# 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 04 DECEMBER 2007

| Erratum Number | Spec 1.1 Page | Section(s) Affected | Description |
|---|---|---|---|
| 56 | 33 | Section 5.3.1.7 | The second sentence of this section is deleted and replaced with the following text:<br>*The Key Epoch shall minimally be one Reel.* |
| 57 | 34 | Section 5.3.2.1 | The first sentence of this section is deleted and replaced with the following text:<br>*MXF Track File Encryption shall be compliant with SMPTE 429-6-2006 D-Cinema Packaging – MXF Track File Essence Encryption.* The following requirements clarify the use of SMPTE 429-6-2006 with this specification. |
| 58 | 34 | Section 5.3.2.1 | The bulleted text of this section is modified as follows:<br>In the 4th bullet, the word "reel" is inserted so that the sentence reads:<br>*"Each reel shall use a single cryptographic key for all frames within the sound or picture Track File"*<br>In the 6th bullet, the following sentence is added after the existing sentence:<br>*"The optional Message Integrity Code (MIC) element of SMPTE 429-6-2006 shall be present."*<br>In the 7th bullet, the following sentence is added after the end of the existing sentence:<br>*"The optional TrackFileID and SequenceNumber elements of SMPTE 429-6-2006 shall be present."* |
| 59 | 34 | Section 5.3.2.2 | The existing text of this section is deleted in its entirety, including Figure 10, and replaced with the following text:<br>**5.3.2.2. Encrypted Track File Constraints**<br>*MXF Track File Encryption shall be compliant with SMPTE 429-6-2006 D-Cinema Packaging – MXF Track File Essence Encryption.* |
| 60 | 41 | Section 6.2.3 | The second sentence of this section is deleted and replaced with the following sentence:<br>*The ingest interface shall comply with either Clause 34 or Clause 44 of IEEE 802.3-2005 for either 1000 Mb/s or 10 Gb/s operation, respectively.* |
| 61 | 50 | Section 7.5.2.1 | The existing Figure 11 is deleted and replaced with the Figure 11 given at the end of this errata document. |

| Erratum Number | Spec 1.1 Page | Section(s) Affected | Description |
|---|---|---|---|
| 62 | 81 | Section 9.4.1 | The published V1.1 errata # 19 for item 6 left off the footnote number “17”. This needs to be put back in. |
| 63 | 81 | Section 9.4.1 | In the last sentence of Item 7, the phrase “*and log*” is inserted after the word “*announce*”. |
| 64 | 84 | Section 9.4.2 | The existing section title is deleted and replaced with the following section title:<br>**Theater System Security Devices** |
| 65 | 85 | Section 9.4.2.4 | In the third paragraph, the second to last sentence is deleted and replaced with the following sentence:<br>*The real time operating system of the SM shall use the National Security Agency (NSA) kernel specifically designed for secure operations (e.g., Security Enhanced Linux (SELinux)).* |
| 66 | 86 | Section 9.4.2.6 (new section) | A new Section 9.4.2.6 is inserted between Section 9.4.2.5 and Section 9.4.3 with the following text:<br>9.4.2.6 Projection Systems<br>From the security perspective, a projection system consists of the projector type 2 Secure Processing Block (SPB) and its “companion” SPB, which will be either the Link Decryptor Block (LDB) or Image Media Block (IMB). A critical security issue is assuring that the clear text image output of the LDB or IMB goes to a legitimate projection device.<br>Therefore Section 9.4.3.6.1 Normative Requirements: Projector Secure Processing Block defines a “marriage” process with the companion SPB. The marriage, in conjunction with the Trusted Device List (TDL) and TLS-based authentication of the companion and projector SPBs, addresses the legitimate projector security issue.<br>The purpose of the marriage is to have a human authority figure supervise the installation of a projection system to assure the physical connection of the two SPBs, which TLS-based authentication alone cannot do. At the time of installation the authority figure can provide visual inspection of the projector to assure it has not been tampered with.<br>Once a projector is installed, the state of marriage is permanent (and monitored) until the authority figure decides to separate the two SPBs (for whatever reason). In addition, this specification establishes logging requirements surrounding projector installation and maintenance functions that record security-critical event information.<br>*It is mandatory that a projection system installation includes the marriage function per Section 9.4.3.6 Functional Requirements for Secure Processing Block Systems (noting the permanently married exception provided for in that section). The marriage process shall require the supervision of a human authority figure, who shall examine projectors as part of the marriage process to assure the associated SPB has not been tampered with.* |
| 67 | 88 | Section 9.4.3.1 | The existing Figure 17 is deleted and replaced with the Figure 17 given at the end of this errata document. |
| 68 | 92 | Section 9.4.3.2 | The existing Figure 19 is deleted and replaced with the Figure 19 given at the end of this errata document. |

