.1.1. SPB Digital Certificate | | | — | — |
| 9 | 5.2.1. TLS Session Initiation | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 10 | 5.2.2.1. Auditorium Security Message Support | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 11 | 5.2.2.2. ASM Failure Behavior | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 12 | 5.2.2.3. ASM "RRP Invalid" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 13 | 5.2.2.4. ASM "GetTime" | | | Applies only to a device which implements features that allow it to | |

| | | | | | |
|---|---|---|---|---|---|
| 13 | 5.2.2.4. ASM "GetTime" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 14 | 5.2.2.5. ASM "GetEventList" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 15 | 5.2.2.6. ASM "GetEventID" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 16 | 5.2.2.7. ASM "LEKeyLoad" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 17 | 5.2.2.8. ASM "LEKeyQueryID" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 18 | 5.2.2.9. ASM "LEKeyQueryAll" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 19 | 5.2.2.10. ASM "LEKeyPurgeID" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 20 | 5.2.2.11. ASM "LEKeyPurgeAll" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 21 | 5.2.2.12. ASM "GetProjCert" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 22 | 5.2.3. TLS Exception Logging | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 23 | 5.3.2.1. Log Structure | | | — | — |
| 24 | 5.3.2.2. Log Records for Multiple Remote SPBs | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 25 | 5.3.2.3. Log Sequence Numbers | | | — | — |
| 26 | 5.3.2.4. Log Collection by the SM | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 27 | 5.3.2.5. General Log System Failure | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 28 | 5.3.2.6. Log Report Signature Validity | | | — | — |
| 29 | 5.3.3.1. SM Proxy of Log Events | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 30 | 5.3.3.2. SM Proxy of Security Operations Events | | | Applies only to a device which implements features that allow it to | |

| | | | | | |
|---|---|---|---|---|---|
| 30 | 5.3.3.2. SM Proxy of Security Operations Events | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 31 | 5.3.3.3. SM Proxy of Security ASM Events | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 32 | 5.4.1.1. FrameSequencePlayed Event | | | — | — |
| 33 | 5.4.1.2. CPLStart Event | | | — | — |
| 34 | 5.4.1.3. CPLEnd Event | | | — | — |
| 35 | 5.4.1.4. PlayoutComplete Event | | | — | — |
| 36 | 5.4.1.5. CPLCheck Event | | | — | — |
| 37 | 5.4.1.6. KDMKeysReceived Event | | | — | — |
| 38 | 5.4.1.7. KDMDeleted Event | | | — | — |
| 39 | 5.4.2.6. SPBStartup and SPBShutdown Events | | | — | — |
| 40 | 5.4.2.7. SPBOpen and SPBClose Events | | | — | — |
| 41 | 5.4.2.8. SPBClockAdjust Event | | | — | — |
| 42 | 5.4.2.9. SPBMarriage and SPBDivorce Events | | | — | — |
| 43 | 5.4.2.10. SPBSoftware Event | | | — | — |
| 44 | 5.4.2.11. SPBSecurityAlert Event | (data only) | | — | — |
| 45 | 6.1.1. Image Integrity Checking | | | — | — |
| 46 | 6.1.2. Sound Integrity Checking | | | — | — |
| 47 | 6.1.4. Restriction of Keying to MD Type | | | — | — |
| 48 | 6.1.5. Restriction of Keying to Valid CPLs | | | — | — |
| 49 | 6.1.6. Remote SPB Integrity Monitoring | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 50 | 6.1.7. SPB Integrity Fault Consequences | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 51 | 6.1.8. Content Key Extension, End of Engagement | | | — | — |
| 52 | 6.1.9. ContentAuthenticator Element Check | | | — | — |
| 53 | 6.1.10. KDM Date Check | | | — | — |
| 54 | 6.1.11. KDM TDL Check | | | — | — |
| 55 | 6.1.12. Maximum Number of DCP Keys | | | — | — |
| 56 | 6.1.13. CPL Id Check | | | — | — |
| 57 | 6.1.15. Restriction of Playback in Absence | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 57 | 6.1.15. Restriction of Playback in Absence of Integrity Pack Metadata | | | — | — |
| 58 | 6.1.19. Plurality of Media Block Identity Certificates | | | — | — |
| 59 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 60 | 6.2.2. Special Auditorium Situation Operations | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 61 | 6.2.3. LE Key Usage | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 62 | 6.2.4. MB Link Encryption | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 63 | 6.3.1. Clock Adjustment | | | — | — |
| 64 | 6.3.2. SPB Type 1 Clock Battery | | | — | — |
| 65 | 6.3.3. Clock Resolution | | | — | — |
| 66 | 6.4.1. FM Application Constraints | | | — | — |
| 67 | 6.4.2. Granularity of FM Control | | | — | — |
| 68 | 6.4.3. FM Payload | | | — | — |
| 69 | 6.4.4. FM Audio Bypass | | | — | — |
| 70 | 6.4.5. Selective Audio FM Control | | | — | — |
| 71 | 6.5.1. Playback of Image Only Material | | | — | — |
| 72 | 6.5.2. Decoder Requirements | | | — | — |
| 73 | 6.6.1. Digital Audio Interfaces | | | — | — |
| 74 | 6.6.2. Audio Sample Rate Conversion | | | — | — |
| 75 | 6.6.3. Audio Delay Setup | | | — | — |
| 76 | 6.6.4. Click Free Splicing of Audio Track Files | | | — | — |
| 77 | 6.7.1. Media Block Overlay | | | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |
| 78 | 6.7.4. Default Timed Text Font | | | — | — |
| 79 | 6.7.6. Timed Text Decryption | | | — | — |
| 80 | 7.2.1. Projector and Direct View Display Physical Protection | | | — | — |
| 81 | 7.2.2. Projector and Direct View Display Security Servicing | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 82 | 7.2.6. SPB2 Secure Silicon Field Replacement | | | — | — |
| 83 | 7.2.7. Systems without Electronic Marriage | | | — | — |
| 84 | 7.2.8. Electronic Marriage Break Key Retaining | | | — | — |
| 85 | 7.3.2. Companion SPBs with Electronic Marriage | | | — | — |
| 86 | 7.3.3. Companion SPB Marriage Break Key Retaining | | | — | — |
| 87 | 7.5.1. Projector Overlay | | | — | — |
| 88 | 7.5.3. Projector Pixel Count/Structure | | | — | — |
| 89 | 7.5.4. Projector Spatial Resolution and Frame Rate Conversion | (data only) | | — | — |
| 90 | 7.5.5. White Point Luminance and Uniformity | (data only) | | — | — |
| 91 | 7.5.6. White Point Chromaticity and Uniformity | (data only) | | — | — |
| 92 | 7.5.7. Sequential Contrast | (data only) | | — | — |
| 93 | 7.5.8. Intra-frame Contrast | (data only) | | — | — |
| 94 | 7.5.9. Grayscale Tracking | (data only) | | — | — |
| 95 | 7.5.10. Contouring | (data only) | | — | — |
| 96 | 7.5.11. Transfer Function | (data only) | | — | — |
| 97 | 7.5.12. Color Accuracy | (data only) | | — | — |
| 98 | 8.1.1. Storage System Ingest Interface | | | — | — |
| 99 | 8.1.2. Storage System Capacity | | | — | — |
| 100 | 8.1.3. Storage System Redundancy | | | — | — |
| 101 | 8.1.4. Storage System Performance | | | — | — |
| 102 | 8.2.2. Show Playlist Creation | (data only) | | — | — |
| 103 | 8.2.3. Show Playlist Format | | | — | — |
| 104 | 8.2.5. Automation Control and Interfaces | | | — | — |
| 105 | 8.2.6. Interrupt Free Playback | | | — | — |
| 106 | 8.2.7. Artifact Free Transition of Image Format | | | — | — |
| 107 | 8.2.8. Restarting Playback | | | — | — |
| 108 | 8.2.9. SMS User Accounts | | | — | Record the available operator roles (names) and whether locally-defined accounts can be created. |
| 109 | 8.2.10. SMS Operator Identification | | | — | — |
| 110 | 8.2.11. SMS Identity and Certificate | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 111 | 8.2.12. Content Keys and TDL check | | | — | — |
| 112 | 8.2.14. KDM Content Keys Check | | | — | — |
| 113 | 8.2.15. Validity of SMS Certificates | | | — | — |

## 15.3. Projector with MB Design Review

For each requirement listed in the table below, prove that the system design meets the requirement by identifying the software or hardware mechanism that implements the requirement and analyzing the design to assure that the requirement has been met, subject to stipulated conditions. If a proof cannot be made, the design will be considered non-compliant with regard to the requirement. To perform this analysis the examiner will require access to exhibit documents (system design artifacts) such as schematic diagrams, implementation source code, unit test source code, state diagrams, design notes, etc. See Chapter 9: FIPS Requirements for a Type 1 SPB and Chapter 10: DCI Requirements Review for more information.

For each requirement, the examiner must record the identifiers of the exhibits consulted in proving the requirement, including applicable version identifiers, section or sheet numbers, grid identifiers, etc., and the examiner must record *Pass* or *Fail* to indicate whether or not the requirement has been met by the design. The examiner may also record any notes relevant to interpreting the exhibits and to the determination of the compliance status.

| Step | Procedure | Pass | Fail | Conditions | Exhibit Identifiers |
|---|---|---|---|---|---|
| 1 | 9.5.1. SM Operating Environment | | | — | |
| 2 | 9.5.2. LE Key Generation | | | — | |
| 3 | 9.5.3. SPB Type 1 Tamper Responsiveness | | | — | |
| 4 | 9.5.4. Security Design Description Requirements | | | — | |
| 5 | 9.5.6. SPB Type 1 FIPS Requirements | | | — | |
| 6 | 9.5.8. Asymmetric Key Generation | | | — | |
| 7 | 9.5.9. Critical Security Parameter Protection | | | — | |
| 8 | 10.4.1. Theater System Reliability | | | — | |
| 9 | 10.4.2. Theater System Storage Security | | | — | |
| 10 | 10.4.3. Security Devices Self-Test Capabilities | | | — | |
| 11 | 10.4.4. Security Entity Physical Protection | | | — | |
| 12 | 10.4.5. Secure SMS-SM Communication | | | — | |
| 13 | 10.4.6. Location of Security Manager | | | — | |
| 14 | 10.4.8. Secure Remote SPB-SM Communications | | | — | |
| 15 | 10.4.9. Playback Preparation | | | — | |
| 16 | 10.4.10. Special Auditorium Situation Detection | | | Applies only to a Type 1 SPB device or module which implements features that allow it to supply keys or content to a remote SPB. | |

| | | | | | |
|---|---|---|---|---|---|
| 17 | 10.4.11. Prevention of Keying of Compromised SPBs | | | — | |
| 18 | 10.4.12. SPB Authentication | | | — | |
| 19 | 10.4.13. TLS Session Key Refreshes | | | — | |
| 20 | 10.4.14. LE Key Issuance | | | — | |
| 21 | 10.4.15. Maximum Key Validity Period | | | — | |
| 22 | 10.4.16. KDM Purge upon Expiry | | | — | |
| 23 | 10.4.17. Key Usage Time Window | | | — | |
| 24 | 10.4.18. Projector Secure Silicon Device | | | — | |
| 25 | 10.4.19. Access to Projector Image Signals | | | — | |
| 26 | 10.4.20. Systems with Electronic Marriage | | | — | |
| 27 | 10.4.21. Systems Without Electronic Marriage | | | — | |
| 28 | 10.4.22. Clock Date-Time-Range | | | — | |
| 29 | 10.4.23. Clock Setup | | | — | |
| 30 | 10.4.24. Clock Stability | | | — | |
| 31 | 10.4.25. Repair and Renewal of SPBs | | | — | |
| 32 | 10.4.26. SPB2 Protected Devices | | | — | |
| 33 | 10.4.27. Clock Continuity | | | — | |
| 34 | 10.4.30. SMS and SPB Authentication and ITM Transport Layer | | | — | |
| 35 | 10.4.31. Idempotency of ITM RRPs | | | — | |
| 36 | 10.4.32. RRP Synchronism | | | — | |
| 37 | 10.4.33. TLS Mode Bypass Prohibition | | | — | |
| 38 | 10.4.34. RRP Broadcast Prohibition | | | — | |
| 39 | 10.4.35. Implementation of Proprietary ITMs | | | — | |
| 40 | 10.4.36. RRP Initiator | | | — | |
| 41 | 10.4.39. RRP "Busy" and Unsupported Types | | | — | |
| 42 | 10.4.40. RRP Operational Messages | | | — | |
| 43 | 10.4.42. FM Algorithm General Requirements | | | — | |
| 44 | 10.4.43. FM Insertion Requirements | | | — | |
| 45 | 10.4.44. IFM Visual Transparency | | | — | |
| 46 | 10.4.45. IFM Robustness | | | — | |
| 47 | 10.4.46. AFM Inaudibility | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 48 | 10.4.47. AFM Robustness | | | — | |
| 49 | 10.4.48. FM Control Instance | | | — | |
| 50 | 10.4.50. SE Log Authoring | | | — | |
| 51 | 10.4.51. SPB Log Storage Requirements | | | — | |
| 52 | 10.4.53. MB Log Storage Capabilities | | | — | |
| 53 | 10.4.54. Logging for Standalone Systems | | | — | |
| 54 | 10.4.55. Logging of Failed Procedures | | | — | |
| 55 | 10.4.56. SPB Log Failure | | | — | |
| 56 | 10.4.57. Log Purging in Failed SPBs | | | — | |
| 57 | 10.4.58. MB Tasks | | | — | |
| 58 | 10.4.59. Type 1 SPB RSA Private Keys | | | — | |
| 59 | 10.4.60. Content Keys Outside Secure Silicon | | | — | |
| 60 | 10.4.61. Prohibition of SPB Type 1 Field Serviceability | | | — | |
| 61 | 10.4.62. Use of Software Protection Methods | | | — | |
| 62 | 10.4.63. TMS Role | | | — | |
| 63 | 10.4.64. D-Cinema Security Parameter Protection | | | — | |
| 64 | 10.4.65. RSA Key Entropy | | | — | |
| 65 | 10.4.66. Preloaded Symmetric Key Entropy | | | — | |
| 66 | 10.4.67. MD Caching of Keys | | | — | |
| 67 | 10.4.68. SPB Type 1 Firmware Modifications | | | — | |
| 68 | 10.4.69. SPB Type 1 Log Retention | | | — | |
| 69 | 10.4.70. ASM Get Time Frequency | | | Applies only to a Type 1 SPB device or module which implements features that allow it to supply keys or content to a remote SPB. | |
| 70 | 10.4.72. SPB Secure Silicon Requirements | | | — | |
| 71 | 10.4.73. SPB Type 1 Battery Life | | | — | |
| 72 | 10.4.74. Companion SPB Retrieve Projector Cert | | | — | |
| 73 | 10.4.75. Log Collection for Married MB | | | — | |
| 74 | 10.4.76. Companion SPB Single Purpose Requirement | | | — | |
| 75 | 10.4.78. Projector SPB Log Reporting Requirements | | | — | |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 76 | 10.4.79. TLS RSA Requirement | | | — | |
| 77 | 10.4.80. Dual Certificate SMS Authentication | | | — | |
| 78 | 10.4.82. Export of KDM-Borne Keys | | | — | |

# Chapter 16. Link Decryptor/Encryptor Consolidated Test Sequence

## 16.1. Overview

The test sequence defined in this chapter is intended to be used to test a Link Decryptor/Encryptor device as the Test Subject, *i.e.* an image processor inserted between an Image Media Block and a Projector. The configuration and architecture of the device may vary, but the test sequence requires that the system consists of a single Type 1 SPB with signal interfaces for images and ASM messages.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 16.2. LD/LE Test Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 5.1.1. SPB Digital Certificate | | | — | — |
| 2 | 5.2.1. TLS Session Initiation | | | — | — |
| 3 | 5.2.2.1. Auditorium Security Message Support | | | — | — |
| 4 | 5.2.2.2. ASM Failure Behavior | | | — | — |
| 5 | 5.2.2.4. ASM "GetTime" | | | — | — |
| 6 | 5.2.2.5. ASM "GetEventList" | | | — | — |
| 7 | 5.2.2.6. ASM "GetEventID" | | | — | — |
| 8 | 5.2.2.7. ASM "LEKeyLoad" | | | | — |
| 9 | 5.2.2.8. ASM "LEKeyQueryID" | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 11 | 5.2.2.10. ASM "LEKeyPurgeID" | | | — | — |
| 12 | 5.2.2.11. ASM "LEKeyPurgeAll" | | | — | — |
| 13 | 5.2.2.12. ASM "GetProjCert" | | | — | — |
| 14 | 5.2.3. TLS Exception Logging | | | — | — |
| 15 | 5.3.2.1. Log Structure | | | — | — |
| 16 | 5.4.2.1. LinkOpened Event | | | — | — |
| 17 | 5.4.2.2. LinkClosed Event | | | — | — |
| 18 | 5.4.2.3. LinkException Event | | | — | — |
| 19 | 5.4.2.4. LogTransfer Event | | | — | — |
| 20 | 5.4.2.5. KeyTransfer Event | | | — | — |
| 21 | 5.4.2.6. SPBStartup and SPBShutdown Events | | | — | — |
| 22 | 5.4.2.8. SPBClockAdjust Event | | | — | — |
| 23 | 5.4.2.10. SPBSoftware Event | | | — | — |
| 24 | 5.4.2.11. SPBSecurityAlert Event | (data only) | | — | — |
| 25 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 26 | 6.3.2. SPB Type 1 Clock Battery | | | — | — |
| 27 | 7.3.4. Remote SPB Clock Adjustment | | | — | — |
| 28 | 7.4.2. LDB TLS Session Constraints | | | — | — |
| 29 | 7.4.5. LDB Key Storage | | | — | — |
| 30 | 7.4.6. LDB Key Purging | | | — | — |

## 16.3. LD/LE Design Review

For each requirement listed in the table below, prove that the system design meets the requirement by identifying the software or hardware mechanism that implements the requirement and analyzing the design to assure that the requirement has been met, subject to stipulated conditions. If a proof cannot be made, the design will be considered non-compliant with regard to the requirement. To perform this analysis the examiner will require access to exhibit documents (system design artifacts) such as schematic diagrams, implementation source code, unit test source code, state diagrams, design notes, etc. See Chapter 9: FIPS Requirements for a Type 1 SPB and Chapter 10: DCI Requirements Review for more information.

For each requirement, the examiner must record the identifiers of the exhibits consulted in proving the requirement, including applicable version identifiers, section or sheet numbers, grid identifiers, etc., and the examiner must record *Pass* or *Fail* to indicate whether or not the requirement has been met by the design. The examiner may also record any notes relevant to interpreting the exhibits and to the determination of the compliance status.

| Step | Procedure | Pass | Fail | Conditions | Exhibit Identifiers |
|---|---|---|---|---|---|
| 1 | 9.5.2. LE Key Generation | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 3 | 9.5.4. Security Design Description Requirements | | | — | |
| 4 | 9.5.6. SPB Type 1 FIPS Requirements | | | — | |
| 5 | 9.5.8. Asymmetric Key Generation | | | — | |
| 6 | 9.5.9. Critical Security Parameter Protection | | | — | |
| 7 | 10.4.1. Theater System Reliability | | | — | |
| 8 | 10.4.3. Security Devices Self-Test Capabilities | | | — | |
| 9 | 10.4.4. Security Entity Physical Protection | | | — | |
| 10 | 10.4.24. Clock Stability | | | — | |
| 11 | 10.4.25. Repair and Renewal of SPBs | | | — | |
| 12 | 10.4.27. Clock Continuity | | | — | |
| 13 | 10.4.30. SMS and SPB Authentication and ITM Transport Layer | | | — | |
| 14 | 10.4.31. Idempotency of ITM RRPs | | | — | |
| 15 | 10.4.32. RRP Synchronism | | | — | |
| 16 | 10.4.33. TLS Mode Bypass Prohibition | | | — | |
| 17 | 10.4.34. RRP Broadcast Prohibition | | | — | |
| 18 | 10.4.35. Implementation of Proprietary ITMs | | | — | |
| 19 | 10.4.36. RRP Initiator | | | — | |
| 20 | 10.4.40. RRP Operational Messages | | | — | |
| 21 | 10.4.50. SE Log Authoring | | | — | |
| 22 | 10.4.51. SPB Log Storage Requirements | | | — | |
| 23 | 10.4.52. Remote SPB Log Storage Requirements | | | — | |
| 24 | 10.4.54. Logging for Standalone Systems | | | — | |
| 25 | 10.4.55. Logging of Failed Procedures | | | — | |
| 26 | 10.4.56. SPB Log Failure | | | — | |
| 27 | 10.4.57. Log Purging in Failed SPBs | | | — | |
| 28 | 10.4.59. Type 1 SPB RSA Private Keys | | | — | |
| 29 | 10.4.61. Prohibition of SPB Type 1 Field Serviceability | | | — | |
| 30 | 10.4.62. Use of Software Protection Methods | | | — | |
| 31 | 10.4.64. D-Cinema Security Parameter Protection | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 32 | 10.4.65. RSA Key Entropy | | | — | |
| 33 | 10.4.66. Preloaded Symmetric Key Entropy | | | — | |
| 34 | 10.4.68. SPB Type 1 Firmware Modifications | | | — | |
| 35 | 10.4.69. SPB Type 1 Log Retention | | | — | |
| 36 | 10.4.72. SPB Secure Silicon Requirements | | | — | |
| 37 | 10.4.73. SPB Type 1 Battery Life | | | — | |
| 38 | 10.4.79. TLS RSA Requirement | | | — | |

# Chapter 17. Digital Cinema Server Consolidated Confidence Sequence

## 17.1. Overview

The confidence sequence defined in this chapter is intended to be used to test a stand-alone d-cinema *server* as the Test Subject. The configuration and architecture of the Test Subject may vary, but the confidence sequence requires that the system consists of at least an Image Media Block (IMB, containing a Security Manager, Media Decryptor, Link Encryptor, etc.) and a Screen Management Server (SMS). For the purpose of this test, the Test Operator may substitute a Theater Management Server (TMS) for the SMS if it implements the required functionality. Wherever a test procedure refers to an SMS, the equivalent TMS may also be used. A complete Server Test Sequence report containing no failures is a prerequisite to execution of this sequence.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject and the original CTP compliance test conducted per Chapter 13: Digital Cinema Server Consolidated Test Sequence. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 17.2. Server Confidence Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 5.1.1. SPB Digital Certificate | | | — | — |
| 2 | 5.3.3.3. SM Proxy of Security ASM Events | | | — | — |
| 3 | 5.4.1.6. KDMKeysReceived Event | | | — | — |
| 4 | 5.4.2.10. SPBSoftware Event | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 5 | 6.1.5. Restriction of Keying to Valid CPLs | | | — | — |
| 6 | 6.1.7. SPB Integrity Fault Consequences | | | — | — |
| 7 | 6.1.8. Content Key Extension, End of Engagement | | | — | — |
| 8 | 6.1.9. ContentAuthenticator Element Check | | | — | — |
| 9 | 6.1.11. KDM TDL Check | | | — | — |
| 10 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 11 | 6.2.4. MB Link Encryption | | | — | — |
| 12 | 6.3.1. Clock Adjustment | | | — | — |
| 13 | 6.4.3. FM Payload | | | — | — |
| 14 | 8.2.7. Artifact Free Transition of Image Format | | | — | — |
| 15 | 8.2.11. SMS Identity and Certificate | | | — | — |
| 16 | 8.2.15. Validity of SMS Certificates | | | — | — |

# Chapter 18. Digital Cinema Projector Consolidated Confidence Sequence

## 18.1. Overview

The confidence sequence defined in this chapter is intended to be used to test a stand-alone d-cinema projector as the Test Subject. The configuration and architecture of the projector may vary, but the confidence sequence requires that the system consists of at least a Link Decryptor Block (LDB) and a light processing system including electronic and optical components (Projector).

Before performing the confidence sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 18.2. Projector Confidence Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 2 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 3 | 7.2.2. Projector and Direct View Display Security Servicing | | | — | — |
| 4 | 7.3.2. Companion SPBs with Electronic Marriage | | | — | — |
| 5 | 7.3.3. Companion SPB Marriage Break Key Retaining | | | — | — |
| 6 | 7.5.3. Projector Pixel Count/Structure | | | — | — |

# Chapter 19. Digital Cinema Projector with MB Consolidated Confidence Sequence

## 19.1. Overview

The confidence sequence defined in this chapter is intended to be used to test a d-cinema projector with an integrated Image Media Block (IMB) as the Test Subject. The configuration and architecture of the system may vary, but the confidence sequence requires that the system consists of at least a light processing system including electronic and optical components (Projector), an Image Media Block (containing a Security Manager, Media Decryptor, etc.), and a Screen Management Server (SMS). For the purpose of this test, the Test Operator may substitute a Theater Management Server (TMS) for the SMS if it implements the required functionality. Wherever a test procedure refers to an SMS, the equivalent TMS may also be used.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 19.2. Projector with MB Confidence Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 5.1.1. SPB Digital Certificate | | | — | — |
| 2 | 5.2.2.7. ASM "LEKeyLoad" | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 3 | 5.3.3.3. SM Proxy of Security ASM Events | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 5.4.1.6. KDMKeysReceived Event | | | — | — |
| 5 | 5.4.2.10. SPBSoftware Event | | | — | — |
| 6 | 6.1.5. Restriction of Keying to Valid CPLs | | | — | — |
| 7 | 6.1.6. Remote SPB Integrity Monitoring | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 8 | 6.1.7. SPB Integrity Fault Consequences | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 9 | 6.1.8. Content Key Extension, End of Engagement | | | — | — |
| 10 | 6.1.9. ContentAuthenticator Element Check | | | — | — |
| 11 | 6.1.11. KDM TDL Check | | | — | — |
| 12 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 13 | 6.2.4. MB Link Encryption | | | Applies only to a device which implements features that allow it to supply keys or content to a remote SPB. | — |
| 14 | 6.3.1. Clock Adjustment | | | — | — |
| 15 | 6.4.3. FM Payload | | | — | — |
| 16 | 7.2.2. Projector and Direct View Display Security Servicing | | | — | — |
| 17 | 7.2.8. Electronic Marriage Break Key Retaining | | | — | — |
| 18 | 7.3.2. Companion SPBs with Electronic Marriage | | | — | — |
| 19 | 7.3.3. Companion SPB Marriage Break Key Retaining | | | — | — |
| 20 | 7.5.3. Projector Pixel Count/Structure | | | — | — |
| 21 | 8.2.7. Artifact Free Transition of Image Format | | | — | — |
| 22 | 8.2.11. SMS Identity and Certificate | | | — | — |
| 23 | 8.2.12. Content Keys and TDL check | | | — | — |
| 24 | 8.2.15. Validity of SMS Certificates | | | — | — |

# Chapter 20. OMB Consolidated Test Sequence

## 20.1. Overview

The test sequence defined in this chapter is intended to be used to test an Outboard Media Block (OMB) as the Test Subject. The configuration and architecture of the system may vary, but the test sequence requires that the system consists of at least an OMB, IMB and SMS. For the purpose of this test, the Test Operator may substitute a Theater Management Server/System (TMS) for the SMS if it implements the required functionality. Wherever a test procedure refers to an SMS, the equivalent TMS may also be used.

Prior to participating in any tests of this chapter, the IMB must be certificated either by a previous Chapter 15 CTP report, by passing all Chapter 15 test requirements as part of the current procedure, or as enabled by a Chapter 15 family grouping or confidence retest.

Digital cinema systems that include an OMB operate in Multiple Media Block (MMB) mode, wherein the SMS is responsible for managing playout processes of the OMB and IMB, and the IMB provides synchronization to the OMB. The IMB must also be able to play only a portion of the total content in a composition, as the OMB will be handling some of the content. Thus, the IMB and SMS must be "MMB Capable" to function within a MMB architecture. This Chapter contains specific tests for the IMB and SMS to test for this capability.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 20.2. OMB Test Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 3.5.10. KDM NonCriticalExtensions Element (OBAE) | | | — | — |
| 2 | 3.5.11. ETM IssueDate Field Check (OBAE) | | | — | — |
| 3 | 3.5.12. Structure ID Check (OBAE) | | | — | — |
| 4 | 3.5.13. Certificate Thumbprint Check (OBAE) | | | — | — |
| 5 | 3.5.14. KeyInfo Field Check (OBAE) | | | — | — |
| 6 | 3.5.15. KDM Malformations (OBAE) | | | — | — |
| 7 | 3.5.16. KDM Signature (OBAE) | | | — | — |
| 8 | 5.1.1. SPB Digital Certificate | | | — | — |
| 9 | 5.3.2.1. Log Structure | | | — | — |
| 10 | 5.3.2.7. Log Sequence Numbers (OBAE) | | | — | — |
| 11 | 5.3.2.8. Log Report Signature Validity | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 11 | 5.3.2.8. Log Report Signature Validity (OBAE) | | | — | — |
| 12 | 5.4.1.8. FrameSequencePlayed Event (OBAE) | | | — | — |
| 13 | 5.4.1.9. CPLStart Event (OBAE) | | | — | — |
| 14 | 5.4.1.10. CPLEnd Event (OBAE) | | | — | — |
| 15 | 5.4.1.11. PlayoutComplete Event (OBAE) | | | — | — |
| 16 | 5.4.1.12. CPLCheck Event (OBAE) | | | — | — |
| 17 | 5.4.1.13. KDMKeysReceived Event (OBAE) | | | — | — |
| 18 | 5.4.1.14. KDMDeleted Event (OBAE) | | | — | — |
| 19 | 5.4.2.6. SPBStartup and SPBShutdown Events | | | — | — |
| 20 | 5.4.2.8. SPBClockAdjust Event | | | — | — |
| 21 | 5.4.2.10. SPBSoftware Event | | | — | — |
| 22 | 6.1.12. Maximum Number of DCP Keys | | | — | — |
| 23 | 6.1.13. CPL Id Check | | | — | — |
| 24 | 6.1.14. CPL Id Check (OBAE) | | | — | — |
| 25 | 6.1.15. Restriction of Playback in Absence of Integrity Pack Metadata | | | — | — |
| 26 | 6.1.16. Restriction of Keying to MDEK Type (OBAE) | | | — | — |
| 27 | 6.1.17. OBAE Integrity Checking | | | — | — |
| 28 | 6.1.18. Content Key Extension, End of Engagement (OBAE) | | | — | — |
| 29 | 6.1.19. Plurality of Media Block Identity Certificates | | | — | — |
| 30 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 31 | 6.1.21. Maximum Number of DCP Keys (OBAE) | | | — | — |
| 32 | 6.1.22. Restriction of Keying to Valid CPLs (OBAE) | | | — | — |
| 33 | 6.1.23. ContentAuthenticator Element Check (OBAE) | | | — | — |
| 34 | 6.1.24. KDM Date Check (OBAE) | | | — | — |
| 35 | 6.3.1. Clock Adjustment | | | — | — |
| 36 | 6.3.2. SPB Type 1 Clock Battery | | | — | — |
| 37 | 6.3.4. Clock Resolution (OMB) | | | — | — |
| 38 | 6.3.5. Clock Adjustment (OMB) | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 39 | 6.4.6. FM Application Constraints (OBAE) | | | — | — |
| 40 | 6.4.7. Granularity of FM Control (OBAE) | | | — | — |
| 41 | 6.4.8. FM Payload (OBAE) | | | — | — |
| 42 | 6.4.9. FM Audio Bypass (OBAE) | | | — | — |
| 43 | 6.5.1. Playback of Image Only Material | | | — | — |
| 44 | 6.8.1. Click Free Splicing of OBAE Track Files | | | — | — |
| 45 | 6.8.2. OBAE Delay Setup | | | — | — |
| 46 | 6.8.3. Maximum Bitrate OBAE | | | — | — |
| 47 | 6.8.4. OBAE Rendering Expectations | | | — | — |
| 48 | 8.1.1. Storage System Ingest Interface | | | — | — |
| 49 | 8.1.2. Storage System Capacity | | | — | — |
| 50 | 8.1.5. Storage System Redundancy (OBAE) | | | — | — |
| 51 | 8.1.6. Storage System Performance (OBAE) | | | — | — |
| 52 | 8.2.3. Show Playlist Format | | | — | — |
| 53 | 8.2.9. SMS User Accounts | | | — | Record the available operator roles (names) and whether locally-defined accounts can be created. |
| 54 | 8.2.11. SMS Identity and Certificate | | | — | — |
| 55 | 8.2.13. Content Keys and TDL check (OBAE) | | | — | — |
| 56 | 8.2.14. KDM Content Keys Check | | | — | — |
| 57 | 8.2.15. Validity of SMS Certificates | | | — | — |
| 58 | 8.2.16. Interrupt Free Playback (OBAE) | | | — | — |
| 59 | 8.2.17. Restarting Playback (OBAE) | | | — | — |
| 60 | 8.2.18. Show Playlist Creation (OBAE) | (data only) | | — | — |
| 61 | 8.2.19. Automation Control and Interfaces (OBAE) | | | — | — |
| 62 | 8.2.20. SMS Operator Identification (OBAE) | | | — | — |

## 20.3. OMB Design Review

For each requirement listed in the table below, prove that the system design meets the requirement by identifying the software or hardware mechanism that implements the requirement and analyzing the design to assure that the requirement has been met, subject to stipulated conditions. If a proof cannot be made, the design will be considered non-compliant with regard to the requirement. To perform this analysis the examiner will require access to exhibit documents (system design artifacts) such as schematic diagrams,

implementation source code, unit test source code, state diagrams, design notes, etc. See Chapter 9: FIPS Requirements for a Type 1 SPB and Chapter 10: DCI Requirements Review for more information.

For each requirement, the examiner must record the identifiers of the exhibits consulted in proving the requirement, including applicable version identifiers, section or sheet numbers, grid identifiers, etc., and the examiner must record Pass or Fail to indicate whether or not the requirement has been met by the design. The examiner may also record any notes relevant to interpreting the exhibits and to the determination of the compliance status

| Step | Procedure | Pass | Fail | Conditions | Exhibit Identifiers |
|---|---|---|---|---|---|
| 1 | 9.5.1. SM Operating Environment | | | — | |
| 2 | 9.5.3. SPB Type 1 Tamper Responsiveness | | | — | |
| 3 | 9.5.4. Security Design Description Requirements | | | — | |
| 4 | 9.5.6. SPB Type 1 FIPS Requirements | | | — | |
| 5 | 9.5.8. Asymmetric Key Generation | | | — | |
| 6 | 9.5.9. Critical Security Parameter Protection | | | — | |
| 7 | 10.4.1. Theater System Reliability | | | — | |
| 8 | 10.4.2. Theater System Storage Security | | | — | |
| 9 | 10.4.3. Security Devices Self-Test Capabilities | | | — | |
| 10 | 10.4.4. Security Entity Physical Protection | | | — | |
| 11 | 10.4.5. Secure SMS-SM Communication | | | — | |
| 12 | 10.4.6. Location of Security Manager | | | — | |
| 13 | 10.4.9. Playback Preparation | | | — | |
| 14 | 10.4.16. KDM Purge upon Expiry | | | — | |
| 15 | 10.4.17. Key Usage Time Window | | | — | |
| 16 | 10.4.22. Clock Date-Time-Range | | | — | |
| 17 | 10.4.23. Clock Setup | | | — | |
| 18 | 10.4.24. Clock Stability | | | — | |
| 19 | 10.4.25. Repair and Renewal of SPBs | | | — | |
| 20 | 10.4.27. Clock Continuity | | | — | |
| 21 | 10.4.28. TLS Endpoints | | | — | |
| 22 | 10.4.28. TLS Endpoints | | | — | |
| 23 | 10.4.30. SMS and SPB Authentication and ITM Transport Layer | | | — | |
| 24 | 10.4.31. Idempotency of ITM RRPs | | | — | |
| 25 | 10.4.32. RRP Synchronism | | | — | |
| 26 | 10.4.33. TLS Mode Bypass Prohibition | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 27 | 10.4.34. RRP Broadcast Prohibition | | | — | |
| 28 | 10.4.35. Implementation of Proprietary ITMs | | | — | |
| 29 | 10.4.36. RRP Initiator | | | — | |
| 30 | 10.4.39. RRP "Busy" and Unsupported Types | | | — | |
| 31 | 10.4.40. RRP Operational Messages | | | — | |
| 32 | 10.4.42. FM Algorithm General Requirements | | | — | |
| 33 | 10.4.43. FM Insertion Requirements | | | — | |
| 34 | 10.4.44. IFM Visual Transparency | | | — | |
| 35 | 10.4.45. IFM Robustness | | | — | |
| 36 | 10.4.46. AFM Inaudibility | | | — | |
| 37 | 10.4.47. AFM Robustness | | | — | |
| 38 | 10.4.48. FM Control Instance | | | — | |
| 39 | 10.4.50. SE Log Authoring | | | — | |
| 40 | 10.4.51. SPB Log Storage Requirements | | | — | |
| 41 | 10.4.53. MB Log Storage Capabilities | | | — | |
| 42 | 10.4.54. Logging for Standalone Systems | | | — | |
| 43 | 10.4.55. Logging of Failed Procedures | | | — | |
| 44 | 10.4.56. SPB Log Failure | | | — | |
| 45 | 10.4.57. Log Purging in Failed SPBs | | | — | |
| 46 | 10.4.58. MB Tasks | | | — | |
| 47 | 10.4.59. Type 1 SPB RSA Private Keys | | | — | |
| 48 | 10.4.60. Content Keys Outside Secure Silicon | | | — | |
| 49 | 10.4.61. Prohibition of SPB Type 1 Field Serviceability | | | — | |
| 50 | 10.4.62. Use of Software Protection Methods | | | — | |
| 51 | 10.4.63. TMS Role | | | — | |
| 52 | 10.4.64. D-Cinema Security Parameter Protection | | | — | |
| 53 | 10.4.65. RSA Key Entropy | | | — | |
| 54 | 10.4.66. Preloaded Symmetric Key Entropy | | | — | |
| 55 | 10.4.67. MD Caching of Keys | | | — | |
| 56 | 10.4.68. SPB Type 1 Firmware | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Modifications | | | — | | |
| 57 | 10.4.69. SPB Type 1 Log Retention | | | — | |
| 58 | 10.4.72. SPB Secure Silicon Requirements | | | — | |
| 59 | 10.4.73. SPB Type 1 Battery Life | | | — | |
| 60 | 10.4.80. Dual Certificate SMS Authentication | | | — | |
| 61 | 10.4.81. Constrained OMB Processing Capability | | | — | |
| 62 | 10.4.82. Export of KDM-Borne Keys | | | — | |
| 63 | 10.4.84. OBAE Addendum | | | — | |
| 64 | 10.4.85. OBAE FM Robustness | | | — | |
| 65 | 10.4.86. OBAE FM Inaudibility | | | — | |

# Chapter 21. Digital Cinema Projector with IMBO Consolidated Test Sequence

## 21.1. Overview

The test sequence defined in this chapter is intended to be used to test a d-cinema projector with an integrated Image Media Block with OMB functions (IMBO) as the Test Subject. The configuration and architecture of the system may vary, but the test sequence requires that the system consists of at least a light processing system including electronic and optical components (Projector), an IMBO (containing a Security Manager, Media Decryptors, image, main sound and OBAE sound processing, etc.), and a Screen Management Server/System (SMS). For the purpose of this test, the Test Operator may substitute a Theater Management Server/System (TMS) for the SMS if it implements the required functionality. Wherever a test procedure refers to an SMS, the equivalent TMS may also be used.

For the purpose of compliance testing as defined in this Chapter, the spatial resolution of the projector shall be no less than that of the Media Block.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 21.2. Digital Cinema Projector with IMBO Test Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in

greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 3.5.1. KDM NonCriticalExtensions Element | | | — | — |
| 2 | 3.5.2. ETM IssueDate Field Check | | | — | — |
| 3 | 3.5.4. Structure ID Check | | | — | — |
| 4 | 3.5.5. Certificate Thumbprint Check | | | — | — |
| 5 | 3.5.7. KeyInfo Field Check | | | — | — |
| 6 | 3.5.8. KDM Malformations | | | — | — |
| 7 | 3.5.9. KDM Signature | | | — | — |
| 8 | 5.1.1. SPB Digital Certificate | | | — | — |
| 9 | 5.3.2.1. Log Structure | | | — | — |
| 10 | 5.3.2.3. Log Sequence Numbers | | | — | — |
| 11 | 5.3.2.6. Log Report Signature Validity | | | — | — |
| 12 | 5.4.1.1. FrameSequencePlayed Event | | | — | — |
| 13 | 5.4.1.2. CPLStart Event | | | — | — |
| 14 | 5.4.1.3. CPLEnd Event | | | — | — |
| 15 | 5.4.1.4. PlayoutComplete Event | | | — | — |
| 16 | 5.4.1.5. CPLCheck Event | | | — | — |
| 17 | 5.4.1.6. KDMKeysReceived Event | | | — | — |
| 18 | 5.4.1.7. KDMDeleted Event | | | — | — |
| 19 | 5.4.1.8. FrameSequencePlayed Event (OBAE) | | | — | — |
| 20 | 5.4.2.6. SPBStartup and SPBShutdown Events | | | — | — |
| 21 | 5.4.2.7. SPBOpen and SPBClose Events | | | — | — |
| 22 | 5.4.2.8. SPBClockAdjust Event | | | — | — |
| 23 | 5.4.2.9. SPBMarriage and SPBDivorce Events | | | — | — |
| 24 | 5.4.2.10. SPBSoftware Event | | | — | — |
| 25 | 5.4.2.11. SPBSecurityAlert Event | (data only) | | — | — |
| 26 | 6.1.1. Image Integrity Checking | | | — | — |
| 27 | 6.1.2. Sound Integrity Checking | | | — | — |
| 28 | 6.1.4. Restriction of Keying to MD Type | | | — | — |
| 29 | 6.1.5. Restriction of Keying to Valid CPLs | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 30 | 6.1.8. Content Key Extension, End of Engagement | | | — | — |
| 31 | 6.1.9. ContentAuthenticator Element Check | | | — | — |
| 32 | 6.1.10. KDM Date Check | | | — | — |
| 33 | 6.1.11. KDM TDL Check | | | — | — |
| 34 | 6.1.12. Maximum Number of DCP Keys | | | — | — |
| 35 | 6.1.13. CPL Id Check | | | — | — |
| 36 | 6.1.14. CPL Id Check (OBAE) | | | — | — |
| 37 | 6.1.15. Restriction of Playback in Absence of Integrity Pack Metadata | | | — | — |
| 38 | 6.1.16. Restriction of Keying to MDEK Type (OBAE) | | | — | — |
| 39 | 6.1.17. OBAE Integrity Checking | | | — | — |
| 40 | 6.1.18. Content Key Extension, End of Engagement (OBAE) | | | — | — |
| 41 | 6.1.19. Plurality of Media Block Identity Certificates | | | — | — |
| 42 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 43 | 6.1.21. Maximum Number of DCP Keys (OBAE) | | | — | — |
| 44 | 6.3.1. Clock Adjustment | | | — | — |
| 45 | 6.3.2. SPB Type 1 Clock Battery | | | — | — |
| 46 | 6.3.3. Clock Resolution | | | — | — |
| 47 | 6.4.1. FM Application Constraints | | | — | — |
| 48 | 6.4.2. Granularity of FM Control | | | — | — |
| 49 | 6.4.3. FM Payload | | | — | — |
| 50 | 6.4.4. FM Audio Bypass | | | — | — |
| 51 | 6.4.5. Selective Audio FM Control | | | — | — |
| 52 | 6.4.6. FM Application Constraints (OBAE) | | | — | — |
| 53 | 6.4.7. Granularity of FM Control (OBAE) | | | — | — |
| 54 | 6.4.8. FM Payload (OBAE) | | | — | — |
| 55 | 6.4.9. FM Audio Bypass (OBAE) | | | — | — |
| 56 | 6.5.1. Playback of Image Only Material | | | — | — |
| 57 | 6.5.2. Decoder Requirements | | | — | — |
| 58 | 6.6.1. Digital Audio Interfaces | | | — | — |
| 59 | 6.6.2. Audio Sample Rate Conversion | | | — | — |
| 60 | 6.6.3. Audio Delay Setup | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 61 | 6.6.4. Click Free Splicing of Audio Track Files | | | — | — |
| 62 | 6.7.1. Media Block Overlay | | | Applies to a Media Block that implements an alpha channel overlay module, a subpicture renderer (a module that converts the subpicture file into a baseband image file with an alpha channel) and a Timed Text renderer (a module that converts Timed Text data into a baseband image file with an alpha channel) | — |
| 63 | 6.7.4. Default Timed Text Font | | | — | — |
| 64 | 6.7.6. Timed Text Decryption | | | — | — |
| 65 | 6.8.1. Click Free Splicing of OBAE Track Files | | | — | — |
| 66 | 6.8.2. OBAE Delay Setup | | | — | — |
| 67 | 6.8.3. Maximum Bitrate OBAE | | | — | — |
| 68 | 6.8.4. OBAE Rendering Expectations | | | — | — |
| 69 | 7.2.1. Projector and Direct View Display Physical Protection | | | — | — |
| 70 | 7.2.2. Projector and Direct View Display Security Servicing | | | — | — |
| 71 | 7.2.6. SPB2 Secure Silicon Field Replacement | | | — | — |
| 72 | 7.2.7. Systems without Electronic Marriage | | | — | — |
| 73 | 7.2.8. Electronic Marriage Break Key Retaining | | | — | — |
| 74 | 7.3.2. Companion SPBs with Electronic Marriage | | | — | — |
| 75 | 7.3.3. Companion SPB Marriage Break Key Retaining | | | — | — |
| 76 | 7.5.1. Projector Overlay | | | — | — |
| 77 | 7.5.3. Projector Pixel Count/Structure | | | — | — |
| 78 | 7.5.4. Projector Spatial Resolution and Frame Rate Conversion | | | — | — |
| 79 | 7.5.5. White Point Luminance and Uniformity | | | — | — |
| 80 | 7.5.6. White Point Chromaticity and Uniformity | | | — | — |
| 81 | 7.5.7. Sequential Contrast | | | — | — |
| 82 | 7.5.8. Intra-frame Contrast | | | — | — |
| 83 | 7.5.9. Grayscale Tracking | | | — | — |
| 84 | 7.5.10. Contouring | | | — | — |

| | | | | | |
|---|---|---|---|---|---|
| 85 | 7.5.11. Transfer Function | | | — | — |
| 86 | 7.5.12. Color Accuracy | | | — | — |
| 87 | 8.1.1. Storage System Ingest Interface | | | — | — |
| 88 | 8.1.2. Storage System Capacity | | | — | — |
| 89 | 8.1.3. Storage System Redundancy | | | — | — |
| 90 | 8.1.4. Storage System Performance | | | — | — |
| 91 | 8.2.2. Show Playlist Creation | | | — | — |
| 92 | 8.2.3. Show Playlist Format | | | — | — |
| 93 | 8.2.5. Automation Control and Interfaces | | | — | — |
| 94 | 8.2.6. Interrupt Free Playback | | | — | — |
| 95 | 8.2.7. Artifact Free Transition of Image Format | | | — | — |
| 96 | 8.2.8. Restarting Playback | | | — | — |
| 97 | 8.2.9. SMS User Accounts | | | — | — |
| 98 | 8.2.10. SMS Operator Identification | | | — | — |
| 99 | 8.2.11. SMS Identity and Certificate | | | — | — |
| 100 | 8.2.12. Content Keys and TDL check | | | — | — |
| 101 | 8.2.13. Content Keys and TDL check (OBAE) | | | — | — |
| 102 | 8.2.14. KDM Content Keys Check | | | — | — |
| 103 | 8.2.15. Validity of SMS Certificates | | | — | — |

## 21.3. Digital Cinema Projector with IMBO Design Review

For each requirement listed in the table below, prove that the system design meets the requirement by identifying the software or hardware mechanism that implements the requirement and analyzing the design to assure that the requirement has been met, subject to stipulated conditions. If a proof cannot be made, the design will be considered non-compliant with regard to the requirement. To perform this analysis the examiner will require access to exhibit documents (system design artifacts) such as schematic diagrams, implementation source code, unit test source code, state diagrams, design notes, etc. See Chapter 9: FIPS Requirements for a Type 1 SPB and Chapter 10: DCI Requirements Review for more information.

For each requirement, the examiner must record the identifiers of the exhibits consulted in proving the requirement, including applicable version identifiers, section or sheet numbers, grid identifiers, etc., and the examiner must record Pass or Fail to indicate whether or not the requirement has been met by the design. The examiner may also record any notes relevant to interpreting the exhibits and to the determination of the compliance status

| Step | Procedure | Pass | Fail | Conditions | Exhibit Identifiers |
|---|---|---|---|---|---|
| 1 | 9.5.1. SM Operating Environment | | | — | |
| 2 | 9.5.3. SPB Type 1 Tamper Responsiveness | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 3 | 9.5.4. Security Design Description Requirements | | | — | |
| 4 | 9.5.6. SPB Type 1 FIPS Requirements | | | — | |
| 5 | 9.5.8. Asymmetric Key Generation | | | — | |
| 6 | 9.5.9. Critical Security Parameter Protection | | | — | |
| 7 | 10.4.1. Theater System Reliability | | | — | |
| 8 | 10.4.2. Theater System Storage Security | | | — | |
| 9 | 10.4.3. Security Devices Self-Test Capabilities | | | — | |
| 10 | 10.4.4. Security Entity Physical Protection | | | — | |
| 11 | 10.4.5. Secure SMS-SM Communication | | | — | |
| 12 | 10.4.6. Location of Security Manager | | | — | |
| 13 | 10.4.9. Playback Preparation | | | — | |
| 14 | 10.4.16. KDM Purge upon Expiry | | | — | |
| 15 | 10.4.17. Key Usage Time Window | | | — | |
| 16 | 10.4.18. Projector Secure Silicon Device | | | — | |
| 17 | 10.4.19. Access to Projector Image Signals | | | — | |
| 18 | 10.4.20. Systems with Electronic Marriage | | | — | |
| 19 | 10.4.21. Systems Without Electronic Marriage | | | — | |
| 20 | 10.4.22. Clock Date-Time-Range | | | — | |
| 21 | 10.4.23. Clock Setup | | | — | |
| 22 | 10.4.24. Clock Stability | | | — | |
| 23 | 10.4.25. Repair and Renewal of SPBs | | | — | |
| 24 | 10.4.26. SPB2 Protected Devices | | | — | |
| 25 | 10.4.27. Clock Continuity | | | — | |
| 26 | 10.4.30. SMS and SPB Authentication and ITM Transport Layer | | | — | |
| 27 | 10.4.31. Idempotency of ITM RRPs | | | — | |
| 28 | 10.4.32. RRP Synchronism | | | — | |
| 29 | 10.4.33. TLS Mode Bypass Prohibition | | | — | |
| 30 | 10.4.34. RRP Broadcast Prohibition | | | — | |
| 31 | 10.4.35. Implementation of Proprietary ITMs | | | — | |
| 32 | 10.4.36. RRP Initiator | | | — | |
| 33 | 10.4.39. RRP "Busy" and Unsupported Types | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 34 | 10.4.40. RRP Operational Messages | | | — | |
| 35 | 10.4.42. FM Algorithm General Requirements | | | — | |
| 36 | 10.4.43. FM Insertion Requirements | | | — | |
| 37 | 10.4.44. IFM Visual Transparency | | | — | |
| 38 | 10.4.45. IFM Robustness | | | — | |
| 39 | 10.4.46. AFM Inaudibility | | | — | |
| 40 | 10.4.47. AFM Robustness | | | — | |
| 41 | 10.4.48. FM Control Instance | | | — | |
| 42 | 10.4.50. SE Log Authoring | | | — | |
| 43 | 10.4.51. SPB Log Storage Requirements | | | — | |
| 44 | 10.4.53. MB Log Storage Capabilities | | | — | |
| 45 | 10.4.54. Logging for Standalone Systems | | | — | |
| 46 | 10.4.55. Logging of Failed Procedures | | | — | |
| 47 | 10.4.56. SPB Log Failure | | | — | |
| 48 | 10.4.57. Log Purging in Failed SPBs | | | — | |
| 49 | 10.4.58. MB Tasks | | | — | |
| 50 | 10.4.59. Type 1 SPB RSA Private Keys | | | — | |
| 51 | 10.4.60. Content Keys Outside Secure Silicon | | | — | |
| 52 | 10.4.61. Prohibition of SPB Type 1 Field Serviceability | | | — | |
| 53 | 10.4.62. Use of Software Protection Methods | | | — | |
| 54 | 10.4.63. TMS Role | | | — | |
| 55 | 10.4.64. D-Cinema Security Parameter Protection | | | — | |
| 56 | 10.4.65. RSA Key Entropy | | | — | |
| 57 | 10.4.66. Preloaded Symmetric Key Entropy | | | — | |
| 58 | 10.4.67. MD Caching of Keys | | | — | |
| 59 | 10.4.68. SPB Type 1 Firmware Modifications | | | — | |
| 60 | 10.4.69. SPB Type 1 Log Retention | | | — | |
| 61 | 10.4.72. SPB Secure Silicon Requirements | | | — | |
| 62 | 10.4.73. SPB Type 1 Battery Life | | | — | |
| 63 | 10.4.74. Companion SPB Retrieve Projector Cert | | | — | |

| | | | | | |
|---|---|---|---|---|---|
| 64 | 10.4.75. Log Collection for Married MB | | | — | |
| 65 | 10.4.76. Companion SPB Single Purpose Requirement | | | — | |
| 66 | 10.4.78. Projector SPB Log Reporting Requirements | | | — | |
| 67 | 10.4.80. Dual Certificate SMS Authentication | | | — | |
| 68 | 10.4.82. Export of KDM-Borne Keys | | | — | |
| 69 | 10.4.84. OBAE Addendum | | | — | |
| 70 | 10.4.85. OBAE FM Robustness | | | — | |
| 71 | 10.4.86. OBAE FM Inaudibility | | | — | |

# Chapter 22. OMB Consolidated Confidence Sequence

## 22.1. Overview

The test sequence defined in this chapter is intended to be used to test for confidence of an Outboard Media Block (OMB) as the Test Subject. The configuration and architecture of the system may vary, but the test sequence requires that the system consists of at least an OMB, IMB and SMS. For the purpose of this test, the Test Operator may substitute a Theater Management Server (TMS) for the SMS if it implements the required functionality. Wherever a test procedure refers to an SMS, the equivalent TMS may also be used. A complete Server Test Sequence report containing no failures is a prerequisite to execution of this sequence.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject and the original CTP compliance test conducted per Chapter 20. OMB Consolidated Test Sequence. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 22.2. OMB Confidence Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 5.1.1. SPB Digital Certificate | | | — | — |
| 2 | 5.4.1.13. KDMKeysReceived Event (OBAE) | | | — | — |
| 3 | 5.4.2.10. SPBSoftware Event | | | — | — |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 6.1.18. Content Key Extension, End of Engagement (OBAE) | | | — | — |
| 5 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 6 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 7 | 6.1.22. Restriction of Keying to Valid CPLs (OBAE) | | | — | — |
| 8 | 6.1.23. ContentAuthenticator Element Check (OBAE) | | | — | — |
| 9 | 6.3.5. Clock Adjustment (OMB) | | | — | — |
| 10 | 6.4.8. FM Payload (OBAE) | | | — | — |
| 11 | 8.2.11. SMS Identity and Certificate | | | — | — |
| 12 | 8.2.13. Content Keys and TDL check (OBAE) | | | — | — |
| 13 | 8.2.15. Validity of SMS Certificates | | | — | — |

# Chapter 23. Digital Cinema Projector with IMBO Consolidated Confidence Sequence

## 23.1. Overview

The test sequence defined in this chapter is intended to be used to test for confidence a d-cinema projector with an integrated Image Media Block with OMB functions (IMBO) as the Test Subject. The configuration and architecture of the system may vary, but the test sequence requires that the system consists of at least a light processing system including electronic and optical components (Projector), an IMBO (containing a Security Manager, Media Decryptors, image, main sound and OBAE sound processing, etc.), and a Screen Management Server/System (SMS). For the purpose of this test, the Test Operator may substitute a Theater Management Server (TMS) for the SMS if it implements the required functionality. Wherever a test procedure refers to an SMS, the equivalent TMS may also be used. A complete Server Test Sequence report containing no failures is a prerequisite to execution of this sequence.

