Digital Cinema System Specification: Compliance Test Plan

Version 1.4b

(build 51a170f)

Approved for Distribution July 18, 2023

Digital Cinema Initiatives, LLC, Member Representative Committee

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 Sandflow Consulting LLC, San Mateo, CA, https://www.sandflow.com/, in the preparation 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

Table of Figures

Table of Examples

Table of Tables

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. Imaging Device — describes test objectives and procedures to test that imaging device 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 Policy and Reporting — Provides an overview of the consolidated testing and test reports and a standard form for reporting details of the testing environment.

  - Chapter 15. Integrated IMB Consolidated Test Sequence

  - Chapter 20. OMB Consolidated Test Sequence

  - Chapter 21. Integrated IMBO Consolidated Test Sequence

  - Chapter 24. SDR Projector Consolidated Test Sequence

  - Chapter 26. HDR Direct View Display Consolidated Test Sequence

  - Chapter 27. SDR Direct View Display Consolidated Test Sequence

  - Chapter 28. HDR Projector 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 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 testing environment 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.

1.4.3. Terms, Definitions and Abbreviated Terms

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 imaging device (see below).

High-Dynamic Range (HDR)
Refers to image content that conforms to the HDR-DCDM characteristics specified at [DCI-HDR].

Standard Dynamic Range (SDR)
Refers to image content that conforms to the Image DCDM characteristics specified at [SMPTE-428-1].

Imaging Device
The imaging device is the device responsible for converting the electrical signals from the Media Block to a human visible picture. This includes all necessary power supplies and cabling. This includes both Projectors and Direct View

Displays.

Testing Organization

An organization which offers testing services based on this document.

Test Operator

A member of the Testing Organization that performs testing services.

Test Subject

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

Theater System

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

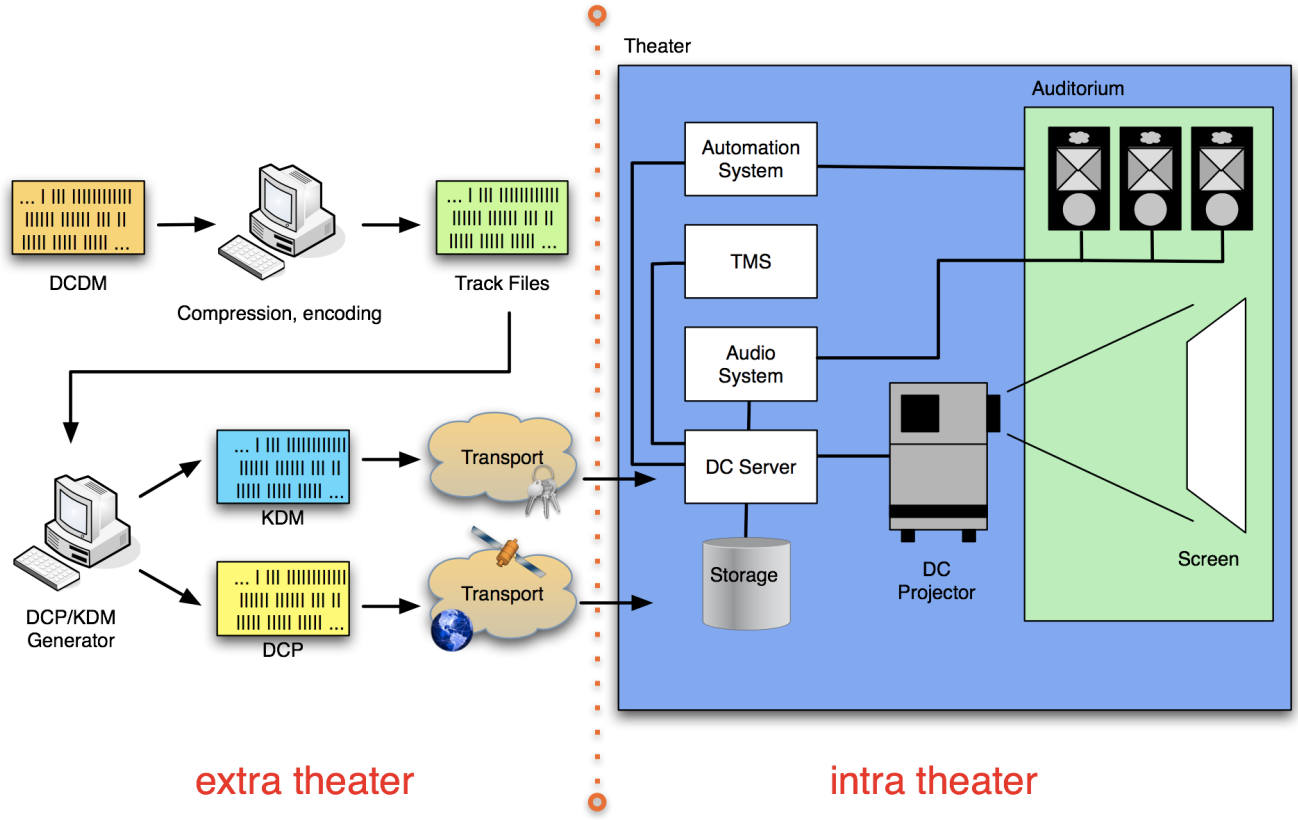

Figure 1.1. Typical DCI Compliant System Configuration

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 theater 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 Imaging Device, 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 Imaging Device'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.

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:

```
$ 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.

Example 2.1. D-Cinema 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 ITU-X509 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 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 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 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 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 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 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 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 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 `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 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 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 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 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 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 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 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 Test Subject 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 SMPTE-430-2
Test Materials	*chain-c3-BER-enc* *chain-c1-root* *chain-c3-root* *IMB-chain-a3-BER-enc* *chain-a3-root* *chain-b1-roo*

2.2.2. Missing Required Fields

Objective

Verify that certificates with missing required fields are rejected by a Test Subject.

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* *chain-c3-no-svf* *chain-c3-no-ver* *chain-c3-no-sn* *chain-c3-no-sig* *chain-c3-no-issuer* *chain-c3-no-subject* *chain-c3-no-spki* *chain-c3-no-val-f* *chain-c3-no-aki-f* *chain-c3-no-keyuse* *chain-c3-no-basic* *chain-c1-root* *chain-c3-root* *chain-a3-no-aki-f* *chain-a3-no-basic* *chain-a3-no-issuer* *chain-a3-no-keyuse* *chain-a3-no-saf* *chain-a3-no-sig* *chain-a3-no-sn* *chain-a3-no-spki*

	chain-a3-no-subject *chain-a3-no-svf* *chain-a3-no-val-f* *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 Test Subject 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 Test Subject 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 Test Subject 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 Test Subject 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 SMPTE-420-2
Test Materials	*chain-c3-path-1* *chain-c3-path-2* *chain-c3-path-3* *chain-c3-path-4* *chain-c3-path-5* *chain-c3-path-6* *chain-c3-path-7* *chain-c3-root* *chain-a3-path-1* *chain-a3-path-2* *chain-a3-path-3* *chain-a3-path-4* *chain-a3-path-5*

	chain-a3-path-6 *chain-a3-path-7* *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 SMPTE-420-2
Test Materials	*chain-c3-org-name* *chain-c3-root* *chain-a3-org-name* *chain-a3-root*

2.2.5. Certificate Role Check

Objective

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

Procedures

Perform an operation on the Test Subject 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, 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 SMPTE-420-2
Test Materials	*chain-c3-role-1* *chain-c3-role-2*

	chain-c3-root *chain-a3-role-1* *chain-a3-role-2* *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 SMPTE-420-2
Test Materials	*chain-c3-date-exp* *chain-c3-root* *chain-a3-date-exp* *chain-a3-root*

2.2.7. Signature Algorithm Check

Objective

Verify that a certificate is rejected by a Test Subject 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 SMPTE-420-2
Test Materials	*chain-c3-osig-type* *chain-c3-isig-type* *chain-c3-iosig-type* *chain-c3-root* *chain-a3-iosig-type* *chain-a3-isig-type* *chain-a3-osig-type* *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 SMPTE-420-2
Test Materials	*chain-c3-no-rsa* *chain-c3-short-rsa* *chain-c3-bad-exp* *chain-c3-root* *chain-a3-no-rsa* *chain-a3-bad-exp* *chain-a3-short-rsa* *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 Test Subject 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 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.):

```
<?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>
```

Example 3.1. Packing List Example (Partial)

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:

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

Example 3.2. checksig execution

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:

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

Example 3.3. dsig_cert.py execution

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.

```
-----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-----
```

Example 3.4. An X.509 certificate in PEM format

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.

```
$ 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
```

Example 3.5. dsig_extract.py execution

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.

```
<?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 3.6. KDM - AuthenticatedPublic 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 3.7. KDM - AuthenticatedPrivate 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#WithComments" 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

Example 3.8. KDM - Signature area

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:

```
$ 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

Example 3.9. kdm-decrypt Usage and Output

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 SMPTE-430-3
Test Equipment	**schema-check** **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** **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

	SMPTE-430-2
Test Equipment	**Text Editor** **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 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. 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 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** **schema-check** **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 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 SMPTE-430-1 SMPTE-430-2
Test Equipment	**Text Editor** **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 SMPTE-429-7 SMPTE-430-1
Test Equipment	**dc-thumbprint** **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** **checksig** **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-DCSS, 9.8 SMPTE-430-1
Test Equipment	**Text Editor**

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 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 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 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 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 SMPTE-430-3
Test Equipment	**Text Editor**

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 SMPTE-429-7 SMPTE-430-1
Test Equipment	**Text Editor** **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 RFC-3339 SMPTE-430-1
Test Equipment	**Text Editor** **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 SMPTE-430-1
Test Equipment	**kdm-decrypt** **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 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 SMPTE-430-1 SMPTE-430-2
Test Equipment	**dc-thumbprint** **kdm-decrypt** **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 SMPTE-430-1
Test Equipment	**Text Editor** **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 SMPTE-430-1
Test Equipment	**Text Editor** **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** **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 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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with non-empty NonCriticalExtensions* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with expired Signer certificate* *KDM issued before certificate valid* *KDM validity exceeds signer validity* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with corrupted CipherData block*

DCI 2K StEM (Encrypted)

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with incorrect signer thumbprint* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with KeyInfo mismatch* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3 SMPTE-430-5
Test Materials	*KDM with empty TDL* *KDM with expired Signer certificate* *KDM with invalid XML* *KDM with invalid MessageType* *KDM with incorrect namespace name value* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3 SMPTE-430-5
Test Materials	*KDM with incorrect message digest* *KDM with incorrect signer thumbprint* *KDM without signer certificate* *KDM signed with incorrect signer certificate format* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with non-empty NonCriticalExtensions (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with expired Signer certificate (OBAE)* *KDM issued before certificate valid (OBAE)* *KDM validity exceeds signer validity (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with corrupted CipherData block (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with incorrect signer thumbprint (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	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 SMPTE-430-1 SMPTE-430-3
Test Materials	*KDM with KeyInfo mismatch (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	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 SMPTE-430-1 SMPTE-430-3 SMPTE-430-5
Test Materials	*KDM with empty TDL (OBAE)* *KDM with expired Signer certificate (OBAE)* *KDM with invalid XML (OBAE)* *KDM with invalid MessageType (OBAE)* *KDM with incorrect namespace name value (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	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 SMPTE-430-1 SMPTE-430-3 SMPTE-430-5
Test Materials	*KDM with incorrect message digest (OBAE)* *KDM with incorrect signer thumbprint (OBAE)* *KDM without signer certificate (OBAE)* *KDM signed with incorrect signer certificate format (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	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, 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]

```
<?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 4.1. Asset Map

```
<?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.

Example 4.2. Volume Index

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 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 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].

```
<?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

Example 4.3. Packing List

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 SMPTE-429-8
Test Equipment	**schema-check** **uuid_check.py** **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 PKCS-1 RFC-3174 SMPTE-429-8
Test Equipment	**checksig** **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].

```
<?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

Example 4.4. Composition Playlist

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 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** **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

```
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)

Example 4.5. MXF Partition Header

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.

```
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

Example 4.6. Source Package structure

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

```
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)

Example 4.7. Cryptographic Framework and Cryptographic Context

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

```
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 (JPEG2000PictureSubDescriptor) 7
             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 = 227f187f007f007ebc76ea76ea76bc6f4c6f4c6f645803580358455fd25fd25f61
```

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

Example 4.8. Essence Descriptor for JPEG 2000

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.

```
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*.

Example 4.9. Essence Descriptor for PCM Audio

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.

```
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

Example 4.10. MXF Random Index Pack (RIP)

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 SMPTE-377-1 SMPTE-379-1 SMPTE-382 SMPTE-422 SMPTE-429-2 SMPTE-429-3 SMPTE-429-4 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 SMPTE-428-7

	SMPTE-429-5 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): 0104000101050303000077888888888
Quantization Default (33): 227f187f007f007ebc76ea76ea76bc6f4c6f4c6f645803580358455fd25fd25
```

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 SMPTE-336 SMPTE-422
Test Equipment	**asdcp-test** **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.

    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.

    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 SMPTE-428-1
Test Equipment	**klvwalk** **asdcp-test** **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 ISO-15444-1

	ISO-15444-1-AMD-1 SMPTE-429-4
Test Equipment	**asdcp-test** **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 SMPTE-428-2 SMPTE-428-3 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 ISO-144496 ISO-15948 SMPTE-428-7
Test Equipment	**schema-check** **ftlint** **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
t0MirEHOVFF4MilIP0iYVjrvb14= 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 PKCS-1 RFC-3174 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 Leaf Certificate Criteria

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 and RES roles	false	true
includes the SM, MIC and RES roles, but does not include the LS role	false	true
includes LS 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 SMPTE-430-2

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
20.4. OMB Confidence Sequence	Pass/Fail	—
21.4. Integrated IMBO Confidence Sequence	Pass/Fail	—
24.2. SDR Projector Test Sequence	Pass/Fail	—
24.4. SDR Projector Confidence Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
26.4. HDR Direct View Display Confidence Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
27.4. SDR Direct View Display Confidence Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—
28.4. HDR Projector Confidence 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

5.2.1. Deleted Section

The section "TLS Session Initiation" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2. Auditorium Security Messages

5.2.2.1. Deleted Section

The section "Auditorium Security Message Support" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.2. Deleted Section

The section "ASM Failure Behavior" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.3. Deleted Section

The section "ASM 'RRP Invalid'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.4. Deleted Section

The section "ASM 'GetTime'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.5. Deleted Section

The section "ASM 'GetEventList'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.6. Deleted Section

The section "ASM 'GetEventID'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.7. Deleted Section

The section "ASM 'LEKeyLoad'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.8. Deleted Section

The section "ASM 'LEKeyQueryID'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.9. Deleted Section

The section "ASM 'LEKeyQueryAll'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.10. Deleted Section

The section "ASM 'LEKeyPurgeID'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.11. Deleted Section

The section "ASM 'LEKeyPurgeAll'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.2.12. Deleted Section

The section "ASM 'GetProjCert'" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.2.3. Deleted Section

The section "TLS Exception Logging" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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

```
<?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#DeviceTypeTokens">SM
    </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

Example 5.1. Log Report Example

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.

```
<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</EventType> 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.

Example 5.2. Log Report Record Example

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.

```
<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-20010315" />
      <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.

Example 5.3. Log Report Signature Example

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. Deleted Section

The section "Log Record Proxy" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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 RFC-4122 SMPTE-430-4 SMPTE-433
Test Equipment	**schema-check** **uuid_check.py**
Test Materials	*DCI 2K StEM (Encrypted)* *KDM for 2K StEM (Encrypted)* *DCI 2K StEM (OBAE) (Encrypted)* *KDM for 2K StEM (Encrypted) (OBAE)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

5.3.2.2. Deleted Section

The section "Log Records for Multiple Remote SPBs" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Text Editor**
Test Materials	*DCI 2K StEM (Encrypted)* *KDM for 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

5.3.2.4. Deleted Section

The section "Log Collection by the SM" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.3.2.5. Deleted Section

The section "General Log System Failure" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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 SMPTE-430-4 SMPTE-430-5 SMPTE-433
Test Equipment	**Text Editor** **openssl**
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Text Editor**
Test Materials	*DCI 2K StEM (OBAE) (Encrypted)* *KDM for 2K StEM (Encrypted) (OBAE)*

Consolidated Test Sequences

Sequence	Type	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 SMPTE-430-4 SMPTE-430-5 SMPTE-433
Test Equipment	**Text Editor** **openssl**
Test Materials	*DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*

Consolidated Test Sequences

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

5.3.3. SM Proxy of Log Events

5.3.3.1. Deleted Section

The section "SM Proxy of Log Events" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.3.3.2. Deleted Section

The section "SM Proxy of Security Operations Events" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.3.3.3. Deleted Section

The section "SM Proxy of Security ASM Events" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.3.3.4. Deleted Section

The section "Remote SPB Time Compensation" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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

	SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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 SMPTE-430-4

	SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock**

Test Materials	*DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (OBAE) (Encrypted)*

KDM for DCI 2K Sync Test (OBAE) (Encrypted)

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
20.4. 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*

Consolidated Test Sequences

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

5.4.2. ASM and Operations Events

5.4.2.1. Deleted Section

The section "LinkOpened Event" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.4.2.2. Deleted Section

The section "LinkClosed Event" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.4.2.3. Deleted Section

The section "LinkException Event" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.4.2.4. Deleted Section

The section "LogTransfer Event" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

5.4.2.5. Deleted Section

The section "KeyTransfer Event" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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].