| Erratum Number | Spec 1.1 Page | Section(s) Affected | Description |
|---|---|---|---|
| 69 | 94 | Section 9.4.3.5 | Item 2 “d” shall be replaced with:<br>“d. Excepting the requirements of item 2c above, the SM shall delete any KDM and associated keys for which the playback time window has expired (passed).” |
| 70 | 95 | Section 9.4.3.5 | The parenthesized phrase of item 10a shall be replaced with:<br>“(i.e., each playout of an encrypted composition requires a new LE key.)” |
| 71 | 97 | Section 9.4.3.6.1 | The existing text of Item 3 is deleted and replaced with the following text:<br>Projector maintenance may involve a marriage (or re-marriage) event, or access to the projector SPB or both. To support projector maintenance, the projector SPB may be serviceable, but access is security-sensitive because of the possibility of tampering during service access.<br>*Once a projector is installed, projector SPB access door “open”, access door “close”, “marriage” and “marriage break” events shall be logged, and the “AuthID” token (see Section 9.4.6.3.8 Log Record Information) shall indicate the responsible exhibition party that executed (or supervised) the event(s). Once a projector is installed, all relevant projector SPB events of Section 9.4.6.3 Logging Subsystem shall be logged 24/7 under both powered and un-powered conditions.*<br>*Playback shall not be permitted and shall terminate if the projector-companion SPB marriage is broken, or a projector SPB access door is open.*<br>To avoid the complexity of retaining its own log records (and the associated need for a clock and battery-backed persistence), the projector SPB may rely upon its companion type 1 SPB by sending projector SPB log event data across the marriage electrical interface to the companion SPB. It is encouraged but not mandatory that projector SPB logs be recorded while a projector is not installed (i.e., not connected to its companion SPB). |
| 72 | 97 | Section 9.4.3.6.1 | In Item 4, the parenthetical text at the end of the sentence is deleted and replaced with the following parenthetical text:<br>*“(see Section 9.5.2.4 Specific Requirements for Type 2 Secure Processing Blocks)”* |
| 73 | 98 | Section 9.4.3.6.1 | In Item 6, the following sentence is added after the existing sentence:<br>The physical requirements for a type 2 SPB are given in Section 9.5.2.4 Specific Requirements for Type 2 Secure Processing Blocks. |
| 74 | 98 | Section 9.4.3.6.2 | In Item 9, the existing text is deleted and replaced with the following text:<br>*Record security event data for logging under both powered and un-powered conditions. Assemble logged information into standardized log records per Section 9.4.6.3 Logging Subsystem. If the LDB provides logging support for the projector SPB via a marriage connection per Section 9.4.3.6.1 Item 3, then the LDB shall provide such logging support 24/7 under both powered and un-powered conditions.* |
| 75 | 99 | Section 9.4.3.6.2 | Item 11 is deleted. |

