DCI Digital Cinema Initiatives, LLC

ERRATA TO DCI DIGITAL CINEMA SYSTEM SPECIFICATION, VERSION 1.1

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

DCI SPECIFICATION ERRATA LISTING 27 AUGUST 2007

Erratum Number	Spec 1.1 Page	Section(s) Affected	Description
1	29	Section 5.2.3	The fifth sentence of the paragraph below Figure 5 (i.e., the first italicized sentence) is deleted and replaced with the following text: *For encrypted essence, the Composition Playlist shall be digitally signed such that modifications to the Composition Playlist (and/or the associated composition) can be detected.*
2	35	Section 5.3.3.1	The second sentence is deleted and replaced with the following non-italicized text: Each Image Track File contains compressed image data and, optionally, may be encrypted.
3	37	Section 5.4.1	The third sentence of this section is deleted and replaced with the following text: *For encrypted essence, the Composition Playlist shall be digitally signed such that modifications to the Composition Playlist (and/or the associated composition) can be detected.*
4	39	Section 5.4.4	The existing text of this section, including the section title, is deleted in its entirety and replaced with the following text: **5.4.4. Security of the CPL** *For encrypted essence, the Composition Playlist shall be digitally signed such that modifications to the Composition Playlist (and/or the associated composition) can be detected. In support of this, the CPL assets "KeyID" and "Hash" elements shall be present in the CPL track file asset structure.*
5	39	Section 5.5.2.3	The following sentence is added after the first sentence of this section: *In particular, where the DCP contains encrypted essence files, the Packing List shall be digitally signed.*
6	39	Section 5.5.2.3	The last sentence of this section is deleted and replaced with the following text: *Content authenticity is verified through signed Composition Playlists and validated Key Delivery Messages.*
7	54	Section 7.5.4.1	The sentence immediately below Figure 13 (beginning "If both Image Media Block…") is deleted.

Erratum Number	Spec 1.1 Page	Section(s) Affected	Description
8	54	Section 7.5.4.2.2	The first two paragraphs of this section are deleted and replaced with the following text: The main function of the Media Block is to provide a secure environment within which to perform content essence decryption. *In support of this, the Media Block shall contain the Security Manager, image, audio and subtitle processing and the associated forensic markers. Link Encryption shall be applied to image essence if the Media Block is not contained within the projection system.*
9	56	Section 7.5.4.3	In the bulleted item entitled Security Messaging, the first sentence is deleted and replaced with the following text: *The Media Block is required to communicate standardized security messages (see Section 9.4.5. Intra-Theater Communications) via a standard 100Base-T Ethernet [IEEE 802.3] interface to the projector and remote Secure Processing Blocks*.
10	56	Section 7.5.5.1	In the third and fifth sentences of the first paragraph, the word “Image” is deleted from the phrases “Image Media Block”.
11	70	Section 8.4.2	The word “Image” is deleted from the title of this section.
12	70	Section 8.4.2	In the first, second and fourth sentences of the first paragraph, the word “Image” is deleted from the phrases “Image Media Block”.
13	71	Section 8.4.3.1	In the last sentence of this section, the word “Image” is deleted from the phrase “Image Media Block”.
14	77	Section 9.3.1	In the definition of Intra-Theater Message (ITM), the term “SEs” is deleted and replaced with the words “security devices”.
15	78	Section 9.3.3	In the last sentence of the first paragraph, the parenthesized phrase “(Security Entities)” is deleted.
16	79	Section 9.3.3.1	The last sentence in the paragraph just above Figure 15 (beginning “Security Entities (SE) are filled with…”) is deleted.
17	81	Section 9.4.1	The existing text of Item 3 is deleted and replaced with the following text: *Every IMB shall include image, audio and subtitle decryption capability.*
18	81	Section 9.4.1	The existing text of Item 4 is deleted and replaced with the following text: *Every IMB shall include image and audio Forensic Marking (FM) capability*.
19	81	Section 9.4.1	The existing text of Item 6 is deleted and replaced with the following text: *Image Media Blocks and Link Decryptor Blocks shall be of the SPB type 1 (see Section 9.4.2.2. The Secure Processing Block (SPB)), and shall be field replaceable, but non-field serviceable.*
20	81	Section 9.4.1	The last three sentences of this section are deleted.
21	82	Section 9.4.1.1	In the second bulleted item at the top of page 82, the word “All” is replaced with the word “Image”.
22	84	Section 9.4.2.2	The second sentence of the first bullet is deleted and replaced with the following text: *Image Media Blocks and Link Decryptor Blocks shall be contained within a type 1 SPB.*