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.

Supporting Materials

Reference Documents	DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8 SMPTE-430-4 SMPTE-430-5 SMPTE-430-6
Test Equipment	**Computer with POSIX OS** **Accurate Real-Time Clock** **Text Editor**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 an Imaging Device, 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 an Imaging Device:

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.

Supporting Materials

Reference Documents	DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8 SMPTE-430-4 SMPTE-430-5 SMPTE-430-6
Test Equipment	**Computer with POSIX OS** **Accurate Real-Time Clock** **Text Editor**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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].

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.

Supporting Materials

Reference Documents	DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8 SMPTE-430-4 SMPTE-430-5 SMPTE-430-6
Test Equipment	**Computer with POSIX OS** **Accurate Real-Time Clock** **Text Editor**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

5.4.2.9. SPBMarriage and SPBDivorce Events

Objective

Verify that the SM of a Media Block, married to an Imaging Device, 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 an Imaging Device:

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 Imaging Device SPB2.

3. Using the manufacturer's documented procedure, remarry the Media Block to its Imaging Device 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 SMPTE-430-4 SMPTE-430-5 SMPTE-430-6
Test Equipment	**Computer with POSIX OS** **Accurate Real-Time Clock** **Text Editor**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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].

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.

Supporting Materials

Reference Documents	DCI-DCSS, 9.4.6.3.7, 9.4.6.3.8 SMPTE-430-4 SMPTE-430-5 SMPTE-430-6
Test Equipment	**Computer with POSIX OS** **Accurate Real-Time Clock** **Text Editor**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
20.4. OMB Confidence Sequence	Pass/Fail	—
21.4. Integrated IMBO Confidence Sequence	Pass/Fail	—

5.4.2.11. SPBSecurityAlert Event

Objective

The following does not apply to a Test Subject that is an Imaging Device SPB. Verify that, where the SM 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 SMPTE-430-4 SMPTE-430-5
Test Equipment	**Computer with POSIX OS** **Accurate Real-Time Clock** **Text Editor**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Data only	—
20.2. OMB Test Sequence	Data only	—
21.2. Integrated 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 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 SMPTE-429-6 SMPTE-429-5
Test Equipment	**Text Editor**
Test Materials	*DCI 2K StEM (Encrypted)* *KDM for 2K StEM (Encrypted)* *DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)* *KDM for DCI Malformed Test 1: Picture with Frame-out-of-order error (Encrypted)* *DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)* *KDM for DCI Malformed Test 5: DCP With an incorrect image TrackFile ID (Encrypted)*

	DCI Malformed Test 9: Picture with HMAC error in MXF Track File (Encrypted) *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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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)* *KDM for DCI Malformed Test 2: Sound with Frame-out-of-order error (Encrypted)* *DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)* *KDM for DCI Malformed Test 4: DCP With an incorrect audio TrackFile ID (Encrypted)* *DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)* *KDM with invalid MIC Key (Sound) for DCI 2K Sync Test with KDM-Borne MIC Keys (Encrypted)* *DCI 2K Sync Test (Encrypted)* *KDM with MIC Key (Sound) for DCI 2K Sync Test (Encrypted)* *DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)* *KDM for DCI Malformed Test 10: Sound with HMAC error in MXF Track File (Encrypted)* *DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)* *KDM for DCI Malformed Test 12: Sound with Check Value error in MXF Track File (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-5
Test Materials	*KDM with mismatched keytype* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-5
Test Materials	*DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)* *KDM for DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)*

	DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted) *KDM for DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)* *DCI Malformed Test 13: CPL that references a non-existent track file (Encrypted)* *KDM for 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)* *KDM for 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)* *KDM for DCI Malformed Test 15: CPL signed by a certificate not conforming to ST 430-2 (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated IMBO Confidence Sequence	Pass/Fail	—

6.1.6. Deleted Section

The section "Remote SPB Integrity Monitoring" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

6.1.7. Deleted Section

The section "SPB Integrity Fault Consequences" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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)* *End of Engagement -Past Time Window Extension (Encrypted)* *KDM for Within Time Window Extension (Encrypted)* *KDM for Past Time Window Extension (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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 SMPTE-429-7 SMPTE-430-1 SMPTE-430-2 SMPTE-430-5
Test Materials	*DCI 2K StEM (Encrypted)* *KDM with invalid ContentAuthenticator* *DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)* *KDM for DCI Malformed Test 16: CPL signed with No Role Certificate (Encrypted)* *DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)* *KDM for DCI Malformed Test 17: CPL signed with Bad Role Certificate (Encrypted)* *DCI Malformed Test 18: CPL signed with Extra Role Certificate (Encrypted)* *KDM for DCI Malformed Test 18: KDM for CPL signed with Extra Role Certificate (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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 SMPTE-430-1 SMPTE-430-5
Test Materials	*KDM with future validity period* *KDM that has recently expired* *KDM that has expired* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 an Imaging Device 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 Imaging Device 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 Imaging Device alone on the TDL*, which is a KDM with a TDL that contains only the certificate thumbprint of the Imaging Device 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 Imaging Device 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.

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 SMPTE-430-1 SMPTE-430-5
Test Materials	*KDM with Assume Trust and random TDL entries* *KDM with the SM alone on the TDL* *KDM with the Imaging Device alone on the TDL* *KDM with random TDL entry* *KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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 SMPTE-430-1
Test Materials	*128 Reel Composition, "A" Series* *128 Reel Composition, "B" Series* *128 Reel Composition, "A" Series (Encrypted)* *128 Reel Composition, "B" Series (Encrypted)* *KDM for 128 Reel Composition, "A" Series (Encrypted)* *KDM for 128 Reel Composition, "B" Series (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3 SMPTE-430-5

Test Materials	*KDM with bad CipherData CompositionPlaylistId value* *KDM with bad CompositionPlaylistId value* *DCI 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-3 SMPTE-430-5
Test Materials	*KDM with bad CipherData CompositionPlaylistId value (OBAE)* *KDM with bad CompositionPlaylistId value (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 m25_integrity_pict_mic_ct.kdm.xml m25_integrity_pict_mic_j2c_ct.mxf	`FrameMICError`	IMB, IMBO
m27_integrity_pict_tfid_ct.cpl.xml m27_integrity_pict_tfid_ct.cpl.xml m27_integrity_pict_tfid_j2c_ct.mxf	`TrackFileIDError`	IMB, IMBO
m26_integrity_pict_snum_ct.cpl.xml m26_integrity_pict_snum_ct.kdm.xml m26_integrity_pict_snum_j2c_ct.mxf	`FrameSequenceError`	IMB, IMBO
m28_integrity_snd_mic_ct.cpl.xml m28_integrity_snd_mic_ct.kdm.xml m28_integrity_snd_mic_pcm_ct.mxf	`FrameMICError`	IMB, IMBO
m30_integrity_snd_tfid_ct.cpl.xml m30_integrity_snd_tfid_ct.kdm.xml m30_integrity_snd_tfid_pcm_ct.mxf	`TrackFileIDError`	IMB, IMBO
m29_integrity_snd_snum_ct.cpl.xml m29_integrity_snd_snum_ct.kdm.xml m29_integrity_snd_snum_pcm_ct.mxf	`FrameSequenceError`	IMB, IMBO
m20_integrity_obae_ms_mic_ct.cpl.xml m20_integrity_obae_ms_mic_ct.kdm.xml 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 m22_integrity_obae_ms_tfid_pcm_ct.mxf	`TrackFileIDError`	IMB, IMBO
m21_integrity_obae_ms_snum_ct.cpl.xml m21_integrity_obae_ms_snum_ct.kdm.xml m21_integrity_obae_ms_snum_pcm_ct.mxf	`FrameSequenceError`	IMB, IMBO
m19_integrity_obae_mic_ct.cpl.xml m19_integrity_obae_mic_ct.kdm.xml m19_integrity_obae_mic_obae_ct.mxf	`FrameMICError`	OMB, IMBO
m24_integrity_obae_tfid_ct.cpl.xml m24_integrity_obae_tfid_ct.kdm.xml m24_integrity_obae_tfid_obae_ct.mxf	`TrackFileIDError`	OMB, IMBO
m23_integrity_obae_snum_ct.cpl.xml m23_integrity_obae_snum_ct.kdm.xml 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

	SMPTE-429-6 SMPTE-430-5
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*M25 Composition with Malformed Integrity Pack: Missing MIC item (Picture) (Encrypted)* *KDM for M25 Composition with Malformed Integrity Pack: Missing MIC item (Picture) (Encrypted)* *M25 Picture Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)* *M27 Composition with Malformed Integrity Pack: Missing TrackFileID item (Picture) (Encrypted)* *KDM for M27 Composition with Malformed Integrity Pack: Missing TrackFileID item (Picture) (Encrypted)* *M27 Picture Track File with Malformed Integrity Pack: Missing TrackFileID item (Encrypted)* *M26 Composition with Malformed Integrity Pack: Missing SequenceNumber item (Picture) (Encrypted)* *KDM for M26 Composition with Malformed Integrity Pack: Missing SequenceNumber item (Picture) (Encrypted)* *M26 Picture Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)* *M28 Composition with Malformed Integrity Pack: Missing MIC item (PCM) (Encrypted)* *KDM for M28 Composition with Malformed Integrity Pack: Missing MIC item (PCM) (Encrypted)* *M28 Sound Track File with Malformed Integrity Pack: Missing MIC item (Encrypted)* *M30 Composition with Malformed Integrity Pack: Missing TrackFileID item (PCM) (Encrypted)* *KDM for M30 Composition with Malformed Integrity Pack: Missing TrackFileID item (PCM) (Encrypted)* *M30 Sound Track File with Malformed Integrity Pack: Missing TrackFileID item (Encrypted)* *M29 Composition with Malformed Integrity Pack: Missing SequenceNumber item (PCM) (Encrypted)* *KDM for M29 Composition with Malformed Integrity Pack: Missing SequenceNumber item (PCM) (Encrypted)* *M29 Sound Track File with Malformed Integrity Pack: Missing SequenceNumber item (Encrypted)* *M20 Composition with Malformed Integrity Pack: Missing MIC item (OBAE Main Sound) (Encrypted)* *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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1 SMPTE-430-5
Test Equipment	**Text Editor**
Test Materials	*KDM with mismatched KeyType value (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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)* *M40 OBAE DCP with Frame-out-of-order error (Encrypted)* *M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)* *DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)* *M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)* *M44 OBAE DCP with HMAC value error in MXF Track File (Encrypted)* *KDM for M40 OBAE DCP with Frame-out-of-order error (Encrypted)* *KDM for M41 OBAE DCP with an incorrect TrackFile ID (Encrypted)* *KDM for M43 OBAE DCP with Check Value error in MXF Track File (Encrypted)* *KDM with invalid MIC Key for DCI 2K Sync Test with MIC Key (OBAE) (Encrypted)* *KDM with MIC Key for DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for M44 OBAE DCP with HMAC Value error in MXF Track File (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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)* *End of Engagement - Within Time Window Extension (OBAE) (Encrypted)* *KDM for Past Time Window Extension (OBAE) (Encrypted)* *KDM for Within Time Window Extension (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
20.4. OMB 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 SMPTE-430-2
Test Materials	*KDM for 2K StEM (Encrypted) (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

6.1.20. Validity of SPB Certificates

Objective

Verify that the certificates of the SPB are valid.

Procedures

1. Obtain, from the manufacturer, (i) the one or more X.509 digital leaf certificates associated with the Test Subject 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 SMPTE-430-2
Test Equipment	**Network Analyzer** **openssl**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
20.4. OMB Confidence Sequence	Pass/Fail	—
20.4. OMB Confidence Sequence	Pass/Fail	—
21.4. Integrated IMBO Confidence Sequence	Pass/Fail	—
24.2. SDR Projector Test Sequence	Pass/Fail	—
24.4. SDR Projector Confidence Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
26.4. HDR Direct View Display Confidence Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
27.4. SDR Direct View Display Confidence Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—
28.4. HDR Projector 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 SMPTE-430-1
Test Materials	*128 Reel Composition, "A" Series (OBAE)* *128 Reel Composition, "B" Series (OBAE)* *128 Reel Composition, "A" Series (OBAE) (Encrypted)* *128 Reel Composition, "B" Series (OBAE) (Encrypted)* *KDM for 128 Reel Composition, "A" Series (OBAE) (Encrypted)* *KDM for 128 Reel Composition, "B" Series (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-5
Test Materials	*DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)* *KDM for DCI Malformed Test 6b: CPL with incorrect track file hashes (OBAE) (Encrypted)* *DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)* *KDM for DCI Malformed Test 7b: CPL with an Invalid Signature (OBAE) (Encrypted)* *DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)* *KDM for DCI Malformed Test 13b: CPL that references a non-existent track file (OBAE) (Encrypted)* *DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)* *KDM for DCI Malformed Test 14b: CPL that does not conform to ST 429-7 (OBAE) (Encrypted)* *DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)* *KDM for DCI Malformed Test 15b: CPL signed by a certificate not conforming to ST 430-2 (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
20.4. OMB Confidence Sequence	Pass/Fail	—
21.4. Integrated IMBO 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 SMPTE-429-7 SMPTE-430-1 SMPTE-430-2 SMPTE-430-5
Test Materials	*DCI 2K StEM (OBAE) (Encrypted)* *KDM with invalid ContentAuthenticator (OBAE)* *DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)* *KDM for DCI Malformed Test 16b: CPL signed with No Role Certificate (OBAE) (Encrypted)* *DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)* *KDM for DCI Malformed Test 17b: CPL signed with Bad Role Certificate (OBAE) (Encrypted)* *DCI Malformed Test 18b: CPL signed with Extra Role Certificate (OBAE) (Encrypted)* *KDM for DCI Malformed Test 18b: KDM for CPL signed with Extra Role Certificate (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
20.4. 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 SMPTE-430-1 SMPTE-430-5
Test Materials	*KDM with future validity period (OBAE)* *KDM that has recently expired (OBAE)* *KDM that has expired (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)*

Consolidated Test Sequences

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

6.2. Link Encryption (LE)

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. Deleted Section

The section "Special Auditorium Situation Operations" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

6.2.3. Deleted Section

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

6.2.4. Deleted Section

The section "MB Link Encryption" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

6.3. Clocks and Time

This section describes general requirements concerning the time awareness of the components of the theater system. 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)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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)* *KDM for 64 1 second reel Composition (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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)* *KDM for 64 1 second reel Composition (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	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)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
20.4. 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** **Accurate Real-Time Clock**
Test Materials	*2K FM Application Constraints (Encrypted)* *KDM for 2K FM Application Constraints (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1
Test Equipment	**FM Detector** **Accurate Real-Time Clock**
Test Materials	*2K FM Control Granularity - No FM (Encrypted)* *2K FM Control Granularity - Image Only FM (Encrypted)* *2K FM Control Granularity - Sound Only FM (Encrypted)* *2K FM Control Granularity - Image and Sound FM (Encrypted)* *KDM for 2K FM Control Granularity - No FM (Encrypted)* *KDM for 2K FM Control Granularity - Image Only FM (Encrypted)* *KDM for 2K FM Control Granularity - Sound Only FM (Encrypted)* *KDM for 2K FM Control Granularity - Image and Sound FM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

6.4.3. FM Payload

Objective

- Verify that the Forensic Marking data payload 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 the correct number of bits is allocated for the time stamp and location data.
- Verify that the entire Forensic Marking data payload is included in each five minute segment.

- Verify that recovery is possible with a 30-minute content sample for positive identification.

Procedures

1. Determine, from the manufacturer, if the location data allows 524,288 (19 bits) or 1,048,576 (20 bits) distinct values.

