Digital Cinema Initiatives, LLC

Digital Cinema System Specification

V1.0

July 20, 2005

Final Approval July 20, 2005
Digital Cinema Initiatives, LLC Member Representatives Committee

NOTICE

Digital Cinema Initiatives, LLC (DCI) is the author and creator of this specification for the purpose of copyright and other laws in all countries throughout the world. The DCI copyright notice must be included in all reproductions, whether in whole or in part, and may not be deleted or attributed to others. DCI hereby grants to its members and their suppliers a limited license to reproduce this specification for their own use, provided it is not sold. Others should obtain permission to reproduce this specification from Digital Cinema Initiatives, LLC.

This document is a specification developed and adopted by Digital Cinema Initiatives, LLC. This document may be revised by DCI. It is intended solely as a guide for companies interested in developing products, which can be compatible with other products, developed using this document. Each DCI member company shall decide independently the extent to which it will utilize, or require adherence to, these specifications. DCI shall not be liable for any exemplary, incidental, proximate or consequential damages or expenses arising from the use of this document. This document defines only one approach to compatibility, and other approaches may be available to the industry.

This document is an authorized and approved publication of DCI. Only DCI has the right and authority to revise or change the material contained in this document, and any revisions by any party other than DCI are unauthorized and prohibited.

Compliance with this document may require use of one or more features covered by proprietary rights (such as features which are the subject of a patent, patent application, copyright, mask work right or trade secret right). By publication of this document, no position is taken by DCI with respect to the validity or infringement of any patent or other proprietary right. DCI hereby expressly disclaims any liability for infringement of intellectual property rights of others by virtue of the use of this document. DCI has not and does not investigate any notices or allegations of infringement prompted by publication of any DCI document, nor does DCI undertake a duty to advise users or potential users of DCI documents of such notices or allegations. DCI hereby expressly advises all users or potential users of this document to investigate and analyze any potential infringement situation, seek the advice of intellectual property counsel, and, if indicated, obtain a license under any applicable intellectual property right or take the necessary steps to avoid infringement of any intellectual property right. DCI expressly disclaims any intent to promote infringement of any intellectual property right by virtue of the evolution, adoption, or publication of this document.

Table of Contents

Table of Figures

Table of Tables

THIS PAGE LEFT BLANK INTENTIONALLY

1. OVERVIEW

1.1. Introduction

A number of significant technology developments have occurred in the past few years that have enabled the digital playback and display of feature films at a level of quality commensurate with that of 35mm film release prints. These technology developments include the introduction of: high-resolution film scanners, digital image compression, high-speed data networking and storage, and advanced digital projection. The combination of these digital technologies has allowed many impressive demonstrations of what is now called "Digital Cinema" These demonstrations, however, have not incorporated all of the components necessary for a broad-based commercially viable Digital Cinema system. These demonstrations have created a great deal of discussion and confusion around defining the quality levels, system specifications, and the engineering standards necessary for implementing a comprehensive Digital Cinema system.

Digital Cinema Initiatives, LLC (DCI) is the entity created by seven motion picture studios: Disney, Fox, Metro-Goldwyn-Mayer[1], Paramount Pictures, Sony Pictures Entertainment, Universal Studios, and Warner Bros. Studios. The primary purpose of DCI is to establish uniform specifications for Digital Cinema. These DCI member companies believe that the introduction of Digital Cinema has the potential for providing real benefits to theater audiences, theater owners, filmmakers and distributors. DCI was created with recognition that these benefits could not be fully realized without industry-wide specifications. All parties involved in the practice of Digital Cinema must be confident that their products and services are interoperable and compatible with the products and services of all industry participants. The DCI member companies further believe that Digital Cinema exhibition will significantly improve the movie-going experience for the public.

1.2. Scope

The document defines technical specifications and requirements for the mastering of, distribution of, and theatrical playback of Digital Cinema content. The details are in the following sections:

- **Digital Cinema Distribution Master (DCDM):** This section provides specifications for the image, audio, subtitle (Timed Text and subpictures) Digital Cinema Distribution Masters. The DCDM-Image defines a common set of image structures for Digital Cinema by specifying an image containers and colorimetry for a Digital Cinema Distribution Master (DCDM). The DCDM-Audio specifies the following characteristics: bit depth, sample rate, minimum channel count, channel mapping and reference levels. The DCDM-subtitles specifies the format of a Digital Cinema subtitle track file. A subtitle track file contains a set of instructions for placing rendered text or graphical overlays at precise locations on distinct groups of motion picture frames. A subtitle track file is an integral component of a Digital Cinema composition and may be present in both mastering and distribution file sets.
- **Compression (Image):** Specifies the DCI compliant JPEG 2000 codestream and JPEG 2000 decoder.
- **Packaging:** This section defines the requirements for packaging the DCDM (image, audio and subtitle) files using (where possible) existing Material eXchange Format (MXF) specifications and eXtensible Mark up Language (XML). The output of this process is the Digital Cinema Package (DCP). This section also defines the requirements for encrypting the essence (sound, picture and subtitles) of the DCP.

[1] Metro-Goldwyn-Mayer withdrew as a Member of DCI in May 2005, prior to the completion of this Specification.

- **Transport:** Defines the movement from distribution centers to theater locations using physical media, virtual private networks or satellite communications.
- **Theater Systems:** Provides requirements for all equipment necessary for theatrical presentation in a typical theater environment. This encompasses digital projectors, media blocks, storage systems, sound systems, the DCP files ingest, theater automation, Screen Management System (SMS) and Theater Management Systems (TMS).
- **Projection**: This section defines the projector and its controlled environment, along with the acceptable tolerances around critical image parameters for Mastering and general Exhibition applications. The goal is to provide a means for achieving consistent and repeatable color image quality. Two levels of tolerances are specified: a tighter tolerance for mastering rooms where critical color judgments are made, and a wider tolerance for satisfactory reproduction in general public exhibition.
- **Security:** The security chapter provides requirements and fundamental specifications for persistent content protection and controlled access in an open security architecture. These objectives are achieved with high security in a multi-user environment via the application of well respected security and encryption standards in primarily three areas: 1) content encryption, 2) security (key) management and 3) high integrity event logging and reporting.

1.3. Document Language

This document consists of normative text and, optional informative text. Normative text is text that describes the elements of the design that are indispensable or contains the conformance language keywords: “shall”, “should” or “may”. Informative text is text that is potentially helpful to the user, but not indispensable and can be removed, changed or added editorially without affecting interoperability. Informative text does not contain any conformance keywords. All text in the document is, by default, normative except: any section titled “Introduction”, any section explicitly labeled as “Informative”, or individual paragraphs that start with the word “Note.” Normative references are those external documents referenced in normative text and are indispensable to the user. Informative, or bibliographic, references are those references made from informative text or are otherwise not indispensable to the user.

The keywords “shall” and “shall not” indicate requirements that must be strictly followed in order to conform to the document and from which no deviation is permitted.

The keywords “should” and “should not” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required. In the negative form, a certain possibility or course of action is deprecated but not prohibited.

The keywords “may” and “need not” indicate a course of action permissible within the limits of the document.

The keyword “reserved” indicates that a condition is not defined and shall have no meaning. However, it may be defined in the future. The keyword “forbidden” is the same as reserved, except that the condition shall never be defined in the future.

A compliant implementation is one that includes all mandatory provisions (“shall”) and, if implemented, all recommended provisions (“should”) as described. A compliant implementation need not implement optional provisions (“may”).

Requirements are indicated with the key phrases “is required to”, “is encouraged to” and “can” which represent “shall,” “should” and “may” (had the text been in a separate requirements document). This is necessary in order to distinguish requirements from the specification conformance language.

Sentences with the following keywords are italics: shall, shall not, should not, is required, is not required, is not encouraged and is encouraged.

The names of standards publications and protocols are placed in [bracketed text]. International and industry standards contain provisions, which, through reference in this text, constitute provisions of this specification. At the time of publication, the editions indicated were valid. These referenced standards are subject to revision, and parties to agreements based upon this specification are encouraged to investigate the possibility of applying the most recent editions of the referenced standards. Section 10 GLOSSARY OF TERMS is a glossary of technical terms and acronyms used throughout this specification. The reader is encouraged to refer to the glossary for any unfamiliar terms and acronyms.

