# DCI Digital Cinema Initiatives, LLC

Errata items are continuing 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, v1.0. Suggested erratum issues may be emailed to dci.info@dcimovies.com. Please include "Errata" in the subject line.

## DCI SPECIFICATION ERRATA LISTING — 21 MARCH 2007

| Erratum | Spec 1.0 Page | Sections Affected | Description |
|---|---|---|---|
| 133 | 86-87 | Section 9.4.3.1 | (The requirements given in the two bulleted paragraphs of text in this section are given in Section 9.4.5.2.3 and are therefore redundant.) The two bulleted paragraphs of text in this section are deleted. |
| 134 | 88 | Section 9.4.3.2 | In the second bullet, the text "one or more Key Delivery Message(s) (KDMs)" is replaced with the text "a Key Delivery Message (KDM)" |
| 135 | 92 | Section 9.4.3.5 | The existing text of Item 2. is deleted and replaced with the following text:<br>"Security Manager (SM) KDM usage policy is specified as follows:<br>*a. Playout shall be fully supported by a single KDM, inclusive of all required essence keys and playout time window (i.e., a playout shall not occur that requires the combination of two or more KDMs).*<br>*b. For any given composition, playout shall be enabled for any start time that is within the KDM's time window.*<br>c. To avoid end of engagement issues, a show time's playout may extend beyond the end of the KDM's playout time window, if started within the KDM playout time window, by a maximum of six (6) hours.<br>d. *Excepting the requirements of (b), the SM shall delete any KDM and associated keys for which the playback time window has expired (passed).*" |
| 136 | 93 | Section 9.4.3.5 | The existing text of Item 9. (b) is deleted and replaced with the following text:<br>"*Usage validity periods of six (6) hours for remote SPBs (in line with the rule of item 2 (c) above).*" |
| 137 | 93 | Section 9.4.3.5 | The existing text of Item 10. (b) is deleted and replaced with the following text:<br>"*Transferring LE keys only to an authenticated and trusted (7) Link Decryptor Security Entity (SE) function.*" |
| 138 | 94 | Section 9.4.3.5 | The existing text of Item 16. is deleted and replaced with the following text:<br>"*Support suite playback enablement (authentication followed by keying) such that no more than one of each type of SE is enabled (i.e., one LD Block, one Image MD, one audio MD), except for content owner-approved special auditorium situations employing the use of multiple Link Encryption operations. SMs shall support the authentication and keying of multiple Link Encryption operation per the requirements of Section 9.4.4.1 Multiple Link Encryption Operation.*" |

| Erratum | Spec 1.0 Page | Sections Affected | Description |
|---|---|---|---|
| 139 | 94 | Section 9.4.3.5 | Item 19. is deleted. |
| 140 | 96 | Section 9.4.3.6.2 | The last sentence of Item 10. is deleted. |
| 141 | 97 | Section 9.4.3.6.2 | A new Section 9.4.3.6.2.1 is added between Section 9.4.3.6.2. and Section 9.4.3.6.3 with the following text:<br>9.4.3.6.2.1 Normative Requirements for LD/LE SPB Devices<br>The following requirements are normative where a special purpose SPB that performs link decryption followed by link encryption is used (see Section 9.4.4.1):<br>1. *Within the LD/LE Device's type 1 SPB perimeter, perform link decryption followed by link encryption at the image essence input and output ports.*<br>2. *Respond to the Security Manager's (SM's) initiatives in establishing a Transport Layer Security (TLS) session and SPB device authentication. Maintain this session until commanded to terminate.*<br>3. *LD/LE SPB Devices shall not establish security communications with more than one SM at a time.*<br>4. *LD/LE SPB Devices shall contain a UTC time reference clock that is battery backed and operative for time stamping log events under powered and un-powered conditions. The SPB shall communicate time information with the SM using standardized Intra-Theater Messaging.*<br>5. *Respond to SM "status" queries, and other Intra-Theater Messages (ITMs) and SM commands as necessary to support SM behavior requirements.*<br>6. *Accept and store LD/LE keys, and associated parameters, provided by the SM. The SPB shall have the capacity to store at least 16 key/parameter sets.*<br>7. *Purge LD/LE keys upon expiration of the SM designated validity period, SM "purge" command, SPB tamper detection, or change in TLS network parameters suggestive of an attack or equipment substitution.*<br>8. *Record security event data for logging under both powered and un-powered conditions. Sign and assemble logged information into standardized log records per Section 9.4.6.3.*<br>9. *Monitor LD/LE SPB Device physical security protection integrity 24/7. In the event of intrusion or other tamper detection, terminate all activity, log the event, and zero all Critical Security Parameters (see Section 9.5.2.6). Do not purge log records.* |
| 142 | 98 | Section 9.4.3.6.4 | The last sentence of Item 9. is deleted. |

