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 24 MARCH 2021

Erratum Number	Spec. 1.4 Page No.	Section(s) Affected	Description
18	106	9.4.3.5	The following is added to item #5: *c. OBAE – Process integrity pack information, including the hash (HMAC).*
19	146	9.5.2.5.1	The Table 20 in Erratum 10 dated 18 November 2020 is deleted and replaced with the following Table 20, revising entries for section 7.4.3.3 and 7.7.2. (The previous table inadvertently increased some DCI security requirements so it is now revised to maintain existing practices.)

Area	ISO 19790 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	*The "cryptographic boundary" shall be the SPB-1 physical perimeter.*
	7.2.4.3	*Degraded mode(s) of operation shall not be permitted.*
Cryptographic module interfaces	7.3.3	*An SPB-1 shall inhibit its control output interface during each error state.*
	7.3.4	*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	*A Maintenance Role shall not be permitted.*
	7.4.3.3	*An SPB-1 may support "self-initiated cryptographic output capability" provided that 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	Environmental Failure Protection (EFP) and Environmental Failure Testing (EFT) requirements are recommended but not required.
	7.7.2	*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. If tamper-evident seals are employed, it is recommended but not required that they be uniquely numbered or independently identifiable. EFP/EFT requirements are recommended but not required.
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