| Erratum Number | Spec 1.1 Page | Section(s) Affected | Description |
|---|---|---|---|
| 76 | 100 | Section 9.4.3.6.3 | A new Item 7 is added with the following text (note that the original Item 7 was deleted in Erratum #39):<br><br>*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 Logging Subsystem. If the IMB provides logging support for the projector SPB via a marriage connection per Section 9.4.3.6.1 Item 3, then the IMB shall provide such logging support 24/7 under both powered and un-powered conditions.* |
| 77 | 101 | Section 9.4.3.6.5 | The existing text of this section is deleted in its entirety and replaced with the following text (note that this erratum deprecates Erratum #41, which is withdrawn):<br><br>The following are considerations for implementation details, and standardization.<br><br>• For the projector system, authentication of the projector SPB to the SM need not require TLS sessions between the SM and both the Projector and Link Decryptor Block SPBs. It may be simpler to have the LDB proxy for a direct SM TLS connection with the projector SPB. *This option enables the projector SPB to avoid having its own, separate TLS session with the SM, but shall not substitute for the requirement for both the LDB and projector certificates to be securely delivered to the SM, and for these two certificates to be on the TDL that is examined by the SM. An option that can avoid this dual certificate requirement is given in the next bullet. In this case, authentication and signal integrity processes shall provide equal protection as in a dual TLS session case.* It is encouraged that a single approach be standardized.<br><br>• The projector/LDB SPB marriage could create a new secret cryptographic identity, which is changed at each installation event. Such an identity would be used for authorization of the combined, married device and used in the TDL as a singular identification, rather than identifying both LDB and projector in the TDL independently. *In this case, authentication and signal integrity processes shall provide equal protection as in a dual TLS session case.* It is encouraged that a single approach be standardized.<br><br>• Communication of the “projector SPB open” event signal should preferably involve a cryptographic secret so that hardware spoofing at the IMB or LDB interface (e.g., extender board attack) is thwarted. |
| 78 | 102 | Section 9.4.3.7 | The existing 4th bulleted text (beginning “Remote SPBs type 1 shall…”) and its sub-bulleted text is deleted and replaced with the following bulleted text:<br><br>• *Remote SPBs type 1 shall have internal UTC time clocks, and maintain time-awareness 24/7 under both powered and un-powered conditions. The Security Manager shall track the time difference between remote SPB clocks and its internal clock by issuance of the "GetTime" standardized security message of Table 15 “Intra-Theater Message Request-Response Pairs” at least once per day.* |

| Erratum Number | Spec 1.1 Page | Section(s) Affected | Description |
|---|---|---|---|
| 79 | 102 | Section 9.4.3.7 | The following sentence is added after the existing sentence of the last bullet of this section:<br>*"Exhibition shall be able to adjust a remote SPB's clock a maximum of +/- fifteen minutes within any calendar year. Time adjustments shall be logged events."* |
| 80 | 103 | Section 9.4.4 | The first sentence of the last paragraph shall be replaced with:<br>"*It is mandatory that a fresh Link Encryption key be used for each movie showing* (i.e., each playout of an encrypted composition requires a new LE key.)" |
| 81 | 115 | Section 9.4.6.1.1 | The following bullet and sub-bullet items are added at the end of this section:<br>• *Forensic Marking shall be permanently associated with the Image Media Block that contains it. To enforce this association, the following requirements are mandatory:*<br>o *Each instance of a Forensic Marking application shall be assigned a unique Forensic Marking Identification (FMID).*<br>o *Forensic Marking shall be manufactured such that the FMID cannot be changed or reprogrammed by any means whatsoever without violation of the IMB's SPB-1 perimeter.*<br>o *Manufacturers of Image Media Blocks shall maintain and make available an accurate, timely database associating each FMID with its associated IMB serial number and IMB digital certificate.*<br>o *Forensic Marking licensors shall insure the uniqueness of FMIDs.* |
| 82 | 118 | Section 9.4.6.3 | The paragraph at the top of the page (before "Definitions related to logging:") is deleted and replaced with the following text:<br>This section sets the logging subsystem requirements for security log data recording and reporting. The log information data formats and structures to be used in conjunction with these requirements are defined in two SMPTE standards:<br>• SMPTE 430-4-2008 D-Cinema Operations – Log Record Format Specification for D-Cinema<br>• SMPTE 430-5-2008 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema<br>SMPTE 430-4-2008 defines the general format for log classes for digital cinema. SMPTE 430-5-2008 defines the specific requirements for the security log class. *All log requirements and terminology of this section are with respect to the SMPTE 430-5-2008 security events class constraints specification.* |
| 83 | 118 | Section 9.4.6.3 | The 5th bulleted item (which begins "Log Message – Standardized Intra-Theater Message…") is deleted. |
| 84 | 118 | Section 9.4.6.3.1 | In Item 2, the name for Section 9.4.6.3.7 is changed to "Security Log Records". |
| 85 | 119 | Section 9.4.6.3.1 | In Item 6, the name for Section 9.4.6.3.6 is changed to "Log Filtering". |