2. Setup and play a show using the composition *2K FM Payload (Encrypted)*, keyed with *KDM for KDM for 2K FM Payload (Encrypted)*.

3. Play a section 30 minutes in length and use appropriate image and audio FM detectors to extract the data payload of the Forensic Marking.

4. Verify that the Forensic Marking decoder indicates that a "positive identification" has been made.

5. Verify that the Forensic Marking decoder reports that the following data is contained within both image and each of the 16 audio channels:

    a. a 16-bit time stamp value.

    b. a location value whose number of bits matches that determined in Step (1).

6. 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:**
> An assessment of whether any allowed value for the time stamp and location data can be included in each 5 minute segments is impractical. For example, veryifying that all specified timestamp values are allowed would require testing to continue for a full calendar year. Instead a design review verifies that all specified timestamp and location values can be carried in the Forensic Marking.

Supporting Materials

Reference Documents	DCI-DCSS, 9.4.6.1.1
Test Equipment	**FM Decoder**
Test Materials	*2K FM Payload (Encrypted)* *KDM for 2K FM Payload (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated IMBO Confidence Sequence	Pass/Fail	—
24.2. SDR Projector Test Sequence	Pass/Fail	—
24.4. SDR Projector Confidence Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
26.4. HDR Direct View Display Confidence Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
27.4. SDR Direct View Display Confidence Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—
28.4. HDR Projector 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)* *KDM for Binary Audio Forensic Marking Test (Encrypted)* *KDM for Binary Selective Audio Forensic Marking Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 - 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)* *Selective Audio FM - All FM (Encrypted)* *Selective Audio FM - Not Above Channel 6 (Encrypted)* *Selective Audio FM - Not Above Channel 8 (Encrypted)* *Selective Audio FM - Not Above Channel 10 (Encrypted)* *Selective Audio FM - Not Above Channel 17 (Encrypted)* *DCI 2K StEM (Encrypted)* *KDM for Selective Audio FM - No FM (Encrypted)* *KDM for Selective Audio FM - All FM (Encrypted)* *KDM for Selective Audio FM - Not Above Channel 6 (Encrypted)* *KDM for Selective Audio FM - Not Above Channel 8 (Encrypted)* *KDM for Selective Audio FM - Not Above Channel 10 (Encrypted)* *KDM for Selective Audio FM - Not Above Channel 17 (Encrypted)* *KDM with two selective audio FM mark URIs*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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
Test Equipment	**FM Detector** **Accurate Real-Time Clock**
Test Materials	*2K FM Application Constraints (OBAE) (Encrypted)* *KDM for 2K FM Application Constraints (OBAE)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-1
Test Equipment	**FM Detector** **Accurate Real-Time Clock**
Test Materials	*2K FM Control Granularity - No FM (OBAE) (Encrypted)* *2K FM Control Granularity - Image Only FM (OBAE) (Encrypted)* *2K FM Control Granularity - OBAE Only FM (OBAE) (Encrypted)* *2K FM Control Granularity - Image and OBAE FM (OBAE) (Encrypted)* *KDM for 2K FM Control Granularity - No FM (OBAE)* *KDM for 2K FM Control Granularity - Image Only FM (OBAE)* *KDM for 2K FM Control Granularity - OBAE Only FM (OBAE)* *KDM for 2K FM Control Granularity - Image and OBAE FM (OBAE)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

6.4.8. FM Payload (OBAE)

Objective

- Verify that the Forensic Marking data payload for OBAE essence 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 the correct number of bits is allocated for the time stamp and location data.
- Verify that the entire Forensic Marking data payload is 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. Determine, from the manufacturer, if the location data allows 524,288 (19 bits) or 1,048,576 (20 bits) distinct values.
2. Setup a show using the composition *2K FM Payload (OBAE) (Encrypted)*, keyed with *KDM for 2K FM Payload (OBAE) (Encrypted)*.
3. Setup the Test Subject with the maximum number of rendered channels supported by the system.
4. 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 the Forensic Marking decoder reports that the following data is contained within each of the rendered audio channels:
        a. a 16-bit time stamp value.
        b. a location value whose number of bits matches that determined in Step (1).
    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:**
> An assessment of whether any allowed value for the time stamp and location data can be included in each 5 minute segments is impractical. For example, veryifying that all specified timestamp values are allowed would require testing to continue for a full calendar year. Instead a design review verifies that all specified timestamp and location values can be carried in the Forensic Marking.

Supporting Materials

Reference Documents	DCI-DCSS, 9.4.6.1.1
Test Equipment	**FM Decoder**
Test Materials	*2K FM Payload (OBAE) (Encrypted)* *KDM for 2K FM Payload (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
20.4. OMB Confidence Sequence	Pass/Fail	—
21.4. Integrated IMBO 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
Test Equipment	**Digital Audio Recorder**

	Sound Editor
Test Materials	*2K FM Payload (OBAE) (Encrypted)* *KDM for 2K FM Payload (OBAE) with FM Bypass (Encrypted)* *2K FM Payload (plaintext OBAE) (Encrypted)* *KDM for 2K FM Payload (plaintext OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

6.5. Image Reproduction

6.5.1. Playback of Image Only Material

Objective

Verify that the theatre system is 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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 Imaging Device 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 Imaging Device'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.

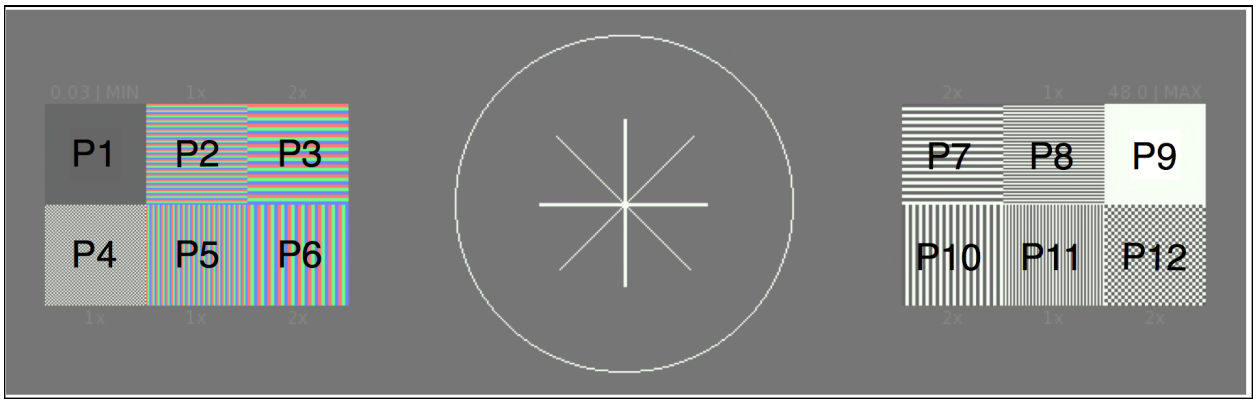

Figure 6.1. Standard Frame Panel Designations

Supporting Materials

Reference Documents	DCI-DCSS, 4.3.2, 2.1.1.4 SMPTE-428-1 SMPTE-430-2
Test Equipment	**48 fps Camera**
Test Materials	*DCI 2K Sync Test* *DCI 2K Sync Test (48fps)* *4K Sync Test* *DCI 2K Moving Gradient* *Color Accuracy Series* *2K DCI Maximum Bitrate Composition (Encrypted)* *4K DCI Maximum Bitrate Composition (Encrypted)* *KDM for 2K Maximum Bitrate Composition (Encrypted)* *KDM for 4K Maximum Bitrate Composition (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 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* *DCI NIST Frame with Pink Noise* *DCI NIST Frame with Pink Noise (96 kHz)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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)* *DCI NIST Frame with 1 kHz tone (-20 dB fs, 96kHz)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 screen of the Imaging Device, 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 imaging 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 Imaging Device, 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.

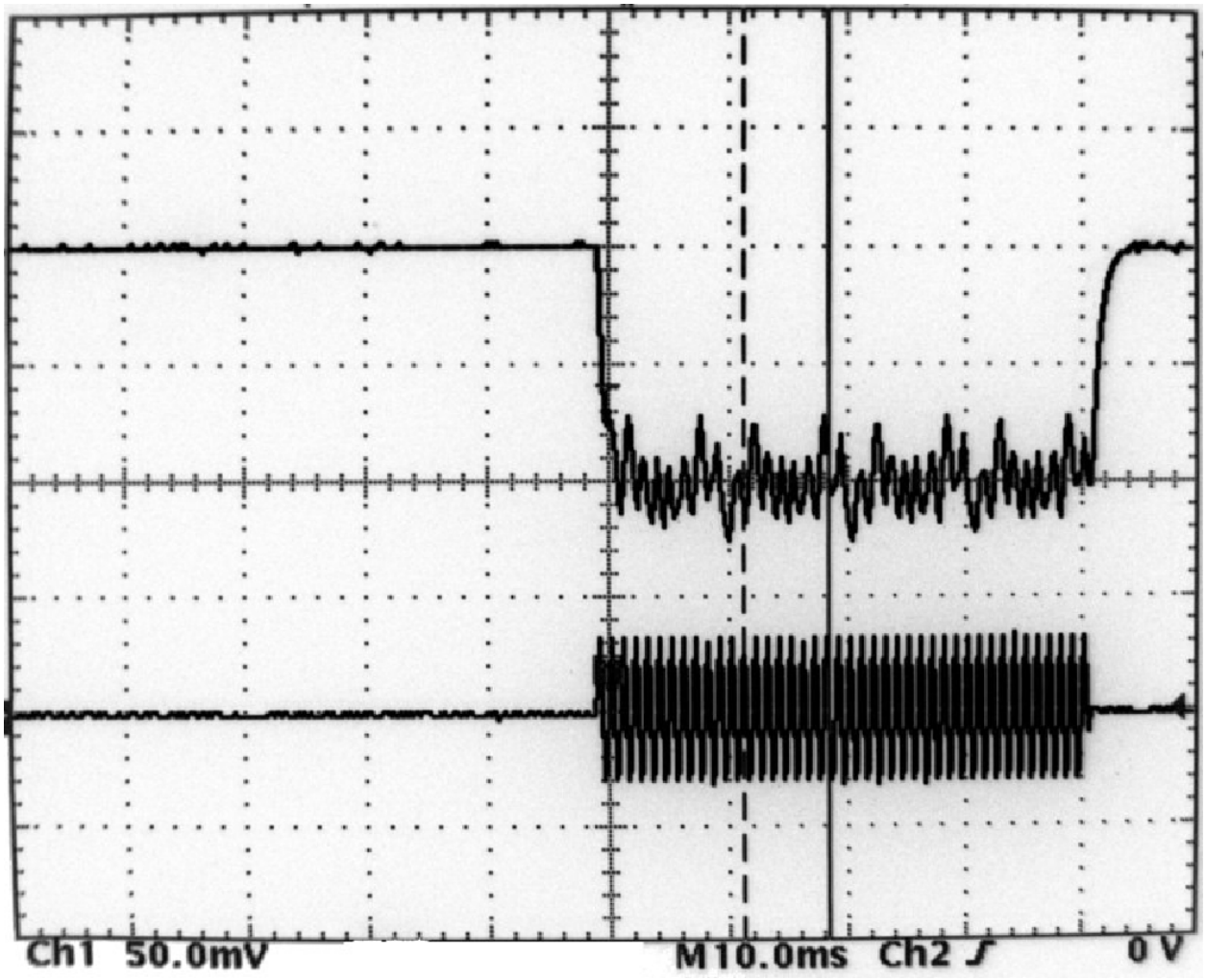

Figure 6.2. Audio Delay Timing

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** **Photodiode**
Test Materials	*DCI 2K Sync Test* *DCI 2K Sync Test (48fps)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

6.7. Timed Text Reproduction

6.7.1. Media Block Overlay

Objective

Verify that the Test Subject renders Timed Text essence correctly.

Procedures

1. Using an Imaging Device 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. Subtitle Test Evaluation and Pass/Fail Criteria 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 SMPTE-429-2
Test Materials	*2K Scope Subtitle Test (Encrypted)* *2K Flat Subtitle Test (Encrypted)* *2K Full Subtitle Test (Encrypted)* *4K Scope Subtitle Test (Encrypted)* *4K Flat Subtitle Test (Encrypted)* *4K Full Subtitle Test (Encrypted)* *2K 48fps Scope Subtitle Test (Encrypted)* *2K 48fps Flat Subtitle Test (Encrypted)* *2K 48fps Full Subtitle Test (Encrypted)* *KDM for 2K Scope Subtitle Test (Encrypted)* *KDM for 2K Flat Subtitle Test (Encrypted)* *KDM for 2K Full Subtitle Test (Encrypted)* *KDM for 4K Scope Subtitle Test (Encrypted)* *KDM for 4K Flat Subtitle Test (Encrypted)* *KDM for 4K Full Subtitle Test (Encrypted)* *KDM for 2K 48fps Scope Subtitle Test (Encrypted)* *KDM for 2K 48fps Flat Subtitle Test (Encrypted)* *KDM for 2K 48fps Full Subtitle Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

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

Only applies to a Test Subject 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).

Verify that the Test Subject 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 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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
24.2. SDR Projector 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 SMPTE-428-7 SMPTE-429-5
Test Materials	*DCI 2K Sync test with Subtitles (Encrypted)* *KDM for DCI 2K Sync Test with Subtitles (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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
Test Equipment	**OBAE Sound System**
Test Materials	*DCP for OBAE Tone Multi-Reel (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 screen of the Imaging Device, 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 imaging 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 Imaging Device, 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
Test Equipment	**Oscilloscope** **Photodiode**
Test Materials	*DCI 2K Sync Test (OBAE)* *DCI 2K Sync Test (48fps) (OBAE)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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	DCI-DCSS, 3.3.4.3, 5.3.4.5 [SMPTE-429-18]
Test Equipment	**OBAE Sound System**
Test Materials	*Maximum Bitrate OBAE (Encrypted)* *KDM for Maximum Bitrate OBAE (Encrypted)* *Maximum Bitrate OBAE 48 fps (Encrypted)* *KDM for Maximum Bitrate OBAE 48 fps (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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	DCI-DCSS, 7.5.6.1 [SMPTE-2098-3]
Test Equipment	**OBAE Sound System**
Test Materials	*OBAE Rendering Expectations*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

Chapter 7. Imaging Device

7.1. Test Environment for Image Measurements

7.1.1 General

When making image measurements on any Imaging Device:

- All required setup and calibration procedures, as recommended by the manufacturer, shall be carried out or verified prior to all measurements.
- Stray light on the screen shall be minimized. The room lights in test environment shall be turned off, with the exception of the minimal lighting provided for working or safety reasons. The use of black nonreflective surfaces with recessed lighting is encouraged.

  Note that, outside of the Test Environment, e.g. in exhibition theaters or review rooms, safety regulations and the placement of exit lights or access lights can result in a higher ambient light level.
- Unless otherwise specified or required:
  - the distance between the front of the **Spectroradiometer** lens and the screen shall be equal to 1.6 times the height of the screen; and
  - the position of the **Spectroradiometer** shall be equidistant from the left and right edges of the screen.
  - the position of the **Spectroradiometer** shall be equidistant from the top and bottom edges of the screen.

In all cases the location of the **Spectroradiometer** shall be appropriate for the **Spectroradiometer** that is used and for the test being conducted.

7.1.2 Projector

With the Projector turned off or the douser closed, the level of ambient light reflected by the screen shall be:

- less than 0.01 cd/m² for an SDR Projector; and
- less than 0.0005 cd/m² for an HDR Projector.

The screen shall 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).

When making image measurements on a Projector:

- The Projector shall be turned on (including the lamp) and allowed to thermally stabilize for 20 to 30 minutes prior to all measurements.
- Unless specified otherwise, the douser shall be open from beginning to end of each test procedure.

7.5.13. Projector Test Environment records information about the test environment in which projector test procedures were conducted.

7.1.3 Direct View Display

With the Direct View Display turned off, the level of ambient light reflected by the screen shall be less than 0.0005 cd/m².

The Direct View Display shall be turned on and allowed to thermally stabilize for 20 to 30 minutes prior to all measurements.

7.5.30. Direct View Display Test Environment records information about the test environment in which the test procedures were conducted.

7.1.4 Stereoscopic Measurements

When performing stereoscopic measurements:

- The Imaging Device shall be enabled for stereoscopic presentations.
- The stereoscopic glasses shall be enabled, if they are active glasses.