Trademarked names are the property of their respective owners.

1.4. System Objectives

At the onset of writing a specification for a Digital Cinema system, DCI acknowledged certain fundamental requirements, which are:

- *The Digital Cinema system shall have the capability to present a theatrical experience that is better than what one could achieve now with a traditional 35mm Answer Print.*
- *This system should be based around global standards, or DCI specifications, that are embraced around the world so that content can be distributed and played anywhere in the world as can be done today with a 35mm film print. These standards should be open published industry standards that are widely accepted and codified by national and international standards bodies such as: ANSI, SMPTE, and ISO/IEC. To the extent that it is possible, the Digital Cinema system shall emulate theater operations and the theater business model, as it exists today.*
- *The system specification, global standards and formats should be chosen so that the capital equipment and operational costs are reasonable and exploit, as much as possible, the economies of scale associated with equipment and technology in use in other industries.*
- *The hardware and software used in the system should be easily upgraded as advances in technology are made. Upgrades to the format shall be designed in a way so that content may be distributed and compatibly played on both the latest DCI-compliant hardware and software, as well as earlier adopted DCI-compliant equipment installations.*
- *The Digital Cinema system shall provide a reasonable path for upgrading to future technologies. It shall be based upon a component architecture (e.g., Mastering, Compression, Encryption, Transport, Storage, Playback, Projection) that allows for the components to be replaced or upgraded in the future without the replacement of the complete system. It is the intention of this Digital Cinema specification to allow for advances in technology and the economics of technology advancement. It has been recognized that these advances may most likely affect the mastering and projection of Digital Cinema content. Therefore, this document will specify, for example, a resolution and color space that may not be obtained in a present day mastering or projection system. However, it is the intent that the rest of the Digital Cinema system be capable of transporting and processing up to the technical limits of the specification.*
- *This document specifies a baseline for the implementation of a Digital Cinema system. The goal of backwards compatibility in this context is to allow, for example, new content at higher resolution and color space to be played out on a projection system that meets the baseline implementation.*
- *The Digital Cinema system shall also not preclude the capability for alternative content presentations.*

- *The Digital Cinema system shall provide a reliability and availability that is equal to, or better than, current film presentation.*
- *Protection of intellectual property is a critical aspect of the design of the system. This security system should be designed using a single common encryption format along with keys to decrypt the content. The method should provide a means to keep the content encrypted from the time it is encoded in post-production until it is projected on a theater screen. Only trusted entities, deployed in secure environments or implementing physical protection, will be given access to the decrypted content. Content will be decrypted contingent upon usage rules agreed on by content owners, Distributors and Exhibitors. The system should also be renewable in case of a breach of security in any part of the system, and include forensic Marking of the content for providing traceable forensic evidence in the case of a theft of the content.*

2. SYSTEM OVERVIEW

2.1. Functional Framework

For the purpose of documenting the specific requirements and specifications for a Digital Cinema system, it is helpful to divide the system into a set of components[2], which are:

- Digital Cinema Distribution Master (DCDM) – Contains system requirements regarding the uncompressed, unencrypted file or set of files containing the content and its associated data.
- Compression – Contains system requirements regarding the process that reduces redundancy in source essence data and its inverse, decompression,
- Packaging – Contains system requirements for the process of encryption and decryption of compressed image and audio essence, wrapping and unwrapping of compressed and encrypted files for distribution and playback.
- Transport – Contains requirements related to the distribution of the packaged media.
- Theater System – Contains system requirements for the equipment installed at a theater for control, scheduling, logging and diagnostics.
- Projection – Contains system requirements regarding the performance characteristics used to display the image on the screen.
- Security – Contains system requirements that bear on the protection of content intellectual property rights. Processes for key management, link encryption, Forensic Marking and logging are constituent elements of the security design.

A functional framework of a Digital Cinema encoding and a decoding system are shown below in Figure 1 and Figure 2.

[2] The specifications and performance requirements for each of these components will be described in the subsequent sections.