| Erratum Number | Spec 1.1 Page | Section(s) Affected | Description |
|---|---|---|---|
| 86 | 119 | Section 9.4.6.3.1 | In Item 7, the name for Section 9.4.6.3.6 is changed to “Log Filtering”. |
| 87 | 119-120 | Section 9.4.6.3.2 | The existing text of this section is deleted in its entirety and replaced with the following text:<br><br>*Log record and report formats shall be compliant with SMPTE 430-5-2008 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema.* |
| 88 | 120-122 | Section 9.4.6.3.3 | The existing text of this section, including Figure 21, is deleted in its entirety and replaced with the following text:<br><br>*Log integrity controls shall be compliant with SMPTE 430-5-2008 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema.* |
| 89 | 122 | Section 9.4.6.3.4 | The existing text of this section is deleted in its entirety and replaced with the following text:<br><br>*Log record sequencing shall be compliant with SMPTE 430-5-2008 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema.* |
| 90 | 122 | Section 9.4.6.3.5 | The existing text of this section is deleted in its entirety and replaced with the following text:<br><br>*Auditorium suites using Link Encryption shall transfer log records from remote Secure Processing Blocks (SPB) to that auditorium’s Image Media Block (IMB) SM using the GetEventList and GetEventID standardized security messages of Table 15 “Intra-Theater Message Request-Response Pairs”.*<br><br>Per Section 9.4.3.7 Theater System Clocks and Trustable Date-Time, the Security Manager collects UTC time-stamped reports from remote SPBs via the GetTime standardized security message. *The SM shall use the GetTime information to calculate the difference between true time (the SM’s time) and time in the remote SPB, and remove the difference in reporting remote SPB event data. The reporting (export) of log information from the IMB shall be by XML structure that is compliant with SMPTE 430-5-2008 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema.* |
| 91 | 122 | Section 9.4.6.3.5.1 | This section is deleted. |
| 92 | 122-123 | Section 9.4.6.3.6 | The existing text of this section, including section name, is deleted in its entirety and replaced with the following text:<br><br>**9.4.6.3.6. Log Filtering**<br><br>*Log record and/or report filtering processes shall be compliant with SMPTE 430-5-2008 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema.*<br><br>For distribution of log information, it may be necessary to filter log content so that log records or reports can be generated that supply log record content selectively to the appropriate recipients. The location(s) where log data filtering takes place (e.g., in the Image Media Block (IMB) or in external theater-controlled devices or processes) is an implementation decision. |