Erratum Number	Spec 1.1 Page	Section(s) Affected	Description
23	85	Section 9.4.2.3	In the first bulleted item (Image Media Block), the first sentence is deleted and replaced with the following text: *The Image Media Block (IMB) is a type of Secure Processing Block (SPB) that shall contain a Security Manager (SM), Image, Audio and Subtitle Media Decryptors (MD), image decoder, Image and Audio Forensic Marking (FM) and optionally Link Encryptor (LE) functions.*
24	85	Section 9.4.2.3	In the second bulleted item (Remote Media Block), the last sentence is deleted and replaced with the following text: *Remote Media Blocks shall not be used in DCI compliant systems.*
25	91	Section 9.4.3.3	In the first bulleted item (Equipment suite preparations), the last sentence of the first paragraph is deleted.
26	94	Section 9.4.3.5	In the second sentence of Item 1, the word "*issuance*" is deleted and replaced with the word "*use*".
27	94	Section 9.4.3.5	In the second sentence of Item 5, the parenthetical phrase is deleted and replaced with the following text: *(including restarts)*
28	95	Section 9.4.3.5	The first two preamble sentences of Item 9 are deleted and replaced with the following text: *Prepare and issue content keys to Media Decryptor (MD) and Forensic Marking (FM) SEs as may require keying per the CPL. Constrain use of keys to:*
29	95	Section 9.4.3.5	The existing text of Item 9.a is deleted and replaced with the following text: *Confirmation (via QuerySPB command) that TLS connections are operative with remote SPBs, and that the QuerySPB Response "general response" element indicator is "0" (RRP successful).*
30	95	Section 9.4.3.5	The existing text of Item 9.d is deleted and replaced with the following text: *Media Decryptors (e.g., image, sound, subtitle, link encryption) in SPBs that meet status requirements of item 14 below.*
31	95	Section 9.4.3.5	The existing text of Item 11 is deleted and replaced with the following text: *Perform suite playback preparations per items 9 and 10 above for each showing, within 30 minutes prior to show time. Though item 9 above establishes key validity periods of six hours, security equipment integrity checks and suite re-keying shall be executed within 30 minutes prior to each show time.*

Erratum Number	Spec 1.1 Page	Section(s) Affected	Description
32	96	Section 9.4.3.5	The existing text of Item 15 is deleted and replaced with the following text: *During all normal operating conditions (including during playback), continuously monitor and log integrity status of remote SPBs so as to preclude delivery of keys/content to, or playback on, compromised or improperly operating security equipment. To support this requirement the QuerySPB command (see Section 9.4.5. Intra-Theater Communications) shall be issued to each remote SPB at least every 30 seconds whenever TLS sessions are open. Receipt of a QuerySPB response indicating a "security alert" condition shall be indicative of a faulty SPB, and shall prevent or terminate playback per the DRM requirements of Section 9.6.1. Digital Rights Management. Once a show has started, failure of a TLS link shall not cause termination of a show (i.e., QuerySPB commands will not successfully execute, but the show should continue to play if possible).*
33	96	Section 9.4.3.5	The last sentence of Item 17 is deleted and replaced with the following text: *Perform the security equipment integrity checks and suite re-keying per item 11 above prior to the next playback.*
34	97	Section 9.4.3.6	The fourth bulleted item (Remote Audio Media Block SPB) is deleted.
35	99	Section 9.4.3.6.2	The existing text of Item 11 is deleted and replaced with the following text: *Monitor projector SPB marriage and operational status 24/7 and create log records and issue QuerySPB alert indicators accordingly.*
36	99	Section 9.4.3.6.3	The following sentence is added to the beginning of Item 3: *The existence of the marriage configuration (i.e., when the IMB and projector are integrated per Section 9.4.3.6.1. Normative Requirements: Projector Secure Processing Block) shall indicate to the Security Manager that link encryption is not needed.*
37	100	Section 9.4.3.6.3	The existing text of Item 4 is deleted and replaced with the following text: *Perform Media Decryption for image, audio and subtitle essence.*
38	100	Section 9.4.3.6.3	The existing text of Item 5 is deleted and replaced with the following text: *Perform Forensic Marking for image and audio essence.*
39	100	Section 9.4.3.6.3	Item 7 (near the top of the page) is deleted.
40	100	Section 9.4.3.6.4	The existing text of this section is deleted in its entirety and replaced with the following text: **9.4.3.6.4. Normative Requirements: Audio Media Block** *Per Section 9.4.2.3 Media Blocks (MBs), audio decryption shall be performed within the Image Media Block (IMB).*
41	101	Section 9.4.3.6.5	The phrase *"(e.g., extender board attack) is thwarted."* is deleted from the end of the third bulleted item and added to the end of the second bulleted item.
42	102	Section 9.4.3.7	In the third bulleted item, the text "+/- *five minutes*" is deleted and replaced with the text "+/- *six minutes*".