| Erratum | Spec 1.0 Page | Sections Affected | Description |
|---|---|---|---|
| 143 | 100 | Section 9.4.4 | A new Section 9.4.4.1 is added after Section 9.4.4 and before Section 9.4.5 with the following text:<br>9.4.4.1 Multiple Link Encryption Operation<br>Content owners may approve the use of multiple Link Encryption stages within a single auditorium for accommodating special auditorium situations. Special auditorium situations are recognized as changes to Auditorium 2 of Figure 16 such as: (i) the insertion of a single image processor between Image Media Block and a LDB/projection system; (ii) the use of multiple LDB/projection systems with a single server/IMB.<br>*Multiple Link Encryption operation shall follow all normal (single) Link Encryption requirements of this section, with the following additional requirements:*<br>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 will return the associated certificate roles for each SPB in the auditorium (i.e., LD/LE SPB device or more than a single LDB/projector).*<br>b. *The SM shall independently authenticate each remote SPB using a dedicated TLS session.*<br>c. *SMs shall enable multiple Link Encryption operation only when the SM receives a KDM whose TDL contains only the identities of the remote SPBs identified during TLS authentication.* This matching is an indication to the SM that the multiple Link Encryption operation has been approved by the content owner.<br>d. *The image processor (LD/LE) device shall be protected by a type 1 SPB. This SPB shall meet the requirements of Section 9.4.3.6.2.1 Normative Requirements for LD/LE SPB Devices.*<br>e. *The SM shall independently key each remote SPB for Link Encryption operation using standardized Intra-Theater security Messaging per Section 9.4.5.*<br>f. *The SM shall not support the use of more than one image processor SPB for any LDB/projector system.*<br>g. The two Link Encryption stages of the image processor configuration may use the same LE key(s). *The SM shall key the multiple LDB/projector configuration using different LE keys for each LDB/projector system.* |
| 144 | 102 | Section 9.4.5.2.3 | In Item 1., a period is placed at the end of the first line of text, so the first sentence reads:<br>"*1. Only the SMS or SM shall set up Transport Layer Security (TLS) sessions.*" |

| Erratum | Spec 1.0 Page | Sections Affected | Description |
|---|---|---|---|
| 145 | 102 | Section 9.4.5.2.3 | Erratum #6 is withdrawn and replaced with this erratum, which is more exact:<br>The existing text of Item 9. is deleted and replaced with the following text:<br>*"Standardized security messages (Category 2 messages of Table 15) shall use, and have exclusive use of, well-known port 1173 (which has been reserved for SMPTE digital cinema use by the Internet Assigned Numbers Authority [IANA]). Operational messages (Category 1 messages of Table 15) shall not use TCP port 1173, but shall operate under TLS."* |
| 146 | 114 | Section 9.4.6.2 | The existing text of Item 5. (which starts "In the event that valid overlapping KDMs exist…") is deleted and replaced with the following text:<br>"[This item left blank intentionally.]" |
| 147 | 114 | Section 9.4.6.2 | The existing text of Item 7. (which starts "The SM and FM Security Entities shall…") is deleted and replaced with the following text:<br>"*The SM and FM Security Entities shall log the presence or absence of audio and image Forensic Marking for each encrypted DCP.*" |
| 148 | 114 | Section 9.4.6.2 | A new Item 8. is added to the end of this section with the following text:<br>"8. *If audio Forensic Marking is enabled, all sixteen audio channels shall be forensically marked.*" |