Before performing the test sequence provided below, the Test Operator should read and understand the documentation provided with the Test Subject and the original CTP compliance test conducted per Chapter 21. Digital Cinema Projector with IMBO Consolidated Test Sequence. If adequate documentation is not available, a Test Subject Representative should be available to provide assistance during the test session.

## 23.2. Digital Cinema Projector with IMBO Confidence Sequence

For each row of the table below, perform the procedure specified in the Procedure column, subject to all conditions specified in the Condition column. Indicate the status of the test in the Pass or Fail column, unless the test is specified as *data only*. Any marks in greyed-out fields indicate a test failure. Report any information listed in the Measured Data column. The Test Operator may record any additional observations.

| Step | Procedure | Pass | Fail | Conditions | Measured data |
|---|---|---|---|---|---|
| 1 | 5.4.1.6. KDMKeysReceived Event | | | — | — |
| 2 | 5.4.2.10. SPBSoftware Event | | | — | — |
| 3 | 6.1.5. Restriction of Keying to Valid CPLs | | | — | — |
| 4 | 6.1.8. Content Key Extension, End of Engagement | | | — | — |
| 5 | 6.1.9. ContentAuthenticator Element Check | | | — | — |
| 6 | 6.1.11. KDM TDL Check | | | — | — |
| 7 | 6.1.18. Content Key Extension, End of Engagement (OBAE) | | | — | — |
| 8 | 6.1.20. Validity of Media Block Certificates | | | — | — |
| 9 | 6.3.1. Clock Adjustment | | | — | — |
| 10 | 6.4.3. FM Payload | | | — | — |
| 11 | 7.2.2. Projector and Direct View Display Security Servicing | | | — | — |
| 12 | 7.3.2. Companion SPBs with Electronic Marriage | | | — | — |
| 13 | 7.5.3. Projector Pixel Count/Structure | | | — | — |
| 14 | 8.2.7. Artifact Free Transition of Image Format | | | — | — |
| 15 | 8.2.11. SMS Identity and Certificate | | | — | — |
| 16 | 8.2.12. Content Keys and TDL check | | | — | — |
| 17 | 8.2.13. Content Keys and TDL check (OBAE) | | | — | — |
| 18 | 8.2.15. Validity of SMS Certificates | | | — | — |

# Appendix A. Test Materials

## A.1. Overview

To facilitate consistent testing of d-cinema equipment, a set of reference files has been produced to be used as directed in the respective test procedures. These materials are described in detail in this Appendix with the intention that the materials can be re-created from the descriptions and used to achieve testing results equivalent to those achieved with the original reference files.

The test material described below consists of digital certificates, Key Delivery Messages (KDM) and D-Cinema Packages (DCP). A DCP can be further deconstructed as a set of Track Files, Composition Playlists and related file descriptions. Some Track Files will be encrypted.

Because the identity of a Test Subject cannot be known until the device has been manufactured, it is not possible to create reference KDM files in advance. It is therefore necessary to divide the test material into two categories: common-use reference material and per-device reference material. Common-use reference material can be created once and used without limit on any compliant system. Per-device reference material must be created for each Test Subject, with foreknowledge of the date and time of the test session.

Two additional categories of reference material exist: compliant and intentionally non-compliant. Most of the material will be "golden" reference files, intended to be entirely compliant with the relevant specifications. Other files, however, will be intentionally broken to allow testing of error detection and recovery mechanisms.

## A.2. Images

### A.2.1. Introduction

This section defines a set of MXF picture track files. For each track file, a description is given which details the images encoded in the file. The image track files will be combined with sound files to make complete compositions (see Section A.4).

### A.2.2. Sync Count

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sync_count_j2c_pt.mxf |
| **Description** | MXF track file containing five seconds (120 frames) of plain frames followed by a ten second countdown and five seconds of plain frames. The countdown consists of ten identical one-second count segments, from 9-0. Each count segment consists of twenty- four frames of the respective digit for the count period. The first frame of each count segment will have a punch set to indicate sync. The example image below shows the first |

| | | |
|---|---|---|
| | frame of the fourth count period, which contains the number 6 (six). | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

**Figure A.1. Sync Count**

## A.2.3. Sync Count (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sync_count_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file, contents are identical to Section A.2.2: Sync Count. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.4. 4K Sync Count

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 4K_sync_count_j2c_pt.mxf | |
| **Description** | 4K Resolution MXF track file, contents are identical to Section A.2.2: Sync Count. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.5. Sync Count, 48fps

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sync_count_48fps_j2c_pt.mxf | |
| **Description** | 48fps MXF track file containing five seconds (240 frames) of plain frames followed by a ten second countdown and five seconds of plain frames. The countdown consists of ten identical one- second count segments, from 9-0. Each count segment consists of forty- eight frames of the respective digit for the count period. The first two frames of each count segment will have a punch set to indicate sync. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:20:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.6. Channel I.D. 5.1

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | channel_id_51_j2c_pt.mxf |
| **Description** | MXF track file containing five seconds (120 frames) of plain frames followed by a thirty second audio channel identification set and five seconds of plain frames. The audio channel identification set consists of six identical five second identifier segments having the following consecutively displayed labels: Left, Center, Right, Left Surround, Right Surround, LFE. Each channel identifier segment consists of five seconds (120 |

| | | |
|---|---|---|
| | frames) of the respective label. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

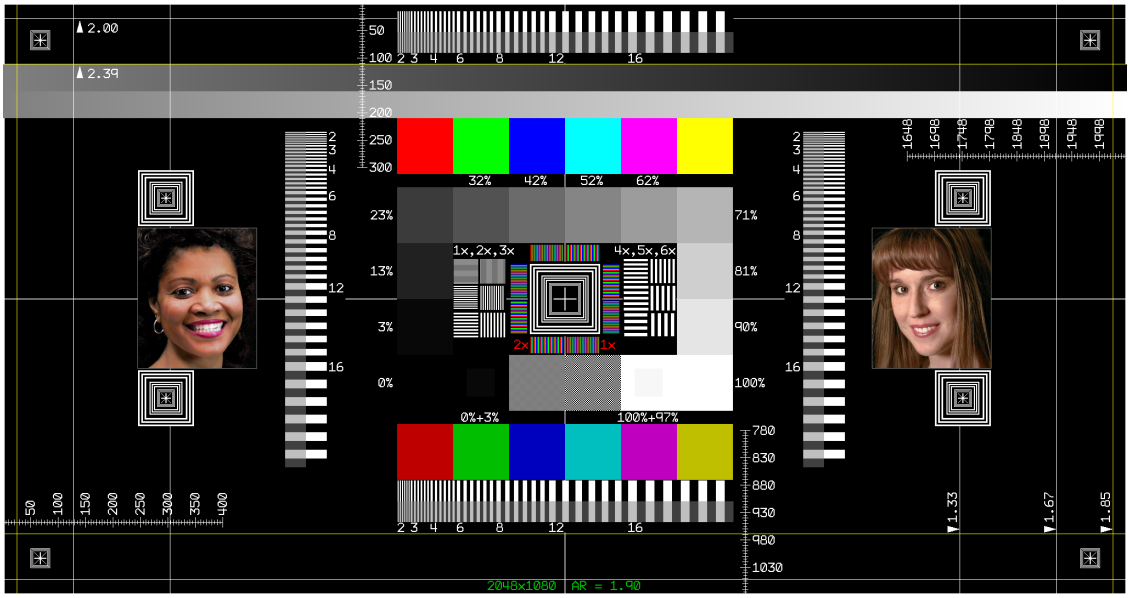
## A.2.7. Channel I.D. 1-16

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | channel_id_01-16_j2c_pt.mxf | |
| **Description** | MXF track file containing two seconds (48 frames) of plain frames followed by an eighty second audio channel identification set and two seconds of plain frames. The audio channel identification set consists of sixteen identical five-second identifier segments displaying consecutively numbered channel labels: 1, 2, 3, 4, etc. through 16. Each channel identifier segment consists of five seconds (120 frames) of the respective label. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:01:24:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.8. "NIST" 2K Test Pattern

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | nist_2k_test_pattern_j2c_pt.mxf | |
| **Description** | MXF track file containing the "DCI NIST" pattern created during original DCI research project. The pattern (shown below) includes geometric dimensions, color chips, dimensional patterns, a grayscale gradient and full-color photographic images. The track file contains 30 seconds (720 frames) of this image. *Note: This image was obtained during the initial DCI study effort. It is used in the CTP because it is familiar to many in the d- cinema industry. The edge offset reticles are not accurate, however they are not used by any CTP procedure*. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

### Figure A.2. "NIST" 2K Test Pattern




## A.2.9. "NIST" 4K Test Pattern

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 4K_nist_test_pattern_j2c_pt.mxf | |
| **Description** | 4K Resolution MXF track file containing the "DCI NIST" pattern as shown in Section A.2.8: "NIST" 2K Test Pattern. The track file contains 30 seconds (720 frames) of this image. *Note: This image was obtained during the initial DCI study effort. It is used in the CTP because it is familiar to many in the d-cinema industry. The edge offset reticles are not accurate, however they are not used by any CTP procedure*. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.10. Black to Gray Step Series

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | gray_step_j2c_pt.mxf |

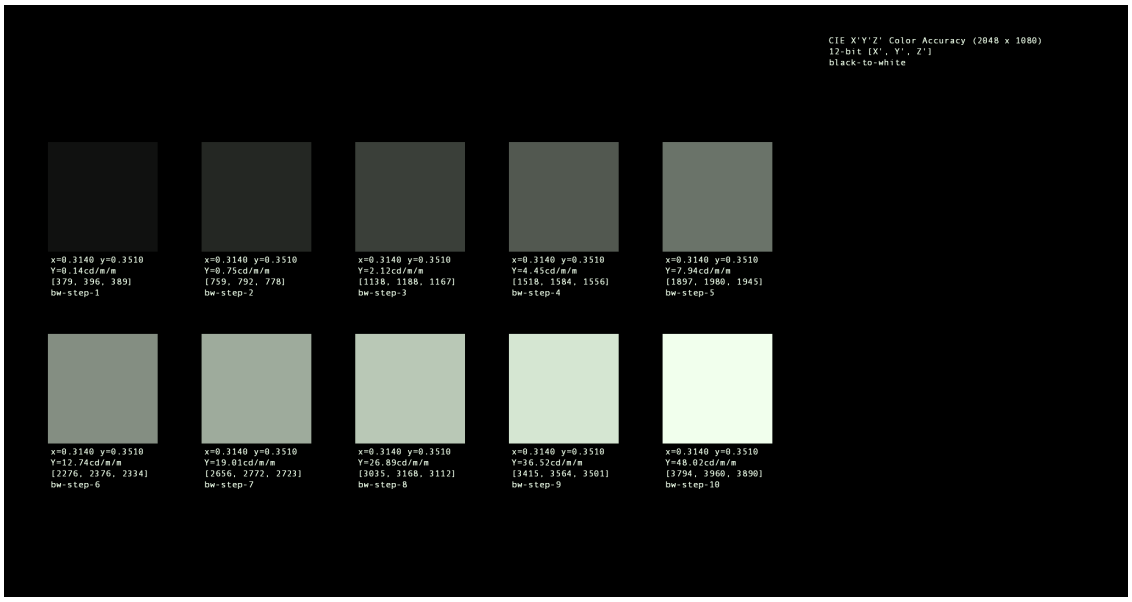
| | | |
|---|---|---|
| **Description** | MXF track file containing five seconds (120 frames) of a chart showing all gray step values for the Black to Gray values in Section 7.5.9: Grayscale Tracking. This is followed by 1 minute of each of the 10 values as a full frame. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:11:05:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

### Figure A.3. Black to Gray Step Series

## A.2.11. Black to White Step Series

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | white_step_j2c_pt.mxf | |
| **Description** | MXF track file containing five seconds (120 frames) of a chart showing all gray step values for the Black to White values in Section 7.5.9: Grayscale Tracking. This is followed by 1 minute of each of the 10 values as a full frame. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:11:05:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

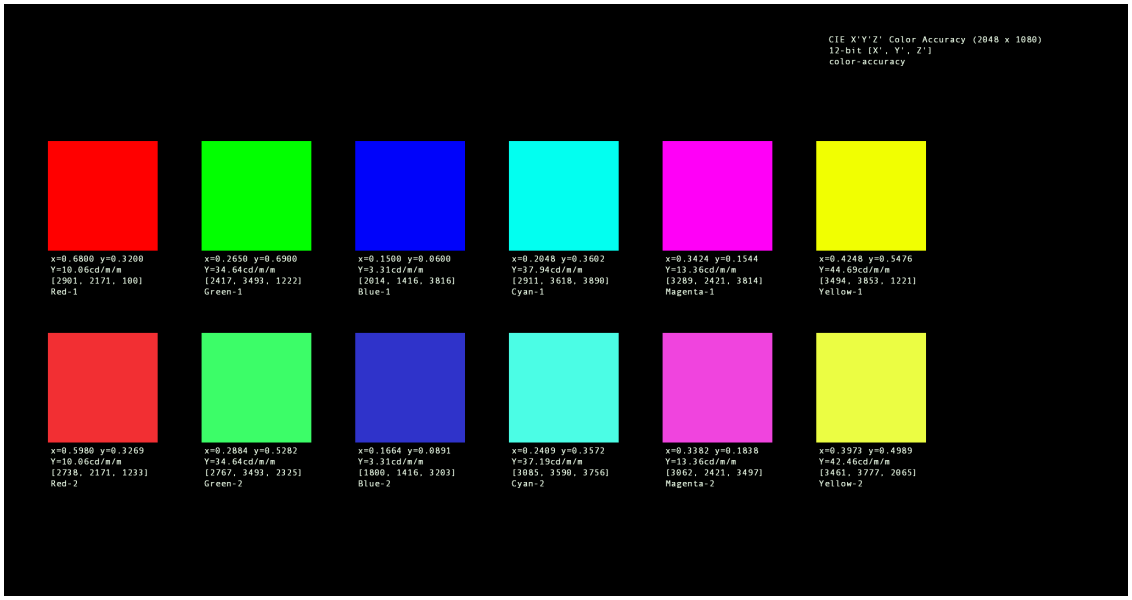
### Figure A.4. Black to White Step Series




## A.2.12. Color Accuracy Series

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | color_accuracy_j2c_pt.mxf | |
| **Description** | MXF track file containing five seconds (120 frames) of a chart showing all color values for the test in Section 7.5.12: Color Accuracy. This is followed by 1 minute of each of the 12 color values as a full frame. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:12:05:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

### Figure A.5. Color Accuracy Series




## A.2.13. 4K Color Accuracy Series

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 4K_color_accuracy_j2c_pt.mxf | |
| **Description** | MXF track file containing the 4K version of the Color Accuracy Series shown in Section A.2.12: Color Accuracy Series. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 12:05:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.14. Black (Empty Frame)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | black_j2c_pt.mxf | |
| **Description** | MXF track file containing 30 seconds (720 frames) of black (all pixels zero). | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:00:30:00 |

| | | |
|---|---|---|
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

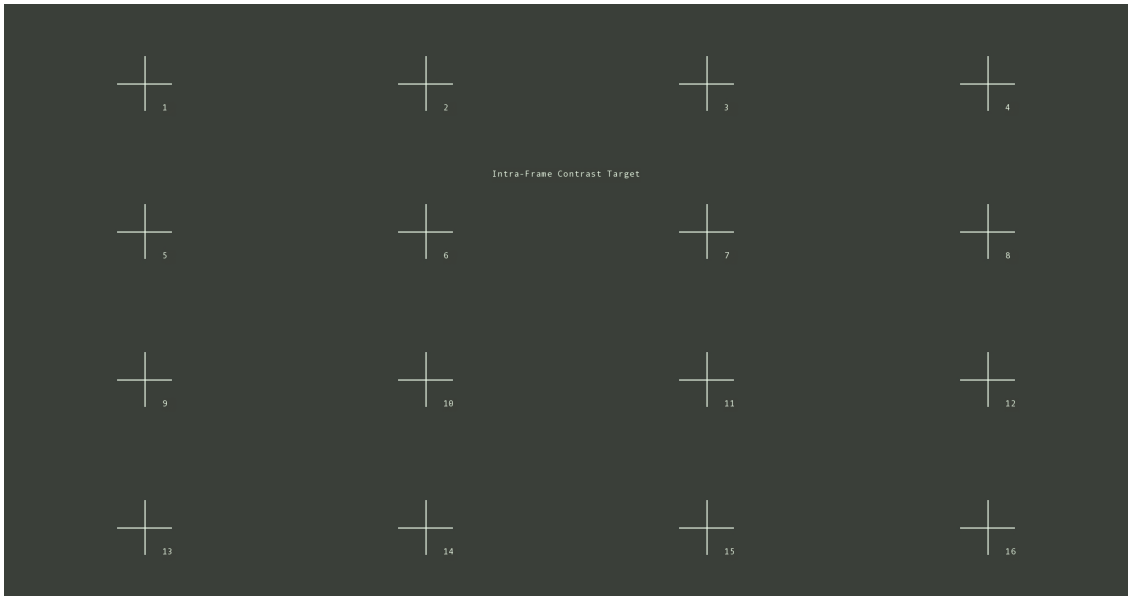
## A.2.15. White (White Frame)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | white_j2c_pt.mxf | |
| **Description** | MXF track file containing 30 seconds (720 frames) of white. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.16. Intra-Frame Contrast Sequence

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 2K_checkerboard_j2c_pt.mxf | |
| **Description** | MXF track file containing alternating checkerboard patterns and an aiming target. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

### Figure A.6. Intra-Frame Contrast Sequence




## A.2.17. Sequential Contrast Sequence

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 2K_sequential_contrast_j2c_pt.mxf | |
| **Description** | MXF track file containing black, white and aiming target frames. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.18. 2K Picture Track File, Maximum Bitrate

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 2K_max_bitrate_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file containing a count to check synchronization between picture and sound, 10 minutes (14,400 frames) of a frame that has a large file size (1,281,818 bytes) and a second sync count. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 00:10:40:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

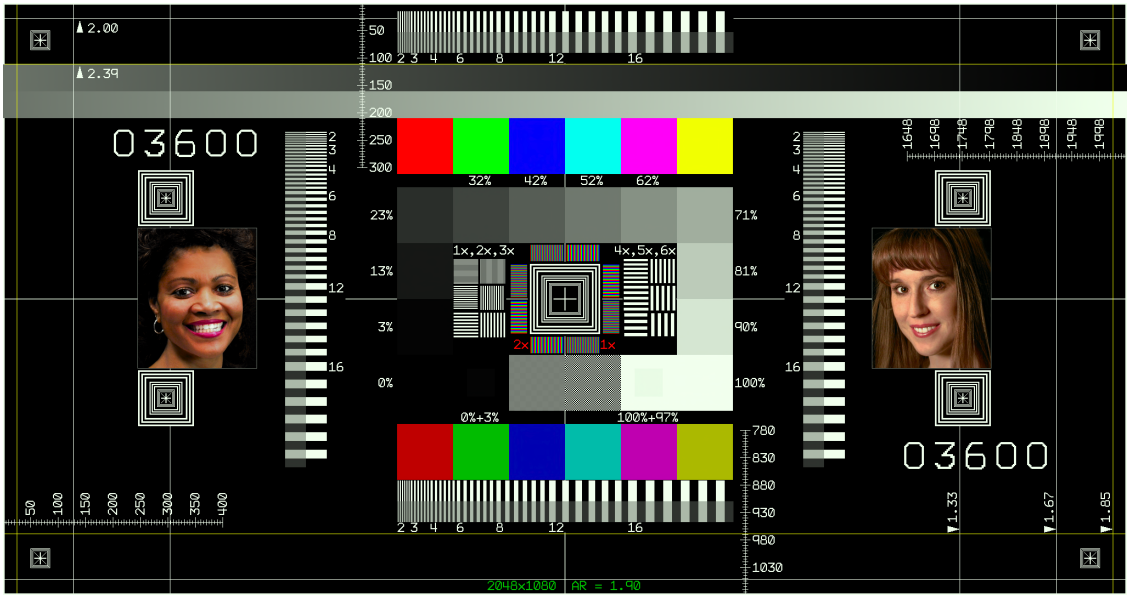
## A.2.19. 4K Picture Track File, Maximum Bitrate

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 4K_max_bitrate_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file containing a count to check synchronization between picture and sound, 10 minutes (14,400 frames) of a frame that has a large file size (1,299,183 bytes) and a second sync count. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:10:40:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.20. DCI Numbered Frame Sequence

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | frame_num_burn_in_j2c_pt.mxf | |
| **Description** | MXF track file containing a sequence of the "DCI NIST" frame that has an overlay of two identical visible number fields. The five digit field contains 00000 in the first frame of the file, with each consecutive frame increasing the count by 1. The last frame will be numbered 07199. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:05:00:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

### Figure A.7. DCI Numbered Frame Sequence




## A.2.21. DCI Numbered Frame Sequence (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | frame_num_burn_in_j2c_ct.mxf | |
| **Description** | MXF track file containing a sequence of the "DCI NIST" frame that has an overlay of two identical visible number fields. The five digit field contains 00000 in the first frame of the file, with each consecutive frame increasing the count by 1. The last frame will be numbered 07199. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:05:00:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.22. DCI Scope Transition Sequence

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | transition-scope_j2c_pt.mxf |
| **Description** | MXF track file containing a sequence of Scope format (A.R. 2.39:1) plain frames, and the label "Scope Transition Test Sequence (2048 x 858)". Each of the first 24 frames of the sequence have two identical overlays displaying a number from 001 through 024. Each of the last 24 frames of the sequence have two |

| | | |
|---|---|---|
| | identical overlays displaying a number from 024 through 001. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:10:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.23. DCI Flat Transition Sequence

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | transition-flat_j2c_pt.mxf | |
| **Description** | MXF track file containing a sequence of Flat format (A.R. 1.85:1) plain frames, and the label "Flat Transition Test Sequence (1998 x 1024)". Each of the first 24 frames of the sequence have two identical overlays displaying a number from 001 through 024. Each of the last 24 frames of the sequence have two identical overlays displaying a number from 024 through 001. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:10:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.24. StEM 2K

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | StEM_2K_j2c_pt.mxf | |
| **Description** | MXF track file containing the complete DCI StEM Mini Movie. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 11:31:21 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.25. StEM 2K (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | StEM_2K_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file containing the complete DCI StEM Mini Movie. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 11:31:21 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.26. StEM 2K Multi-Reel A (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c multi | |
| **Filename** | StEM_2K_j2c_multi_A_ct_.mxf | |
| **Description** | A set of encrypted MXF track files containing 2k image essence for the DCI StEM Mini Movie. 128 files, each with a duration of 5 seconds. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **SegmentCount** | 128 |
| | **Encryption** | AES-128 |
| | **SegmentDuration** | 00:05:00 |
| | **Duration** | 00:10:40:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.27. StEM 2K Multi-Reel B (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c multi |

| | | |
|---|---|---|
| **Filename** | StEM_2K_j2c_multi_B_ct_.mxf | |
| **Description** | A set of encrypted MXF track files containing 2k image essence for the DCI StEM Mini Movie. Identical to StEM_2K_j2c_multi_A_ct | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **SegmentCount** | 128 |
| | **Encryption** | AES-128 |
| | **SegmentDuration** | 00:05:00 |
| | **Duration** | 00:10:40:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.28. StEM 2K Multi-Reel A

| | | |
|---|---|---|
| **Type** | MXF j2c multi | |
| **Filename** | StEM_2K_j2c_multi_A_pt_.mxf | |
| **Description** | A set of plaintext MXF track files containing 2k image essence for the DCI StEM Mini Movie. 128 files, each with a duration of 5 seconds. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **SegmentCount** | 128 |
| | **SegmentDuration** | 00:05:00 |
| | **Duration** | 00:10:40:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.29. StEM 2K Multi-Reel B

| | |
|---|---|
| **Type** | MXF j2c multi |
| **Filename** | StEM_2K_j2c_multi_B_pt_.mxf |
| **Description** | A set of plaintext MXF track files containing 2k image essence for the DCI StEM Mini Movie. Identical to StEM_2K_j2c_multi_A_pt |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 |

| | | |
|---|---|---|
| **Meta** | **SegmentCount** | 128 |
| | **SegmentDuration** | 00:05:00 |
| | **Duration** | 00:10:40:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.30. StEM 2K 48 fps

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | StEM_2K_48fps_j2c_pt.mxf | |
| **Description** | MXF track file containing a 48 fps DCI StEM Mini Movie clip. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:51:46 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.31. pixel_structure_N_2k_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | pixel_structure_N_2k_j2c_pt.mxf | |
| **Description** | See Section 7.5.3: Projector Pixel Count/Structure for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.32. pixel_structure_S_2k_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | pixel_structure_S_2k_j2c_pt.mxf | |
| **Description** | See Section 7.5.3: Projector Pixel Count/Structure for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.33. pixel_structure_E_2k_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | pixel_structure_E_2k_j2c_pt.mxf | |
| **Description** | See Section 7.5.3: Projector Pixel Count/Structure for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.34. pixel_structure_W_2k_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | pixel_structure_W_2k_j2c_pt.mxf | |
| **Description** | See Section 7.5.3: Projector Pixel Count/Structure for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.35. pixel_structure_N_4k_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | pixel_structure_N_4k_j2c_pt.mxf | |
| **Description** | See Section 7.5.3: Projector Pixel Count/Structure for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.36. pixel_structure_S_4k_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | pixel_structure_S_4k_j2c_pt.mxf | |
| **Description** | See Section 7.5.3: Projector Pixel Count/Structure for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.37. pixel_structure_E_4k_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | pixel_structure_E_4k_j2c_pt.mxf | |
| **Description** | See Section 7.5.3: Projector Pixel Count/Structure for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 4096x2160 |

| | | |
|---|---|---|
| | **EditRate** | 24/1 |

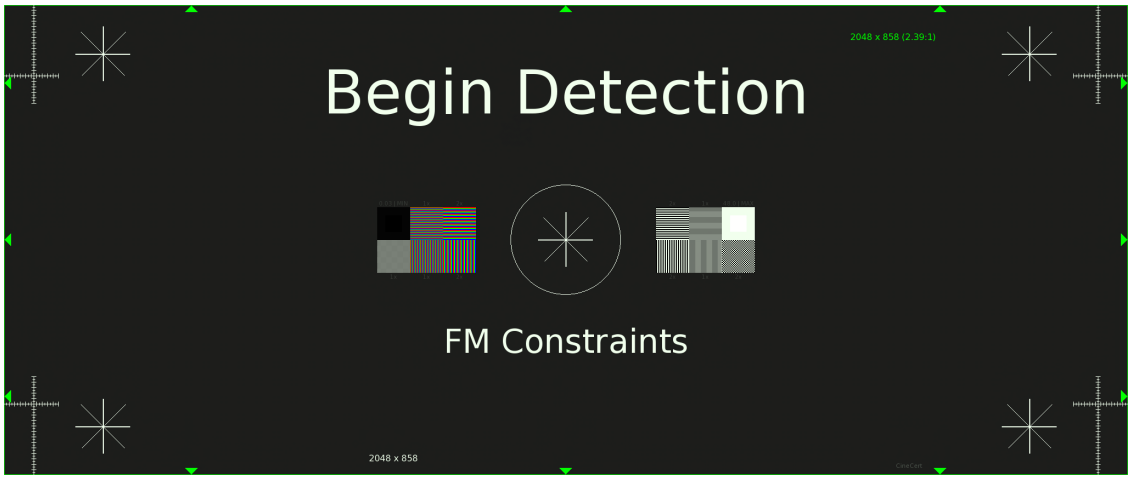
## A.2.38. pixel_structure_W_4k_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | pixel_structure_W_4k_j2c_pt.mxf | |
| **Description** | See Section 7.5.3: Projector Pixel Count/Structure for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.39. FM Constraints Begin (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | fm_constraints_begin_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file with 10 seconds of slate reading "Begin Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

### Figure A.8. FM Constraints Begin (Encrypted)




## A.2.40. FM Constraints Begin (Plaintext)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | fm_constraints_begin_j2c_pt.mxf | |
| **Description** | Plaintext MXF track file with 10 seconds of slate reading "Begin Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.41. FM Constraints End (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | fm_constraints_end_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file with 10 seconds of slate reading "End Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.42. FM Constraints End (Plaintext)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | fm_constraints_end_j2c_pt.mxf | |
| **Description** | Plaintext MXF track file with 10 seconds of slate reading "End Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.43. 2K FM Control Granularity Begin (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 2K_fm_control_granularity_begin_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file with 10 seconds of slate reading "Begin Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.44. Deleted Section

The section "2K FM Control Granularity Begin" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.2.45. 2K FM Control Granularity End (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 2K_fm_control_granularity_end_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file with 10 seconds of slate reading "End Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.46. Deleted Section

The section "2K FM Control Granularity End" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.2.47. 2K FM Payload Begin (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | 2K_fm_payload_begin_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file with 10 seconds of slate reading "Begin Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.48. 2K FM Payload End (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | 2K_fm_payload_end_j2c_ct.mxf |
| | |

| | | |
|---|---|---|
| **Description** | Encrypted MXF track file with 10 seconds of slate reading "End Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.49. Binary Audio FM Bypass

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | binary_audio_fm_bypass_j2c_pt.mxf | |
| **Description** | Plaintext MXF track file with 10 minutes of slate reading "Binary Audio FM Bypass". | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:10:00:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.50. Selective FM Begin

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | selective_fm_begin_j2c_pt.mxf | |
| **Description** | Plaintext MXF track file with 10 seconds of slate reading "Begin Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.51. Selective FM End

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | selective_fm_end_j2c_pt.mxf | |
| **Description** | Plaintext MXF track file with 10 seconds of slate reading "End Detection" and 5 seconds of black. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.52. Timed Text Example with Missing Font

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | std_ctp_text_no_font_pt.mxf | |
| **Description** | MXF track file containing timed text using an OpenType font. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-5 | |
| **Malformations** | The font shall not be present in the track file. | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **EditRate** | 24/1 |

## A.2.53. DCI_gradient_step_s_white_j2c_pt

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | DCI_gradient_step_s_white_j2c_pt.mxf | |
| **Description** | See Section 6.5.2: Decoder Requirements for description. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-431-2 | |
| **Meta** | **Duration** | 00:00:16:16 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

### Figure A.9. DCI_gradient_step_s_white_j2c_pt

## A.2.54. Deleted Section

The section "DCI_gradient_step_s_color_j2c_pt" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.2.55. Deleted Section

The section "Timed Text Example with Font" was deleted. The section number is maintained here to preserve the numbering of subsequent sections

## A.2.56. Deleted Section

The section "Timed Text Example with PNG" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.2.57. Sync Count Text

| | |
|---|---|
| **Type** | MXF text |
| **Filename** | sync_count_tt_pt.mxf |

| | | |
|---|---|---|
| **Description** | MXF track file containing timed text using a font and images. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-5, SMPTE-428-7 | |
| **Meta** | **Duration** | 00:00:22:00 |
| | **EditRate** | 24/1 |

## A.2.58. Sync Count Text (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sync_count_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text using a font and images. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-5 | |
| **Meta** | **Duration** | 00:00:22:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.59. subtitle background

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | subtitle_background_j2c_pt.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-4, SMPTE-422 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.60. Deleted Section

The section "Plain_Frame_nosub_j2c_ct" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.2.61. m01 Picture Frame Out Of Order (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | m01_pict_frame_oo_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file containing the first 5 seconds (120 frames) of the NIST test pattern. The order of the first two frames has been deliberately swapped. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Malformations** | The first two image frames of the track file have been swapped. | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:05:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.62. m03 Sound Splice

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | m03_snd_splc_j2c_pt.mxf | |
| **Description** | MXF track file containing one minute (1440 frames) of plain frames with the label "m03 Sound Splice Test". | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.63. m05 Picture Track File With Wrong TrackFile ID (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | m05_pict_wrong_file_j2c_ct.mxf |
| **Description** | MXF track file in which the integrity pack of the 7th frame has the TrackFile ID replaced with a different |

| | |
|---|---|
| | value. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 |
| **Meta** | **Encryption** AES-128<br>**Duration** 00:00:05:00<br>**PixelArraySize** 2048x1080<br>**EditRate** 24/1<br>**CiphertextHeader** yes |

## A.2.64. m09 Picture track file with bad HMAC (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | m09_pict_bad_hmac_j2c_ct.mxf |
| **Description** | Picture track file in which one of the HMAC values for a single frame has been changed. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 |
| **Malformations** | The file contains a replacement EKLV packet for the seventh frame (index 6). The replacement packet is taken from another track file having a different PackageUID but encrypted with the same symmetric key. |
| **Meta** | **Encryption** AES-128<br>**Duration** 00:00:05:00<br>**PixelArraySize** 2048x1080<br>**EditRate** 24/1 |

## A.2.65. m11 Picture With Bad Check Value (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | m11_pict_bad_chuk_j2c_ct.mxf |
| **Description** | MXF track file containing one EKLV packet with an invalid Check Value. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 |
| **Meta** | **Encryption** AES-128<br>**Duration** 00:00:05:00<br>**PixelArraySize** 2048x1080 |

| | | |
|---|---|---|
| | **EditRate** | 24/1 |

## A.2.66. 2K Scope Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.67. 2K Scope Subtitle Test Background - Reel 2

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_01_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.68. 2K Scope Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.69. 2K Scope Subtitle Test Background - Reel 4

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_03_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.70. 2K Scope Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.71. 2K Scope Subtitle Test Background - Reel 6

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sub_test_2K_scope_05_j2c_ct.mxf |
| | |

| | | |
|---|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.72. 2K Scope Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.73. 2K Scope Subtitle Test Background - Reel 8

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_07_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.74. 2K Scope Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.75. 2K Scope Subtitle Test Background - Reel 10

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_scope_09_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 24/1 |

## A.2.76. 4K Scope Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.77. 4K Scope Subtitle Test Background - Reel 2

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_01_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.78. 4K Scope Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.79. 4K Scope Subtitle Test Background - Reel 4

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_03_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArravSize** | 4096x1716 |

| | | |
|---|---|---|
| | **EditRate** | 24/1 |

## A.2.80. 4K Scope Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.81. 4K Scope Subtitle Test Background - Reel 6

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_05_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.82. 4K Scope Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.83. 4K Scope Subtitle Test Background - Reel 8

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_07_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.84. 4K Scope Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_scope_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.85. 4K Scope Subtitle Test Background - Reel 10

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sub_test_4K_scope_09_j2c_ct.mxf |
| | |

| | | |
|---|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 4096x1716 |
| | **EditRate** | 24/1 |

## A.2.86. 2K 48fps Scope Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.87. 2K 48fps Scope Subtitle Test Background - Reel 2

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_01_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.88. 2K 48fps Scope Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.89. 2K 48fps Scope Subtitle Test Background - Reel 4

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_03_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.90. 2K 48fps Scope Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.91. 2K 48fps Scope Subtitle Test Background - Reel 6

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_05_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.92. 2K 48fps Scope Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.93. 2K 48fps Scope Subtitle Test Background - Reel 8

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_07_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArravSize** | 2048x858 |

| | | |
|---|---|---|
| | **EditRate** | 48/1 |

## A.2.94. 2K 48fps Scope Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.95. 2K 48fps Scope Subtitle Test Background - Reel 10

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_scope_09_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.96. 2K Flat Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.97. 2K Flat Subtitle Test Background - Reel 2

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_01_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.98. 2K Flat Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.99. 2K Flat Subtitle Test Background - Reel 4

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sub_test_2K_flat_03_j2c_ct.mxf |
| | |

| | | |
|---|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.100. 2K Flat Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.101. 2K Flat Subtitle Test Background - Reel 6

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_05_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.102. 2K Flat Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.103. 2K Flat Subtitle Test Background - Reel 8

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_07_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.104. 2K Flat Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.105. 2K Flat Subtitle Test Background - Reel 10

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_flat_09_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 24/1 |

## A.2.106. 4K Flat Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.107. 4K Flat Subtitle Test Background - Reel 2

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_01_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArravSize** | 3996x2160 |

| | | |
|---|---|---|
| | **EditRate** | 24/1 |

## A.2.108. 4K Flat Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.109. 4K Flat Subtitle Test Background - Reel 4

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_03_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.110. 4K Flat Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.111. 4K Flat Subtitle Test Background - Reel 6

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_05_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.112. 4K Flat Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.113. 4K Flat Subtitle Test Background - Reel 8

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sub_test_4K_flat_07_j2c_ct.mxf |
| | |

| | | |
|---|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.114. 4K Flat Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.115. 4K Flat Subtitle Test Background - Reel 10

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_flat_09_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 3996x2160 |
| | **EditRate** | 24/1 |

## A.2.116. 2K 48fps Flat Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 48/1 |

## A.2.117. 2K 48fps Flat Subtitle Test Background - Reel 2

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_01_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 48/1 |

## A.2.118. 2K 48fps Flat Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 48/1 |

## A.2.119. 2K 48fps Flat Subtitle Test Background - Reel 4

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_03_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 48/1 |

## A.2.120. 2K 48fps Flat Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 48/1 |

## A.2.121. 2K 48fps Flat Subtitle Test Background - Reel 6

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_05_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArravSize** | 1998x1080 |

| | | |
|---|---|---|
| | **EditRate** | 48/1 |

## A.2.122. 2K 48fps Flat Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 48/1 |

## A.2.123. 2K 48fps Flat Subtitle Test Background - Reel 8

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_07_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 1998x1080 |
| | **EditRate** | 48/1 |

## A.2.124. 2K 48fps Flat Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.125. 2K 48fps Flat Subtitle Test Background - Reel 10

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_flat_09_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 2048x858 |
| | **EditRate** | 48/1 |

## A.2.126. 2K Full Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.127. 2K Full Subtitle Test Background - Reel 2

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sub_test_2K_full_01_j2c_ct.mxf |
| | |

| | | |
|---|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.128. 2K Full Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.129. 2K Full Subtitle Test Background - Reel 4

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_03_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.130. 2K Full Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.131. 2K Full Subtitle Test Background - Reel 6

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_05_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.132. 2K Full Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.133. 2K Full Subtitle Test Background - Reel 8

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_07_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.134. 2K Full Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.135. 2K Full Subtitle Test Background - Reel 10

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_2K_full_09_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArravSize** | 2048x1080 |

| | | |
|---|---|---|
| | **EditRate** | 24/1 |

## A.2.136. 4K Full Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.137. 4K Full Subtitle Test Background - Reel 2

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_01_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.138. 4K Full Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.139. 4K Full Subtitle Test Background - Reel 4

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_03_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.140. 4K Full Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.141. 4K Full Subtitle Test Background - Reel 6

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sub_test_4K_full_05_j2c_ct.mxf |
| | |

| | | |
|---|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.142. 4K Full Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.143. 4K Full Subtitle Test Background - Reel 8

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_07_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.144. 4K Full Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.145. 4K Full Subtitle Test Background - Reel 10

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_4K_full_09_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 4096x2160 |
| | **EditRate** | 24/1 |

## A.2.146. 2K 48fps Full Subtitle Test Background - Reel 1

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_00_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:14:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.147. 2K 48fps Full Subtitle Test Background - Reel 2

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_01_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:40:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.148. 2K 48fps Full Subtitle Test Background - Reel 3

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_02_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:52:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.149. 2K 48fps Full Subtitle Test Background - Reel 4

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_03_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArravSize** | 2048x1080 |

| | | |
|---|---|---|
| | **EditRate** | 48/1 |

## A.2.150. 2K 48fps Full Subtitle Test Background - Reel 5

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_04_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.151. 2K 48fps Full Subtitle Test Background - Reel 6

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_05_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:15:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.152. 2K 48fps Full Subtitle Test Background - Reel 7

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_06_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 00:01:31:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.153. 2K 48fps Full Subtitle Test Background - Reel 8

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_07_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:10:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.154. 2K 48fps Full Subtitle Test Background - Reel 9

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sub_test_48fps_full_08_j2c_ct.mxf | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:01:45:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.155. 2K 48fps Full Subtitle Test Background - Reel 10

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sub_test_48fps_full_09_j2c_ct.mxf |
| | |

| | | |
|---|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-2, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:30:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 48/1 |

## A.2.156. 2K Scope Subtitle Test - Timed Text track file - Reel 1

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_00_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.157. 2K Scope Subtitle Test - Timed Text track file - Reel 2

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_01_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.158. 2K Scope Subtitle Test - Timed Text track file - Reel 3

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_02_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.159. 2K Scope Subtitle Test - Timed Text track file - Reel 4

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_03_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.160. 2K Scope Subtitle Test - Timed Text track file - Reel 5

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_04_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.161. 2K Scope Subtitle Test - Timed Text track file - Reel 6

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_05_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.162. 2K Scope Subtitle Test - Timed Text track file - Reel 7

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_06_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.163. 2K Scope Subtitle Test - Timed Text track file - Reel 8

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_07_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **EditRate** | 24/1 |

## A.2.164. 2K Scope Subtitle Test - Timed Text track file - Reel 9

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_08_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.165. 2K Scope Subtitle Test - Timed Text track file - Reel 10

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_scope_09_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.166. 4K Scope Subtitle Test - Timed Text track file - Reel 8

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_4K_scope_07_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |

| | | |
|---|---|---|
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.167. 4K Scope Subtitle Test - Timed Text track file - Reel 9

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_4K_scope_08_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.168. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 1

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_00_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.169. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 2

| | |
|---|---|
| **Type** | MXF text |
| **Filename** | sub_test_48fps_scope_01_tt_ct.mxf |

| | | |
|---|---|---|
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.170. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 3

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_02_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.171. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 4

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_03_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.172. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 5

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_04_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.173. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 6

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_05_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.174. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 7

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_06_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.175. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 8

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_07_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.176. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 9

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_08_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.177. 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 10

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_scope_09_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **EditRate** | 48/1 |

## A.2.178. 2K Flat Subtitle Test - Timed Text track file - Reel 1

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_00_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.179. 2K Flat Subtitle Test - Timed Text track file - Reel 2

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_01_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.180. 2K Flat Subtitle Test - Timed Text track file - Reel 3

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_02_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |

| | | |
|---|---|---|
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.181. 2K Flat Subtitle Test - Timed Text track file - Reel 4

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_03_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.182. 2K Flat Subtitle Test - Timed Text track file - Reel 5

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_04_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.183. 2K Flat Subtitle Test - Timed Text track file - Reel 6

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_05_tt_ct.mxf | |

| | | |
|---|---|---|
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.184. 2K Flat Subtitle Test - Timed Text track file - Reel 7

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_06_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.185. 2K Flat Subtitle Test - Timed Text track file - Reel 8

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_07_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.186. 2K Flat Subtitle Test - Timed Text track file - Reel 9

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_08_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.187. 2K Flat Subtitle Test - Timed Text track file - Reel 10

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_flat_09_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.188. 4K Flat Subtitle Test - Timed Text track file - Reel 8

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_4K_flat_07_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.189. 4K Flat Subtitle Test - Timed Text track file - Reel 9

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_4K_flat_08_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.190. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 1

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_00_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.191. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 2

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_01_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **EditRate** | 48/1 |

## A.2.192. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 3

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_02_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.193. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 4

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_03_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.194. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 5

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_04_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |

| | | |
|---|---|---|
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.195. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 6

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_05_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.196. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 7

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_06_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.197. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 8

| | |
|---|---|
| **Type** | MXF text |
| **Filename** | sub_test_48fps_flat_07_tt_ct.mxf |

| | | |
|---|---|---|
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.198. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 9

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_08_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.199. 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 10

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_flat_09_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.200. 2K Full Subtitle Test - Timed Text track file - Reel 1

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_00_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.201. 2K Full Subtitle Test - Timed Text track file - Reel 2

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_01_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.202. 2K Full Subtitle Test - Timed Text track file - Reel 3

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_02_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.203. 2K Full Subtitle Test - Timed Text track file - Reel 4

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_03_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.204. 2K Full Subtitle Test - Timed Text track file - Reel 5

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_04_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.205. 2K Full Subtitle Test - Timed Text track file - Reel 6

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_05_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **EditRate** | 24/1 |

## A.2.206. 2K Full Subtitle Test - Timed Text track file - Reel 7

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_06_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.207. 2K Full Subtitle Test - Timed Text track file - Reel 8

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_07_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.208. 2K Full Subtitle Test - Timed Text track file - Reel 9

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_08_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |

| | | |
|---|---|---|
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.209. 2K Full Subtitle Test - Timed Text track file - Reel 10

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_2K_full_09_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.210. 4K Full Subtitle Test - Timed Text track file - Reel 8

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_4K_full_07_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.211. 4K Full Subtitle Test - Timed Text track file - Reel 9

| | |
|---|---|
| **Type** | MXF text |
| **Filename** | sub_test_4K_full_08_tt_ct.mxf |

| | | |
|---|---|---|
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 24/1 |

## A.2.212. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 1

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_00_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.213. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 2

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_01_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.214. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 3

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_02_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.215. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 4

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_03_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.216. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 5

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_04_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.217. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 6

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_05_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.218. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 7

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_06_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.219. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 8

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_07_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **EditRate** | 48/1 |

## A.2.220. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 9

| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_08_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.221. 2K 48fps Full Subtitle Test - Timed Text track file - Reel 10

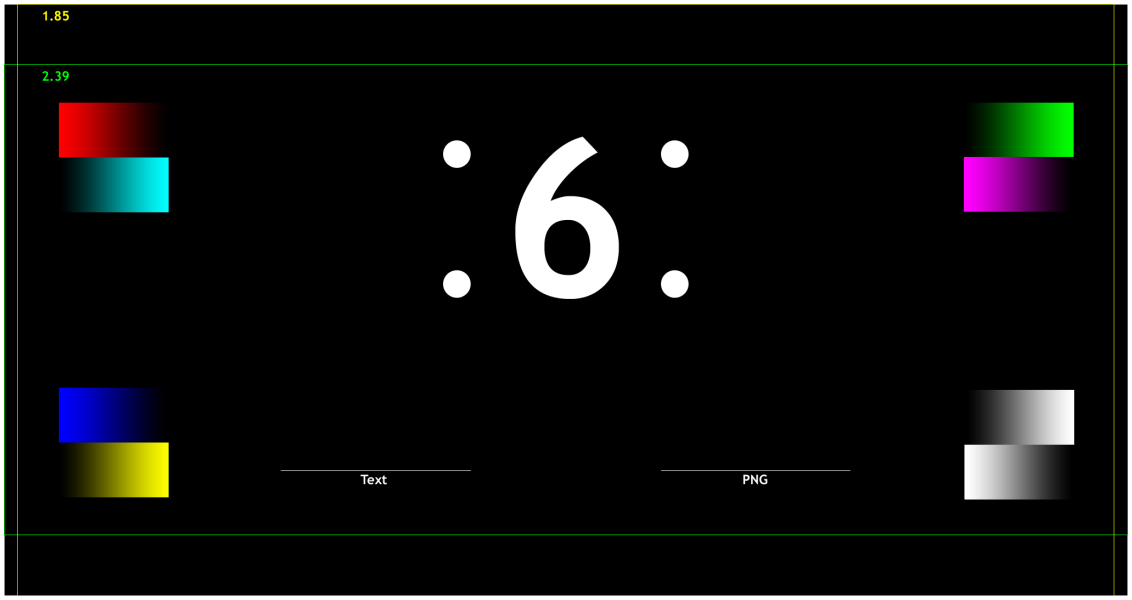
| | | |
|---|---|---|
| **Type** | MXF text | |
| **Filename** | sub_test_48fps_full_09_tt_ct.mxf | |
| **Description** | Encrypted MXF track file containing timed text test content. | |
| **Conforms to** | SMPTE-377-1, SMPTE-428-7, SMPTE-429-5, SMPTE-429-6 | |
| **Meta** | **Duration** | 00:01:00:00 |
| | **Encryption** | AES-128 |
| | **EditRate** | 48/1 |

## A.2.222. Sync Count with Subtitle Reticles

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | sync_count_with_subs_j2c_pt.mxf |
| **Description** | MXF track file containing five seconds (120 frames) of plain frames with reticles. followed by a ten second countdown and five seconds of plain frames with subtitle reticles. The countdown consists of ten identical one-second count segments, from 9-0. Each count segment consists of twenty-four frames of the respective digit for the count period. The first frame of each count segment will have a punch set to indicate sync. The |

| | | |
|---|---|---|
| | example image below shows the first frame of the fourth count period, which contains the number 6 (six). | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

### Figure A.10.Sync Count with Subtitle Reticles




## A.2.223. Sync Count with Subtitle Reticles (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF j2c | |
| **Filename** | sync_count_with_subs_j2c_ct.mxf | |
| **Description** | Encrypted MXF track file, contents are identical to Section A.2.222: Sync Count with Subtitle Reticles. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:20:00 |
| | **PixelArraySize** | 2048x1080 |
| | **EditRate** | 24/1 |

## A.2.224. StEM 2K Multi-Reel C (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c multi |
| **Filename** | StEM_2K_j2c_multi_C_ct_.mxf |
| **Description** | A set of encrypted MXF track files containing 2k image essence for the DCI StEM Mini Movie. 64 files, each with a duration of 1 second. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 |
| **Meta** | **SegmentCount** 64<br>**Encryption** AES-128<br>**SegmentDuration** 00:01:00<br>**Duration** 00:01:04:00<br>**PixelArraySize** 2048x858<br>**EditRate** 24/1 |

## A.2.225. M25 Picture Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | m25_integrity_pict_mic_j2c_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count* but the 1,441th edit unit is missing the MIC item. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 |
| **Malformations** | The 1,441th edit unit is missing the MIC item |

## A.2.226. M27 Picture Track File with Malformed Integrity Pack: Missing TrackFileID item (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | m27_integrity_pict_tfid_j2c_ct.mxf |

| | |
|---|---|
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count* but the 1,441th edit unit is missing the TrackFileID item. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 |
| **Malformations** | The 1,441th edit unit is missing the TrackFileID item |

## A.2.227. M26 Picture Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c |
| **Filename** | m26_integrity_pict_snum_j2c_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count* but the 1,441th edit unit is missing the SequenceNumber item. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 |
| **Malformations** | The 1,441th edit unit is missing the SequenceNumber item |

## A.2.228. Sync Count with KDM-Borne MIC Key

| | |
|---|---|
| **Type** | MXF j2c mkey |
| **Filename** | sync_count_j2c_mkey_pt.mxf |
| **Description** | Same as A.2.2. Sync Count, but with KDM-borne MIC Keys. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 |

## A.2.229. Sync Count with KDM-Borne MIC Key (Encrypted)

| | |
|---|---|
| **Type** | MXF j2c mkey |
| **Filename** | sync_count_j2c_mkey_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to A.2.228. Sync Count with KDM-Borne MIC Key. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 |

### A.2.230. OBAE Rendering Expectations Guide

| | |
|---|---|
| **Type** | MXF j2c mkey |
| **Filename** | obae_render_test_j2c_pt.mxf |
| **Description** | MXF track file whose image contents illustrates the expected acoustic output resulting from the rendering of A.3.90. OBAE Rendering Test. |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4, SMPTE-429-6 |

## A.3. Sound

### A.3.1. Introduction

This section defines a set of MXF sound track files. For each track file, a description is given which details the sounds encoded in the file. The sound track files will be combined with image files to make complete compositions (see Section A.4).

