DCI Digital Cinema Initiatives, LLC

REVISION TO DCI *DIGITAL CINEMA SYSTEM SPECIFICATION*

COMPLIANCE TEST PLAN, VERSION 1.2.1

Special Note: DCI recognizes and acknowledges the serious hardships faced by the cinema industry due to the COVID pandemic. During this time DCI is not specifying new requirements unless truly necessary. In the case of the U.S. government's migration from FIPS 140-2 to FIPS 140-3, revisions to the CTP are needed so that manufacturers can continue to design and implement new media blocks that will meet DCI's and the industry's security needs. The FIPS-related revisions given below are deliberately aimed to be minimally impactful to the manufacturing process under FIPS 140-3.

CTP Revision items continue to be evaluated and will be posted after agreement by the DCI membership that the specific CTP Revision needs to modify the DCI Digital Cinema System Specification, Compliance Test Plan, Version 1.2.1. Suggested CTP Revision issues may be emailed to dci.info@dcimovies.com. Please include "CTP Revision" in the subject line.

DCI DCSS CTP v1.2.1 REVISION 24 MARCH 2021

Revision Date	Revision Stage Type	CTP v1.2 Page No.	Sections Affected	Problem Description	Revision Description
24 March 2021	1	347	Chapter 9	Chapter 9 requirements need to be revised to include FIPS 140-3 compliance. Unless otherwise noted as a "FIPS 140-3 only test," the changes described herein are cosmetic, in that they expand the scope of existing FIPS 140-2 tests to include FIPS 140-3 for Type 1 SPB compliance.	Revisions to the CTP generally, and to Chapter 9 and subsequent sections are described below, in numerical sequence.

1. Unless otherwise indicated herein, all references to "FIPS 140-2" throughout the CTP are changed to "FIPS 140." This shall be understood to refer generically to either/both FIPS 140-2 or FIPS 140-3 as applicable (and not to the original FIPS 140 standard, withdrawn in June 1997).

Chapter 9 Revisions:

2. The opening paragraph of CTP Chapter 9 is replaced with the following:

   Type 1 Secure Processing Blocks (SPB) are required by DCI to conform to a U.S. National Institute of Standards and Technology (NIST) FIPS 140 version in effect at the time of DCI compliance testing. Testing for compliance with FIPS 140 is performed by independent laboratories accredited by NIST NVLAP.

3. A new Chapter 9 second paragraph is added as follows:

   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 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.

4. In Section 9.1, the following sentence under “Security Element Documentation” is deleted:

   A checklist summarizing the documentation requirements of the standard is found in FIPS PUB 140-2 Appendix A.

5. In Section 9.1, the following sentence under “Operational Testing” is deleted:

   For FIPS 140-2 Level 3, a minimum of five production grade samples of the cryptographic module will be physically attacked and destroyed by the CMT lab during the validation testing process.

6. The opening paragraph of Section 9.2 is replaced with the following (delete second sentence):

   The CMT laboratory will review and analyze design materials during the validation testing process. The following list shows the documents generally expected to be submitted.

7. Section 9.3 is replaced in its entirety with:

   A FIPS 140 validation test report is created by CMT laboratory engineers for submission to CMVP. The report details the documentation received and the test engineer's evaluation of the implementation's fidelity to the documentation and FIPS 140 requirements. The module tested receives a FIPS 140 validation certificate (i.e., either FIPS 140-2 or FIPS 140-3) once the CMVP reviews and approves the test report.

8. Section 9.5 changes

The following Section 9.5 tests have been revised to validate compliance to either FIPS 140-2 or FIPS 140-3, as applicable for the device under test (“deleted” tests are not listed). Per item #1 above (with the exception of the “FIPS 140-2” appearances in the “Reference Document ID” tables), all references to FIPS 140-2 in the text of the tests of Section 9.5 have been changed to “FIPS 140.” Additionally, “[FIPS-140-3]” has been added to all FIPS references in the “Reference Document ID” tables.

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 Document ID Reference Document Section(s)
[DCI-DCSS] , 9.5.2.5, 9.5.2.7
[FIPS-140-2], [FIPS-140-3]

9.5.2. LE Key Generation

Verify the following:

1. That, for a Test Subject implementing a Link Encryptor (LE), the Test Subject supports keying of the Link Encryptor (LE) by generating unpredictable keys and having a controlled usage validity period.

2. That, for a Test Subject implementing a Link Encryptor (LE) or Link Decryptor (LD) SE,

a. Link Encryptor (LE) keys are 112 bits in length for TDES or 128 bits in length for AES, and that those keys are generated according to the requirements of the [DCI-DCSS], Sections 9.7.6 and 9.5.2.5.

b. Link Encryption is implemented according to [SMPTE-rdd-20]

c. Link Encryption keys are distributed using the appropriate Standardized Security Messages of [DCI-DCSS], Section 9.4.5.2.4 and, specifically, not distributed using in-band techniques.

