DCI Digital Cinema Initiatives, LLC

Errata To DCI *Digital Cinema System Specification, Version 1.2 With Errata As Of 30 August 2012 Incorporated*

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 With Errata As Of 30 August 2012 Incorporated*. Suggested Erratum issues may be emailed to dci.info@dcimovies.com. Please include “Errata” in the subject line.

Note: Page numbers reference the replacement Chapter 9 of Erratum 9.

DCI Specification Errata Listing 2 March 2017

Erratum Number	Spec. 1.2 with Errata Incorporated Page No.	Section(s) Affected	Description
25	85	9.4.1	The following sentence is added to the end of item #3: *With exception of subtitle essence (see Section 9.7.3 “Subtitle Encryption”), encrypted essence files shall be decrypted in real-time during playout, and at all other times shall remain encrypted as received in the DCP.*
26	93	9.4.2.7	A new section 9.4.2.7 is added as follows: **9.4.2.7 Auxiliary Data Processing** *Aux Data (AD) shall be considered essence defined under [SMPTE ST429-14: “D-Cinema Packaging -- Aux Data File”], subject to the exceptions specified herein.* Aux Data is treated as a generic essence type. This means the specific functional requirements for AD decryption and post-decryption processing (e.g., decoding, forensic marking, etc.) must be known for a given implementation, but are out of scope of this specification except as provided for in Section 9.4.3.6.4 “Normative requirements: Outboard Media Block (OMB)”. By way of example, image essence and audio essence (sometimes referred to as main image and main audio to avoid confusion with emerging types of AD), subtitle essence and Object-Based Audio Essence (OBAE) processing requirements are expressly addressed by this specification, and are thus distinguished from generic Aux Data essence types. *Encrypted Aux Data (AD) shall be decrypted only within a Media Block (MB) using the “MDX1” AD essence KeyType delivered by a KDM.* (See [SMPTE ST430-1: “D-Cinema Operations – Key Delivery Message”].) *The MDX2 KeyType shall be reserved for future use.* Aux Data that is not encrypted is not subject to the security constraints of this specification.

Erratum Number	Spec. 1.2 with Errata Incorporated Page No.	Section(s) Affected	Description
27	99	9.4.3.5	The first sentence of item #1 is replaced with: Validate Key Delivery Messages per (a) the three validity checks of Section 6.1.2 of the KDM specification (SMPTE 430-1: D-Cinema Operations – Key Delivery Message), and (b) confirming the KDM’s CipherData element matches the contents and format of the table of said Section 6.1.2, of the KDM specification.
28	100	9.4.3.5	Item #4 is replaced in its entirety with: *4. Validate Composition Playlists (CPL), and log results as a prerequisite to the associated composition playback. For encrypted content, validation shall confirm that:* *a. The associated KDM's ContentAuthenticator element matches a certificate thumbprint of one of the certificates in the CPL's signer chain (see item 1 above), and that such certificate indicate only a “Content Signer” (CS) role per Section 5.3.4, “Naming and Roles” of the certificate specification (SMPTE 430-2 D-Cinema Operation - Digital Certificate).* *b. All the content essence keys carried in the AuthenticatedPrivate element of the associated KDM are reflected (i.e., must exactly match those listed) in the CPL.*