### A.3.2. Sync Count 5.1

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | sync_count_51_pcm_pt.mxf | |
| **Description** | MXF track file containing six channels of audio. Channels 1,2,4,5 and 6 are silent. Channel 3 (Center) contains five seconds (120 frames) of silence followed by a ten second countdown and five seconds of silence. The countdown consists of ten identical one-second count segments. Each count segment consists of one frame (2000 samples) encoding of a 1 kHz sine wave at -20 dBFS, followed by 23 frames of silence. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Duration** | 00:20:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.3. Sync Count 5.1 (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | sync_count_51_pcm_ct.mxf | |
| **Description** | Encrypted MXF track file, contents are identical to Section A.3.2: Sync Count 5 | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Encryption** | AES-128 |
| | **Duration** | 00:20:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.4. Sync Count 5.1 48fps

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | sync_count_51_48fps_pcm_pt.mxf | |
| **Description** | MXF track file containing six channels of audio. Channels 1,2,4,5 and 6 are silent. Channel 3 (Center) contains five seconds (240 frames) of silence followed by a ten second countdown and five seconds of silence. The countdown consists of ten identical one-second count segments. Each count segment consists of two frames (2000 samples) encoding of a 1 kHz sine wave at -20 dBFS, followed by 46 frames of silence. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Duration** | 00:20:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 48/1 |

## A.3.5. Channel I.D. 5.1

| | |
|---|---|
| **Type** | MXF pcm |

| | | |
|---|---|---|
| **Filename** | channel_id_51_pcm_pt.mxf | |
| **Description** | MXF track file containing a repeated voice announcement of the channel label of the respective channel: Left (Channel 1), Center (Channel 3), Right (Channel 2), Left Surround (Channel 5), Right Surround (Channel 6), LFE (Channel 4). Voice announcements are sequential, in the order given here. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Malformations** | | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Duration** | 00:40:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.6. Channel I.D. 1-16

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | channel_id_01-16_pcm_pt.mxf | |
| **Description** | MXF track file containing a sequential voice announcement of the channel number of the respective channel. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Duration** | 01:24:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.7. Pink Noise, 16 Channels

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | pink_noise_1-16_pcm_pt.mxf | |
| **Description** | Pink (1/ f) noise at -20 dBFS on sixteen channels, band limited to 22 KHz. Identical, sample-aligned signal must be used on all channels. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Duration** | 00:30:00 |

| | | |
|---|---|---|
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.8. Pink Noise, 16 Channels, 96 kHz

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | pink_noise_1-16_96khz_pcm_pt.mxf | |
| **Description** | Pink (1/ f) noise at -20 dBFS on sixteen channels, band limited to 44 KHz. Identical, sample-aligned signal must be used on all channels. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Duration** | 00:30:00 |
| | **SampleRate** | 96000 |
| | **EditRate** | 24/1 |

## A.3.9. Deleted Section

The section "Pink Noise, 16 Channels, 96 kHz (Encrypted)" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.3.10. Maximum Bitrate, 16 Channels, 96 kHz (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | max_bitrate_1-16_96khz_pcm_ct.mxf | |
| **Description** | Encrypted MXF sound track file containing a count to check synchronization between picture and sound, 10 minutes of pink (1/ f) noise at -20 dBFS on all sixteen channels, band limited to 44 KHz and a second sync count. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Encryption** | AES-128 |
| | **Duration** | 00:10:40:00 |

| | | |
|---|---|---|
| | **SampleRate** | 96000 |
| | **EditRate** | 24/1 |

## A.3.11. 1 kHz Sine Wave

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | 1_khz_sine_wave_pcm_pt.mxf | |
| **Description** | MXF track file containing 1 kHz sine wave on sixteen channels at -20 dBFS. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Duration** | 02:00:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.12. 1 kHz Sine Wave, 16 Channels 96kHz

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | 1_khz_sine_wave_96khz_pcm_pt.mxf | |
| **Description** | MXF track file containing 96kHz sample rate 1 kHz sine wave on sixteen channels at -20 dBFS. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Duration** | 02:00:00 |
| | **SampleRate** | 96000 |
| | **EditRate** | 24/1 |

## A.3.13. 400 hz sine wave

| | |
|---|---|
| **Type** | MXF pcm |
| | |

| | | |
|---|---|---|
| **Filename** | 400_hz_sine_wave_pcm_pt.mxf | |
| **Description** | MXF track file containing 400 Hz sine wave on six channels at -20 dBfs (dB Full Scale). LFE channel is full-range. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Duration** | 02:00:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.14. Deleted Section

The section "400 hz sine wave (Encrypted)" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.3.15. 400 hz sine wave, WTF (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | 400_hz_sine_wave_wtf_pcm_ct.mxf | |
| **Description** | Encrypted MXF track file containing 400 Hz sine wave on sixteen channels at -20 dBfs (dB Full Scale). LFE channel is full-range. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Encryption** | AES-128 |
| | **Duration** | 02:00:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.16. Silence, 5.1

| | |
|---|---|
| **Type** | MXF pcm |

| | | |
|---|---|---|
| **Filename** | black_51_pcm_pt.mxf | |
| **Description** | MXF track file containing six channels of silence. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Duration** | 02:00:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.17. Silence, 5.1, 15 minutes

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | black_long_51_pcm_pt.mxf | |
| **Description** | MXF track file containing six channels of silence. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Duration** | 00:15:00:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.18. Silence, 5.1, 15 minutes (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | black_long_51_pcm_ct.mxf | |
| **Description** | MXF track file containing six channels of silence. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6 | |
| **Prerequisites** | *Silence, 5.1, 15 minutes* | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Encryption** | AES-128 |
| | **Duration** | 00:15:00:00 |

| | | |
|---|---|---|
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.19. StEM 5.1 Sound

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | StEM_51_pcm_pt.mxf | |
| **Description** | MXF track file containing 5.1 sound essence for the DCI StEM Mini Movie. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Duration** | 11:31:21 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.20. StEM 5.1 Sound (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | StEM_51_pcm_ct.mxf | |
| **Description** | Encrypted MXF track file containing 5.1 sound essence for the DCI StEM Mini Movie. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-429-4 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Encryption** | AES-128 |
| | **Duration** | 11:31:21 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.21. StEM 5.1 Sound Multi-Reel A (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm multi | |
| **Filename** | StEM_51_pcm_multi_A_ct_.mxf | |
| **Description** | A set of encrypted MXF track files containing 5.1 sound essence for the DCI StEM Mini Movie. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-429-4 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **SegmentCount** | 128 |
| | **Encryption** | AES-128 |
| | **SegmentDuration** | 00:05:00 |
| | **Duration** | 00:10:40:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.22. StEM 5.1 Sound Multi-Reel B (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm multi | |
| **Filename** | StEM_51_pcm_multi_B_ct_.mxf | |
| **Description** | A set of encrypted MXF track files containing 5.1 sound essence for the DCI StEM Mini Movie. Identical to StEM_51_pcm_multi_A_ct | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-429-4 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **SegmentCount** | 128 |
| | **Encryption** | AES-128 |
| | **SegmentDuration** | 00:05:00 |
| | **Duration** | 00:10:40:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.23. StEM 5.1 Sound Multi-Reel A

| | |
|---|---|
| **Type** | MXF pcm multi |

| | |
|---|---|
| **Filename** | StEM_51_pcm_multi_A_pt_.mxf |
| **Description** | A set of plaintext MXF track files containing 5.1 sound essence for the DCI StEM Mini Movie. 128 files, each with a duration of 5 seconds. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-429-4 |
| **Meta** | **SoundFormat** 5.1<br>**SegmentCount** 128<br>**SegmentDuration** 00:05:00<br>**Duration** 00:10:40:00<br>**SampleRate** 48000<br>**EditRate** 24/1 |

## A.3.24. StEM 5.1 Sound Multi-Reel B

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | StEM_51_pcm_multi_B_pt_.mxf |
| **Description** | A set of plaintext MXF track files containing 5.1 sound essence for the DCI StEM Mini Movie. Identical to StEM_51_pcm_multi_A_pt |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-429-4 |
| **Meta** | **SoundFormat** 5.1<br>**SegmentCount** 128<br>**SegmentDuration** 00:05:00<br>**Duration** 00:10:40:00<br>**SampleRate** 48000<br>**EditRate** 24/1 |

## A.3.25. StEM 48fps 5.1 Sound

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | StEM_48fps_51_pcm_pt.mxf |
| **Description** | MXF track file containing 5.1 sound essence for the 48 fps DCI StEM Mini Movie. |
| | |

| | | |
|---|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Duration** | 00:51:46 |
| | **SampleRate** | 48000 |
| | **EditRate** | 48/1 |

## A.3.26. Deleted Section

The section "FM StEM 5.1 Sound (Encrypted)" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.3.27. FM StEM WTF Sound

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | fm_StEM_wtf_pcm_pt.mxf | |
| **Description** | MXF track file for FM testing containing WTF sound essence for the DCI StEM Mini Movie. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Duration** | 11:31:21 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.28. FM StEM WTF Sound (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | fm_StEM_wtf_pcm_ct.mxf | |
| **Description** | Encrypted MXF track file for FM testing containing WTF sound essence for the DCI StEM Mini Movie. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-429-4 | |
| **Meta** | **SoundFormat** | WTF |
| | **Encryption** | AES-128 |

| | | |
|---|---|---|
| | **Duration** | 11:31:21 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.29. Binary Audio FM Bypass WTF Sound (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | binary_audio_fm_bypass_wtf_pcm_ct.mxf | |
| **Description** | Encrypted MXF track file for FM testing containing known binary audio content on 16 channels of WTF format sound essence. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-429-4 | |
| **Meta** | **SoundFormat** | WTF |
| | **Encryption** | AES-128 |
| | **Duration** | 10:00:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.30. m02 Sound Frame Out Of Order (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | m02_snd_frame_oo_51_pcm_ct.mxf | |
| **Description** | Malformed, encrypted MXF track file containing six channels of 400Hz sine waves. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-4 | |
| **Malformations** | The KLV packets containing edit units 01 and 02 are swapped. | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Encryption** | AES-128 |
| | **Duration** | 00:00:05:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.31. m04 Sound Track File With Wrong TrackFile ID (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | m04_sndtk_wrong_file_pcm_ct.mxf | |
| **Description** | MXF track file in which the integrity pack of the 7th frame has the TrackFile ID replaced with a different value. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:05:00 |
| | **EditRate** | 24/1 |

## A.3.32. m10 Sound track file with bad HMAC (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | m10_snd_bad_hmac_pcm_ct.mxf | |
| **Description** | Sound track file in which one of the HMAC values for a single frame has been changed. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Malformations** | The file contains a replacement EKLV packet for the seventh frame (index 6). The replacement packet is taken from another track file having a different PackageUID but encrypted with the same symmetric key. | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Encryption** | AES-128 |
| | **Duration** | 00:00:05:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.33. m12 Sound Track File With Bad Check Value (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| | |

| | | |
|---|---|---|
| **Filename** | m12_snd_bad_chuk_pcm_ct.mxf | |
| **Description** | MXF track file containing one EKLV packet with an invalid Check Value. | |
| **Conforms to** | SMPTE-377-1, SMPTE-422, SMPTE-429-3, SMPTE-429-4 | |
| **Meta** | **Encryption** | AES-128 |
| | **Duration** | 00:00:05:00 |
| | **EditRate** | 24/1 |

## A.3.34. 400 hz sine wave, WTF

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | 400_hz_sine_wave_wtf_pcm_pt.mxf | |
| **Description** | MXF track file containing 400 Hz sine wave on sixteen channels at -20 dBfs (dB Full Scale). LFE channel is full-range. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 | |
| **Meta** | **SoundFormat** | WTF |
| | **Duration** | 02:00:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.35. Silence, 5.1 (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | black_51_pcm_ct.mxf | |
| **Description** | Encrypted MXF track file containing six channels of silence. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6 | |
| **Prerequisites** | *Silence, 5.1* | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Encryption** | AES-128 |
| | **Duration** | 02:00:00 |
| | **SampleRate** | 48000 |

| | | |
|---|---|---|
| | **EditRate** | 24/1 |

## A.3.36. Silence, 5.1, 48 fps (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm | |
| **Filename** | black_51_48fps_pcm_ct.mxf | |
| **Description** | 48 Frames per second (fps) MXF track file containing six channels of silence. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **Encryption** | AES-128 |
| | **Duration** | 00:02:00:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 48/1 |

## A.3.37. StEM 5.1 Sound Multi-Reel C (Encrypted)

| | | |
|---|---|---|
| **Type** | MXF pcm multi | |
| **Filename** | StEM_51_pcm_multi_C_ct_.mxf | |
| **Description** | A set of encrypted MXF track files containing 5.1 sound essence for the DCI StEM Mini Movie. 64 files, each with a duration of 1 second. | |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-429-4 | |
| **Meta** | **SoundFormat** | 5.1 |
| | **SegmentCount** | 64 |
| | **Encryption** | AES-128 |
| | **SegmentDuration** | 00:01:00 |
| | **Duration** | 00:01:04:00 |
| | **SampleRate** | 48000 |
| | **EditRate** | 24/1 |

## A.3.38. Sync Count OBAE (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | sync_count_obae_ct.mxf |
| **Description** | Encrypted version of Section A.3.39: Sync Count OBAE |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.39. Sync Count OBAE

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | sync_count_obae_pt.mxf |
| **Description** | Immersive Audio track file where the center channel of the 9.1OH bed contains five seconds (120 frames) of silence followed by a ten second countdown and five seconds of silence. The countdown consists of ten identical one-second count segments. Each count segment consists of one frame (2000 samples) encoding of a 1 kHz sine wave at -20 dBFS, followed by 23 frames of silence. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.40. Main Sound for Sync Count OBAE (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | sync_count_obae_ms_ct.mxf |
| **Description** | Encrypted version of Section A.3.41: Main Sound for Sync Count OBAE. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.41. Main Sound for Sync Count OBAE

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | sync_count_obae_ms_pt.mxf |
| | |

| | |
|---|---|
| **Description** | Sound Track File as specified in SMPTE ST 429-19, where the FSK synchronization signal is intended to synchronize playback of Section A.3.39: Sync Count OBAE. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.42. Main Sound for StEM OBAE (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | StEM_obae_ms_ct.mxf |
| **Description** | Encrypted version of Section A.3.43: Main Sound for StEM OBAE. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.43. Main Sound for StEM OBAE

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | StEM_obae_ms_pt.mxf |
| **Description** | Sound Track File as specified in SMPTE ST 429-19, where the FSK synchronization signal is intended to synchronize playback of Section A.3.45: StEM OBAE. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.44. StEM OBAE (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | StEM_obae_ct.mxf |
| **Description** | Encrypted version of Section A.3.45: StEM OBAE |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.45. StEM OBAE

| | |
|---|---|
| **Type** | MXF obae |

| | |
|---|---|
| **Filename** | StEM_obae_pt.mxf |
| **Description** | Immersive Audio track file for the StEM mini-movie. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.46. M28 Sound Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | m28_integrity_snd_mic_pcm_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count 5.1* but the 1,441th edit unit is missing the MIC item. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6 |
| **Malformations** | The 1,441th edit unit is missing the MIC item |

## A.3.47. M30 Sound Track File with Malformed Integrity Pack: Missing TrackFileID item (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | m30_integrity_snd_tfid_pcm_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count 5.1* but the 1,441th edit unit is missing the TrackFileID item. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6 |
| **Malformations** | The 1,441th edit unit is missing the TrackFileID item |

## A.3.48. M29 Sound Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | m29_integrity_snd_snum_pcm_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count 5.1* but the 1,441th edit unit is missing the SequenceNumber item. |

| | |
|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6 |
| **Malformations** | The 1,441th edit unit is missing the SequenceNumber item |

## A.3.49. M20 Sound Track File with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | m20_integrity_obae_ms_mic_pcm_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Main Sound for Sync Count OBAE* but the 1,441th edit unit is missing the MIC item. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |
| **Malformations** | The 1,441th edit unit is missing the MIC item |

## A.3.50. M22 Sound Track File with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | m22_integrity_obae_ms_tfid_pcm_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Main Sound for Sync Count OBAE* but the 1,441th edit unit is missing the TrackFileID item. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |
| **Malformations** | The 1,441th edit unit is missing the TrackFileID item |

## A.3.51. M21 Sound Track File with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | m21_integrity_obae_ms_snum_pcm_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Main Sound for Sync Count OBAE* but the 1,441th edit unit is missing the SequenceNumber item. |

| | |
|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |
| **Malformations** | The 1,441th edit unit is missing the SequenceNumber item |

## A.3.52. M19 OBAE Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | m19_integrity_obae_mic_obae_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count OBAE* but the 1,441th edit unit is missing the MIC item. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-492-18, SMPTE-429-6 |
| **Malformations** | The 1,441th edit unit is missing the MIC item |

## A.3.53. M24 OBAE Track File with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | m24_integrity_obae_tfid_obae_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count OBAE* but the 1,441th edit unit is missing the TrackFileID item. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-492-18, SMPTE-429-6 |
| **Malformations** | The 1,441th edit unit is missing the TrackFileID item |

## A.3.54. M23 OBAE Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | m23_integrity_obae_snum_obae_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count OBAE* but the 1,441th edit unit is missing the SequenceNumber item. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-492-18, SMPTE-429-6 |

| | |
|---|---|
| **Malformations** | The 1,441th edit unit is missing the SequenceNumber item |

## A.3.55. StEM OBAE Multi-Reel C (Encrypted)

| | |
|---|---|
| **Type** | MXF obae multi |
| **Filename** | StEM_obae_multi_C_ct_.mxf |
| **Description** | A set of encrypted track files containing OBAE essence for the DCI StEM Mini Movie. 64 files, each with a duration of 1 second. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-429-18 |

## A.3.56. Main Sound for StEM OBAE Multi-Reel C (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | StEM_obae_ms_multi_C_ct_.mxf |
| **Description** | A set of encrypted sound track files, where the FSK synchronization signal is intended to synchronize playback of Section A.3.55: StEM OBAE Multi-Reel C (Encrypted). 64 files, each with a duration of 1 second. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.57. M40 OBAE Track File with Frame-out-of-order error (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | m40_obae_frame_oo_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count OBAE* but the KLV packets for the 1st and 2nd edit units are swapped. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-492-18, SMPTE-429-6 |
| **Malformations** | The 1st and 2nd edit units contain out-of-order Sequence Number item values. |

## A.3.58. M41 OBAE Track File With Wrong TrackFile ID (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | m41_obae_wrong_file_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count OBAE* but with the TrackFile ID item value of the 7th edit unit replaced with a different value. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-492-18, SMPTE-429-6 |
| **Malformations** | The TrackFile ID item value of the 7th edit unit is not equal to the identifier of the Track File. |

## A.3.59. Sync Count OBAE with MIC Key (Encrypted)

| | |
|---|---|
| **Type** | MXF obae mkey |
| **Filename** | sync_count_obae_mkey_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count OBAE*, with the MIC item value computed using the MIC Key `c5 9a f6 6f bd e0 70 39 ba 36 2c 62 e8 21 e6 02`. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-492-18, SMPTE-429-6, DCI-DCSS |

## A.3.60. M43 OBAE Track File With Bad Check Value (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | m43_obae_bad_chuk_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count OBAE* but with the Check Value of the 7th edit unit replaced with an invalid value. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-492-18, SMPTE-429-6 |
| **Malformations** | The Check Value value of the 7th edit unit is invalid. |

## A.3.61. Sync Count 5.1 with KDM-Borne MIC Key

| | |
|---|---|
| **Type** | MXF pcm mkey |

| | |
|---|---|
| **Filename** | sync_count_51_pcm_mkey_pt.mxf |
| **Description** | Same as *Sync Count 5.1* but with KDM-borne MIC Keys. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 |

## A.3.62. Sync Count 5.1 with KDM-Borne MIC Key (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | sync_count_51_pcm_mkey_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to A.3.61. Sync Count 5.1 with KDM-Borne MIC Key. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6 |

## A.3.63. M44 OBAE Track File With Bad HMAC Value (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | m44_obae_bad_hmac_ct.mxf |
| **Description** | Encrypted MXF track file, contents are identical to *Sync Count OBAE* but with the HMAC value of the 7th edit unit replaced with an invalid value. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-492-18, SMPTE-429-6 |
| **Malformations** | The HMAC value of the 7th edit unit is invalid. |

## A.3.64. OBAE Tone Multi-Reel (Encrypted)

| | |
|---|---|
| **Type** | MXF obae multi |
| **Filename** | OBAE_tone_multi_ct_.mxf |
| **Description** | Encrypted version of A.3.65. OBAE Tone Multi-Reel |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.65. OBAE Tone Multi-Reel

| | |
|---|---|
| **Type** | MXF obae multi |
| **Filename** | OBAE_tone_multi_pt_.mxf |
| **Description** | Sequence of 20 OBAE Track Files, each 1 second long, whose IA Frame contents, when concatenated, form a single continuous IA Bitstream. The IA Bitstream consists of (a) 9.1OH bed channels, each containing a 400 Hz sine wave tone (-20 dBFS), and (b) one stationary object, using a 400 Hz sine wave tone (-20 dBFS). |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.66. Main Sound for OBAE Tone Multi-Reel (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | OBAE_tone_multi_ms_ct_.mxf |
| **Description** | Encrypted version of A.3.67. Main Sound for OBAE Tone Multi-Reel |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.67. Main Sound for OBAE Tone Multi-Reel

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | OBAE_tone_multi_ms_pt_.mxf |
| **Description** | Sequence of Sound Track Files, each as specified in SMPTE ST 429-19, where the FSK synchronization signal is intended to synchronize playback of A.3.65. OBAE Tone Multi-Reel. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.68. Audio Tone Multi-Reel (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | audio_tone_multi_ct_.mxf |
| **Description** | Encrypted version of A.3.69. Audio Tone Multi-Reel |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-6, SMPTE-382 |

## A.3.69. Audio Tone Multi-Reel

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | audio_tone_multi_pt_.mxf |
| **Description** | Sequence of 20 audio track files, each 1 second long, whose contents, when concatenated, consists of a continuous 400 Hz sine wave on sixteen channels at -20 dBfs (dB Full Scale). The LFE channel is full-range. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 |

## A.3.70. Main Sound for Sync Count (48fps) OBAE

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | sync_count_48fps_obae_ms_pt.mxf |
| **Description** | Sound Track File as specified in SMPTE ST 429-19, where the FSK synchronization signal is intended to synchronize playback of Sync Count (48fps) OBAE. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.71. Sync Count (48fps) OBAE

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | sync_count_48fps_obae_pt.mxf |
| **Description** | Identical content to Sync Count OBAE, but framed at 48 fps. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.72. 400 hz sine wave (OBAE)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | 400_hz_sine_wave_obae_pt.mxf |
| **Description** | The IA Bitstream consists of (a) 9.1OH bed channels, each containing a 400 Hz sine wave tone (-20 dBFS), and (b) one stationary object located on the ceiling (z=1), using a 400 Hz sine wave tone (-20 dBFS). |

| | |
|---|---|
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.73. 400 hz sine wave (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | 400_hz_sine_wave_obae_ct.mxf |
| **Description** | Encrypted version of A.3.72. 400 hz sine wave (OBAE) |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.74. Main Sound for 400 hz sine wave (OBAE)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | 400_hz_sine_wave_obae_ms_pt.mxf |
| **Description** | Sound Track File as specified in SMPTE ST 429-19 that contains only an FSK synchronization signal intended to synchronize playback of A.3.72. 400 hz sine wave (OBAE). |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.75. FM StEM OBAE

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | fm_StEM_obae_pt.mxf |
| **Description** | Intended to accompany the DCI StEM Mini Movie for FM testing. The IA Bitstream consists of (a) 9.1OH bed channels, each containing a 400 Hz sine wave tone (-20 dBFS), and (b) one object, using a 400 Hz sine wave tone (-20 dBFS), whose trajectory uniformly covers the unit hemisphere. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.76. FM StEM OBAE (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | fm_StEM_obae_ct.mxf |

| | |
|---|---|
| **Description** | Encrypted version of A.3.75. FM StEM OBAE |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.77. Main Sound for FM StEM OBAE

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | fm_StEM_obae_ms_pt.mxf |
| **Description** | Sound Track File as specified in SMPTE ST 429-19, that contains only an FSK synchronization signal intended to synchronize playback of A.3.75. FM StEM OBAE. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.78. StEM OBAE Multi-Reel A

| | |
|---|---|
| **Type** | MXF obae multi |
| **Filename** | StEM_obae_multi_A_pt_.mxf |
| **Description** | A set of plaintext Immersive Audio track files for the StEM mini-movie. 128 files, each with a duration of 5 seconds. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.79. Main Sound for StEM OBAE Multi-Reel A

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | StEM_obae_ms_multi_A_pt_.mxf |
| **Description** | A set of plaintext Sound Track Files, each as specified in [SMPTE-429-19], where the FSK synchronization signal is intended to synchronize playback of Section A.3.45: StEM OBAE. 128 files, each with a duration of 5 seconds. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.80. StEM OBAE Multi-Reel B

| | |
|---|---|
| **Type** | MXF obae multi |
| **Filename** | StEM_obae_multi_B_pt_.mxf |
| **Description** | Set of Track Files whose essence and segmentation are identical to those at A.3.78. StEM OBAE Multi-Reel A. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.81. Main Sound for StEM OBAE Multi-Reel B

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | StEM_obae_ms_multi_B_pt_.mxf |
| **Description** | Set of Track Files whose essence and segmentation are identical to those at A.3.79. Main Sound for StEM OBAE Multi-Reel A. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.82. StEM OBAE Multi-Reel A (Encrypted)

| | |
|---|---|
| **Type** | MXF obae multi |
| **Filename** | StEM_obae_multi_A_ct_.mxf |
| **Description** | Encrypted version of A.3.78. StEM OBAE Multi-Reel A, where the same cryptographic key is used for every 2 consecutive Track Files, resulting in 64 distinct cryptographic keys being used. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.83. Main Sound for StEM OBAE Multi-Reel A (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | StEM_obae_ms_multi_A_ct_.mxf |
| **Description** | Encrypted version of A.3.79. Main Sound for StEM OBAE Multi-Reel A, where the same cryptographic key is used for every 2 consecutive Track Files, resulting in 64 distinct cryptographic keys being used. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.84. StEM OBAE Multi-Reel B (Encrypted)

| | |
|---|---|
| **Type** | MXF obae multi |
| **Filename** | StEM_obae_multi_B_ct_.mxf |
| **Description** | Encrypted version of A.3.80. StEM OBAE Multi-Reel B, where the same cryptographic key is used for every 2 consecutive Track Files, resulting in 64 distinct cryptographic keys being used. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.85. Main Sound for StEM OBAE Multi-Reel B (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm multi |
| **Filename** | StEM_obae_ms_multi_B_ct_.mxf |
| **Description** | Encrypted version of A.3.81. Main Sound for StEM OBAE Multi-Reel B, where the same cryptographic key is used for every 2 consecutive Track Files, resulting in 64 distinct cryptographic keys being used. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.86. Maximum Bitrate OBAE 48 fps (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | maximum_bitrate_48Hz_obae_obae_ct.mxf |
| **Description** | Intended to accompany *StEM 2K 48 fps*. The IA Bitstream is 120s long, has a frame rate of 48 Hz and each frame is the maximum size specified in [SMPTE-429-18]. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.87. Main Sound for Maximum Bitrate OBAE 48 fps (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | maximum_bitrate_48Hz_obae_pcm_ct.mxf |
| | |

| | |
|---|---|
| **Description** | Sound Track File as specified in SMPTE ST 429-19, that contains only an FSK synchronization signal intended to synchronize playback of A.3.86. Maximum Bitrate OBAE 48 fps (Encrypted). |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.88. Maximum Bitrate OBAE (Encrypted)

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | maximum_bitrate_24Hz_obae_obae_ct.mxf |
| **Description** | Intended to accompany *StEM 2K*. The IA Bitstream is 120s long, has a frame rate of 24 Hz and each frame is the maximum size specified in [SMPTE-429-18]. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18, SMPTE-429-6 |

## A.3.89. Main Sound for Maximum Bitrate OBAE (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | maximum_bitrate_24Hz_obae_pcm_ct.mxf |
| **Description** | Sound Track File as specified in SMPTE ST 429-19, that contains only an FSK synchronization signal intended to synchronize playback of A.3.88. Maximum Bitrate OBAE (Encrypted). |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.3.90. OBAE Rendering Test

| | |
|---|---|
| **Type** | MXF obae |
| **Filename** | obae_render_test_j2c_pt.mxf |
| **Description** | Exercises selected OBAE bitstream capabilities. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-429-18 |

## A.3.91. Main Sound for OBAE Rendering Test

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | obae_render_test_ms_pt.mxf |
| **Description** | Sound Track File as specified in SMPTE ST 429-19, that contains only an FSK synchronization signal intended to synchronize playback of A.3.90. OBAE Rendering Test. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

### A.3.92. Silence w/ HI/VI

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | obae_render_test_ms_silence_pt.mxf |
| **Description** | Sound Track File that contains silence on all channels but HI/VI. |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382 |

### A.3.93. Main Sound for 400 hz sine wave (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | MXF pcm |
| **Filename** | 400_hz_sine_wave_obae_ms_ct.mxf |
| **Description** | Encrypted version of A.3.74. Main Sound for 400 hz sine wave (OBAE) |
| **Conforms to** | SMPTE-377-1, SMPTE-429-3, SMPTE-382, SMPTE-429-6, SMPTE-430-12, SMPTE-430-12-AM1-2019, SMPTE-429-19 |

## A.4. D-Cinema Packages

### A.4.1. Introduction

This section defines a set of D-Cinema Compositions and D-Cinema Packages. The Compositions depend upon the track files created in Section A.2 and Section A.3. The Packages contain the Compositions for ingest.

### A.4.2. DCI 2K Sync Test

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count*, *Sync Count 5.1* |

## A.4.3. DCI 2K Sync Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Sync Count 5.1 (Encrypted)* |

## A.4.4. DCI 2K Sync test with Subtitles

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sync_test_with_subs.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count with Subtitle Reticles*, *Sync Count 5.1*, *Sync Count Text* |

## A.4.5. DCI 2K Sync test with Subtitles (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sync_test_with_subs_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count with Subtitle Reticles (Encrypted)*, *Sync Count 5.1 (Encrypted)*, *Sync Count Text (Encrypted)* |

## A.4.6. DCI 2K Sync Test (48fps)

| | |
|---|---|

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sync_test_48fps.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count*, *48fps*, *Sync Count 5.1 48fps* |
| **Meta** | **EditRate** 48/1 |

## A.4.7. 4K Sync Test

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 4K_sync_test.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *4K Sync Count*, *Sync Count 5.1* |

## A.4.8. DCI 5.1 Channel Identification

| | |
|---|---|
| **Type** | CPL |
| **Filename** | channel_id_51_pt.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Channel I.D. 5.1*, *Channel I.D. 5.1* |

## A.4.9. DCI 1-16 Numbered Channel Identification

| | |
|---|---|
| **Type** | CPL |
| **Filename** | channel_id_01-16.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Channel I.D. 1-16*, *Channel I.D. 1-16* |

## A.4.10. DCI NIST Frame with silence

| | |
|---|---|
| **Type** | CPL |
| **Filename** | nist_pattern_black_audio.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, Silence, 5.1* |

## A.4.11. 4K DCI NIST Frame with silence

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 4K_nist_pattern.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 4K Test Pattern, Silence, 5.1* |

## A.4.12. DCI NIST Frame with Pink Noise

| | |
|---|---|
| **Type** | CPL |
| **Filename** | nist_pattern_pink_noise.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, Pink Noise, 16 Channels* |

## A.4.13. DCI NIST Frame with 1 kHz tone (-20 dB fs)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | nist_pattern_1k.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, 1 kHz Sine Wave* |

## A.4.14. DCI NIST Frame with Pink Noise (96 kHz)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | nist_pattern_pink_noise_96k.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, Pink Noise, 16 Channels, 96 kHz* |

## A.4.15. DCI NIST Frame with 1 kHz tone (-20 dB fs, 96kHz)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | nist_pattern_1k_96k.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, 1 kHz Sine Wave, 16 Channels 96kHz* |

## A.4.16. DCI NIST Frame no sound files

| | |
|---|---|
| **Type** | CPL |
| **Filename** | nist_pattern_no_audio.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern* |

## A.4.17. DCI 2K Image with Frame Number Burn In

| | |
|---|---|
| **Type** | CPL |
| **Filename** | frame_num_burn_in.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *DCI Numbered Frame Sequence, Silence, 5.1, 15 minutes* |

## A.4.18. DCI 2K Image with Frame Number Burn In (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | frame_num_burn_in_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *DCI Numbered Frame Sequence (Encrypted), Silence, 5.1, 15 minutes (Encrypted)* |

## A.4.19. DCI 2K Image with Frame Number Burn In (Flat)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | frame_count_flat_2_reels.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *DCI Flat Transition Sequence, Silence, 5.1* |

## A.4.20. DCI 2K Image with Frame Number Burn In (Scope)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | frame_count_scope_2_reels.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *DCI Scope Transition Sequence, Silence, 5.1* |

## A.4.21. DCI 2K StEM

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_pt.cpl.xml |
| **Description** | A plaintext composition consisting of the StEM 2K image and 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K, StEM 5.1 Sound* |

## A.4.22. DCI 2K StEM (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_ct.cpl.xml |
| **Description** | An encrypted composition consisting of the encrypted StEM 2K image and encrypted 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted)*, *StEM 5.1 Sound (Encrypted)* |

## A.4.23. DCI 2K StEM Test Sequence

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_sequence_pt.cpl.xml |
| **Description** | A plaintext composition consisting of six (6) reels. Each reel is composed of the StEM 2K image and 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K*, *StEM 5.1 Sound* |

## A.4.24. DCI 2K StEM Test Sequence (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_sequence_ct.cpl.xml |
| **Description** | An encrypted composition consisting of six (6) reels. Each reel is composed of the encrypted StEM 2K image and encrypted 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted)*, *StEM 5.1 Sound (Encrypted)* |

## A.4.25. DCI 2K 48fps StEM

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_48fps_pt.cpl.xml |
| **Description** | A plaintext composition consisting of the StEM 2K 48 fps image and 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |

| | |
|---|---|
| **Prerequisites** | *StEM 2K 48 fps, StEM 48fps 5.1 Sound* |

## A.4.26. 128 Reel Composition, "A" Series

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_128_a_reels_pt.cpl.xml |
| **Description** | A plaintext composition consisting of one hundred and twenty eight (128) reels. Each reel is composed of part of the plaintext StEM 2K image and plaintext 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K Multi-Reel A, StEM 5.1 Sound Multi-Reel A* |

## A.4.27. 128 Reel Composition, "B" Series

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_128_b_reels_pt.cpl.xml |
| **Description** | A plaintext composition consisting of one hundred and twenty eight (128) reels. Each reel is composed of part of the plaintext StEM 2K image and plaintext 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K Multi-Reel B, StEM 5.1 Sound Multi-Reel B* |

## A.4.28. 128 Reel Composition, "A" Series (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_128_a_reels_ct.cpl.xml |
| **Description** | An encrypted composition consisting of one hundred and twenty eight (128) reels. Each reel is composed of part of the encrypted StEM 2K image and encrypted 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K Multi-Reel A (Encrypted), StEM 5.1 Sound Multi-Reel A (Encrypted)* |

## A.4.29. 128 Reel Composition, "B" Series (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_128_b_reels_ct.cpl.xml |
| **Description** | An encrypted composition consisting of one hundred and twenty eight (128) reels. Each reel is composed of part of the encrypted StEM 2K image and encrypted 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K Multi-Reel B (Encrypted)*, *StEM 5.1 Sound Multi-Reel B (Encrypted)* |

## A.4.30. 64 Reel Composition, 1 Second Reels (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_64_1_second_reels_ct.cpl.xml |
| **Description** | An encrypted composition consisting of sixty four (64) reels, each with a duration of 1 second. Each reel is composed of part of the encrypted StEM 2K image and encrypted 5.1 sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K Multi-Reel C (Encrypted)*, *StEM 5.1 Sound Multi-Reel C (Encrypted)* |

## A.4.31. 2K FM Application Constraints (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_constraints_ct.cpl.xml |
| **Description** | A composition consisting of FM testing instructions and both encrypted and plaintext StEM 2K image and 16 channel WTF format sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *FM Constraints Begin (Plaintext)*, *FM Constraints Begin (Encrypted)*, *FM Constraints End (Plaintext)*, *FM Constraints End (Encrypted)*, *400 hz sine wave, WTF (Encrypted)*, *400 hz sine wave, WTF*, *StEM 2K (Encrypted)*, *StEM 2K*, *FM StEM WTF Sound*, *FM StEM WTF Sound (Encrypted)* |

## A.4.32. 2K FM Control Granularity - No FM (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_control_granularity_no_fm.cpl.xml |
| **Description** | An encrypted composition containing the encrypted StEM 2K image and encrypted 16 channel WTF format sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *2K FM Control Granularity Begin (Encrypted), 2K FM Control Granularity End (Encrypted), 400 hz sine wave, WTF (Encrypted), StEM 2K (Encrypted), FM StEM WTF Sound (Encrypted)* |

## A.4.33. 2K FM Control Granularity - Image Only FM (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_control_granularity_image_only_fm.cpl.xml |
| **Description** | An encrypted composition containing the FM encrypted StEM 2K image and encrypted 16 channel WTF format sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *2K FM Control Granularity Begin (Encrypted), 2K FM Control Granularity End (Encrypted), 400 hz sine wave, WTF (Encrypted), StEM 2K (Encrypted), FM StEM WTF Sound (Encrypted)* |

## A.4.34. 2K FM Control Granularity - Sound Only FM (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_control_granularity_sound_only_fm.cpl.xml |
| **Description** | An encrypted composition containing the encrypted StEM 2K image and encrypted 16 channel WTF format sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *2K FM Control Granularity Begin (Encrypted), 2K FM Control Granularity End (Encrypted), 400 hz sine wave, WTF (Encrypted), StEM 2K (Encrypted), FM StEM WTF Sound (Encrypted)* |

## A.4.35. 2K FM Control Granularity - Image and Sound FM (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_control_granularity_image_and_sound_fm.cpl.xml |
| **Description** | An encrypted composition containing of the encrypted StEM 2K image and encrypted 16 channel WTF format sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *2K FM Control Granularity Begin (Encrypted)*, *2K FM Control Granularity End (Encrypted)*, *400 hz sine wave, WTF (Encrypted)*, *StEM 2K (Encrypted)*, *FM StEM WTF Sound (Encrypted)* |

## A.4.36. 2K FM Payload (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_payload_ct.cpl.xml |
| **Description** | An encrypted composition for FM detection containing the encrypted StEM 2K image and encrypted 16 channel WTF format sound track files. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *2K FM Payload Begin (Encrypted)*, *2K FM Payload End (Encrypted)*, *400 hz sine wave, WTF (Encrypted)*, *StEM 2K (Encrypted)*, *FM StEM WTF Sound (Encrypted)* |

## A.4.37. Binary Audio Forensic Marking Bypass Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | binary_audio_fm_ct.cpl.xml |
| **Description** | An encrypted composition containing an encrypted 48 kHz sound track file with 16 channels of audio in WTF format. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Binary Audio FM Bypass*, *Binary Audio FM Bypass WTF Sound (Encrypted)* |

## A.4.38. Selective Audio FM - All FM (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | selective_audio_fm_all-fm_ct.cpl.xml |
| **Description** | An encrypted composition containing an encrypted sound track file with 16 channels of audio. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Selective FM Begin*, *Selective FM End*, *400 hz sine wave, WTF (Encrypted)*, *StEM 2K*, *FM StEM WTF Sound (Encrypted)* |

## A.4.39. Selective Audio FM - No FM (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | selective_audio_fm_no-fm_ct.cpl.xml |
| **Description** | An encrypted composition containing an encrypted sound track file with 16 channels of audio. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Selective FM Begin*, *Selective FM End*, *400 hz sine wave, WTF (Encrypted)*, *StEM 2K*, *FM StEM WTF Sound (Encrypted)* |

## A.4.40. Selective Audio FM - Not Above Channel 6 (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | selective_audio_fm_6ch_ct.cpl.xml |
| **Description** | An encrypted composition containing an encrypted sound track file with 16 channels of audio. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Selective FM Begin*, *Selective FM End*, *400 hz sine wave, WTF (Encrypted)*, *StEM 2K*, *FM StEM WTF Sound (Encrypted)* |

## A.4.41. Selective Audio FM - Not Above Channel 8 (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | selective_audio_fm_8ch_ct.cpl.xml |
| **Description** | An encrypted composition containing an encrypted sound track file with 16 channels of audio. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Selective FM Begin, Selective FM End, 400 hz sine wave, WTF (Encrypted), StEM 2K, FM StEM WTF Sound (Encrypted)* |

## A.4.42. Selective Audio FM - Not Above Channel 10 (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | selective_audio_fm_10ch_ct.cpl.xml |
| **Description** | An encrypted composition containing an encrypted sound track file with 16 channels of audio. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Selective FM Begin, Selective FM End, 400 hz sine wave, WTF (Encrypted), StEM 2K, FM StEM WTF Sound (Encrypted)* |

## A.4.43. Selective Audio FM - Not Above Channel 17 (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | selective_audio_fm_17ch_ct.cpl.xml |
| **Description** | An encrypted composition containing an encrypted sound track file with 16 channels of audio. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Selective FM Begin, Selective FM End, 400 hz sine wave, WTF (Encrypted), StEM 2K, FM StEM WTF Sound (Encrypted)* |

## A.4.44. 2K DCI Maximum Bitrate Composition (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_max_bitrate_ct.cpl.xml |
| **Description** | Encrypted composition containing picture and sound track files of the maximum allowable bitrate. |
| **Conforms to** | SMPTE-429-7 |

| | |
|---|---|
| **Prerequisites** | *2K Picture Track File, Maximum Bitrate, Maximum Bitrate, 16 Channels, 96 kHz (Encrypted)* |

## A.4.45. 4K DCI Maximum Bitrate Composition (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 4K_max_bitrate_ct.cpl.xml |
| **Description** | Encrypted composition containing picture and sound track files of the maximum allowable bitrate. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *4K Picture Track File, Maximum Bitrate, Maximum Bitrate, 16 Channels, 96 kHz (Encrypted)* |

## A.4.46. End of Engagement - Past Time Window Extension (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | holdover_long_ct.cpl.xml |
| **Description** | An encrypted composition with duration of 6 hours and 11 minutes. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted), StEM 5.1 Sound (Encrypted)* |

## A.4.47. End of Engagement - Within Time Window Extension (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | holdover_short_ct.cpl.xml |
| **Description** | An encrypted composition with duration of 5 hours and 59 minutes and 30 seconds. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted), StEM 5.1 Sound (Encrypted)* |

## A.4.48. Deleted Section

The section "Multi-line Subtitle Test" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.4.49. Deleted Section

The section "Multi-line PNG Subtitle Test" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.4.50. Deleted Section

The section "Subtitle Test Part 1" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.4.51. Deleted Section

The section "Subtitle Test Part 2" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.4.52. Deleted Section

The section "Subtitle Test Part 3" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.4.53. DCI Black Spacer - 5 seconds

| | |
|---|---|
| **Type** | CPL |
| **Filename** | black_spacer_5s.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Black (Empty Frame)*, *Silence, 5.1* |

## A.4.54. White Frame Sequence

| | |
|---|---|
| **Type** | CPL |
| **Filename** | white_pt.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *White (White Frame), Silence, 5.1* |

## A.4.55. Intra-Frame Contrast Sequence

| | |
|---|---|
| **Type** | CPL |
| **Filename** | checkerboard_pt.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-431-2 |
| **Prerequisites** | *Intra-Frame Contrast Sequence, Silence, 5.1* |

## A.4.56. Sequential Contrast and Uniformity Sequence

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sequential_contrast_pt.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-431-2 |
| **Prerequisites** | *Sequential Contrast Sequence, Silence, 5.1* |

## A.4.57. DCI Gray Steps

| | |
|---|---|
| **Type** | CPL |
| **Filename** | gray_step.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Black to Gray Step Series, Silence, 5.1, 15 minutes* |

## A.4.58. DCI White Steps

| | |
|---|---|
| **Type** | CPL |
| **Filename** | white_step.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Black to White Step Series, Silence, 5.1, 15 minutes* |

## A.4.59. DCI 2K Moving Gradient

| | |
|---|---|
| **Type** | CPL |
| **Filename** | moving-gradient-white.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *DCI_gradient_step_s_white_j2c_pt, Silence, 5.1* |

## A.4.60. Deleted Section

The section "DCI 2K Moving Gradient" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.4.61. Color Accuracy Series

| | |
|---|---|
| **Type** | CPL |
| **Filename** | color_accuracy_pt.cpl.xml |
| **Description** | Composition containing five seconds (120 frames) of a chart showing all color values for the test in Section 7.5.12: Color Accuracy. This is followed by 1 minute of each of the 12 color values as a full frame. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Color Accuracy Series, Silence, 5.1, 15 minutes* |

## A.4.62. 4K Color Accuracy Series

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 4K_color_accuracy_pt.cpl.xml |
| **Description** | 4K composition containing contents identical to Section A.4.61: Color Accuracy Series |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *4K Color Accuracy Series, Silence, 5.1, 15 minutes* |

## A.4.63. Pixel Structure Pattern N 2k

| | |
|---|---|
| **Type** | CPL |
| **Filename** | pixel_structure_N_2k_pt.cpl.xml |
| **Description** | North-oriented pixel structure test pattern featuring 16 x 16 and 8 x 8 pixel patterns with binary position indicators. See Section 7.5.3: Projector Pixel Count/Structure for description. |
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *pixel_structure_N_2k_j2c_pt, Silence, 5.1* |

## A.4.64. Pixel Structure Pattern S 2k

| | |
|---|---|
| **Type** | CPL |
| **Filename** | pixel_structure_S_2k_pt.cpl.xml |
| **Description** | South-oriented pixel structure test pattern featuring 16 x 16 and 8 x 8 pixel patterns with binary position indicators. See Section 7.5.3: Projector Pixel Count/Structure for description. |
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *pixel_structure_S_2k_j2c_pt, Silence, 5.1* |

## A.4.65. Pixel Structure Pattern E 2k

| |
|---|

| | |
|---|---|
| **Type** | CPL |
| **Filename** | pixel_structure_E_2k_pt.cpl.xml |
| **Description** | East-oriented pixel structure test pattern featuring 16 x 16 and 8 x 8 pixel patterns with binary position indicators. See Section 7.5.3: Projector Pixel Count/Structure for description. |
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *pixel_structure_E_2k_j2c_pt*, *Silence*, *5.1* |

## A.4.66. Pixel Structure Pattern W 2k

| | |
|---|---|
| **Type** | CPL |
| **Filename** | pixel_structure_W_2k_pt.cpl.xml |
| **Description** | West-oriented pixel structure test pattern featuring 16 x 16 and 8 x 8 pixel patterns with binary position indicators. See Section 7.5.3: Projector Pixel Count/Structure for description. |
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *pixel_structure_W_2k_j2c_pt*, *Silence*, *5.1* |

## A.4.67. Pixel Structure Pattern N 4k

| | |
|---|---|
| **Type** | CPL |
| **Filename** | pixel_structure_N_4k_pt.cpl.xml |
| **Description** | North-oriented pixel structure test pattern featuring 16 x 16 pixel patterns with binary position indicators. See Section 7.5.3: Projector Pixel Count/Structure for description. |
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *pixel_structure_N_4k_j2c_pt*, *Silence*, *5.1* |

## A.4.68. Pixel Structure Pattern S 4k

| | |
|---|---|
| **Type** | CPL |
| **Filename** | pixel_structure_S_4k_pt.cpl.xml |
| **Description** | South-oriented pixel structure test pattern featuring 16 x 16 pixel patterns with binary position indicators. See Section 7.5.3: Projector Pixel Count/Structure for description. |

| | |
|---|---|
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *pixel_structure_S_4k_j2c_pt*, *Silence, 5.1* |

## A.4.69. Pixel Structure Pattern E 4k

| | |
|---|---|
| **Type** | CPL |
| **Filename** | pixel_structure_E_4k_pt.cpl.xml |
| **Description** | East-oriented pixel structure test pattern featuring 16 x 16 pixel patterns with binary position indicators. See Section 7.5.3: Projector Pixel Count/Structure for description. |
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *pixel_structure_E_4k_j2c_pt*, *Silence, 5.1* |

## A.4.70. Pixel Structure Pattern W 4k

| | |
|---|---|
| **Type** | CPL |
| **Filename** | pixel_structure_W_4k_pt.cpl.xml |
| **Description** | West-oriented pixel structure test pattern featuring 16 x 16 pixel patterns with binary position indicators. See Section 7.5.3: Projector Pixel Count/Structure for description. |
| **Conforms to** | SMPTE-429-7, SMPTE-431-1 |
| **Prerequisites** | *pixel_structure_W_4k_j2c_pt*, *Silence, 5.1* |

## A.4.71. DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m01_pict_frame_oo_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *m01 Picture Frame Out Of Order (Encrypted)*, *400 hz sine wave* |

## A.4.72. DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m02_snd_frame_oo_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, m02 Sound Frame Out Of Order (Encrypted)* |

## A.4.73. DCI Malformed Test 3: Sound Splice Tests

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m03_snd_splc_test.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *m03 Sound Splice, 400 hz sine wave* |

## A.4.74. DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m04_sndtk_wrong_file_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, m04 Sound Track File With Wrong TrackFile ID (Encrypted)* |

## A.4.75. DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m05_pict_wrong_file_ct.cpl.xml |

| | |
|---|---|
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *m05 Picture Track File With Wrong TrackFile ID (Encrypted), 400 hz sine wave* |

## A.4.76. DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m06_cpl_hash_error_ct.cpl.xml |
| **Description** | The contents of Asset Hash elements are replaced with random values. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted), StEM 5.1 Sound (Encrypted)* |
| **Meta** | **Signature** no |

## A.4.77. DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m07_cpl_invalid_signature_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted), StEM 5.1 Sound (Encrypted)* |
| **Malformations** | The contents of dsig:DigestValue are replaced with a random value. |

## A.4.78. DCI Malformed Test 8: DCP with timed text and a missing font

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m08_dcp_timetext_missing_font_pt.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *subtitle background, Silence, 5.1, Timed Text Example with Missing Font* |

## A.4.79. DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m09_pict_bad_hmac_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *m09 Picture track file with bad HMAC (Encrypted), 400 hz sine wave* |

## A.4.80. DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m10_snd_bad_hmac_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, m10 Sound track file with bad HMAC (Encrypted)* |

## A.4.81. DCI Malformed Test 11: Picture with Check Value error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m11_pict_bad_chuk_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *m11 Picture With Bad Check Value (Encrypted), 400 hz sine wave* |

## A.4.82. DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | CPL |

| | |
|---|---|
| **Filename** | m12_snd_bad_chuk_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *"NIST" 2K Test Pattern, m12 Sound Track File With Bad Check Value (Encrypted)* |

## A.4.83. DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m13_cpl_missing_asset_ct.cpl.xml |
| **Description** | The MainSound asset of this composition is an reference to a non-existent track file. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count (Encrypted)* |
| **Malformations** | The Id element of the MainSound shall be a random value. |
| **Meta** | **Signature** no |

## A.4.84. DCI Malformed Test 14: CPL that does not conform to ST 429-7 (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m14_cpl_format_error_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count (Encrypted), Sync Count 5.1 (Encrypted)* |
| **Malformations** | Create valid CPL using an ad-hoc namespace name. |
| **Meta** | **Signature** no |

## A.4.85. DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted)

| | |
|---|---|
| **Type** | CPL |

| | |
|---|---|
| **Filename** | m15_cpl_signer_format_error_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count (Encrypted), Sync Count 5.1 (Encrypted)* |
| **Malformations** | Create valid CPL signature using a SHA-1 certificate chain. |
| **Meta** | **Signature** no |

## A.4.86. DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m16_cpl_malf_signer_no_role_ct.cpl.xml |
| **Description** | A composition consisting of the encrypted StEM 2K image and encrypted 5.1 sound track files, signed with a certificate that has no role. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted), StEM 5.1 Sound (Encrypted)* |
| **Malformations** | The signer certificate of the CPL has no role instead of CS. |
| **Meta** | **Register** no<br>**Signature** no |

## A.4.87. DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m17_cpl_malf_signer_bad_role_ct.cpl.xml |
| **Description** | An encrypted composition consisting of the encrypted StEM 2K image and encrypted 5.1 sound track files, signed with a certificate with an incorrect role. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted), StEM 5.1 Sound (Encrypted)* |
| **Malformations** | The signer certificate of the CPL has the role of SM instead of CS. |
| **Meta** | **Register** no<br>**Signature** no |

## A.4.88. DCI Malformed Test 18: CPL signed with Extra Role Certificate (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m18_cpl_malf_signer_extra_role_ct.cpl.xml |
| **Description** | An encrypted composition consisting of the encrypted StEM 2K image and encrypted 5.1 sound track files, signed with a certificate with an extra role. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *StEM 2K (Encrypted), StEM 5.1 Sound (Encrypted)* |
| **Malformations** | The signer certificate of the CPL has the roles of CS and SM instead of only CS. |
| **Meta** | **Register** no<br>**Signature** no |

## A.4.89. Deleted Section

The section "DCI DCP 2K (Encrypted)" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.4.90. DCI DCP 2K Multi-Reel 128 A (Encrypted)

| | |
|---|---|
| **Type** | DCP |
| **Filename** | DCI_2K_128_multi_a_tests |
| **Description** | DCP containing 128 reel StEM, 5 seconds per reel, set A |
| **Conforms to** | SMPTE-429-8, SMPTE-429-9 |
| **Prerequisites** | *128 Reel Composition, "A" Series (Encrypted)* |

## A.4.91. DCI DCP 2K Multi-Reel 128 B (Encrypted)

| | |
|---|---|
| **Type** | DCP |

| | |
|---|---|
| **Filename** | DCI_2K_128_multi_b_tests |
| **Description** | DCP containing 128 reel StEM, 5 seconds per reel, set B |
| **Conforms to** | SMPTE-429-8, SMPTE-429-9 |
| **Prerequisites** | *128 Reel Composition, "B" Series (Encrypted)* |

## A.4.92. DCI DCP 2K Multi-Reel 64 (Encrypted)

| | |
|---|---|
| **Type** | DCP |
| **Filename** | DCI_2K_64_multi_tests |
| **Description** | DCP containing 64 reel StEM, 1 second per reel |
| **Conforms to** | SMPTE-429-8, SMPTE-429-9 |
| **Prerequisites** | *64 Reel Composition, 1 Second Reels (Encrypted)* |

## A.4.93. DCI DCP 2K, Malformed (Encrypted)

| | |
|---|---|
| **Type** | DCP |
| **Filename** | DCI_2K_malf |
| **Description** | DCP containing malformed test compositions |
| **Conforms to** | SMPTE-429-8, SMPTE-429-9 |
| **Prerequisites** | *DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted), DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted), DCI Malformed Test 3: Sound Splice Tests, DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted), DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted), DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted), DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted), DCI Malformed Test 8: DCP with timed text and a missing font, DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted), DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted), DCI Malformed Test 11: Picture with Check Value error in MXF Track File (Encrypted), DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted), DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted), DCI Malformed Test 14: CPL that does not conform to ST 429-7 (Encrypted), DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted), DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted), DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted), DCI Malformed Test 18: CPL signed with Extra Role Certificate (Encrypted)* |
| **Malformations** | None |
| **Meta** | **yes** ExplicitPKLContents |

## A.4.94. DCI DCP 4K (Encrypted)

| | |
|---|---|
| **Type** | DCP |
| **Filename** | DCI_4K_tests |
| **Description** | DCP containing well-formed 4K test compositions |
| **Conforms to** | SMPTE-429-8, SMPTE-429-9 |
| **Prerequisites** | *4K Color Accuracy Series*, *4K DCI Maximum Bitrate Composition (Encrypted)*, *4K DCI NIST Frame with silence*, *4K Sync Test*, *Pixel Structure Pattern E 4k*, *Pixel Structure Pattern N 4k*, *Pixel Structure Pattern S 4k*, *Pixel Structure Pattern W 4k*, *4K Scope Subtitle Test (Encrypted)*, *4K Flat Subtitle Test (Encrypted)*, *4K Full Subtitle Test (Encrypted)* |

## A.4.95. 2K Scope Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_2K_scope_ct.cpl.xml |
| **Description** | 2K Scope Subtitle Test (Encrypted) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |
| **Prerequisites** | *Silence*, *5.1 (Encrypted)*, *2K Scope Subtitle Test Background - Reel 1*, *2K Scope Subtitle Test - Timed Text track file - Reel 1*, *2K Scope Subtitle Test Background - Reel 2*, *2K Scope Subtitle Test - Timed Text track file - Reel 2*, *2K Scope Subtitle Test Background - Reel 3*, *2K Scope Subtitle Test - Timed Text track file - Reel 3*, *2K Scope Subtitle Test Background - Reel 4*, *2K Scope Subtitle Test - Timed Text track file - Reel 4*, *2K Scope Subtitle Test Background - Reel 5*, *2K Scope Subtitle Test - Timed Text track file - Reel 5*, *2K Scope Subtitle Test Background - Reel 6*, *2K Scope Subtitle Test - Timed Text track file - Reel 6*, *2K Scope Subtitle Test Background - Reel 7*, *2K Scope Subtitle Test - Timed Text track file - Reel 7*, *2K Scope Subtitle Test Background - Reel 8*, *2K Scope Subtitle Test - Timed Text track file - Reel 8*, *2K Scope Subtitle Test Background - Reel 9*, *2K Scope Subtitle Test - Timed Text track file - Reel 9*, *2K Scope Subtitle Test Background - Reel 10*, *2K Scope Subtitle Test - Timed Text track file - Reel 10* |

## A.4.96. 2K Flat Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_2K_flat_ct.cpl.xml |
| **Description** | 2K Flat Subtitle Test (Encrypted) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |

| | |
|---|---|
| **Prerequisites** | *Silence, 5.1 (Encrypted), 2K Flat Subtitle Test Background - Reel 1, 2K Flat Subtitle Test - Timed Text track file - Reel 1, 2K Flat Subtitle Test Background - Reel 2, 2K Flat Subtitle Test - Timed Text track file - Reel 2, 2K Flat Subtitle Test Background - Reel 3, 2K Flat Subtitle Test - Timed Text track file - Reel 3, 2K Flat Subtitle Test Background - Reel 4, 2K Flat Subtitle Test - Timed Text track file - Reel 4, 2K Flat Subtitle Test Background - Reel 5, 2K Flat Subtitle Test - Timed Text track file - Reel 5, 2K Flat Subtitle Test Background - Reel 6, 2K Flat Subtitle Test - Timed Text track file - Reel 6, 2K Flat Subtitle Test Background - Reel 7, 2K Flat Subtitle Test - Timed Text track file - Reel 7, 2K Flat Subtitle Test Background - Reel 8, 2K Flat Subtitle Test - Timed Text track file - Reel 8, 2K Flat Subtitle Test Background - Reel 9, 2K Flat Subtitle Test - Timed Text track file - Reel 9, 2K Flat Subtitle Test Background - Reel 10, 2K Flat Subtitle Test - Timed Text track file - Reel 10* |

## A.4.97. 2K Full Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_2K_full_ct.cpl.xml |
| **Description** | 2K Full Subtitle Test (Encrypted) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |
| **Prerequisites** | *Silence, 5.1 (Encrypted), 2K Full Subtitle Test Background - Reel 1, 2K Full Subtitle Test - Timed Text track file - Reel 1, 2K Full Subtitle Test Background - Reel 2, 2K Full Subtitle Test - Timed Text track file - Reel 2, 2K Full Subtitle Test Background - Reel 3, 2K Full Subtitle Test - Timed Text track file - Reel 3, 2K Full Subtitle Test Background - Reel 4, 2K Full Subtitle Test - Timed Text track file - Reel 4, 2K Full Subtitle Test Background - Reel 5, 2K Full Subtitle Test - Timed Text track file - Reel 5, 2K Full Subtitle Test Background - Reel 6, 2K Full Subtitle Test - Timed Text track file - Reel 6, 2K Full Subtitle Test Background - Reel 7, 2K Full Subtitle Test - Timed Text track file - Reel 7, 2K Full Subtitle Test Background - Reel 8, 2K Full Subtitle Test - Timed Text track file - Reel 8, 2K Full Subtitle Test Background - Reel 9, 2K Full Subtitle Test - Timed Text track file - Reel 9, 2K Full Subtitle Test Background - Reel 10, 2K Full Subtitle Test - Timed Text track file - Reel 10* |

## A.4.98. 4K Scope Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_4K_scope_ct.cpl.xml |
| **Description** | 4K Scope Subtitle Test (Encrypted) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |
| **Prerequisites** | *Silence, 5.1 (Encrypted), 4K Scope Subtitle Test Background - Reel 1, 2K Scope Subtitle Test - Timed Text track file - Reel 1, 4K Scope Subtitle Test Background - Reel 2, 2K Scope Subtitle Test - Timed Text track file - Reel 2, 4K Scope Subtitle Test Background - Reel 3, 2K Scope Subtitle Test - Timed Text track file - Reel 3, 4K Scope Subtitle Test Background - Reel 4, 2K Scope Subtitle Test - Timed Text track file - Reel 4, 4K Scope Subtitle Test Background - Reel 5, 2K Scope Subtitle Test - Timed Text track file - Reel 5, 4K Scope Subtitle Test Background - Reel 6, 2K Scope Subtitle Test - Timed Text track file - Reel 6, 4K Scope Subtitle Test Background - Reel 7, 2K Scope Subtitle Test - Timed Text track file - Reel 7, 4K Scope Subtitle Test Background - Reel 8, 4K Scope Subtitle Test - Timed Text track file - Reel 8, 4K Scope Subtitle Test* |

| | |
|---|---|
| | *Background - Reel 9, 4K Scope Subtitle Test - Timed Text track file - Reel 9, 4K Scope Subtitle Test Background - Reel 10, 2k Scope Subtitle Test - Timed Text track file - Reel 10* |