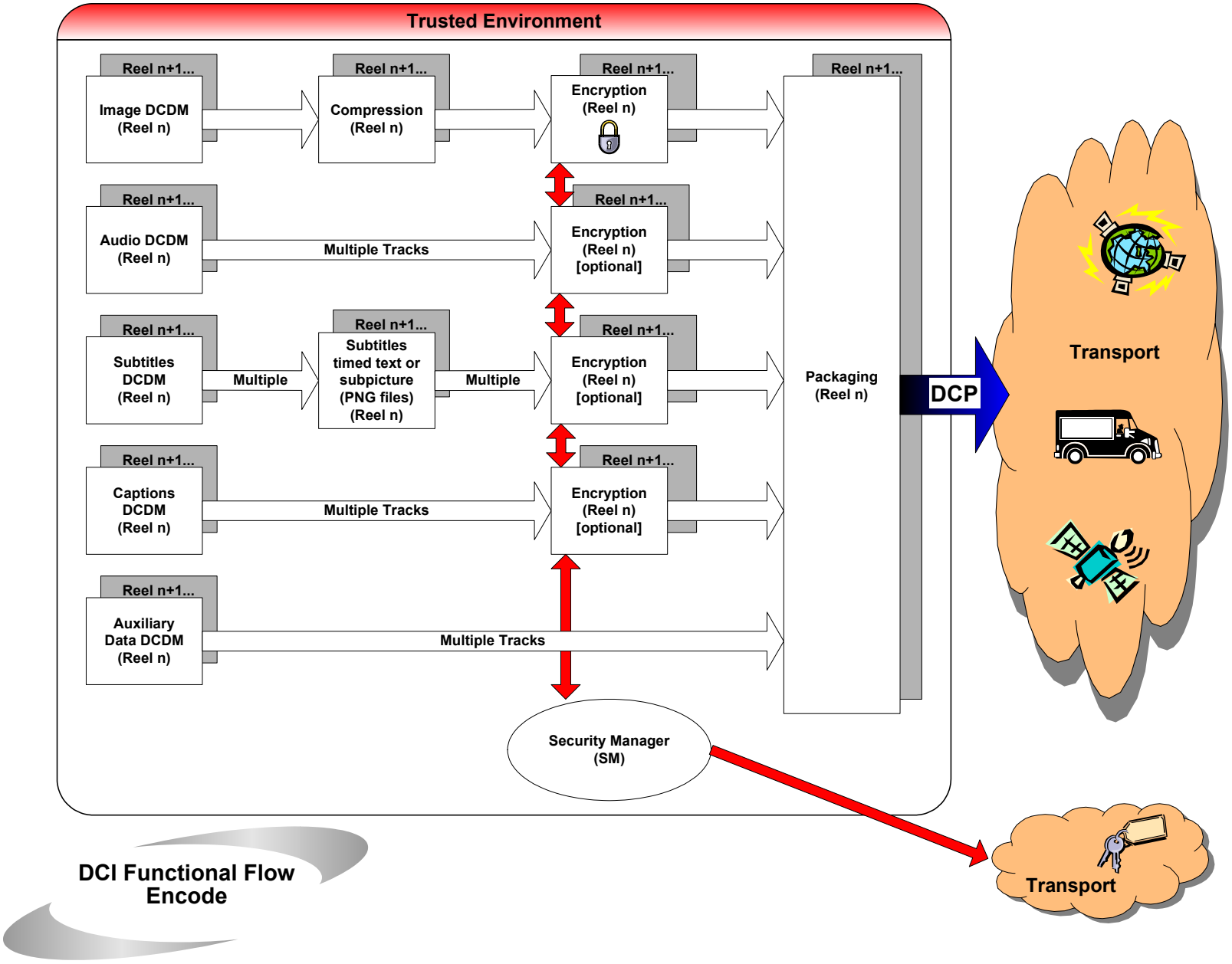

Figure 1: System Overview Functional Encode Flow

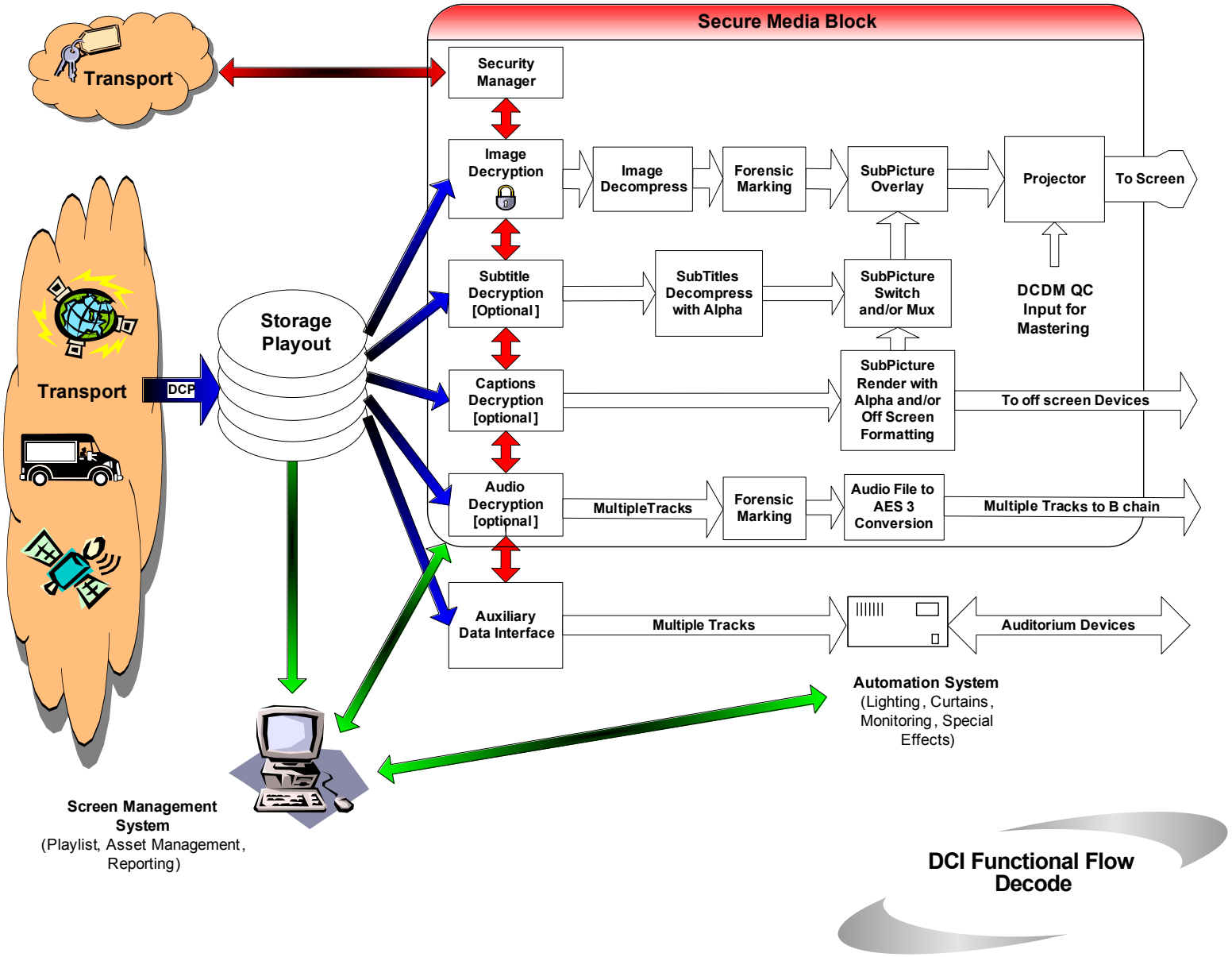

Figure 2: System Overview Functional Decode Flow

2.1.1. Major System Concepts

2.1.1.1. Digital Source Master (DSM)

The Digital Source Master (DSM) is created in post-production and can be used to convert into a Digital Cinema Distribution Master (DCDM). The DSM can also be used to convert to a film duplication master, a home video master, and/or a master for archival purposes. It is not the intention of this document to, in any way, specify the DSM. This is left to the discretion of the content provider. The content could come from a wide range of sources with a wide range of technical levels.

2.1.1.2. Composition

When discussing Digital Cinema content, it was realized that other content besides feature films would make use of the same digital system. Therefore, a new term was created to refer to any content that would have similar requirements to feature film content. The term “Composition” refers to all of the essence and metadata required for a single presentation of a feature, or a trailer, or an advertisement, or a logo to create a presentation using a digital system. This term will be used throughout this document and is intended to refer to a single element such as one and only one feature, trailer, advertisement or logo.

2.1.1.3. Digital Cinema Distribution Master (DCDM)

This document specifies a DCDM for the purpose of exchanging the image, audio, subtitles and auxiliary data to encoding systems and to the Digital Cinema playback system. The DCDM is the output of the Digital Cinema post-production process (not to be confused with the feature post-production process, which creates the DSM) and is the image structure, audio structure, subtitle structure. These structures are mapped into data file formats that make up the DCDM. This master set of files can then be given a quality control check to verify items like synchronization and that the composition is complete. This requires the DCDM files to be played back directly to the final devices (e.g., projector and sound system) in their native decrypted, uncompressed, unpackaged form.

2.1.1.4. Digital Cinema Package (DCP)

Once the DCDM is compressed, encrypted and packaged for distribution, it is considered to be the Digital Cinema Package or DCP. This term is used to distinguish the package from the raw collection of files known as the DCDM. Shown below is a typical flow for Digital Cinema. When the DCP arrives at the theater, it is eventually unpackaged, decrypted and decompressed to create the DCDM*, where DCDM* image is visually indistinguishable from the original DCDM image.

DSM → DCDM → DCP → DCDM* → Image and Sound

Note: Integrated projector and Media Blocks are strongly recommended. However in the exclusive case to accommodate a 2K, 48 FPS, 12 bit DCDM to use [SMPTE 372M Dual Link HD-SDI] as an interface, it is acceptable, but not recommended, to allow 10 bit color sub-sampling to create the DCDM* at the output of the Image Media Block decoder. This bit depth reduction and color subsampling is only allowed in the single combination of a DCDM at 2K, 48 FPS being transported over a link encrypted SMPTE 372M connection.

2.1.1.5. Hierarchical Image Structure

The DCDM shall use a hierarchical image structure that supports both 2K and 4K resolution files (See Section 3.2.1 Image Concepts and Requirements), so that studios can choose to deliver either 2K or 4K masters and both 2K and 4K projectors can be

deployed and supported. The supported mastering and projecting combinations are illustrated in Figure 3,

Media Blocks (MB) for 2K projectors are required to be able to extract and display the 2K-resolution component from the 2K/4K DCP file(s). Media Blocks for 4K projectors are required to be able to output and display the full 4K DCDM. In the case of a 2K DCDM, the output of the Media Block is a 2K image. It is the responsibility of the 4K projectors to up-sample the image.