| Erratum Number | Spec 1.1 Page | Section(s) Affected | Description |
|---|---|---|---|
| 93 | 123-125 | Section 9.4.6.3.7 | The existing text of this section, including section name and tables, is deleted in its entirety and replaced with the following text:<br><br>**9.4.6.3.7. Security Log Records**<br><br>*Log records for the "security class" shall be compliant with SMPTE 430-5-2008 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema.* |
| 94 | 125 | Section 9.4.6.3.8 | The existing text of this section is deleted in its entirety and replaced with the following text:<br><br>*The logging subsystem shall follow the requirements for specific log data to be recorded as defined in SMPTE 430-5-2008 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema.* SMPTE 430-5-2008 defines the following data types for the "Security Class" category of log information:<br><br>EventType – Identifies a log record as being associated with one of a Playout, Validation, Key, ASM or Operations event.<br><br>EventSubType – Specifies what information is to be logged for each Event Sub Type record.<br><br>*Each Secure Processing Block (SPB) type shall log the Event Sub Type records as shown in Table 33 below.*<br><br>[Insert Table 33 (see below) here]<br><br>*In addition to the requirements specified in SMPTE 430-5-2008, the following shall be normative for DCI compliance:*<br><br>*1. SPBs shall log each of the "Exception" events identified in the EventSubType Record descriptions for the applicable Event Sub Type records per Table 33. The SPB shall record the appropriate Exception record(s) as specified in the SMPTE 430-5-2008 EventSubType definitions.*<br><br>*2. The SPBSecurityAlert Operations EventSubType shall be recorded for conditions that require replacement of the SPB (i.e., equipment tampering or failure) per Section 9.6.1.3 Digital Rights Management: Security Entity Equipment.*<br><br>3. *The AuthID token for the Playout Event Sub Type events shall carry the value indicated by the SMS AuthorityID per Section 9.4.2.5 Screen Management System. Per section 9.4.2.6 Projection Systems, the AuthID token for the Operations Event Sub Type events shall indicate the identity of the authority figure responsible for the event.* |
| 95 | 129 | Section 9.5.2.4 | The existing text of the 4th bulleted item is deleted and replaced with the following text:<br><br>• *For the projector SPB physical perimeter, Table 36 FIPS 140-2 level 3 requirements shall be followed for area (row) number 5 (physical security), following the area 5 guidelines for "Multiple-Chip Standalone Cryptographic Modules".* |

| Erratum Number | Spec 1.1 Page | Section(s) Affected | Description |
|---|---|---|---|
| 96 | 129 | Section 9.5.2.4 | The following paragraph is added between the 4th bulleted item and the last paragraph of this section:<br><br>"The FIPS references of only this section establish technical and robustness thresholds for selected aspects of projector SPB implementations. The requirements to follow FIPS 140-2 guidelines do not require FIPS certification or strict FIPS 140-2 documentation or evaluation criteria be undertaken." |
| 97 | 130 | 9.5.2.5 | The following paragraph is added to the end of this section:<br><br>"FIPS 140-2 level 3 devices provide physical and logical protection of their parameters and functions 24/7 and shall be able to respond to attacks under both powered and un-powered conditions. This means that if a type 1 SPB requires a power source to accomplish tamper detection and response, it must zeroize its Critical Security Parameters (CSPs) prior to any situation arising where such power source may not be available. By way of example, if a type 1 SPB is in storage and relying upon a battery for tamper detection and response, it must self-destruct prior to a battery depletion condition which would not support proper tamper detection and/or response." |
| 98 | 142 | 10 | The following item is added to the Glossary:<br><br>FMID – Acronym for Forensic Marking Identification. The FMID is a unique fixed identifier of the specific instance of the Forensic Marking application. |