## A.4.99. 4K Flat Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_4K_flat_ct.cpl.xml |
| **Description** | 4K Flat Subtitle Test (Encrypted) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |
| **Prerequisites** | *Silence, 5.1 (Encrypted), 4K Flat Subtitle Test Background - Reel 1, 2K Flat Subtitle Test - Timed Text track file - Reel 1, 4K Flat Subtitle Test Background - Reel 2, 2K Flat Subtitle Test - Timed Text track file - Reel 2, 4K Flat Subtitle Test Background - Reel 3, 2K Flat Subtitle Test - Timed Text track file - Reel 3, 4K Flat Subtitle Test Background - Reel 4, 2K Flat Subtitle Test - Timed Text track file - Reel 4, 4K Flat Subtitle Test Background - Reel 5, 2K Flat Subtitle Test - Timed Text track file - Reel 5, 4K Flat Subtitle Test Background - Reel 6, 2K Flat Subtitle Test - Timed Text track file - Reel 6, 4K Flat Subtitle Test Background - Reel 7, 2K Flat Subtitle Test - Timed Text track file - Reel 7, 4K Flat Subtitle Test Background - Reel 8, 4K Flat Subtitle Test - Timed Text track file - Reel 8, 4K Flat Subtitle Test Background - Reel 9, 4K Flat Subtitle Test - Timed Text track file - Reel 9, 4K Flat Subtitle Test Background - Reel 10, 2K Flat Subtitle Test - Timed Text track file - Reel 10* |

## A.4.100. 4K Full Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_4K_full_ct.cpl.xml |
| **Description** | 4K Full Subtitle Test (Encrypted) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |
| **Prerequisites** | *Silence, 5.1 (Encrypted), 4K Full Subtitle Test Background - Reel 1, 2K Full Subtitle Test - Timed Text track file - Reel 1, 4K Full Subtitle Test Background - Reel 2, 2K Full Subtitle Test - Timed Text track file - Reel 2, 4K Full Subtitle Test Background - Reel 3, 2K Full Subtitle Test - Timed Text track file - Reel 3, 4K Full Subtitle Test Background - Reel 4, 2K Full Subtitle Test - Timed Text track file - Reel 4, 4K Full Subtitle Test Background - Reel 5, 2K Full Subtitle Test - Timed Text track file - Reel 5, 4K Full Subtitle Test Background - Reel 6, 2K Full Subtitle Test - Timed Text track file - Reel 6, 4K Full Subtitle Test Background - Reel 7, 2K Full Subtitle Test - Timed Text track file - Reel 7, 4K Full Subtitle Test Background - Reel 8, 4K Full Subtitle Test - Timed Text track file - Reel 8, 4K Full Subtitle Test Background - Reel 9, 4K Full Subtitle Test - Timed Text track file - Reel 9, 4K Full Subtitle Test Background - Reel 10, 2K Full Subtitle Test - Timed Text track file - Reel 10* |

## A.4.101. 2K 48fps Scope Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_48fps_scope_ct.cpl.xml |
| **Description** | 2K 48fps Scope Subtitle Test (Encrypted) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |
| **Prerequisites** | *Silence, 5.1, 48 fps (Encrypted), 2K 48fps Scope Subtitle Test Background - Reel 1, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 1, 2K 48fps Scope Subtitle Test Background - Reel 2, 48fps Scope Subtitle Test - Timed Text track file - Reel 2, 2K 48fps Scope Subtitle Test Background - Reel 3, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 3, 2K 48fps Scope Subtitle Test Background - Reel 4, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 4, 2K 48fps Scope Subtitle Test Background - Reel 5, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 5, 2K 48fps Scope Subtitle Test Background - Reel 6, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 6, 2K 48fps Scope Subtitle Test Background - Reel 7, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 7, 2K 48fps Scope Subtitle Test Background - Reel 8, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 8, 2K 48fps Scope Subtitle Test Background - Reel 9, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 9, 2K 48fps Scope Subtitle Test Background - Reel 10, 2K 48fps Scope Subtitle Test - Timed Text track file - Reel 10* |

## A.4.102. 2K 48fps Flat Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_48fps_flat_ct.cpl.xml |
| **Description** | 2K 48fps Flat Subtitle Test (Encrypted) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |
| **Prerequisites** | *Silence, 5.1, 48 fps (Encrypted), 2K 48fps Flat Subtitle Test Background - Reel 1, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 1, 2K 48fps Flat Subtitle Test Background - Reel 2, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 2, 2K 48fps Flat Subtitle Test Background - Reel 3, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 3, 2K 48fps Flat Subtitle Test Background - Reel 4, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 4, 2K 48fps Flat Subtitle Test Background - Reel 5, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 5, 2K 48fps Flat Subtitle Test Background - Reel 6, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 6, 2K 48fps Flat Subtitle Test Background - Reel 7, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 7, 2K 48fps Flat Subtitle Test Background - Reel 8, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 8, 2K 48fps Flat Subtitle Test Background - Reel 9, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 9, 2K 48fps Flat Subtitle Test Background - Reel 10, 2K 48fps Flat Subtitle Test - Timed Text track file - Reel 10* |

## A.4.103. 2K 48fps Full Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | sub_test_48fps_full_ct.cpl.xml |
| **Description** | 2K 48fps Full Subtitle Test (Encrypted) |
| | |

| | |
|---|---|
| **Conforms to** | SMPTE-429-7, SMPTE-429-2 |
| **Prerequisites** | *Silence, 5.1, 48 fps (Encrypted), 2K 48fps Full Subtitle Test Background - Reel 1, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 1, 2K 48fps Full Subtitle Test Background - Reel 2, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 2, 2K 48fps Full Subtitle Test Background - Reel 3, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 3, 2K 48fps Full Subtitle Test Background - Reel 4, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 4, 2K 48fps Full Subtitle Test Background - Reel 5, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 5, 2K 48fps Full Subtitle Test Background - Reel 6, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 6, 2K 48fps Full Subtitle Test Background - Reel 7, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 7, 2K 48fps Full Subtitle Test Background - Reel 8, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 8, 2K 48fps Full Subtitle Test Background - Reel 9, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 9, 2K 48fps Full Subtitle Test Background - Reel 10, 2K 48fps Full Subtitle Test - Timed Text track file - Reel 10* |

## A.4.104. DCI DCP 2K Multi-Reel 128 A (Unencrypted)

| | |
|---|---|
| **Type** | DCP |
| **Filename** | DCI_2K_128_multi_a_tests_pt |
| **Description** | DCP containing 128 reel StEM, 5 seconds per reel, set A, Unencrypted |
| **Conforms to** | SMPTE-429-8, SMPTE-429-9 |
| **Prerequisites** | *128 Reel Composition, "A" Series* |
| **Malformations** | None |

## A.4.105. DCI DCP 2K Multi-Reel 128 B (Unencrypted)

| | |
|---|---|
| **Type** | DCP |
| **Filename** | DCI_2K_128_multi_b_tests_pt |
| **Description** | DCP containing 128 reel StEM, 5 seconds per reel, set B, Unencrypted |
| **Conforms to** | SMPTE-429-8, SMPTE-429-9 |
| **Prerequisites** | *128 Reel Composition, "B" Series* |

## A.4.106. DCI 2K Sync Test (OBAE)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test_obae.cpl.xml |

| | |
|---|---|
| **Description** | A Composition that contains an Immersive Audio Track, as specified in SMPTE ST 429-18. It is intended to facilitate test procedures where timing measurements are performed. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-19 |
| **Prerequisites** | *Sync Count*, *Main Sound for Sync Count OBAE*, *Sync Count OBAE* |

## A.4.107. DCI 2K Sync Test (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test_obae_ct.cpl.xml |
| **Description** | Encrypted version of Section A.4.106: DCI 2K Sync Test (OBAE) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *Sync Count OBAE (Encrypted)* |

## A.4.108. DCI 2K StEM (OBAE)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_obae_pt.cpl.xml |
| **Description** | A plaintext composition consisting of the StEM 2K image and an Immersive Audio Track, as specified in SMPTE ST 429-18. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K*, *Main Sound for StEM OBAE*, *StEM OBAE* |

## A.4.109. DCI 2K StEM (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_obae_ct.cpl.xml |
| **Description** | Encrypted version of Section A.4.108: DCI 2K StEM (OBAE) |
| **Conforms to** | SMPTE-429-7, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K (Encrypted)*, *Main Sound for StEM OBAE (Encrypted)*, *StEM OBAE (Encrypted)* |

## A.4.110. DCI 2K Sync Test with subtitles (OBAE)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test_with_subs_obae.cpl.xml |
| **Description** | A Composition that contains an Immersive Audio and Subtitle Tracks. It is intended to facilitate test procedures where timing measurements are performed. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *Sync Count with Subtitle Reticles*, *Main Sound for Sync Count OBAE*, *Sync Count OBAE*, *Sync Count Text* |

## A.4.111. DCI 2K Sync Test with subtitles (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test_with_subs_obae_ct.cpl.xml |
| **Description** | Encrypted version of *DCI 2K Sync Test with subtitles (OBAE)* |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *Sync Count with Subtitle Reticles (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *Sync Count OBAE (Encrypted)*, *Sync Count Text (Encrypted)* |

## A.4.112. M25 Composition with Malformed Integrity Pack: Missing MIC item (Picture) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m25_integrity_pict_mic_ct.cpl.xml |
| **Description** | Composition where a MIC item is missing from the Main Picture Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16 |
| **Prerequisites** | *M25 Picture Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)*, *Main Sound for StEM OBAE (Encrypted)* |
| **Malformations** | A MIC item is missing from the Main Picture Track File |

## A.4.113. M27 Composition with Malformed Integrity Pack: Missing TrackFileID item (Picture) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m27_integrity_pict_tfid_ct.cpl.xml |
| **Description** | Composition where a TrackFileID item is missing from the Main Picture Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16 |
| **Prerequisites** | *M27 Picture Track File with Malformed Integrity Pack: Missing TrackFileID item (Encrypted)*, *Main Sound for StEM OBAE (Encrypted)* |
| **Malformations** | A TrackFileID item is missing from the Main Picture Track File |

## A.4.114. M26 Composition with Malformed Integrity Pack: Missing SequenceNumber item (Picture) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m26_integrity_pict_snum_ct.cpl.xml |
| **Description** | Composition where a SequenceNumber item is missing from the Main Picture Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16 |
| **Prerequisites** | *M26 Picture Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)*, *Sync Count 5.1 (Encrypted)* |
| **Malformations** | A SequenceNumber item is missing from the Main Picture Track File |

## A.4.115. M28 Composition with Malformed Integrity Pack: Missing MIC item (PCM) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m28_integrity_snd_mic_ct.cpl.xml |
| **Description** | Composition where a MIC item is missing from the Main Sound Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16 |
| **Prerequisites** | *M28 Sound Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)*, *Sync Count* |

| | |
|---|---|
| | *(Encrypted)* |
| **Malformations** | A MIC item is missing from the Main Sound Track File |

## A.4.116. M30 Composition with Malformed Integrity Pack: Missing TrackFileID item (PCM) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m30_integrity_snd_tfid_ct.cpl.xml |
| **Description** | Composition where a TrackFileID item is missing from the Main Sound Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16 |
| **Prerequisites** | *M30 Sound Track File with Malformed Integrity Pack: Missing TrackFileID item (Encrypted)*, *Sync Count (Encrypted)* |
| **Malformations** | A TrackFileID item is missing from the Main Sound Track File |

## A.4.117. M29 Composition with Malformed Integrity Pack: Missing SequenceNumber item (PCM) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m29_integrity_snd_snum_ct.cpl.xml |
| **Description** | Composition where a SequenceNumber item is missing from the Main Sound Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16 |
| **Prerequisites** | *M29 Sound Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)*, *Sync Count (Encrypted)* |
| **Malformations** | A SequenceNumber item is missing from the Main Sound Track File |

## A.4.118. M20 Composition with Malformed Integrity Pack: Missing MIC item (OBAE Main Sound) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m20_integrity_obae_ms_mic_ct.cpl.xml |
| **Description** | OBAE Composition where a MIC item is missing from the Main Sound Track File |

| | |
|---|---|
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *M20 Sound Track File with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted), Sync Count (Encrypted), Sync Count OBAE (Encrypted)* |
| **Malformations** | A MIC item is missing from the Main Sound Track File |

## A.4.119. M22 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE Main Sound) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m22_integrity_obae_ms_tfid_ct.cpl.xml |
| **Description** | OBAE Composition where a TrackFileID item is missing from the Main Sound Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *M22 Sound Track File with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted), Sync Count (Encrypted), Sync Count OBAE (Encrypted)* |
| **Malformations** | A TrackFileID item is missing from the Main Sound Track File |

## A.4.120. M21 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE Main Sound) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m21_integrity_obae_ms_snum_ct.cpl.xml |
| **Description** | OBAE Composition where a SequenceNumber item is missing from the Main Sound Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *M21 Sound Track File with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted), Sync Count (Encrypted), Sync Count OBAE (Encrypted)* |
| **Malformations** | A SequenceNumber item is missing from the Main Sound Track File |

## A.4.121. M19 Composition with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |

| | |
|---|---|
| **Filename** | m19_integrity_obae_mic_ct.cpl.xml |
| **Description** | OBAE Composition where a MIC item is missing from the OBAE Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *M19 OBAE Track File with Malformed Integrity Pack: Missing MIC item (Encrypted), Sync Count (Encrypted), Main Sound for Sync Count OBAE (Encrypted)* |
| **Malformations** | A MIC item is missing from the OBAE Track File |

## A.4.122. M24 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m24_integrity_obae_tfid_ct.cpl.xml |
| **Description** | OBAE Composition where a TrackFileID item is missing from the OBAE Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *M24 OBAE Track File with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted), Sync Count (Encrypted), Main Sound for Sync Count OBAE (Encrypted)* |
| **Malformations** | A TrackFileID item is missing from the OBAE Track File |

## A.4.123. M23 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m23_integrity_obae_snum_ct.cpl.xml |
| **Description** | OBAE Composition where a SequenceNumber item is missing from the OBAE Track File |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *M23 OBAE Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted), Sync Count (Encrypted), Main Sound for Sync Count OBAE (Encrypted)* |
| **Malformations** | A SequenceNumber item is missing from the OBAE Track File |

## A.4.124. 64 Reel Composition, 1 Second Reels (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_64_1_second_reels_obae_ct.cpl.xml |
| **Description** | An encrypted OBAE composition consisting of sixty four (64) reels, each with a duration of 1 second. Each reel is composed of part of the encrypted StEM 2K image and encrypted OBAE track files. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K Multi-Reel C (Encrypted)*, *StEM OBAE Multi-Reel C (Encrypted)*, *Main Sound for StEM OBAE Multi-Reel C (Encrypted)* |

## A.4.125. M40 OBAE DCP with Frame-out-of-order error (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m40_obae_frame_oo_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *M40 OBAE Track File with Frame-out-of-order error (Encrypted)* |

## A.4.126. M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m41_obae_wrong_file_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *M41 OBAE Track File With Wrong TrackFile ID (Encrypted)* |

## A.4.127. DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test_obae_mkey_ct.cpl.xml |
| **Description** | Same as A.4.107. DCI 2K Sync Test (OBAE) (Encrypted) but with the OBAE Track File using a KDM-borne MIC Key. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| | |

| | |
|---|---|
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *Sync Count OBAE with MIC Key (Encrypted)* |

## A.4.128. M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m43_obae_bad_chuk_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *M43 OBAE Track File With Bad Check Value (Encrypted)* |

## A.4.129. End of Engagement - Past Time Window Extension (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | holdover_long_obae_ct.cpl.xml |
| **Description** | An encrypted OBAE composition with duration of 6 hours and 11 minutes. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K (Encrypted)*, *Main Sound for StEM OBAE (Encrypted)*, *StEM OBAE (Encrypted)* |

## A.4.130. End of Engagement - Within Time Window Extension (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | holdover_short_obae_ct.cpl.xml |
| **Description** | An encrypted OBAE composition with duration of 5 hours and 59 minutes and 30 seconds. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K (Encrypted)*, *Main Sound for StEM OBAE (Encrypted)*, *StEM OBAE (Encrypted)* |

## A.4.131. DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test_mkey_ct.cpl.xml |
| **Description** | Same as A.4.3. DCI 2K Sync Test (Encrypted) but with KDM-borne MIC Keys. |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count 5.1 with KDM-Borne MIC Key (Encrypted)*, *Sync Count with KDM-Borne MIC Key (Encrypted)* |

## A.4.132. M44 OBAE DCP with HMAC value error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m44_obae_bad_hmac_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *M44 OBAE Track File With Bad HMAC Value (Encrypted)* |

## A.4.133. DCP for OBAE Tone Multi-Reel (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | OBAE_tone_multi_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *OBAE Tone Multi-Reel (Encrypted)*, *Main Sound for OBAE Tone Multi-Reel (Encrypted)* |

## A.4.134. DCP for Audio Tone Multi-Reel (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| | |

| | |
|---|---|
| **Filename** | audio_tone_multi_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Audio Tone Multi-Reel (Encrypted)* |

## A.4.135. DCI 2K Sync Test (48fps) (OBAE)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_sync_test_48fps_obae.cpl.xml |
| **Description** | A 48 fps Composition that contains an Immersive Audio Track, as specified in SMPTE ST 429-18. It is intended to facilitate test procedures where timing measurements are performed. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-19 |
| **Prerequisites** | *Sync Count*, *48fps*, *Main Sound for Sync Count OBAE (48fps)*, *Sync Count OBAE (48fps)* |

## A.4.136. 2K FM Application Constraints (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_constraints_obae_ct.cpl.xml |
| **Description** | A composition consisting of FM testing instructions and both encrypted and plaintext StEM 2K image and OABE track files. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *FM Constraints Begin (Plaintext)*, *FM Constraints Begin (Encrypted)*, *FM Constraints End (Plaintext)*, *FM Constraints End (Encrypted)*, *400 hz sine wave (OBAE)*, *400 hz sine wave (OBAE) (Encrypted)*, *Main Sound for 400 hz sine wave (OBAE)*, *StEM 2K (Encrypted)*, *StEM 2K*, *FM StEM OBAE*, *FM StEM OBAE (Encrypted)*, *Main Sound for FM StEM OBAE* |

## A.4.137. 2K FM Control Granularity - No FM (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_control_granularity_no_fm_obae.cpl.xml |
| **Description** | An encrypted composition containing image and OBAE essence, for the purpose of detecting the forensic marking application. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |

| | |
|---|---|
| **Prerequisites** | *2K FM Control Granularity Begin (Encrypted), 2K FM Control Granularity End (Encrypted), 400 hz sine wave (OBAE) (Encrypted), Main Sound for 400 hz sine wave (OBAE), StEM 2K (Encrypted), FM StEM OBAE (Encrypted), Main Sound for FM StEM OBAE* |

## A.4.138. 2K FM Control Granularity - Image Only FM (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_control_granularity_image_only_fm_obae.cpl.xml |
| **Description** | An encrypted composition containing image and OBAE essence, for the purpose of detecting the forensic marking application. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *2K FM Control Granularity Begin (Encrypted), 2K FM Control Granularity End (Encrypted), 400 hz sine wave (OBAE) (Encrypted), Main Sound for 400 hz sine wave (OBAE), StEM 2K (Encrypted), FM StEM OBAE (Encrypted), Main Sound for FM StEM OBAE* |

## A.4.139. 2K FM Control Granularity - OBAE Only FM (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_control_granularity_obae_only_fm_obae.cpl.xml |
| **Description** | An encrypted composition containing image and OBAE essence, for the purpose of detecting the forensic marking application. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *2K FM Control Granularity Begin (Encrypted), 2K FM Control Granularity End (Encrypted), 400 hz sine wave (OBAE) (Encrypted), Main Sound for 400 hz sine wave (OBAE), StEM 2K (Encrypted), FM StEM OBAE (Encrypted), Main Sound for FM StEM OBAE* |

## A.4.140. 2K FM Control Granularity - Image and OBAE FM (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_control_granularity_image_and_obae_fm_obae.cpl.xml |
| | |

| | |
|---|---|
| **Description** | An encrypted composition containing image and OBAE essence, for the purpose of detecting the forensic marking application. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *2K FM Control Granularity Begin (Encrypted)*, *2K FM Control Granularity End (Encrypted)*, *400 hz sine wave (OBAE) (Encrypted)*, *Main Sound for 400 hz sine wave (OBAE)*, *StEM 2K (Encrypted)*, *FM StEM OBAE (Encrypted)*, *Main Sound for FM StEM OBAE* |

## A.4.141. 128 Reel Composition, "A" Series (OBAE)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_128_a_reels_obae_pt.cpl.xml |
| **Description** | A plaintext composition consisting of one hundred and twenty eight (128) reels, where no two reels reference identical main picture, main sound or OBAE track files. The main picture, main sound and OBAE tracks are based on those of Section A.4.108: DCI 2K StEM (OBAE). |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K Multi-Reel A*, *StEM OBAE Multi-Reel A*, *Main Sound for StEM OBAE Multi-Reel A* |

## A.4.142. 128 Reel Composition, "B" Series (OBAE)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_128_b_reels_obae_pt.cpl.xml |
| **Description** | A plaintext composition consisting of one hundred and twenty eight (128) reels, where no two reels reference identical main picture, main sound or OBAE track files. The main picture, main sound and OBAE tracks are based on those of Section A.4.108: DCI 2K StEM (OBAE). |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K Multi-Reel B*, *StEM OBAE Multi-Reel B*, *Main Sound for StEM OBAE Multi-Reel B* |

## A.4.143. 128 Reel Composition, "A" Series (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_128_a_reels_obae_ct.cpl.xml |
| **Description** | Encypted version of A.4.141. 128 Reel Composition, "A" Series (OBAE) where 256 distinct cryptographic keys are used: 128 for the main picture track and 64 for each of the main sound and OBAE tracks. |

| | |
|---|---|
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K Multi-Reel A (Encrypted)*, *StEM OBAE Multi-Reel A (Encrypted)*, *Main Sound for StEM OBAE Multi-Reel A (Encrypted)* |

## A.4.144. 128 Reel Composition, "B" Series (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_StEM_128_b_reels_obae_ct.cpl.xml |
| **Description** | Encypted version of A.4.142. 128 Reel Composition, "B" Series (OBAE) where 256 distinct cryptographic keys are used: 128 for the main picture track and 64 for each of the main sound and OBAE tracks. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K Multi-Reel B (Encrypted)*, *StEM OBAE Multi-Reel B (Encrypted)*, *Main Sound for StEM OBAE Multi-Reel B (Encrypted)* |

## A.4.145. 2K FM Payload (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_payload_obae_ct.cpl.xml |
| **Description** | An encrypted composition for FM payload retrieval containing encrypted StEM 2K image and corresponding OBAE essence, preceded and followed by slates. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *2K FM Payload Begin (Encrypted)*, *2K FM Payload End (Encrypted)*, *400 hz sine wave (OBAE) (Encrypted)*, *Main Sound for 400 hz sine wave (OBAE)*, *StEM 2K (Encrypted)*, *Main Sound for FM StEM OBAE*, *FM StEM OBAE (Encrypted)* |

## A.4.146. 2K FM Payload (plaintext OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_fm_payload_pt_obae_ct.cpl.xml |
| **Description** | A version of A.4.145. 2K FM Payload (OBAE) (Encrypted) where the OBAE essence is plaintext. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *2K FM Payload Begin (Encrypted)*, *2K FM Payload End (Encrypted)*, *400 hz sine wave (OBAE)*, *Main Sound for 400 hz sine wave (OBAE)*, *StEM 2K (Encrypted)*, *Main Sound for FM StEM OBAE*, *FM StEM OBAE* |

## A.4.147. Maximum Bitrate OBAE (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | maximum_bitrate_24Hz_obae_ct.cpl.xml |
| **Description** | A encrypted composition intended to exercise the maximum OBAE bitrate at a frame rate of 24 Hz. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K*, *Maximum Bitrate OBAE 48 fps (Encrypted)*, *Main Sound for Maximum Bitrate OBAE 48 fps (Encrypted)* |

## A.4.148. Maximum Bitrate OBAE 48 fps (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | maximum_bitrate_48Hz_obae_ct.cpl.xml |
| **Description** | A encrypted composition intended to exercise the maximum OBAE bitrate at a frame rate of 48 Hz. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-19 |
| **Prerequisites** | *StEM 2K 48 fps*, *Maximum Bitrate OBAE (Encrypted)*, *Main Sound for Maximum Bitrate OBAE (Encrypted)* |

## A.4.149. OBAE Rendering Expectations

| | |
|---|---|
| **Type** | CPL |
| **Filename** | obae_rendering_test_pt.cpl.xml |
| **Description** | Composition intended to evaluate whether OBAE rendering expectations are met. Some reels contain neither a sync signal nor OBAE Track Files. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-18 |
| **Prerequisites** | *OBAE Rendering Expectations Guide*, *OBAE Rendering Test*, *Main Sound for OBAE Rendering Test*, *Silence w/ HI/VI* |

## A.4.150. DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m06b_cpl_hash_error_obae_ct.cpl.xml |
| **Description** | The contents of Asset Hash elements are replaced with random values. |
| **Conforms to** | SMPTE-429-19 |
| **Prerequisites** | *StEM 2K (Encrypted)*, *Main Sound for StEM OBAE (Encrypted)*, *StEM OBAE (Encrypted)* |
| **Malformations** | The contents of Asset Hash elements are replaced with random values. |

## A.4.151. DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m07b_cpl_invalid_signature_obae_ct.cpl.xml |
| **Conforms to** | SMPTE-429-19 |
| **Prerequisites** | *StEM 2K (Encrypted)*, *Main Sound for StEM OBAE (Encrypted)*, *StEM OBAE (Encrypted)* |
| **Malformations** | The contents of dsig:DigestValue are replaced with a random value. |

## A.4.152. DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m13b_cpl_missing_asset_obae_ct.cpl.xml |
| **Description** | The MainSound asset of this composition is an reference to a non-existent track file. |
| **Conforms to** | SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *Sync Count OBAE (Encrypted)* |
| **Malformations** | The Id element of the MainSound shall be a random value. |

## A.4.153. DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |

| | |
|---|---|
| **Filename** | m14b_cpl_format_error_obae_ct.cpl.xml |
| **Conforms to** | SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *Sync Count OBAE (Encrypted)* |
| **Malformations** | Create valid CPL using an ad-hoc namespace name. |

## A.4.154. DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m15b_cpl_signer_format_error_obae_ct.cpl.xml |
| **Conforms to** | SMPTE-429-19 |
| **Prerequisites** | *Sync Count (Encrypted)*, *Main Sound for Sync Count OBAE (Encrypted)*, *Sync Count OBAE (Encrypted)* |
| **Malformations** | Create valid CPL signature using a SHA-1 certificate chain. |

## A.4.155. DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m16b_cpl_malf_signer_no_role_obae_ct.cpl.xml |
| **Description** | A composition signed with a certificate that has no role. |
| **Conforms to** | SMPTE-429-19 |
| **Prerequisites** | *StEM 2K (Encrypted)*, *Main Sound for StEM OBAE (Encrypted)*, *StEM OBAE (Encrypted)* |
| **Malformations** | The signer certificate of the CPL has no role instead of CS. |

## A.4.156. DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m17b_cpl_malf_signer_bad_role_obae_ct.cpl.xml |
| **Description** | An encrypted composition signed with a certificate with an incorrect role. |

| | |
|---|---|
| **Conforms to** | SMPTE-429-19 |
| **Prerequisites** | *StEM 2K (Encrypted), Main Sound for StEM OBAE (Encrypted), StEM OBAE (Encrypted)* |
| **Malformations** | The signer certificate of the CPL has the role of SM instead of CS. |

## A.4.157. DCI Malformed Test 18b: CPL signed with Extra Role Certificate (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | m18b_cpl_malf_signer_extra_role_obae_ct.cpl.xml |
| **Description** | An encrypted composition signed with a certificate with an extra role. |
| **Conforms to** | SMPTE-429-19 |
| **Prerequisites** | *StEM 2K (Encrypted), Main Sound for StEM OBAE (Encrypted), StEM OBAE (Encrypted)* |
| **Malformations** | The signer certificate of the CPL has the roles of CS and SM instead of only CS. |

## A.4.158. OBAE Rendering Expectations (Clip)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | obae_rendering_test_clip_pt.cpl.xml |
| **Description** | First three reels of *OBAE Rendering Expectations* |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-18 |
| **Prerequisites** | *OBAE Rendering Expectations* |

## A.4.159. DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | frame_num_burn_in_obae_ct.cpl.xml |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-18 |
| **Prerequisites** | *DCI Numbered Frame Sequence (Encrypted), 400 hz sine wave (OBAE) (Encrypted), Main Sound for 400 hz sine wave (OBAE) (Encrypted)* |

### A.4.160. 2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | CPL |
| **Filename** | 2K_max_bitrate_obae_ct.cpl.xml |
| **Description** | Encrypted composition containing picture, sound and OBAE track files of the maximum allowable bitrate. |
| **Conforms to** | SMPTE-429-7, SMPTE-429-16, SMPTE-429-18 |
| **Prerequisites** | *2K Picture Track File*, *Maximum Bitrate*, *Maximum Bitrate OBAE (Encrypted)*, *Main Sound for Maximum Bitrate OBAE (Encrypted)* |

## A.5. Digital Certificates

Six certificate chains are defined, which separate certificates by device type and level of conformity. In the descriptions below, the IMB label refers to a certificate which contains roles for a Media Block (MB) or a certificate which signs such certificates. Similarly, PRJ refers to certificates or signers associated with a projector and KDS refers to certificates associated with a Key Distribution System (a KDM authoring entity).

- Chain A1 contains valid IMB certificates.
- Chain A2 contains valid IMB certificates but the chain has no intermediate signers.
- Chain A3 contains invalid IMB certificates.
- Chain B1 contains valid PRJ certificates.
- Chain C1 contains valid KDS certificates.
- Chain C3 contains invalid KDS certificates.

### A.5.1. Chain A1 IMB Certificate Files

Contents removed, not used by any procedure

### A.5.2. Chain A2 IMB Certificate Files

Contents removed, not used by any procedure

## A.5.3. Chain A3 IMB Certificate Files

### A.5.3.1. chain-a3-root

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-root.pem |
| **Description** | Root cert, malformed leaves |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-root-key* |

### A.5.3.2. chain-a3-signer1

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-osig-type.pem |
| **Description** | Intermediate Signer, level one |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-root*, *chain-a3-signer1-key* |

### A.5.3.3. chain-a3-osig-type

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-osig-type.pem |
| **Description** | Signature algorithm of outside signature not sha256WithRSAEncryption |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Signature algorithm of outside signature is sha1WithRSAEncryption |

### A.5.3.4. chain-a3-isig-type

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-isig-type.pem |
| **Description** | Signature algorithm inside signature not sha256WithRSAEncryption |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Signature algorithm inside the signature is sha1WithRSAEncryption |

### A.5.3.5. chain-a3-iosig-type

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-iosig-type.pem |
| **Description** | Signature algorithm inside and outside identical, but not sha256WithRSAEncryption |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Signature algorithm is sha1WithRSAEncryption |

### A.5.3.6. chain-a3-no-rsa

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-short-rsa.pem |
| **Description** | Public Key not an RSA Key |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-no-rsa-key* |
| **Malformations** | Public Key is a DSA key. |

### A.5.3.7. chain-a3-short-rsa

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-short-rsa.pem |
| **Description** | Public Key Length 1024 bit |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-short-rsa-key* |
| **Malformations** | Public key is 1024 bits. |

### A.5.3.8. chain-a3-bad-exp

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-bad-exp.pem |
| **Description** | Public Key Exponent other than the required 65537 |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-bad-exp-key* |
| **Malformations** | Public Key Exponent is 3. |

### A.5.3.9. IMB-chain-a3-BER-enc

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-BER-enc.pem |
| **Description** | Encoded as BER (not DER) |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Certificate uses BER encoding. |

### A.5.3.10. chain-a3-no-saf

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-svf.pem |
| **Description** | Missing SignatureAlgorithm field |

| | |
|---|---|
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | SignatureAlgorithm field is not present |

### A.5.3.11. chain-a3-no-svf

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-svf.pem |
| **Description** | Missing SignatureValue field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Missing SignatureValue field |

### A.5.3.12. chain-a3-no-ver

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-ver.pem |
| **Description** | Missing Version field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Missing Version field |

### A.5.3.13. chain-a3-no-sn

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-sn.pem |
| **Description** | Missing SerialNumber field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Missing SerialNumber field |

### A.5.3.14. chain-a3-no-sig

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-issuer.pem |
| **Description** | Missing Signature field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key*, *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Missing Signature field |

### A.5.3.15. chain-a3-no-issuer

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-issuer.pem |
| **Description** | Missing Issuer field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | The Issuer field is not present. |

### A.5.3.16. chain-a3-no-subject

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-subject.pem |
| **Description** | Missing Subject field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Missing Subject field |

### A.5.3.17. chain-a3-no-spki

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-spki.pem |
| **Description** | Missing SubjectPublicKeyInfo field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Missing SubjectPublicKeyInfo field |

### A.5.3.18. chain-a3-no-val-f

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-aki-f.pem |
| **Description** | Missing Validity field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Missing Validity field |

### A.5.3.19. chain-a3-no-aki-f

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-aki-f.pem |
| **Description** | Missing AuthorityKeyIdentifier field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | The AuthorityKeyIdentifier is not present. |

### A.5.3.20. chain-a3-no-keyuse

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-keyuse.pem |
| **Description** | Missing KeyUsage field |

| | |
|---|---|
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | The Key Usage field is not present. |

### A.5.3.21. chain-a3-no-basic

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-no-basic.pem |
| **Description** | Missing BasicConstraint field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | The Basic Constraints field is not present. |

### A.5.3.22. chain-a3-path-1

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-path-2.pem |
| **Description** | Cert.Auth. true, PathLen present and positive |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |

### A.5.3.23. chain-a3-path-2

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-path-2.pem |
| **Description** | Cert.Auth. true, PathLen present and positive |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |

### A.5.3.24. chain-a3-path-3

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-path-3.pem |
| **Description** | Cert.Auth. true, PathLen present and negative |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | PathLen is -1. |

### A.5.3.25. chain-a3-path-4

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-path-4.pem |
| **Description** | Cert.Auth. false, PathLen absent |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |

### A.5.3.26. chain-a3-path-5

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-path-6.pem |
| **Description** | Cert.Auth. false, PathLen positive |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |

### A.5.3.27. chain-a3-path-6

| | |
|---|---|
| **Type** | IMB Certificate |
| | |

| | |
|---|---|
| **Filename** | IMB-chain-a3-path-6.pem |
| **Description** | Cert.Auth. false, PathLen positive |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |

### A.5.3.28. chain-a3-path-7

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-path-7.pem |
| **Description** | Cert.Auth. false, PathLen negative |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |

### A.5.3.29. chain-a3-org-name

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-org-name.pem |
| **Description** | OrganizationName in subject and issuer fields does not match |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | OrganizationName in subject field has first two letters transposed. |

### A.5.3.30. chain-a3-role-1

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-role-2.pem |
| **Description** | Cert.Auth. False, no role specified in CommonName |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Common Name begins with a period (".") |

### A.5.3.31. chain-a3-role-2

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-role-2.pem |
| **Description** | Non-SMS role in CN |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Common Name does not include SMS in the section to the left of the first period ("."). |

### A.5.3.32. chain-a3-date-exp

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | IMB-chain-a3-date-exp.pem |
| **Description** | Expired |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-a3-signer1*, *chain-a3-leaf-key* |
| **Malformations** | Certificate Not After field contains a date value in the past. |

## A.5.4. Chain B1 Certificate Files

### A.5.4.1. chain-b1-root

| | |
|---|---|
| **Type** | PRJ Certificate |
| **Filename** | PRJ-chain-b1-root.pem |
| **Description** | Self-signed root certificate for PRJ devices |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-b1-root-key* |

## A.5.5. Chain C1 Certificate Files

### A.5.5.1. chain-c1-root

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c1-root.pem |
| **Description** | Self-signed root certificate for KDS devices |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c1-root-key* |

## A.5.6. Chain C3 Certificate Files

### A.5.6.1. chain-c3-root

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-root.pem |
| **Description** | Self-signed root certificate for KDS devices |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-root-key* |

### A.5.6.2. chain-c3-signer1

| | |
|---|---|
| **Type** | IMB Certificate |
| **Filename** | KDS-chain-c3-signer1.pem |
| **Description** | Intermediate Signer, level one |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-root*, *chain-c3-signer1-key* |

### A.5.6.3. chain-c3-osig-type

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-osig-type.pem |
| **Description** | Signature algorithm of outside signature is sha1WithRSAEncryption |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |

### A.5.6.4. chain-c3-isig-type

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-isig-type.pem |
| **Description** | Signature algorithm inside signature not sha256WithRSAEncryption |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Signature algorithm inside the signature is sha1WithRSAEncryption |

### A.5.6.5. chain-c3-iosig-type

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-iosig-type.pem |
| **Description** | Signature algorithm inside and outside identical, but not sha256WithRSAEncryption |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Signature algorithm is sha1WithRSAEncryption |

### A.5.6.6. chain-c3-no-rsa

| |
|---|

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-short-rsa.pem |
| **Description** | Public Key not an RSA Key |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-no-rsa-key* |
| **Malformations** | Public key is DSA key |

### A.5.6.7. chain-c3-short-rsa

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-short-rsa.pem |
| **Description** | Public Key Length 1024 bit |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-short-rsa-key* |
| **Malformations** | Public key is 1024 bits. |

### A.5.6.8. chain-c3-bad-exp

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-bad-exp.pem |
| **Description** | Public Key Exponent other than default 65537 |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-bad-exp-key* |
| **Malformations** | Public Key Exponent is 3. |

### A.5.6.9. chain-c3-BER-enc

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-BER-enc.pem |
| **Description** | Encoded as BER (not DER) |

| | |
|---|---|
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Certificate uses BER encoding. |

### A.5.6.10. chain-c3-no-saf

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-svf.pem |
| **Description** | Missing SignatureAlgorithm field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | SignatureAlgorithm field is not present |

### A.5.6.11. chain-c3-no-svf

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-svf.pem |
| **Description** | Missing SignatureValue field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Missing SignatureValue field |

### A.5.6.12. chain-c3-no-ver

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-ver.pem |
| **Description** | Missing Version field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Missing Version field |

### A.5.6.13. chain-c3-no-sn

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-sn.pem |
| **Description** | Missing SerialNumber field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Missing SerialNumber field |

### A.5.6.14. chain-c3-no-sig

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-issuer.pem |
| **Description** | Missing Signature field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Missing Signature field |

### A.5.6.15. chain-c3-no-issuer

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-issuer.pem |
| **Description** | Missing Issuer field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | The Issuer field is not present. |

### A.5.6.16. chain-c3-no-subject

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-subject.pem |
| **Description** | Missing Subject field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Missing Subject field |

### A.5.6.17. chain-c3-no-spki

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-spki.pem |
| **Description** | Missing SubjectPublicKeyInfo field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Missing SubjectPublicKeyInfo field |

### A.5.6.18. chain-c3-no-val-f

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-aki-f.pem |
| **Description** | Missing Validity field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Missing Validity field |

### A.5.6.19. chain-c3-no-aki-f

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-aki-f.pem |
| **Description** | Missing AuthorityKeyIdentifier field |

| | |
|---|---|
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | The AuthorityKeyIdentifier is not present. |

### A.5.6.20. chain-c3-no-keyuse

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-keyuse.pem |
| **Description** | Missing KeyUsage field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | The Key Usage field is not present. |

### A.5.6.21. chain-c3-no-basic

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-no-basic.pem |
| **Description** | Missing BasicConstraint field |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | The Basic Constraints field is not present. |

### A.5.6.22. chain-c3-path-1

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-path-2.pem |
| **Description** | Cert.Auth. true, PathLenpresent and zero |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |

### A.5.6.23. chain-c3-path-2

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-path-2.pem |
| **Description** | Cert.Auth. true, PathLen present and positive |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |

### A.5.6.24. chain-c3-path-3

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-path-3.pem |
| **Description** | Cert.Auth. true, PathLen present and negative |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | PathLen is -1. |

### A.5.6.25. chain-c3-path-4

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-path-4.pem |
| **Description** | Cert.Auth. false, PathLen absent |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |

### A.5.6.26. chain-c3-path-5

| | |
|---|---|
| **Type** | KDS Certificate |
| | |

| | |
|---|---|
| **Filename** | KDS-chain-c3-path-6.pem |
| **Description** | Cert.Auth. false, PathLen zero |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |

### A.5.6.27. chain-c3-path-6

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-path-6.pem |
| **Description** | Cert.Auth. false, PathLen positive |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |

### A.5.6.28. chain-c3-path-7

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-path-7.pem |
| **Description** | Cert.Auth. false, PathLen negative |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |

### A.5.6.29. chain-c3-org-name

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-org-name.pem |
| **Description** | OrganizationName in subject and issuer fields does not match |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | OrganizationName in subject field has first two letters transposed. |

### A.5.6.30. chain-c3-role-1

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-date-exp.pem |
| **Description** | Cert.Auth. False, no role specified in CommonName |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Common Name begins with a period (".") |

### A.5.6.31. chain-c3-date-exp

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-date-exp.pem |
| **Description** | Expired |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |
| **Malformations** | Certificate Not After field contains a date value in the past. |

### A.5.6.32. chain-c3-role-2

| | |
|---|---|
| **Type** | KDS Certificate |
| **Filename** | KDS-chain-c3-role-2.pem |
| **Description** | Cert.Auth. False, role error (CN contains only FMI). |
| **Conforms to** | SMPTE-430-2 |
| **Prerequisites** | *chain-c3-signer1*, *chain-c3-leaf-key* |

## A.5.7. Public/Private Key Pairs

### A.5.7.1. chain-a3-bad-exp-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | IMB-chain-a3-bad-exp-key.pem |
| **Description** | RSA keypair for Public Key Exponent other than the required 65537 |
| **Conforms to** | SMPTE-430-2 |
| **Malformations** | Public Key Exponent is 3. |

### A.5.7.2. chain-a3-leaf-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | IMB-chain-a3-leaf-key.pem |
| **Description** | RSA keypair for leaf |
| **Conforms to** | SMPTE-430-2 |

### A.5.7.3. chain-a3-no-rsa-key

| | |
|---|---|
| **Type** | DSA keypair |
| **Filename** | IMB-chain-a3-no-rsa-key.pem |
| **Description** | DSA keypair for Public Key not an RSA Key |
| **Conforms to** | SMPTE-430-2 |
| **Malformations** | Public Key is a DSA key. |

### A.5.7.4. chain-a3-root-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | IMB-chain-a3-root-key.pem |
| **Description** | RSA keypair for root cert, malformed leaves |
| | |

| | |
|---|---|
| **Conforms to** | SMPTE-430-2 |

### A.5.7.5. chain-a3-short-rsa-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | IMB-chain-a3-short-rsa-key.pem |
| **Description** | RSA keypair for Public Key Length 1024 bit |
| **Conforms to** | SMPTE-430-2 |
| **Malformations** | Public key is 1024 bits. |

### A.5.7.6. chain-a3-signer1-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | IMB-chain-a3-signer1-key.pem |
| **Description** | RSA keypair for Intermediate Signer, level one |
| **Conforms to** | SMPTE-430-2 |

### A.5.7.7. chain-c1-root-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | KDS-chain-c1-root-key.pem |
| **Description** | RSA keypair for self-signed root certificate for KDS devices |
| **Conforms to** | SMPTE-430-2 |

### A.5.7.8. chain-c3-bad-exp-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | KDS-chain-c3-bad-exp-key.pem |
| **Description** | RSA keypair for Public Key Exponent other than default 65537 |
| | |

| | |
|---|---|
| **Conforms to** | SMPTE-430-2 |
| **Malformations** | Public Key Exponent is 3. |

### A.5.7.9. chain-c3-leaf-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | KDS-chain-c3-leaf-key.pem |
| **Description** | RSA keypair for leaf |
| **Conforms to** | SMPTE-430-2 |

### A.5.7.10. chain-c3-no-rsa-key

| | |
|---|---|
| **Type** | DSA keypair |
| **Filename** | KDS-chain-c3-no-rsa-key.pem |
| **Description** | DSA keypair for Public Key not an RSA Key |
| **Conforms to** | SMPTE-430-2 |
| **Malformations** | Public Key is a DSA key. |

### A.5.7.11. chain-c3-root-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | KDS-chain-c3-root-key.pem |
| **Description** | RSA keypair for self-signed root certificate for KDS devices |
| **Conforms to** | SMPTE-430-2 |

### A.5.7.12. chain-c3-short-rsa-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | KDS-chain-c3-short-rsa-key.pem |
| | |

| | |
|---|---|
| **Description** | RSA keypair for Public Key Length 1024 bit |
| **Conforms to** | SMPTE-430-2 |
| **Malformations** | Public key is 1024 bits. |

### A.5.7.13. chain-c3-signer1-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | KDS-chain-c3-signer1-key.pem |
| **Description** | RSA keypair for Intermediate Signer, level one |
| **Conforms to** | SMPTE-430-2 |

### A.5.7.14. chain-b1-root-key

| | |
|---|---|
| **Type** | RSA keypair |
| **Filename** | PRJ-chain-b1-root-key.pem |
| **Description** | RSA keypair for self-signed root certificate for PRJ devices |
| **Conforms to** | SMPTE-430-2 |

# A.6. Key Delivery Messages

## A.6.1. Introduction

The KDM files defined in this section must be generated for the device under test and the time and date of the test procedure.

## A.6.2. KDM for DCI 2K Sync Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_sync_test_ct.kdm.xml |

| | |
|---|---|
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test (Encrypted)* |

## A.6.3. KDM for DCI 2K Sync Test with Subtitles (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sync_test_with_subs_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync test with Subtitles (Encrypted)* |

## A.6.4. KDM for DCI 2K Image with Frame Number Burn In (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | frame_num_burn_in_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Image with Frame Number Burn In (Encrypted)* |

## A.6.5. KDM for 2K StEM (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K StEM (Encrypted)* |

## A.6.6. KDM for 2K StEM Sequence (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| | |

| | |
|---|---|
| **Filename** | 2K_StEM_sequence_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K StEM Test Sequence (Encrypted)* |

## A.6.7. KDM for 128 Reel Composition, "A" Series (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_128_a_reels_ct.kdm.xml |
| **Description** | KDM that has all content keys for the track files referenced by the CPL, and additionally has one each of key types FMIK and FMAK. The FMIK and FMAK key values shall be appropriate for the specifications of the FM system used by the Test Subject. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *128 Reel Composition, "A" Series (Encrypted)* |

## A.6.8. KDM for 128 Reel Composition, "B" Series (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_128_b_reels_ct.kdm.xml |
| **Description** | KDM that has all content keys for the track files referenced by the CPL, and additionally has one each of key types FMIK and FMAK. The FMIK and FMAK key values shall be appropriate for the specifications of the FM system used by the Test Subject. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *128 Reel Composition, "B" Series (Encrypted)* |

## A.6.9. KDM for 64 1 second reel Composition (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_64_1_second_reels_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *64 Reel Composition, 1 Second Reels (Encrypted)* |

## A.6.10. KDM for 2K FM Application Constraints (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_constraints_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Application Constraints (Encrypted)* |

## A.6.11. KDM for 2K FM Control Granularity - No FM (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_control_granularity_no_fm.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Control Granularity - No FM (Encrypted)* |

## A.6.12. KDM for 2K FM Control Granularity - Image Only FM (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_control_granularity_image_only_fm.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Control Granularity - Image Only FM (Encrypted)* |

## A.6.13. KDM for 2K FM Control Granularity - Sound Only FM (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_control_granularity_sound_only_fm.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |

| | |
|---|---|
| **Prerequisites** | *2K FM Control Granularity - Sound Only FM (Encrypted)* |

## A.6.14. KDM for 2K FM Control Granularity - Image and Sound FM (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_control_granularity_image_and_sound_fm.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Control Granularity - Image and Sound FM (Encrypted)* |

## A.6.15. KDM for 2K FM Payload (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_payload_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Payload (Encrypted)* |

## A.6.16. KDM for Binary Audio Forensic Marking Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | binary_audio_fm_ct.kdm.xml |
| **Description** | KDM with "no FM mark" flag applied to audio. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *Binary Audio Forensic Marking Bypass Test (Encrypted)* |

## A.6.17. KDM for Binary Selective Audio Forensic Marking Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |

| | |
|---|---|
| **Filename** | binary_selective_audio_fm_6ch_ct.kdm.xml |
| **Description** | KDM with audio forensic marking disabled on audio channels above 6 using the "selective audio FM mark" command. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *Binary Audio Forensic Marking Bypass Test (Encrypted)* |

## A.6.18. KDM for Selective Audio FM - All FM (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | selective_audio_fm_all-fm_ct.kdm.xml |
| **Description** | KDM with all audio forensic marking enabled on all audio channels. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *Selective Audio FM - All FM (Encrypted)* |

## A.6.19. KDM for Selective Audio FM - No FM (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | selective_audio_fm_no-fm_ct.kdm.xml |
| **Description** | KDM with all audio forensic marking disabled by the "no FM mark" URI. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *Selective Audio FM - No FM (Encrypted)* |

## A.6.20. KDM for Selective Audio FM - Not Above Channel 6 (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | selective_audio_fm_6ch_ct.kdm.xml |
| **Description** | KDM with audio forensic marking disabled on audio channels above 6 using the "selective audio FM mark" command. The KDM also has the "no FM mark" URI, which should be overridden by the "selective audio FM mark" URI. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |

| | |
|---|---|
| **Prerequisites** | *Selective Audio FM - Not Above Channel 6 (Encrypted)* |

## A.6.21. KDM for Selective Audio FM - Not Above Channel 8 (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | selective_audio_fm_8ch_ct.kdm.xml |
| **Description** | KDM with audio forensic marking disabled on audio channels above 8 using the "selective audio FM mark" command. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *Selective Audio FM - Not Above Channel 8 (Encrypted)* |

## A.6.22. KDM for Selective Audio FM - Not Above Channel 10 (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | selective_audio_fm_10ch_ct.kdm.xml |
| **Description** | KDM with audio forensic marking disabled on audio channels above 10 using the "selective audio FM mark" command. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *Selective Audio FM - Not Above Channel 10 (Encrypted)* |

## A.6.23. KDM for Selective Audio FM - Not Above Channel 17 (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | selective_audio_fm_17ch_ct.kdm.xml |
| **Description** | KDM with audio forensic marking disabled on audio channels above 17 using the "selective audio FM mark" command. The KDM also has the "no FM mark" URI, which should be overridden by the "selective audio FM mark" URI. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *Selective Audio FM - Not Above Channel 17 (Encrypted)* |

## A.6.24. KDM with two selective audio FM mark URIs

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-2-selective-fm-cmds.kdm.xml |
| **Description** | KDM that contains more than one selective audio FM mark URIs |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K StEM (Encrypted)* |
| **Malformations** | KDM contains one `ForensicMarkFlag` element with the value "http:// www.dcimovies.com/430-1/2006/KDM#mrkflg-audio-disable-above-channel-06", and one `ForensicMarkFlag` element with the value "http:// www.dcimovies.com/430-1/2006/KDM#mrkflg-audio-disable-above-channel-08" |

## A.6.25. KDM for 2K Maximum Bitrate Composition (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_max_bitrate_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K DCI Maximum Bitrate Composition (Encrypted)* |

## A.6.26. KDM for 4K Maximum Bitrate Composition (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 4K_max_bitrate_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *4K DCI Maximum Bitrate Composition (Encrypted)* |

## A.6.27. KDM for Past Time Window Extension (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| | |

| | |
|---|---|
| **Filename** | holdover_long_ct-kdm-short-expire.kdm.xml |
| **Description** | KDM that has a validity period that is current, but expires in the near future |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *End of Engagement - Past Time Window Extension (Encrypted)* |
| **Malformations** | The value of the ContentKeysNotValidAfter element is a UTC timestamp no greater than 60 minutes in the future. |

## A.6.28. KDM for Within Time Window Extension (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | holdover_short_ct-kdm-short-expire.kdm.xml |
| **Description** | KDM that has a validity period that is current, but expires in the near future |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *End of Engagement - Within Time Window Extension (Encrypted)* |
| **Malformations** | The value of the ContentKeysNotValidAfter element is a UTC timestamp no greater than 60 minutes in the future. |

## A.6.29. KDM for DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m01_pict_frame_oo_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)* |

## A.6.30. KDM for DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m02_snd_frame_oo_ct.kdm.xml |
| | |

| | |
|---|---|
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted)* |

## A.6.31. KDM for DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m04_sndtk_wrong_file_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)* |

## A.6.32. KDM for DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m05_pict_wrong_file_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)* |

## A.6.33. KDM for DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m06_cpl_hash_error_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)* |

## A.6.34. KDM for DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m07_cpl_invalid_signature_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)* |

## A.6.35. KDM for DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m09_pict_bad_hmac_ct.kdm.xml |
| **Description** | The KDM does not contain a KDM-borne MIC Key. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted)* |

## A.6.36. KDM for DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m10_snd_bad_hmac_ct.kdm.xml |
| **Description** | The KDM does not contain a KDM-borne MIC Key. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)* |

## A.6.37. KDM for DCI Malformed Test 11: Picture with Check Value error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m11_pict_bad_chuk_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 11: Picture with Check Value error in MXF Track File (Encrypted)* |

## A.6.38. KDM for DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m12_snd_bad_chuk_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)* |

## A.6.39. KDM for DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m13_cpl_missing_asset_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted)* |

## A.6.40. KDM for DCI Malformed Test 14: CPL that does not conform to ST 429-7 (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m14_cpl_format_error_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 14: CPL that does not conform to ST 429-7 (Encrypted)* |

## A.6.41. KDM for DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted)

| | |
|---|---|
| **Type** | KDM |

| | |
|---|---|
| **Filename** | m15_cpl_signer_format_error_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted)* |

## A.6.42. KDM for DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m16_cpl_malf_signer_no_role_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)* |

## A.6.43. KDM for DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m17_cpl_malf_signer_bad_role_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)* |

## A.6.44. KDM for DCI Malformed Test 18: KDM for CPL signed with Extra Role Certificate (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m18_cpl_malf_signer_extra_role_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 18: CPL signed with Extra Role Certificate (Encrypted)* |

## A.6.45. KDM with invalid XML

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-any.kdm.xml |
| **Description** | KDM that contains an invalid XML file format |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | Missing </DCinemaSecurityMessage> tag |

## A.6.46. KDM that has expired

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-expired.kdm.xml |
| **Description** | KDM that has a validity period that has expired |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The value of the ContentKeysNotValidAfter element is a UTC timestamp at least 24 hours in the past. |

## A.6.47. KDM with future validity period within the UTC offset

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-near-future.kdm.xml |
| **Description** | KDM that has a validity period in the future according to the full ContentKeysNotValidBefore timestamp but is valid now if the UTC offset is ignored. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The value of the ContentKeysNotValidBefore element is a UTC timestamp between 4 and 6 hours in the future, with a local offset of -06:00. |

## A.6.48. KDM that has recently expired

| | |
|---|---|
| **Type** | KDM |

| | |
|---|---|
| **Filename** | kdm-recent-expired.kdm.xml |
| **Description** | KDM that has a validity period that has expired according to the full ContentKeysNotValidAfter timestamp but that has not expired if the local offset is ignored. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The value of the ContentKeysNotValidAfter element is a UTC timestamp between 4 and 6 hours in the past, with a local offset of +06:00. |

## A.6.49. KDM with incorrect message digest

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-sig-digest.kdm.xml |
| **Description** | KDM in which a Signature Digest has been altered |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The plaintext form of the encrypted message digest in the signature is not the same value as a calculated message digest of the KDM. |

## A.6.50. KDM with future validity period

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-future-cy2024.kdm.xml |
| **Description** | KDM that has a validity period that is in the future |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The value of the ContentKeysNotValidBefore element is a UTC timestamp at least 24 hours in the future. |