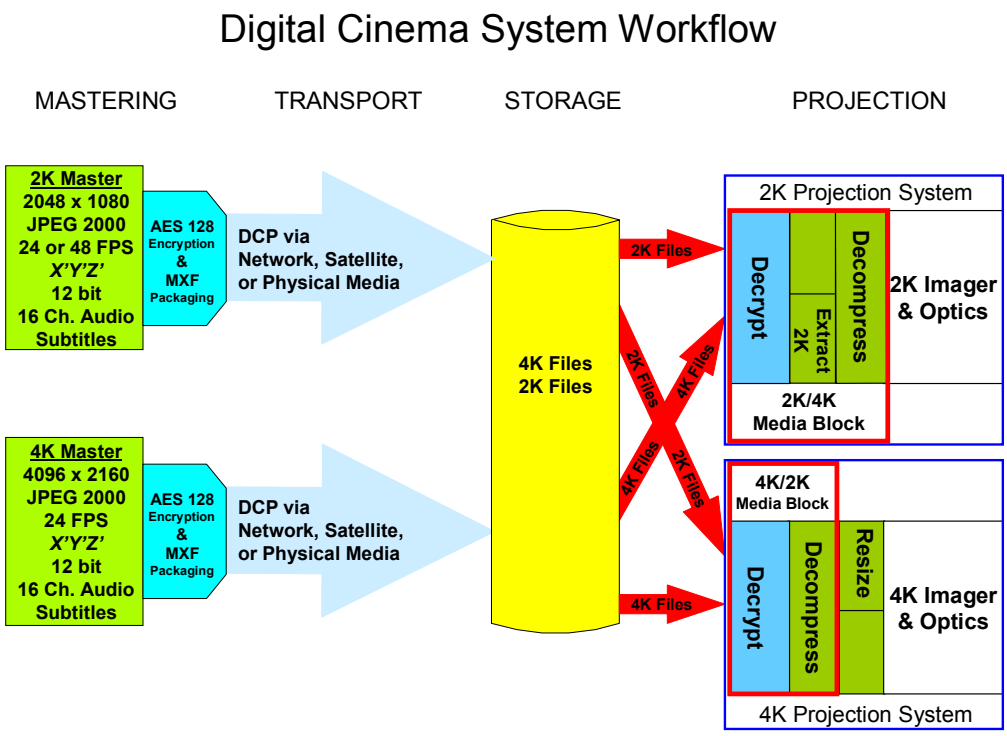

Figure 3: Hierarchical Image Structure

2.1.1.6. File / Frame-Based System

This Digital Cinema system is built upon a data file-based design, i.e., all of the content is made up of data stored in files. These files are organized around the image frames. The file is the most basic component of the system.

2.1.1.7. Store and Forward

This Digital Cinema system uses a store-and-forward method for distribution. This allows the files to be managed, processed and transported in non-real time. Non-real time could be interpreted as slower than real time, or faster than real time. After being transported to the theater, the files are stored on a file server until playback. However, during playback and projection, the Digital Cinema content plays out in real time.

2.1.1.8. Reels

Feature films have been sub-divided for some time into discreet temporal units for film systems called reels. This concept and practice will continue in use for the Digital Cinema system. In Digital Cinema, a reel represents a conceptual period of time having

a specific duration chosen by the content provider. Digital Cinema reels can then be electronically spliced together to create a feature presentation.

2.1.1.9. Component Design

For the purpose of interoperability, the hardware and software used in the Digital Cinema system should be easily upgraded as advances in technology are made. Upgrades to the format should be designed in a way so that content can be distributed and played on the latest hardware and software, as well as earlier DCI-compliant equipment installations.

The Digital Cinema system should provide a reasonable path for upgrading to future technologies. It should be based upon a component architecture (e.g., Mastering, Compression, Encryption, Transport, Storage, Playback, Projection), that allows for the components to be replaced or upgraded in the future without the replacement of the complete system. It is the intention of this Digital Cinema specification to allow for advances in technology and the economics of technology advancement.

2.1.1.10. Storage and Media Block

Storage and Media Block are components of the theater playback system. Storage is the file server that holds the packaged content for eventual playback. The Media Block is the hardware device (or devices) that converts the packaged content into the streaming data that ultimately turns into the pictures and sound in the theater. These two components can be physically contained together or they can be physically separate from each other. Media Blocks are secure enitities and the specific nature of that security is defined in Section 9 SECURITY.

3. DIGITAL CINEMA DISTRIBUTION MASTER

3.1. Overview

3.1.1. Introduction

The Digital Cinema Distribution Master, or DCDM, is a collection of data file formats, whose function is to provide an interchange standard for Digital Cinema presentations. It is a representation of images, audio and other information, whose goal is to provide a complete and standardized way to communicate movies (compositions) between studio, post-production and exhibition. A specific instance of a DCDM is derived from a Digital Source Master (DSM) that is created as a result of a post-production assembly of the elements of a movie (composition). A DCDM can be transformed into a Digital Cinema Package for distribution to exhibition sites (see Section 5 PACKAGING). Alternatively, it can be sent directly to a playback system for quality control tasks.

3.1.2. DCDM System Overview

For the purpose of documenting the specific requirements and specifications for the DCDM, it is helpful to divide the system into a set of components. The specifications and requirements for each of these components will be described in the following sections:

- **Image** – The image specification and file format
- **Audio** – The audio specification and file format
- **Subtitles**
  - **Subpicture** – The pre-rendered open text specification and file format
  - **Timed Text** – The Timed Text data specification and file format
- **Auxiliary Data** – The auxiliary data specification and file format

3.1.3. Major DCDM Concepts

The Digital Cinema Distribution Master (DCDM) is the fundamental interchange element in the system. Since digital mastering technology will continue to change and develop with time, the DCDM is designed to accommodate growth. There are several areas that will be affected by the progression of the mastering technology, such as color space, resolution, sampling frequencies, quantizing bit depths and interfaces.

In the process of creating feature films, a Digital Source Master, or DSM, is produced. The DSM creates many elements (e.g., Film Distribution Masters, DCDM, Home Video Masters and Broadcast Masters). It is not the goal of this specification to define the DSM. Instead, it is recognized that the DSM can be made of any color space, resolution, sampling frequency, color component bit depths and many other metrics.

If the content does not meet this DCDM specification, it is the content provider's responsibility to convert the DSM into the DCDM specification, defined in this section, before it can be used in the Digital Cinema system.

A set of DCDM files (image, audio, subtitles, etc.) contains all of the content required to provide a Digital Cinema presentation. The DCDM provides two functions, an interchange file format, and a playback format that is directly sent from the Media Block to the projector (this is referred to as DCDM*). *For use in interchange, the encoding process can be performed in real time or non-real time. For use in playback, the DCDM* is logically required to playback in real time.*

Metadata within the DCDM provides a method to synchronize image, audio, subtitles and auxiliary data. This method is used to synchronize the tracks in order to maintain frame-based lip sync from the beginning to the end of a presentation. This is different from the requirement to synchronize the system clocks of different pieces of equipment to run at consistent frequencies. The first part addresses the packaging of the picture, sound and subtitles in such a way as to establish and maintain a timing relationship between these tracks of essence. The second part addresses the inter-operability of equipment in a theater system and is therefore discussed in Section 7 THEATER SYSTEMS.

3.1.4. DCDM Fundamental Requirements

3.1.4.1. Common File Formats

The DCDM is required to use a common standardized file format for each element (image, audio, subtitles, etc.). The DCDM image file format is required to be an MXF-conformant file, based on existing SMPTE standards. The DCDM audio file format is required to be based on Broadcast Wave.

3.1.4.2. Frame Rates

The DCDM image structure is required to support a frame rate of 24.000 Hz. The DCDM image structure can also support a frame rate of 48.000 Hz for 2K image content only. The frame rate of any individual DCDM master is required to remain constant. Metadata is carried in the image data file format to indicate the frame rate.

3.1.4.3. Synchronization

Files within the DCDM set are required to carry information to provide for frame-based synchronization between each file. At a minimum, they are required to include a "start of file" and a continuous frame count.

3.2. Image Specification

3.2.1. Image Concepts and Requirements

3.2.1.1. Introduction

This section defines a common interchange for Digital Cinema uncompressed image structures and files. This includes an image structure, aspect ratios, common color space, bit depth, transfer function, and the file format required to present content properly to a Digital Cinema projector.

3.2.1.2. Image Structure

The DCDM shall provide an image structure container that consists of either a 2K (2048 x 1080) or 4K (4096 x 2160) image file as defined in Table 1. It is expected that the image structure shall use one of the two containers such that either the horizontal or vertical resolution is filled. For example, a 4K image file with a 2.39:1 aspect ratio would require an image structure of 4096 x 1714, therefore filling the horizontal resolution of the 4K container. *The pixel orientation, as displayed on the screen, shall be understood to flow from left to right and top to bottom. Also, the horizontal and vertical pixel count shall begin with 0. For example, the top left pixel of the displayed image shall be anotated as (0, 0).*

Container Level	Horizontal Pixels	Vertical Pixels	Container Aspect Ratio	Pixel Aspect Ratio	Frame Rate
1	4096	2160	1.896	1:1	24.00
2	2048	1080	1.896	1:1	48.00
3	2048	1080	1.896	1:1	24.00

Table 1: Image Structure Container

3.2.1.3. Center of Image

The center of the image structure shall correspond to the center of its image structure container stated in Table 1. Horizontally, there will be an equal number of pixels to the left and to the right of the center point. Vertically, there will be an equal number of pixels above and below the center point. For 4K image structure, the center is between horizontal pixel 2047 and 2048 and between vertical pixels 1079 and 1080. For 2K image structure, the center is between horizontal pixel 1023 and 1024 and between vertical pixels 539 and 540.