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 (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). 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 Direct View 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 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	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector 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 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 Imaging Device's 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	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
24.4. SDR Projector Confidence Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
26.4. HDR Direct View Display Confidence Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
27.4. SDR Direct View Display Confidence Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—
28.4. HDR Projector 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	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.2.7. Systems without Electronic Marriage

Objective

Verify that in the configuration of a permanently married companion SPB (MB), the companion SPB is not field replaceable and requires the Imaging Device SPB and companion SPB system to both be replaced in the event of an SPB failure.

Procedures

Verify that the companion SPB Type 1 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	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.2.8. Electronic Marriage Break Key Retaining

Objective

Verify that breaking the marriage between the Imaging Device and its companion SPB (MB) does not zeroize the Imaging Device 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 MBs.)

1. Using procedures and tools provided by the manufacturer of the Imaging Device, 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 Imaging Device 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	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector 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) that implement electronic marriage functions.

- Verify that as part of the installation, or reinstallation, (*i.e.*, mechanical connection to the Imaging Device and electrical initiation) an electrical and logical marriage of the companion SPB (MB) with the Imaging Device 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 (Encrypted)*.

2. Power down the system, locate the field-replaceable companion SPB (MB), 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 Imaging Device 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 Imaging Device 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 SMPTE-430-5
Test Materials	*DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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 Imaging Device SPB (type 2) does not zeroize the MB'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 MBs.

In the case of an MB that is married to an Imaging Device 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 Imaging Device 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 Imaging Device 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 Imaging Device 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.

Supporting Materials

Reference Documents	DCI-DCSS, 9.4.3.6.2, 9.4.3.6.3, 9.5.1.2
Test Materials	*DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

7.3.4. Deleted Section

The section "Remote SPB Clock Adjustment" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

7.4. Link Decryptor Block

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. Deleted Section

The section "LDB TLS Session Constraints" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

7.4.3. Deleted Section

The section "LDB Time-Awareness" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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. Deleted Section

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

7.4.6. Deleted Section

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

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. Image Reproduction

7.5.1. Deleted Section

The section "Projector Overlay" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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. Imaging Device Pixel Count/Structure

Objective

Verify that the sampling structure of the displayed picture array (pixel count of the imaging device) 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 and Direct View Displays: 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 screen. 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.

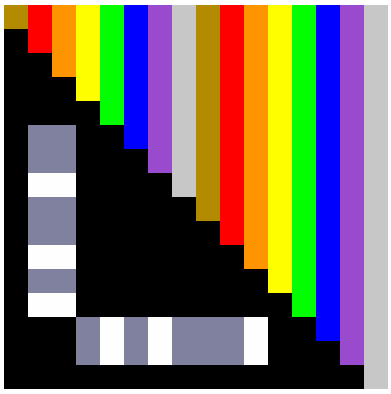

Figure 7.1. Pixel Structure 16 x 16 Array

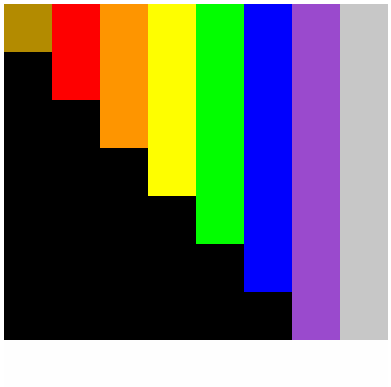

Figure 7.2. Pixel Structure 8 x 8 Array

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 [DV-ADD]
Test Materials	*Pixel Structure Pattern N 2k* *Pixel Structure Pattern S 2k* *Pixel Structure Pattern E 2k* *Pixel Structure Pattern W 2k* *Pixel Structure Pattern N 4k*

Pixel Structure Pattern S 4k
Pixel Structure Pattern E 4k
Pixel Structure Pattern W 4k

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
24.4. SDR Projector Confidence Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
26.4. HDR Direct View Display Confidence Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
27.4. SDR Direct View Display Confidence Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—
28.4. HDR Projector Confidence Sequence	Pass/Fail	—

7.5.4. Deleted Section

The section "Projector Spatial Resolution and Frame Rate Conversion" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

7.5.5. Deleted Section

The section "White Point Luminance and Uniformity" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

7.5.6. Deleted Section

The section "White Point Chromaticity and Uniformity" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

7.5.7. Deleted Section

The section "Sequential Contrast" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

7.5.8. SDR Intra-frame Contrast

Objective

Verify that the Imaging Device maintains white and black luminance when a non-uniform picture is presented.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Display the checkerboard test pattern *Intra-Frame Contrast Sequence*.

3. Measure L_{WL}, L_{WR}, L_{KL} and L_{KR} according to:

- the *checkerboard luminance & contrast (n×m)* procedure at [ICDM IDMS], if the Test Subject is a Direct View Display; or

- the *checkerboard contrast ratio* procedure at [ICDM IDMS], if the Test Subject is a Projector; or

4. Verify that:

   - if the Test Subject is a Direct View Display, L_{WL} and L_{WR} are each equal to 48.0 ± 3.5 cd/m², and L_{KL} and L_{KR} are each within the range [0.01, 0.024] cd/m²; or

   - if the Test Subject is a Projector, L_{WL} and L_{WR} are each equal to 48.0 ± 3.5 cd/m², and L_{KL} and L_{KR} each do not exceed 0.52 cd/m².

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	DCI-DCSS, 8.3.4.8 SMPTE-431-2
Test Equipment	**Spectroradiometer**
Test Materials	*Intra-Frame Contrast Sequence*

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector 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 test environment requirements detailed in Section 7.1 have been performed.

1. Power-down the Test Subject. Alternatively, the douser can be closed if the Test Subject is a Projector.

2. Use a **Spectroradiometer** to measure and record the Luminance of the ambient light reflected from the screen.

3. Power-up the Test Subject. Alternatively, the douser can be open if the Test Subject is a Projector.

4. Display no image or display black code values, and, using a **Spectroradiometer**, measure and record the Luminance of the light reflected from the screen.

5. Play back the DCP *DCI White Steps* (black-to-white gray step-scale test pattern).

6. 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**.

7. 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.

8. Play back the DCP *DCI Gray Steps* (black-to-dark gray step-scale test pattern).

9. 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**.

10. 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 SMPTE-431-2
Test Equipment	**Spectroradiometer**
Test Materials	*DCI White Steps* *DCI Gray Steps*

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Data only	—
26.2. HDR Direct View Display Test Sequence	Data only	—
27.2. SDR Direct View Display Test Sequence	Data only	—
28.2. HDR Projector Test Sequence	Data only	—

7.5.10. SDR Contouring

Objective

Confirm the Imaging Device exhibits no visible contouring when presenting an SDR composition.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Play back *SDR Dark Gray Scale* and measure, using a a **Spectroradiometer**, the luminance L_i at the center of the screen of each full-screen gray patch.

3. Calculate the set of second approximate derivatives from the set of measurements $\{L_i\}$ according to the *slope monotonicity of gray scale* procedure at [ICDM IDMS].

4. Verify that all the second approximate derivatives are greater than 0.

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	DCI-DCSS, 8.3.3 [SMPTE-431-2]
Test Materials	*SDR Dark Gray Scale*

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.11. SDR Transfer Function

Objective

Verify that the correct SDR transfer function is used by the imaging device.

Procedures

Note: Prior to taking measurements, ensure that the setup and test environment requirements detailed in Section 7.1 have been performed.

1. Display *2K Full SDR Black* and, using a **Spectroradiometer**, measure the output luminance to a precision of 1 mcd/m², and record the result as the *screen black level*.

2. Play back the DCP *DCI White Steps*.

3. For each of the ten steps of the pattern listed in Table A-2 of [SMPTE-431-2], measure the output luminance with a **Spectroradiometer**, subtract the *screen black level* obtained in step (1), and verify that the result is

within the tolerance specified in Table 7.5.

4. Play back the DCP *DCI Gray Steps*.

5. For each of the ten steps of the pattern listed in Table A-3 of [SMPTE-431-2], measure the output luminance with a **Spectroradiometer**, subtract the *screen black level* obtained in step (1), and verify that the result is within the tolerance specified in Table 7.5.

Any verification that fails is cause to fail this test.

Table 7.5.11(a) Black-to-white gray step-scale test pattern nominal luminance values

Step Number	Nominal Luminance above the Screen Black Level (cd/m²)	Tolerance
1	0.121	±5%
2	0.731	±5%
3	2.098	±3%
4	4.432	±3%
5	7.917	±3%
6	12.718	±3%
7	18.988	±3%
8	26.870	±3%
9	36.497	±3%
10	47.999	±3%

Table 7.5.11(b) Black-to-dark gray step-scale test pattern nominal luminance values

Step Number	Nominal Luminance above the Screen Black Level (cd/m²)	Tolerance
1	0.006	±20%
2	0.038	±5%
3	0.111	±5%
4	0.234	±5%
5	0.418	±5%
6	0.670	±5%
7	1.002	±3%
8	1.418	±3%
9	1.928	±3%
10	2.531	±3%

Supporting Materials

Reference Documents	DCI-DCSS, 9.3.4.11 SMPTE-431-2 [DV-ADD]
Test Equipment	**Spectroradiometer**

Test Materials	*DCI White Steps* *DCI Gray Steps* *2K Full SDR Black*

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.12. SDR Color Accuracy

Objective

Verify that all colors are accurately reproduced within the tolerances as specified in [SMPTE-431-2].

Procedures

1. Setup the Imaging Device and test environment according to 7.1. Test Environment for Image Measurements.
2. Using *Color Accuracy Series*, measure and record the luminance and chromaticity coordinates for the following patches, according to the *full-screen arbitrary color (R, G, B)* procedure at [ICDM IDMS]:
    - *Red-1*
    - *Green-1*
    - *Blue-1*
3. Verify that the measured chromaticity coordinates for each of the patches are equal to the *Red*, *Green* and *Blue* reference values for *Color Accuracy* that are specified at [SMPTE-431-2], Table A.1, within review room tolerances.
4. Verify that the measured luminance for each of the patches is ±3% of the *Output Luminance* values specified at [SMPTE-431-2], Table A.4.

Any measurement outside of specified tolerances is caused to fail this test.

Supporting Materials

Reference Documents	DCI-DCSS, 8.3.3 SMPTE-431-2
Test Equipment	**Spectroradiometer**
Test Materials	*Color Accuracy Series*

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector 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 **Spectroradiometer** lens and the center of the screen.
5. Record the approximate vertical angle of incidence of the front of the **Spectroradiometer** lens to the center of the screen.
6. Record the approximate horizontal angle of incidence of the front of the **Spectroradiometer** 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	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	All data recorded per the test procedure
28.2. HDR Projector Test Sequence	Pass/Fail	All data recorded per the test procedure

7.5.14. HDR White Luminance and Chromaticity

Objective

Verify that the luminance and chromaticity of HDR white are within tolerances:

- at the center of the Imaging Device; and
- at the edges of the Imaging Device.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.
2. Display the white frame of *HDR Sequential Contrast and Uniformity Sequence*.
3. Measure the luminance and chromaticity coordinates according to the *full-screen arbitrary color (R, G, B)* procedure at [ICDM IDMS].
4. Verify that the measured luminance and chromaticity coordinates are within the *center luminance* and *center chromaticity* tolerances, respectively, specified for specified at Table 7.5 for the Test Subject. Any measurement outside of the specified tolerances is caused to fail this test.
5. Measure the luminance nonuniformity $\mathcal{N}$ and maximum chromaticity difference $\Delta u'v'$ according to the *sampled vantage-point uniformity* procedure at [ICDM IDMS].
6. Verify that $\mathcal{N}$ and $\Delta u'v'$ do not exceed their respective maximum values specified at Table 7.5 for the Test Subject.

Any verification that fails is cause to fail this test.

Table 7.5.14(a) HDR White (Peak)

Parameter	Test Subject	
	Projector	Direct View Display
Center luminance (cd/m²)	299.6 ± 18	299.6 ± 9
Center chrominance (x, y)	(0.3127 ± 0.002, 0.3290 ± 0.002)	

Table 7.5.14(b) HDR White (Angular Nonuniformity)

Parameter	Test Subject	
	Projector	Direct View Display
Maximum $\mathcal{N}$	15%	6%
Maximum $\Delta u'v'$	0.0182	

Supporting Materials

Reference Documents	[ICDM IDMS] [DCI-HDR] [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*HDR Sequential Contrast and Uniformity Sequence*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.15. SDR White Luminance and Chromaticity

Objective

Verify that the luminance and chromaticity of SDR white are within tolerances:

- at the center of the Imaging Device; and
- at the edges of the Imaging Device.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed. For the remainder of this test procedure, the **Spectroradiometer** shall be positioned as specified at 7.1.1 General, disregarding positioning recommendations made at [ICDM IDMS].
2. Display the white frame of *Sequential Contrast and Uniformity Sequence*.
3. Measure the luminance and chromaticity coordinates according to the *full-screen arbitrary color (R, G, B)* procedure at [ICDM IDMS].
4. Verify that the measured luminance and chromaticity coordinates are within the *center luminance* and *center chromaticity* tolerances, respectively, specified for specified at Table 7.5 for the Test Subject. Any measurement outside of the specified tolerances is caused to fail this test.
5. Measure the luminance nonuniformity $\mathcal{N}$ and maximum chromaticity difference $\Delta u'v'$ according to the *sampled vantage-point uniformity* procedure at [ICDM IDMS].
6. Verify that $\mathcal{N}$ and $\Delta u'v'$ do not exceed their respective maximum values specified at Table 7.5 for the Test Subject.

Any verification that fails is cause to fail this test.

Table 7.5.15(a) SDR White (Peak)

Parameter	Test Subject	
	Projector	Direct View Display
Center luminance (cd/m²)	48.0 ± 3.5	
Center chrominance (*x*, *y*)	(0.314 ± 0.002, 0.351 ± 0.002)	

Table 7.5.15(b) SDR White (Angular Nonuniformity)

Parameter	Test Subject	
	Projector	Direct View Display
Maximum ΔN	20%	6%
Maximum $\Delta u'v'$	0.0171	

Supporting Materials

Reference Documents	[ICDM IDMS] [DV-ADD] DCI-DCSS, 8.3.4.3, 8.3.4.4 SMPTE-431-1
Test Equipment	**Spectroradiometer**
Test Materials	*Sequential Contrast and Uniformity Sequence*

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.16. HDR Color Luminance and Chromaticity

Objective

Confirm that HDR color reproduction, as measured at the center of the Imaging Device, is within tolerances.

Procedures

1. Setup the Imaging Device and test environment according to 7.1. Test Environment for Image Measurements.

2. Using *HDR Color Accuracy Series*, measure and record the luminance and chromaticity coordinates for the following Patch Code Values, according to the *full-screen arbitrary color (R, G, B)* procedure at [ICDM IDMS]:

    - *Red-1*

- *Green-1*
- *Blue-1*

3. Verify that the measured chromaticity coordinates for *Red-1*, *Green-1* and *Blue-1* are equal to the reference values for *Color Accuracy* that are specified at [DCI-HDR], within the review room tolerances corresponding to the Test Subject.

4. Verify that the measured luminance for *Red-1*, *Green-1* and *Blue-1* are within the tolerances specified at Table 7.5.

Any measurement outside of specified tolerances is caused to fail this test.

Table 7.5.16 Target HDR color luminances and chromaticities

Patch	Nominal values (cd/m²)	Tolerances	
		Projector	Direct View Display
Red-1	68.13	±6%	±3%
Green-1	207.35		
Blue-1	23.86		

Supporting Materials

Reference Documents	[ICDM IDMS] [DCI-HDR] [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*HDR Color Accuracy Series*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.17. HDR Minimum Active Black Level

Objective

Confirm that the minimum active black level as measured in the center of the Imaging Device is within tolerances.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Display the black frame of *HDR Sequential Contrast and Uniformity Sequence*.

3. Measure the luminance according to the *full-screen black* procedure at [ICDM IDMS].

4. Verify that each measured luminance is equal to the nominal value for *Minimum Active Black Level* specified at [DCI-HDR], within the review room tolerances corresponding to the Test Subject. Any measurement outside of the specified tolerances is caused to fail this test.

Supporting Materials

Reference Documents	[ICDM IDMS] [DCI-HDR] [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*HDR Sequential Contrast and Uniformity Sequence*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.18. SDR Inactive Black Level (Direct View Display)

Objective

1. Verify that pixels outside the decoded image area are not emitting any light.

2. Verify that pixels outside the area specified by the MainPictureActiveArea item of the CPL metadata are not emitting any light.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. For each of the following test materials, display the material and verify by visual inspection that: (a) registration marks are visible and (b) pixels outside the rectangular area delineated by the registration marks are not emitting any light:

    - *2K Full SDR Black with Marks*
    - *2K Scope SDR Black with Marks*
    - *2K Flat SDR Black with Marks*

- *4K Full SDR Black with Marks*
- *4K Scope SDR Black with Marks*
- *4K Flat SDR Black with Marks*

Any verification that fails is cause to fail this test.

