DCI Digital Cinema Initiatives, LLC

ERRATA TO DCI *DIGITAL CINEMA SYSTEM SPECIFICATION, VERSION 1.4*

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 DCSS 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 errata given below are deliberately aimed to be minimally impactful to the manufacturing process under FIPS 140-3.

Errata items continue to be evaluated and will be posted after agreement by the DCI membership that the specific erratum needs to modify the DCI *Digital Cinema System Specification, Version 1.4, dated 20 July 2020*. Suggested Erratum issues may be emailed to dci.info@dcimovies.com. Please include "Errata" in the subject line.

DCI SPECIFICATION ERRATA LISTING 18 NOVEMBER 2020

Erratum Number	Spec. 1.4 Page No.	Section(s) Affected	Description
3	84	9.1	The following paragraph is added to the end of section 9.1: This specification originally referenced only Federal Information Standards Publication (FIPS) 140-2 "Security Requirements for Cryptographic Modules." As NIST has now released FIPS 140-3, this specification now references both standards. Except as expressly stated in Section 9.5.2.5 FIPS 140 Requirements for Type 1 Secure Processing Blocks, all appearances of "FIPS 140-2" are replaced with "FIPS 140."
4	95	9.4.2.4	The third paragraph of this section is deleted as redundant.
5	135	9.4.6.3.9	The title and text of this section is obsolete and is deleted and replaced with: [This Item Left Blank Intentionally]
6	139	9.5.2.2	Item "a" of the first bullet of this section is replaced with: *a. Secure Silicon integrated circuits used for Digital Cinema security applications shall meet FIPS 140-2 or 140-3 level 3 "Physical Security" area requirements as defined for "single-chip cryptographic modules". (No other FIPS area requirements are mandated.)*
7	143-146	9.5.2.5	Section 9.5.2.5 title and text is deleted and replaced with the following:

Erratum Number	Spec. 1.4 Page No.	Section(s) Affected	Description
9.5.2.5 FIPS 140 Requirements for Type 1 Secure Processing Blocks *Robustness requirements for type 1 Digital Cinema Secure Processing Blocks (SPBs) shall meet the requirements of Federal Information Processing Standards 140 (FIPS 140), which specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunications systems.*[18] There have been several iterations of FIPS 140, referred to as FIPS 140-1, FIPS 140-2 and FIPS 140-3 respectively. *To become FIPS certified, type 1 SPB cryptographic modules shall be evaluated by a FIPS accredited laboratory against a then-active FIPS 140 version.* Once an SPB has received FIPS 140 certification, this specification considers its certificate valid for subsequent production of that model, independently of whether or not FIPS 140 certification processes have changed. However, FIPS guidelines mandate that design changes made to an SPB may require recertification of the device. *In such event the then-active FIPS 140 certification requirements shall be used in obtaining a valid FIPS certificate to meet the requirements of this specification.* Suppliers are advised that a FIPS certified cryptographic module that has not been reviewed by an accredited FIPS laboratory within five years of its certification date will be automatically moved from the FIPS 140 "active" module status list to the "historical" list until such time as it is reviewed. Though a historical listing does not impact a module's status with respect to its approval for Digital Cinema applications, suppliers are encouraged to maintain their SPB type 1 devices on the FIPS 140 active list. General FIPS 140 requirements: • *Type 1 SPBs shall be FIPS 140 certified to a security "Level 3," subject to the additional requirements or exceptions as noted for FIPS 140-3 and FIPS 140-2 in Sections 9.5.2.5.1 and 9.5.2.5.2 below.* • *Type 1 SPBs shall provide physical and logical protection of their security parameters and functions 24/7 and shall be able to respond to attacks under both powered and un-powered conditions. By way of example, if a type 1 SPB is in storage and relying upon a battery for tamper detection and response, it shall zeroize its Critical Security Parameters (CSPs) prior to a battery depletion condition which would not support proper tamper detection and/or response.* • *Type 1 SPB suppliers shall at all times ensure that their published FIPS Security Policy document(s) accurately reflect the current state of the SPB design and functionality.*[19]			
8	143	9.5.2.5	Placed at the end of the first sentence of this section, the text of Footnote 18 is replaced with: See https://csrc.nist.gov/publications/
9	145	9.5.2.5	Footnote 19 is moved to the end of this section and the text replaced with: [This Footnote Left Blank Intentionally]