3.2.1.4. Colorimetry

The color encoding of the Digital Cinema Distribution Master (DCDM) embodies a device-independent, X'Y'Z' color space. Since the DCDM incorporates all of the creative color decisions and these decisions will be made on a calibrated projector in a controlled mastering room, it is by definition an output-referred image state as described in [CIE Publication 15:2004, Colorimetry, 3rd Edition]. The picture is colorimetrically defined for its intended display on the cinema screen.

3.2.1.5. Encoding Primaries

The DCDM shall use the 1931 CIE system of colorimetry [CIE Publication 15.2 (1986) Colorimetry] (x, y coordinates) to describe the color primaries X, Y, and Z as a gamut container (see Table 2).

Encoding Primaries	x	y	u'	v'
X	1.0000	0.0000	4.0000	0.0000
Y	0.0000	1.0000	0.0000	0.6000
Z	0.0000	0.0000	0.0000	0.0000

Table 2: Chromaticity Coordinates[3] of the Encoding Primaries

3.2.1.6. Transfer Function

The CIE XYZ tristimulus values must be calculated with a normalizing constant that sets the Y tristimulus value equal to the absolute luminance[4] in cd/m^2. With this specification of the color, the following equations define the encoding transfer function.[5]

[3] x, y, u', v' refers to the chromaticity coordinates defined by the CIE.

[4] The peak luminance as shown in the transfer function equation is 52.37 cd/m^2. The extra headroom is reserved to accommodate a range of white points including D_{55}, D_{61} and D_{65}, while still supporting the reference white luminance of 48 cd/m^2 as specified in SMPTE 196E for Digital Cinema-Screen Luminance Level, Chromaticity and Uniformity.

[5] The INT operator returns the value of 0 for fractional parts in the range of 0 to 0.4999… and +1 for fractional parts in the range 0.5 to 0.9999…, i.e., it rounds up fractions above 0.5.

$$CV_{X'} = INT\left[4095 * \left(\frac{X}{52.37}\right)^{1/2.6}\right]$$

$$CV_{Y'} = INT\left[4095 * \left(\frac{Y}{52.37}\right)^{1/2.6}\right]$$

$$CV_{Z'} = INT\left[4095 * \left(\frac{Z}{52.37}\right)^{1/2.6}\right]$$

3.2.1.7. Bit Depth

The bit depth for each code value for a color component shall be 12 bits. This yields 36 bits per pixel.

3.2.1.8. Aspect Ratio

Some examples for the accommodation of images of various aspect ratios in the containers are shown in Table 3.

Where:

Ph = number of active horizontal pixels in image

Pv = number of active vertical pixels in image

AR = the aspect ratio of the image (ratio of width to height, expressed as a decimal)

Level	Ph	Pv	AR	Pixel Aspect Ratio
1	4096	1714	2.39	1:1
1	3996	2160	1.85	1:1
2	2048	858	2.39	1:1
2	1998	1080	1.85	1:1

Table 3: Example Image Aspect Ratios

3.2.2. DCDM Image File Format

3.2.2.1. Introduction

The DCDM image file format is mapped into MXF. *A single file shall only contain elements from a single reel.*

3.2.2.2. DCDM Mapping into MXF File Format

The DCDM Image Structure shall be mapped into the MXF file format using [SMPTE 384M, Material Exchange Format (MXF), Mapping of Uncompressed Pictures into the Generic Container], and further constrained as follows:

- The DCDM file structure shall use the frame wrapping method.

- Metadata representing the frame position in sequence or frame count shall be provided for each frame. The remaining items shall be listed once per reel.

3.2.2.3. Synchronization

The DCDM file format is required to contain metadata that indicates the first frame of image. The metadata is required to contain a continuous frame count from the first frame.

3.2.2.4. Image Metadata Required Fields

Image information and parameters, required to successfully interchange the DCDM Image Structure, shall be provided to the transport mechanism that will contain the DCDM. Since the DCDM may use different methods for transport, it is not appropriate at this time to specify the metadata format for the following information. It is up to the transport file or interface to map the information into its own format.

The information, as shown in Table 4, is the minimum required information to successfully interchange files.

Data Element Name	Data Element Definition
Active Horizontal Pixels (Ph)	Total number of active horizontal pixels in the image container
Active Vertical Pixels (Pv)	Total number of active vertical pixels in the image container
DCDM Container Level	The number of the DCDM container level of the container used
Frame Rate	The rate that images are to be projected, expressed in frames per second

Table 4: Required Image Structure Information

3.3. Audio Specification

3.3.1. Audio Concepts and Requirements

Digital Cinema audio requires standardized characteristics, channel mapping and a file format to successfully playback in a motion picture theater.

3.3.2. Audio Characteristics

3.3.2.1. Introduction

The necessary characteristics for standardized audio are: bit depth, sample rate, reference level and channel count. These parameters are given below.

3.3.2.2. Bit Depth

The bit depth shall be 24 bits per sample. Material having other bit depths shall be justified to the most significant bit per [AES3-2003 Section 4.1.1].

3.3.2.3. Sample Rate

Irrespective of the associated image frame rate, the audio sample rate shall be either forty-eight or ninety-six thousand samples per second per channel, commonly expressed as 48.000 or 96.000 kHz. At 24 FPS playback, there are exactly 2,000 audio samples per frame for 48.000 kHz and exactly 4,000 audio samples per frame for 96.000 kHz. At 48 FPS playback, there are exactly 1,000 audio samples per frame for 48.000 kHz and exactly 2,000 audio samples per frame for 96.000 kHz.

A theater playback system shall have the capability of performing sample rate conversion as needed.

3.3.2.4. Channel count

The delivered digital audio, contained within the Digital Cinema Package (DCP), shall support a channel count of sixteen full-bandwidth channels.

3.3.2.5. Digital Reference Level

Digital inputs and outputs shall have a nominal reference level of -20 dBFS (decibel below full scale) and output 85 dBc (decibels refenced to the carrier) sound pressure level per channel measured with pink noise.

3.3.3. Channel Mapping

Channel mapping defines where the individual audio channels are assigned and the labeling of channels in a Digital Cinema audio system. This is done to aid in the identification and the location of channels, thus, enabling uniform expression and communication of source audio channels to Digital Cinema playback loudspeakers. The general parameters for 8 and 6 channel mapping are given in Table 5 and Table 6 for reference. Suggested speaker placement for a Digital Cinema auditorium is shown in Figure 4.

AES Pair#/Ch#	Channel #	Label / Name	Description
1/1	1	L/Left	Far left screen loudspeaker
1/2	2	R/Right	Far right screen loudspeaker
2/1	3	C/Center	Center screen loudspeaker
2/2	4	LFE/Screen	Screen Low Frequency Effects subwoofer loudspeakers
3/1	5	Ls/Left Surround	Left wall surround loudspeakers
3/2	6	Rs/Right Surround	Right wall surround loudspeakers
4/1	7	Lc/Left Center	Mid left to center screen loudspeaker
4/2	8	Rc/Right Center	Mid right to center screen loudspeaker
5/1	9		Unused
5/2	10		Unused/User Defined
6/1	11		Unused/User Defined
6/2	12		Unused/User Defined
7/1	13		Unused/User Defined
7/2	14		Unused/User Defined
8/1	15		Unused/User Defined
8/2	16		Unused/User Defined

Table 5: Eight Channel Mapping

AES Pair#/Ch#	Channel #	Label / Name	Description
1/1	1	L/Left	Far left screen loudspeaker
1/2	2	R/Right	Far right screen loudspeaker
2/1	3	C/Center	Center screen loudspeaker
2/2	4	LFE/Screen	Screen Low Frequency Effects subwoofer loudspeakers
3/1	5	Ls/Left Surround	Left wall surround loudspeakers
3/2	6	Rs/Right Surround	Right wall surround loudspeakers
4/1	7		Unused
4/2	8		Unused
5/1	9		Unused
5/2	10		Unused/User Defined
6/1	11		Unused/User Defined
6/2	12		Unused/User Defined
7/1	13		Unused/User Defined
7/2	14		Unused/User Defined
8/1	15		Unused/User Defined
8/2	16		Unused/User Defined

