DCI Digital Cinema Initiatives, LLC

ERRATA TO DCI *DIGITAL CINEMA SYSTEM SPECIFICATION, VERSION 1.3*

Errata items continue to be evaluated and will be posted after agreement by the DCI membership that the specific errata need to modify the DCI *Digital Cinema System Specification, Version 1.3*, dated 27 June 2018. Suggested Errata issues may be emailed to dci.info@dcimovies.com. Please include "Errata" in the subject line.

DCI SPECIFICATION ERRATA LISTING: **1 OCTOBER 2018**

Erratum Number	Spec. 1.3 Page No.	Section(s) Affected	Description
1	27	3.3.4.3	A new section 3.3.4.3 is added as follows: **3.3.4.3. Object-Based Audio Essence (OBAE)** *Object-Based Audio Essence (OBAE) implementations shall meet all requirements as defined in the Digital Cinema Object-Based Audio Addendum approved by Digital Cinema Initiatives, LLC (DCI) on 23 August 2018.* This specification refers to OBAE in lieu of Immersive Audio.
2	94	9.4.2.5	The last bullet of this section is replaced with the following two bullets: • *If multiple SMSs are present, exhibition shall designate one to TLS connect with, and be used for identity logging by, all SMs participating in any given showing.* • *Upon the completion of each show playback (i.e., execution of the show playlist) the SMS shall query each participating Media Bock SM for its flagged indication that a PlayoutComplete security log report has been prepared, upon which indication the SMS shall collect the report. For Multiple Media Block (MMB) show playback situations the reports from each MB shall be stored in a collocated fashion such that all the reports for any given playback are readily available, for a period of at least one year.* Exhibition is free to use a storage location of their choice (i.e., the SMS may pass the collected reports to external storage). See Sections 9.4.3.6.1 Logging Requirements, item #18 and 9.4.6.3.10 Logging Failures for associated information regarding SM behavior.

Erratum Number	Spec. 1.3 Page No.	Section(s) Affected	Description
3	107	9.4.3.6.1	The following is added as a new paragraph after the first paragraph of item #3: *A security access opening event shall be electronically detected, and projector SPB designs shall prevent playout unless the detector(s) indicate all security access openings are closed. (Projector SPB "maintenance" and "security" servicing is defined in Section 9.5.2.4 Specific requirements for Type 2 Secure Processing Blocks.)*
4	128	9.4.6.3.1	New item #18 is added to this section as follows: 18. *Upon the completion of each show playback (i.e., execution of the show playlist) a Media Block SM shall:* *a. Within 60 seconds, prepare a log report containing a "PlayoutComplete" log record (per SMPTE 430-5 D-Cinema Operation – Security Log Event Class and Constrains for D-Cinema) for each encrypted composition of the just executed show playlist.* *b. Set a flag indicating that the PlayoutComplete report(s) has been prepared, which will be notification for the SMS to collect the PlayoutComplete report(s) from the MB.* *c. Reset the flag once the PlayoutComplete report(s) has been collected by the SMS, and disallow the next playback event until the SMS has so collected the report(s) (and the flag has been reset).* *For Multiple Media Block (MMB) show playback situations the SMS must collect a log report(s) from each participating MB.* See the associated SMS requirements at Section 9.4.2.5 Screen Management System (SMS).
5	132	9.4.6.3.8	The following new bullet is added to the end of this section: • *For the FrameSequencePlayed Record (SMPTE ST 430-5 section 7.3.1.1), if the track file is an OBAE track tile, the Parameters list shall contain a name/value pair whose name element shall contain the token OBAEMark, and whose Value element shall contain one of two tokens, either "true" or "false", indicating that a forensic mark was or was not inserted during playout.*