3. For each of the following test materials, display the material and verify by visual inspection that: (a) registration marks are visible and (b) no red pixels are visible:
   - *2K Full SDR Black with Active Area*
   - *2K Scope SDR Black with Active Area*
   - *2K Flat SDR Black with Active Area*
   - *4K Full SDR Black with Active Area*
   - *4K Scope SDR Black with Active Area*
   - *4K Flat SDR Black with Active Area*

   Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	[DV-ADD]
Test Materials	*2K Full SDR Black with Marks* *2K Scope SDR Black with Marks* *2K Flat SDR Black with Marks* *4K Full SDR Black with Marks* *4K Scope SDR Black with Marks* *4K Flat SDR Black with Marks* *2K Full SDR Black with Active Area* *2K Scope SDR Black with Active Area* *2K Flat SDR Black with Active Area* *4K Full SDR Black with Active Area* *4K Scope SDR Black with Active Area* *4K Flat SDR Black with Active Area*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.19. Horizontal and Vertical Full Screen Off-Axis Uniformity (Direct View Display)

Objective

Verify the full screen off-axis uniformity performance of the Imaging Device.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Display the white frame from *Sequential Contrast and Uniformity Sequence* and, for each of the angular positions specified in Table 7.1:

    - measure the *luminance change ratio* according to the *viewing-angle luminance change ratio* procedure at [ICDM IDMS].

    - measure the *viewing-angle color variation* according to the *viewing-angle color variation* procedure at [ICDM IDMS].

3. Verify that each of the measured *luminance change ratio* and *viewing-angle color variation* satisfy the tolerance specified at Table 7.1.

Any verification that fails is cause to fail this test.

Table 7.1. Measurement positions and tolerances for horizontal and vertical full screen off-axis performance measurements

Angular positions	***Luminance change ratio* tolerance**	***Viewing-angle color variation* tolerance**
+10° vertically (up)	Full Screen Vertical Off-Axis Luminance Uniformity at [DV-ADD]	Full Screen Vertical Off-Axis White Chromaticity Uniformity at [DV-ADD]
-35° vertically (down)		
-60° horizontally (left)	Full Screen Horizontal Off-Axis Luminance Uniformity at [DV-ADD]	Full Screen Horizontal Off-Axis White Chromaticity Uniformity at [DV-ADD]
+60° horizontally (right)		

Supporting Materials

Reference Documents	[ICDM IDMS]

	[DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*Sequential Contrast and Uniformity Sequence*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.20. Stereoscopic Extinction Ratio

Objective

Confirm that, when reproducing stereoscopic presentations, the Imaging Device achieves the required minimum extinction ratio.

Procedures

This test procedure only applies to a Test Subject that supports stereoscopic presentations.

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Using *Stereoscopic SDR Contrast Test Patterns*, measure the extinction ratios $\chi_{sys\mathcal{L}}$ and $\chi_{sys\mathcal{R}}$ according to the *stereoscopic extinction ratio & crosstalk* procedure at [ICDM IDMS].

3. Verify that $\chi_{sys\mathcal{L}}$ and $\chi_{sys\mathcal{R}}$ each equals or exceeds the *Tolerance* for the *Stereoscopic Extinction Ratio* specified at [DV-ADD].

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	[ICDM IDMS] [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*Stereoscopic SDR Contrast Test Patterns*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.21. SDR Stereoscopic Peak White Luminance

Objective

Confirm that, when reproducing stereoscopic presentations, the Imaging Device achieves the required SDR peak white luminance.

Procedures

This test procedure only applies to a Test Subject that supports SDR stereoscopic presentations.

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Using *Stereoscopic SDR Contrast Test Patterns*, measure the average stereo luminance L_{ave} according to the *stereoscopic luminance & luminance difference* procedure at [ICDM IDMS].

3. Verify that L_{ave} is within the tolerances for the *Stereoscopic Peak White Luminance* specified at [DV-ADD].

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	[ICDM IDMS] [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*Stereoscopic SDR Contrast Test Patterns*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.22. Surface Reflectivity (Direct View Display)

Objective

- Verify that the diffuse surface reflectivity of the imaging device is within limits

- Verify that the specular surface reflectivity of the imaging device is within limits

Procedures

Note:
If the measurement device or procedure reports the diffuse reflectivity at different optical wavelengths, the

weighted average using the CIE Y Color Matching Function shall be used to combine different values at different wavelengths into a single diffuse reflectivity value that is photometrically weighted.

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. With the Imaging Device turned off, measure the *reflectance with specular excluded*, $\rho_{\theta/de}$, according to the *sampling-sphere implementation (specular excluded)* procedure at [ICDM IDMS].

3. Verify that $\rho_{\theta/de}$ is less than or equal to the *Diffuse Reflectivity* specified at [DV-ADD].

4. With the Imaging Device turned off, measure the *reflectance*, $\rho_{8/di}$, according to the *sampling-sphere implementation* procedure at [ICDM IDMS].

5. Verify that $\rho_{8/di}$ - $\rho_{\theta/de}$ is less than or equal to the *Spectral Reflectivity* specified at [DV-ADD].

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	[ICDM IDMS] [DV-ADD]
Test Equipment	**Spectroradiometer**

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.23. Vignetting (Direct View Display)

Objective

Verify that the imaging device does not exhbit vignetting.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Using the full-frame white target from *Sequential Contrast and Uniformity Sequence*, measure the nonuniformity $\mathcal{N}$ according to the *sampled uniformity* procedure at [ICDM IDMS].

3. Verify that $\mathcal{N}$ meets the tolerance for the *Full-Screen Sampled Nonuniformity* specified at [DV-ADD].

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	[ICDM IDMS] [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*Sequential Contrast and Uniformity Sequence*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.24. SDR Stereoscopic Minimum Active Black Level

Objective

Confirm that the stereoscopic display system achieves the required SDR minimum active black level.

Procedures

This test procedure only applies to a Test Subject that supports SDR stereoscopic presentations.

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Using *Stereoscopic SDR Contrast Test Patterns*, measure the left eye black level, $L_{\mathcal{L}KK}$, and the right eye black level, $R_{\mathcal{L}KK}$, according to the *stereoscopic contrast ratio* procedure at [ICDM IDMS].

3. Verify that both $L_{\mathcal{L}KK}$ and $R_{\mathcal{L}KK}$ are within the limits for the *Stereoscopic Minimum Active Black Level* specified at [DV-ADD].

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	[ICDM IDMS] [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*Stereoscopic SDR Contrast Test Patterns*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.25. Image Upscaling Artifacts

Objective

Confirm that the imaging system does not exhibit upscaling artifacts.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Display *4K Scaling Test Patterns*.

3. Verify that, when viewed from a distance of one screen height from the imaging device, the displayed image appear as illustrated at Figure A.2.254 and is free of artifacts, including spatial discontinuity artifacts (jaggies), ringing artifacts and aliasing artifacts, as illustrated in Figure 7.25(a), Figure 7.25(b) and Figure 7.25(c).

Any verification that fails is cause to fail this test.

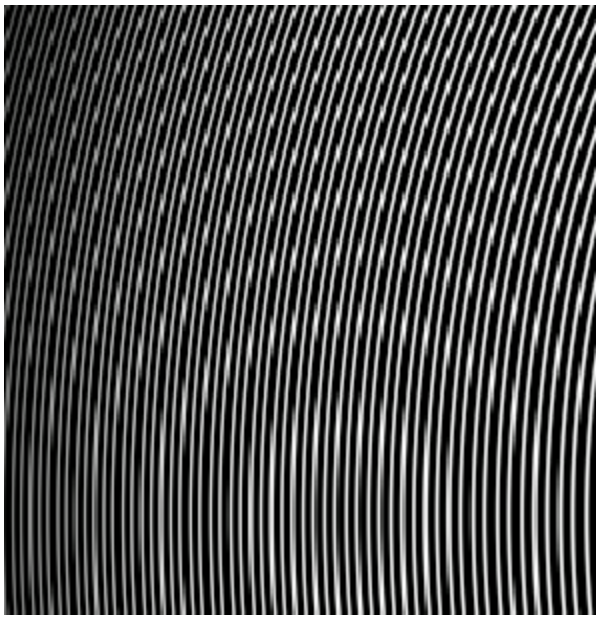

Figure 7.25(a). Sample aliasing artifacts

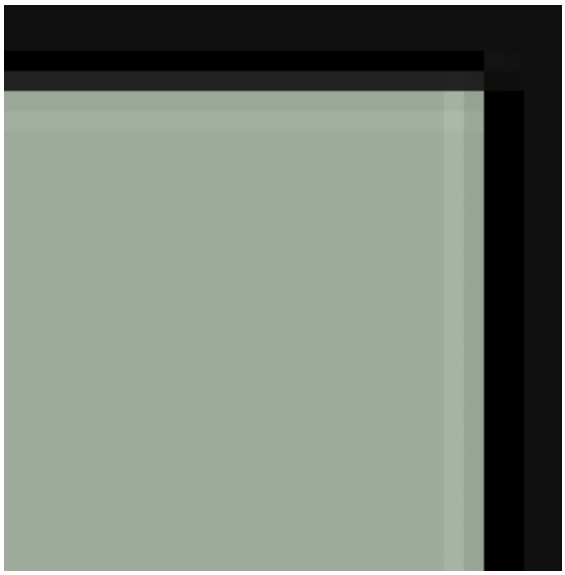

Figure 7.25(b). Sample ringing artifacts

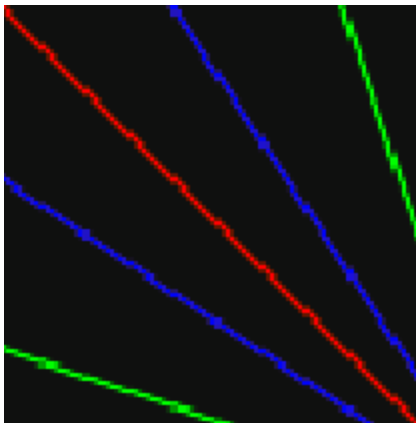

Figure 7.25(c). Sample spatial discontinuities (jaggies)

Supporting Materials

Reference Documents	[ICDM IDMS] [DV-ADD]
Test Materials	*4K Scaling Test Patterns*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.26. SDR Stereoscopic Color Accuracy

Objective

Verify that, when reproducing a stereoscopic presentation, the Imaging Device reproduces colors within the tolerances specified in [SMPTE-431-2].

Procedures

1. Setup the Imaging Device and test environment according to 7.1. Test Environment for Image Measurements.

2. Using *Steroscopic Color Accuracy Series*, measure and record the luminance and chromaticity coordinates for the following patches, according to the *full-screen arbitrary color (R, G, B)* procedure at [ICDM IDMS]:

    - *Red-1*
    - *Green-1*
    - *Blue-1*

3. Verify that the measured chromaticity coordinates for each of the patches are equal to the *Red*, *Green* and *Blue* reference values for *Color Accuracy* that are specified at [SMPTE-431-2], Table A.1, within review room tolerances.

4. Verify that the measured luminance for each of the patches is ±3% of the *Output Luminance* values specified at [SMPTE-431-2], Table A.4.

Any measurement outside of specified tolerances is caused to fail this test.

Supporting Materials

Reference Documents	DCI-DCSS, 8.3.3 SMPTE-431-2 [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*Steroscopic Color Accuracy Series*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.27. Sub-pixel Spatial Coincidence (Direct View Display)

Objective

Verify that the spatial arrangement of the color primary elements do not introduce objectionable geometric anomalies such as fringing artifacts.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Using *4K White Lines*, verify that no color fringing artifacts are visible. Figure 7.5 illustrates one example of fringing artifacts where a nominally vertical white line appears, as seen from the normal seating area, as disjointed line segments of varying colors.

Any verification that fails is cause to fail this test.

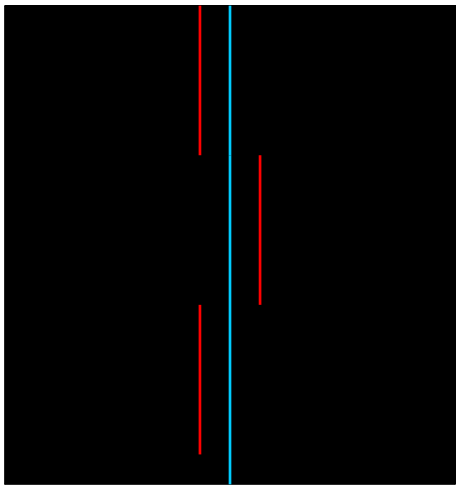

Figure 7.5.27 Illustration of a fringing artifact (not to scale)

Supporting Materials

Reference Documents	[DV-ADD]
Test Materials	*4K White Lines*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.28. HDR Transfer Function

Objective

Verify that the correct HDR transfer function is used by the Imaging Device.

Procedures

Note: Prior to taking measurements, ensure that the setup and test environment requirements detailed in Section 7.1 have been performed.

1. Play back the DCP *DCI HDR White Steps*.

2. For each of the ten steps of Table 3 at [DCI-HDR], measure the output luminance with a **Spectroradiometer** and verify that the result is within the tolerance specified in Table 7.5.

3. Play back the DCP *DCI HDR Gray Steps*.

4. For each of the ten steps of Table 4 at [DCI-HDR], measure the output luminance with a **Spectroradiometer** and verify that the result is within the tolerance specified in Table 7.5.

Any verification that fails is cause to fail this test.

Table 7.5.28(a) HDR black-to-white gray step-scale test pattern nominal luminance values

Step Number	Nominal Luminance (cd/m²)	Tolerance	
		Projector	Direct View Display
1	0.50	±5%	±12%
2	1.00	±5%	±12%
3	2.00	±3%	±6%
4	5.00	±3%	±6%
5	9.99	±3%	±6%
6	20.00	±3%	±6%
7	50.01	±3%	±6%
8	100.10	±3%	±6%
9	200.21	±3%	±6%
10	299.64	±3%	±6%

Table 7.5.28(b) HDR black-to-dark gray step-scale test pattern nominal luminance values

Step Number	Nominal Luminance (cd/m²)	Tolerance	
		Projector	Direct View Display
1	0.0050	±20%	±20%
2	0.0075	±20%	±20%
3	0.0100	±20%	±20%
4	0.0151	±20%	±20%
5	0.0202	±5%	±12%
6	0.0352	±5%	±12%
7	0.0501	±5%	±12%
8	0.0752	±5%	±12%
9	0.0998	±5%	±12%
10	0.1997	±5%	±12%

Supporting Materials

Reference Documents	[DCI-HDR] [DV-ADD]
Test Equipment	**Spectroradiometer**
Test Materials	*DCI HDR Gray Steps* *DCI HDR White Steps* *HDR Sequential Contrast and Uniformity Sequence*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.29. SDR Minimum Active Black Level

Objective

Verify that the Imaging Device achieves the required minimum luminance when presented with an SDR full black signal.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. For each of the following test materials, display the material and measure the luminance according to the *full-screen black* procedure at [ICDM IDMS]:

    - *2K Full SDR Black*
    - *2K Scope SDR Black*
    - *2K Flat SDR Black*
    - *4K Full SDR Black*
    - *4K Scope SDR Black*
    - *4K Flat SDR Black*

3. Verify that the measured luminance is within the range:

    - [0.01, 0.024] cd/m², if the Test Subject is a Direct View Display; or

- [0.01, 0.032] cd/m², if the Test Subject is a Projector.

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	[ICDM IDMS] SMPTE-431-2
Test Equipment	**Spectroradiometer**
Test Materials	*2K Full SDR Black* *2K Scope SDR Black* *2K Flat SDR Black* *4K Full SDR Black* *4K Scope SDR Black* *4K Flat SDR Black*

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.30. Direct View Display Test Environment

Objective

Record information about the test environment in which the reported Direct View Display measurements were made.

Procedures

1. Setup the test environment as specified in 7.1. Test Environment for Image Measurements.

2. Record the height and width of the Direct View Display in units of meters.

3. Record the number of modules that comprise the Direct View Display, in both the horizontal and vertical directions.

4. With the Direct View Display switched off, record, in units of cd/m², the luminance at the center of the Direct View Display.

Failure to record any data is cause to fail this test.