Table 6: Six Channel Mapping

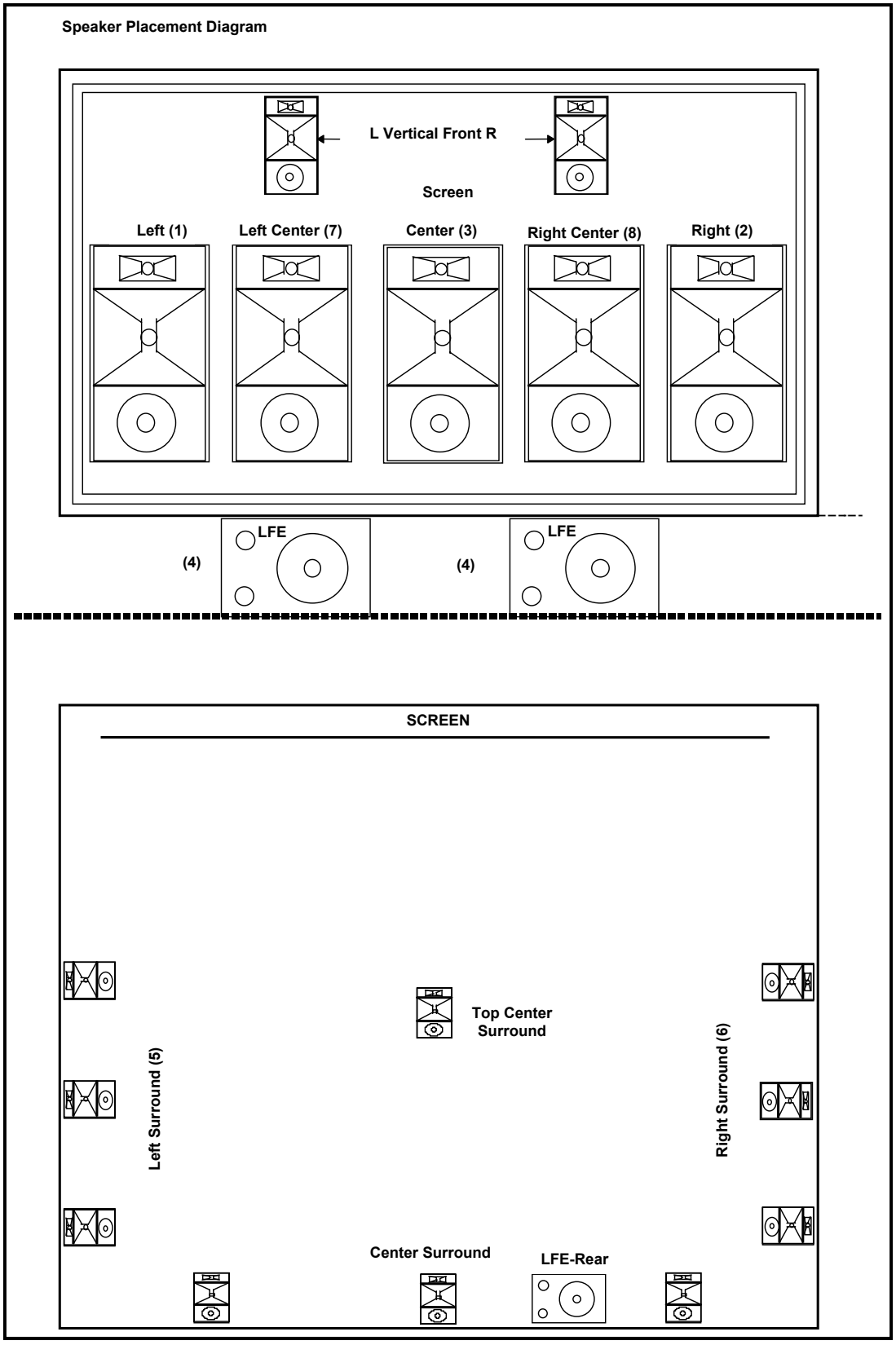

Figure 4: Suggested Auditorium Speaker Placement

3.3.4. File Format

3.3.4.1. General

The audio file format shall comply with the Broadcast Wave file format (.wav), per [ITU Tech 3285 version 1 (PCM WAVE coding)], is extended and constrained as further described here.

The audio file shall remain uncompressed throughout the Digital Cinema system. This shall include packaging, distribution and storage.

3.3.4.2. Synchronization

The Broadcast Wave (.wav) file is required to contain metadata that indicates the first sample of audio data. The metadata is also required to contain a continuous frame count relative to the image as well as the sample rate.

3.3.4.3. Dynamic Downmixing

The file format, or packaging format, is required to provide a metadata flag (Yes/No condition) to indicate whether dynamic down mixing is allowed. If dynamic downmixing is allowed, then metadata is required to be provided to accomplish this task. This metadata is required to not be modified in any way.

Dynamic downmixing could be used in the cases of a theater's playback system that receives a 7.1 mix with the capability of supporting only a 5.1 mix. During post-production, one could create a dynamic downmixing for such a condition using metadata that could be sent with the audio file.

3.3.4.4. Dynamic Range Control

The file format, or packaging format, is required to provide a metadata flag (Yes/No condition) to indicate whether dynamic range control is allowed. If dynamic range control is allowed, then metadata is required to be provided to accomplish this task. This metadata is required to not be modified in any way.

Dynamic range control could be used in the cases of a theater's playback system where the operator might want to limit the sound level not to exceed 95 dBc sound pressure level.

3.4. Text Rendering

3.4.1. Text Rendering Concepts and Requirements

Digital Cinema has a subtitling system that can convey multiple languages. Along with subtitling, there are text localizations, titling and captioning that may also be a part of the new Digital Cinema experience. However, captioning and subtitling are identified as two separate systems having different roles in the presentation of contentand may have different methods of rendering.

Traditionally, the audience for captioning is the deaf and hard of hearing (D/HOH). The delivery can be done in different ways. These include closed systems that are optional-to-the-viewer delivery and are usually displayed on a personal device (such as a wireless receiver), or delivery to an obscured device that is viewable with an appliance (such as a rear-wall display viewed through a mirror).

Subtitling is generally associated with a foreign language translation for localizing a movie in a particular geopraphic territory. Subtitles are typically open or displayed on the screen as part of the movie, without option. Subtitling and ocalizations are generally designed for a particular look with creatively chosen fonts and drop shadows.

With captioning, the source language (what is spoken in the movie) and the target language (what appears as captions) are most often, as in the case of English, the same. For subtitling, the source language and target language are different because the goal of subtitling is to translate the movie.

Subtitles and captions, if supplied, may be one or more of the following:

- *Pre-composited into the Digital Cinema image files (burned-in)*
- *Pre-rendered PNG bitmaps (subpicture), or*
- *Documents containing text and attributes for:*
    - *Rendering in a specified font (Timed Text) and overlaid by the server, an in-line processor or the Digital Cinema projector*
    - *LED displays driven by a captioning processor receiving data from the Digital Cinema server, or*
    - *Separate projection systems driven by a captioning processor receiving data from the Digital Cinema server*

Section 3.4.2 Subpicture defines the subpicture specifications, while Section 3.4.3 Timed Text Concepts and Requirements defines the specification for Timed Text streams, which can be used for either subtitles or captions or both. Burned-in subtitles are not addressed since they are something that would occur in the mastering of the content and would be inherent in the image.

3.4.2. Subpicture

3.4.2.1. Introduction

A subpicture data stream is a multiple-image data stream intended for the transport of visual data supplemental to a motion picture. The data is designed for graphic overlay with the main image of a Digital Cinema motion picture. It is designed only for an open display and not for a closed display. It is envisoned that the subpicture data stream, when employed, will typically be used for the transport of subtitle data.