## A.6.51. KDM with empty TDL

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-no-tdl.kdm.xml |

| | |
|---|---|
| **Description** | KDM that has an empty Trusted Device List (TDL) |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The DeviceList element of the KDM is empty. |

## A.6.52. KDM with Assume Trust and random TDL entries

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-assume-trust-and-more.kdm.xml |
| **Description** | KDM with a TDL consisting of one entry Assume Trust entry (*i.e.* "2jmj7l5rSw0yVb/ vlWAYkK/YBwk=") and one random entry. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.53. KDM with the SM alone on the TDL

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-self-tdl.kdm.xml |
| **Description** | KDM with a single entry on its TDL corresponding the recipient's SM certificate. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.54. KDM with the projector and LDB on the TDL

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-ldb-projector-tdl.kdm.xml |
| **Description** | KDM with two entries on its TDL corresponding the projector SPB and LDB connected to the MB. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.55. KDM with the projector alone on the TDL

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-projector-tdl.kdm.xml |
| **Description** | KDM with a single entry on its TDL corresponding the projector SPB connected to the MB. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.56. KDM with the LDB alone on the TDL

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-ldb-tdl.kdm.xml |
| **Description** | KDM with a single entry on its TDL corresponding the LDB connected to the MB. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.57. Deleted Section

The section "KDM with imminent expiration date" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

## A.6.58. KDM with corrupted CipherData block

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-CipherData-block.kdm.xml |
| **Description** | KDM that contains an Invalid Structure ID field in the CipherData element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| | |

| | |
|---|---|
| **Malformations** | The first byte of the Structure ID field contained in the <enc:CipherValue> element inside the <enc:CipherData> element has been changed from "F1" to "1F" |

## A.6.59. KDM with incorrect signer thumbprint

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-signer-tp.kdm.xml |
| **Description** | KDM for which the Thumbprint of the Signer's Certificate does not match the Signer of the KDM |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The thumbprint of the signer certificate as listed in the KDM is incorrect and does not match the thumbprint for the issuing certificate. |

## A.6.60. KDM without signer certificate

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-chain.kdm.xml |
| **Description** | KDM in which the Certificate chain does not contain the Signer's Certificate |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The certificate that signed the KDM is not included in the KDM. |

## A.6.61. KDM without AuthorityKey certificate

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-chain-no-cert-authkeyid.kdm.xml |
| **Description** | KDM in which the Certificate chain does not contain the certificate specified by the AuthorityKeyIdentifier value in the Signer Certificate |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | A KDM that specifies the signer's issuer certificate as the AuthorityKeyIdentifier but which does not contain |

| | |
|---|---|
| | that certificate. |

## A.6.62. KDM with KeyInfo mismatch

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-bad-keyinfo.kdm.xml |
| **Description** | KeyInfo field of the audio EncryptedKey element does not match the KeyInfo field of the image EncryptedKey element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The KeyInfo element of the audio encrypted key data contains the correct Issuer Name and an incorrect IssuerSerial of the certificate of the recipient of the KDM. |

## A.6.63. KDM with invalid MessageType

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-MessageType.kdm.xml |
| **Description** | KDM with an Invalid MessageType element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | MessageType element contains: "http://www.smpte-qa.org/430-1/2006/KDM#kdm-key-type" |

## A.6.64. KDM with expired Signer certificate

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-expired-signer.kdm.xml |
| **Description** | KDM with an expired Signer's Certificate and an ETM IssueDate later than Signer's Certificate expiry date |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | KDM signer's certificate's Validity "Not After" date is earlier than ETM IssueDate |

## A.6.65. KDM issued before certificate valid

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-issue-before-cert-valid.kdm.xml |
| **Description** | KDM with a valid Signer's Certificate, but ETM issue date before Signer's Certificate issue date |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The <IssueDate> element contains a date prior to the date of the signer certificate's Validity "Not Before" date. |

## A.6.66. KDM validity exceeds signer validity

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-signer-cert-exp-before-kdm-expires.kdm.xml |
| **Description** | KDM with a validity period that extends beyond the validity of Signer's Certificate expiry date. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The KDM has a ContentKeysNotValidAfter value later than the signer certificate's "Not After" value. |

## A.6.67. KDM with mismatched keytype

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-mismatched-key-keytype.kdm.xml |
| **Description** | KDM with an encryption key that is valid but has an incorrect keytype |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | Key is a valid image encryption key but has the keytype "MDAK". |

## A.6.68. KDM with non-empty NonCriticalExtensions

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-with-non-crit-exts.kdm.xml |
| **Description** | KDM with a non-empty NonCriticalExtensions element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.69. KDM with invalid ContentAuthenticator

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-ContentAuthenticator.kdm.xml |
| **Description** | KDM with an Invalid ContentAuthenticator element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | the content of the ContentAuthenticator element shall contain a thumbprint of a D-Cinema cert that does not match one in the signer chain of the CPL that the KDM references. |

## A.6.70. KDM with bad CompositionPlaylistId value

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-CompositionPlaylistId.kdm.xml |
| **Description** | KDM with an incorrect value in the CompositionPlaylistId element. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The content of the CompositionPlaylistId element shall contain a UUID value that does not match the Id value of the associated CPL. |

## A.6.71. KDM with bad CipherData CompositionPlaylistId value

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-CipherData-CPLId.kdm.xml |
| **Description** | KDM with an incorrect value in the CompositionPlaylistId field of the CipherData structure. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The content of the CompositionPlaylistId field of the CipherData structure shall contain a UUID value that does not match the Id value of the associated CPL. |

## A.6.72. KDM with incorrect namespace name value

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-namespace.kdm.xml |
| **Description** | KDM has the wrong namespace name. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The namespace name corresponding to the top level XML element does not match the value given in SMPTE-430-3-2006. The bogus value `http://www.smpte-qa.org/schemas/430-3/2001/ETMshall` be used. |

## A.6.73. KDM with random TDL entry

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-random-tdl.kdm.xml |
| **Description** | KDM has a random entry that does not match any known remote SPB. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The DeviceInfoList contains a single entry, a randomly generated value. |

## A.6.74. KDM signed with incorrect signer certificate format

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-signer-format.kdm.xml |
| **Description** | KDM which has been signed with a certificate not conforming with SMPTE-430-2-2006. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |
| **Malformations** | The certificate that signed the KDM is Interop format. |

## A.6.75. KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-assume-trust.kdm.xml |
| **Description** | KDM which has only the empty-string thumbprint "assume trust" in the TDL (*i.e.* "2jmj7l5rSw0yVb/vlWAYkK/YBwk="). |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.76. KDM for 2K StEM with Device Specific Special Auditorium TDL

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_ct_device_specific_special_auditorium.kdm.xml |
| **Description** | KDM that has a TDL containing the certificate thumbprints of devices specific to a Special Auditorium Situation. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K StEM (Encrypted)* |

## A.6.77. KDM for DCI 2K StEM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-5-3-2-2.kdm.xml |
| **Description** | KDM for DCI 2K StEM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.78. KDM with a TDL including Responder A

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-6-1-7-responder-a.kdm.xml |
| **Description** | KDM with a TDL that contains the thumbprint for the certificate of Responder A |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.79. KDM with a TDL including Responder B

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-6-1-7-responder-b.kdm.xml |
| **Description** | KDM with a TDL that contains the thumbprint for the certificate of Responder B |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted)* |

## A.6.80. KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and an additional device certificate

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-6-2-2-special-auditorium-situation-and-additional-thumbprint.kdm.xml |
| **Description** | KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and an additional device certificate. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for DCI 2K Sync Test (Encrypted)* |

## A.6.81. KDM with a TDL that contains all but one of the certificate thumbprints for the devices in the special auditorium situation

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-6-2-2-special-auditorium-situation-less-one-thumbprint.kdm.xml |
| **Description** | KDM with a TDL that contains all but one of the certificate thumbprints for the devices in that special auditorium situation. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for DCI 2K Sync Test (Encrypted)* |

## A.6.82. KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and the "assume trust" thumbprint

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-6-2-2-special-auditorium-situation-and-assume-trust-thumbprint.kdm.xml |
| **Description** | KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation and the "assume trust" thumbprint. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| | |

| | |
|---|---|
| **Prerequisites** | *KDM for DCI 2K Sync Test (Encrypted)* |

## A.6.83. KDM with a TDL that contains one more LD/LE device thumbprints than there are LD/projector thumbprints in the special auditorium situation

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-6-2-2-special-auditorium-situation-and-additional-ld-le-thumbprint.kdm.xml |
| **Description** | KDM with a TDL that contains one more LD/LE device thumbprints than there are LD/ projector thumbprints in the special auditorium situation. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for DCI 2K Sync Test (Encrypted)* |

## A.6.84. KDM with Assume Trust TDL Entry for DCI 2K Sync Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-6-2-2-assume-trust.kdm.xml |
| **Description** | KDM which has only the empty-string thumbprint "assume trust" in the TDL (*i.e.* "2jmj7l5rSw0yVb/vlWAYkK/YBwk="). |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for DCI 2K Sync Test (Encrypted)* |

## A.6.85. KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-6-2-2-special-auditorium-situation.kdm.xml |
| **Description** | KDM with a TDL that contains all of the certificate thumbprints for the devices in the special auditorium situation. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| | |

| | |
|---|---|
| **Prerequisites** | *KDM for DCI 2K Sync Test (Encrypted)* |

## A.6.86. KDM for 2K Scope Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_2K_scope_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K Scope Subtitle Test (Encrypted)* |

## A.6.87. KDM for 2K Flat Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_2K_flat_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K Flat Subtitle Test (Encrypted)* |

## A.6.88. KDM for 2K Full Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_2K_full_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K Full Subtitle Test (Encrypted)* |

## A.6.89. KDM for 4K Scope Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_4K_scope_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| | |

| | |
|---|---|
| **Prerequisites** | *4K Scope Subtitle Test (Encrypted)* |

## A.6.90. KDM for 4K Flat Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_4K_flat_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *4K Flat Subtitle Test (Encrypted)* |

## A.6.91. KDM for 4K Full Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_4K_full_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *4K Full Subtitle Test (Encrypted)* |

## A.6.92. KDM for 2K 48fps Scope Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_48fps_scope_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K 48fps Scope Subtitle Test (Encrypted)* |

## A.6.93. KDM for 2K 48fps Flat Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_48fps_flat_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| | |

| | |
|---|---|
| **Prerequisites** | *2K 48fps Flat Subtitle Test (Encrypted)* |

## A.6.94. KDM for 2K 48fps Full Subtitle Test (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | sub_test_48fps_full_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K 48fps Full Subtitle Test (Encrypted)* |

## A.6.95. KDM for DCI 2K Sync Test (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_sync_test_obae_ct.kdm.xml |
| **Description** | KDM for Section A.4.107: DCI 2K Sync Test (OBAE) (Encrypted) |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test (OBAE) (Encrypted)* |

## A.6.96. KDM with bad CompositionPlaylistId value (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-CompositionPlaylistId-obae.kdm.xml |
| **Description** | KDM with an incorrect value in the CompositionPlaylistId element. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The content of the CompositionPlaylistId element shall contain a UUID value that does not match the Id value of the associated CPL. |

## A.6.97. KDM with bad CipherData CompositionPlaylistId value (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-CipherData-CPLId-obae.kdm.xml |
| **Description** | KDM with an incorrect value in the CompositionPlaylistId field of the CipherData structure. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The content of the CompositionPlaylistId field of the CipherData structure shall contain a UUID value that does not match the Id value of the associated CPL. |

## A.6.98. KDM for 2K StEM (Encrypted) (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K StEM (OBAE) (Encrypted)* |

## A.6.99. KDM for DCI 2K Sync test with Subtitles (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_sync_test_with_subs_obae_ct.kdm.xml |
| **Description** | KDM for *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* |

## A.6.100. KDM for DCI 2K Sync test with Subtitles (Encrypted): missing picture essence key

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m0100_missing_key_pict.kdm.xml |
| **Description** | KDM for *DCI 2K Sync test with Subtitles (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |

| | |
|---|---|
| **Prerequisites** | *DCI 2K Sync test with Subtitles (Encrypted)* |
| **Malformations** | The KDM is missing a single picture essence key used by the associated CPL. |

## A.6.101. KDM for DCI 2K Sync test with Subtitles (Encrypted): missing sound essence key

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m0102_missing_key_snd.kdm.xml |
| **Description** | KDM for *DCI 2K Sync test with Subtitles (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync test with Subtitles (Encrypted)* |
| **Malformations** | The KDM is missing a single sound essence key used by the associated CPL. |

## A.6.102. KDM for DCI 2K Sync test with Subtitles (Encrypted): missing subtitle essence key

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m0104_missing_key_sub.kdm.xml |
| **Description** | KDM for *DCI 2K Sync test with Subtitles (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync test with Subtitles (Encrypted)* |
| **Malformations** | The KDM is missing a single subtitle essence key used by the associated CPL. |

## A.6.103. KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing picture essence key

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m0106_missing_key_pict_obae.kdm.xml |
| **Description** | KDM for *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |

| | |
|---|---|
| **Prerequisites** | *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* |
| **Malformations** | The KDM is missing a single picture essence key used by the associated CPL. |

## A.6.104. KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing sound essence key

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m0108_missing_key_snd_obae.kdm.xml |
| **Description** | KDM for *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* |
| **Malformations** | The KDM is missing a single sound essence key used by the associated CPL. |

## A.6.105. KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing picture subtitle key

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m0110_missing_key_sub_obae.kdm.xml |
| **Description** | KDM for *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* |
| **Malformations** | The KDM is missing a single subtitle essence key used by the associated CPL. |

## A.6.106. KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing OBAE key

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m0112_missing_key_obae_obae.kdm.xml |
| **Description** | KDM for *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |

| | |
|---|---|
| **Prerequisites** | *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* |
| **Malformations** | The KDM is missing a single OBAE essence key used by the associated CPL. |

## A.6.107. KDM for M25 Composition with Malformed Integrity Pack: Missing MIC item (Picture) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m25_integrity_pict_mic_ct.kdm.xml |
| **Description** | KDM for *M25 Composition with Malformed Integrity Pack: Missing MIC item (Picture) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M25 Composition with Malformed Integrity Pack: Missing MIC item (Picture) (Encrypted)* |

## A.6.108. KDM for M27 Composition with Malformed Integrity Pack: Missing TrackFileID item (Picture) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m27_integrity_pict_tfid_ct.cpl.xml |
| **Description** | KDM for *M27 Composition with Malformed Integrity Pack: Missing TrackFileID item (Picture) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M27 Composition with Malformed Integrity Pack: Missing TrackFileID item (Picture) (Encrypted)* |

## A.6.109. KDM for M26 Composition with Malformed Integrity Pack: Missing SequenceNumber item (Picture) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m26_integrity_pict_snum_ct.kdm.xml |
| **Description** | KDM for *M26 Composition with Malformed Integrity Pack: Missing SequenceNumber item (Picture) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M26 Composition with Malformed Integrity Pack: Missing SequenceNumber item (Picture) (Encrypted)* |

## A.6.110. KDM for M28 Composition with Malformed Integrity Pack: Missing MIC item (PCM) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m28_integrity_snd_mic_ct.kdm.xml |
| **Description** | KDM for *M28 Composition with Malformed Integrity Pack: Missing MIC item (PCM) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M28 Composition with Malformed Integrity Pack: Missing MIC item (PCM) (Encrypted)* |

## A.6.111. KDM for M30 Composition with Malformed Integrity Pack: Missing TrackFileID item (PCM) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m30_integrity_snd_tfid_ct.kdm.xml |
| **Description** | KDM for *M30 Composition with Malformed Integrity Pack: Missing TrackFileID item (PCM) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M30 Composition with Malformed Integrity Pack: Missing TrackFileID item (PCM) (Encrypted)* |

## A.6.112. KDM for M29 Composition with Malformed Integrity Pack: Missing SequenceNumber item (PCM) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m29_integrity_snd_snum_ct.kdm.xml |
| **Description** | KDM for *M29 Composition with Malformed Integrity Pack: Missing SequenceNumber item (PCM) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M29 Composition with Malformed Integrity Pack: Missing SequenceNumber item (PCM) (Encrypted)* |

## A.6.113. KDM for M20 Composition with Malformed Integrity Pack: Missing MIC item (OBAE Main Sound) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m20_integrity_obae_ms_mic_ct.kdm.xml |
| **Description** | KDM for *M20 Composition with Malformed Integrity Pack: Missing MIC item (OBAE Main Sound) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M20 Composition with Malformed Integrity Pack: Missing MIC item (OBAE Main Sound) (Encrypted)* |

## A.6.114. KDM for M22 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE Main Sound) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m22_integrity_obae_ms_tfid_ct.kdm.xml |
| **Description** | KDM for *M22 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE Main Sound) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M22 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE Main Sound) (Encrypted)* |

## A.6.115. KDM for M21 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE Main Sound) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m21_integrity_obae_ms_snum_ct.kdm.xml |
| **Description** | KDM for *M21 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE Main Sound) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M21 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE Main Sound) (Encrypted)* |

## A.6.116. KDM for M19 Composition with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m19_integrity_obae_mic_ct.kdm.xml |
| **Description** | KDM for *M19 Composition with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M19 Composition with Malformed Integrity Pack: Missing MIC item (OBAE) (Encrypted)* |

## A.6.117. KDM for M24 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m24_integrity_obae_tfid_ct.kdm.xml |
| **Description** | KDM for *M24 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M24 Composition with Malformed Integrity Pack: Missing TrackFileID item (OBAE) (Encrypted)* |

## A.6.118. KDM for M23 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m23_integrity_obae_snum_ct.kdm.xml |
| **Description** | KDM for *M23 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M23 Composition with Malformed Integrity Pack: Missing SequenceNumber item (OBAE) (Encrypted)* |

## A.6.119. KDM with mismatched KeyType value (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-mismatched-key-keytype-obae.kdm.xml |
| **Description** | KDM with an cryptographic key that is valid for an OBAE track file but has an incorrect `KeyType` value. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | Key is a valid OBAE cryptographic key but is associated with the `KeyType` value `"MDAK"`. |

## A.6.120. KDM with incorrect message digest (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-sig-digest-obae.kdm.xml |
| **Description** | KDM in which a Signature Digest has been altered |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The plaintext form of the encrypted message digest in the signature is not the same value as a calculated message digest of the KDM. |

## A.6.121. KDM that has expired (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-expired-obae.kdm.xml |
| **Description** | KDM that has a validity period that has expired |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The value of the ContentKeysNotValidAfter element is a UTC timestamp at least 24 hours in the past. |

## A.6.122. KDM with future validity period (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-future-obae.kdm.xml |
| **Description** | KDM that has a validity period that is in the future |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The value of the ContentKeysNotValidBefore element is a UTC timestamp at least 24 hours in the future. |

## A.6.123. KDM with empty TDL (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-no-tdl-obae.kdm.xml |
| **Description** | KDM that has an empty Trusted Device List (TDL) |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The DeviceList element of the KDM is empty. |

## A.6.124. KDM with Assume Trust TDL Entry (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-assume-trust-obae.kdm.xml |
| **Description** | KDM which has only the empty-string thumbprint "assume trust" in the TDL (*i.e.* "2jmj7l5rSw0yVb/vlWAYkK/YBwk="). |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |

## A.6.125. KDM with invalid XML (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-any-obae.kdm.xml |
| **Description** | KDM that contains an invalid XML file format |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | Missing </DCinemaSecurityMessage> tag |

## A.6.126. KDM for 64 1 second reel Composition (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_64_1_second_reels_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *64 Reel Composition, 1 Second Reels (OBAE) (Encrypted)* |

## A.6.127. KDM for M40 OBAE DCP with Frame-out-of-order error (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m40_obae_frame_oo_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M40 OBAE DCP with Frame-out-of-order error (Encrypted)* |

## A.6.128. KDM for M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)

| | |
|---|---|
| **Type** | KDM |

| | |
|---|---|
| **Filename** | m41_obae_wrong_file_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)* |

## A.6.129. KDM for DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM mkey |
| **Filename** | 2K_sync_test_obae_mkey_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)* |

## A.6.130. KDM for M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m43_obae_bad_chuk_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)* |

## A.6.131. KDM with invalid MIC Key for DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM mkey |
| **Filename** | m120_bad_mkey_2K_sync_test_obae_mkey_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)* |
| **Malformations** | The MIC Key specified in the KDM does not match the MIC Key used to generate the MIC item in the OBAE Track File. |

## A.6.132. KDM with MIC Key for DCI 2K Sync Test (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM mkey |
| **Filename** | m121_mkey_2K_sync_test_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test (OBAE) (Encrypted)* |
| **Malformations** | The KDM contains a MIC Key for an OBAE Track File that does not use a KDM-borne MIC Key. |

## A.6.133. KDM for Past Time Window Extension (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | holdover_long_obae_ct-kdm-short-expire.kdm.xml |
| **Description** | KDM that has a validity period that is current, but expires in the near future |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *End of Engagement - Past Time Window Extension (OBAE) (Encrypted)* |
| **Malformations** | The value of the ContentKeysNotValidAfter element is a UTC timestamp no greater than 60 minutes in the future. |

## A.6.134. KDM for Within Time Window Extension (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | holdover_short_obae_ct-kdm-short-expire.kdm.xml |
| **Description** | KDM that has a validity period that is current, but expires in the near future |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *End of Engagement - Within Time Window Extension (OBAE) (Encrypted)* |
| **Malformations** | The value of the ContentKeysNotValidAfter element is a UTC timestamp no greater than 60 minutes in the future. |

## A.6.133. KDM with MIC Key (Sound) for DCI 2K Sync Test (Encrypted)

| | |
|---|---|
| **Type** | KDM mkey |
| **Filename** | m122_mkey_sound_2K_sync_test_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test (Encrypted)* |
| **Malformations** | The KDM contains a MIC Key for a Sound Track File that does not use a KDM-borne MIC Key. |

## A.6.134. KDM with invalid MIC Key (Sound) for DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)

| | |
|---|---|
| **Type** | KDM mkey |
| **Filename** | m123_bad_mkey_sound_2K_sync_test_mkey_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)* |
| **Malformations** | The MIC Key specified in the KDM does not match the MIC Key used to generate the MIC item in the Sound Track File. |

## A.6.135. KDM with MIC Key (Picture) for DCI 2K Sync Test (Encrypted)

| | |
|---|---|
| **Type** | KDM mkey |
| **Filename** | m124_mkey_pict_2K_sync_test_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test (Encrypted)* |
| **Malformations** | The KDM contains a MIC Key for a Picture Track File that does not use a KDM-borne MIC Key. |

## A.6.136. KDM with invalid MIC Key (Picture) for DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)

| | |
|---|---|
| **Type** | KDM mkey |
| **Filename** | m125_bad_mkey_pict_2K_sync_test_mkey_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)* |
| **Malformations** | The MIC Key specified in the KDM does not match the MIC Key used to generate the MIC item in the Picture Track File. |

## A.6.137. KDM for M44 OBAE DCP with HMAC Value error in MXF Track File (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m44_obae_bad_hmac_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *M44 OBAE DCP with HMAC value error in MXF Track File (Encrypted)* |

## A.6.140. KDM for 2K FM Application Constraints (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_constraints_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Application Constraints (OBAE) (Encrypted)* |

## A.6.141. KDM for 2K FM Control Granularity - No FM (OBAE)

| | |
|---|---|
| **Type** | KDM |

| | |
|---|---|
| **Filename** | 2K_fm_control_granularity_no_fm_obae.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Control Granularity - No FM (OBAE) (Encrypted)* |

## A.6.142. KDM for 2K FM Control Granularity - Image Only FM (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_control_granularity_image_only_fm_obae.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Control Granularity - Image Only FM (OBAE) (Encrypted)* |

## A.6.143. KDM for 2K FM Control Granularity - OBAE Only FM (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_control_granularity_obae_only_fm_obae.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Control Granularity - OBAE Only FM (OBAE) (Encrypted)* |

## A.6.144. KDM for 2K FM Control Granularity - Image and OBAE FM (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_control_granularity_image_and_obae_fm_obae.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Control Granularity - Image and OBAE FM (OBAE) (Encrypted)* |

## A.6.145. KDM for 128 Reel Composition, "A" Series (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_128_a_reels_obae_ct.kdm.xml |
| **Description** | KDM that has all content keys for the track files referenced by the CPL, and additionally has one each of key types FMIK, FMAK. The FMIK and FMAK key values shall be appropriate for the specifications of the FM system used by the Test Subject. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *128 Reel Composition, "A" Series (OBAE) (Encrypted)* |

## A.6.146. KDM for 128 Reel Composition, "B" Series (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_StEM_128_b_reels_obae_ct.kdm.xml |
| **Description** | KDM that has all content keys for the track files referenced by the CPL, and additionally has one each of key types FMIK and FMAK. The FMIK and FMAK key values shall be appropriate for the specifications of the FM system used by the Test Subject. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *128 Reel Composition, "B" Series (OBAE) (Encrypted)* |

## A.6.147. KDM for 2K FM Payload (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_payload_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Payload (OBAE) (Encrypted)* |

## A.6.148. KDM for Maximum Bitrate OBAE (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | maximum_bitrate_24Hz_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |

| | |
|---|---|
| **Prerequisites** | *Maximum Bitrate OBAE (Encrypted)* |

## A.6.149. KDM for Maximum Bitrate OBAE 48 fps (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | maximum_bitrate_48Hz_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *Maximum Bitrate OBAE 48 fps (Encrypted)* |

## A.6.150. KDM for 2K FM Payload (plaintext OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_payload_pt_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Payload (plaintext OBAE) (Encrypted)* |

## A.6.151. KDM for 2K FM Payload (OBAE) with FM Bypass (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_fm_bypass_obae_ct.kdm.xml |
| **Description** | KDM with "no FM mark" flag applied to OBAE essence. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *2K FM Payload (OBAE) (Encrypted)* |

## A.6.152. KDM with non-empty NonCriticalExtensions (OBAE)

| | |
|---|---|
| **Type** | KDM |
| | |

| | |
|---|---|
| **Filename** | kdm-with-non-crit-exts-obae.kdm.xml |
| **Description** | KDM with a non-empty NonCriticalExtensions element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |

## A.6.153. KDM with expired Signer certificate (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-expired-signer-obae.kdm.xml |
| **Description** | KDM with an expired Signer's Certificate and an ETM IssueDate later than Signer's Certificate expiry date |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | KDM signer's certificate's Validity "Not After" date is earlier than ETM IssueDate |

## A.6.154. KDM issued before certificate valid (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-issue-before-cert-valid-obae.kdm.xml |
| **Description** | KDM with a valid Signer's Certificate, but ETM issue date before Signer's Certificate issue date |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The <IssueDate> element contains a date prior to the date of the signer certificate's Validity "Not Before" date. |

## A.6.155. KDM validity exceeds signer validity (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-signer-cert-exp-before-kdm-expires-obae.kdm.xml |
| **Description** | KDM with a validity period that extends beyond the validity of Signer's Certificate expiry date. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |

| | |
|---|---|
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The KDM has a ContentKeysNotValidAfter value later than the signer certificate's "Not After" value. |

## A.6.156. KDM with corrupted CipherData block (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-CipherData-block-obae.kdm.xml |
| **Description** | KDM that contains an Invalid Structure ID field in the CipherData element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The first byte of the Structure ID field contained in the <enc:CipherValue> element inside the <enc:CipherData> element has been changed from "F1" to "1F" |

## A.6.157. KDM with incorrect signer thumbprint (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-signer-tp-obae.kdm.xml |
| **Description** | KDM for which the Thumbprint of the Signer's Certificate does not match the Signer of the KDM |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The thumbprint of the signer certificate as listed in the KDM is incorrect and does not match the thumbprint for the issuing certificate. |

## A.6.158. KDM with KeyInfo mismatch (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-bad-keyinfo-obae.kdm.xml |
| **Description** | KeyInfo field of the audio EncryptedKey element does not match the KeyInfo field of the image EncryptedKey element. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |

| | |
|---|---|
| **Malformations** | The KeyInfo element of the audio encrypted key data contains the correct Issuer Name and an incorrect IssuerSerial of the certificate of the recipient of the KDM. |

## A.6.159. KDM with invalid MessageType (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-MessageType-obae.kdm.xml |
| **Description** | KDM with an Invalid MessageType element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | MessageType element contains: "http://www.smpte-qa.org/430-1/2006/KDM#kdm-key-type" |

## A.6.160. KDM with incorrect namespace name value (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-namespace-obae.kdm.xml |
| **Description** | KDM has the wrong namespace name. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The namespace name corresponding to the top level XML element does not match the value given in SMPTE-430-3-2006. The bogus value `http://www.smpte-qa.org/schemas/430-3/2001/ETMshall` be used. |

## A.6.161. KDM without signer certificate (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-chain-obae.kdm.xml |
| **Description** | KDM in which the Certificate chain does not contain the Signer's Certificate |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The certificate that signed the KDM is not included in the KDM. |

## A.6.162. KDM signed with incorrect signer certificate format (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-signer-format-obae.kdm.xml |
| **Description** | KDM which has been signed with a certificate not conforming with SMPTE-430-2-2006. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The certificate that signed the KDM is Interop format. |

## A.6.163. KDM for DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m06b_cpl_hash_error_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)* |

## A.6.164. KDM for DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m07b_cpl_invalid_signature_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)* |

## A.6.165. KDM for DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m13b_cpl_missing_asset_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)* |

## A.6.166. KDM for DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m14b_cpl_format_error_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)* |

## A.6.167. KDM for DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m15b_cpl_signer_format_error_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)* |

## A.6.168. KDM with invalid ContentAuthenticator (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-malf-bad-ContentAuthenticator-obae.kdm.xml |
| **Description** | KDM with an Invalid ContentAuthenticator element |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | the content of the ContentAuthenticator element shall contain a thumbprint of a D-Cinema cert that does not match one in the signer chain of the CPL that the KDM references. |

## A.6.169. KDM for DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m16b_cpl_malf_signer_no_role_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)* |

## A.6.170. KDM for DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m17b_cpl_malf_signer_bad_role_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)* |

## A.6.171. KDM for DCI Malformed Test 18b: KDM for CPL signed with Extra Role Certificate (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | m18b_cpl_malf_signer_extra_role_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI Malformed Test 18b: CPL signed with Extra Role Certificate (OBAE) (Encrypted)* |

## A.6.172. KDM that has recently expired (OBAE)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | kdm-recent-expired_obae.kdm.xml |

| | |
|---|---|
| **Description** | KDM that has a validity period that has expired according to the full ContentKeysNotValidAfter timestamp but that has not expired if the local offset is ignored. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *KDM for 2K StEM (Encrypted) (OBAE)* |
| **Malformations** | The value of the ContentKeysNotValidAfter element is a UTC timestamp between 4 and 6 hours in the past, with a local offset of +06:00. |

## A.6.173. KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_sync_test_with_subs_obae_ct.kdm.xml |
| **Description** | KDM for *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* |

## A.6.174. KDM for DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | frame_num_burn_in_obae_ct.kdm.xml |
| **Description** | KDM for *DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)*. |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |
| **Prerequisites** | *DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)* |

## A.6.175. KDM for 2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)

| | |
|---|---|
| **Type** | KDM |
| **Filename** | 2K_max_bitrate_obae_ct.kdm.xml |
| **Conforms to** | SMPTE-430-1, SMPTE-430-3 |

| | |
|---|---|
| **Prerequisites** | *2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)* |

# Appendix B. Equipment List

## B.1. Hardware

**AES3 Audio Analyzer**
Digital audio signal analyzer with AES-3 inputs.

**Sound System**
5.1 or 7.1 sound system with calibrated level control.

**Computer with POSIX OS**
Computer with POSIX-like Operating System (OS), such as Linux or Mac OS X. The system must support TCP/IP via 1000 Mb/s ethernet and be backward-compatible to support 100 Mb/ s Ethernet.

**Digital Clock**
Digital quartz time-of-day clock displaying time accurate to the second

**Oscilloscope**
Digital storage oscilloscope, 200 MHz or better, with two or more inputs plus external trigger.

**Accurate Real-Time Clock**
A real-time clock that uses an external reference to maintain precise time (within 1 ms). The external reference should be WWV, GPS or NTP traceable to a trusted hardware clock.

**FM Decoder**
Forensic mark decoder for image, sound or OBAE essence. The exact type of decoder is dependent upon the type of watermark to be decoded. This equipment is expected to collect the full payload of the forensic marking system.

**FM Detector**
Forensic mark detector for image or sound essence. The exact type of detector is dependent upon the type of watermark to be detected. This equipment is expected to simply detect the presence of the forensic mark.

**Ethernet Switch**
A 1000Base-T Ethernet switch capable of sustained full-rate throughput on at least two portpairs. The device must also be able to configure one or more ports as "monitor" ports (selected traffic on the switch can be copied to the monitor port to facilitate diagnostic capture).

**Photodiode**
Photodiode, of the type most sensitive in the human visible electromagnetic spectrum (about 390 nm to 780 nm), fitted with suitable length of shielded cable, terminated in a BNC connector.

**Photometer**
Photometer as described in [SMPTE-431-1]

**Spectroradiometer**
Spectroradiometer as described in [SMPTE-431-1].

**Stopwatch**
Digital stopwatch with .01 second resolution.

**Still Camera**
Digital still image camera.

**48 fps Camera**
Camera and recorder/reproducer system capable of 48fps (or better) capture rate.

**SPB-2 Access Tools**
Tools, supplied by the manufacturer of an SPB-2 device, required to gain authorized access to the protected area of the SPB-2.

**D.U.T. Twin**
A device identical to the Device Under Test.

**DCI Projector Pair**
Two DCI-complaint projectors of the same model and revision.

**Dual-Link Monitor**
Dual-link HD monitor.

**Bridge Tap Connector**
Connector with a bridge tap takeoff point, *e.g.* a "BNC Tee".

**GPIO Test Fixture**
A test fixture comprising L.E.D. indicators, switches and a power supply, per the schematic in Appendix E.

**DCI Projector**
DCI-compliant standalone projector.

**DCI Server**
DCI-compliant server (includes Image/Sound Media Block)

**LDB Monitor**
LDB diagnostic utility

**Digital Audio Recorder**
Audio recorder capable of bit-accurate capture of digital audio channels, e.g, AES/EBU channels.

**OBAE Sound System**
Calibrated OBAE reproduction environment and system.

## B.2. Software

**Audio Editor**
A digital audio workstation (DAW), such as Pro Tools or Audacity.

**asm-responder**
Auditorium Security Message (ASM) responder simulator. Allows inspection of ASM communications behavior in a peer device. See Appendix D for more information.

**asm-requester**
Auditorium Security Message (ASM) requester simulator. Allows inspection of ASM communications behavior in a peer device. See Appendix D for more information.

**ftlint**
The ftlint command line utility from the FreeType library.
It is available from http://www.freetype.org/.

**Network Analyzer**
Network analysis tool such as Wireshark or tcpdump.
It is available from http://www.wireshark.org/.

**Text Editor**
Any text editor that can display and write plain text, such as emacs or vi, etc.

**Sound Editor**
Any sound editing software that provides sample-accurate manipulations of audio waveforms.

**OpenJPEG**
JPEG 2000 encoder/decoder software such as OpenJPEG.
It is available from http://www.openjpeg.org/.

**j2c-scan**
JPEG 2000 scanner based on the **OpenJPEG** library. The source code for this program is available in Section C.8.

**identify**

identify is part of the ImageMagick library and utility suite.
It is available from http://www.imagemagick.org/.

**klvwalk**
The klvwalk utility from the free asdcplib software package.
It is available from http://www.cinecert.com/asdcplib/

**asdcp-test**
The asdcp-test utility from the free asdcplib software package.
It is available from http://www.cinecert.com/asdcplib/.

**openssl**
General purpose command line utility from the OpenSSL software package.
It is available from http://www.openssl.org/.

**schema-check**
Validating XML Parser (note: may use parser from Xerces package). The source code for thisprogram is available in Section C.3.
It is available from http://xml.apache.org/security/.

**checksig**
XML Signature validator, distributed with the XML Security library.
It is available from http://xml.apache.org/security/.

**dsig_cert.py**
XML Signature certificate manipulator. The source code for this program is available in Section C.8.

**dsig_extract.py**
XML Signature certificate extractor. The source code for this program is available in Section C.9.

**uuid_check.py**
UUID validator. The source code for this program is available in Section C.7.

**dc-thumbprint**
Certificate thumbprint calculator. The source code for this program is available in Section C.2.

**eab_calc.py**
Delta E*ab Calculator for color accuracy measurements. The source code for this program is available in Section C.6.

**kdm-decrypt**
KDM decryption tool. The source code for this program is available in Section C.4.

[This Page Left Blank Intentionally]

# Appendix C. Source Code

## C.1. Overview

Wherever possible, the computer programs used in the test procedures in this document are freely available. Where appropriate, the listings in Appendix B provide a URL where the software can be obtained.

In some cases, it was necessary to develop programs because free alternatives were not available. Those programs are presented here in source code form along with instructions for building and executing the programs.

The programs are expressed in the C, C++ and Python programming languages. Build instructions and prerequisites for the C and C++ programs are given in the comments at the beginning of each source module. Machine readable copies of the programs are available in the `source-code` directory in the Reference Materials distribution (see Appendix A).

## C.2. dc-thumbprint

This program reads a PEM formatted X509 certificate and calculates a SHA-1 message digest over the signed portion of the certificate as required by [SMPTE-430-2] . The value is encoded as a Base64 string and returned on `stdout`. The following example illustrates this usage:

### Example C.1. dc-thumbprint execution

```
$ dc-thumbprint my-cert.pem
aZMVnZ/TzEvLUCmQFcc8U0je9uo=
```

### C.2.1. dc-thumbprint Source Code Listing

```
/*
 * dc-thumbprint.c -- calculate certificate thumbprint of PEM-encoded
 *                    X.509 document per SMPTE 430-2
 *
 * $Id$
 *
 * This program requires OpenSSL. To build:
 *  $ cc -o dc-thumbprint dc-thumbprint.c -lcrypto
 */

#include <stdio.h>
#include <string.h>
#include <openssl/sha.h>
```

```
#include <openssl/pem.h>
#include <openssl/x509.h>

typedef unsigned char byte_t;

char*
encodeBase64(byte_t* in_buf, int in_len, char* out_buf, size_t out_len)
{
  BIO *bmem, *b64;
  BUF_MEM *bptr;

  b64 = BIO_new(BIO_f_base64());
  bmem = BIO_new(BIO_s_mem());
  b64 = BIO_push(b64, bmem);
  BIO_write(b64, in_buf, in_len);

  if ( BIO_flush(b64) != 1 )
    {
      fprintf(stderr, "write to buffer failed.\n");
      return 0;
    }

  BIO_get_mem_ptr(b64, &bptr);

  if ( bptr->length + 1 > out_len )
    {
      fprintf(stderr, "encoding exceeds buffer length.\n");
      return 0;
    }

  memcpy((byte_t*)out_buf, bptr->data, bptr->length-1);
  out_buf[bptr->length-1] = 0;

  return out_buf;
}


int
main(int argc, char** argv)
{
    byte_t sha_value[20];     /* buffer for resulting thumbprint digest */
    char sha_base64[64];      /* buffer for Base64 version of the thumbprint digest */
    byte_t p_key_buf[8192];   /* buffer holds DER encoded certificate body */
    size_t length;            /* length of DER encoded certificate body (p_key_buf) */
    byte_t* p = p_key_buf;    /* pointer that OpenSSL will move at will */
    SHA_CTX SHA;              /* SHA-1 context for thumbprint */
    FILE* fp;                 /* PEM source file */
    X509* x509obj;            /* X509 object for mangling certificate contents */

    OpenSSL_add_all_digests();

    if ( argc != 2 )
    {
        fprintf(stderr, "USAGE: dc-thumbprint cert-file.pem\n");
        return 1;
    }

    if ( (fp = fopen (argv[1], "r")) == 0 )
    {
        perror("fopen");
        return 2;
    }

    if ( (x509obj = PEM_read_X509(fp, 0, 0, 0)) == 0 )
    {
      fprintf(stderr, "Error decoding file %s\n", argv[1]);
      fclose (fp);
      return 3;
```

```
    }

    fclose (fp);

    /* get the certificate body as a DER string */
    if ( i2d_re_X509_tbs(x509obj, &p) == 0 )
    {
        fprintf(stderr, "i2d_re_X509_tbs error\n");
        return 4;
    }

    length = p - p_key_buf;

    if ( length > 8192 )
    {
        fprintf(stderr, "i2d_re_X509_tbs value exceeds buffer length\n");
        return 5;
    }

  SHA1_Init(&SHA);
  SHA1_Update(&SHA, p_key_buf, length);
  SHA1_Final(sha_value, &SHA);

  if ( encodeBase64(sha_value, 20, sha_base64, 64) == 0 )
    return 6;

  printf("%s\n", sha_base64);
  return 0;
}

/*
 * end dc-thumbprint.c
 */
```

# C.3. schema-check

This program parses and validates XML instance documents. When an XML document is specified alone, the file is checked for well-formedness but is not validated. When an XML document is specified with one or more schema files, **schema-check** validates that file against the schemas. Only one file to be tested may be specified at a time. Note that schema files must be listed in order of dependency (most dependent last). The following example illustrates using the program to check well-formedness:

## Example C.2. Using schema-check to check well-formedness

```
$ schema-check perfect-movie.cpl.xml
```

The next example shows how to use the program to check for valid content:

## Example C.3. Using schema-check to check validity

```
$ schema-check perfect-movie.cpl.xml SMPTE-428-7.xsd
```

## C.3.1. schema-check Source Code Listing

```
//
// schema-check.cpp -- test XML document against schema
//
// $Id$
//
// This program requires the Xerces-c XML library. To build:
//  $ c++ -o schema-check schema-check.cpp -lxerces-c
//

#include <iostream>
#include <list>
#include <string>
#include <cstdio>

#include <xercesc/util/OutOfMemoryException.hpp>
#include <xercesc/dom/DOM.hpp>
#include <xercesc/parsers/XercesDOMParser.hpp>
#include <xercesc/framework/XMLGrammarDescription.hpp>
#include <xercesc/sax/ErrorHandler.hpp>
#include <xercesc/sax/SAXParseException.hpp>

using std::cerr;
using std::endl;
XERCES_CPP_NAMESPACE_USE

// ---------------------------------------------------------------------------
// Utility  code adapted from the DOMPrint program distributed with Xerces-c

// simple transcoding wrapper
class StrX
{
  char*   fLocalForm;

public :
  StrX(const XMLCh* const toTranscode) { fLocalForm = XMLString::transcode(toTranscode); }
  ~StrX() { XMLString::release(&fLocalForm); }
  const char* localForm() const { return fLocalForm; }
};

std::ostream&
operator<<(std::ostream& target, const StrX& toDump)
{
  target << toDump.localForm();
  return target;
}

// error handler interface
class DOMTreeErrorReporter : public ErrorHandler
{
public:
  void warning(const SAXParseException& toCatch) {}
  void resetErrors() {}

  void error(const SAXParseException& toCatch) {
    cerr << "Error at file \"" << StrX(toCatch.getSystemId())
         << "\", line " << toCatch.getLineNumber()
         << ", column " << toCatch.getColumnNumber() << endl
         << "   Message: " << StrX(toCatch.getMessage()) << endl;
  }
```

```
  void fatalError(const SAXParseException& toCatch) {
    cerr << "Fatal Error at file \"" << StrX(toCatch.getSystemId())
         << "\", line " << toCatch.getLineNumber()
         << ", column " << toCatch.getColumnNumber() << endl
         << "   Message: " << StrX(toCatch.getMessage()) << endl;
  }
};

// ---------------------------------------------------------------------------

int
main(int argc, const char** argv)
{
  try
    {
      XMLPlatformUtils::Initialize();
    }
  catch(const XMLException& e)
    {
      StrX tmp_e(e.getMessage());
      cerr << "Xerces initialization error: " << tmp_e.localForm() << endl;
      return 2;
    }

  // check command line for arguments
  if ( argc < 2 )
    {
      cerr << "usage: schema-check <xml-file> [<schema-file> ...]" << endl;
      return 3;
    }

  for ( int i = 1; i < argc; i++ )
    {
      FILE *f = fopen(argv[i], "r");
      if ( f == 0 )
        {
          perror(argv[i]);
          return 4;
        }
    }

  XercesDOMParser *parser = new XercesDOMParser;
  DOMTreeErrorReporter *errReporter = new DOMTreeErrorReporter();
  parser->setErrorHandler(errReporter);

  parser->setDoNamespaces(true);
  parser->setCreateEntityReferenceNodes(true);
  parser->useCachedGrammarInParse(true);

  if ( argc > 2 )
    {
      parser->setDoSchema(true);
      parser->setValidationScheme(AbstractDOMParser::Val_Always);
      parser->setValidationSchemaFullChecking(true);

      for ( int i = 2; i < argc; i++ )
        {
          if ( parser->loadGrammar(argv[i], Grammar::SchemaGrammarType, true) == 0 )
            {
              cerr << "Error loading grammar " << std::string(argv[i]) << endl;
              return 4;
            }
        }
    }

  bool errorsOccured = true;
  try
    {
```

```
      parser->parse(argv[1]);
      errorsOccured = false;
    }
  catch ( const OutOfMemoryException& )
    {
      cerr << "Out of memory exception." << endl;
    }
  catch ( const XMLException& e )
    {
      cerr << "An error occurred during parsing" << endl
           << "   Message: " << StrX(e.getMessage()) << endl;
    }
  catch ( const DOMException& e )
    {
      const unsigned int maxChars = 2047;
      XMLCh errText[maxChars + 1];

      cerr << endl
           << "A DOM error occurred during parsing: '" << std::string(argv[1]) << "'" << endl
           << "DOM Exception code:  " << e.code << endl;

      if ( DOMImplementation::loadDOMExceptionMsg(e.code, errText, maxChars) )
        cerr << "Message is: " << StrX(errText) << endl;
    }
  catch (...)
    {
      cerr << "An unclassified error occurred during parsing." << endl;
    }

  return errorsOccured ? 1 : 0;
}

//
// end schema-check.cpp
//
```

## C.4. kdm-decrypt

This program reads a KDM and an RSA private key in PEM format and decrypts the EncryptedKey elements in the KDM. The decrypted key blocks are printed to `stdout`. Note that key blocks in the KDM must have been encrypted using the public key which corresponds to the RSA key given as the second argument to this program.

### Example C.4. kdm-decrypt execution

```
$ kdm-decrypt test_file.kdm.xml my_id_key.pem
        CipherDataID: f1dc124460169a0e85bc300642f866ab
SignerThumbprint: q5Oqr6GkfG6W2HzcBTee5m0Qjzw=
          CPL Id: 119d8990-2e55-4114-80a2-e53f3403118d
          Key Id: b6276c4b-b832-4984-aab6-250c9e4f9138
        Key Type: MDIK
      Not Before: 2007-09-20T03:24:53-00:00
        Not After: 2007-10-20T03:24:53-00:00
          Key Data: 7f2f711f1b4d44b83e1dd1bf90dc7d8c
```

## C.4.1. kdm-decrypt Source Code Listing

```
//
// kdm-decrypt.cpp -- decrypt and display KDM EncryptedKey elements
//
// $Id$
//
// This program requires the Xerces-c XML, XMLSecurity, OpenSSL
// and asdcplib libraries. To build:
//
// c++ -o kdm-decrypt kdm-decrypt.cpp
//     -lxerces-c -lxml-security-c -lkumu -lcrypto
//

#include <KM_util.h>
#include <KM_fileio.h>
#include <ctype.h>
#include <iostream>
#include <string>
#include <openssl/pem.h>
#include <xercesc/util/OutOfMemoryException.hpp>
#include <xercesc/parsers/XercesDOMParser.hpp>
#include <xercesc/framework/MemBufInputSource.hpp>
#include <xsec/framework/XSECProvider.hpp>
#include <xsec/framework/XSECException.hpp>
#include <xsec/enc/XSECCryptoException.hpp>
#include <xsec/enc/OpenSSL/OpenSSLCryptoKeyRSA.hpp>

XERCES_CPP_NAMESPACE_USE
using std::cout;
using std::cerr;
using std::endl;
using namespace Kumu;

const size_t KeyType_Length = 4;
const size_t DateTime_Length = 25;
const ui32_t X509Thumbprint_Length = 20;

// A structure to hold key block data retrieved during a decrypt operation.
struct S430_2_KeyBlock
{
  byte_t CipherDataID[UUID_Length];
  byte_t SignerThumbprint[X509Thumbprint_Length];
  byte_t CPLId[UUID_Length];
  byte_t KeyType[KeyType_Length];
  byte_t KeyId[UUID_Length];
  byte_t NotBefore[DateTime_Length];
  byte_t NotAfter[DateTime_Length];
  byte_t KeyData[SymmetricKey_Length];

  S430_2_KeyBlock() {
    memset(this, 0, sizeof(S430_2_KeyBlock));
  }

  std::string Dump() const;
};

std::string safe_char(char c) {
  char b[2] = {'*', 0};
  if ( isprint(c) ) b[0] = c;
  return b;
}
```

```
// Pretty-print key block data.
std::string
S430_2_KeyBlock::Dump() const
{
  using std::string;
  Kumu::Identifier<X509Thumbprint_Length> TmpThumbprint;
  UUID   TmpUUID;
  char   tmp_buf[64];
  string out_string;

  bin2hex(CipherDataID, UUID_Length, tmp_buf, 64);
  out_string = "    CipherDataID: " + string(tmp_buf);
  TmpThumbprint.Set(SignerThumbprint);
  out_string += "\nSignerThumbprint: " + string(TmpThumbprint.EncodeBase64(tmp_buf, 64));
  TmpUUID.Set(CPLId);
  out_string += "\n          CPL Id: " + string(TmpUUID.EncodeHex(tmp_buf, 64));
  TmpUUID.Set(KeyId);
  out_string += "\n          Key Id: " + string(TmpUUID.EncodeHex(tmp_buf, 64));
  out_string += "\n        Key Type: "
    + safe_char(KeyType[0]) + safe_char(KeyType[1])
    + safe_char(KeyType[2]) + safe_char(KeyType[3]);
  assert(DateTime_Length<64);
  tmp_buf[DateTime_Length] = 0;
  memcpy(tmp_buf, NotBefore, DateTime_Length);
  out_string += "\n      Not Before: " + string(tmp_buf);
  memcpy(tmp_buf, NotAfter, DateTime_Length);
  out_string += "\n       Not After: " + string(tmp_buf);
  bin2hex(KeyData, UUID_Length, tmp_buf, 64);
  out_string += "\n        Key Data: " + string(tmp_buf);
  out_string += "\n";
  return out_string;
}

// Given a KDM string and a parsed RSA key, decrypt the key blocks
// in the KDM and print them to stdout.
int
decrypt_kdm(const std::string& KDMDocument, EVP_PKEY* Target)
{
  assert(Target);

  XercesDOMParser* parser = new XercesDOMParser;
  parser->setDoNamespaces(true);
  parser->setCreateEntityReferenceNodes(true);

  try
    {
      MemBufInputSource xmlSource(reinterpret_cast<const XMLByte*>(KDMDocument.c_str()),
                                  static_cast<XMLSize_t>(KDMDocument.length()),
                                  "pidc_rules_file");
      parser->parse(xmlSource);
      int errorCount = parser->getErrorCount();
      if ( errorCount > 0 )
        {
          cerr << "XML parse errors: " << errorCount << endl;
          return -1;
        }
    }
  catch ( const OutOfMemoryException& )
    {
      cerr << "Out of memory exception." << endl;
    }
  catch ( const XMLException& e )
    {
      char* emsg = XMLString::transcode(e.getMessage());
      cerr << "An error occurred during parsing" << endl
           << "   Message: " << emsg << endl;
          XSEC_RELEASE_XMLCH(emsg);
```

```
  }
catch ( const DOMException& e )
  {
    const unsigned int maxChars = 2047;
    XMLCh errText[maxChars + 1];

    cerr << endl
         << "DOM Exception code is:  " << e.code << endl;

    if ( DOMImplementation::loadDOMExceptionMsg(e.code, errText, maxChars) )
      {
        char* emsg = XMLString::transcode(errText);
        cerr << "Message is: " << emsg << endl;
        XSEC_RELEASE_XMLCH(emsg);
      }
  }
catch (...)
  {
    cerr << "Unexpected XML parser error." << endl;
  }

try
  {
    XSECProvider prov;
    OpenSSLCryptoKeyRSA* PrivateKey = new OpenSSLCryptoKeyRSA(Target);
    if ( PrivateKey == 0 )
      {
        cerr << "Error reading private key" << endl;
        return -1;
      }

    DOMDocument* doc = parser->getDocument();
    assert(doc);
    XENCCipher* cipher = prov.newCipher(doc);
    cipher->setKEK(PrivateKey);

    DOMNodeIterator* Iter =
      ((DOMDocumentTraversal*)doc)->createNodeIterator(doc,
                                                       (DOMNodeFilter::SHOW_ELEMENT),
                                                       0,  false);
    assert(Iter);
    DOMNode* Node;
    int keys_accepted = 0;
    int key_nodes_found = 0;

    while ( (Node = Iter->nextNode()) != 0 )
      {
        char* n = XMLString::transcode(Node->getLocalName());
        if ( n == 0 ) continue;

        if ( strcmp(n, "EncryptedKey") == 0 )
          {
            key_nodes_found++;
            S430_2_KeyBlock CipherData;
            ui32_t decrypt_len =
              cipher->decryptKey((DOMElement*)Node,
                                 (byte_t*)&CipherData, sizeof(CipherData));

            if ( decrypt_len == sizeof(CipherData) )
              {
                keys_accepted++;
                cout << CipherData.Dump();
              }
            else if ( decrypt_len > 0 )
              cerr << "Unexpected cipher block length: " << decrypt_len << endl;
            else
              cerr << "Error decoding key block: " << key_nodes_found << endl;
          }
```

```
        XSEC_RELEASE_XMLCH(n);
      }

    Iter->release();
  }
 catch (XSECException &e)
  {
    char* emsg = XMLString::transcode(e.getMsg());
    cerr << "Key decryption error: " << emsg << endl;
    XSEC_RELEASE_XMLCH(emsg);
    return -1;
  }
 catch (XSECCryptoException &e)
  {
    cerr << "Crypto error: " << e.getMsg() << endl;
    return -1;
  }
 catch (...)
  {
    cerr << "Unexpected decryption error." << endl;
  }

 delete parser;
 return 0;
}

//
int
main(int argc, const char** argv)
{
 if ( argc < 3 )
  {
    cerr << "USAGE: kdm-decrypt <kdm-file> <RSA-PEM-file>" << endl;
    return 2;
  }

 try
  {
    XMLPlatformUtils::Initialize();
    XSECPlatformUtils::Initialise();
  }
 catch(const XMLException& e)
  {
    char* emsg = XMLString::transcode(e.getMessage());
    cerr << "Xerces or XMLSecurity initialization error: " << emsg << endl;
    XSEC_RELEASE_XMLCH(emsg);
    return 3;
  }
 catch (...)
  {
    cerr << "Unexpected Xerces or XMLSecurity initialization error." << endl;
  }

 FILE* fp = fopen (argv[2], "r");
 if ( fp == 0 )
  {
    perror(argv[2]);
    return 4;
  }

 EVP_PKEY* Target = PEM_read_PrivateKey(fp, 0, 0, 0);
 fclose(fp);

 if ( Target == 0 )
  {
    cerr << "Error reading RSA key in file " << std::string(argv[2]) << endl;
    return 5;
```

```
    }

  std::string XML_doc;
  Result_t result = ReadFileIntoString(argv[1], XML_doc);
  if ( KM_FAILURE(result) )
    {
      cerr << "Error reading XML file " << std::string(argv[1]) << endl;
      return 6;
    }

  if ( decrypt_kdm(XML_doc, Target) != 0 )
    return 1;

  return 0;
}

//
// end kdm-decrypt.cpp
//
```

## C.5. j2c-scan

This program reads a JPEG 2000 codestream from a file and produces parametric data on the standard output. The following example illustrates this usage:

### Example C.5. j2c-scan execution

```
$ j2c-scan test_frame_000002.j2c
coding parameters
  digital cinema profile: none
  rsiz capabilities: standard
  pixel offset from top-left corner: (0, 0)
  tile width/height in pixels: (2048, 1080)
  image width/height in tiles: (1, 1)
  tile #1
    coding style: 1
    progression order: Component-Position-Resolution-Layer
    POC marker flag: 0
    number of quality layers: 1
      rate for layer #1: 0.0
    multi-component transform flag: 1
    component #1
      coding style: 1
      number of resolutions: 6
      code block width/height: (5, 5)
      code block coding style: 0
      discrete wavelet transform identifier: 0
      quantization style: 2
      number of guard bits: 1
      step size pairs: 16
      region of interest shift: 0
    component #2
      coding style: 1
      number of resolutions: 6
      code block width/height: (5, 5)
      code block coding style: 0
      discrete wavelet transform identifier: 0
      quantization style: 2
      number of guard bits: 1
```

```
      step size pairs: 16
      region of interest shift: 0
    component #3
      coding style: 1
      number of resolutions: 6
      code block width/height: (5, 5)
      code block coding style: 0
      discrete wavelet transform identifier: 0
      quantization style: 2
      number of guard bits: 1
      step size pairs: 16
      region of interest shift: 0
```

## C.5.1. j2c-scan Source Code Listing

```
/*
 * j2c-scan.cpp -- parse j2c file and display data concerning it
 *
 * $Id$
 *
 * This program requires version 1.5.2 of the OpenJPEG
 * library. Furthermore, it requires the header files "openjpeg.h" and
 * "j2k.h" from its source distribution. Copy these headers to your
 * build directory. After doing so, execute the following to build:
 *  $ c++ -o j2c-scan j2c-scan.cpp -lopenjpeg
 */

#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include "openjpeg.h"
#include "j2k.h"

static void
j2k_dump_cp (opj_image_t * image, opj_cp_t * cp)
{
  const char *s;
  int i, j;
  int step_size_pairs;
  printf ("coding parameters\n");
  if (cp->comment != NULL)
    {
      printf ("  coding comment: %p\n", cp->comment);
    }
  switch (cp->cinema)
    {
    case OFF:      s = "none";      break;
    case CINEMA2K_24:      s = "2k @ 24 fps";      break;
    case CINEMA2K_48:      s = "2k @ 48 fps";      break;
    case CINEMA4K_24:      s = "4k @ 24 fps";      break;
    default:      s = "unknown";      break;
    }
  printf ("  digital cinema profile: %s\n", s);
  switch (cp->rsiz)
    {
    case STD_RSIZ:      s = "standard";      break;
    case CINEMA2K:      s = "2k digital cinema";      break;
    case CINEMA4K:      s = "4k digital cinema";      break;
    default:      s = "unknown";      break;
    }
  printf ("  rsiz capabilities: %s\n", s);
  printf ("  pixel offset from top-left corner: (%d, %d)\n", cp->tx0,
```

```
          cp->ty0);
  printf ("  tile width/height in pixels: (%d, %d)\n", cp->tdx, cp->tdy);
  printf ("  image width/height in tiles: (%d, %d)\n", cp->tw, cp->th);
  for (i = 0; i < cp->tw * cp->th; i++)
    {
      printf ("  tile #%d\n", i + 1);
      printf ("    coding style: %x\n", cp->tcps[i].csty);
      switch (cp->tcps[i].prg)
        {
        case LRCP:        s = "Layer-Resolution-Component-Position";      break;
        case RLCP:        s = "Resolution-Layer-Component-Position";      break;
        case RPCL:        s = "Resolution-Position-Component-Layer";      break;
        case PCRL:        s = "Position-Component-Resolution-Layer";      break;
        case CPRL:        s = "Component-Position-Resolution-Layer";      break;
        default:          s = "unknown";          break;
        }
      printf ("    progression order: %s\n", s);
      printf ("    POC marker flag: %d\n", cp->tcps[i].POC);
      printf ("    number of quality layers: %d\n", cp->tcps[i].numlayers);
      for (j = 0; j < cp->tcps[i].numlayers; j++)
        {
          printf ("      rate for layer #%d: %.1f\n", j + 1,
                  cp->tcps[i].rates[j]);
        }
      printf ("    multi-component transform flag: %d\n", cp->tcps[i].mct);
      for (j = 0; j < image->numcomps; j++)
        {
          printf ("    component #%d\n", j + 1);
          printf ("      coding style: %x\n", cp->tcps[i].tccps[j].csty);
          printf ("      number of resolutions: %d\n",
                  cp->tcps[i].tccps[j].numresolutions);
          printf ("      code block width/height: (%d, %d)\n",
                  cp->tcps[i].tccps[j].cblkw, cp->tcps[i].tccps[j].cblkh);
          printf ("      code block coding style: %x\n",
                  cp->tcps[i].tccps[j].cblksty);
          printf ("      discrete wavelet transform identifier: %d\n",
                  cp->tcps[i].tccps[j].qmfbid);
          printf ("      quantization style: %d\n",
                  cp->tcps[i].tccps[j].qntsty);
          printf ("      number of guard bits: %d\n",
                  cp->tcps[i].tccps[j].numgbits);
          step_size_pairs =
            (cp->tcps[i].tccps[j].qntsty ==
             J2K_CCP_QNTSTY_SIQNT) ? 1 : cp->tcps[i].tccps[j].numresolutions *
            3 - 2;
          printf ("      step size pairs: %d\n", step_size_pairs);
          printf ("      region of interest shift: %d\n",
                  cp->tcps[i].tccps[j].roishift);
        }
    }
}

void
error_callback (const char *msg, void *client_data)
{
  FILE *stream = (FILE *) client_data;
  fprintf (stream, "[ERROR] %s", msg);
}

void
warning_callback (const char *msg, void *client_data)
{
  FILE *stream = (FILE *) client_data;
  fprintf (stream, "[WARNING] %s", msg);
}


int
```

```
main (int argc, char *argv[])
{
  char *filename;               /* name of the file to process */
  FILE *fp;                     /* input file pointer */
  int file_length;              /* length of the input file */
  unsigned char *buffer = NULL; /* in-memory buffer containing the input file */
  opj_cio_t *cio = NULL;        /* OpenJPEG wrapper around file buffer */
  opj_dparameters_t parameters; /* decompression parameters */
  opj_dinfo_t *dinfo = NULL;    /* pointer to a JPEG-2000 decompressor */
  opj_event_mgr_t event_mgr;    /* manager of events' callback functions */
  opj_image_t *image = NULL;    /* pointer to the decoded image */

  memset (&event_mgr, 0, sizeof (opj_event_mgr_t));
  event_mgr.error_handler = error_callback;
  event_mgr.warning_handler = warning_callback;
  event_mgr.info_handler = NULL;

  /* establish default decoding parameters for JPEG-2000 codestreams */
  opj_set_default_decoder_parameters (&parameters);
  parameters.decod_format = 0;

  if (argc != 2)
    {
      fprintf (stderr, "USAGE: j2c-scan file.j2c\n");
      return 1;
    }
  filename = argv[1];
  strncpy (parameters.infile, filename, sizeof (parameters.infile) - 1);

  /* read the input file and put it in memory */
  fp = fopen (parameters.infile, "rb");
  if (fp == NULL)
    {
      perror ("fopen");
      return 2;
    }
  fseek (fp, 0, SEEK_END);
  file_length = (int) ftell (fp);
  fseek (fp, 0, SEEK_SET);
  buffer = (unsigned char *) malloc (file_length);
  fread (buffer, sizeof (unsigned char), file_length, fp);
  fclose (fp);

  /* decode the JPEG-2000 codestream */
  dinfo = opj_create_decompress (CODEC_J2K);
  opj_set_event_mgr ((opj_common_ptr) dinfo, &event_mgr, stderr);
  opj_setup_decoder (dinfo, &parameters);
  cio = opj_cio_open ((opj_common_ptr) dinfo, buffer, file_length);
  image = opj_decode (dinfo, cio);
  if (image == NULL)
    {
      fprintf (stderr, "ERROR -> j2c-scan: failed to decode image!\n");
      opj_destroy_decompress (dinfo);
      opj_cio_close (cio);
      free (buffer);
      return 1;
    }
  opj_cio_close (cio);
  free (buffer);

  /* display information about the image */
  j2k_dump_cp (image, ((opj_j2k_t *) dinfo->j2k_handle)->cp);

  /* free the memory */
  opj_destroy_decompress (dinfo);
  opj_image_destroy (image);
```

```
  return 0;
}
```

## C.6. eab_calc.py

This program reads a measured set of xyY values and a set of reference values and calculates the Delta E*ab value of the two. This calculation is required to perform the test in Section 7.5.12. The following example illustrates this usage:

### Example C.6. eab_calc.py execution

```
$ eab_calc.py 0.2650 0.6900 34.64 0.2719 0.6835 34.64
L=88.0 a*=-110.2 b*=106.1
L=88.0 a*=-106.2 b*=106.0
DeltaE=4.0
```

## C.6.1. eab_calc.py Source Code Listing

```
#!/usr/bin/env python
#
# eab_calc.py -- Calculate Delta E*ab from xyY inputs.
#                Adapted from the examples in SMPTE EG432-1.
#
# $Id$
#
from __future__ import print_function

import sys

reference = ((0.6800, 0.3200, 10.06),
             (0.2650, 0.6900, 34.64),
             (0.1500, 0.0600, 3.31),
             (0.2048, 0.3602, 37.94),
             (0.3424, 0.1544, 13.36),
             (0.4248, 0.5476, 44.69),
             (0.5980, 0.3269, 10.06),
             (0.2884, 0.5282, 34.64),
             (0.1664, 0.0891, 3.31),
             (0.2409, 0.3572, 37.19),
             (0.3382, 0.1838, 13.36),
             (0.3973, 0.4989, 42.46),
             )

# Simplified operation: fill in "measured" table
# and call without arguments.
measured = ((0.6767, 0.3201, 9.912),
            (0.2694, 0.6836, 33.930),
            (0.1511, 0.0621, 3.422),
            (0.2037, 0.3578, 36.920),
            (0.3407, 0.1546, 13.180),
            (0.4223, 0.5473, 43.490),
            (0.5963, 0.3264, 9.848),
            (0.2861, 0.5280, 33.580),
            (0.1671, 0.0897, 3.323),
```

```
            (0.2392, 0.3551, 36.170),
            (0.3365, 0.1828, 13.110),
            (0.3953, 0.4983, 41.300)
            )

_Xwhite = 42.940 # d-cinema reference white constants
_Ywhite = 48.0
_Zwhite = 45.812

def _Lab_f1(measured, white_ref):
    q = measured / white_ref
    if q > 0.008856:
        return pow(q, 1.0/3.0)
    return (1.0 / 3.0) * pow(29.0 / 6.0, 2) * q + (4.0 / 29.0)

class Lab_set:
    def init_with_xyY(self, x, y, Y):
        X = ( x / y ) * Y
        z = 1 - x - y
        Z = ( z / y ) * Y
        return self.init_with_XYZ(X,Y,Z)

    def init_with_XYZ(self, X, Y, Z):
        Yratio = _Lab_f1(Y, _Ywhite);
        self.L = 116.0 * Yratio - 16;
        self.a = 500.0 * ( _Lab_f1(X, _Xwhite) - Yratio );
        self.b = 200.0 * ( Yratio - _Lab_f1(Z, _Zwhite) );
        return self

    def calc_DeltaE(self, rhs):
        sum = pow(self.L - rhs.L, 2)
        sum += pow(self.a - rhs.a, 2)
        sum += pow(self.b - rhs.b, 2);
        return pow(sum, 0.5);

    def __repr__(self):
        return "L=%.1f a*=%.1f b*=%.1f" % (self.L, self.a, self.b)


if __name__ == "__main__":
    if len(sys.argv) == 1:
        for i in range(12):
            measured_data = Lab_set().init_with_xyY(*measured[i])
            reference_data = Lab_set().init_with_xyY(*reference[i])
            print(" measured: %s %s" % (measured[i], measured_data))
            print("reference: %s %s" % (reference[i], reference_data))
            print("DeltaE=%.1f" % (reference_data.calc_DeltaE(measured_data)))
        sys.exit(0)

    elif len(sys.argv) != 7:
        sys.stderr.write("usage: Eab_calc <x-m> <y-m> <Y-m> <x-ref> <y-ref> <Y-ref>\n")
        sys.exit(1)

    measured_data = Lab_set().init_with_xyY(float(sys.argv[1]),
                                            float(sys.argv[2]),
                                            float(sys.argv[3]))

    reference_data = Lab_set().init_with_xyY(float(sys.argv[4]),
                                             float(sys.argv[5]),
                                             float(sys.argv[6]))

    print(" measured: %s" % (measured_data))
    print("reference: %s" % (reference_data))
    print("DeltaE=%.1f" % (reference_data.calc_DeltaE(measured_data)))

#
# end eab_calc.py
#
```

## C.7. uuid_check.py

This program reads one or more XML files containing d-cinema metadata and tests each of the UUID values for compliance with [RFC-4122]. The program will emit a message on `stderr` for each malformed UUID that is encountered. The following example illustrates this usage for a KDM file:

### Example C.7. uuid_check.py execution

```
$ uuid_check.py Example.kdm.xml
UUID: 7556bff9-58f9-4320-bb1f-fb594219a957
UUID: bdb3a717-5062-4822-8dfc-0dc6570cc116
UUID: 71f7926e-8ce6-4763-b14b-0ef7dcd952f5
UUID: 6083adad-472c-43da-b131-c6dc601cd154
UUID: aeaae312-a257-11da-a601-8b319b685f8e
```

## C.7.1. uuid_check Source Code Listing

```
#!/usr/bin/env python
#
# uuid_check.py -- Scan an XML file and see that all UUID values
#                  conform to RFC-4122
#
# $Id$
#
from __future__ import print_function

import sys, re

# regular expressions for use below
urn_uuid_re = re.compile('urn:uuid:([^<]*)')
uuid_re = re.compile('^[0-9a-f]{8}-[0-9a-f]{4}-\
([1-5])[0-9a-f]{3}-[8-9a-b][0-9a-f]{3}-[0-9a-f]{12}$', re.IGNORECASE)

#
def uuid_scan(text):
    uuid_list = []
    while text:
        match = urn_uuid_re.search(text)
        if not match: break

        uuid_val = match.group(1)
        text = text[match.end():]

        match = uuid_re.match(uuid_val)
        if not match:
            sys.stderr.write("urn:uuid: value is not an RFC-4122 UUID: %s\n" % (uuid_val))
            continue

        type = int(match.group(1)[0])
        if type not in (1, 4, 5):
            sys.stderr.write("Unexpected UUID type: %d for value %s\n" % (type, uuid_val))

        uuid_list.append(uuid_val)
```

```
    return uuid_list

#
#
if len(sys.argv) < 2:
    sys.stderr.write("usage: uuid_check.py <xml-file> [...]\n")
    sys.exit(1)

for filename in sys.argv[1:]:
    try:
        handle = open(filename)
        text = handle.read()
        handle.close()

    except Exception as e:
        print("{0}: {1}".format(filename, e))

    else:
        for uuid in uuid_scan(text):
            print("UUID: {0}".format(uuid))

#
# end uuid_check.py
#
```

# C.8. dsig_cert.py

This program reads a signed XML file and re-writes the file to the standard output using the certificate order expected by the **checksig** program from the XML Security package. The following example illustrates this usage for a KDM file:

### Example C.8. dsig_cert.py execution

```
$ dsig_cert.py test-kdm.xml >tmp.xml
$ checksig tmp.xml
Signature verified OK!
```

## C.8.1. dsig_cert.py Source Code Listing

```
#!/usr/bin/env python
#
# dsig_cert.py -- Re-order certificates in an XML signature
#
# NOTE: This program requires Python 2.7 or greater
#
# $Id$
#
from __future__ import print_function

import sys, re
from subprocess import Popen, PIPE

# regular expressions for use below
```

```
SignatureValue_end_re = re.compile('</(?:[\w\-]+:)?SignatureValue[^>]*>')
X509Data_re = re.compile('<(?:[\w\-]+:)X509Data[^>]*>(.*?)</(?:[\w\-]+:)X509Data\s*>\s+',
                         re.DOTALL)
X509Certificate_re = re.compile('X509Certificate[^>]*>(.*?)</', re.DOTALL)
dnQualifier_re = re.compile('dnQualifier=([\\w+/]+=)')

#
def get_dnq_type(pem_text, type):
    """Extract the dnQualifier value for the given certificate and common name."""
    handle = Popen(('/usr/bin/openssl', 'x509', '-noout', '-'+type),
                   stdin=PIPE, stdout=PIPE, close_fds=True)

    handle.stdin.write(pem_text)
    handle.stdin.close()
    name_text = handle.stdout.read()
    handle.wait()

    if handle.returncode != 0:
        raise Exception("No X509Certificate element in {0}".format(pem_text))

    dnq = dnQualifier_re.search(name_text.replace('\\', ''))
    if not dnq:
        raise Exception("Error retrieving dnQualifier from {0}.".format(type))

    return dnq.group(1)

#
def PEMify(base64_text):
    """ create canonical PEM lines from any base64 input"""
    in_text = re.sub('[\r\n]', '', base64_text)
    idx = 0
    end = len(in_text)
    retval = ''
    while idx < end:
        retval += in_text[idx:idx+64] + '\n'
        idx += 64

    return retval

#
class dsig_certificate_set:
    """An object for manipulating XML Signature certificates."""
    def __init__(self, xml_doc):
        """Initialize with a signed XML document string."""
        body_end = SignatureValue_end_re.search(xml_doc)

        if not body_end:
            raise Exception("Document does not contain a SignatureValue element.")

        self.kdm_head = xml_doc[:body_end.end()]
        xml_doc = xml_doc[body_end.end():]
        self.X509Data_list = []

        x509_data = X509Data_re.search(xml_doc)
        if x509_data:
            self.kdm_head += xml_doc[:x509_data.start()]

        while x509_data:
            x509_text = xml_doc[x509_data.start():x509_data.end()]
            self.X509Data_list.append({ 'text': x509_text })
            xml_doc = xml_doc[x509_data.end():]
            x509_data = X509Data_re.search(xml_doc)

        self.kdm_tail = xml_doc

        for x509_data in self.X509Data_list:
            # extract the certificate
            cert = X509Certificate_re.search(x509_data['text'])
```

```
            if not cert:
                raise Exception("No X509Certificate element in {0}".format(x509_data['text']))

            cert = PEMify(cert.group(1))
            cert = "-----BEGIN CERTIFICATE-----\n%s-----END CERTIFICATE-----\n" % (cert)

            x509_data['subject_dnq'] = get_dnq_type(cert, 'subject')
            x509_data['issuer_dnq'] = get_dnq_type(cert, 'issuer')
            x509_data['pem_cert'] = cert

    def order_by_dnq(self):
        """Arrange certificates in leaf-root order."""
        root = None
        issuer_map = {}

        for x509_data in self.X509Data_list:
            if x509_data['subject_dnq'] == x509_data['issuer_dnq']:
                if root:
                    raise Exception("Certificate list contains multiple roots.")
                root = x509_data
            else:
                issuer_map[x509_data['issuer_dnq']] = x509_data

        if not root:
            raise Exception("Self-signed root certificate not found.")

        tmp_list = [root];
        try:
            key = tmp_list[-1]['subject_dnq']
            next = issuer_map[key]
            while next:
                tmp_list.append(next)
                key = tmp_list[-1]['subject_dnq']
                next = issuer_map[key]
        except:
            pass

        if len(self.X509Data_list) != len(tmp_list):
            raise Exception("Certificates do not form a complete chain.")

        tmp_list.reverse()
        self.X509Data_list = tmp_list
        return self

    def write_certs(self, prefix='cert_set_'):
        """Write PEMcertificates to files using the optional filename prefix value."""
        count = 1
        for x509_data in self.X509Data_list:
            filename = "%s%d.pem" % (prefix, count)
            handle = open(filename, 'w')
            handle.write(x509_data['pem_cert'])
            handle.close()
            count += 1

    def __repr__(self):
        cert_text = ''
        for cert in self.X509Data_list:
            cert_text += cert['text']

        return self.kdm_head + cert_text + self.kdm_tail

#
if __name__ == '__main__':
    if len(sys.argv) < 2:
        sys.stderr.write("usage: dsig_cert.py <xml-file>\n")
        sys.exit(1)

    try:
```

```
        handle = open(sys.argv[1])
        text = handle.read()
        handle.close()

        cert_set = dsig_certificate_set(text)
        cert_set.order_by_dnq()
        print(cert_set)
    except Exception as e:
        print(e)

#
# end dsig_cert.py
#
```

# C.9. dsig_extract.py

This program reads a signed XML file and writes the certificates contained within to individual PEM files. As shown below, the `-p` option can be used to provide a prefix for the automatically-generated filenames. In this example, the input document contained four certificates.

### Example C.9. dsig_extract.py execution

```
$ dsig_extract.py -p my_prefix_ test-kdm.xml
$ ls my_prefix_*
my_prefix_1.pem
my_prefix_2.pem
my_prefix_3.pem
my_prefix_4.pem
```

## C.9.1. dsig_extract.py Source Code Listing

```
#!/usr/bin/env python
#
# dsig_extract.py -- Extract certificates from an XML signature
#
# $Id$
#
from __future__ import print_function

from dsig_cert import dsig_certificate_set
import sys

prefix = 'xmldsig_cert_'
filename = None

def usage():
    sys.stderr.write("usage: dsig_extract.py [-p <prefix>] <xml-file>\n")
    sys.exit(1)

if len(sys.argv) < 2:
    usage()

if sys.argv[1] == '-p':
```

```
    if len(sys.argv) < 4:
        usage()
    prefix = sys.argv[2]
    filename = sys.argv[3]
else:
    filename = sys.argv[1]

try:
    handle = open(filename)
    text = handle.read()
    handle.close()

    set = dsig_certificate_set(text)
    set.write_certs(prefix=prefix)

except Exception as e:
    print(e)

#
# end dsig_extract.py
#
```

# Appendix D. ASM Simulator

The **asm-requester** and **asm-responder** programs implement the Auditorium Security Message (ASM) protocol defined in [SMPTE-430-6]. Both programs have command-line options that are required for each invocation, *e.g.*, to specify the TLS certificate, certificate chain, and RSA private key. In the examples presented throughout this document, these options are collectively referred to as (`... standard options ...`). The use of this shorthand is intended to allow the reader to concentrate on the options that define program behavior for the respective procedure.

**asm-requester** issues request messages to an ASM responder, such as an LDB. The program has command-line options to specify the destination IP address and the certificate, certificate chain, and RSA private key that comprise its identity. Additional options signal the type of message to be sent (from the set in [SMPTE-430-6]) and the message parameters. Program status and response values are displayed and may optionally be saved to disk.

**asm-responder** responds to requests from an ASM requester, *i.e.* a Security Manager (SM). It maintains a persistent state from startup, logging events that occur until the program is terminated. The program has command-line options to specify the IP bind address and TCP port, plus the certificate, certificate chain, and RSA private key that comprise its identity. Other options to control its message response behavior, *e.g.*, causing the program to respond to all request messages with "Busy". Files containing XML messages can be specified at invocation to pre-load log events to be returned in response to GetEventList messages.

The **asm-requester** and **asm-responder** programs are not provided with this document. They are described in detail in this appendix to allow Testing Organizations and other interested parties to develop an implementation that can provide the services required to execute the respective test procedures defined in this document. In lieu of developing this program, interested parties may instead choose to instrument an existing ASM requester or ASM responder implementation.

**Note:**
DCI compliant ASM implementations may differ in the way they present certificates during the TLS handshake. An implementation must supply the leaf certificate that identifies the device, but implementations may optionally supply the signing certificates that correspond to the leaf. Peer devices must work correctly regardless of the presence of a complete or partial chain. Some test procedures check this functionality directly, thus **asm-requester** and **asm-responder** must implement *both* certificate exchange modes.

## D.1. ASM Requester and Responder

### Name

**asm-requester** — initiate Request-Response-Pair (RRP) messagetype requests to an RRP responder

### Synopsis

```
asm-requester [--captured-prefix<hex-string>] [--damage-queryspb] [--disable-certificate-validation ]
[--disable-proper-cipher] [--disable-strict-reponse-times] [--interval <integer>]
[--end-time <YYYY-MM-DDThh:mm:ss>] [--key <hex-string-representation-of-key>] [--library-versions]
[--link-encryption-file <link-encryption-file>] [--validity-period <length in seconds>]
```

```
[--attribute-data <string>] [--log-format-S1] [--messagetype BadRequest|GetTime|GetEventList|
GetEventID|QuerySPB|LEKeyLoad|LEKeyQueryID|LEKeyQueryAll|LEKeyPurgeID|
LEKeyPurgeAll|X-GetEventBatch] [--misc-id id] [--pem-path <directory>] [--queryspb-interval>seconds<]
[--repeat-count <count>] [--request-id <id-number>] [--responder-address <address>]
[--responder-certificate-file-dump <responder-certificate.pem>]
[--start-time <YYYY-MM-DDThh:mm:ss>] [--use-16k-packets] [--verbose] [--X-geteventbatch-directory <director
asm-requester [-h|--help]
```

## Description

**asm-requester** is an ASM requester simulator. It initiates request-response-pair (RRP) messages with a responder at a specified IP address. There are two modes of operation: single request per invocation and multiple requests per invocation (interactive mode). See *INTERACTIVE MODE* for more information. **asm-requester** recognizes ASM message types specified in [SMPTE-430-6].

## Options

- `--attribute-data <hex-string>` -- Specify a value to be used as the seed for the counter mode cipher as specified by [SMPTE-430-6]. The value specified must be a 16-character long hexadecimal string. This option is only used, and is required, when the messagetype is `LEKeyLoad`.
- `--captured-prefix <filename-prefix>` -- Specify a filename prefix for logging responses from a responder to a file. The default is to write received responses to standard output.
- `--damage-queryspb` -- Send an incorrect (shortened) length on QuerySPB requests in violation of SMPTE 430-6-2010
- `--disable-certificate-validation` -- Causes the **asm-requester** to skip validation of the responder's certificate during TLS negotiation.
- `--disable-proper-cipher` -- Disables AES-128 as an allowable cipher (in violation of SMPTE 430-6-2010.)
- `--disable-strict-reponse-times` -- Disables validation of the 2-second response time as specified in S430-6-2008.
- `--end-time <timestamp>` -- Specify the end timestamp for retrieving events using GetEventList. The timestamp is a UTC format timestamp, formatted as YYYY-MM-DDThh:mm:ss.
- `--interval<seconds as integer>` -- The interval, in seconds, between repetitions of commands. When absent, the messagetype request is sent only once.
- `--key <hex-string-representation-of-key>` -- A hexadecimal key representing the symmetric key used to decrypt protected content. This option is only used, and is required, when the messagetype is `LEKeyLoad`.
- `--library-versions` -- Display detailed library information
- `--log-format-S1` -- Indicates the responder returns logs in the Series 1 binary format instead of the XMLformat defined by SMPTE 430-4.
- `--link-encryption-file=<link-encryption-file>` -- For the LEKeyLoad request, a tab-delimited file that contains one or more link encryption key quartets {ID, key, duration, seed}. Useful for batch key loads.
- `--messagetype <messagetype>` -- Specify the messagetype of the RRP being initiated. Valid message types are listed in the MESSAGE TYPES section below.
- `--misc-id id` -- This option is used for specifying identifiers for messagetypes that require them. The value of this option depends on the messagetype specified. For example, when the messagetype is LEKeyLoad, the misc-id will be the KeyID that

corresponds to the key being transmitted. When the messagetype is GetEventID, this will be the event ID number.

- `--pem-path <directory>` -- Specify a directory that contains a certificate (certificate.pem), private key (privatekey.pem), and certificate chain (a file of sequentually ordered certificates named chain.pem).
- `--queryspb-interval>seconds<` -- Specifies the interval, in seconds, for a connected interactive requester to make a QuerySPB request. A value of '0' (zero) disables this option.
- `--repeat-count <count>` -- The number of times a message request is sent to the responder, subject to any specified wait periods or intervals. The message ID will increment by one each time.
- `--request-id <id-string>` -- Specify an ID to be used with messagetypes that set or request a response based on an ID.
- `--responder-address <address>` -- The IP address of the responder to which the request will be sent.
- `--responder-certificate-file-dump <responder-certificate.pem>` -- Write out a file containing the responder's PEM encoded certificate.
- `--start-time <timestamp>` -- Specify the starting timestamp for retrieving events using GetEventList. The timestamp is a UTC format timestamp, formatted as YYYY-MM-DDThh:mm:ss.
- `--use-16k-packets` -- Break compliance with S430-6-2010 for compliance with RFC 2246 by allowing a maximum TLS plaintext length of 16 kilobytes instead of 512 bytes.
- `--validity-period <seconds>` -- the validity period of the key specified with the `--key option`. This option is only used, and is required, when the messagetype is `LEKeyLoad`.
- `--verbose` -- Enable verbose message output.
- `--X-geteventbatch-directory=<directory>` -- Specify directory for writing events retrieved using XGetEventBatch.
- `--version` -- Prints version information and then quits

## Message Types

ASM messages types fit into two categories: General Purpose ASM commands and Link Encryption ASM commands. Only one command (messagetype request) can be specified at a time. The following list describes the ASM Responder message types are accepted by the `--messagetype` (or available in the Interactive Mode) option:

**BadRequest**
Issues a request for an unknown message type to illicit a "BadRequest" response.

**GetTime**
Issues a request for the current time of the responder

**GetEventList**
Issues a request for the list of events recorded between specified start and stop times.

**GetEventID**
Issues a request for the log record matching one of the log record IDs returned from a GetEventList response

**GetProjCert**
Issues a request for the connected projector's certificate. The certificate received in response to this command is saved in DER format to the file "GetProjCert.der" and the general status and length of captured certificate are printed to the screen. Note that this MessageType is only available in Interactive Mode (see below).

**QuerySPB**
Issues a request for a system status report from the responder.

**LEKeyLoad**
Issues an LEKeyLoad message containing a link decryption key to the responder. Note that this messagetype requires the --key, --validity-period, and --attribute-data options.

**LEKeyQueryID**
Issues an LEKeyQuery message specifying the ID of a link decryption key

**LEKeyQueryAll**
Issues an LEKeyQueryALL message to a responder.

**LEKeyPurgeID**
Issues an LEKeyPurgeID message containing an ID of a key to be purged.

**LEKeyPurgeAll**
Issues an LEKeyPurgeAll message instructing a responder to purge all link decryption keys.

**X-GetEventBatch**
Gets batches of event

## Retrieved Messages

Once the request has been sent and either a response received or the timeout period exceeded, the message and/or status of the message is displayed to the screen and, optionally, recorded to a file using the `--captured-prefix` option to save it to a file.

## Interactive Mode

When **asm-requester** is invoked without the `--messagetype` option it enters its interactive mode and presents a menu of messagetypes that can be requested:

```
Press '0' to issue a bad request.
Press '1' to issue a GetTime request.
Press '2' to issue a GetEventList request.
Press '3' to issue a GetEventID request.
Press '4' to issue a QuerySPB request.
Press '5' to issue a LEKeyLoad request.
Press '6' to issue a LEKeyQueryID request.
Press '7' to issue a LEKeyQueryAll request.
Press '8' to issue a LEKeyPurgeID request.
Press '9' to issue a LEKeyPurgeAll request.
Press 'C' to issue a GetProjCert request.
Artifically generated meta-requests are also available:
Press 'z' to issue a GetEventList request followed by a GetEventID request for each event.
The returned event logs are placed into a directory.
Press 'X' to inject bad data into the TLS stream in violation of SMPTE 430-6-2010.
Press control-C to quit.
```

Message requests are selected by entering the corresponding number and pressing [Enter]. When the selected messagetype requires additional information, **asm-requester** will prompt for it.

```
2
Please enter the desired start and stop times in ISO 8601 time range format
      ("YYYY-MM-DDThh:mm:ss/YYYY-MM-DDThh:mm:ss"):
(press 'x' to return to the previous menu).
Press control-C to quit.
2009-03-26T16:02:58/2009-03-26T16:26:07
2009-04-02T20:50:52Z For request no. 0
      Retrieved 3 items from the list: [3, 4, 5]
      General response status: successful
Please enter the desired start and stop times in ISO 8601 time range format
      ("YYYY-MM-DDThh:mm:ss/YYYY-MM-DDThh:mm:ss"):
```

```
(press 'x' to return to the previous menu).
Press control-C to quit.
```

For some message types, like `LEKeyLoad`, sub-menus are presented depending on the information to be supplied:

```
5
Press '1' to enter the keys by hand.
Press '2' to load the keys from a file.
(press 'x' to return to the previous menu).
```

## Examples

```
$ asm-requester --responder-address 192.168.1.100 \
--pem-path /home/asm/pem_dir/ \
--captured-prefix virt-ldb-001-test01- \
--messagetype GetEventList
```

Starts an instance of the **asm-requester** with the specified PEM directory, establishes a TLS connection to 192.168.1.100, then sends a GetEventList message request. Output is logged to a file starting with the filename "virt-ldb-001-test01-".

## Name

asm-responder — respond to Request-Response-Pair (RRP) messagetype requests from an RRP requester

## Synopsis

```
asm-responder [--allowed-idle-time <seconds>] [--bind-address <address>] [--bind-port <port>] [--captured-prefix <file-prefix>] [--damage-queryspb] [--disable-certificate-validation ] [--disable-proper-cipher] [--disable-realtime-logs] [--enable-debug-event-id-response] [--enable-GetProjCert-response] [--log-directory <log-directory>] [-- library-versions] [ --max-message-size <size>] [--pr-certificate-file <cert-file>] [--preload-log-event <xml-file>] [--requester-certificate-file-dump <requester-certificate.pem>] [--respond-wtih-state <string>] [--respond-with-status <string>] [--set-timezone-offset <minutes>] [--tls-only] [--use-16k-packets] [--wait-before-responding <non-negative-float>] [--verbose]
```

## Description

**asm-responder** is an ASM responder simulator. It will respond to ASM Request messages received from an ASM requester. **asm-responder** recognizes ASM message types specified by SMPTE 430-6. When invoked, the responder will respond with a status messagetype of "Successful" (default), "Busy", "Invalid", or "Failed" as specified using the --respond-with or as specified at run time. More information about this is available in the RUNTIME OPTIONS and INTERACTIVE MENU sections below.

## Options

- `--allowed-idle-time <seconds>` -- Number of seconds before an idle connection may be pre-empted. Default is 90 seconds.
- `--bind-address <address>` -- The IP address on which to bind and listen for connections. If no address is specified, localhost is used.
- `--bind-port <port>` -- The TCP port number on which to bind and listen for connections. If no port is specified, the default port of 1173 is used.
- `--captured-prefix <file-prefix>` -- Specify a filename prefix for logging responses from a responder to a file. The default is to write received responses to standard output.
- `--damage-queryspb` -- Send an incorrect (shortened) length on QuerySPB responses in violation of SMPTE 430-6-2010.
- `--disable-certificate-validation` -- Disables the validation of the certificate(s) received from the remote requester during TLS initiation.
- `--disable-proper-cipher` -- Disables AES-128 as an allowable cipher (in violation of SMPTE 430-6-2010.)
- `--disable-realtime-logs` -- Disable interactive security log recording.
- `--enable-debug-event-id-response` -- Allow the sending of debug event IDs, instead of indicating a bad request.
- `--enable-GetProjCert-response` -- Allow the sending of the GetProjCert response, instead of indicating a bad request. Default is disabled.
- `--log-directory<log-directory>` -- The directory into which log records should be saved. The default value of `./logDirectory` is used if no log directory is specified.
- `--library-versions` -- Display detailed library information
- `--max-message-size <size>` -- Specify the maximum message size, in bytes, that can be received by the responder.
- `--pem-path <directory>` -- Specify a directory that contains a certificate (certificate.pem), private key (privatekey.pem), and certificate chain (a file of sequentually ordered certificates named chain.pem).
- `--pr-certificate-file <cert-file>` -- Specify a file that contains a PEM or DER certificate that represents the PR identity that the **asm-responder** is married to. (Used in the GetProjCert response).
- `--preload-log-event <event-log-file.xml>` -- Specify a file containing a log event. This option may be used multiple times, but only a single file may be specified per use.
- `--requester-certificate-file-dump <requester-certificate.pem>` -- Write out a file containing the requester's PEM encoded certificate.
- `--respond-with-state=<string>` -- Respond to all "QuerySPB" request messages with the specified response, either NotPlaying, Playing, or SecurityAlert
- `--respond-with-status=<string>` -- Respond to all request messages with the specified general response.
- `--set-timezone-offset <minutes>` -- Specify UTC offset, in minutes, for emitted logs.
- `--tls-only` -- This option causes **asm-responder** to establish a TLS session when requested, then ignore (not respond to) any messages sent from a requester.
- `--use-16k-packets` --Break compliance with S430-6-2010 for compliance with RFC 2246 by allowing a maximum TLS plaintext length of 16 kilobytes instead of 512 bytes.
- `--wait-before-responding=<non-negative-float>` -- The length of time in seconds after receiving a request to wait before sending its response.
- `--verbose` -- Enable verbose message output.
- `--version` -- Prints version information and then quits

## Message Types

ASM messages types fit into two categories: General Purpose ASM commands and Link Encryption ASM commands. Only one command (messagetype request) can be specified at a time. The following list describes the ASM Responder message types that are recognized by the responder, and the action and response generated by receiving each message type:

**BadRequest**
Respond with a "BadRequest" response.

**GetTime**
Responds with a GetTime response message

**GetEventList**
Responds with a message containing the list of events recorded between the start and stop times

**GetEventID**
Responds with a message containing the log record matching the log record ID specified in the Requester's request message.

**GetProjCert**
Responds with a message containing the PR certificate specified by the --pr-certificate-file option in DER form.

**QuerySPB**
Responds with a message containing a system status report.

**LEKeyLoad**
Accepts a Link Encryption key and responds with a message indicating that the key was received.

**LEKeyQueryID**
Responds with a message indicating the presence or absence of the key matching the KeyID specified in the requester's message.

**LEKeyQueryAll**
Responds with a message containing all of the KeyIDs corresponding to the Link Decryption keys in the responder.

**LEKeyPurgeID**
Deletes the specified key, and responds with a message indicating that the key matching the KeyID specified by the requester has been deleted.

**LEKeyPurgeAll**
Deletes all Link Encryption keys and responds with a message indicating that the key matching the KeyID specified by the requester has been deleted.

## Runtime Options

When the **asm-responder** is invoked to respond with a status, either "Successful" (default), "Busy", "Invalid", or "Failed". If no status is specified, the default status of "Successful" is used. While the **asm-responder** is running this value can be changed by typing 0, 1, 2, or 3 and pressing [Enter]. Values are as follows:

0. Successful

1. Busy

2. Invalid

3. Failed

## INTERACTIVE MENUS

**asm-responder** emulates a physical device in that it has a secured "perimeter" as well as a marriageable SPB. The devices are married/divorced and opened/closed based on log events, whether preloaded or generated interactively. If the "perimeter" is open or "SPB" is not married, the responder will return a security alert to any QuerySPB requests. Otherwise, it will return the emulated playback state, which can be set via the "Press '3' to toggle the responder's playback status." menu option.

When invoked, **asm-responder** will enter its interactive menu mode. From this menu, responses to messagetype requests can be specified by entering the letter or number that corresponds to your selection followed by [Enter]. Specifying a response message type on the command will configure the responder for that query response when it is initialized. 'x' returns to the previous menu, and [Ctrl-C] exits the responder. Other letter and number functions are context dependent and their use changes depending on the current menu.

When the responder initializes the top level menu is presented:

```
$ ./asm-responder.py --pem-path=/home/asm/id --bind-address 127.0.0.1
The responder has started running.
Press '1' to display/modify a general response element.
Press '2' to create an operations security log.
Press '3' to toggle the responder's playback status.
Press '4' to toggle the responder's acceptance of GetEventID requests of debug log records.
Press 'X' to inject bad data into the TLS stream in violation of SMPTE 430-6-2010.
Press control-C to quit.
```

From this menu, we can see and modify the type of responses that will be sent (1), we can generate a security log (2), we can induce errors into the TLS stream, or quit ([Ctrl-C]). Entering '1' will display the list of event queries and the response that will be sent when that type of query message is received. Any (or all) of the message responses can be changed by selecting the message type, as described below.

```
1
Please select the request for which the response element should be modified:
Press 'a' for all requests.
Press 'b' for BadRequest (currently Successful).
Press 'c' for GetTime (currently Successful).
Press 'd' for GetEventList (currently Successful).
Press 'e' for GetEventID (currently Successful).
Press 'f' for QuerySPB (currently Successful).
Press 'g' for LEKeyLoad (currently Successful).
Press 'h' for LEKeyQueryID (currently Successful).
Press 'i' for LEKeyQueryAll (currently Successful).
Press 'j' for LEKeyPurgeID (currently Successful).
Press 'k' for LEKeyPurgeAll (currently Successful).
Press 'l' for GetProjCert (currently Successful).
Press 'x' to return to the main menu.
Press control-C to quit.
```

When a request type is chosen, a menu to select the response to the query will be presented. Once a response is selected, the responses for that query will correspond to the newly chosen response.

```
b
Please select which response should be returned for BadRequest:
Press '0' for "RRP successful".
Press '1' for "RRP failed".
Press '2' for "RRP invalid".
Press '3' for "Responder busy".
Press 'x' to return to the main menu.
Press control-C to quit.
1
```

The query menu is presented with the newly updated message query response.

```
Please select the request for which the response element should be modified:
Press 'a' for all requests.
Press 'b' for BadRequest (currently Failed).
Press 'c' for GetTime (currently Successful).
Press 'd' for GetEventList (currently Successful).
Press 'e' for GetEventID (currently Successful).
Press 'f' for QuerySPB (currently Successful).
Press 'g' for LEKeyLoad (currently Successful).
Press 'h' for LEKeyQueryID (currently Successful).
Press 'i' for LEKeyQueryAll (currently Successful).
Press 'j' for LEKeyPurgeID (currently Successful).
Press 'k' for LEKeyPurgeAll (currently Successful).
Press 'l' for GetProjCert (currently Successful).
Press 'x' to return to the main menu.
Press control-C to quit.
```

## Log records

The responder application generates records log events that occur and writes them to the specified log directory. Unless specified, logs are written to `./logDirectory/<private-key-hex-thumbprint>`. Log entries can be added to the responder by means of the `--preload-log-event` option, or by generating them via the interactive menu. The responder caches log entries as a means of providing a memory between invocations, so logs previously preloaded do not need to be preloaded again unless multiple instances of a log event record are desired. Log records can be generated by selecting '2' from the interactive menu, then selecting the type of log entry to be generated, and lastly entering the desired datestamp for the log entry:

```
The responder has started running.
Press '1' to display/modify a general response element.
Press '2' to create an operations security log.
Press control-C to quit.
2
Please select the type of operations log to write:
Press '1' for SPBOpen.
Press '2' for SPBClose.
Press '3' for SPBMarriage.
Press '4' for SPBDivorce.
Press '5' for SPBClockAdjust.
Press '6' for SPBSoftware.
Press '7' for SPBSecurityAlert.
Press 'x' to return to the main menu.
Press control-C to quit.
5
Please enter an ISO-8601 (YYYY-mm-ddTHH:MM:SS) timestamp (or press ENTER for the current time)
  in the LOCAL timezone for the SPBClockAdjust record:
Press 'x' to return to the main menu.
Press control-C to quit.
[Enter]
Log created.
```

Log records present in the log record directory are read in when the responder is initialized, and are used to respond to log requests:

```
$ ./asm-responder.py --pem-path=/home/asm/id --bind-address 127.0.0.1
Loading a log event with a timestamp of 2009-03-26T15:58:40+00:00
Loading a log event with a timestamp of 2009-03-26T16:02:58+00:00
Loading a log event with a timestamp of 2009-03-26T16:14:48+00:00
The responder has started running.
```

Similarly, log entries can be preloaded using the --preload-log-event option. Preloaded log entries are loaded before logs present in the log directory.

```
$ ./asm-responder.py --pem-path=/home/asm/id --bind-address 127.0.0.1 \
--preload-log-event /home/asm/xml/KeyTransfer.xml
Loading a log event with a timestamp of 2008-12-05T08:00:01+00:00
Loading a log event with a timestamp of 2009-03-26T15:58:40+00:00
Loading a log event with a timestamp of 2009-03-26T16:02:58+00:00
Loading a log event with a timestamp of 2009-03-26T16:14:48+00:00
```

One log record, BogusLogFormat.xml, intentionally causes the responder to respond with a "BadRequest " response. When the `BogusLogFormat.xml` has been preloaded, and a specified `GetEventID` corresponds to the BogusLogFormat record, the responder will issue a "BadRequest" response with a general response element of "Responder Busy" and the request copy field will be null for that event only [SMPTE-430-6-2010, sec 7.1, bullet 3]. If the `--enable-debugevent-id-response` option is specified, the responder will instead respond with a `GetEventID` response with a general response element of "RRP Successful" and the BogusLogFormat log record in the log record field of the response.

### Examples

```
$ asm-responder --bind-address 192.168.1.100
  --pem-path /tmp/testing-device-crypto-id
```

Invokes **asm-responder** configured with the default responses.

```
$ asm-responder --bind-address 192.168.1.100
--pem-path /tmp/testing-device-crypto-id
--respond-with Busy
```

Invokes **asm-responder** configured to respond to all message requests with a "ResponderBusy" response

## D.2. Example Log Records

The following sections provide the text of the log records to be used with the `--preload-log-event` option of the **asm-responder** program.

### D.2.1. KeyTransfer

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000005</lr:EventID>
    <lr:TimeStamp>2008-12-05T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>665</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">ASM</lr:EventType>
    <lr:recordBodyHash>3fGsFdLkaoY2WZDqfPZnW4wrISg=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000005</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-ASM">KeyTransfer
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>DeviceConnectedID</dcml:Name>
        <dcml:Value xsi:type="ds:DigestValueType">thisisadcinspb1devicecert/M=</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.2. LinkClosed

```
<?xml version="1.0" encoding="UTF-8"?>
<LogRecord xmlns="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/" xmlns:xs="http://www.w3.org/2001/XMLSc
```

```
hema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dc
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  <LogRecordHeader>
    <EventID>urn:uuid:12345678-9abc-def1-2345-000000000002</EventID>
    <TimeStamp>2008-12-02T08:00:01-08:00</TimeStamp>
    <EventSequence>662</EventSequence>
    <DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </DeviceSourceID>
    <EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</EventClass>
    <EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">ASM</EventType>
    <recordBodyHash>oU2PhjuLqThJRHhv0c74T7y4PP0=</recordBodyHash>
  </LogRecordHeader>
  <LogRecordBody>
    <EventID>urn:uuid:12345678-9abc-def1-2345-000000000002</EventID>
    <EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-ASM">LinkClosed</EventSu
    <Parameters>
      <dcml:Parameter>
        <dcml:Name>DeviceConnectedID</dcml:Name>
        <dcml:Value xsi:type="ds:DigestValueType">thisisadcinspb1devicecert/M=</dcml:Value>
      </dcml:Parameter>
    </Parameters>
  </LogRecordBody>
  <LogRecordSignature>
    <HeaderPlacement>start</HeaderPlacement>
    <SequenceLength>90</SequenceLength>
  </LogRecordSignature>
</LogRecord>
```

## D.2.3. LinkException

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000003</lr:EventID>
    <lr:TimeStamp>2008-12-03T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>663</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes"
       >ASM</lr:EventType>
    <lr:recordBodyHash>qTr2Ix0vSwq8ga1r8taCmIMEUmw=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000003</lr:EventID>
    <lr:EventSubType
     scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-ASM"
     >LinkException
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>DeviceConnectedID</dcml:Name>
        <dcml:Value xsi:type="ds:DigestValueType">thisisadcinspb1devicecert/M=</dcml:Value>
```

```
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.4. LinkOpened

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000001</lr:EventID>
    <lr:TimeStamp>2008-12-01T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>661</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">ASM</lr:EventType>
    <lr:recordBodyHash>NRvkzUwLMoJHvOArIT/icRR0igg=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000001</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-ASM">LinkOpened
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>DeviceConnectedID</dcml:Name>
        <dcml:Value xsi:type="ds:DigestValueType">thisisadcinspb1devicecert/M=</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.5. LogTransfer

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000004</lr:EventID>
    <lr:TimeStamp>2008-12-04T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>664</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">ASM</lr:EventType>
    <lr:recordBodyHash>axJxhHABMr+P7sTtHfTZCIRa0e0=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000004</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-ASM">LogTransfer
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>DeviceConnectedID</dcml:Name>
        <dcml:Value xsi:type="ds:DigestValueType">thisisadcinspb1devicecert/M=</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.6. Prop1

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:2de0414a-ba29-49e7-bf38-0f1d322d9bdd</lr:EventID>
    <lr:TimeStamp>2008-12-01T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>675</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.fooby.foo/Debug/</lr:EventClass>
    <lr:EventType scope="http://www.fooby.foo/#FooTypes">Info</lr:EventType>
    <lr:recordBodyHash>AdVWKQumXjtZPxh6JyZeXHDe79s=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:2de0414a-ba29-49e7-bf38-0f1d322d9bdd</lr:EventID>
    <lr:EventSubType scope="http://www.fooby.foo/#EventSubTypes-FOO">Prop1</lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>Foo</dcml:Name>
        <dcml:Value xsi:type="xs:string">Fooby</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.7. Prop2

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:33bda81a-ef49-4d56-ac09-bcb7abb09478</lr:EventID>
    <lr:TimeStamp>2008-12-01T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>676</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.barby.bar/Debug/</lr:EventClass>
    <lr:EventType scope="http://www.barby.bar/#BarTypes">Info</lr:EventType>
    <lr:recordBodyHash>WVIMoL8/9+xSlkfrK+AdXIh8UZY=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:33bda81a-ef49-4d56-ac09-bcb7abb09478</lr:EventID>
    <lr:EventSubType scope="http://www.barby.bar/#EventSubTypes-BAR">Prop2</lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>Bar</dcml:Name>
        <dcml:Value xsi:type="xs:string">Barby</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.8. Prop3

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:e9f0c6a6-5f61-4261-949b-48d45723e3df</lr:EventID>
    <lr:TimeStamp>2008-12-01T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>677</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.dooby.doo/Debug/</lr:EventClass>
    <lr:EventType scope="http://www.dooby.doo/#DooTypes">Info</lr:EventType>
    <lr:recordBodyHash>cxaJlphGq50fjCYtWb8aptWz0XU=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:e9f0c6a6-5f61-4261-949b-48d45723e3df</lr:EventID>
    <lr:EventSubType scope="http://www.dooby.doo/#EventSubTypes-DOO">Prop3</lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>Doo</dcml:Name>
        <dcml:Value xsi:type="xs:string">Dooby</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.9. SPBClockAdjust

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000012</lr:EventID>
    <lr:TimeStamp>2008-12-12T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>672</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>GlmZQsgXbRxKk2JzmPpHqDpPhjA=</lr:recordBodyHash>
  </lr:LogRecordHeader>

  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000012</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBClockA
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>TimeOffset</dcml:Name>
        <dcml:Value xsi:type="xs:integer">120</dcml:Value>
      </dcml:Parameter>
      <dcml:Parameter>
        <dcml:Name>AuthId</dcml:Name>
        <dcml:Value xsi:type="xs:string">TheIdentityThatSetTheTime</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>

  </lr:LogRecordBody>

  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>

</lr:LogRecord>
```

## D.2.10. SPBClose

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000007</lr:EventID>
    <lr:TimeStamp>2008-12-07T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>667</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>8o5NylM2iifHT3y2WYN28A1vY2k=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000007</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBClose
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>AuthId</dcml:Name>
        <dcml:Value xsi:type="xs:string">TheIdentityThatAuthorizedtheSPBClose</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.11. SPBDivorce

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000009</lr:EventID>
    <lr:TimeStamp>2008-12-09T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>669</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>i/Ki+2oWxVQal7Bhwt/ZzE6TP+M=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000009</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBDivorc
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>DeviceConnectedID</dcml:Name>
        <dcml:Value xsi:type="ds:DigestValueType">thisisadcinspb2devicecert/A=</dcml:Value>
      </dcml:Parameter>
      <dcml:Parameter>
        <dcml:Name>AuthId</dcml:Name>
        <dcml:Value xsi:type="xs:string">TheIdentityThatAuthorizedtheDivorce</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.12. SPBMarriage

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000008</lr:EventID>
    <lr:TimeStamp>2008-12-08T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>668</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>hiraA3hRIcV8fKOwNqLEhjNuF5Y=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000008</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBMarria
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>DeviceConnectedID</dcml:Name>
        <dcml:Value xsi:type="ds:DigestValueType">thisisadcinspb2devicecert/A=</dcml:Value>
      </dcml:Parameter>
      <dcml:Parameter>
        <dcml:Name>AuthId</dcml:Name>
        <dcml:Value xsi:type="xs:string">TheIdentityThatAuthorizedtheMarriage</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.13. SPBOpen

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000006</lr:EventID>
    <lr:TimeStamp>2008-12-06T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>666</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>JXeqZabUCW5BsVeYVn8Q4oBw/Fw=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000006</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBOpen
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>AuthId</dcml:Name>
        <dcml:Value xsi:type="xs:string">TheIdentityThatAuthorizedtheSPBOpen</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.14. SPBSecurityAlert

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000014</lr:EventID>
    <lr:TimeStamp>2008-12-14T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>420</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>n7fBiDi4PUyy9uxfh3ode/kbCRY=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000014</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBSecuri
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>UnknownError</dcml:Name>
        <dcml:Value xsi:type="xs:string">IAmDeeplyTroubled</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>

  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.15. SPBShutdown

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000010</lr:EventID>
    <lr:TimeStamp>2008-12-10T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>670</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>m+R6vBSS8aZOC4WgQMcBXx/fBc8=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000010</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBShutdc
    </lr:EventSubType>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.16. SPBSoftware

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000013</lr:EventID>
    <lr:TimeStamp>2008-12-13T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>673</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>onrvqtocUYXdhNtNNvpjYtRS8pQ=</lr:recordBodyHash>
  </lr:LogRecordHeader>

  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000013</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBSoftwa
    </lr:EventSubType>
    <lr:Parameters>
      <dcml:Parameter>
        <dcml:Name>SoftwareVersion</dcml:Name>
        <dcml:Value xsi:type="xs:string">StringRepresentingTheNewSoftwareVersion</dcml:Value>
      </dcml:Parameter>
      <dcml:Parameter>
        <dcml:Name>AuthId</dcml:Name>
        <dcml:Value xsi:type="xs:string">TheIdentityThatAuthorizedTheSoftwareInstallation</dcml:Value>
      </dcml:Parameter>
      <dcml:Parameter>
        <dcml:Name>SignerID</dcml:Name>
        <dcml:Value xsi:type="xs:string">thisisadcinsigndevicecert/A=</dcml:Value>
      </dcml:Parameter>
    </lr:Parameters>
  </lr:LogRecordBody>

  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>

</lr:LogRecord>
```

## D.2.17. SPBStartup

```
<?xml version="1.0" encoding="UTF-8"?>
<lr:LogRecord xmlns:lr="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
```

```
">

  <lr:LogRecordHeader>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000011</lr:EventID>
    <lr:TimeStamp>2008-12-11T08:00:01-08:00</lr:TimeStamp>
    <lr:EventSequence>671</lr:EventSequence>
    <lr:DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">thisisadcinspb1devicecert/A=</dcml:PrimaryID>
    </lr:DeviceSourceID>
    <lr:EventClass>http://www.smpte-ra.org/430-5/2008/SecurityLog/</lr:EventClass>
    <lr:EventType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventTypes">Operations</lr:EventType>
    <lr:recordBodyHash>k9WRHg78rcBBOxwZz5QCnIsNrU8=</lr:recordBodyHash>
  </lr:LogRecordHeader>
  <lr:LogRecordBody>
    <lr:EventID>urn:uuid:12345678-9abc-def1-2345-000000000011</lr:EventID>
    <lr:EventSubType scope="http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations">SPBStartu
    </lr:EventSubType>
  </lr:LogRecordBody>
  <lr:LogRecordSignature>
    <lr:HeaderPlacement>start</lr:HeaderPlacement>
    <lr:SequenceLength>90</lr:SequenceLength>
  </lr:LogRecordSignature>
</lr:LogRecord>
```

## D.2.18. BogusLogFormat

```
<?xml version="1.0" encoding="UTF-8"?>
<LogRecord xmlns="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
  xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/">
  <LogRecordHeader xmlns="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
    xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/">
    <EventID>urn:uuid:22a815e4-8b5d-4763-ac67-a67578ad76e6</EventID>
    <TimeStamp>2011-02-02T14:20:44-08:00</TimeStamp>
    <EventSequence>0</EventSequence>
    <DeviceSourceID>
      <dcml:PrimaryID idtype="CertThumbprint">AAAAAAAAAAAAAAAAAAAAAAAAAAA=</dcml:PrimaryID>
    </DeviceSourceID>
    <EventClass>http://www.cinecert.com/430-4/2008/DebugLog/</EventClass>
    <EventType scope="http://www.cinecert.com/430-4/2008/DebugLog/#EventTypes">GetEventID</EventType>
    <recordBodyHash>5YoEzNqBbMdm352NVCkpWJDtU9A=</recordBodyHash>
  </LogRecordHeader>
  <LogRecordBody xmlns="http://www.smpte-ra.org/schemas/430-4/2008/LogRecord/"
    xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes/">
    <EventID>urn:uuid:22a815e4-8b5d-4763-ac67-a67578ad76e6</EventID>
    <EventSubType scope="http://www.cinecert.com/430-4/2008/DebugLog/#EventSubTypes-geteventid">Disable</EventS
  </LogRecordBody>
</LogRecord>
```

# Appendix E. GPIO Test Fixture

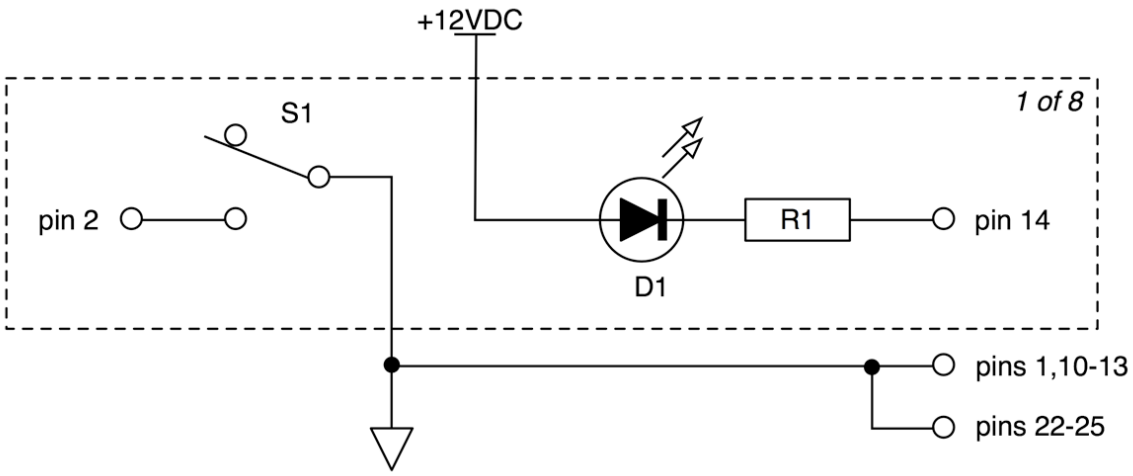
The GPIO test fixture has eight outputs, which connect to ground via normally-open switch contacts. These outputs are expected to interface to command and/or status inputs of the d-cinema equipment under test.