Erratum Number	Spec. 1.4 Page No.	Section(s) Affected	Description
10	146	9.5.2.5.1	The following new section is added after Section 9.5.2.5: **9.5.2.5.1 SPBs Meeting FIPS 140-3 Requirements** *Specific requirements for type 1 SPBs certified to FIPS 140-3 are provided in Table 20.* Table 20 references "areas" related to the design and implementation of a cryptographic module as specified in FIPS 140-3 and ISO/IEC 19790:2012(E) "Information technology – Security techniques – Security requirements for cryptographic modules," and references "sections" found therein. [Table 20 is located below at the end of this errata list.]
11	146	9.5.2.5.2	The following new section is added after Section 9.5.2.5.1 **9.5.2.5.2 SPBs Meeting FIPS 140-2 Requirements** *Type 1 SPBs certified to FIPS 140-2 shall meet the requirements of FIPS 140-2 Level 3 in all areas, subject to the following exceptions or additional notes:* • *Area 1 – Cryptographic Module Specification shall only be required to meet Security Level 2 requirements.* • *Area 2 – Logical data port separation requirements shall be supported by the use of Transport Layer Security (TLS) protection on well-known port 1173 as defined in Section 9.4.5.2.3 General RRP Requirements.* • *Area 6 – The software/firmware operating environment of Secure Processing Blocks (SPBs) shall be restricted to the Limited or Non-Modifiable Operational Environment.* • *Area 8 – Secure Processing Blocks (SPBs) shall only be required to meet Security Level 2 business use A FCC class requirements.* • Area 10 – Design Assurance requirements may meet Security Level 2 requirements. • *Area 1 and Area 11 – Vendor-specified Security Policy specifications shall be in alignment with and fully support the requirements of this Digital Cinema specification, in addition to vendor-specific policies.*
12	146	9.5.2.7	The first paragraph of this section is replaced with: In addition to the "limited" or "non-modifiable" Operational Environment requirements of FIPS 140, the following defines additional requirements for making software or firmware changes to type 1 Secure Processing Blocks (SPB):[20]

Erratum Number	Spec. 1.4 Page No.	Section(s) Affected	Description
13	146	9.5.2.7	Footnote 20 is moved to the end of the first paragraph of this section, and the text replaced with: *The terms software or firmware shall mean all operating system and/or embedded executable code within an SPB, and this specification does not otherwise distinguish between software, firmware or ROM based code.*
14	147	9.5.2.7	The 4th and 5th bulleted items of this section are deleted and replaced with the following bulleted item: • *Log the firmware change event per the requirements of Section 9.4.6.3.8 Log Record Information.*
15	152	9.7.6	"or FIPS 140-2 IG 7.8" is deleted from the first sentence of this section.

Area	140-3 Section	DCI requirements are per FIPS 140-3 Level 3 unless otherwise noted, inclusive of the following specific requirements:
Cryptographic module specification	7.2.3 7.2.4.3	*The "cryptographic boundary" shall be the SPB-1 physical perimeter.* *Degraded mode(s) of operation shall not be permitted.*
Cryptographic module interfaces	7.3.3 7.3.4	*An SPB-1 shall inhibit its control output interface during each error state.* *Trusted Channel interface requirements of this specification shall be supported by the use of Transport Layer Security (TLS) protection per Section 9.4.5.1 "Transport Layer Security Sessions, End Points and Intra-Theater Messaging."* *Logical data port separation requirements shall be supported by the use of TLS protection on well-known port 1173 as defined in Section 9.4.5.2.3 General RRP Requirements.*
Roles, services and authentication	7.4.2 7.4.3.3	*A Maintenance Role shall not be permitted.* *An SPB-1 shall not support "self-initiated cryptographic output capability" (a User Role and/or Crypto Officer Role shall be required to support the AuthorityID per Section 9.4.2.5 "Screen Management System").*
Software / Firmware	7.5	No DCI specific requirements.
Operational environment	7.6.1	*The operational environment shall be constrained to the limited or non-modifiable operational environment.*
Physical security	7.7.1 7.7.2	EFP/EFT requirements are recommended but not required. *The strength and hardness of SPB-1 physical security enclosure material(s) over the SPB-1's range of operation, storage, and distribution shall be verified by review of design documentation. Additionally, destructive physical attacks shall be performed on SPB-1 at nominal temperature(s) to verify the strength and hardness of SPB-1 physical security enclosure material(s).* Destructive physical attacks on SPB-1 at additional temperatures is recommended but not required. EFP/EFT requirements: See 7.7.1.
Non-invasive security	7.8	No DCI specific requirements.
SSP management	7.9	No DCI specific requirements.
Self-tests	7.10.3.8	*The specified Security Policy maximum time between periodic self-tests shall not be more than one week.* SPB-1 designs should ensure that automatic periodic self-tests do not occur during playback of a DCP.
Life-cycle assurance	7.11.8	End of life procedures for the secure destruction of SPB-1 are deferred to the equipment owner and/or equipment manufacturer.
Mitigation of other attacks	7.12	No DCI specific requirements.

Table 20: FIPS 140-3 Area Requirements