Supporting Materials

Test Equipment	**Spectroradiometer**

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	All data recorded per the test procedure
27.2. SDR Direct View Display Test Sequence	Pass/Fail	All data recorded per the test procedure

7.5.31. Automatic SDR/HDR mode switching

Objective

Verify that the projection system automatically switches between SDR and HDR presentation.

Procedures

1. Setup the test environment as specified in 7.1. Test Environment for Image Measurements.
2. Build a show playlist out of the following compositions, in the order listed and without any automation or configuration related to HDR and SDR presentation:
    a. *SDR Detection*
    b. *HDR Detection*
    c. *SDR Detection*
3. Play back the show, and measure and record the luminance for each of the *SDR dark*, *SDR light*, *HDR dark* and *HDR light* patches according to the *full-screen arbitrary color (R, G, B)* procedure at [ICDM IDMS].
4. Build a show playlist out of the following compositions, in the order listed and without any automation or configuration related to HDR and SDR presentation:
    a. *HDR Detection*
    b. *SDR Detection*
    c. *HDR Detection*
5. Play back the show, and measure and record the luminance for each of the *SDR dark*, *SDR light*, *HDR dark* and *HDR light* patches according to the *full-screen arbitrary color (R, G, B)* procedure at [ICDM IDMS].
6. Verify that, in all cases, the measured luminance for the patches are within the allowable luminance ranges specified at Table 7.5.

Any verification that fails is cause to fail this test.

Table 7.5.31 Target SDR and HDR luminances

Patch	Allowable luminance range (cd/m²)	
	Projector	Direct View Display
SDR dark	[0.01, 0.032]	[0.01, 0.024]
SDR light	15.20 ± 0.46	
HDR dark	0.005 ± 0.001	
HDR light	299.6 ± 18	299.6 ± 9

Supporting Materials

Reference Documents	[DCI-HDR]
Test Materials	*SDR Detection* *HDR Detection*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.32. HDR Inactive Black Level (Direct View Display)

Objective

1. Verify that pixels outside the decoded image area are not emitting any light.

2. Verify that pixels outside the area specified by the MainPictureActiveArea item of the CPL metadata are not emitting any light.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. For each of the following test materials, display the material and verify by visual inspection that: (a) registration marks are visible and (b) pixels outside the rectangular area delineated by the registration marks are not emitting any light:

    - *2K Full HDR Black with Marks*
    - *2K Scope HDR Black with Marks*
    - *2K Flat HDR Black with Marks*

- *4K Full HDR Black with Marks*
- *4K Scope HDR Black with Marks*
- *4K Flat HDR Black with Marks*

Any verification that fails is cause to fail this test.

3. For each of the following test materials, display the material and verify by visual inspection that: (a) registration marks are visible and (b) no red pixels are visible:
   - *2K Full HDR Black with Active Area*
   - *2K Scope HDR Black with Active Area*
   - *2K Flat HDR Black with Active Area*
   - *4K Full HDR Black with Active Area*
   - *4K Scope HDR Black with Active Area*
   - *4K Flat HDR Black with Active Area*

   Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	[DV-ADD] [DCI-HDR]
Test Materials	*2K Full HDR Black with Marks* *2K Scope HDR Black with Marks* *2K Flat HDR Black with Marks* *4K Full HDR Black with Marks* *4K Scope HDR Black with Marks* *4K Flat HDR Black with Marks* *2K Full HDR Black with Active Area* *2K Scope HDR Black with Active Area* *2K Flat HDR Black with Active Area* *4K Full HDR Black with Active Area* *4K Scope HDR Black with Active Area* *4K Flat HDR Black with Active Area*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—

7.5.33. Image Frame Rates

Objective

Verify that the Imaging Device displays every frame at all required frame rates.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Play each of the following compositions in turn:

    a. If the Test Subject is an SDR Projector:

    - *2K 2D 24 FPS Test*
    - *2K 2D 48 FPS Test*
    - *4K 2D 24 FPS Test*

    b. For all other Test Subjects:

    - *2K 2D 24 FPS Test*
    - *2K 2D 48 FPS Test*
    - *2K 2D 60 FPS Test*
    - *2K 2D 96 FPS Test*
    - *2K 2D 120 FPS Test*
    - *4K 2D 24 FPS Test*
    - *4K 2D 48 FPS Test*
    - *4K 2D 60 FPS Test*

3. For each of the compositions played above, and as illustrated at Figure 7.5, verify that:

    - the movement of the pendulum is smooth and uninterrupted;

- the timecode is displayed at the bottom of the frame matches the one displayed at the top right of the frame;
- for 4K compositions, the word 4K is displayed at the center of the image;
- the words "left" and "right" are heard through the **Sound System** as the pendulum reaches the extreme left and right of its trajectory, respectively; and
- the following words appear: 1, 2, 3, 4, 5, even and odd.

Any verification that fails is cause to fail this test.

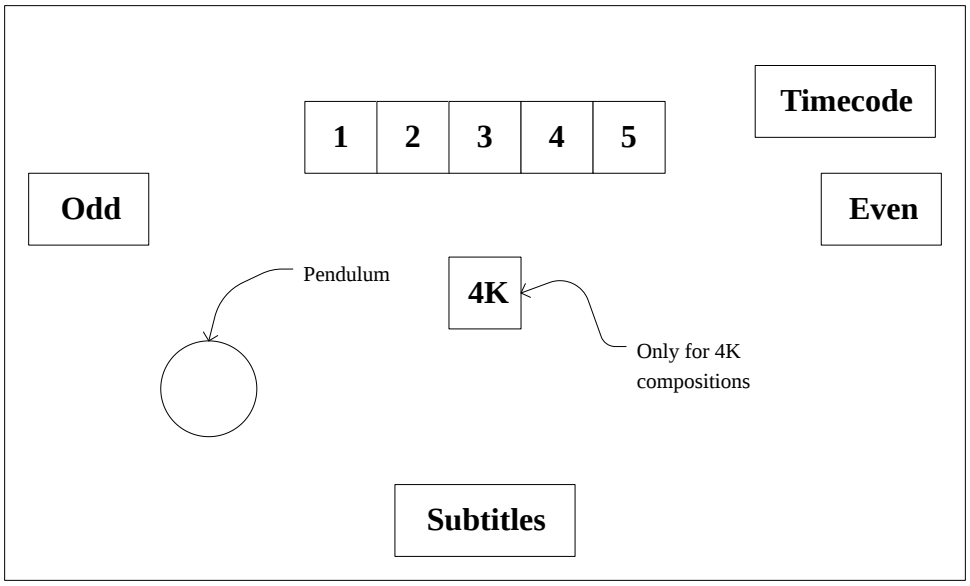

Figure 7.5.33. Location of the elements displayed when testing image frame rates (not to scale)

Supporting Materials

Reference Documents	[DV-ADD] DCI-DCSS, 3.2.1
Test Equipment	**Sound System**
Test Materials	*2K 2D 24 FPS Test* *2K 2D 48 FPS Test* *2K 2D 60 FPS Test* *2K 2D 96 FPS Test* *2K 2D 120 FPS Test* *4K 2D 24 FPS Test* *4K 2D 48 FPS Test* *4K 2D 60 FPS Test*

Consolidated Test Sequences

Sequence	Type	Measured Data
24.2. SDR Projector Test Sequence	Pass/Fail	—
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

7.5.34. Stereoscopic Image Frame Rates

Objective

Verify that, for stereoscopic presentations, the Imaging Device displays every frame at all required frame rates.

Procedures

This test procedure only applies to Test Subject that support stereoscopic presentations.

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Play each of the following compositions in turn:

    - *2K Stereoscopic 24 FPS Test*
    - *2K Stereoscopic 48 FPS Test*
    - *2K Stereoscopic 60 FPS Test*

3. For each of the compositions played above, and as illustrated at Figure 7.5, verify that:

    - the movement of the pendulum is smooth and uninterrupted;
    - the pendulum pops out of the screen;
    - the timecode is displayed at the bottom of the frame matches the one displayed at the top right of the frame;
    - the words "left" and "right" are heard through the **Sound System** as the pendulum reaches the extreme left and right of its trajectory, respectively;
    - the words `left` and `right` appear only in the left and right eye, respectively; and
    - the following words appear: `1`, `2`, `3`, `4`, `5`, `even` and `odd`.

Any verification that fails is cause to fail this test.

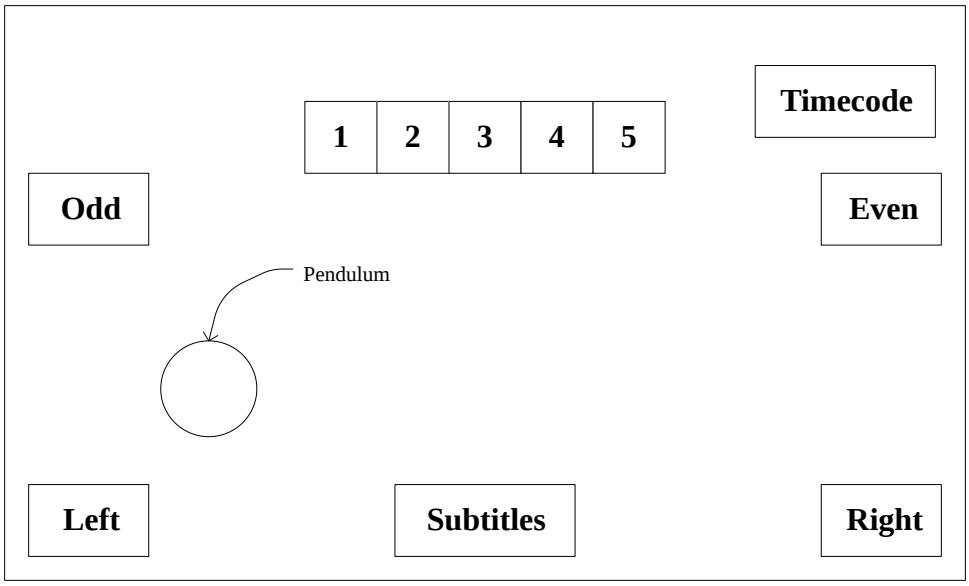

Figure 7.5.34. Location of the elements displayed when testing stereoscopic image frame rates (not to scale)

Supporting Materials

Reference Documents	[DV-ADD] DCI-DCSS, 10.2.2
Test Equipment	**Sound System**
Test Materials	*2K Stereoscopic 24 FPS Test* *2K Stereoscopic 48 FPS Test* *2K Stereoscopic 60 FPS Test*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
27.2. SDR Direct View Display Test Sequence	Pass/Fail	—

7.5.35. HDR Contouring

Objective

Confirm the Imaging Device exhibits no visible contouring when presenting an HDR composition.

Procedures

1. Ensure that the Imaging Device setup and test environment requirements detailed in 7.1. Test Environment for Image Measurements have been performed.

2. Play back *HDR Dark Gray Scale* and measure, using a a **Spectroradiometer**, the luminance L_i at the center of the screen of each full-screen gray patch.

3. Calculate the set of second approximate derivatives from the set of measurements $\{L_i\}$ according to the *slope monotonicity of gray scale* procedure at [ICDM IDMS].

4. Verify that all the second approximate derivatives are greater than 0.

Any verification that fails is cause to fail this test.

Supporting Materials

Reference Documents	DCI-DCSS, 8.3.3 [SMPTE-431-2] [DCI-HDR]
Test Materials	*HDR Dark Gray Scale*

Consolidated Test Sequences

Sequence	Type	Measured Data
26.2. HDR Direct View Display Test Sequence	Pass/Fail	—
28.2. HDR Projector Test Sequence	Pass/Fail	—

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 IEEE-802-3
Test Equipment	**Network Analyzer**
Test Materials	*DCI 2K StEM Test Sequence (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 a drive 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 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 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)* *KDM for 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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)* *KDM for 2K Maximum Bitrate Composition (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—

8.1.5. Deleted Section

The section "Storage System Redundancy (OBAE)" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
Test Materials	*2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)* *KDM for 2K DCI Maximum Bitrate Composition (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO 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* *DCI 2K StEM (Encrypted)* *KDM for 2K StEM (Encrypted)* *DCI Black Spacer - 5 seconds*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Data only	—
21.2. Integrated IMBO Test Sequence	Data only	—

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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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	**GPIO Test Fixture**
Test Materials	*DCI 2K StEM Test Sequence*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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* *DCI 5.1 Channel Identification* *DCI 2K Sync test with Subtitles (Encrypted)* *DCI 2K StEM (Encrypted)* *KDM for DCI 2K Sync Test with Subtitles (Encrypted)*

KDM for 2K StEM (Encrypted)

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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)* *DCI 2K Image with Frame Number Burn In (Scope)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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, a 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)* *DCI 2K Image with Frame Number Burn In (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	Record the available operator roles (names) and whether locally-defined accounts can be created.
21.2. Integrated IMBO Test Sequence	Pass/Fail	Record the available operator roles (names) and whether locally-defined accounts can be created.

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)* *KDM for 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 that identifies the SMS entity.
- 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** **openssl**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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 SMPTE-430-1
Test Materials	*DCI 2K StEM (Encrypted)* *DCI 2K Sync Test (Encrypted)* *KDM for DCI 2K Sync Test (Encrypted)* *KDM with incorrect message digest* *KDM that has expired* *KDM with future validity period* *KDM with invalid XML* *KDM with empty TDL* *KDM with Assume Trust TDL Entry for 2K StEM (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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 is 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 SMPTE-430-1
Test Materials	*DCI 2K StEM (OBAE) (Encrypted)* *DCI 2K Sync Test (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test (OBAE) (Encrypted)* *KDM with incorrect message digest (OBAE)* *KDM that has expired (OBAE)* *KDM with future validity period (OBAE)* *KDM with invalid XML (OBAE)* *KDM with empty TDL (OBAE)* *KDM with Assume Trust TDL Entry (OBAE)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
20.4. OMB Confidence Sequence	Pass/Fail	—
21.4. Integrated 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 8.2, 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 8.2.14. 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 SMPTE-430-1
Test Equipment	**Accurate Real-Time Clock** **Text Editor**
Test Materials	*DCI 2K Sync test with Subtitles (Encrypted)* *DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* *KDM for DCI 2K Sync test with Subtitles (Encrypted): missing picture essence key* *KDM for DCI 2K Sync test with Subtitles (Encrypted): missing sound essence key* *KDM for DCI 2K Sync test with Subtitles (Encrypted): missing subtitle essence key* *KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing picture essence key*

	KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing sound essence key *KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing picture subtitle key* *KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted): missing OBAE key*

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated 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 SMPTE-430-2
Test Equipment	**Network Analyzer** **openssl**

Consolidated Test Sequences

Sequence	Type	Measured Data
15.2. Integrated IMB Test Sequence	Pass/Fail	—
15.4. Integrated IMB Confidence Sequence	Pass/Fail	—
21.2. Integrated IMBO Test Sequence	Pass/Fail	—
21.4. Integrated 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
Test Materials	*DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* *KDM for DCI 2K Sync Test with subtitles (OBAE) (Encrypted)* *OBAE Rendering Expectations (Clip)* *DCI 2K StEM (OBAE) (Encrypted)* *KDM for 2K StEM (Encrypted) (OBAE)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO 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, a 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 (OBAE) (Encrypted)* *DCI 2K Image with Frame Number Burn In (OBAE) (Encrypted)*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Pass/Fail	—
21.2. Integrated IMBO 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
Test Materials	*DCI 2K StEM (OBAE)* *DCI 2K StEM (OBAE) (Encrypted)* *KDM for 2K StEM (Encrypted) (OBAE)* *DCI Black Spacer - 5 seconds*

Consolidated Test Sequences

Sequence	Type	Measured Data
20.2. OMB Test Sequence	Data only	—
21.2. Integrated IMBO Test Sequence	Data only	—

8.2.19. Deleted Section

The section "Automation Control and Interfaces (OBAE)" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
Test Materials	*DCI 2K StEM (OBAE) (Encrypted)* *KDM for 2K StEM (Encrypted) (OBAE)*

Consolidated Test Sequences

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

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 CMVP testing 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 CMVP testing 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 CMVP testing laboratory 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 CMVP Testing Laboratory

FIPS 140 testing is performed by an accredited CMVP testing laboratory. This CMVP testing laboratory will assist the manufacturer in preparing the required documentation and will test sample devices for conformance to the documentation. The CMVP testing 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 CMVP testing laboratory or the manufacturer.