The fixture has eight inputs, which connect to powered, current limited LEDs and will illuminate when the corresponding input is grounded. These inputs interface to command and/or status outputs of the d-cinema equipment under test.

Example circuits are provided below. Interface of outputs, inputs and ground is made via a single DB-25 female connector on the test fixture.

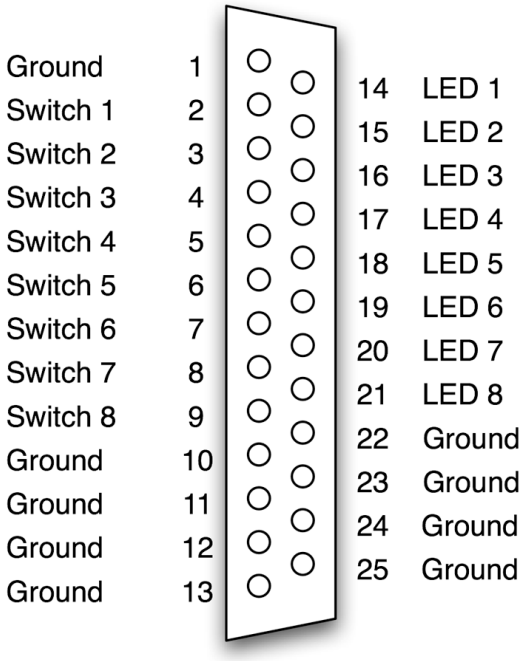
Testing Entities are not required to follow the above design, and are free to develop their own equipment and connector standards. The manufacturer of the d-cinema equipment being tested is responsible for providing a cable, appropriate for the individual device under test, that will interface to the test fixture being used.

## Figure E.1. GPIO Test Fixture Schematic




Note that the LED inputs are internally current limited. External devices will be expected to sink 25mA per channel. Also, the test fixture has an integral PSU (the PSU may be external but it must use a different connector).

## Figure E.2. GPIO Test Fixture Connector


Ground 1
Switch 1 2
Switch 2 3
Switch 3 4
Switch 4 5
Switch 5 6
Switch 6 7
Switch 7 8
Switch 8 9
Ground 10
Ground 11
Ground 12
Ground 13
14 LED 1
15 LED 2
16 LED 3
17 LED 4
18 LED 5
19 LED 6
20 LED 7
21 LED 8
22 Ground
23 Ground
24 Ground
25 Ground

# Appendix F. Reference Documents


**AES3-2003**
*AES standard for digital audio - Digital input-output interfacing - Serial transmission format for two-channel linearly represented digital audio data, Audio Engineering Society*, September 9, 2003

**CIE-15-2004**
*Colorimetry, 3rd Edition, International Commission on Illumination*, 2004

**DCI-DCSS**
*Digital Cinema System Specification Version 1.4.1*, DCI, October 13, 2021.
https://dcss.dcimovies.com/87da0904badd1e28efc83e860d0d572a6cf4399a/dcss.html

**OBAE-ADD**
*Digital Cinema Object-Based Audio Addendum*, DCI, October 1, 2018

**FIPS-140-2**
*FIPS 140-2: Security Requirements for Cryptographic Modules*, NIST, Decemer 12, 2002

**FIPS-140-3**
*FIPS 140-3: Security Requirements for Cryptographic Modules*, NIST, March 22, 2019

**FIPS-180-2**
*FIPS 180-2: Secure Hash Standard*, NIST, August 1, 2002

**FIPS-197**
*FIPS 197: Advanced Encryption Standard (AES)*, NIST, November 26, 2001

**FIPS-198a**
*FIPS 198a: The Keyed-Hash Message Authentication Code (HMAC)*, NIST, March 6, 2002

**IEEE-802-3**
*802-3: Standard for Information technology—Telecommunications and information exchange between systems— Local and metropolitan area networks—Specific requirements Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*, IEEE, 2005

**ISO-144496**
*ISO/IEC 144496: Information technology - Computer graphics and image processing - Font Compression and Streaming*, ISO/IEC, 2004

**ISO-15948**
*ISO-15948: Information technology - Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification*, ISO/IEC, 2004

**ISO-15444-1**
*ISO/IEC 15444-1 2004, Information Technology: JPEG 2000 Image Coding System*, ISO/IEC, 2004

**ISO-15444-1-AMD-1**
*ISO/IEC 15444-1/Amd1:2006 Codestream restrictions - Amendment 1: Profiles for digital cinema applications*, ISO/IEC, 2004

**ISO-10646**
*ISO 10646: Information technology – Universal Multiple-Octet Coded Character Set (UCS)*, ISO/ IEC, December 15, 2003

**ITU-X509**
*ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, ITU, June 1997

**NIST-800-38A**
*NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, NIST, Morris Dworkin, December 2001

**NIST-800-38F**

*NIST Special Publication 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, NIST, December 2012

**PKCS-1**
*PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories*, June 14, 2002

**RFC-1421**
*RFC 1421: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures"*, IETF, J. Linn, February 1993

**RFC-2045**
*RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"*, IETF, N. Freed, N. Borenstein, November 1996

**RFC-2246**
*RFC 2246: "The TLS Protocol Version 1.0"*, IETF, T. Dierks, C. Allen, January 1999

**RFC-2246**
*RFC 5246: "The TLS Protocol Version 1.2"*, IETF, T. Dierks, E. Rescorla, August 2008

**RFC-8446**
*RFC 8446: "The TLS Protocol Version 1.3"*, IETF, E. Rescorla, August 2018

**RFC-2253**
*RFC 2253: "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names"*, IETF,

**RFC-3174**
*RFC 3174: "US Secure Hash Algorithm 1 (SHA1)"*, IETF, September 2001

**RFC-3339**
*RFC 3339: "Date and Time on the Internet: Timestamps"*, IETF, July 2002

**RFC-3447**
*RFC 3447: "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"*, IETF, J. Jonsson, B. Kaliski, February 2003

**RFC-4122**
*RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace"*, IETF, P. Leach, M. Mealling, July 2005

**SMPTE-330**
*SMPTE Standard for Television – Unique Material Identifier (UMID)*, SMPTE, 2011

**SMPTE-336**
*SMPTE Standard for Television - Data Encoding Protocol using Key-Length-Value*, SMPTE, 2007

**SMPTE-372**
*Television - Dual Link 292M Interface for 1920 x 1080 Picture Raster*, SMPTE, 2011

**SMPTE-377-1**
*SMPTE Standard for Television – Material Exchange Format (MXF) – File Format Specification"*, SMPTE, 2011

**SMPTE-379-1**
*SMPTE Standard for Television – Material Exchange Format (MXF) – MXF Generic Container*, SMPTE, 2009

**SMPTE-382**
*Material Exchange Format (MXF) – Mapping AES3 and Broadcast Wave Audio into the MXF Generic Container*, SMPTE, 2007

**SMPTE-390**
*Television - Material Exchange Format (MXF) - Specialized Operational Pattern "Atom" (Simplified Representation of a Single Item)*, SMPTE, 2011

**SMPTE-410**
*Material Exchange Format - Generic Stream Partition*, SMPTE, 2008

**SMPTE-422**
*Material Exchange Format - Mapping JPEG 2000 Codestreams into the MXF Generic Container*, SMPTE, 2006

**SMPTE-428-1**
*D-Cinema Distribution Master - Image Structure*, SMPTE, 2006

**SMPTE-428-2**
*D-Cinema Distribution Master- Audio Characteristics*, SMPTE, 2006

**SMPTE-428-3**
*D-Cinema Distribution Master - Audio Channel Mapping*, SMPTE, 2006

**SMPTE-428-7**
*D-Cinema Distribution Master - Subtitle*, SMPTE, 2010

**SMPTE-428-10**
*D-Cinema Distribution Master - Closed Caption and Closed Subtitle*, SMPTE, 2008

**SMPTE-428-12**
*D-Cinema Distribution Master - Common Audio Channels and Soundfield Groups*, SMPTE, 2013

**SMPTE-429-2**
*D-Cinema Packaging - Operational Constraints*, SMPTE, 2011

**SMPTE-429-3**
*D-Cinema Packaging - Sound and Picture Track File Application*, SMPTE, 2007

**SMPTE-429-4**
*D-Cinema Packaging - MXF JPEG2000 Application*, SMPTE, 2006

**SMPTE-429-5**
*D-Cinema Packaging - Subtitling Distribution Format*, SMPTE, 2009

**SMPTE-429-6**
*D-Cinema Packaging - Track File Essence Encryption*, SMPTE, 2006

**SMPTE-429-7**
*D-Cinema Packaging - Composition Playlist Application*, SMPTE, 2006

**SMPTE-429-8**
D-Cinema Packaging - Packing List, SMPTE, 2007

**SMPTE-429-9**
*D-Cinema Packaging - Asset Mapping*, SMPTE, 2007

**SMPTE-429-10**
*D-Cinema Packaging - Stereoscopic Picture Track File*, SMPTE, 2008

**SMPTE-429-12**
*D-Cinema Packaging - Caption and Closed Subtitle*, SMPTE, 2008

**SMPTE-429-14**
*D-Cinema Packaging - Aux Data Track File*, SMPTE, 2014

**SMPTE-429-16**
*D-Cinema Packaging - Additional Composition Metadata and Guidelines*, SMPTE, 2014

**SMPTE-429-18**
*D-Cinema Packaging - Immersive Audio Track File*, SMPTE, 2019

**SMPTE-429-19**
*D-Cinema Packaging - DCP Operational Constraints for Immersive Audio*, SMPTE, 2019

**SMPTE-430-1**
*D-Cinema Operations - Key Delivery Message*, SMPTE, 2009

**SMPTE-430-2**
*D-Cinema Operations - Digital Certificate*, SMPTE, 2006

**SMPTE-430-3**
*D-Cinema Operations - Generic Extra-Theatre Message Format*, SMPTE, 2008

**SMPTE-430-4**
*D-Cinema Operations - Log Records Format*, SMPTE, 2008

**SMPTE-430-5**
*D-Cinema Operations - Security Log Event Class and Constraints*, SMPTE, 2011

**SMPTE-430-6**
*D-Cinema Operations - Auditorium Security Messages for Intra-Theater Communications"*, SMPTE, 2010

**SMPTE-430-12**

*D-Cinema Operations – FSK Synchronization Signal*, SMPTE, 2014

**SMPTE-430-12-AM1-2019**
*D-Cinema Operations – FSK Synchronization Signal – Amendment 1*, SMPTE, 2019

**SMPTE-431-1**
*D-Cinema Quality - Screen Luminance Level, Chromaticity, and Uniformity*, SMPTE, 2006

**SMPTE-431-2**
*D-Cinema Quality - Reference Projector and Environment*, SMPTE, 2011

**SMPTE-432-1**
*Digital Source Processing - Color Processing for D-Cinema*, SMPTE, 2010

**SMPTE-432-2**
*Digital Source Processing - D-Cinema Low Frequency Effects (LFE) Channel Audio Characteristics*, SMPTE, 2006

**SMPTE-433**
*D-Cinema - XML Data Types*, SMPTE, 2008

**SMPTE-rdd-20**
*D-Cinema - CineLink 2 link encryption protocol*, SMPTE, 2010

**SMPTE-2098-2**
*Immersive Audio Bitstream Specification*, SMPTE, 2019

**SMPTE-2098-3**
*Immersive Audio Renderer Expectations and Testing Recommendations*, SMPTE, 2020

**SMPTE-2098-5**
*D-Cinema Immersive Audio Channels and Soundfield*, SMPTE, 2018

# Appendix G. Digital Cinema System Specification References to CTP

| DCSS Section | CTP Procedure Title | CTP Section |
|---|---|---|
| 2.1.1.4 | Decoder Requirements | 6.5.2. |
| 3.1 | OBAE Addendum | 10.4.84. |
| 3.2 | OBAE Addendum | 10.4.84. |
| 3.2.1.2 | Image Structure Container and Image Container Format | 4.5.1. |
| 3.2.1.3 | Image Structure Container and Image Container Format | 4.5.1. |
| 3.2.1.5 | Image Compression Standard & Encoding Parameters | 4.5.2. |
| 3.2.1.7 | Image Structure Container and Image Container Format | 4.5.1. |
| 3.3 | OBAE Addendum | 10.4.84. |
| 3.3.2.1 | Audio Sample Rate Conversion | 6.6.2. |
| 3.3.2.2 | Audio Characteristics | 4.5.3. |
| 3.3.4 | Timed Text Track File Format | 4.4.3. |
| 3.3.4.1 | Audio Characteristics | 4.5.3. |
| 3.4 | OBAE Addendum | 10.4.84. |
| 3.4.2.2 | Timed Text Resource Encoding | 4.5.4. |
| 3.4.3 | Default Timed Text Font | 6.7.4. |
| 3.4.3.4 | Timed Text Resource Encoding | 4.5.4. |
| 4.2 | Image Compression Standard & Encoding Parameters | 4.5.2. |
| 4.3.2 | Decoder Requirements | 6.5.2. |
| 4.4 | Image Compression Standard & Encoding Parameters | 4.5.2. |
| 4.4.3.2 | Timed Text Resource Encoding | 4.5.4. |
| 5.2.2.2 | Image and Audio Packaging Standard | 4.4.2. |
| 5.2.2.3 | Image and Audio Packaging Standard | 4.4.2. |
| 5.2.2.4 | Image and Audio Packaging Standard | 4.4.2. |
| 5.2.2.5 | Image and Audio Packaging Standard | 4.4.2. |
| 5.2.2.6 | Image and Audio Packaging Standard | 4.4.2. |
| 5.2.2.6 | DCP Integrity | 4.6.1. |
| 5.2.3 | Composition Playlist File | 4.3.1. |
| | | |

| | | |
|---|---|---|
| 5.2.3 | Composition Playlist Signature Validation | 4.3.2. |
| 5.3.1 | Image and Audio Packaging Standard | 4.4.2. |
| 5.3.1.3 | Track File Length | 4.4.4. |
| 5.3.1.3 | Playback of Image Only Material | 6.5.1. |
| 5.3.1.6 | Click Free Splicing of Audio Track Files | 6.6.4. |
| 5.3.1.6 | Click Free Splicing of OBAE Track Files | 6.8.1. |
| 5.3.1.7 | Composition Playlist Key Usage | 4.3.3. |
| 5.3.1.9 | DCP Integrity | 4.6.1. |
| 5.3.2 | Image and Audio Packaging Standard | 4.4.2. |
| 5.3.3.2 | Image Track File Frame Boundary | 4.4.5. |
| 5.3.4.2 | Audio Track File Frame Boundary | 4.4.6. |
| 5.4.2 | Composition Playlist File | 4.3.1. |
| 5.4.3 | Composition Playlist File | 4.3.1. |
| 5.4.3.2 | Composition Playlist File | 4.3.1. |
| 5.4.3.3 | Composition Playlist File | 4.3.1. |
| 5.4.3.4 | Composition Playlist File | 4.3.1. |
| 5.4.3.6 | Composition Playlist Signature Validation | 4.3.2. |
| 5.4.4 | Composition Playlist Signature Validation | 4.3.2. |
| 5.5.2.1 | Asset Map File | 4.1.1. |
| 5.5.2.1 | Volume Index File | 4.1.2. |
| 5.5.2.3 | Packing List Signature Validation | 4.2.2. |
| 5.5.2.3 | DCP Integrity | 4.6.1. |
| 5.5.3.1 | Packing List File | 4.2.1. |
| 5.5.3.2 | Packing List File | 4.2.1. |
| 5.5.3.2 | Packing List Signature Validation | 4.2.2. |
| 5.5.3.2 | DCP Integrity | 4.6.1. |
| 6.2.3 | Storage System Ingest Interface | 8.1.1. |
| 7.2.3.1 | Theater System Reliability | 10.4.1. |
| 7.2.3.2 | Theater System Reliability | 10.4.1. |
| 7.2.3.5 | Show Playlist Creation | 8.2.2. |
| 7.2.3.5 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.2.3.7 | Show Playlist Creation | 8.2.2. |
| 7.2.3.7 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.2.3.11 | Storage System Capacity | 8.1.2. |

| | | |
|---|---|---|
| 7.2.3.13 | Restarting Playback | 8.2.8. |
| 7.2.3.13 | Restarting Playback (OBAE) | 8.2.17. |
| 7.3 | Show Playlist Format | 8.2.3. |
| 7.3.4 | Show Playlist Creation | 8.2.2. |
| 7.3.4 | Automation Control and Interfaces | 8.2.5. |
| 7.3.4 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.3.4 | Automation Control and Interfaces (OBAE) | 8.2.19. |
| 7.4.1.1 | Show Playlist Creation | 8.2.2. |
| 7.4.1.1 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.4.1.2 | Show Playlist Creation | 8.2.2. |
| 7.4.1.2 | Restarting Playback | 8.2.8. |
| 7.4.1.2 | Restarting Playback (OBAE) | 8.2.17. |
| 7.4.1.2 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.4.1.3 | Show Playlist Creation | 8.2.2. |
| 7.4.1.3 | SMS User Accounts | 8.2.9. |
| 7.4.1.3 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.4.1.4 | Show Playlist Creation | 8.2.2. |
| 7.4.1.4 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.4.1.5 | Show Playlist Creation | 8.2.2. |
| 7.4.1.5 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.4.1.6 | Show Playlist Creation | 8.2.2. |
| 7.4.1.6 | Show Playlist Format | 8.2.3. |
| 7.4.1.6 | Automation Control and Interfaces | 8.2.5. |
| 7.4.1.6 | Artifact Free Transition of Image Format | 8.2.7. |
| 7.4.1.6 | Show Playlist Creation (OBAE) | 8.2.18. |
| 7.4.1.6 | Automation Control and Interfaces (OBAE) | 8.2.19. |
| 7.4.1.7 | Automation Control and Interfaces | 8.2.5. |
| 7.4.1.7 | Automation Control and Interfaces (OBAE) | 8.2.19. |
| 7.4.1.8 | Audio Delay Setup | 6.6.3. |
| 7.4.1.8 | OBAE Delay Setup | 6.8.2. |
| 7.4.1.8 | Interrupt Free Playback | 8.2.6. |
| 7.4.1.8 | Restarting Playback | 8.2.8. |
| 7.4.1.8 | Interrupt Free Playback (OBAE) | 8.2.16. |
| 7.4.1.8 | Restarting Playback (OBAE) | 8.2.17. |

| | | |
|---|---|---|
| 7.4.4.2.5 | Projector Overlay | 7.5.1. |
| 7.5.3.2 | Storage System Redundancy | 8.1.3. |
| 7.5.3.2 | Storage System Redundancy (OBAE) | 8.1.5. |
| 7.5.3.3 | Storage System Performance | 8.1.4. |
| 7.5.3.3 | Storage System Performance (OBAE) | 8.1.6. |
| 7.5.3.4 | Storage System Performance | 8.1.4. |
| 7.5.3.4 | Storage System Performance (OBAE) | 8.1.6. |
| 7.5.3.6 | Storage System Performance | 8.1.4. |
| 7.5.3.6 | Storage System Performance (OBAE) | 8.1.6. |
| 7.5.3.8 | Theater System Storage Security | 10.4.2. |
| 7.5.4.2.5 | Media Block Overlay | 6.7.1. |
| 7.5.4.2.6 | Media Block Overlay | 6.7.1. |
| 7.5.4.2.6 | Projector Overlay | 7.5.1. |
| 7.5.4.2.7 | Media Block Overlay | 6.7.1. |
| 7.5.4.2.7 | Projector Overlay | 7.5.1. |
| 7.5.4.3 | Digital Audio Interfaces | 6.6.1. |
| 7.5.6.1 | Digital Audio Interfaces | 6.6.1. |
| 7.5.6.2 | Digital Audio Interfaces | 6.6.1. |
| 7.5.7.2 | Automation Control and Interfaces | 8.2.5. |
| 7.5.7.2 | Automation Control and Interfaces (OBAE) | 8.2.19. |
| 8.2.2.6 | Projector Pixel Count/Structure | 7.5.3. |
| 8.2.2.7 | Projector Pixel Count/Structure | 7.5.3. |
| 8.2.2.7 | Projector Spatial Resolution and Frame Rate Conversion | 7.5.4. |
| 8.2.2.8 | Projector Spatial Resolution and Frame Rate Conversion | 7.5.4. |
| 8.2.2.10 | MB Link Encryption | 6.2.4. |
| 8.3.3 | Contouring | 7.5.10. |
| 8.3.4.3 | White Point Luminance and Uniformity | 7.5.5. |
| 8.3.4.4 | White Point Luminance and Uniformity | 7.5.5. |
| 8.3.4.5 | White Point Chromaticity and Uniformity | 7.5.6. |
| 8.3.4.6 | White Point Chromaticity and Uniformity | 7.5.6. |
| 8.3.4.7 | Sequential Contrast | 7.5.7. |
| 8.3.4.8 | Intra-frame Contrast | 7.5.8. |
| 8.3.4.9 | Grayscale Tracking | 7.5.9. |
| 8.3.4.13 | Color Accuracy | 7.5.12. |

| | | |
|---|---|---|
| 8.4.2 | MB Link Encryption | 6.2.4. |
| 8.4.3.1 | MB Link Encryption | 6.2.4. |
| 9.3.3.2 | Security Entity Physical Protection | 10.4.4. |
| 9.3.4.11 | Transfer Function | 7.5.11. |
| 9.4.1 | Theater System Storage Security | 10.4.2. |
| 9.4.1 | Security Devices Self-Test Capabilities | 10.4.3. |
| 9.4.1.1 | SMS Operator Identification | 8.2.10. |
| 9.4.1.1 | SMS Operator Identification (OBAE) | 8.2.20. |
| 9.4.1.1 | Security Entity Physical Protection | 10.4.4. |
| 9.4.1.1 | Secure SMS-SM Communication | 10.4.5. |
| 9.4.2.2 | Projector and Direct View Display Physical Protection | 7.2.1. |
| 9.4.2.4 | SM Operating Environment | 9.5.1. |
| 9.4.2.4 | Location of Security Manager | 10.4.6. |
| 9.4.2.4 | Secure Remote SPB-SM Communications | 10.4.8. |
| 9.4.2.5 | SMS Identity and Certificate | 8.2.11. |
| 9.4.2.5 | Validity of SMS Certificates | 8.2.15. |
| 9.4.2.5 | Self-initiated cryptographic output capability | 9.5.14. |
| 9.4.2.5 | Self-initiated cryptographic output capability | 9.5.14. |
| 9.4.2.5 | Secure SMS-SM Communication | 10.4.5. |
| 9.4.2.5 | SMS and SPB Authentication and ITM Transport Layer | 10.4.30. |
| 9.4.2.5 | RRP Operational Messages | 10.4.40. |
| 9.4.2.5 | Dual Certificate SMS Authentication | 10.4.80. |
| 9.4.2.7 | Constrained OMB Processing Capability | 10.4.81. |
| 9.4.2.7 | Encrypted Auxiliary Data Processing | 10.4.83. |
| 9.4.3.2 | Content Keys and TDL check | 8.2.12. |
| 9.4.3.2 | Content Keys and TDL check (OBAE) | 8.2.13. |
| 9.4.3.2.6 | LDB Time-Awareness | 7.4.3. |
| 9.4.3.5 | KDM NonCriticalExtensions Element | 3.5.1. |
| 9.4.3.5 | ETM IssueDate Field Check | 3.5.2. |
| 9.4.3.5 | Structure ID Check | 3.5.4. |
| 9.4.3.5 | Certificate Thumbprint Check | 3.5.5. |
| 9.4.3.5 | KeyInfo Field Check | 3.5.7. |
| 9.4.3.5 | KDM Malformations | 3.5.8. |
| 9.4.3.5 | KDM Signature | 3.5.9. |

| | | |
|---|---|---|
| 9.4.3.5 | KDM NonCriticalExtensions Element (OBAE) | 3.5.10. |
| 9.4.3.5 | ETM IssueDate Field Check (OBAE) | 3.5.11. |
| 9.4.3.5 | Structure ID Check (OBAE) | 3.5.12. |
| 9.4.3.5 | Certificate Thumbprint Check (OBAE) | 3.5.13. |
| 9.4.3.5 | KeyInfo Field Check (OBAE) | 3.5.14. |
| 9.4.3.5 | KDM Malformations (OBAE) | 3.5.15. |
| 9.4.3.5 | KDM Signature (OBAE) | 3.5.16. |
| 9.4.3.5 | TLS Session Initiation | 5.2.1. |
| 9.4.3.5 | Auditorium Security Message Support | 5.2.2.1. |
| 9.4.3.5 | ASM "GetProjCert" | 5.2.2.12. |
| 9.4.3.5 | TLS Exception Logging | 5.2.3. |
| 9.4.3.5 | Image Integrity Checking | 6.1.1. |
| 9.4.3.5 | Sound Integrity Checking | 6.1.2. |
| 9.4.3.5 | Restriction of Keying to MD Type | 6.1.4. |
| 9.4.3.5 | Restriction of Keying to Valid CPLs | 6.1.5. |
| 9.4.3.5 | Remote SPB Integrity Monitoring | 6.1.6. |
| 9.4.3.5 | SPB Integrity Fault Consequences | 6.1.7. |
| 9.4.3.5 | Content Key Extension, End of Engagement | 6.1.8. |
| 9.4.3.5 | ContentAuthenticator Element Check | 6.1.9. |
| 9.4.3.5 | KDM TDL Check | 6.1.11. |
| 9.4.3.5 | CPL Id Check | 6.1.13. |
| 9.4.3.5 | CPL Id Check (OBAE) | 6.1.14. |
| 9.4.3.5 | Restriction of Playback in Absence of Integrity Pack Metadata | 6.1.15. |
| 9.4.3.5 | Restriction of Keying to MDEK Type (OBAE) | 6.1.16. |
| 9.4.3.5 | OBAE Integrity Checking | 6.1.17. |
| 9.4.3.5 | Content Key Extension, End of Engagement (OBAE) | 6.1.18. |
| 9.4.3.5 | Restriction of Keying to Valid CPLs (OBAE) | 6.1.22. |
| 9.4.3.5 | ContentAuthenticator Element Check (OBAE) | 6.1.23. |
| 9.4.3.5 | Special Auditorium Situation Operations | 6.2.2. |
| 9.4.3.5 | Timed Text Decryption | 6.7.6. |
| 9.4.3.5 | KDM Content Keys Check | 8.2.14. |
| 9.4.3.5 | LE Key Generation | 9.5.2. |
| 9.4.3.5 | Location of Security Manager | 10.4.6. |
| 9.4.3.5 | Playback Preparation | 10.4.9. |

| | | |
|---|---|---|
| 9.4.3.5 | Special Auditorium Situation Detection | 10.4.10. |
| 9.4.3.5 | Prevention of Keying of Compromised SPBs | 10.4.11. |
| 9.4.3.5 | SPB Authentication | 10.4.12. |
| 9.4.3.5 | TLS Session Key Refreshes | 10.4.13. |
| 9.4.3.5 | LE Key Issuance | 10.4.14. |
| 9.4.3.5 | Maximum Key Validity Period | 10.4.15. |
| 9.4.3.5 | KDM Purge upon Expiry | 10.4.16. |
| 9.4.3.5 | Key Usage Time Window | 10.4.17. |
| 9.4.3.5(9a) | ASM "RRP Invalid" | 5.2.2.3. |
| 9.4.3.5(15) | ASM "RRP Invalid" | 5.2.2.3. |
| 9.4.3.5(9d) | Export of KDM-Borne Keys | 10.4.82. |
| 9.4.3.6.1 | KDM TDL Check | 6.1.11. |
| 9.4.3.6.1 | Projector and Direct View Display Physical Protection | 7.2.1. |
| 9.4.3.6.1 | Projector and Direct View Display Security Servicing | 7.2.2. |
| 9.4.3.6.1 | Electronic Marriage Break Key Retaining | 7.2.8. |
| 9.4.3.6.1 | Companion SPBs with Electronic Marriage | 7.3.2. |
| 9.4.3.6.1 | Projector Secure Silicon Device | 10.4.18. |
| 9.4.3.6.1 | Access to Projector Image Signals | 10.4.19. |
| 9.4.3.6.1 | Systems with Electronic Marriage | 10.4.20. |
| 9.4.3.6.1 | Projector SPB Log Reporting Requirements | 10.4.78. |
| 9.4.3.6.2 | TLS Session Initiation | 5.2.1. |
| 9.4.3.6.2 | TLS Exception Logging | 5.2.3. |
| 9.4.3.6.2 | Companion SPBs with Electronic Marriage | 7.3.2. |
| 9.4.3.6.2 | Companion SPB Marriage Break Key Retaining | 7.3.3. |
| 9.4.3.6.2 | LDB TLS Session Constraints | 7.4.2. |
| 9.4.3.6.2 | LDB Key Storage | 7.4.5. |
| 9.4.3.6.2 | LDB Key Purging | 7.4.6. |
| 9.4.3.6.2 | SPB Type 1 Tamper Responsiveness | 9.5.3. |
| 9.4.3.6.2 | Companion SPB Single Purpose Requirement | 10.4.76. |
| 9.4.3.6.2.1 | SPB Type 1 Tamper Responsiveness | 9.5.3. |
| 9.4.3.6.2.1 | SPB Type 1 Log Retention | 10.4.69. |
| 9.4.3.6.3 | Timed Text Decryption | 6.7.6. |
| 9.4.3.6.3 | Companion SPBs with Electronic Marriage | 7.3.2. |
| 9.4.3.6.3 | Companion SPB Marriage Break Key Retaining | 7.3.3. |

| | | |
|---|---|---|
| 9.4.3.6.3 | SPB Type 1 Tamper Responsiveness | 9.5.3. |
| 9.4.3.6.3 | MB Tasks | 10.4.58. |
| 9.4.3.6.3 | SPB Type 1 Log Retention | 10.4.69. |
| 9.4.3.6.3 | Log Collection for Married MB | 10.4.75. |
| 9.4.3.6.3 | Companion SPB Single Purpose Requirement | 10.4.76. |
| 9.4.3.6.3 | Standalone MB Single Purpose Requirement | 10.4.77. |
| 9.4.3.6.3(5) | Constrained OMB Processing Capability | 10.4.81. |
| 9.4.3.6.4 | Restriction of Playback in Absence of Integrity Pack Metadata | 6.1.15. |
| 9.4.3.6.4 | Restriction of Keying to MDEK Type (OBAE) | 6.1.16. |
| 9.4.3.6.4 | OBAE Integrity Checking | 6.1.17. |
| 9.4.3.6.4 | KDM Content Keys Check | 8.2.14. |
| 9.4.3.6.4 | MB Tasks | 10.4.58. |
| 9.4.3.6.4 | Constrained OMB Processing Capability | 10.4.81. |
| 9.4.3.6.4 | Encrypted Auxiliary Data Processing | 10.4.83. |
| 9.4.3.6.5 | TLS Session Initiation | 5.2.1. |
| 9.4.3.6.5 | ASM "GetProjCert" | 5.2.2.12. |
| 9.4.3.6.5 | KDM TDL Check | 6.1.11. |
| 9.4.3.6.5 | Companion SPB Retrieve Projector Cert | 10.4.74. |
| 9.4.3.6.6 | KDM TDL Check | 6.1.11. |
| 9.4.3.6.6 | Systems without Electronic Marriage | 7.2.7. |
| 9.4.3.6.6 | Systems Without Electronic Marriage | 10.4.21. |
| 9.4.3.7 | Clock Adjustment | 6.3.1. |
| 9.4.3.7 | SPB Type 1 Clock Battery | 6.3.2. |
| 9.4.3.7 | Clock Resolution | 6.3.3. |
| 9.4.3.7 | Clock Resolution (OMB) | 6.3.4. |
| 9.4.3.7 | Clock Adjustment (OMB) | 6.3.5. |
| 9.4.3.7 | Remote SPB Clock Adjustment | 7.3.4. |
| 9.4.3.7 | Clock Date-Time-Range | 10.4.22. |
| 9.4.3.7 | Clock Setup | 10.4.23. |
| 9.4.3.7 | Clock Stability | 10.4.24. |
| 9.4.3.7 | Clock Continuity | 10.4.27. |
| 9.4.3.7 | ASM Get Time Frequency | 10.4.70. |
| 9.4.3.7 | SPB Type 1 Battery Life | 10.4.73. |
| 9.4.4 | LE Key Usage | 6.2.3. |

| | | |
|---|---|---|
| 9.4.4 | MB Link Encryption | 6.2.4. |
| 9.4.4 | LE Key Generation | 9.5.2. |
| 9.4.4.1 | Special Auditorium Situation Operations | 6.2.2. |
| 9.4.4.1 | Special Auditorium Situation Detection | 10.4.10. |
| 9.4.5 | ASM "RRP Invalid" | 5.2.2.3. |
| 9.4.5 | ASM "GetTime" | 5.2.2.4. |
| 9.4.5 | ASM "GetEventList" | 5.2.2.5. |
| 9.4.5 | ASM "GetEventID" | 5.2.2.6. |
| 9.4.5 | ASM "LEKeyLoad" | 5.2.2.7. |
| 9.4.5 | ASM "LEKeyQueryID" | 5.2.2.8. |
| 9.4.5 | ASM "LEKeyQueryAll" | 5.2.2.9. |
| 9.4.5 | ASM "LEKeyPurgeID" | 5.2.2.10. |
| 9.4.5 | ASM "LEKeyPurgeAll" | 5.2.2.11. |
| 9.4.5 | Constrained OMB Processing Capability | 10.4.81. |
| 9.4.5.1 | Secure SMS-SM Communication | 10.4.5. |
| 9.4.5.1 | Secure Remote SPB-SM Communications | 10.4.8. |
| 9.4.5.1 | TLS Endpoints | 10.4.28. |
| 9.4.5.1 | SMS and SPB Authentication and ITM Transport Layer | 10.4.30. |
| 9.4.5.2.1 | Idempotency of ITM RRPs | 10.4.31. |
| 9.4.5.2.3 | TLS Session Initiation | 5.2.1. |
| 9.4.5.2.3 | Auditorium Security Message Support | 5.2.2.1. |
| 9.4.5.2.3 | TLS Exception Logging | 5.2.3. |
| 9.4.5.2.3 | Security Design Description Requirements | 9.5.4. |
| 9.4.5.2.3 | RRP Synchronism | 10.4.32. |
| 9.4.5.2.3 | TLS Mode Bypass Prohibition | 10.4.33. |
| 9.4.5.2.3 | RRP Broadcast Prohibition | 10.4.34. |
| 9.4.5.2.3 | Implementation of Proprietary ITMs | 10.4.35. |
| 9.4.5.2.3 | RRP Initiator | 10.4.36. |
| 9.4.5.2.3 | RRP "Busy" and Unsupported Types | 10.4.39. |
| 9.4.5.2.3(9) | Secure Remote SPB-SM Communications | 10.4.8. |
| 9.4.5.2.3.(9) | Secure SMS-SM Communication | 10.4.5. |
| 9.4.5.2.3.(9) | RRP Operational Messages | 10.4.40. |
| 9.4.5.2.4 | ASM "GetProjCert" | 5.2.2.12. |
| 9.4.5.2.4 | RRP Operational Messages | 10.4.40. |

| | | |
|---|---|---|
| 9.4.5.2.4 | TLS RSA Requirement | 10.4.79. |
| 9.4.5.3 | Auditorium Security Message Support | 5.2.2.1. |
| 9.4.5.3.2 | TLS Session Initiation | 5.2.1. |
| 9.4.5.3.2 | ASM Failure Behavior | 5.2.2.2. |
| 9.4.5.3.2 | Secure Remote SPB-SM Communications | 10.4.8. |
| 9.4.5.3.2 | Maximum Key Validity Period | 10.4.15. |
| 9.4.5.3.2 | Dual Certificate SMS Authentication | 10.4.80. |
| 9.4.6.1.1 | FM Payload | 6.4.3. |
| 9.4.6.1.1 | FM Payload (OBAE) | 6.4.8. |
| 9.4.6.1.1 | FM Algorithm General Requirements | 10.4.42. |
| 9.4.6.1.1 | FM Insertion Requirements | 10.4.43. |
| 9.4.6.1.2 | IFM Visual Transparency | 10.4.44. |
| 9.4.6.1.2 | IFM Robustness | 10.4.45. |
| 9.4.6.1.3 | AFM Inaudibility | 10.4.46. |
| 9.4.6.1.3 | AFM Robustness | 10.4.47. |
| 9.4.6.1.3 | OBAE FM Robustness | 10.4.85. |
| 9.4.6.1.3 | OBAE FM Inaudibility | 10.4.86. |
| 9.4.6.2 | FM Application Constraints | 6.4.1. |
| 9.4.6.2 | Granularity of FM Control | 6.4.2. |
| 9.4.6.2 | FM Audio Bypass | 6.4.4. |
| 9.4.6.2 | Selective Audio FM Control | 6.4.5. |
| 9.4.6.2 | FM Application Constraints (OBAE) | 6.4.6. |
| 9.4.6.2 | Granularity of FM Control (OBAE) | 6.4.7. |
| 9.4.6.2 | FM Audio Bypass (OBAE) | 6.4.9. |
| 9.4.6.2 | FM Control Instance | 10.4.48. |
| 9.4.6.2(9) | FM Insertion Requirements | 10.4.43. |
| 9.4.6.3.1 | Log Records for Multiple Remote SPBs | 5.3.2.2. |
| 9.4.6.3.1 | Log Sequence Numbers | 5.3.2.3. |
| 9.4.6.3.1 | Log Collection by the SM | 5.3.2.4. |
| 9.4.6.3.1 | General Log System Failure | 5.3.2.5. |
| 9.4.6.3.1 | Log Report Signature Validity | 5.3.2.6. |
| 9.4.6.3.1 | Log Sequence Numbers (OBAE) | 5.3.2.7. |
| 9.4.6.3.1 | Log Report Signature Validity (OBAE) | 5.3.2.8. |
| 9.4.6.3.1 | Remote SPB Time Compensation | 5.3.3.4. |

| | | |
|---|---|---|
| 9.4.6.3.1 | SE Log Authoring | 10.4.50. |
| 9.4.6.3.1 | SPB Log Storage Requirements | 10.4.51. |
| 9.4.6.3.1 | Remote SPB Log Storage Requirements | 10.4.52. |
| 9.4.6.3.1 | MB Log Storage Capabilities | 10.4.53. |
| 9.4.6.3.1 | Logging for Standalone Systems | 10.4.54. |
| 9.4.6.3.2 | Log Structure | 5.3.2.1. |
| 9.4.6.3.3 | Log Report Signature Validity | 5.3.2.6. |
| 9.4.6.3.3 | Log Report Signature Validity (OBAE) | 5.3.2.8. |
| 9.4.6.3.4 | Log Sequence Numbers | 5.3.2.3. |
| 9.4.6.3.4 | Log Sequence Numbers (OBAE) | 5.3.2.7. |
| 9.4.6.3.5 | Remote SPB Time Compensation | 5.3.3.4. |
| 9.4.6.3.7 | Log Report Signature Validity | 5.3.2.6. |
| 9.4.6.3.7 | Log Report Signature Validity (OBAE) | 5.3.2.8. |
| 9.4.6.3.7 | SM Proxy of Log Events | 5.3.3.1. |
| 9.4.6.3.7 | SM Proxy of Security Operations Events | 5.3.3.2. |
| 9.4.6.3.7 | SM Proxy of Security ASM Events | 5.3.3.3. |
| 9.4.6.3.7 | FrameSequencePlayed Event | 5.4.1.1. |
| 9.4.6.3.7 | CPLStart Event | 5.4.1.2. |
| 9.4.6.3.7 | CPLEnd Event | 5.4.1.3. |
| 9.4.6.3.7 | PlayoutComplete Event | 5.4.1.4. |
| 9.4.6.3.7 | CPLCheck Event | 5.4.1.5. |
| 9.4.6.3.7 | KDMKeysReceived Event | 5.4.1.6. |
| 9.4.6.3.7 | KDMDeleted Event | 5.4.1.7. |
| 9.4.6.3.7 | FrameSequencePlayed Event (OBAE) | 5.4.1.8. |
| 9.4.6.3.7 | CPLStart Event (OBAE) | 5.4.1.9. |
| 9.4.6.3.7 | CPLEnd Event (OBAE) | 5.4.1.10. |
| 9.4.6.3.7 | PlayoutComplete Event (OBAE) | 5.4.1.11. |
| 9.4.6.3.7 | CPLCheck Event (OBAE) | 5.4.1.12. |
| 9.4.6.3.7 | KDMKeysReceived Event (OBAE) | 5.4.1.13. |
| 9.4.6.3.7 | KDMDeleted Event (OBAE) | 5.4.1.14. |
| 9.4.6.3.7 | LinkOpened Event | 5.4.2.1. |
| 9.4.6.3.7 | LinkClosed Event | 5.4.2.2. |
| 9.4.6.3.7 | LinkException Event | 5.4.2.3. |
| 9.4.6.3.7 | LogTransfer Event | 5.4.2.4. |

| | | |
|---|---|---|
| 9.4.6.3.7 | KeyTransfer Event | 5.4.2.5. |
| 9.4.6.3.7 | SPBStartup and SPBShutdown Events | 5.4.2.6. |
| 9.4.6.3.7 | SPBOpen and SPBClose Events | 5.4.2.7. |
| 9.4.6.3.7 | SPBClockAdjust Event | 5.4.2.8. |
| 9.4.6.3.7 | SPBMarriage and SPBDivorce Events | 5.4.2.9. |
| 9.4.6.3.7 | SPBSoftware Event | 5.4.2.10. |
| 9.4.6.3.7 | SPBSecurityAlert Event | 5.4.2.11. |
| 9.4.6.3.7 | Logging of Failed Procedures | 10.4.55. |
| 9.4.6.3.8 | KDM Malformations | 3.5.8. |
| 9.4.6.3.8 | KDM Malformations (OBAE) | 3.5.15. |
| 9.4.6.3.8 | SM Proxy of Log Events | 5.3.3.1. |
| 9.4.6.3.8 | SM Proxy of Security Operations Events | 5.3.3.2. |
| 9.4.6.3.8 | SM Proxy of Security ASM Events | 5.3.3.3. |
| 9.4.6.3.8 | FrameSequencePlayed Event | 5.4.1.1. |
| 9.4.6.3.8 | CPLStart Event | 5.4.1.2. |
| 9.4.6.3.8 | CPLEnd Event | 5.4.1.3. |
| 9.4.6.3.8 | PlayoutComplete Event | 5.4.1.4. |
| 9.4.6.3.8 | CPLCheck Event | 5.4.1.5. |
| 9.4.6.3.8 | KDMKeysReceived Event | 5.4.1.6. |
| 9.4.6.3.8 | KDMDeleted Event | 5.4.1.7. |
| 9.4.6.3.8 | FrameSequencePlayed Event (OBAE) | 5.4.1.8. |
| 9.4.6.3.8 | CPLStart Event (OBAE) | 5.4.1.9. |
| 9.4.6.3.8 | CPLEnd Event (OBAE) | 5.4.1.10. |
| 9.4.6.3.8 | PlayoutComplete Event (OBAE) | 5.4.1.11. |
| 9.4.6.3.8 | CPLCheck Event (OBAE) | 5.4.1.12. |
| 9.4.6.3.8 | KDMKeysReceived Event (OBAE) | 5.4.1.13. |
| 9.4.6.3.8 | KDMDeleted Event (OBAE) | 5.4.1.14. |
| 9.4.6.3.8 | LinkOpened Event | 5.4.2.1. |
| 9.4.6.3.8 | LinkClosed Event | 5.4.2.2. |
| 9.4.6.3.8 | LinkException Event | 5.4.2.3. |
| 9.4.6.3.8 | LogTransfer Event | 5.4.2.4. |
| 9.4.6.3.8 | KeyTransfer Event | 5.4.2.5. |
| 9.4.6.3.8 | SPBStartup and SPBShutdown Events | 5.4.2.6. |
| 9.4.6.3.8 | SPBOpen and SPBClose Events | 5.4.2.7. |

| | | |
|---|---|---|
| 9.4.6.3.8 | SPBClockAdjust Event | 5.4.2.8. |
| 9.4.6.3.8 | SPBMarriage and SPBDivorce Events | 5.4.2.9. |
| 9.4.6.3.8 | SPBSoftware Event | 5.4.2.10. |
| 9.4.6.3.8 | SPBSecurityAlert Event | 5.4.2.11. |
| 9.4.6.3.8 | SPBSecurityAlert Event | 5.4.2.11. |
| 9.4.6.3.8 | FM Application Constraints (OBAE) | 6.4.6. |
| 9.4.6.3.8 | Granularity of FM Control (OBAE) | 6.4.7. |
| 9.4.6.3.8 | Logging of Failed Procedures | 10.4.55. |
| 9.4.6.3.8 | Projector SPB Log Reporting Requirements | 10.4.78. |
| 9.4.6.3.10 | Logging of Failed Procedures | 10.4.55. |
| 9.4.6.3.10 | SPB Log Failure | 10.4.56. |
| 9.4.6.3.10 | Log Purging in Failed SPBs | 10.4.57. |
| 9.4.6.3.10 | SPB Type 1 Log Retention | 10.4.69. |
| 9.5.1 | Basic Certificate Structure | 2.1.1. |
| 9.5.1 | SignatureAlgorithm Fields | 2.1.2. |
| 9.5.1 | SignatureValue Field | 2.1.3. |
| 9.5.1 | SerialNumber Field | 2.1.4. |
| 9.5.1 | SubjectPublicKeyInfo Field | 2.1.5. |
| 9.5.1 | Validity Field | 2.1.7. |
| 9.5.1 | AuthorityKeyIdentifier Field | 2.1.8. |
| 9.5.1 | KeyUsage Field | 2.1.9. |
| 9.5.1 | Basic Constraints Field | 2.1.10. |
| 9.5.1 | Public Key Thumbprint | 2.1.11. |
| 9.5.1 | Organization Name Field | 2.1.12. |
| 9.5.1 | Entity Name and Roles Field | 2.1.14. |
| 9.5.1 | Unrecognized Extensions | 2.1.15. |
| 9.5.1 | Signature Validation | 2.1.16. |
| 9.5.1 | Certificate Chains | 2.1.17. |
| 9.5.1 | ASN.1 DER Encoding Check | 2.2.1. |
| 9.5.1 | Missing Required Fields | 2.2.2. |
| 9.5.1 | PathLen Check | 2.2.3. |
| 9.5.1 | OrganizationName Match Check | 2.2.4. |
| 9.5.1 | Certificate Role Check | 2.2.5. |
| 9.5.1 | Validity Date Check | 2.2.6. |

| | | |
|---|---|---|
| 9.5.1 | Signature Algorithm Check | 2.2.7. |
| 9.5.1 | Public Key Type Check | 2.2.8. |
| 9.5.1 | Issuer Certificate Presence Check | 2.2.9. |
| 9.5.1 | SPB Digital Certificate | 5.1.1. |
| 9.5.1 | TLS Session Initiation | 5.2.1. |
| 9.5.1 | Validity of Media Block Certificates | 6.1.20. |
| 9.5.1 | SMS Identity and Certificate | 8.2.11. |
| 9.5.1 | Validity of SMS Certificates | 8.2.15. |
| 9.5.1 | Type 1 SPB RSA Private Keys | 10.4.59. |
| 9.5.1 | Content Keys Outside Secure Silicon | 10.4.60. |
| 9.5.1 | Dual Certificate SMS Authentication | 10.4.80. |
| 9.5.1.1 | KeyUsage Field | 2.1.9. |
| 9.5.1.1 | SPB Digital Certificate | 5.1.1. |
| 9.5.1.1 | Log Report Signature Validity | 5.3.2.6. |
| 9.5.1.1 | Log Report Signature Validity (OBAE) | 5.3.2.8. |
| 9.5.1.1 | Systems Without Electronic Marriage | 10.4.21. |
| 9.5.1.2 | KeyUsage Field | 2.1.9. |
| 9.5.1.2 | SPB Digital Certificate | 5.1.1. |
| 9.5.1.2 | Log Report Signature Validity | 5.3.2.6. |
| 9.5.1.2 | Log Report Signature Validity (OBAE) | 5.3.2.8. |
| 9.5.1.2 | Companion SPB Marriage Break Key Retaining | 7.3.3. |
| 9.5.1.2 | Systems Without Electronic Marriage | 10.4.21. |
| 9.5.1.2 | Dual Certificate SMS Authentication | 10.4.80. |
| 9.5.1.3 | SPB Digital Certificate | 5.1.1. |
| 9.5.1.3 | Plurality of Media Block Identity Certificates | 6.1.19. |
| 9.5.2.2 | Projector and Direct View Display Physical Protection | 7.2.1. |
| 9.5.2.2 | SPB Type 1 Tamper Responsiveness | 9.5.3. |
| 9.5.2.2 | Type 1 SPB RSA Private Keys | 10.4.59. |
| 9.5.2.2 | Content Keys Outside Secure Silicon | 10.4.60. |
| 9.5.2.2 | Use of Software Protection Methods | 10.4.62. |
| 9.5.2.2 | SPB Secure Silicon Requirements | 10.4.72. |
| 9.5.2.3 | SPB2 Secure Silicon Field Replacement | 7.2.6. |
| 9.5.2.3 | Repair and Renewal of SPBs | 10.4.25. |
| 9.5.2.3 | Prohibition of SPB Type 1 Field Serviceability | 10.4.61. |

| | | |
|---|---|---|
| 9.5.2.4 | Projector and Direct View Display Physical Protection | 7.2.1. |
| 9.5.2.4 | Projector and Direct View Display Security Servicing | 7.2.2. |
| 9.5.2.4 | SPB2 Protected Devices | 10.4.26. |
| 9.5.2.4.1 | Projector and Direct View Display Physical Protection | 7.2.1. |
| 9.5.2.4.1 | Projector and Direct View Display Security Servicing | 7.2.2. |
| 9.5.2.5 | SM Operating Environment | 9.5.1. |
| 9.5.2.5 | LE Key Generation | 9.5.2. |
| 9.5.2.5 | SPB Type 1 Tamper Responsiveness | 9.5.3. |
| 9.5.2.5 | Security Design Description Requirements | 9.5.4. |
| 9.5.2.5 | SPB Type 1 FIPS Requirements | 9.5.6. |
| 9.5.2.5 | Asymmetric Key Generation | 9.5.8. |
| 9.5.2.5 | Critical Security Parameter Protection | 9.5.9. |
| 9.5.2.5 | TMS Role | 10.4.63. |
| 9.5.2.5.1 | Degraded mode(s) of operation prohibited | 9.5.11. |
| 9.5.2.5.1 | Control output inhibition | 9.5.12. |
| 9.5.2.5.1 | Maintenance role/interface prohibited | 9.5.13. |
| 9.5.2.5.1 | Self-initiated cryptographic output capability | 9.5.14. |
| 9.5.2.5.1 | Self-initiated cryptographic output capability | 9.5.15. |
| 9.5.2.5.1 | Periodic self-tests | 9.5.16. |
| 9.5.2.6 | SPB Type 1 Tamper Responsiveness | 9.5.3. |
| 9.5.2.6 | Critical Security Parameter Protection | 9.5.9. |
| 9.5.2.6 | D-Cinema Security Parameter Protection | 10.4.64. |
| 9.5.2.7 | SM Operating Environment | 9.5.1. |
| 9.5.2.7 | SPB Type 1 Firmware Modifications | 10.4.68. |
| 9.6.1 | Location of Security Manager | 10.4.6. |
| 9.6.1.2 | Location of Security Manager | 10.4.6. |
| 9.7.2 | Timed Text Decryption | 6.7.6. |
| 9.7.4 | Content Keys Outside Secure Silicon | 10.4.60. |
| 9.7.5 | Composition Playlist Signature Validation | 4.3.2. |
| 9.7.5 | DCP Integrity | 4.6.1. |
| 9.7.6 | LE Key Generation | 9.5.2. |
| 9.7.6 | Asymmetric Key Generation | 9.5.8. |
| 9.7.6 | RSA Key Entropy | 10.4.65. |
| 9.7.6 | Preloaded Symmetric Key Entropy | 10.4.66. |

| | | |
|---|---|---|
| 9.7.7 | Composition Playlist File | 4.3.1. |
| 9.7.7 | Maximum Number of DCP Keys | 6.1.12. |
| 9.7.7 | Maximum Number of DCP Keys (OBAE) | 6.1.21. |
| 9.7.7 | MD Caching of Keys | 10.4.67. |
| 9.8 | Basic Certificate Structure | 2.1.1. |
| 9.8 | SignatureAlgorithm Fields | 2.1.2. |
| 9.8 | SignatureValue Field | 2.1.3. |
| 9.8 | SerialNumber Field | 2.1.4. |
| 9.8 | SubjectPublicKeyInfo Field | 2.1.5. |
| 9.8 | Validity Field | 2.1.7. |
| 9.8 | AuthorityKeyIdentifier Field | 2.1.8. |
| 9.8 | KeyUsage Field | 2.1.9. |
| 9.8 | Basic Constraints Field | 2.1.10. |
| 9.8 | Public Key Thumbprint | 2.1.11. |
| 9.8 | Organization Name Field | 2.1.12. |
| 9.8 | OrganizationUnitName Field | 2.1.13. |
| 9.8 | Entity Name and Roles Field | 2.1.14. |
| 9.8 | Unrecognized Extensions | 2.1.15. |
| 9.8 | Signature Validation | 2.1.16. |
| 9.8 | Certificate Chains | 2.1.17. |
| 9.8 | ASN.1 DER Encoding Check | 2.2.1. |
| 9.8 | Missing Required Fields | 2.2.2. |
| 9.8 | PathLen Check | 2.2.3. |
| 9.8 | OrganizationName Match Check | 2.2.4. |
| 9.8 | Certificate Role Check | 2.2.5. |
| 9.8 | Validity Date Check | 2.2.6. |
| 9.8 | Signature Algorithm Check | 2.2.7. |
| 9.8 | Public Key Type Check | 2.2.8. |
| 9.8 | Issuer Certificate Presence Check | 2.2.9. |
| 9.8 | ETM Structure | 3.3.1. |
| 9.8 | ETM Validity Date Check | 3.3.2. |
| 9.8 | ETM Signer Element | 3.3.3. |
| 9.8 | ETM EncryptionMethod Element | 3.3.4. |
| 9.8 | KDM MessageType Element | 3.4.1. |

| | | |
|---|---|---|
| 9.8 | KDM SubjectName Element | 3.4.2. |
| 9.8 | KDM ContentAuthenticator Element | 3.4.3. |
| 9.8 | KDM KeyIdList/TypedKeyId Field | 3.4.5. |
| 9.8 | KDM EncryptedData Element | 3.4.7. |
| 9.8 | KDM KeyInfo Element | 3.4.8. |
| 9.8 | KDM DeviceListDescription Element | 3.4.9. |
| 9.8 | KDM CompositionPlaylistId Element | 3.4.13. |
| 9.8 | KDM Validity Fields | 3.4.14. |
| 9.8 | KDM KeyIdList Element | 3.4.15. |
| 9.8 | KDM CipherData Structure ID | 3.4.16. |
| 9.8 | KDM CipherData Signer Thumbprint | 3.4.17. |
| 9.8 | KDM CipherData Validity | 3.4.18. |
| 9.8 | KDM CipherData CPL ID | 3.4.19. |
| 9.8 | KDM NonCriticalExtensions Element | 3.5.1. |
| 9.8 | ETM IssueDate Field Check | 3.5.2. |
| 9.8 | Structure ID Check | 3.5.4. |
| 9.8 | Certificate Thumbprint Check | 3.5.5. |
| 9.8 | KeyInfo Field Check | 3.5.7. |
| 9.8 | KDM Malformations | 3.5.8. |
| 9.8 | KDM Signature | 3.5.9. |
| 9.8 | KDM NonCriticalExtensions Element (OBAE) | 3.5.10. |
| 9.8 | ETM IssueDate Field Check (OBAE) | 3.5.11. |
| 9.8 | Structure ID Check (OBAE) | 3.5.12. |
| 9.8 | Certificate Thumbprint Check (OBAE) | 3.5.13. |
| 9.8 | KeyInfo Field Check (OBAE) | 3.5.14. |
| 9.8 | KDM Malformations (OBAE) | 3.5.15. |
| 9.8 | KDM Signature (OBAE) | 3.5.16. |
| 9.8 | KDM Date Check | 6.1.10. |
| 9.8 | KDM TDL Check | 6.1.11. |
| 9.8 | CPL Id Check | 6.1.13. |
| 9.8 | CPL Id Check (OBAE) | 6.1.14. |
| 9.8 | KDM Date Check (OBAE) | 6.1.24. |

[This Page Left Blank Intentionally]

# Appendix H. Abbreviations

**AD**
Auxiliary Data

**AES**
Audio Engineering Society

**AES**
Advanced Encryption Standard

**CPL**
Composition PlayList

**DCI**
Digital Cinema Initiatives, LLC

**DCDM**
Digital Cinema Distribution Master

**DCP**
Digital Cinema Package

**DSM**
Digital Source Master

**ETM**
Extra Theater Message

**FM**
Forensic Marking

**FMID**
Forensic Marking Identification

**GUI**
Graphical User Interface

**IMB**
Image Media Block

**IMBO**
Image Media Block with OMB Functions

**ISO**
International Organization for Standards

**IETF**
Internet Engineering Task Force

**J2K**
JPEG2000

**KDM**
Key Delivery Message

**LCD**
Liquid Crystal Display

**LD**
Link Decryptor

**LDB**
Link Decryptor Block

**LE**
Link Encryptor

**MB**
Media Block

**MD**
Media Decryptor

**OBAE**
Object Based Audio Essence

**OMB**
Outboard Media Block

**POSIX**
Portable Operating System Interface

**RAID**
Redundant Array of Independent Disks (formerly: Redundant Array of Inexpensive Disks)

**SM**
Security Manager

**SMS**
Screen Managemnt System

**SPB**
Secure Processing Block

**SPL**
Show Play List

**SMPTE**
Society of Motion Picture and Television Engineers

**StEM**
Standard Evaluation Material

**TCP/IP**
Transmission Control Protocol/Internet Protocol

**TDL**
Trusted Device List

**TLS**
Transport Layer Security, also known as Secure Socket Layer (SSL)

**TMS**
Theater Management System

**UMID**
Unique Material Identifier

**USB**
Universal Serial Bus

**UUID**
Universally Unique Identifier

**WTF**
Wild Track Format (numbered audio channels)

**XML**
eXtensible Markup Language

# Appendix I. Subtitle Test Evaluation and Pass/Fail Criteria

## Overview

The following describes evaluation requirements, basic and specific pass/fail criteria to be used when testing the subtitle rendering capabilities of the Test Subject, as called for in Section 6.7.1: Media Block Overlay and Section 7.5.1: Projector Overlay.