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.4.3.5, 9.4.4, 9.5.2.5, 9.7.6
[FIPS-140-2], [FIPS-140-3]
[SMPTE-rdd-20]

9.5.3. SPB Type 1 Tamper Responsiveness

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 Document ID Reference Document Section(s)
[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]

9.5.4. Security Design Description Requirements

Verify that equipment suppliers define and describe their respective security designs surrounding the use of port 1173 per the requirements of [FIPS-140] "Cryptographic Module (Ports and) Interfaces" and the [DCI-DCSS], Section 9.5.2.5 and its subsections.

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.4.5.2.3, 9.5.2.5
[FIPS-140-2], [FIPS-140-3]

9.5.6. SPB Type 1 FIPS Requirements

Verify the following: The device meets and is validated for the requirements of [FIPS-140] Level 3 in all areas except those subject to the exceptions or additional notes as specified in the [DCI-DCSS], Section 9.5.2.5 and its subsections.

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5
[FIPS-140-2], [FIPS-140-3]

9.5.8. Asymmetric Key Generation

Verify that keys are generated as specified in [RFC-3447] and per the requirements of [FIPS-140] and Section 9.5.2.5 and its subsections.

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5, 9.7.6
[RFC-3447]
[FIPS-140-2], [FIPS-140-3]

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 [FIPS-140] and the requirements of [DCI-DCSS], Section 9.5.2.5 and its subsections:

1. Device Private Keys - RSA private key that devices use to prove their identity and facilitate secure Transport Layer Security (TLS) communications.

2. Content Encryption Keys - Key Delivery Message (KDM) AES keys that protect content.

3. Content Integrity Keys - HMAC-SHA-1 keys that protect the integrity of compressed content (integrity pack check parameters).

4. This step has been deleted.

5. Link Encryption Keys - Keys that protect the privacy and integrity of uncompressed content for link encryption.

6. TLS secrets - These are transient keys/parameters used or generated in support of TLS and Auditorium Security Messaging (ASM).

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5, 9.5.2.6
[FIPS-140-2], [FIPS-140-3]

The following tests are applicable only to Type 1 SPBs certified for FIPS 140-3:

9.5.11 Degraded mode(s) of operation prohibited

Verify that degraded mode(s) of operation, as defined in [FIPS 140-3], are not implemented.

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5.1
[FIPS-140-3]

9.5.12 Control output inhibition

Verify that the SPB Type 1 inhibits its control output interface during each error state, as defined in [FIPS 140-3].

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5.1
[FIPS-140-3]

9.5.13 Maintenance role/interface prohibited

Verify that a maintenance role/interface, as defined in [FIPS 140-3], is not implemented.

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5.1
[FIPS-140-3]

9.5.14 Self-initiated cryptographic output capability

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], Section 9.4.2.5.

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5, 9.4.2.5
[FIPS-140-3]

9.5.15 Physical security

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 Type 1 at nominal temperature(s) verified the strength and hardness of SPB Type 1 physical security enclosure material(s).

Reference Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5.1
[FIPS-140-3]

9.5.16 Periodic self-tests

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 Document ID Reference Document Section(s)
[DCI-DCSS] 9.5.2.5.1
[FIPS-140-3]

End of Chapter 9 Revisions

9. The text of Section 10.4.72 is replaced with the following, expanding scope to include FIPS 140-3:

Verify that the SPB's Secure Silicon device meets FIPS 140 "level 3" Physical Security area requirements as defined for FIPS 140-2 or FIPS 140-3 "single-chip cryptographic modules." Failure of this verification is cause to fail this test.

10. The following document is added to Appendix F "Reference Documents," below the [FIPS 140-2] listing (the FIPS 140-2 listing remains as is, and is not changed to "FIPS 140"):

[FIPS-140-3] FIPS Pub 140-3 – "Security Requirements for Cryptographic Modules," March 22, 2019

Revision Date	Revision Stage Type	CTP v1.2 Page No.	Sections Affected	Problem Description	Revision Description
24 March 2021	1	381	11.1	Clarify that compliant certificated devices that are not a targeted Device Under Test needn't undergo re-testing as part of a given consolidated test procedure.	Replace the third paragraph of Section 11.1 as indicated below.

Current Section 11.1 Third Paragraph Text:

Each certificated device must be singularly compliant to be listed in line 9, by passing all applicable consolidated test requirements as part of the current procedure. The Test Subject shall not indicate a line 11 "pass" unless all designated certificated devices are compliant.

Revised Section 11.1 Third Paragraph Text:

Each certificated device must be singularly compliant to be listed in line 9, either by passing all applicable consolidated test requirements as part of the current procedure, or as part of a previous CTP report, or as enabled by a family grouping or confidence retest. The Test Subject shall not indicate a line 11 "pass" unless all designated certificated devices are compliant.