DCI Digital Cinema Initiatives, LLC

ERRATA TO DCI DIGITAL CINEMA SYSTEM SPECIFICATION, VERSION 1.2

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 1.2. Suggested erratum issues may be emailed to dci.info@dcimovies.com. Please include "Errata" in the subject line.

DCI SPECIFICATION ERRATA LISTING — 30 AUGUST 2012

Erratum Number	Spec 1.2 Page	Section(s) Affected	Description
90	134-135	Section 9.5.1	In Erratum 70, the second paragraph of Section 9.5.1.1 is amended to read as follows: *The identity of a device shall be represented by its certificate. The make and model of each certificated device shall be carried in the assigned certificate, and the serial number and device role(s) (see below) shall in particular be carried in the Common Name (CN) field of the assigned certificate. The make, model and serial number of each certificated device shall be placed on the exterior of said device in a manner that is easily read by a human.*
91	17	Section 1.3	Second sentence in the second to the last paragraph is replaced with: *The most recent editions of the referenced standards shall be valid unless otherwise exempted in this specification."*
92	117	Section 9.4.3.6.6	The following is added at the end of this section: Note: For permanently married implementations where there are no remote SPBs the KDM need not carry Trusted Device List (TDL) information. The KDM syntax requirement that the associated "DeviceList" element not be empty can be satisfied by placing any Digital Cinema certificate thumbprint in this field.

Erratum Number	Spec 1.2 Page	Section(s) Affected	Description
93	119	Section 9.4.4.1	Errata 87 is redacted and replaced with: The title of this section is changed to "Special Auditorium Situations", and the entire section is replaced with: “Special Auditorium Situations” are defined to allow the Image Media Block (IMB) to operate with more than a single projector. *Special Auditorium Situations shall be enabled by the following methods:* • *IMB with Multiple Link Encryption means the use of (i) more than one remote LDB/projector pair with a single IMB, or (ii) an LD/LE image processor SPB inserted between the IMB and one or more remote LDB/projector pair(s).* • *Integrated IMB with Link Encryption means the use of an integrated and married IMB/projector pair, where the IMB also outputs a Link Encrypted image signal to one or more remote LDB/projector pair(s). The IMB shall simultaneously meet all requirements for both integrated and non-integrated projector system implementations.* *SMs shall enable Special Auditorium Situations to operate only when the SM receives a KDM whose Trusted Device List (TDL) contains only the identities of the SPBs it is enabling for playback. For IMB with Multiple Link Encryption operation these shall be the remote SPBs identified during TLS authentication (see details below). For Integrated IMB with Link Encryption this additionally includes the identity of the projector to which the IMB is married.* This matching is an indication to the SM that Special Auditorium Situations operation has been approved by the content owner. *IMB with Multiple Link Encryption operation or Integrated IMB with Link Encryption operation shall follow all normal (single) Link Encryption requirements of this section, with the following additional requirements:* *a. SM behavior shall be designed to identify a Special Auditorium Situation during the auditorium security network TLS session establishment. The digital certificate exchange with remote SPBs shall return the associated certificate roles for each SPB in the auditorium.* *b. The SM shall independently authenticate each remote SPB against the TDL using a dedicated TLS session.* *c. The SM shall independently key each remote SPB for Link Encryption operation using standardized Intra-Theater (security) Messaging per Section 9.4.5.* *d. The SM shall not support the use of more than one LD/LE image processor SPB for any given projector.* *e.* The Link Encryption stages of the LD/LE image processor configuration may use the same LE key(s). Similarly, the SM may key the multiple LDB/projector configuration using the same LE key for each LDB/projector system.

Erratum Number	Spec 1.2 Page	Section(s) Affected	Description
94	134	Section 9.5.1.2	The following paragraph is added at the end of (new) section 9.5.1.2 "Dual Certificate Implementations": In addition to the above, dual certificate implementations require Digital Cinema certificate validation rules that may not be reflected in the current SMPTE digital cinema specification (see DCSS Section 9.8, SMPTE430-2: "D-Cinema Operations – Digital Certificate"). The affected validation rule is driven by the "Key Usage" constraints as given in Table 2 of SMPTE430-2 ("Field Constraints for Digital Cinema Certificates"), which is then reflected in validation rule # 6 of section 6.2 "Validation Rules". *For dual certificate implementations validation rule # 6 shall be as stated in SMPTE430-2 for single certificate implementations, except as follows:* • *SM Cert – The DigitalSignature flag shall not be set.* • *LS Cert – The KeyEncipherment flag shall not be set.*
95	135	Section 9.5.2.2	The last sentence of the opening paragraph of this section is replaced with: *CSPs and plain text content essence shall be physically protected by Secure Silicon and/or Secure Processing Blocks as described below:*
96	136	Section 9.5.2.2	The "Secure Silicon" bullet is replaced with: • **Secure Silicon** – Sensitive data contained within a Secure Silicon integrated circuit (IC) can only be compromised by a physical attack on the IC. *All type 1 and type 2 Secure Processing Blocks (SPB) shall contain a Secure Silicon IC compliant to the following requirements:* ***a**. Secure Silicon integrated circuits used for Digital Cinema security applications shall meet FIPS 140-2 level 3 area five (physical security) requirements as defined for "single-chip cryptographic modules" (no other FIPS 140-2 area requirements are mandated).* ***b**. Other than as part of the manufacturing process, SPB private keys used for device identity (see section 9.5.1 "Digital Certificates") shall not exist outside of the Secure Silicon IC. For purposes of clarity, this means that (1) private keys (whether encrypted or not) shall not be moved or copied from Secure Silicon, and (2) the CipherValue element(s) of the KDM's AuthenticatedPrivate element shall be decrypted by and within the Secure Silicon IC.* ***c.** Decrypted (plain text) content image keys may be moved from the Secure Silicon IC for purposes of decrypting image essence during playout only. They shall at all other times be contained within the Secure Silicon IC, or be stored off-chip in an encrypted fashion per the requirements of section 9.7.4 "Protection of Content Keys"*