It is expected that the Test Operator shall, by referencing both the CPL and the referenced subtitle track file XML, confirm that all elements expected to appear on (or off) screen for each scene, do so with all intended characteristics. This includes, but is not limited to, positioning, alignment, font size, color, script, effect, effect color, italic, underline, bold, aspect adjust and spacing, whether specified directly, default values, or inherited from ancestor values or defaults.

The colorimetric relationship between the PNG image and the image contained in the DCDM* is, at the time of publication of this document, under study. Unexpected appearance of saturation, hue, luminance and bit-depth of PNG images should be noted in the test results and brought to the attention of the manufacturer pending further work to quantify this relationship. At this time, the Test Subject shall not be subject to failing this test on such characteristics.

The behavior of the `Direction` attribute of the `Text` element and/or the Unicode Bidirectional Algorithm is, at the time of publication of this document, under study. Scenes that utilize these features should be noted in the test results and brought to the attention of the manufacturer pending further work to quantify this relationship. At this time, the Test Subject shall not be subject to failing this test on such characteristics

## Basic Pass/Fail Criteria:

This section describes general pass/fail criteria to be applied to all scenes unless Specific Criteria directs otherwise.

**Main Picture Image Track Files - Labels**: The image track files referenced by the compositions have a burned-in label in a small text font, centered horizontally and close to the bottom of the main picture. The label is comprised of the image structure of the sequence being viewed (2K, 4K, or 2K-48fps), the aspect ratio, and the name of the scene. The name of the scene may be used to locate specific pass/fail requirements for a particular scene, and descriptive notes to the test operator, providing additional context.

**Bounding Boxes**: White bounding boxes, with a one pixel size, are burned into the image track files to confirm correct positioning of the rendered timed text. Some slides, mainly those that announce upcoming scenes, present timed text that do not have bounding boxes. When bounding boxes are displayed, the associated text is intended to fall completely within the boxes. Differences in implementations can produce significant differences in the vertical positioning of text, depending on whether the renderer uses the baseline of the text characters, or the edges of the rendered characters for positioning. Exceeding the bounding boxes shall not be cause to fail the test.

**Composition Main Picture and Alpha Channel Timing**: The appearance of a particular label on the main picture, is intended to be accompanied by that scene's rendered text, and/or PNG images, as determined by the provided `FadeUpTime` and `FadeDownTime` Text and/or Image element parameters, or their default value of 2 frames if none are specified. For example, for the beginning title slide, "2K-scope-title", the image track file will display the label for 240 frames (10 seconds). The `FadeUpTime` and `FadeDownTime` parameters are not specified for the accompanying timed text, so for the 1st frame that displays the image label no timed text should be visible, the 2nd frame should have the timed text at 50% opacity of the rendered intent (the element's final opacity is specified by a parameter of the Font element), and frames 3 until 238 inclusive should have the timed text at 100% opacity of the rendered intent. Frame 239 should be

identical to frame 2, and frame 240 should have no visible timed text. Except where specified, if the timing of the rendered text and/or PNG images differs by more than plus or minus 3 frames from that commanded by the Subtitle DCDM and the controlling CPL, this is cause to fail the test.

Some of the slides that test PNG images have `FadeUpTime` and `FadeDownTime` values of zero, so it is not expected, or correct behavior, for the corresponding image track labels to be visible with these slides.

# Specific Pass/Fail Criteria.

This section lists pass/fail criteria specific to each scene in the composition. The identifier for each scene is constructed by prepending the image structure and aspect-ratio for the variant under test to the scene title. E.g. "2K-scope-title" or "2K-48fpsflat-title" as applicable. For each of the scenes, refer to the text below the identifier. Descriptions of scene specific elements may be described more fully. Scene specific pass/fail requirements are presented as bullet lists.

**Scene 1: <2K|4K[-48fps]-scope|flat|full>-title**

The evaluation of the first scene, and all subsequent scenes, must be determined from the display of a normal, single, continuous playback of the composition. To clarify, the composition must be selected, or loaded into a show playlist, and caused to play without using functions such as "pause" or "rewind", which may cause buffering, or other system behaviors that may have an effect of the ability of the system to display subtitles with the correct timing relationship to the other essence tracks.

- The rendered subtitle text must appear on screen within 3 seconds of the appearance of the label in the main picture. If this requirement is not observed, this is cause to fail this test.

**Scene 2: <2K|4K[-48fps]-scope|flat|full>-out-of-bounds-character-codes**

- In the top bounding box, the appearance of any character, space, partial character, or partial space, other than the words "Digital", and "Cinema", with no spaces between them, is cause to fail this test.
- In the middle bounding box, the appearance of any character, or partial character, is cause to fail this test.
- In the lower bounding box, the appearance of any character, space, partial character, or partial space, other than the letters "ABCDEF", with no spaces between them, is cause to fail this test.

**Scene 3: <2K|4K[-48fps]-scope|flat|full>-control-codes**

- In the top bounding box, the appearance of any character, space, partial character, or partial space, other than the words "Digital", and "Cinema", with no spaces between them, is cause to fail this test.
- In the middle bounding box, the appearance of any character, or partial character, is cause to fail this test.
- • In the lower bounding box, the appearance of any character, space, partial character, or partial space, other than the letters "ABCDEF", with no spaces between them, is cause to fail this test.

**Scene 4: <2K|4K[-48fps]-scope|flat|full>-4-byte-UTF-8-characters**

Record whether the Test Subject displays any rendered subtitles during this slide. Note: Failure to display four domino shapes is not cause to fail this test.

- If glyphs other than four domino shapes are displayed, this is cause to fail this test.

**Scene 5: <2K|4K[-48fps]-scope|flat|full>-default-font-size-attribute**

- If all the "M"s are not the same size, this is cause to fail this test.

**Scene 6: <2K|4K[-48fps]-scope|flat|full>-font-effects-1**

The text in this slide is intended to be red in color. The presence of the shadow and/or border, can cause the red to be perceived differently.

- If the size of the rendered characters does not vary in accordance with the labeled point values, this is cause to fail this test.

- If the body of all text is not substantially red, this is cause to fail this test.
- If any border or shadow effect is visible on any text labeled "No-shadow", this is cause to fail this test.
- If a green shadow effect is not visible on all text labeled "Green-Shadow", this is cause to fail this test.
- If any effect, other than a green shadow, is visible on any text labeled "Green-Shadow", this is cause to fail this test.
- If a white border effect is not visible on all text labeled "White-Border", this is cause to fail this test
- If any effect, other than a white border, is visible on any text labeled "White-Border", this is cause to fail this test.

**Scene 7: <2K|4K[-48fps]-scope|flat|full>-font-sub-super-script-1**

- If the baseline of any of the words "Normal" is not on the same level vertically, this is cause to fail this test.
- If the baseline of the word "Super" is not above that of the words "Normal", this is cause to fail this test
- If the baseline of the word "Sub" is not below that of the words "Normal", this is cause to fail this test.
- If the size of the words "Super" and "Sub" is not 0.6em compared with the 1.0em size of the words "Normal", inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion.
- If the baseline of the words "Super" and "Sub" is not offset by a minimum of 0.3em, and a maximum of 0.7em, of the baseline of the 1.0em size of the words "Normal", inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion.

**Scene 8: <2K|4K[-48fps]-scope|flat|full>-font-sub-super-script-2**

The scene contains two subtitle instances indicated by their respective bounding boxes, one above the other, designated "upper" and "lower" accordingly.

- If the baseline of both the words "Normal" on each of the two instances is not on the same level vertically, inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion.
- If the baseline of both the words "Super" is not above that of the words "Normal" on the upper instance, inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion
- If the baseline of both the words "Sub" is not below that of the words "Normal" on the lower instance, inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion
- If the baseline of the both the words "Super", or both the words "Sub", are not on the same level vertically, inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion
- If the size of the both the words "Super", or both the words "Sub", are not the same, inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion

**Scene 9: <2K|4K[-48fps]-scope|flat|full>-font-sub-super-script-3**

The scene contains two subtitle instances indicated by their respective bounding boxes, one above the other, designated "upper" and "lower" accordingly.

- For the upper instance, if the baselines of both the words "Super" are not on the same level, and above that of the word "Normal", inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion
- for the lower instance, if the baselines of both the words "Sub" are not on the same level, and below that of the word "Normal", inform the manufacturer that the Test Subject may not be fully compliant with newer Standards, but do not fail the device on this criterion

**Scene 10: <2K|4K[-48fps]-scope|flat|full>-font-italic-weight-bold-1**

- If the text on any of the lines with the bounding boxes is not yellow, this is cause to fail this test.

- If the text in each of the three lines with the bounding boxes does not have font effects corresponding to the labels, this is cause to fail this test.

**Scene 11: <2K|4K[-48fps]-scope|flat|full>-font-color-effectcolor-opacity-1**

- If the opacity of the text in the left column does not vary according to the labels, this is cause to fail this test.
- If the opacity of the border effect around the text in the right column does not vary according to the labels, record the result.

**Scene 12: <2K|4K[-48fps]-scope|flat|full>-position-screen-center-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.

**Scene 13: <2K|4K[-48fps]-scope|flat|full>-position-screen-center**

- If the text is not near the center of the screen, this is cause to fail this test.

**Scene 14: <2K|4K[-48fps]-scope|flat|full>-position-screen-4-edges-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.

**Scene 15: <2K|4K[-48fps]-scope|flat|full>-position-screen-4-edges**

- If any of the labeled rendered texts are in an incorrect location, this is cause to fail this test.

**Scene 16: <2K|4K[-48fps]-scope|flat|full>-position-screen-4-corners-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.

**Scene 17: <2K|4K[-48fps]-scope|flat|full>-position-screen-4-corners-1**

With the publication of ST 428-7:2014, the behavior of the alignment of rendered Text elements has changed. In the 2010 revision, the top, center, or bottom of the subtitle instance bounding box is aligned to the primary picture according to the Valign attribute. The 2014 revision aligns the baseline of the rendered text to the primary picture according to the Valign attribute.

- If any of the labeled rendered texts are in an incorrect location, this is cause to fail this test.
- If the Test Subject implements the 2014 Standard, only the descenders of the "Top-Left" and "Top-Right" labels are expected to appear on screen. If this is the case, do not fail the device on this criterion. However, if rendered text is visible outside the limits of the primary picture, this is cause to fail this test.
- If the Test Subject implements the 2014 Standard, the descenders of the "Bottom-Left" and "Bottom-Right" labels are expected to not appear on screen. If this is the case, do not fail the device on this criterion. However, if rendered text is visible outside the limits of the primary picture, this is cause to fail this test.

**Scene 18: <2K|4K[-48fps]-scope|flat|full>-position-screen-4-corners-2**

With the publication of ST 428-7:2014, the behavior of the alignment of rendered Text elements has changed. In the 2010 revision, the top, center, or bottom of the subtitle instance bounding box is aligned to the primary picture according to the Valign attribute. The 2014 revision aligns the baseline of the rendered text to the primary picture according to the Valign attribute.

- If any of the labeled rendered texts are in an incorrect location, this is cause to fail this test.

**Scene 19: <2K|4K[-48fps]-scope|flat|full>-position-text-off-screen-1**

- Except for the scene identifier, and the sentence inside the bounding box, the presence of any other text, partial text, or rendered artifacts is cause to fail this test with the exception of the case noted in the following item.
- The display of some of the edge-most pixels from a single off-screen character at the edge of the screen is acceptable due to implicit variation in absolute font character placement. If any pixels are displayed from an off-screen text character, record the result.

**Scene 20: <2K|4K[-48fps]-scope|flat|full>-position-text-off-screen-2**

- Except for the scene identifier, and the sentence inside the bounding box, the presence of any other text, partial text, or rendered artifacts is cause to fail this test.

**Scene 21: <2K|4K[-48fps]-scope|flat|full>-font-aspect-adjust-tests**

- If either of the two shapes that have a horizontal bar across them are not circles, this is cause to fail this test.
- If the shapes to the left of the circle with the bar in the top row do not appear as progressively narrower ellipses (the further away they are) this is cause to fail this test.
- If the shapes to the right of the circle with the bar in the top row do not appear as progressively wider ellipses (the further away they are) this is cause to fail this test.
- If the spaces between the shapes appear inconsistent with the increasing width of the shapes, this is cause to fail this test.

**Scene 22: <2K|4K[-48fps]-scope|flat|full>-space-element-tests**

- If the pairs of "M"s are not farthest apart at the top, progressively becoming closer going down, and closest together at the bottom, this is cause to fail this test.

**Scene 23: <2K|4K[-48fps]-scope|flat|full>-428-7-ruby-example-1**

- If 3 CJK characters are not displayed with 6 CJK characters above them, this is cause to fail this test

**Scene 24: <2K|4K[-48fps]-scope|flat|full>-428-7-ruby-example-2**

- If 11 large CJK characters are not displayed, this is cause to fail this test
- If 2 small CJK characters are not displayed below the first 2 large CJK characters, this is cause to fail this test
- If 6 small CJK characters are not displayed below the fourth, fifth, and sixth large CJK characters, this is cause to fail this test

**Scene 25: <2K|4K[-48fps]-scope|flat|full>-428-7-ruby-example-3**

- If the horizontal text "1963" does not appear at the top, this is cause to fail this test
- If there are not 9 CJK characters, vertically rendered below the "1963", this is cause to fail this test.

**Scene 26: <2K|4K[-48fps]-scope|flat|full>-ruby-test-1**

- If smaller annotation text reading "World Wide Web" is not displayed close to, and centered above, the larger base text "WWW", this is cause to fail this test.

**Scene 27: <2K|4K[-48fps]-scope|flat|full>-ruby-test-2**

- If smaller annotation text reading "Month Day Year" is not displayed close to, and centered above, the larger base text "10 31 2002", this is cause to fail this test.

**Scene 28: <2K|4K[-48fps]-scope|flat|full>-ruby-test-3**

- If smaller annotation text reading "Expiration Date" is not displayed close to, and centered below, the larger base text "10 31 2002", this is cause to fail this test.

**Scene 29: <2K|4K[-48fps]-scope|flat|full>-ruby-test-4**

- If smaller annotation text reading "W3C Associate Chairman" is not displayed close to, and centered below, 4 larger CJK characters, this is cause to fail this test.

**Scene 30: <2K|4K[-48fps]-scope|flat|full>-ruby-test-5**

- If smaller, vertical annotation text reading "Shinkansen" from top to bottom, is not displayed close to, and centered on the left, and right sides of 3 larger vertical CJK characters, this is cause to fail this test.

**Scene 31: <2K|4K[-48fps]-scope|flat|full>-ruby-aspectadjust-test**

- If any of the shapes are not as described, or missing, this is cause to fail this test.

**Scene 32: <2K|4K[-48fps]-scope|flat|full>-ruby-offset-test**

The pair of labels with the text 'Offset="-1"' are not expected to be exactly aligned and may vary according to the implementation. The objective of the test is to show that an offset value of -1 causes the pair to be closer than a bigger number.

- If the size of both labels in all the pairs is not equal, this is cause to fail this test.
- If the vertical offset between the four pairs of rendered text labels is not greatest on the left and least on the right, this is cause to fail this test.
- If the vertical offset between the pair of labels 'Default Offset (0)' and 'Offset="0"' is not equal, this is cause to fail this test. Note: The parentheses descend below the baseline of the remainder of the characters, which can cause the text to be further apart in this instance.

**Scene 33: <2K|4K[-48fps]-scope|flat|full>-ruby-spacing-test**

The pair of circles with the label 'Spacing="-1"' are not expected to be exactly aligned and may vary according to the implementation. The objective of the test is to show that an offset value of -1 causes the pair to be closer than a bigger number.

- If the horizontal spacing between the four pairs of same colored circles is not greatest on the left and least on the right, this is cause to fail this test.
- If the horizontal spacing between the pair of green circles and the pair of blue circles is not equal, this is cause to fail this test.

**Scene 34: <2K|4K[-48fps]-scope|flat|full>-ruby-cumulative-spacing-test**

- If the spacing between the circles in each colored set is not equal, this is cause to fail this test.

**Scene 35: <2K|4K[-48fps]-scope|flat|full>-image-main-picture-equivalency**

- If the size of the two apples is not equal, this is cause to fail this test.
- Differences in saturation, hue, luminance and bit-depth between the two images should be noted in the test results, and brought to the attention of the manufacturer. At this time, the Test Subject shall not be subject to failing this test because of such differences.

**Scene 36: <2K|4K[-48fps]-scope|flat|full>-image-positioning**

Three PNG images, with associated descriptive text, will fade in, then fade out, in sequence during this scene. Each image is an exact third, horizontally, of the scope aspect-ratio. Note that the images, as displayed in the flat aspect-ratio variant, will be slightly larger than one third of the screen width, and will not fill the screen vertically in both the flat, and full, aspect-ratio variants (the images will have their top edge aligned with the top edge of the main picture.

- If the location of any image does not match the descriptive text, this is cause to fail this test.
- If any image, or associated descriptive text does not appear when expected, this is cause to fail this test.
- If any image, or associated descriptive text does not fade in, and fade out, when expected, this is cause to fail this test.
- If the size of any image does not meet the description above, this is cause to fail this test.

**Scene 37: <2K|4K[-48fps]-scope|flat|full>-image-to-image-transition-test-1-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.

**Scene 38: <2K|4K[-48fps]-scope|flat|full>-image-to-image-transition-test-1**

A single PNG image will fill the entire screen horizontally for the first half of this scene. For the second half of the scene, the single image will be replaced by two half horizontal screen images, positioned as to be equivalent to their locations on the single image. All `FadeDownTime` and `FadeUpTime` elements are set to 00:00:00:00 which will result in a seamless transition between the subtitle instances.

- If the image displayed on the screen flickers, or any part of the image is not displayed, record the result.

**Scene 39: <2K|4K[-48fps]-scope|flat|full>-image-image-text-transparency-test-1-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.

- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 40: <2K|4K[-48fps]-scope|flat|full>-image-image-text-transparency-test-1**

This scene will display a PNG image of a seascape overlaid with a PNG image of a square yellow frame with a transparent background. Inside the yellow frame will be the rendered text "Digital Cinema", in purple.

- If the seascape, square frame, or rendered text is missing, this is cause to fail this test.
- If the seascape is not visible through both the square frame and the rendered text, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 41: <2K|4K[-48fps]-scope|flat|full>-image-image-image-transparency-test-1-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 42: <2K|4K[-48fps]-scope|flat|full>-image-image-image-transparency-test-1**

This scene will display a PNG image of a seascape overlaid with a PNG image of a square yellow frame with a transparent background. Inside the yellow frame is overlaid a PNG image of a smaller, rectangular purple frame and the text "Digital Cinema", in purple, and a transparent background.

- If the seascape, square frame, smaller rectangular frame, or PNG text are missing, this is cause to fail this test.
- If the seascape is not visible through both the square frame, the rectangular frame, and the text, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 43: <2K|4K[-48fps]-scope|flat|full>-image-image-text-transparency-test-2-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 44: <2K|4K[-48fps]-scope|flat|full>-image-image-text-transparency-test-2**

This scene will display a PNG image of a seascape overlaid with rendered text. Overlaid over the text, is a PNG image of a rose that has a transparent background. The rose will completely cover the rendered text.

- If the seascape, or the rose, are missing, this is cause to fail this test.
- If the seascape is not visible up to the edges of the rose, this is cause to fail this test.
- If any text is visible, other than the scene label in the flat and full variants, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 45: <2K|4K[-48fps]-scope|flat|full>-image-transparency-test-1**

This scene will display a green background in the main picture. Overlaid in the center, is a PNG image of a house that has transparent windows.

- If a house is not displayed in the center of the green background, this is cause to fail this test.
- If the green background is not visible through the windows of the house, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 46: <2K|4K[-48fps]-scope|flat|full>-multi-image-multi-text-test-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 47: <2K|4K[-48fps]-scope|flat|full>-multi-image-multi-text-test**

In the first half of this scene, PNG images of a house and rose, each with descriptive text overlaid, will fade in. Halfway through the scene, PNG images of an apple and a lamp, each with descriptive text, will fade in, for a total of four PNG images and four descriptive text overlays.

- If the PNG images of the house and rose, with their respective text overlays, do not appear during the first half of the scene, and do not remain on screen after their appearance, for the remainder of the scene, this is cause to fail this test.
- If the PNG images of the apple and lamp, with their respective text overlays, do not appear on screen during the second half of the scene, this is cause to fail this test.
- Per the provisions of section 6.1.6 in SMPTE ST 428-7:2014, in cases where two subtitle instances have overlapping time windows, the values of `FadeUpTime` and `FadeDownTime` elements, or their defaults, may be considered to be equal to zero. If any of the fades specified in the XML are rendered as if they were zero, this shall not be cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 48: <2K|4K[-48fps]-scope|flat|full>-image-rose-flicker-test-announce**

- If rendered text, describing the following scene, is not displayed, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 49: <2K|4K[-48fps]-scope|flat|full>-image-rose-flicker-test**

- If a rose does not appear near the center of the screen, this is cause to fail this test.
- If the rose flickers, disappears, or exhibits any other dynamic visual artifacts, this is cause to fail this test.
- For 4K test material, some renderers may be unable to display images without flickering, lagging or may display images incompletely. If the renderer displays image anomalies with 4K test material, record the result.

**Scene 50: <2K|4K[-48fps]-scope|flat|full>-text-flicker-test**

- If text inside the bounding box does not appear on the screen, this is cause to fail this test.
- If the text flickers, disappears, or exhibits any other dynamic visual artifacts, this is cause to fail this test.

**Scene 51: <2K|4K[-48fps]-scope|flat|full>-text-direction-test-1**

This scene is for informational data only. Describe the appearance of the rendered text elements displayed on the screen.

**Scene 52: <2K|4K[-48fps]-scope|flat|full>-text-direction-test-2**

This scene is for informational data only. Describe the appearance of the rendered text elements displayed on the screen.

**Scene 53: <2K|4K[-48fps]-scope|flat|full>-text-direction-test-3**

This scene is for informational data only. Describe the appearance of the rendered text elements displayed on the screen.

**Scene 54: <2K|4K[-48fps]-scope|flat|full>-text-valign-direction-test-1**

This scene is for informational data only. Describe the appearance of the rendered text elements displayed on the screen.

**Scene 55: <2K|4K[-48fps]-scope|flat|full>-end-title**

- If the rendered text does not appear on the screen, this is cause to fail this test.

# Appendix J. OBAE Test Evaluation Requirements

## J.1. Overview

This appendix specifies requirements and expected acoustic outcome from the rendering of *OBAE Rendering Expectations* by an **OBAE Sound System**.

## J.2. Configuration

The **OBAE Sound System** shall be configured as an *Ideal Environment*, as specified at [SMPTE-2098-3].

## J.3. Requirements

The test material consists of a sequence of scenes, identified in the top right corner of the image, as illustrated at Figure J.1..

The expectations for each scene are described using a combination of text and images, as illustrated at Figure J.1..

Sounds heard during each scene shall conform to the expectations specified for the scene by the corresponding table in J.4. Expectations.

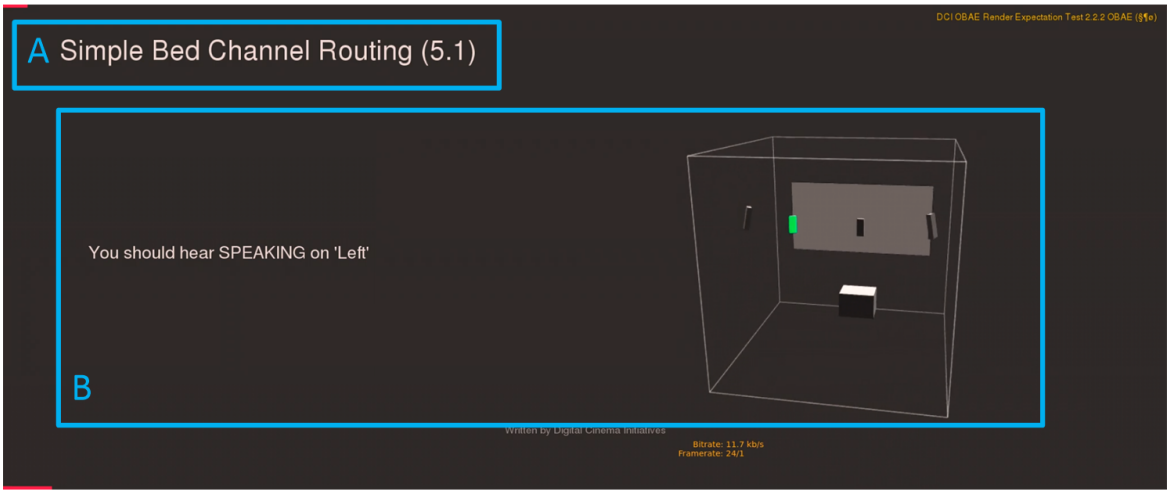
There shall be no sounds heard other than those specified at J.4. Expectations.

Expectations that refer to a specific loudpspeaker, e.g. "Left Speaker", shall be skipped if the **OBAE Sound System** is not equipped with that loudpspeaker.

Loudspeakers are defined at [SMPTE-428-12] and [SMPTE-2098-5].

All sounds heard shall be free of artifacts, e.g. "zipper" noise, discontinuities, clicks.

### Figure J.1. Visual contents of the OBAE Rendering Expectations test material.




A. Text identifying the scene.

B. Text and imagery indicating rendering expectations.

# J.4. Expectations

### Table J.1. Sync Test

| Text on screen | Expectations |
|---|---|
| `BEEP!` | A sound is heard |

### Table J.2. Simple Bed Channel Routing (5.1)

| Text on screen | Expectations |
|---|---|
| `You should hear SPEAKING on 'Left'` | The word "speaking" is heard from the Left speaker |
| `You should hear PINK on 'Left'` | Pink noise is heard from the Left speaker |
| `You should hear SPEAKING on 'Right'` | The word "speaking" is heard from the Right speaker |
| `You should hear PINK on 'Right'` | Pink noise is heard from the Right speaker |
| `You should hear SPEAKING on 'Center'` | The word "speaking" is heard from the Center speaker |
| `You should hear PINK on 'Center'` | Pink noise is heard from the Center speaker |
| `You should hear SPEAKING on 'LFE'` | The word "speaking" is heard from the LFE speaker |
| `You should hear PINK on 'LFE'` | Pink noise is heard from the LFE speaker |
| `You should hear SPEAKING on 'Left Surround'` | The word "speaking" is heard from the Left Surround speaker |

| | |
|---|---|
| You should hear PINK on 'Left Surround' | Pink noise is heard from the Left Surround speaker |
| You should hear SPEAKING on 'Right Surround' | The word "speaking" is heard from the Right Surround speaker |
| You should hear PINK on 'Right Surround' | Pink noise is heard from the Right Surround speaker |

### Table J.3. Simple Bed Channel Routing (7.1DS)

| Text on screen | Expectations |
|---|---|
| You should hear SPEAKING on 'Left' | The word "speaking" is heard from the Left speaker |
| You should hear PINK on 'Left' | Pink noise is heard from the Left speaker |
| You should hear SPEAKING on 'Right' | The word "speaking" is heard from the Right speaker |
| You should hear PINK on 'Right' | Pink noise is heard from the Right speaker |
| You should hear SPEAKING on 'Center' | The word "speaking" is heard from the Center speaker |
| You should hear PINK on 'Center' | Pink noise is heard from the Center speaker |
| You should hear SPEAKING on 'LFE' | The word "speaking" is heard from the LFE speaker |
| You should hear PINK on 'LFE' | Pink noise is heard from the LFE speaker |
| You should hear SPEAKING on 'Left Side Surround' | The word "speaking" is heard from the Left Side Surround speaker |
| You should hear PINK on 'Left Side Surround' | Pink noise is heard from the Left Side Surround speaker |
| You should hear SPEAKING on 'Right Side Surround' | The word "speaking" is heard from the Right Side Surround speaker |
| You should hear PINK on 'Right Side Surround' | Pink noise is heard from the Right Side Surround speaker |
| You should hear SPEAKING on 'Left Rear Surround' | The word "speaking" is heard from the Left Rear Surround speaker |
| You should hear PINK on 'Left Rear Surround' | Pink noise is heard from the Left Rear Surround speaker |
| You should hear SPEAKING on 'Right Rear Surround' | The word "speaking" is heard from the Right Rear Surround speaker |
| You should hear PINK on 'Right Rear Surround' | Pink noise is heard from the Right Rear Surround speaker |

### Table J.4. Simple Bed Channel Routing (9.1OH)

| Text on screen | Expectations |
|---|---|
| You should hear SPEAKING on 'Left' | The word "speaking" is heard from the Left speaker |
| You should hear PINK on 'Left' | Pink noise is heard from the Left speaker |

| | |
|---|---|
| `You should hear SPEAKING on 'Right'` | The word "speaking" is heard from the Right speaker |
| `You should hear PINK on 'Right'` | Pink noise is heard from the Right speaker |
| `You should hear SPEAKING on 'Center'` | The word "speaking" is heard from the Center speaker |
| `You should hear PINK on 'Center'` | Pink noise is heard from the Center speaker |
| `You should hear SPEAKING on 'LFE'` | Sound is heard from the LFE speaker |
| `You should hear PINK on 'LFE'` | Sound is heard from the LFE speaker |
| `You should hear SPEAKING on 'Left Side Surround'` | The word "speaking" is heard from the Left Side Surround speaker |
| `You should hear PINK on 'Left Side Surround'` | Pink noise is heard from the Left Side Surround speaker |
| `You should hear SPEAKING on 'Right Side Surround'` | The word "speaking" is heard from the Right Side Surround speaker |
| `You should hear PINK on 'Right Side Surround'` | Pink noise is heard from the Right Side Surround speaker |
| `You should hear SPEAKING on 'Left Rear Surround'` | The word "speaking" is heard from the Left Rear Surround speaker |
| `You should hear PINK on 'Left Rear Surround'` | Pink noise is heard from the Left Rear Surround speaker |
| `You should hear SPEAKING on 'Right Rear Surround'` | The word "speaking" is heard from the Right Rear Surround speaker |
| `You should hear PINK on 'Right Rear Surround'` | Pink noise is heard from the Right Rear Surround speaker |
| `You should hear SPEAKING on 'Left Top Surround'` | The word "speaking" is heard from the Left Top Surround speaker |
| `You should hear PINK on 'Left Top Surround'` | Pink noise is heard from the Left Top Surround speaker |
| `You should hear SPEAKING on 'Right Top Surround'` | The word "speaking" is heard from the Right Top Surround speaker |
| `You should hear PINK on 'Right Top Surround'` | Pink noise is heard from the Right Top Surround speaker |

### Table J.5. '91OH' Bed - Gain Test

| Text on screen | Expectations |
|---|---|
| `You should hear pink-noise`<br>`GainPrefix = ONE` | Pink noise is heard. The noise maintains consistent timbre, loudness, and size. |
| `You should hear Silence`<br>`GainPrefix = zero` | No sound is heard. |
| `You should hear the volume changing`<br>`GainPrefix = CUSTOM` | |

| | |
|---|---|
| `gain=X.XX` | Pink noise is heard. For three times in a row, the loudness of the pink noise monotically increases from silence, and then monotically decrease back to silence. The loudness scales with the value of `gain`. The noise maintains consistent timbre and size. |
| | |

### Table J.6. '91OH' Bed - Decorrelation Test

| Text on screen | Expectations |
|---|---|
| `You should hear pink noise`<br>`ChannelDecorCoefPrefix = NONE` | Pink noise is heard. |
| `You should hear pink noise`<br>`ChannelDecorCoefPrefix = MAX` | Pink noise is heard. |
| `You should hear pink noise`<br>`ChannelDecorCoefPrefix = CUSTOM XX%` | Pink noise is heard. The noise maintains consistent loudness. |

### Table J.7. Pink Noise 13.1HT Bed with 3 Spoken Conditional Beds

| Text on screen | Expectations |
|---|---|
| `You should not hear pink noise`<br>`The 13.1HT pink noise is superseded by one of the 5.1, 7.1DS, 9.1OH beds` | No sound is heard. |

### Table J.8. Bed Remap Test (Source: 13.1HT Bed, Dest: 5.1, 7.1DS, 11.1HT, 9.1OH)

| Text on screen | Expectations |
|---|---|
| `You should only hear pink noise on Center (NOT from Left)` | Pink noise is heard from the Center speaker only |
| `You should only hear pink noise on Right (NOT from Center)` | Pink noise is heard from the Right speaker only |
| `You should only hear pink noise on Left (NOT from Right)` | Pink noise is heard from the Left speaker only |
| `You should only hear pink noise on Center (NOT from Left Side Surround)` | Pink noise is heard from the Center speaker only |
| `You should only hear pink noise on Left (NOT from Right Side Surround)` | Pink noise is heard from the Left speaker only |
| `You should only hear pink noise on Center (NOT from Left Rear Surround)` | Pink noise is heard from the Center speaker only |
| `You should only hear pink noise on Left (NOT from Right Rear Surround)` | Pink noise is heard from the Left speaker only |
| `You should only hear pink noise on Right (NOT from LFE)` | Pink noise is heard from the Right speaker only |

| | |
|---|---|
| `You should only hear pink noise on Center (NOT from Left Height)` | Pink noise is heard from the Center speaker only |
| `You should only hear pink noise on Right (NOT from Center Height)` | Pink noise is heard from the Right speaker only |
| `You should only hear pink noise on Left (NOT from Right Height)` | Pink noise is heard from the Left speaker only |
| `You should only hear pink noise on Center (NOT from Left Surround Height)` | Pink noise is heard from the Center speaker only |
| `You should only hear pink noise on Left (NOT from Right Surround Height)` | Pink noise is heard from the Left speaker only |
| `You should only hear pink noise on Right (NOT from Top Surround)` | Pink noise is heard from the Right speaker only |
| The noise maintains consistent timbre and loudness in each test. | |

### Table J.9. Mixing of Two Simultaneous Beds

| Text on screen | Expectations |
|---|---|
| `You should hear: SPEAKING on 'Left'` | The word "speaking" is heard from the Left speaker |
| `You should hear: PINK on 'Left'` | Pink noise is heard from the Left speaker |
| `You should hear: SPEAKING on 'Left Center'` | The word "speaking" is heard from the Left Center speaker |
| `You should hear: PINK on 'Left Center'` | Pink noise is heard from the Left Center speaker |
| `You should hear: SPEAKING on 'Center'` | The word "speaking" is heard from the Center speaker |
| `You should hear: PINK on 'Center'` | Pink noise is heard from the Center speaker |
| `You should hear: SPEAKING on 'Right Center'` | The word "speaking" is heard from the Right Center speaker |
| `You should hear: PINK on 'Right Center'` | Pink noise is heard from the Right Center speaker |
| `You should hear: SPEAKING on 'Right'` | The word "speaking" is heard from the Right speaker |
| `You should hear: PINK on 'Right'` | Pink noise is heard from the Right speaker |
| `You should hear: SPEAKING on 'Left Side Surround'` | The word "speaking" is heard from the Left Side Surround speaker |
| `You should hear: PINK on 'Left Side Surround'` | Pink noise is heard from the Left Side Surround speaker |
| `You should hear: SPEAKING on 'Left Surround'` | The word "speaking" is heard from the Left Surround speaker |
| `You should hear: PINK on 'Left Surround'` | Pink noise is heard from the Left Surround speaker |
| `You should hear: SPEAKING on 'Left Rear Surround'` | The word "speaking" is heard from the Left Rear Surround speaker |
| `You should hear: PINK on 'Left Rear` | |

| | |
|---|---|
| Surround' | Pink noise is heard from the Left Rear Surround speaker |
| You should hear: SPEAKING on 'Right Rear Surround' | The word "speaking" is heard from the Right Rear Surround speaker |
| You should hear: PINK on 'Right Rear Surround' | Pink noise is heard from the Right Rear Surround speaker |
| You should hear: SPEAKING on 'Right Side Surround' | The word "speaking" is heard from the Right Side Surround speaker |
| You should hear: PINK on 'Right Side Surround' | Pink noise is heard from the Right Side Surround speaker |
| You should hear: SPEAKING on 'Right Surround' | The word "speaking" is heard from the Right Surround speaker |
| You should hear: PINK on 'Right Surround' | Pink noise is heard from the Right Surround speaker |
| You should hear: SPEAKING on 'Left Top Surround' | The word "speaking" is heard from the Left Top Surround speaker |
| You should hear: PINK on 'Left Top Surround' | Pink noise is heard from the Left Top Surround speaker |
| You should hear: SPEAKING on 'Right Top Surround' | The word "speaking" is heard from the Right Top Surround speaker |
| You should hear: PINK on 'Right Top Surround' | Pink noise is heard from the Right Top Surround speaker |
| You should hear: SPEAKING on 'LFE' | Sound is heard from the LFE speaker |
| You should hear: PINK on 'LFE' | Sound is heard from the LFE speaker |
| You should hear: SPEAKING on 'Left Height' | Sound is heard from the Left Height speaker |
| You should hear: PINK on 'Left Height' | Pink noise is heard from the Left Height speaker |
| You should hear: SPEAKING on 'Right Height' | Sound is heard from the Right Height speaker |
| You should hear: PINK on 'Right Height' | Pink noise is heard from the Right Height speaker |
| You should hear: SPEAKING on 'Center Height' | Sound is heard from the Center Height speaker |
| You should hear: PINK on 'Center Height' | Pink noise is heard from the Center Height speaker |
| You should hear: SPEAKING on 'Left Surround Height' | The word "speaking" is heard from the Left Surround Height speaker |
| You should hear: PINK on 'Left Surround Height' | Pink noise is heard from the Left Surround Height speaker |
| You should hear: SPEAKING on 'Right Surround Height' | The word "speaking" is heard from the Right Surround Height speaker |
| You should hear: PINK on 'Right Surround Height' | Pink noise is heard from the Right Surround Height speaker |
| You should hear: SPEAKING on 'Left Side Surround Height' | The word "speaking" is heard from the Left Side Surround Height speaker |
| You should hear: PINK on 'Left Side | |

| | |
|---|---|
| Surround Height' | Pink noise is heard from the Left Side Surround Height speaker |
| You should hear: SPEAKING on 'Right Side Surround Height' | The word "speaking" is heard from the Right Side Surround Height speaker |
| You should hear: PINK on 'Right Side Surround Height' | Pink noise is heard from the Right Side Surround Height speaker |
| You should hear: SPEAKING on 'Left Rear Surround Height' | The word "speaking" is heard from the Left Rear Surround Height speaker |
| You should hear: PINK on 'Left Rear Surround Height' | Pink noise is heard from the Left Rear Surround Height speaker |
| You should hear: SPEAKING on 'Right Rear Surround Height' | The word "speaking" is heard from the Right Rear Surround Height speaker |
| You should hear: PINK on 'Right Rear Surround Height' | Pink noise is heard from the Right Rear Surround Height speaker |
| You should hear: SPEAKING on 'Top Surround' | The word "speaking" is heard from the Top Surround speaker |
| You should hear: PINK on 'Top Surround' | Pink noise is heard from the Top Surround speaker |

### Table J.10. Object Gain Test

| Text on screen | Expectations |
|---|---|
| You should hear pink noise<br>GainPrefix = ONE | Pink noise is heard. The noise maintains consistent timbre, location, size and loudness. |
| You should hear silence<br>GainPrefix = ZERO | No sound is heard. |
| You should hear the volume changing<br>GainPrefix = CUSTOME (X.XX) | Pink noise is heard. Three times in a row, the loudness of the pink noise monotically increases from silence, and then monotically decrease back to silence. The loudness scales with the value of GainPrefix. The noise maintains consistent timbre and size. |

### Table J.11. Object Snap Test

| Text on screen | Expectations |
|---|---|
| Snap off<br>Angle: XXX° | A point source emitting pink noise is heard, making four revolutions clockwise around the room. The motion of the point source is continuous. |
| Snap On<br>Angle: XXX° | A point source emitting pink noise is heard, making four revolutions clockwise around the room. Sound is heard from only one loudspeaker at any given time. |
| SnapTolerance<br>Angle: XXX° | A point source emitting pink noise is heard, making four revolutions clockwise around the room. Sound |

| |
|---|
| may be heard from one or more loudspeakers at any given time. |
| The noise maintains consistent timbre, loudness, and size in each test. |

### Table J.12. Object Zone Gain Test (using ZERO/ONE gain flags)

| Text on screen | Expectations |
|---|---|
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the SCREEN LEFT zone` | Pink noise is heard only from screen loudspeakers left of center. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the SCREEN CENTER zone` | Pink noise is heard only from screen center loudspeakers. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the SCREEN RIGHT zone` | Pink noise is heard only from screen loudspeakers right of center. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the WALL LEFT zone` | Pink noise is heard only from loudspeakers on left wall. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the WALL RIGHT zone` | Pink noise is heard only from loudspeakers on right wall. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the REAR LEFT zone` | Pink noise is heard only from loudspeakers on left half of rear wall. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the REAR RIGHT zone` | Pink noise is heard only from loudspeakers on right half of rear wall. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the OVERHEAD LEFT zone` | Pink noise is heard only from overhead loudspeakers left of center. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the OVERHEAD RIGHT zone` | Pink noise is heard only from overhead loudspeakers right of center. |
| The noise maintains consistent timbre, loudness, and size in each test. | |

### Table J.13. Object Zone Gain Test (using decimal gain)

| Text on screen | Expectations |
|---|---|
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the SCREEN LEFT zone` | Pink noise is heard only from screen loudspeakers left of center. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the SCREEN CENTER zone` | Pink noise is heard only from screen center loudspeakers. |

| | |
|---|---|
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the SCREEN RIGHT zone` | Pink noise is heard only from screen loudspeakers right of center. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the WALL LEFT zone` | Pink noise is heard only from loudspeakers on left wall. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the WALL RIGHT zone` | Pink noise is heard only from loudspeakers on right wall. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the REAR LEFT zone` | Pink noise is heard only from loudspeakers on left half of rear wall. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the REAR RIGHT zone` | Pink noise is heard only from loudspeakers on right half of rear wall. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the OVERHEAD LEFT zone` | Pink noise is heard only from overhead loudspeakers left of center. |
| `Angle: XXX°`<br>`You should hear pink noise ONLY in the OVERHEAD RIGHT zone` | Pink noise is heard only from overhead loudspeakers right of center. |
| The noise maintains consistent timbre, loudness, and size in each test. | |

### Table J.14. Object Spread Test

| Text on screen | Expectations |
|---|---|
| `Location: Overhead`<br>`Spread Mode: Low-Rez`<br>`Spread Value: X.XX` | Pink noise is heard centered overhead. The perceived extent of the sound source may flucuates with the `Spread Value`. |
| `Location: Overhead`<br>`Spread Mode: One-D`<br>`Spread Value: X.XX` | Pink noise is heard centered overhead. The perceived extent of the sound source may flucuates with the `Spread Value`. |
| `Location: Overhead`<br>`Spread Mode: Three-D`<br>`Spread Value: x=X.XX, y=X.XX, z=X.XX` | Pink noise is heard centered on the screen. The perceived extent of the sound source may flucuates with the `Spread Value`. |
| `Location: Screen`<br>`Spread Mode: Low-Rez`<br>`Spread Value: X.XX` | Pink noise is heard centered on the screen. The perceived extent of the sound source may flucuates with the `Spread Value`. |
| `Location: Screen`<br>`Spread Mode: One-D`<br>`Spread Value: X.XX` | Pink noise is heard centered on the screen. The perceived extent of the sound source may flucuates with the `Spread Value`. |
| `Location: Screen`<br>`Spread Mode: Three-D`<br>`Spread Value: x=X.XX, y=X.XX, z=X.XX` | Pink noise is heard centered on the screen. The perceived extent of the sound source may flucuates with the `Spread Value`. |
| The noise maintains consistent loudness in each test. | |

### Table J.15. Object - Decorrelation Test

| Text on screen | Expectations |
|---|---|
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = NONE`<br>`Location: Screen` | Pink noise is heard, centered on the screen. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = MAX`<br>`Location: Screen` | Pink noise is heard, centered on the screen. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = CUSTOM (XX%)`<br>`Location: Screen` | Pink noise is heard, centered on the screen. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = NONE`<br>`Location: Rear` | Pink noise is heard, centered on the rear wall. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = MAX`<br>`Location: Rear` | Pink noise is heard, centered on the rear wall. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = CUSTOM (XX%)`<br>`Location: Rear` | Pink noise is heard, centered on the rear wall. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = NONE`<br>`Location: Left` | Pink noise is heard, centered on the left wall. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = MAX`<br>`Location: Left` | Pink noise is heard, centered on the left wall. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = CUSTOM (XX%)`<br>`Location: Left` | Pink noise is heard, centered on the left wall. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = NONE`<br>`Location: Right` | Pink noise is heard, centered on the right wall. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = MAX`<br>`Location: Right` | Pink noise is heard, centered on the right wall. |
| `You should hear pink noise`<br>`ObjectDecorCoefPrefix = CUSTOM (XX%)`<br>`Location: Right` | Pink noise is heard, centered on the right wall. |
| The noise maintains consistent loudness in each test. | |

### Table J.16. Multiple Objects (3) combined with Snap/Spread Test

| Text on screen | Expectations |
|---|---|
| `You should hear a 3 note chord (one note per object)` | |

| | |
|---|---|
| Spread On | A sound is heard, centered on the screen. |
| You should hear a 3 note chord (one note per object)<br>Snap Off, Spread Off | A sound is heard, centered on the screen. |
| You should hear a 3 note chord (one note per object)<br>Snap On | A sound is heard, centered on the screen. |
| You should hear a 3 note chord (one note per object)<br>SnapTolerance | A sound is heard, centered on the screen. |

### Table J.17. Pan Sub-Block Test #2

| Text on screen | Expectations |
|---|---|
| Sub-blocks: XXXXXX<br>RPM: XX<br>Angle: XXXXXXXX | Pink noise is heard, moving clockwise around the room. The noise maintains consistent loudness, timbre and size. |

### Table J.18. 10 Simultaneous Objects, No Bed

| Text on screen | Expectations |
|---|---|
| You should hear no drop-outs<br>Active Object: XX | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but remains primarily on the screen. |

### Table J.19. 15 Simultaneous Objects, No Bed

| Text on screen | Expectations |
|---|---|
| You should hear no drop-outs<br>Active Object: XX | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but remains primarily on the screen. |

### Table J.20. 18 Simultaneous Objects, No Bed

| Text on screen | Expectations |
|---|---|
| You should hear no drop-outs<br>Active Object: XX | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but remains primarily on the screen. |

### Table J.21. 30 Simultaneous Objects, No Bed

| Text on screen | Expectations |
|---|---|

| |
|---|
| shift but remains primarily on the screen. |

### Table J.22. 50 Simultaneous Objects, No Bed

| Text on screen | Expectations |
|---|---|
| `You should hear no drop-outs`<br>`Active Object: XX` | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but remains primarily on the screen. |

### Table J.23. 128 Simultaneous Objects, No Bed

| Text on screen | Expectations |
|---|---|
| `You should hear no drop-outs`<br>`Active Object: XX` | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but should remain primarily on the screen. |

### Table J.24. 10 Simultaneous Objects, Quiet 9.1OH Bed

| Text on screen | Expectations |
|---|---|
| `You should hear no drop-outs`<br>`Active Object: XX` | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but should remain primarily on the screen. |

### Table J.25. 15 Simultaneous Objects, Quiet 9.1OH Bed

| Text on screen | Expectations |
|---|---|
| `You should hear no drop-outs`<br>`Active Object: XX` | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but should remain primarily on the screen. |

### Table J.26. 18 Simultaneous Objects, Quiet 9.1OH Bed

| Text on screen | Expectations |
|---|---|
| `You should hear no drop-outs`<br>`Active Object: XX` | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but should remain primarily on the screen. |

### Table J.27. 30 Simultaneous Objects, Quiet 9.1OH Bed

| Text on screen | Expectations |
|---|---|
| `You should hear no drop-outs`<br>`Active Object: XX` | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but should remain primarily on the screen. |

### Table J.28. 50 Simultaneous Objects, Quiet 9.1OH Bed

| Text on screen | Expectations |
|---|---|
| `You should hear no drop-outs`<br>`Active Object: XX` | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but should remain primarily on the screen. |

### Table J.29. 118 Simultaneous Objects, Quiet 9.1OH Bed

| Text on screen | Expectations |
|---|---|
| `You should hear no drop-outs`<br>`Active Object: XX` | Pink noise is heard. The noise maintains consistent loudness and timbre. The location of the noise may shift but should remain primarily on the screen. |

### Table J.30. Authoring Tool Info Test

| Text on screen | Expectations |
|---|---|
| `You should hear a 5.1 pink-noise bed`<br>`Note: authoring info located at the Beginning of the iaFrame ChildElements` | Pink noise is heard. The noise maintains consistent loudness, timbre and size. |

### Table J.31. Authoring Tool Info Test

| Text on screen | Expectations |
|---|---|
| `You should hear a 5.1 pink-noise bed`<br>`Note: authoring info located at the End of the iaFrame ChildElements` | Pink noise is heard. The noise maintains consistent loudness, timbre and size. |

### Table J.32. Unknown Element Test

| Text on screen | Expectations |
|---|---|
| `You should hear a 5.1 pink-noise bed`<br>`Unknown element located at the beginning of the IAFrame` | Pink noise is heard. The noise maintains consistent loudness, timbre and size. |

### Table J.33. Unknown Element Test

| Text on screen | Expectations |
|---|---|
| `You should hear a 5.1 pink-noise bed`<br>`Unknown element located at the end of the IAFrame` | Pink noise is heard. The noise maintains consistent loudness, timbre and size. |

### Table J.34. User Data Test

| Text on screen | Expectations |
|---|---|
| `You should hear a 5.1 pink-noise bed`<br>`User Data located at the Beginning of the iaFrame ChildElements` | Pink noise is heard. The noise maintains consistent loudness, timbre and size. |

### Table J.35. User Data Test

| Text on screen | Expectations |
|---|---|
| `You should hear a 5.1 pink-noise bed`<br>`User Data located at the End of the iaFrame ChildElements` | Pink noise is heard. The noise maintains consistent loudness, timbre and size. |

### Table J.36. Audio Description Test

| Text on screen | Expectations |
|---|---|
| `You should hear a pink-noise bed`<br>`Audio Description: AMBIENCE, EFFECTS` | Pink noise is heard. |
| `You should hear a pink-noise bed`<br>`Audio Description: DIALOG, FOLEY, MUSIC` | Pink noise is heard. |
| `You should hear a pink-noise bed`<br>`Audio Description: AMBIENCE, DIALOG` | Pink noise is heard. |
| `You should hear a pink-noise bed`<br>`Audio Description: MUSIC` | Pink noise is heard. |
| `You should hear a pink-noise bed`<br>`Audio Description: AMBIENCE, DIALOG, EFFECTS` | Pink noise is heard. |
| `You should hear a pink-noise bed`<br>`Audio Description: ADDITIONAL, DIALOG`<br>`Note: there is a custom Audio Description present` | Pink noise is heard. |
| The noise maintains consistent loudness, timbre and size in each test. | |