Erratum Number	Spec 1.1 Page	Section(s) Affected	Description
43	102	Section 9.4.4	The following sentence is added to the end of the first paragraph: *The Security Manager shall enforce link encryption operations per the requirements of this section in all applications except where the Image Media Block and the projector are married per Section 9.4.3.6.3. Normative Requirements: Image Media Block, Item 3.*
44	102	Section 9.4.4	The following sentence is added to the end of the second paragraph: *Link Encryption keys shall be delivered to the LDB using the appropriate category 2 standardized security messages of Table 15 Intra-Theater Messages Request-Response Pairs.*
45	104	Section 9.4.5.2	The third sentence (i.e., *"The following shall be normative for DCI compliance:*" and the two bulleted items that follow) is deleted.
46	105	Section 9.4.5.2.3	The existing text of Item 3 is deleted and replaced with the following text: *During normal operations, Secure Processing Blocks (SPBs) shall maintain their TLS communications sessions with the SM open and active at all times.*
47	106	Section 9.4.5.2.4	The existing text of this section, including Table 15, is deleted and replaced with the following text and a new Table 15 (given on the last page herein): **9.4.5.2.4. Request Response Pairs (RRP)** Table 15 lists "standardized security messages" (category 2) and suggested "operational messages" (category 1). *The following establishes the implementation requirements for these message types:* • **Standardized Security Messages** - *Standardized security messages shall be compliant to SMPTE 430-6-2007 D-Cinema Operations – Auditorium Security Messages, and shall consist only of messages listed as category 2 messages of Table 15. These messages are used between the Image Media Block and remote SPBs, with the IMB as the Requestor (RRP initiator). The security data and related information that is the subject of these messages shall be communicated only via standardized security messages.* • **Operational Messages** – The implementation of operational messages is not normatively specified. *However, to support log event recording (see Section 9.4.6.3. Logging Subsystem), it shall be mandatory that Security Managers functionally support Table 15 category 1 operational messages. This means that the SM must be capable of performing the function, whether via ITM command, or other control means. The functional approach shall specify an "AuthorityID", which is intended to indicate the SMS operator, per Section 9.4.2.5. Screen Management System.* The term "Auditorium Security Messages" (ASMs) in SMPTE 430-6-2007 corresponds to the term "standardized security messages" in this specification. The combination of the terms "standardized security messages" and "operational messages" are referred to in this specification as Intra-Theater Messages (ITMs).
48	107	Section 9.4.5.3	The existing paragraph of text for this section is deleted and replaced with the following sentence: This section provides particular requirements for specific messages.