NIST makes available the list of accredited CMVP testing laboratories on the agency web site (see http://csrc.nist.gov/groups/STM/ testing_labs/index.html). Any of the testing 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 CMVP testing laboratories and CMVP testing 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 CMVP testing laboratory is a proprietary and closely controlled document. The manufacturer must ensure that it has permission to disclose the test report to the 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 CMVP procedures. The manufacturer must work with the CMVP testing laboratory 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 CMVP testing 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 CMVP testing 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 CMVP testing 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 CMVP testing laboratory 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 CMVP testing 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 CMVP testing laboratory. The submission may be rejected, in which case the manufacturer and CMVP testing 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 CMVP testing 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 CMVP testing 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. CMVP Testing Laboratory Reports

A FIPS 140 validation test report is created by CMVP testing 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 CMVP testing 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 Testing Organization must obtain an official copy of the FIPS 140 validation test report directly from the CMVP testing laboratory 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 FIPS-140-2 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

9.5.2. Deleted Section

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

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 FIPS-140-2 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

9.5.4. Deleted Section

The section "Security Design Description Requirements" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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 RFC-3447 FIPS-140-2 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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. *This step has been deleted*
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 FIPS-140-2 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

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 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

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 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

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 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

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 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

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 FIPS-140-3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

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 appicable requirement specified in this Chapter. To see which requirements are relevant to a particular Test Subject 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector 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)
- Forensic Marker (FM)

Reference Documents	DCI-DCSS, 9.4.1.1, 9.3.3.2

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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] [RFC-2246] [RFC-8446] DCI-DCSS, 9.4.1.1, 9.4.2.5, 9.4.5.1, 9.4.5.2.3.(9)

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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. Deleted Section

The section "Secure Remote SPB-SM Communications" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.10. Deleted Section

The section "Special Auditorium Situation Detection" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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.

Reference Documents	DCI-DCSS, 9.4.3.5

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.12. Deleted Section

The section "SPB Authentication" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

10.4.13. TLS Session Key Refreshes

The section "TLS Session Key Refreshes" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

10.4.14. LE Key Issuance

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

10.4.15. Maximum Key Validity Period

The section "Maximum Key Validity Period" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.18. Imaging Device Secure Silicon Device

Verify that the Imaging Device 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
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector Design Review	Pass/Fail

10.4.19. Access to Imaging Device Image Signals

Verify that the Imaging Device SPB design does not allow physical access to signals running between the companion SPB and the Imaging Device SPB without breaking the marriage.

Reference Documents	DCI-DCSS, 9.4.3.6.1

Sequence	Type
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector Design Review	Pass/Fail

10.4.20. Systems with Electronic Marriage

Verify that an electronic marriage is planned upon installation of a MB Imaging Device 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
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector Design Review	Pass/Fail

10.4.21. Systems Without Electronic Marriage

Verify that in the configuration of a permanently married companion SPB (MB) the companion SPB is not field replaceable and require the Imaging Device SPB and companion SPB system to both be replaced in the event of an SPB failure.

If 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
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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.

Reference Documents	DCI-DCSS, 9.4.3.7

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector 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 Imaging Device SPB; perimeter access panel monitoring

b. the Imaging Device 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
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO 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. Deleted Section

The section "SMS and SPB Authentication and ITM Transport Layer" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

10.4.31. Deleted Section

The section "Idempotency of ITM RRPs" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.34. Deleted Section

The section "RRP Broadcast Prohibition" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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 SMPTE-430-6

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.36. Deleted Section

The section "RRP Initiator" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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] [RFC-2246] [RFC-8446] DCI-DCSS, 9.4.2.5, 9.4.5.2.4, 9.4.5.2.3.(9)

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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 or 20-bit "location" Forensic Marking Identification (FMID) that is permanently associated with the associated MB.
- Verify that all FM inserters insert a 16-bit time stamp that increments by 1 every 15 minutes and resets to zero once per year.

Reference Documents	DCI-DCSS, 8.2.2.9, 9.4.6.1.1, 9.4.6.2(9)

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
21.3. Integrated 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 SMPTE-430-1

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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. Deleted Section

The section "SE Log Authoring" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.52. Deleted Section

The section "Remote SPB Log Storage Requirements" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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.

Reference Documents	DCI-DCSS, 9.4.6.3.1

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.54. Deleted Section

The section "Logging for Standalone Systems" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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 Imaging Device SPB, 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

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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 NIST-800-38F

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.70. Deleted Section

The section "ASM Get Time Frequency" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.74. Companion SPB Retrieve Imaging Device Cert

Only applies to a Test Subject that is a Companion SPB (SM).

Verify that the Test Subject retrieves the Imaging Device SPB certificate over the marriage connection.

Reference Documents	DCI-DCSS, 9.4.3.6.5

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.75. Log Collection for Married MB

Verify that, when integrated within an Imaging Device as a companion SPB, or permanently married to the Imaging Device, the MB provides 24/7 log recording support, and storage of all log records associated with the Imaging Device SPB.

Reference Documents	DCI-DCSS, 9.4.3.6.3

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
21.3. Integrated 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 designed to operate with an integrated Imaging Device.

Verify that the Test Subject does not operate unless integrated with an Imaging Device SPB. In particular,

- if the Test Subject is a MB, verify that the Test Subject cannot perform any composition decryption function unless integrated within and married to an Imaging Device SPB.

Reference Documents	DCI-DCSS, 9.4.3.6.3, 9.4.3.6.2

Sequence	Type
15.3. Integrated IMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.77. Deleted Section

The section "Standalone MB Single Purpose Requirement" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

10.4.78. Imaging Device SPB Log Reporting Requirements

Verify that the Imaging Device 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
24.3. SDR Projector Design Review	Pass/Fail
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail
28.3. HDR Projector 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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.4.80. TLS Authentication of Dual Certificate SM

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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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 (Imaging Device or other MB), except to accept non-security messaging; and
- Process essence other than the following:

- Object-Based Audio Essence (OBAE) as defined in Section 3.3 of [DCI-DCSS]; 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, 3.3, 9.1, 9.4.3.6.3(5), 9.4.3.6.4, 9.4.2.7, 9.4.5 SMPTE-429-14

Sequence	Type
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
15.3. Integrated IMB Design Review	Pass/Fail
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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 SMPTE-429-14

10.4.84. Deleted Section

The section "OBAE Addendum" was deleted. The section number is maintained here to preserve the numbering of subsequent sections.

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

Sequence	Type
20.3. OMB Design Review	Pass/Fail
21.3. Integrated 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

Sequence	Type
20.3. OMB Design Review	Pass/Fail
21.3. Integrated IMBO Design Review	Pass/Fail

10.5. DCI Requirements for Imaging Devices

Each of the subsections below describes a DCI requirement that shall be verified by examining the manufacturer's documentation.

10.5.1. Pixel Visibility (Direct View Display)

Verify, according to the following steps, that the display pixel density of the imaging device is equal to or greater than 60 display pixels per degree when viewed at 1.6 screen heights:

1. Based on manufacturer's information, determine the number of display pixels R_h of the imaging device in the vertical direction when displaying the 4096x2160 DCI container. The term display pixel is defined at [DV-ADD].
2. Compute the pixel density at viewing distance of 1.6 screen heights $P_{1.6}$ according to the equation
   $P_{1.6} = 1 / \arctan(1 / (1.6 \cdot R_h))$
   where arctan() is the inverse-tangent function that returns units of degrees, i.e. arctan(1) = 45 degrees.
3. A value $P_{1.6}$ smaller than 60 display pixels per degree is cause to fail this test.

Note: The nominal average human vision performance called 20/20 vision corresponds to the ability to resolve 30 cycles per degree. On an imaging device the minimum pixel density that can show 30 cycles per degree is 60 pixels per degree.

Reference Documents	[DV-ADD]

Sequence	Type
26.3. HDR Direct View Display Design Review	Pass/Fail
27.3. SDR Direct View Display Design Review	Pass/Fail

PART III. CONSOLIDATED TEST PROCEDURES

The chapters in this part contain Test Sequences and a standardized Test Report for testing Digital Cinema equipment. Each Test Sequence subjects a Test Subject to a set of Tests selected from Part I. Procedural Tests and Part II. Design Evaluation Guidelines.

The Test Subject is specified at the opening of each Test Sequence chapter and at Table 11.2. Each Test Subject comprises a single *certificated device*.

Chapter 11. Testing Policy and Reporting

11.1. Test Reports

A Test Report consists of information about a Test Session recorded as specified in Table 11.1. All fields shall be filled in.

Each certificated device listed on line 9 of a Test Report, with the exception of an SMS, shall be a DCI compliant certificated device as defined below.

Note: NOTE 1: Certificated devices listed on line 9 of a Test Report might have achieved DCI compliance against different versions of the CTP.

Note: EXAMPLE 1: An IMB that achieved DCI-compliance per CTP 1.3 can be used when performing Chapter 24. SDR Projector Consolidated Test Sequence in this version of the CTP.

For a permanently married Imaging Device, line 9 of a Test Report shall identify the Imaging Device and companion device (per [DCI-DCSS], Section 9.4.3.6.6).

For an integrated SMS, line 9 of a Test Report shall identify the SMS and IMB (per [DCI-DCSS], Section 9.4.2.5, first bullet).

To assure clarity, line 9 of a Test Report shall include the text "permanently married" or "permanently integrated" as applicable.

Table 11.1. Test Session Data

0. Reporting date	
0. Test Start Date	
0. CTP version	
0. Name of Testing Organization	
0. Address of Testing Organization	
0. Name of Test Operator	
0. Test location (if not at Testing Organization's site)	
0. Name of Test Subject Representative	
0. Address of Test Subject Representative	
0. Make and model of Test Subject (to be included on the DCI listing hot link)	
0. Serial and model numbers identifying each of the participating certificated devices, including software and/or firmware version numbers as applicable.	
0. Test sequence performed (select one)	☐ Chapter 15. Integrated IMB Consolidated Test Sequence ☐ Chapter 20. OMB Consolidated Test Sequence ☐ Chapter 21. Integrated IMBO Consolidated Test Sequence ☐ Chapter 24. SDR Projector Consolidated Test Sequence ☐ Chapter 26. HDR Direct View Display Consolidated Test Sequence ☐ Chapter 27. SDR Direct View Display Consolidated Test Sequence ☐ Chapter 28. HDR Projector Consolidated Test Sequence
0. Test status (select one)	☐ Pass ☐ Fail
0. Sequences performed (select one)	☐ Test Sequence and Design Review ☐ Confidence Sequence (Confidence Retest)

A Test Session is the collection of Test Results gathered by subjecting a set of certificated devices to one of the Test Sequences listed in Table 11.2, with the set of certificated devices including at least those required by the Test Sequence. A certificated device is defined by the combination of its manufacturer, product name and model/version number.

Note: NOTE 2: the set of certificated devices used for a Test Session cannot change, e.g., the same IMB is used for all tests specified in a Test Session against Chapter 24. SDR Projector Consolidated Test Sequence.

Note: NOTE 3: two IMBs with different model/version number are not the same IMB when creating a Test Session.

Table 11.2. Test Sequences

Test sequence	Test subject	Certificated device that comprise the Test subject	Certificated devices required to perform the Test Sequence
Chapter 15. Integrated IMB Consolidated Test Sequence	Integrated IMB	IMB	Imaging Device, IMB, SMS
Chapter 20. OMB Consolidated Test Sequence	Outboard Media Block	OMB	Imaging Device, OMB, IMB, SMS
Chapter 21. Integrated IMBO Consolidated Test Sequence	Integrated IMBO	IMBO	Imaging Device, IMBO, SMS
Chapter 24. SDR Projector Consolidated Test Sequence	Projector	Projector	Projector, IMB or IMBO, SMS
Chapter 26. HDR Direct View Display Consolidated Test Sequence	Direct View Display	Direct View Display	Direct View Display, IMB or IMBO, SMS
Chapter 27. SDR Direct View Display Consolidated Test Sequence	Direct View Display	Direct View Display	Direct View Display, IMB or IMBO, SMS
Chapter 28. HDR Projector Consolidated Test Sequence	Projector	Projector	Projector, IMB or IMBO, SMS

A Test Result is the outcome of evaluating a set of certificated devices against the steps and requirements of a single Test specified in this version of the CTP. Each Test specifies the type of test result generated, either PASS, FAIL or measured data.

A Test Result may, at the discretion of the Testing Organization, be reused across multiple Test Sessions, and thus different Test Sequences, if and only if (a) the underlying test is identical and (b) the set of certificated devices subjected to the Test are identical. The Testing Organization is required to attest that both conditions (a) and (b) are met.

Note: NOTE 4: The above constraints require the supplier(s) of each certificated device to present to the Testing Organization the Test Results to be reused.

EXAMPLE 2: the Test Result obtained by subjecting an SMS to 8.1.1. Storage System Ingest Interface in the course of performing a Test Session against Chapter 15. Integrated IMB Consolidated Test Sequence can be reused when subjecting the same SMS (as defined by its manufacturer, product name and model/version number) to the same test procedure in the course of performing a Test Session against Chapter 21. Integrated IMBO Consolidated Test Sequence.

EXAMPLE 3: the Test Result obtained by subjecting an IMB to 5.1.1. SPB Digital Certificate as specified in CTP 1.2.1 cannot be reused when subjecting the same IMB against the same test procedure in this version of CTP since 5.1.1. SPB Digital Certificate is not identical in both versions of the CTP.

The status of the Test Session is PASS if none of the test results is FAIL; the status of the Test Session is FAIL otherwise.

The certificated device that comprises a Test Subject of a Test Session whose status is PASS is a “DCI compliant certificated device”.

Note: NOTE 5: A “DCI compliant certificated device” is defined in the context of a specific Test Session, i.e., for a particular set of certificated devices and set of tests defined in a specific version of the CTP. As such, while the certificated device remains DCI-compliant in perpetuity within that context, not all Test Results associated with the DCI compliant certificated device can necessarily be reused in all future Test Sessions in which the certificated device is involved, as described in this section.

11.2. Testing Policy

11.2.1. Definitions

Non-Programmable Related Components (NPRC)

Any non-programmable devices that do not affect compliance of the current DCSS, e.g., nonprogrammable integrated circuits, resistors, capacitors, transistors, inductors, lamps, fans, displays, power supplies, switches,

connectors, fuses, passive components, mechanical components, etc.

11.2.2. Combining Devices into Families

An entity may aggregate some of its products that only have different NPRCs into a family group by attesting to the similarity of that family group in a letter, signed by a person who has authority to bind the entity under test to the terms of said letter. The letter shall be sent to the contracted licensed test entity and to DCI at dci.info@dcimovies.com.

The letter, which will be attached to the detailed report of the tested device, will clearly and comprehensively provide detailed information and justification as described below:

- Clear justification for combining various products into a family group.
- Itemized model number and description of the product tested and each of the products proposed to be in the same family group.
- Clear itemized differences between each product model in a proposed family group.
- Attest that all SPB-1 electrical, mechanical, and data-protocol interfaces and behavior are identical among all models of the proposed family group.
- Attest that all implementations of SPB-2 normative device requirements are identical among all models of the proposed family group.

Further, the form specified in Table 11.3 shall be attached to the letter to identify the general family group information. This form will be published with the summary report of the tested device on the DCI Compliant Family Groups web site page.

Table 11.3. General family group information

Manufacturer		
Testament Submission Date		
Equipment Tested		
Family Item 0	Make	
	Model	
	Version	
Family Item 1	Make	
	Model	
	Version	
Family Item 2	Make	
	Model	
	Version	
(add items as needed)		
Printed Name		
Job Title		
Signature		

11.2.3. Equipment Component Failures during Testing

11.2.3.1. Failures within the Test Subject

If any NPRCs fail within a Test Subject during CTP testing, the components may be replaced with *equivalent* units (having identical technical specifications) and testing resumed from a test point before any anomalous behavior was first observed. In order to assure compliance, the DCI licensed entity will determine the appropriate resumption point and continue testing all procedures thereafter in numerical order.

If any programmable components (e.g., FPGAs) fail within a Test Subject during CTP testing and it can be shown rigorously by the manufacturer that a completely identical component with identical programming is available (same component, version and programming), the programmable component may be replaced with the identical component and testing resumed from a test point before any anomalous behavior was first observed. In order to assure compliance, the DCI licensed entity will determine the appropriate resumption point and continue testing all procedures thereafter in numerical order.

It is recognized that when an SPB-1 or SPB-2 is replaced, the private key will necessarily change. However, the certificate formulation (e.g., digest method, subject name component values (O, OU), subject name CN roles, RSA, key length, extensions, etc.) will need to be identical to that of the certificate in the original SPB so as to result in the same system behavior.