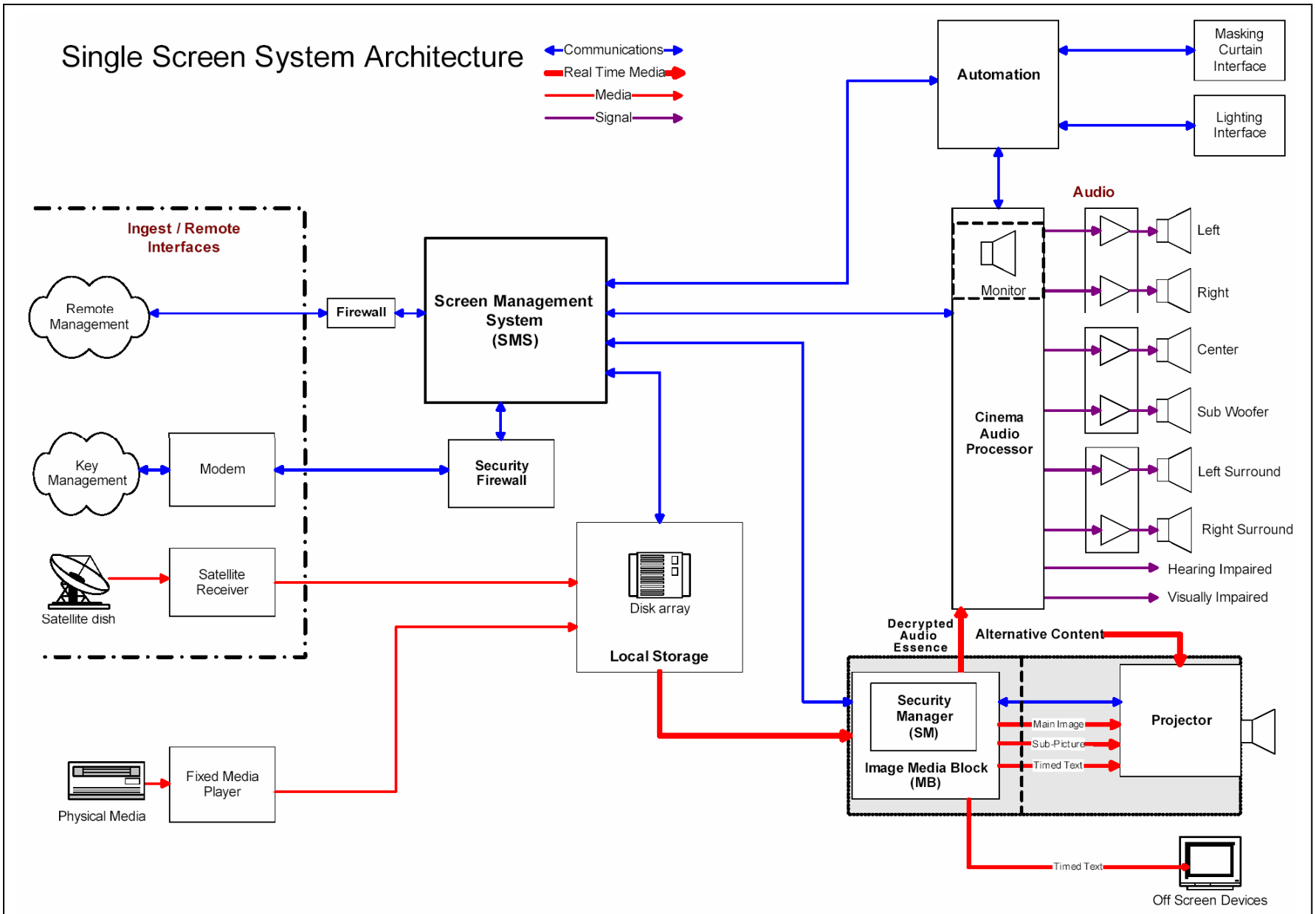


**Figure 11: Single-Screen System Architecture**

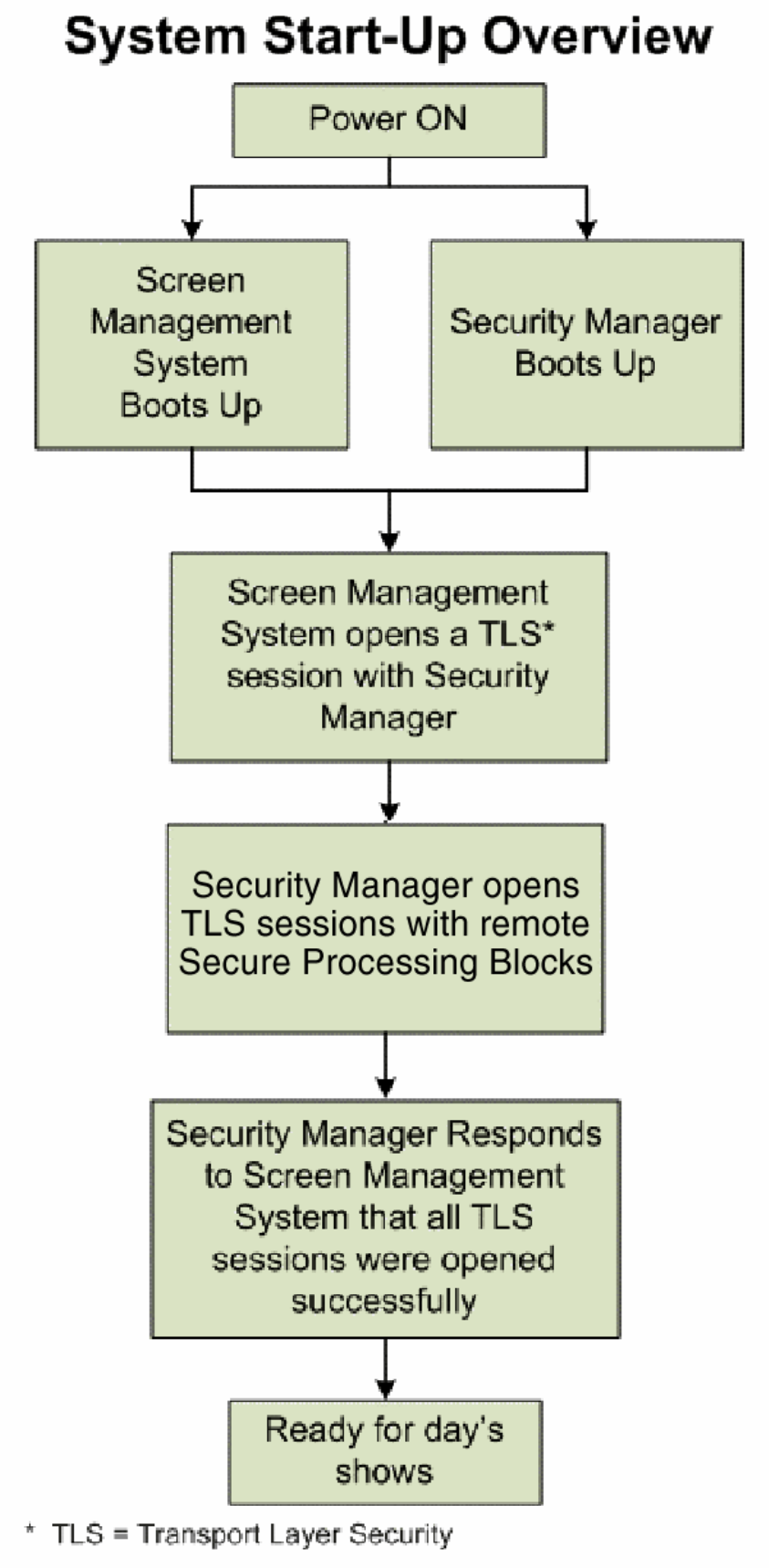


**Figure 17: System Start-Up Overview**

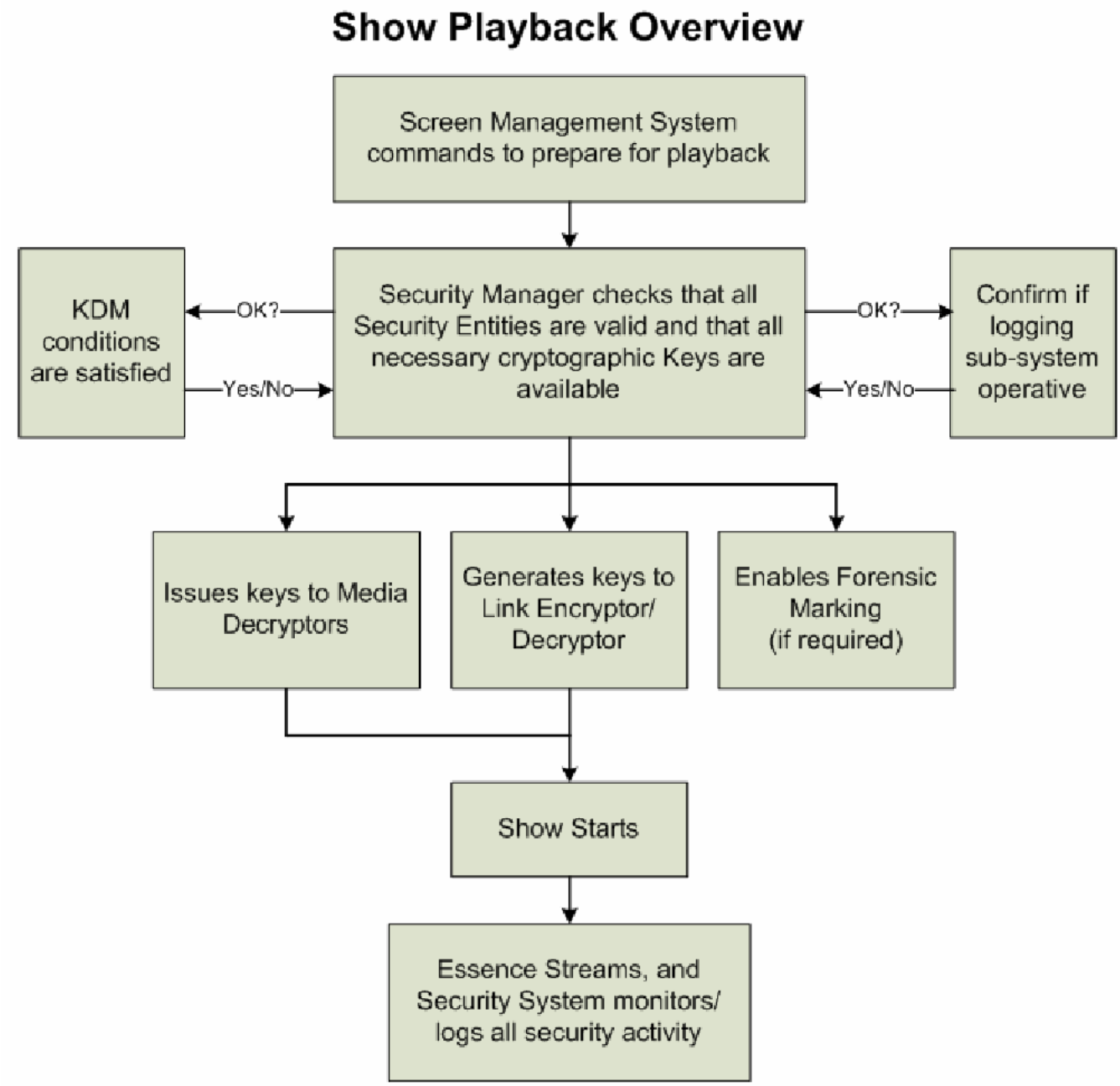


**Figure 19: Show Playback Overview**

**Table 33: Security Log Event Types and Subtypes**

| | IMB | LDB | LD/LE SPB | Proj. SPB |
|---|---|---|---|---|
| **Playout Event Sub Types** | | | | |
| FrameSequencePlayed | X | | | |
| CPLStart | X | | | |
| CPLEnd | X | | | |
| PlayoutComplete | X | | | |
| | | | | |
| **Validation Event Sub Types** | | | | |
| CPLCheck | X | | | |
| | | | | |
| **Key Event Sub Types** | | | | |
| KDMKeysReceived | X | | | |
| KDMDeleted | X | | | |
| | | | | |
| **ASM Event Sub Types** | | | | |
| LinkOpened | X | X | X | X [1] |
| LinkClosed | X | X | X | X [1] |
| LinkException | X | X | X | X [1] |
| LogTransfer | X | X | X | X [2] |
| KeyTransfer | X | X | X | |
| | | | | |
| **Operations Event Sub Types** | | | | |
| SPBOpen | | | | X |
| SPBClose | | | | X |
| SPBMarriage | X [3] | X | | X |
| SPBDivorce | X [3] | X | | X |
| SPBShutdown | X | X | X | X |
| SPBStartup | X | X | X | X |
| SPBClockAdjust [4] | X | X | X | X |
| SPBSoftware | X | X | X | X |
| SPBSecurityAlert | X | X | X | X |

[1] Applicable if the Projector SPB has its own TLS session with the IMB.
[2] Applicable if the Projector SPB records its own log records, and transfers them over TLS.
[3] Applicable when no Link Encryption is used.
[4] Applicable if the SPB has a clock that is adjustable.