3.4.2.2. File Format

Subpicture data is required to be encoded as a standardized, XML-based document. Such a standard is required to define both Timed Text and subpicture encoding methods allowing mixed-media rendering. Subpicture frames are required to be encoded as [ISO/IEC 15948:2004] PNG files.

3.4.2.3. Rendering Intent

The PNG file is required to be rendered with knowledge of color space and pixel matrix of the DCDM. The PNG file is required to be mastered at the same resolution as the DCDM.

For example, a DCP containing a 4K master will require 4K PNG files and no other resolution PNG files. When played on a 2K projector, it is the responsibility of the 2K projector to downsample the 4K PNG files such that they display with the correct size with respect to the image data. And, a DCP containing a 2K master will require 2K PNG files and no other resolution PNG files. When played on a 4K projector, it is the responsibility of the 4K projector to upsample the 2K PNG files appropriately.

3.4.2.4. Frame Rate and Timing

The XML navigation file specifies the temporal resolution of the subpicture file. *A Frame count, Time In, Time Out, Fade Up Time and Fade Down Time, which correspond to the*

image, shall be included. The subpicture frame rate shall be equal to the frame rate of the associated DCDM image file.

3.4.2.5. Synchronization

The equipment or system that encodes or decodes the subpicture file is required to ensure that temporal transitions within the subpicture file are correctly synchronized with other associated DCDM files. The Digital Cinema equipment and subpicture file is required to re-synchronize after a restart of the system.

3.4.3. Timed Text Concepts and Requirements

3.4.3.1. Introduction

Timed Text (e.g., captions and/or subtitles) is text information that may be presented at definite times during a Digital Cinema presentation.

3.4.3.2. File Format

Timed Text data is required to be encoded as a standardized, XML-based document.

Note: This provides for presentation via:

- Overlay in main or secondary projector image (open), or
- External display (closed)

3.4.3.3. Character Sets

The Timed Text file format is required to support the full range of the Unicode™[6] character set.

3.4.3.4. Restart

The Digital Cinema equipment and Timed Text file is required to re-synchronize after a restart of the system.

3.4.3.5. Default Font

Font files are required to be used to render Timed Text for subtitle applications. Font files can be used to render Timed Text for caption applications. *When used, font files are required to conform to [ISO/IEC 00000 OpenType[7]]. Timed Text files are required to be accompanied by all font files required for reproduction of the Timed Text.*

The Timed Text file format is required to support a default character set. It is required that there be a default Unicode™ character set and a default font for that character set.

In event that an external font file is missing or damaged, the subtitle rendering device is required to use a default font supplied by the manufacturer. The default character set is required to be a Unicode™ ISO Latin-1 character set. The default font is required to conform to [ISO/IEC 00000 OpenType] and support the ISO Latin-1 character set.

3.4.3.6. Identification

The Timed Text format requires the cardinal language of the text to be identified.

[6] The Unicode Consortium. The Unicode Standard, Version 4.0.1, defined by: The Unicode Standard, Version 4.0 (Reading, MA, Addison-Wesley, 2003. ISBN 0-321-18578-1), as amended by Unicode 4.0.1 (http://www.unicode.org/versions/Unicode4.0.1/)
[7] OpenType specification is a work-in-progress. Number will be added when completed.

3.4.3.7. Searchability

A pure text stream is encouraged to isolate content from rendering markup for searchability.

3.4.3.8. Multiple Captions

The Timed Text format shall allow the display of multiple captions simultaneously. There shall be a maximum number of 3 lines of text allowed for simultaneous display.

Note: This allows for spatial representation for captions when two people are talking simultaneously.

3.4.3.9. Synchronization

The equipment or system that encodes or decodes the Timed Text file is required to ensure that temporal transitions within the data stream are correctly synchronized with other associated DCDM data streams.

3.4.4. Auxiliary Data Concepts and Requirements

Current day control systems, usually called automation systems, orchestrate theater sub-systems such as curtains, masking and lights. Digital Cinema control methods are expected to differ significantly from those found in theaters today. Supervisory types of control will be much broader in application than in today's systems, allowing interface to specialized controls for theatrical events.

Many of these concepts and requirements are covered in Section 5 PACKAGING and Section 7 THEATER SYSTEMS. Some of the fundamental information pertaining to encoding is covered here, with the detailed information for its use covered in Section 7 THEATER SYSTEMS.

3.4.5. Show Controls

3.4.5.1. Introduction

Many of today's automation controls are driven by a time-based event list such as the system's Show Playlist, and can be classified by their show control functions, as in the partial list below.

- First frame of content
- First frame of intermission
- First frame of end credits
- First frame of end credits on black
- Last frame of content

Show control events or cues are required for the theater system operator to pre-program the timing of show control events. Such events or cues may indicate events such as the beginning of the title, beginning of the intermission, beginning of the credits, and the end of the feature. The events or cues will normally be placed into the Digital Cinema Composition Playlist, as defined in Section 5 PACKAGING. If more extensive show control is required, then a show control DCDM auxiliary data file can be used.

3.4.5.2. DCDM Auxiliary Data File Format

An Auxiliary Data File may be included. If present, the format shall fully conform with [SMPTE Standard for Television 12M, Audio and Film-Time and Control Code]. Using this method, control information may be imbedded into the user bits of the 24 FPS LTC time code.

4. COMPRESSION

4.1. Introduction

Image Compression for Digital Cinema uses data reduction techniques to decrease the size of the data for economical delivery and storage. The system uses perceptual coding techniques to achieve an image compression that is visually lossless. It is important to note that image compression is typically used to ensure meeting transmission bandwidth or media storage limitations. This results in image quality being dependent on scene content and delivered bit rate. Digital Cinema image compression is much less dependent upon bandwidth or storage requirements, thereby making bit rate dependent on desired image quality rather than the reverse.

4.2. Compression Standard

The compression standard shall be JPEG 2000 (see [ISO/IEC 15444-1]).

4.3. Decoder Specification

4.3.1. Definitions

- A 2K distribution – the resolution of the DCDM*[8] container is 2048 x 1080.
- A 4K distribution – the resolution of the DCDM*[8] container is 4096 x 2160.
- A 2K decoder outputs up to 2048 x 1080 resolution data.
- A 4K decoder outputs up to 4096 x 2160 resolution data from a 4K compressed file and outputs up to 2048 x 1080 resolution data from a 2K compressed file.
- *All decoders shall decode both 2K and 4K distributions.* It is the responsibility of the 4K projector to upres the 2K file. In the case of a 2K decoder and a 4K distribution, the 2K decoder need read only that data necessary to decode a 2K output from the 4K distribution. The decoder (be it a 2K decoder or a 4K decoder) need not up-sample a 2K image to a 4K projector or down-sample a 4K image to a 2K projector.

4.3.2. Decoder Requirements

- *Once deployed, the decoder, for any given projector, shall not be required to be upgraded.*
- *The output of the decoder shall conform to Section 3.2 Image Specification.* These images are basically:
  - 4K = 4096 x 2160 at 24 FPS
  - 2K = 2048 x 1080 at 24 or 48 FPS
  - Color: 12 bit, X'Y'Z'
- *Enhanced parameter choices shall not be allowed in future distribution masters, if they break decodability in a deployed compliant decoder.*
- *All decoders shall decode each color component at 12 bits per sample with equal color/component bandwidth. Decoders shall not subsample chroma.*
- *A 4K decoder shall decode all data for every frame in a 4K distribution. A decoder shall not discard data (including resolution levels or quality layers) to keep up with peak decoding rates.*

[8] The DCP arrives at the theater, it is unpackaged, decrypted and decompressed to create the DCDM*, where DCDM* is visually indistinguishable from the original DCDM (where the orginal DCDM is the input to the Digital Cinema Mastering process).