Erratum Number	Spec. 1.3 Page No.	Section(s) Affected	Description
6	132	9.4.6.3.10	The text of this section is replaced with: *The secure logging requirements of this Section 9.4.6.3 Logging Subsystem are required to be functionally executed and fully operable as a prerequisite to playback. Per Section 9.4.6.3.1 Logging Requirements, Security Managers (SM) shall prevent the playout of encrypted content for which:* • *It has not collected log records from remote Secure processing Blocks (SPBs) per item #8,* • *The SMS has not collected the PlayoutComplete report per item #18,* • *There is any indication that the next playback will not record and report log records as required.* *Behavior of SPBs shall be specified and designed to immediately terminate operation and require replacement upon any failure of its secure logging operation. Resident log records in failed SPBs shall not be purgeable except by authorized repair centers, which shall be capable of securely recovering such log records.*

Erratum Number	Spec. 1.3 Page No.	Section(s) Affected	Description
7	137	9.5.2.4	Section 9.5.2.4 is replaced in its entirety with:

9.5.2.4. Specific Requirements for Type 2 Secure Processing Blocks

The SPB type 2 container has been defined specifically for protection of image essence exiting either a Link Decryptor Block or Image Media Block (companion SPBs to the projector SPB) and entering the projector. The purpose of this SPB is to protect the image essence signal as far as practical, recognizing that "all the way to light" production is not possible. It is also preferable not to impose formal FIPS 140-2 requirements on this SPB, as the security and signal flow functions are relatively simple.

General requirements for SPBs are defined in Section 9.4.2.2 "The Secure Processing Block (SPB)," and Section 9.5.2.2 "Physical Security of Sensitive Data." Specific requirements for projection systems are defined in Section 9.4.3.6.1 "Normative Requirements: Projection Systems." As explained there, the type 2 SPB – also referred to as a projector SPB – is permitted to be opened for maintenance. To assure adequate protection of signals and circuits within the projector SPB, the following address physical requirements, and are in addition to those of the above noted sections:

- *The projector SPB shall be designed for two types of access: "security servicing" and "non-security servicing."* Security servicing is defined as having access to Security-Sensitive Signals, which are the companion SPB's output image essence signals or image signals derived from said output signals, or the projector SPB security access opening/detection circuits and associated signals.

- *For non-security servicing (i.e., maintenance), Security-Sensitive Signals shall not be accessible via the SPB's maintenance door opening(s). In other words, there shall be a partition that separates security-related signals/circuits from non-security related maintenance accessible areas, which shall serve as the boundary of the type 2 SPB and deny access to Security-Sensitive Signals, without causing permanent and easily visible damage.*

- *Security servicing shall trigger a security access opening event per Section 9.4.3.6.1 "Normative Requirements: Projection Systems", and be performed only under the supervision of the projector manufacturer per Section 9.5.2.3 "Repair and Renewal". The triggering and clearing (i.e., reset) of a security access opening event shall be respectively logged as an "SPBOpen" and "SPBClose" security log, per Section 9.4.6.3.8 "Log Record Information".*

- *Projector SPB security access openings (i.e., doors or panels that enable access for security servicing) shall be lockable using pick-resistant mechanical locks employing physical or logical keys.*

- *Protection from external probing of Security-Sensitive Signals shall be provided by assuring barriers exist to prevent access to such signals via ventilation holes or other openings.*

In summary, the projector SPB physical perimeter provides for unencumbered maintenance access, and security-critical signals are protected via security access opening door locks and opening detection. Exhibition visual inspection is relied upon to detect physical abuse that might allow compromise of, or access to, decrypted image essence.

Erratum Number	Spec. 1.3 Page No.	Section(s) Affected	Description
8	138	9.5.2.4	New section 9.5.2.4.1 is added as follows:

9.5.2.4.1. Direct View Display Systems

A direct view display system is defined as a light emission display comprised of a combination of flat panel display cabinets conjoined so as to form a single large display. LED-based panels are typical, but *the requirements herein shall apply to any image-forming display technology so comprised.*

Industry design approaches and terminology varies. This specification defines the component parts as follows:

a) **Screen:** The complete direct view cinema display system including all Pixels sufficient to display the entire image, and typically comprised of a plurality of Cabinets with a supporting structure, associated electronics and cabling.

