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 be modified in the DCI Specification.
Please send suggested errata issues to dci.info@dcimovies.com Please include - Subject: ERRATA

DCI Specification Errata Listing 28-Mar-06

<table>
<tr><th>Erratum</th><th>Spec 1.0 Page</th><th>Sections Affected</th><th>Description</th></tr>
<tr><td>1</td><td>80,96</td><td>9.4.1 Item (2) and 9.4.3.6.1 Item (7).</td><td>Both sections (which have to do with projector SPB requirements) incorrectly reference "9.7.3 Subtitle Encryption" rather than "9.5.2 Robustness".</td></tr>
<tr><td>2</td><td>81</td><td>9.4.1</td><td>For clarification, subtitle decryption is expected to be performed in the server or the Image Media Block. It is not expected that subtitle decryption will be performed in the projector post-Image Media Block or post-Link Decryptor Block. See also footnote 19.</td></tr>
<tr><td>3</td><td>52</td><td>7.5.3.7 Table 9</td><td>Incorrect Calculated Table Values
Replace Table 9 with the Following:
<table>
<tr><th>Average Bit Rate (Mbits/sec)</th><th>3 Hour Image (GBytes)</th><th>3 Hour Audio (GBytes)</th><th>20 min. pre-show (Gbytes)</th><th>Sub Picture (GBytes)</th><th>Timed Text (GBytes)</th><th>Aux Data (GBytes)</th><th>3 Hour Total (GBytes)</th></tr>
<tr><td>250</td><td>337.500</td><td>2.281</td><td>37.500</td><td>0.300</td><td>0.001</td><td>0.001</td><td>377.582</td></tr>
<tr><td>200</td><td>270.000</td><td>2.281</td><td>30.000</td><td>0.300</td><td>0.001</td><td>0.001</td><td>302.582</td></tr>
<tr><td>125</td><td>168.750</td><td>2.281</td><td>18.750</td><td>0.400</td><td>0.001</td><td>0.001</td><td>190.182</td></tr>
<tr><td>100</td><td>135.000</td><td>2.281</td><td>15.000</td><td>0.600</td><td>0.001</td><td>0.001</td><td>152.882</td></tr>
<tr><td>80</td><td>108.000</td><td>2.281</td><td>12.000</td><td>0.800</td><td>0.001</td><td>0.001</td><td>123.082</td></tr>
</table>
Table 9: Example of Storage Capacity for one 3-Hour Feature (12 bits @ 24 FPS)</td></tr>
<tr><td>4</td><td>97</td><td>9.4.3.6.3</td><td>It is clarified that Section 9.4.3.6.3 item (2) refers to an integrated IMB/Projector implementation (as opposed to an integrated IMB/server implementation) and should be considered part of item (4).</td></tr>
<tr><td>5</td><td>98</td><td>9.4.3.6.6</td><td>Section 9.4.3.6.6 should clarify that in the case where the Projector and companion SPB are inseparable, a single Digital Cinema Certificate shall represent both the Projector and its companion SPB (Image Media Block or Link Decryptor Block). This change follows Erratum 10 - “single digital certificate per SPB” constraint in Section 9.5.1.</td></tr>
<tr><td>6</td><td>103</td><td>9.4.5.2.4 Table 15</td><td>Table 15 Category 1 "operational messages” of Section 9.4.5.2.4 are not considered security messages. Therefore, following the requirements of Section 9.4.5.2.3 #9, operational messages shall not use TCP port 1173. Operational messages shall follow other stated RRP requirements, and operate under TLS.</td></tr>
<tr><td>7</td><td>113</td><td>9.4.6.2</td><td>The ‘no FM mark’ state described in Section 9.4.6.2 item 3a shall not be indicated by a default key, but shall be indicated by the ‘ForensicMarkFlagList’ element of the KDM. All other references to such default key in Section 9.4.6.2 (or other sections as applicable) shall similarly accept the ‘no FM mark indicator as being this KDM element.’</td></tr>
</table>

8	115	9.4.6.3.1	Item (9) of Section 9.4.6.3.1 shall be replaced as follows: "The Image Media Block shall internally store at least twelve (12) months of typical log data accumulation for the auditorium in which it is installed, including log data collected from the associated remote SPBs."
9	120	9.4.6.3.7 Table 34	The “Log Messages/Log Management” class (Table 34) was designed to provide a record of log upload events. Since stored logs are not deleted from the SPB after uploads (but remain for twelve months), this record class is not required.
10	122	9.5.1	The first paragraph of Section 9.5.1 shall be changed to indicate that a) each SPB carry “exactly one” Digital Cinema certificate, and b) SEs contained within an SPB shall share this one certificate (with their roles appropriately noted as stated). Footnote 28 is no longer needed. In addition, the reference to RFC2459 shall be changed to RFC3280 (RFC 3280 obsoletes RFC2459).
11	124	9.5.2.2	"Secure Silicon” (item (a) of the first bullet, Section 9.5.2.2) shall only be required to meet FIPS 140-2 level 3 row (area) five: “physical security requirements".
12	125	9.5.2.3	The reference in the last sentence of this section is incorrect and should be “9.5.2.7 - SPB Firmware Modifications".
13	127	9.5.2.5	Delete the second bullet point (Nr3). (FIPS processes are eased by separating FIPS roles and authentication from DCI device/operator roles and authentication. The former is addressed by vendors as part of FIPS documentation, the latter is addressed by the TLS authentication and AuthorityID requirements of Section 9.4.5).
14	127	9.5.2.5	Table 37 does not reflect the most current FIPS 140-2 table, and shall be considered informative (refer to FIPS 140-2 publications for the most current version of this table).
15	128	9.5.2.6	Section 9.5.2.6 shall be re-titled “Critical Security Parameters and D-Cinema Security Parameters.” Items #6 (forensic marking parameters) and #8 (log data/parameters) shall not be classified as FIPS 140-2 Critical Security Parameters (CSP), but shall be classified as "D-Cinema Security Parameters". Item #9 shall be replaced with: 'D-Cinema Security Parameters (DCSP) shall at all times be protected by a type 1 SPB perimeter (except where log data is extracted per Section 9.4.6.3)'
16	128	9.5.2.7	The information requirements of bullet two shall include time/date and version number information

			associated with any firmware change, in addition to the authority figure. The requirements for FIPS Level 3 audit/recording of bullet four are encouraged but shall be optional.
17	129	9.5.4	For clarification, subtitle decryption is expected to be performed in the server or the Image Media Block. It is not expected that subtitle decryption will be performed in the projector post-Image Media Block or post-Link Decryptor Block. If subtitle decryption does not take place in the Image Media Block or server (such that subtitle decryption keys must be exported from the IMB and transported to the subtitle decryptor location), subtitle decryption keys shall be transported to the subtitle decryptor via the standard 'KeyLoad' Intra-Theater Message (ITM - see Section 9.4.5) operating under TLS.
18	130	9.5.6	The following sentence shall be appended to the end of the first bullet of Section 9.5.6: 'In particular, such firewall protection shall prevent (filter) communications to or from any port 1173, other than directly between security equipment within a single auditorium'.
19	135	9.7.6	Though intended to specify key generation . requirements for both symmetric and asymmetric cryptographic needs, the stated RFC 3447 covers only the latter (RSA keys). Symmetric key generation shall be per ANSI X9.31