Erratum Number	Spec 1.1 Page	Section(s) Affected	Description
49	107-110	Section 9.4.5.3.1	The existing text of this section, including all subsections and tables, is deleted and replaced with the following text: [This section left blank intentionally.]
50	110-112	Section 9.4.5.3.2	The existing text of this section, including all subsections and tables, is deleted and replaced with the following text: **9.4.5.3.2. Image Media Block SM to Remote SPB Messages** *Image Media Block to remote SPB messages are category 2 Intra-Theater Messages of Table 15. Standardized security messages are defined in SMPTE 430-6-2007 D-Cinema Operations – Auditorium Security Messages.* *The following requirements are in addition to those in SMPTE 430-6-2007:* • *SPB security devices shall be designed to meet the round trip latency requirements suggested in SMPTE 430-6-2007.* • *A remote SPB shall respond to the QuerySPB command (i.e., the "ResponderBusy" general response element code "3" is not permitted).* To meet this requirement, vendors are encouraged to assure that adequate message processing periods exist between this and other RRP command types. • *The following QuerySPB "security alert" conditions are defined, and shall be reported per status code "2" of this command's response:* 1. *SPB perimeter open (e.g., service access door).* 2. *Marriage broken event detected (see Section 9.4.3.6.1. Normative Requirements: Projector Secure Processing Block).* 3. *Conditions that require replacement of the SPB (i.e., equipment tampering or failure) per Section 9.6.1.3. Digital Rights Management: Security Entity (SE) Equipment.* • *The LEKeyLoad command "expire time" shall be 6 hours per Section 9.4.3.5. Functions of the Security Manager (SM), Item 9.b.*
51	114	Section 9.4.6.1	The first sentence is deleted and replaced with the following text: *These specifications require that image and audio Forensic Marking (FM) capability be included in each Image Media Block.*
52	117	Section 9.4.6.2	The existing text of Item 7 is deleted and replaced with the following text: *SM control of the Forensic Marking "no FM mark" state in remote SPBs shall be communicated via a Table 15 category 2 standardized security Intra-Theater Message (see Section 9.4.5. Intra-Theater Communications).*
53	119	Section 9.4.6.3.1	The following two sentences are added to the end of Item 14: *The accuracy of the time stamp relative to the actual event shall not exceed one (1) second. Accuracy shall mean the latency between the occurrence of the event and the indicated time stamp.*
54	125	Section 9.4.6.3.9	In the second sentence, the text "SBP" is deleted and the text "SPB" is inserted in its place.

Erratum Number	Spec 1.1 Page	Section(s) Affected	Description
55	133	Section 9.5.4	The existing text of this section is deleted and replaced with the following text: **9.5.4. Subtitle Processing** Subtitle encryption is directed primarily against interception during transport, and cryptographic protection within the theater is not required. *Thus there are no protection requirements imposed on subtitle post-decryption processes, other than its implementation shall not weaken or otherwise effect the security operations of other Security Entities or SPBs.* As an alternative to encryption of subtitle essence, the Composition Playlist (CPL) SubtitleTrackFileAssetType "Hash" element may be used to validate the integrity of received subtitle content that has not been encrypted. *The optional subtitle hash element, if used, shall be present and in the same signed CPL used for the image and audio.* This integrity check could be performed by the Security Manager, but may also be performed externally to the IMB by, for example, the SMS.

The following new Table 15 is part of Erratum 47 above:

Message Category	Function
1. SMS to SM	***Suggested operational messages***
StartSuite	Commands SM to establish TLS sessions with remote SPBs
StopSuite	Commands SM to terminate TLS sessions with remote SPBs
CPLValidate	Requests that the SM perform a CPL validation check
KDMValidate	Requests that the SM perform a KDM validation check
TimeAdj	Adjusts time at SM (within annual limits)
2. IMB SM to SPB	***Standardized security messages***
BadRequest	Special "Response" indicating failure to process a "Request"
GetTime	Requests a snapshot of a remote SPBs absolute (UTC) time
GetEventList	Requests a list of logged event IDs for a specified time window
GetEventID	Requests the return of a specified logged event by ID
QuerySPB	Interrogates a remote SPB as to health and status
LEKeyLoad	Delivers one or more LE keys to a Link Decryptor Block (LDB)
LEKeyQueryID	Interrogates the LDB for the presence of a specified LE key
LEKeyQueryAll	Requests a report of all active LE keys by key ID
LEKeyPurgeID	Commands the LDB to purge a specified LE key
LEKeyPurgeAll	Commands the LDB to purge all active LE keys

Table 15: Intra-theater Message (ITM) Request-Response Pairs (RRP)