b) **Cabinet:** The physical structure and associated electronics which contains a portion of the image area of a Screen. The emissive surface area of a Cabinet is typically comprised of a plurality of Modules.

c) **Module:** A component including an array of Pixels physically positioned so as to form a portion of the front display surface of a Cabinet. The Module is typically the smallest field-serviceable light-emitting component of a Screen.

d) **Display Pixel:** The smallest grouping of light emitting elements within a Module, and capable of broad-spectrum (not monochromatic) light emissions. A Display Pixel (or Pixel herein) is often comprised of a triplet of red, green and blue light emitting diodes.

The physical characteristics of a direct view display require that the front Screen area comprise part of the display's type 2 SPB physical perimeter. This may prevent it from meeting the "hard, opaque physical security perimeter" requirements of Section 9.4.2.2 "The Secure Processing Block (SPB)", and/or the "SPB hardware module" requirements of Section 9.5.2.2 "Physical Security of Sensitive Data". The following defines type 2 SPB accommodations for direct view displays.

Security servicing and non-security servicing definitions for direct view display systems apply as follows:

Security servicing – Opening or removal of a Cabinet or Module that compromises the type 2 SPB security perimeter and exposes Security-Sensitive Signals. *Such opening or removal shall trigger a security access opening event.* (It is permitted for one security access opening event to reflect the occurrence of simultaneous opening or removal of a plurality of Cabinets and/or Modules as part of a single servicing event.)

Non-security servicing – The opening of a Cabinet or Module that does not expose Security-Sensitive Signals.

For Cabinets having front removable Modules:

- *The removal of a Module shall expose only those Pixel signals accessible via the electrical connection(s) associated with the Module removed, but shall not otherwise expose Security-Sensitive Signals or compromise the type 2 SPB perimeter.*

- *The removal of any Module shall be detected and prevent playout of an encrypted composition.*

- *The removal of more than fifteen (15) Modules, or a Module quantity that exposes Pixel signals constituting more than 5% of the screen area, whichever is less, within any eight hour period, shall trigger a security access opening event.*

Once triggered, to clear (i.e., reset) a security access opening event shall require:

1. *Remedy of the cause of the event (i.e., closure of the security access door or panel, replacement/ reassembly of the Cabinet(s) and/or Module(s), etc.), and*

2. *The supervision of the manufacturer in the use of a physical key and/or logical code.*

For purposes of clarity, a security access opening event shall remain active pending the above closure requirements, and such event shall be bookended by SPBOpen and SPBClose security log records.

The following requirements apply to a fully assembled direct view display system:

1. *The physical intrusion barrier presented by the light emitting front surface of Cabinets or Modules shall not be able to be penetrated without permanently destroying the proper operation of a Cabinet and/or Module so penetrated, and leaving permanent and easily visible damage.*

2. *Cabinets and/or Modules shall be mechanically interlocked to each other directly and/or via the supporting frame structure such that any separation that would enable access to internal signals will cause permanent and easily visible damage.*

3. *Any access to light emitting (Pixel generating) component electrical signals from the surface of the Screen shall be limited to individual component pins, and there shall be no access to signals that would constitute a portion of the picture image beyond the Pixel by Pixel level.*

All other projector and projector SPB requirements of this specification shall remain in place.

In summary, security objectives for a direct view display Secure Processing Block (SPB) are fundamentally the same as for projectors. To avoid influencing electro-mechanical designs, the requirements of this specification are focused on access to Security-Sensitive Signals for direct view display systems, rather than specific requirements for the type 2 SPB physical boundary itself.

9	146	9.7.4	The second paragraph of this section is replaced with: *Per the requirements of Section 9.5.2.2 "Physical Security of Sensitive Data", item c, once decrypted from the KDM, content keys shall be protected at all times (except while being used during playback) by being stored within the Secure Silicon integrated circuit, or by AES key wrapping per NIST SP800-38F if stored external to the Secure Silicon IC.*