11.2.3.2. Failures of Devices Connected to the Test Subject

Any device that fails during CTP testing that is connected to the Test Subject may be repaired and then verified as to its correct behavior. If correct behavior is verified, testing may resume from a test point before any anomalous behavior was first observed.

11.2.4. Changes to Previously DCI CTP Compliant Devices

11.2.4.1. General

Once compliance has been established for a particular device model per this specification, all product changes shall maintain compliance with the [DCI-DCSS] and this specification. Product changes may require retesting to ensure continued compliance. For the avoidance of doubt, no retesting is required if there are no product changes.

11.2.4.2. SPB Type 1 (SPB-1) Devices

Changes of any kind may require retesting of the SPB-1 device for FIPS 140 compliance by a Cryptographic Module Validation Program (CMVP) testing laboratory. The extent of retesting of FIPS compliance shall be at the determination of the CMVP testing laboratory. Device manufacturers shall notify DCI at dci.info@dcimovies.com of all SPB-1 upgrades prior to deployment, identifying all relevant component version numbers.

11.2.4.3. NPRC

Replacing NPRCs with technically equivalent components will not require retesting.

11.2.4.4. Software/Firmware and Confidence Retesting

All changes to software and firmware shall maintain compliance with the [DCI-DCSS] and this specification. Device manufacturers shall notify DCI at dci.info@dcimovies.com of all upgrades prior to deployment, identifying all relevant component version numbers.

Changes to software or firmware shall require Confidence Retesting by a licensed DCI test entity on a “three-year or four-upgrade cycle” if either

a. one, two or three upgrades are deployed within three years of the CTP compliance date, the device shall undergo a Confidence Retest prior to its third-year anniversary date; or

b. a fourth upgrade is intended to be deployed within three years of the CTP compliance date, the device shall undergo a Confidence Retest with the cumulative changes of all four upgrades installed prior to the deployment of that fourth upgrade.

Any Confidence Retest of updated software or firmware shall be conducted against the version of this specification in force as of the date the device is submitted for Confidence Retest, subject to the following exceptions.

To minimize barriers to upgrades, SPB devices that are *already listed* on the Compliant Equipment page of the DCI website may be excused from CTP tests associated with the bullets below for purposes of a Confidence Retest:

- Dual Media Block digital certificate requirements of [DCI-DCSS], Section 9.5.1, which were changed by DCI-DCSS-ERR-20110420.
- Secure silicon integrated circuit requirements of [DCI-DCSS], Section 9.5.2.2, which were changed by [DCI-DCSS-ERR-20160830].
- Self-generated RSA key pair establishment per [DCI-DCSS], Section 9.5.1, which was changed by [DCI-DCSS-ERR-20160428].
- Evolving NIST/FIPS requirements for SP800-90B and SP800-56Br2 compliance, per the [DCI-NIST-NOTE].

Confidence Retests have been selected to assure that software/firmware changes have not impacted critical security functionality. Hardware, integrated circuit, FIPS related issues, etc., are addressed by Sections 11.2.4.2. SPB Type 1 (SPB-1) Devices and 11.2.4.3. NPRC.

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. Deleted Chapter

The chapter "Digital Cinema Server Consolidated Test Sequence" was deleted. The chapter number is maintained here to preserve the numbering of subsequent sections.

Chapter 14. Deleted Chapter

The chapter "Standalone D-Cinema Projector Consolidated Test Sequence" was deleted. The chapter number is maintained here to preserve the numbering of subsequent sections.

Chapter 15. Integrated IMB Consolidated Test Sequence

15.1. Overview

The test sequence defined in this chapter is intended to be used to test a 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. Integrated IMB 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	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	5.4.2.6. SPBStartup and SPBShutdown Events			
20	5.4.2.7. SPBOpen and SPBClose Events			
21	5.4.2.8. SPBClockAdjust Event			
22	5.4.2.9. SPBMarriage and SPBDivorce Events			
23	5.4.2.10. SPBSoftware Event			
24	5.4.2.11. SPBSecurityAlert Event	(data only)		
25	6.1.1. Image Integrity Checking			
26	6.1.2. Sound Integrity Checking			
27	6.1.4. Restriction of Keying to MD Type			
28	6.1.5. Restriction of Keying to Valid CPLs			
29	6.1.8. Content Key Extension, End of Engagement			
30	6.1.9. ContentAuthenticator Element Check			
31	6.1.10. KDM Date Check			
32	6.1.11. KDM TDL Check			
33	6.1.12. Maximum Number of DCP Keys			
34	6.1.13. CPL Id Check			
35	6.1.15. Restriction of Playback in Absence of Integrity Pack Metadata			
36	6.1.19. Plurality of Media Block Identity Certificates			
37	6.1.20. Validity of SPB Certificates			

38	6.3.1. Clock Adjustment			
39	6.3.2. SPB Type 1 Clock Battery			
40	6.3.3. Clock Resolution			
41	6.4.1. FM Application Constraints			
42	6.4.2. Granularity of FM Control			
43	6.4.3. FM Payload			
44	6.4.4. FM Audio Bypass			
45	6.4.5. Selective Audio FM Control			
46	6.5.1. Playback of Image Only Material			
47	6.5.2. Decoder Requirements			
48	6.6.1. Digital Audio Interfaces			
49	6.6.2. Audio Sample Rate Conversion			
50	6.6.3. Audio Delay Setup			
51	6.6.4. Click Free Splicing of Audio Track Files			
52	6.7.1. Media Block Overlay			
53	6.7.4. Default Timed Text Font			
54	6.7.6. Timed Text Decryption			
55	7.3.2. Companion SPBs with Electronic Marriage			
56	7.3.3. Companion SPB Marriage Break Key Retaining			
57	8.1.1. Storage System Ingest Interface			
58	8.1.2. Storage System Capacity			
59	8.1.3. Storage System Redundancy			
60	8.1.4. Storage System Performance			
61	8.2.2. Show Playlist Creation	(data only)		
62	8.2.3. Show Playlist Format			
63	8.2.5. Automation Control and Interfaces			
64	8.2.6. Interrupt Free Playback			
65	8.2.7. Artifact Free Transition of Image Format			
66	8.2.8. Restarting Playback			
67	8.2.9. SMS User Accounts			
68	8.2.10. SMS Operator Identification			
69	8.2.11. SMS Identity and Certificate			
70	8.2.12. Content Keys and TDL check			
71	8.2.14. KDM Content Keys Check			
72	8.2.15. Validity of SMS Certificates			

15.3. Integrated IMB 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	Exhibit Identifiers

1	9.5.1. SM Operating Environment			
2	9.5.3. SPB Type 1 Tamper Responsiveness			
3	9.5.6. SPB Type 1 FIPS Requirements			
4	9.5.8. Asymmetric Key Generation			
5	9.5.9. Critical Security Parameter Protection			
6	9.5.11. Degraded mode(s) of operation prohibited			
7	9.5.12. Control output inhibition			
8	9.5.13. Maintenance role/interface prohibited			
9	9.5.14. Self-initiated cryptographic output capability			
10	9.5.15. Self-initiated cryptographic output capability			
11	9.5.16. Periodic self-tests			
12	10.4.1. Theater System Reliability			
13	10.4.2. Theater System Storage Security			
14	10.4.3. Security Devices Self-Test Capabilities			
15	10.4.4. Security Entity Physical Protection			
16	10.4.5. Secure SMS-SM Communication			
17	10.4.6. Location of Security Manager			
18	10.4.9. Playback Preparation			
19	10.4.11. Prevention of Keying of Compromised SPBs			
20	10.4.16. KDM Purge upon Expiry			
21	10.4.17. Key Usage Time Window			
22	10.4.22. Clock Date-Time-Range			
23	10.4.23. Clock Setup			
24	10.4.24. Clock Stability			
25	10.4.25. Repair and Renewal of SPBs			
26	10.4.27. Clock Continuity			
27	10.4.28. TLS Endpoints			
28	10.4.32. RRP Synchronism			
29	10.4.33. TLS Mode Bypass Prohibition			
30	10.4.35. Implementation of Proprietary ITMs			
31	10.4.39. RRP "Busy" and Unsupported Types			
32	10.4.40. RRP Operational Messages			
33	10.4.42. FM Algorithm General Requirements			
34	10.4.43. FM Insertion Requirements			
35	10.4.44. IFM Visual Transparency			
36	10.4.45. IFM Robustness			
37	10.4.46. AFM Inaudibility			
38	10.4.47. AFM Robustness			
39	10.4.48. FM Control Instance			

15.4. Integrated IMB 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	Measured data
1	5.1.1. SPB Digital Certificate			
2	5.4.1.6. KDMKeysReceived Event			
3	5.4.2.10. SPBSoftware Event			
4	6.1.5. Restriction of Keying to Valid CPLs			
5	6.1.8. Content Key Extension, End of Engagement			
6	6.1.9. ContentAuthenticator Element Check			
7	6.1.11. KDM TDL Check			
8	6.1.20. Validity of SPB Certificates			
9	6.3.1. Clock Adjustment			
10	6.4.3. FM Payload			
11	7.3.2. Companion SPBs with Electronic Marriage			
12	7.3.3. Companion SPB Marriage Break Key Retaining			
13	8.2.7. Artifact Free Transition of Image Format			
14	8.2.11. SMS Identity and Certificate			
15	8.2.12. Content Keys and TDL check			
16	8.2.15. Validity of SMS Certificates			

Chapter 16. Deleted Chapter

The chapter "Link Decryptor/Encryptor Consolidated Test Sequence" was deleted. The chapter number is maintained here to preserve the numbering of subsequent sections.

Chapter 17. Deleted Chapter

The chapter "Digital Cinema Server Consolidated Confidence Sequence" was deleted. The chapter number is maintained here to preserve the numbering of subsequent sections.

Chapter 18. Deleted Chapter

The chapter "Standalone D-Cinema Projector Consolidated Test Sequence" was deleted. The chapter number is maintained here to preserve the numbering of subsequent sections.

Chapter 19. Deleted Chapter

The chapter "Integrated IMB Consolidated Confidence Sequence" was moved to 15.4. Integrated IMB Confidence Sequence. The chapter number is maintained here to preserve the numbering of subsequent sections.

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, Projector, 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.

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	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 (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	5.4.2.11. SPBSecurityAlert Event	(data only)		
23	6.1.14. CPL Id Check (OBAE)			
24	6.1.15. Restriction of Playback in Absence of Integrity Pack Metadata			
25	6.1.16. Restriction of Keying to MDEK Type (OBAE)			
26	6.1.17. OBAE Integrity Checking			
27	6.1.18. Content Key Extension, End of Engagement (OBAE)			
28	6.1.19. Plurality of Media Block Identity Certificates			
29	6.1.20. Validity of SPB Certificates			
30	6.1.21. Maximum Number of DCP Keys (OBAE)			
31	6.1.22. Restriction of Keying to Valid CPLs (OBAE)			
32	6.1.23. ContentAuthenticator Element Check (OBAE)			
33	6.1.24. KDM Date Check (OBAE)			
34	6.3.1. Clock Adjustment			
35	6.3.2. SPB Type 1 Clock Battery			
36	6.3.4. Clock Resolution (OMB)			

37	6.3.5. Clock Adjustment (OMB)			
38	6.4.6. FM Application Constraints (OBAE)			
39	6.4.7. Granularity of FM Control (OBAE)			
40	6.4.8. FM Payload (OBAE)			
41	6.4.9. FM Audio Bypass (OBAE)			
42	6.5.1. Playback of Image Only Material			
43	6.8.1. Click Free Splicing of OBAE Track Files			
44	6.8.2. OBAE Delay Setup			
45	6.8.3. Maximum Bitrate OBAE			
46	6.8.4. OBAE Rendering Expectations			
47	8.1.6. Storage System Performance (OBAE)			
48	8.2.13. Content Keys and TDL check (OBAE)			
49	8.2.14. KDM Content Keys Check			
50	8.2.16. Interrupt Free Playback (OBAE)			
51	8.2.17. Restarting Playback (OBAE)			
52	8.2.18. Show Playlist Creation (OBAE)	(data only)		
53	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	Exhibit Identifiers

1	9.5.1. SM Operating Environment			
2	9.5.3. SPB Type 1 Tamper Responsiveness			
3	9.5.6. SPB Type 1 FIPS Requirements			
4	9.5.8. Asymmetric Key Generation			
5	9.5.9. Critical Security Parameter Protection			
6	9.5.11. Degraded mode(s) of operation prohibited			
7	9.5.12. Control output inhibition			
8	9.5.13. Maintenance role/interface prohibited			
9	9.5.14. Self-initiated cryptographic output capability			
10	9.5.15. Self-initiated cryptographic output capability			
11	9.5.16. Periodic self-tests			
12	10.4.1. Theater System Reliability			
13	10.4.2. Theater System Storage Security			
14	10.4.3. Security Devices Self-Test Capabilities			
15	10.4.4. Security Entity Physical Protection			
16	10.4.5. Secure SMS-SM Communication			
17	10.4.6. Location of Security Manager			
18	10.4.9. Playback Preparation			
19	10.4.11. Prevention of Keying of Compromised SPBs			
20	10.4.16. KDM Purge upon Expiry			
21	10.4.17. Key Usage Time Window			
22	10.4.22. Clock Date-Time-Range			
23	10.4.23. Clock Setup			
24	10.4.24. Clock Stability			
25	10.4.25. Repair and Renewal of SPBs			
26	10.4.27. Clock Continuity			
27	10.4.28. TLS Endpoints			
28	10.4.32. RRP Synchronism			
29	10.4.33. TLS Mode Bypass Prohibition			
30	10.4.35. Implementation of Proprietary ITMs			
31	10.4.39. RRP "Busy" and Unsupported Types			
32	10.4.40. RRP Operational Messages			
33	10.4.42. FM Algorithm General Requirements			
34	10.4.43. FM Insertion Requirements			
35	10.4.48. FM Control Instance			
36	10.4.51. SPB Log Storage Requirements			
37	10.4.53. MB Log Storage Capabilities			
38	10.4.55. Logging of Failed Procedures			
39	10.4.56. SPB Log Failure			

20.4. 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	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 SPB Certificates			
6	6.1.20. Validity of SPB 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	8.2.13. Content Keys and TDL check (OBAE)			

Chapter 21. Integrated IMBO Consolidated Test Sequence

21.1. Overview

The test sequence defined in this chapter is intended to be used to test 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. Integrated 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	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	5.4.1.9. CPLStart Event (OBAE)			
21	5.4.1.10. CPLEnd Event (OBAE)			
22	5.4.1.11. PlayoutComplete Event (OBAE)			
23	5.4.1.12. CPLCheck Event (OBAE)			
24	5.4.2.6. SPBStartup and SPBShutdown Events			
25	5.4.2.7. SPBOpen and SPBClose Events			
26	5.4.2.8. SPBClockAdjust Event			
27	5.4.2.9. SPBMarriage and SPBDivorce Events			
28	5.4.2.10. SPBSoftware Event			
29	5.4.2.11. SPBSecurityAlert Event	(data only)		
30	6.1.1. Image Integrity Checking			
31	6.1.2. Sound Integrity Checking			
32	6.1.4. Restriction of Keying to MD Type			
33	6.1.5. Restriction of Keying to Valid CPLs			
34	6.1.8. Content Key Extension, End of Engagement			
35	6.1.9. ContentAuthenticator Element Check			
36	6.1.10. KDM Date Check			
37	6.1.11. KDM TDL Check			
38	6.1.12. Maximum Number of DCP Keys			

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	5.4.1.9. CPLStart Event (OBAE)			
21	5.4.1.10. CPLEnd Event (OBAE)			
22	5.4.1.11. PlayoutComplete Event (OBAE)			
23	5.4.1.12. CPLCheck Event (OBAE)			
24	5.4.2.6. SPBStartup and SPBShutdown Events			
25	5.4.2.7. SPBOpen and SPBClose Events			
26	5.4.2.8. SPBClockAdjust Event			
27	5.4.2.9. SPBMarriage and SPBDivorce Events			
28	5.4.2.10. SPBSoftware Event			
29	5.4.2.11. SPBSecurityAlert Event	(data only)		
30	6.1.1. Image Integrity Checking			
31	6.1.2. Sound Integrity Checking			
32	6.1.4. Restriction of Keying to MD Type			
33	6.1.5. Restriction of Keying to Valid CPLs			
34	6.1.8. Content Key Extension, End of Engagement			
35	6.1.9. ContentAuthenticator Element Check			
36	6.1.10. KDM Date Check			
37	6.1.11. KDM TDL Check			
38	6.1.12. Maximum Number of DCP Keys			
39	6.1.13. CPL Id Check			