Erratum Number	Spec. 1.2 with Errata Incorporated Page No.	Section(s) Affected	Description
29	100	9.4.3.5	Item #6 of this section is replaced with: As of January 1, 2016, Federal Information Processing Standards (FIPS) compliance requirements disallow use of the random number generator (RNG) as specified in [SMPTE ST429-6: “D-Cinema Packaging – MXF Track File Essence Encryption”]. Additionally, a KDM key type is needed to support encryption of generic Auxiliary Data (AD) essence per [SMPTE ST429-14: “D-Cinema Packaging – Aux Data File”]. These are addressed by the following requirements for support of KDMs carrying “MIC” and “Aux Data” key types: a. *Media Block (MB) SMs shall support the receipt and processing of KDMs carrying the MIC and Aux Data (AD) key types.* (See [SMPTE ST430-1: “D-Cinema Operations – Key Delivery Message”].) b. *MB SMs shall perform the content hash (HMAC) integrity check of above item 5 using the KDM-borne MIC keys if present (and shall not derive the MIC key from KDM content keys).* c. *MB SMs capable of processing KDM-borne MIC keys shall indicate so by including “MIC” in their digital certificate roles (see role definitions of Section 9.5.1.1 “Single Certificate Implementations”).* d. *MB SMs shall not implement the Random Number Generator (RNG) defined (for the purpose of MIC key derivation) in [SMPTE ST429-6: D-Cinema Packaging – MXF Track File Essence Encryption].* e. *When receiving a KDM type that does not contain a MIC key, MB SMs shall perform all the content integrity checks specified in above item 5 except the hash (HMAC) check.*
30	106	9.4.3.6.4	Item number 1 of this section is replaced with: *Perform the following itemized SM functions as defined under Section 9.4.3.5 Functions of the Security Manager (SM): #1, #2, #3, #4, #5, #6, #9 (except for sub-items a and c), #12, #13, #14, #18.*
31	106	9.4.3.6.3	The following is added as new number 8: 8. An IMB intended for operation in Multiple Media Block (MMB) installations shall be capable of operating as either a “source” or “sink” of synchronization information per the requirements of Section 7.5.4.2.1 “Synchronization”.
32	107	9.4.3.6.4	The following is added below the existing bullet of item number 4: • *Auxiliary Data (AD) essence per [SMPTE ST429-14: D-Cinema Packaging – Aux Data Track File], subject to the constraints of Section 9.4.2.7 “Auxiliary Data Processing.”*

Erratum Number	Spec. 1.2 with Errata Incorporated Page No.	Section(s) Affected	Description
33	107	9.4.3.6.4	The following is added as new number 6: 6. Operate as a “sink” of synchronization information per the requirements of Section 7.5.4.2.1 “Synchronization”.
34	119	9.4.6.2	The following replaces the existing item #9: *9. Notwithstanding the exceptions defined in Section 9.4.6.2, all decrypted audio shall be forensically-marked. A Forensic Mark is required to be inserted in real time into the audio content at the earliest point after decryption and prior to the audio content data being present on any data bus outside the Media Block (see Section 9.4.6.1 “Forensic Marking”).*
35	127	9.5.1.1	The following is added above the existing “note” at the bottom of Erratum 13: *The following role(s) shall be included for the IMB and OMB, as applicable:* • KDM-borne MIC Key capable MB – MIC
36	131	9.5.2.5	The following paragraph is added below the last bullet of this section: This specification requires all Media Blocks (MB) to be FIPS 140-2 certified per the requirements of this section. MB suppliers shall at all times ensure that their published FIPS Security Policy document(s) accurately reflect the current state of the MB design and functionality.
37	141	9.7.4	The second sentence of this section is replaced with: “The above RSA asymmetric protection, or symmetric key wrapping per SP800-38F may be used to protect the storage of keys once decrypted from the KDM within a Media Block (e.g., where off-secure-silicon IC memory is used for key caching within a Media Decryptor)."
38	141	9.7.6	The entirety of this section is replaced with: *“Asymmetric keys (RSA keys) shall be generated as specified in FIPS 186-4. Symmetric keys shall be generated from the output of a SP800-90A DRBG as per SP800-133 or FIPS 140-2 IG 7.8.* *RSA asymmetric keys shall be 2048 bits in length and be generated from two or three prime numbers, each of which must be at least 680 bits long. The mechanism used to generate RSA key pairs must have at least 128 bits of entropy. A vendor shall keep records of only the public keys, and shall not keep any record of the matching private keys.* *See Section 9.5.1 “Digital Certificates” for additional requirements for the generation, storage and utility of keys.”*