- *A 2K decoder shall decode 2K data for every frame in a 4K distribution and it shall decode a 2K distribution. It may discard only the highest resolution level of a 4K distribution. It shall not discard other data such as further resolution levels or quality layers.*
- *All decoders shall implement the 9/7 inverse wavelet transform with at least 16 bit fixed point precision.*
- *All decoders shall implement the inverse Irreversible Color Transform (ICT) using at least 16 bit fixed point precision.*

4.4. Codestream Specification

All codestreams shall fully conform with [ISO 15444-1:2004/PDAM 1 (soon to be Amendment 1)], as more fully constrained as follows:

- *All image frames shall be untiled. More precisely, the entire image shall be encoded as a single tile.*
- *The image and tile origins shall both be at (0, 0).*
- *There shall be no more than 5 wavelet transform levels for 2K content and no more than 6 wavelet transform levels for 4K content. There shall be no less than one wavelet transform level for 4K content. Additionally, every color component of every frame of a distribution shall have the same number of wavelet transform levels.*
- *Codeblocks shall be of size 32x32.*
- *The codeblock coding style shall be SPcod, SPcoc = 0b00000000.*
- *All precinct sizes at all resolutions shall be 256x256, except the lowest frequency subband, which shall have a precinct size of 128x128.*
- *There shall be no region of interest, i.e., Region of interest (RGN) marker segments are disallowed.*
- *Coding style Default (COD), Coding style Component (COC), Quantization Default (QCD), and Quantization Component (QCC) marker segments shall appear only in the main header.*
- *Packed Packet headers, Main header (PPM) and Packed Packet headers, Tile-part header (PPT) marker segments are forbidden.*
- *The progression order for a 2K distribution shall be Component-Position-Resolution-Layer (CPRL). Progression Order Change (POC) marker segments are forbidden in 2K distributions.*
- *For a 4K distribution, there shall be exactly one POC marker segment in the main header. Other POC marker segments are forbidden. The POC marker segment shall specify exactly two progressions having the following parameters:*
    - First progression:
      RSpoc = 0, CSpoc = 0, LYEpoc = L, REpoc = D, CEpoc = 3, Ppoc = 4
    - Second progression:
      RSpoc = D, CSpoc = 0, LYEpoc = L, REpoc = D+1, CEpoc = 3, Ppoc = 4
    - In the above, D is the number of wavelet transform levels and L is the number of quality layers. The constant 3 specifies the number of color components, and the constant 4 specifies CPRL progression.

  Note: This POC marker segment ensures that all 2K data precede all 4K data. Within each portion (2K, 4K), all data for color component 0 precede all data for color component 1, which in turn precede all data for color component 2.

- *Each compressed frame of a 2K distribution shall have exactly 3 tile parts. Each tile part shall contain all data from one color component.*
- *Each compressed frame of a 4K distribution shall have exactly 6 tile parts. Each of the first 3 tile parts shall contain all data necessary to decompress one 2K color component. Each of the next 3 tile parts shall contain all additional data necessary to decompress one 4K color component. The resulting compliant codestream structure is diagramed in Table 7. Assuming D wavelet transform levels (D+1 resolutions), the box labeled 2K_i (i = 0, 1, 2) contains all JPEG 2000 packets for color component i, resolutions 0 through D-1. The box labeled 4K_i (i = 0, 1, 2) contains all JPEG 2000 packets for color component i, resolution D.*

Main Header	Tile-part Header	2K_0	Tile-part Header	2K_1	Tile-part Header	2K_2	Tile-part Header	4K_0	Tile-part Header	4K_1	Tile-part Header	4K_2

Table 7: Codestream Structure

- *Tile-part Lengths, Main header (TLM) marker segments shall be required in all frames of all distributions.*

  Note: This facilitates extraction of color components and resolutions (2K vs. 4K).
- *Distribution masters shall have exactly one quality layer.*
- *For a frame rate of 24 FPS, a 2K distribution shall have a maximum of 1,302,083 bytes per frame (aggregate of all three color components). Additionally, it shall have a maximum of 1,041,666 bytes per color component per frame.*

  Note: For information purposes only, this yields a maximum of 250 Mbits/sec total and a maximum of 200 Mbits/sec per color component.
- *For a frame rate of 48 FPS, a 2K distribution shall have a maximum of 651,041 bytes per frame (aggregate of all three color components). Additionally, it shall have a maximum of 520,833 bytes per color component per frame.*

  Note: For information purposes only, this yields a maximum of 250 Mbits/sec total and a maximum of 200 Mbits/sec per color component.
- *A 4K distribution shall have a maximum of 1,302,083 bytes per frame (aggregate of all three color components). Additionally, the 2K portion of each frame shall satisfy the 24 FPS 2K distribution requirements as stated above.*

  Note: For information purposes only, this yields a maximum of 250 Mbits/sec total and a maximum of 200 Mbits/sec per color component.

THIS PAGE LEFT BLANK INTENTIONALLY

5. PACKAGING

5.1. Introduction

The DCDM, as stated in the System Overview, is a collection of files, such as picture essence files and audio essence files. These files, as they stand by themselves, do not represent a complete presentation. Synchronization tools, asset management tools, metadata, content protection and other information are required for a complete presentation to be understood and played back as it was intended. This is especially important when the files become compressed and/or encrypted and are no longer recognizable as image essence or audio essence in this state. Packaging is a way to organize and wrap this material in such a way as to make it suitable for storage and transmission to its destination, where it can be stored and then easily unwrapped for a coherent playback. In seeking a common interchange standard for Digital Cinema between post-production and exhibition, it is understood that there may be multiple sources of content, distributed by more than one distributor, shown in a single show. This will require special consideration to achieve DCP interchange. Thus, an interchange packaging structure is needed that operates across several domains. The section also provides a set of requirements for the Material eXchange Format (MXF) track file encryption. These requirements are complementary to the requirements in Section 9.7 Essence Encryption and Cryptography.

5.2. Packaging System Overview

5.2.1. Functional Framework

For the purpose of documenting the specific requirements for a Digital Cinema Packaging system, it is helpful to divide the system into a set of components. The performance requirements for each of these components will be described in the following sections:

- **Composition** – A self-contained representation of a single complete Digital Cinema work, such as a motion picture, or a trailer, or an advertisement, etc.
- **Distribution Package** – The physical files and the list describing the files and providing a means for authentication as delivered in a Distribution Package (from Distributor to Exhibitor).

5.2.2. Packaging Fundamental Requirements

5.2.2.1. Introduction

Digital Cinema presents a challenge to create a versatile packaging system. Throughout this system, some basic requirements are needed and are stated below.

5.2.2.2. Open Standard

The Packaging standard is required to be based upon an open worldwide standard. This format is encouraged to be a license-free technology. It is required to be a complete standard that equipment receiving a compliant package can process and interpret unambiguously.

5.2.2.3. Interoperable

The Packaging format is required to have an open framework that accommodates compressed, encrypted files as well as all other files used in Digital Cinema.

5.2.2.4. Scalable

The Packaging format is required to accommodate any number of essence or metadata components. There is no limit on the number of files included in the package or the size of the files.

5.2.2.5. Supports Essential Business Functions

The Packaging format is required to support content structure as needed during booking, fulfillment, show preparation, booking updates, secure licensed playback and logging.

5.2.2.6. Secure

The Packaging format is required to support integrity and security at two levels: (1) a basic level which can provide reasonable assurance of file integrity without reference to licenses or a Security Manager (SM), and (2) an engagement-specific level representing a particular business-to-business relationship.

5.2.2.7. Extensible

The Packaging format is required to allow for new Digital Cinema features (compositions) to be contained within the package.

5.2.2.8. Synchronization

The Packaging format is required to provide support for synchronization of the essence and metadata elements.

5.2.2.9. Human Readable Metadata

Human readable metadata is required to be in English (default) but can be provided in other languages as well.

5.2.3. Packaging Concepts

It is common practice to divide a feature film into reels of between 10 and 20 minutes in length for post-production, and distribution. These reels are then assembled, together with other content, to create the modern platters that are used in exhibition today. *This concept of reels is required to be supported with Digital Cinema content.*

The Digital Cinema Packaging System is built on a hierarchal structure. The most basic element of the packaging system begins with track files. These are the smallest elements of a package that can be managed or replaced as a distinct asset. *A track file can contain essence and/or metadata. Its duration is set to be convenient to the processes and systems that utilize it.* These can be image tracks, audio tracks, subtitle tracks or any other essence and/or metadata tracks. A Composition Playlist specifies the sequence of track files that create sequence conceptual reels into a composition. This is illustrated in Figure 5.

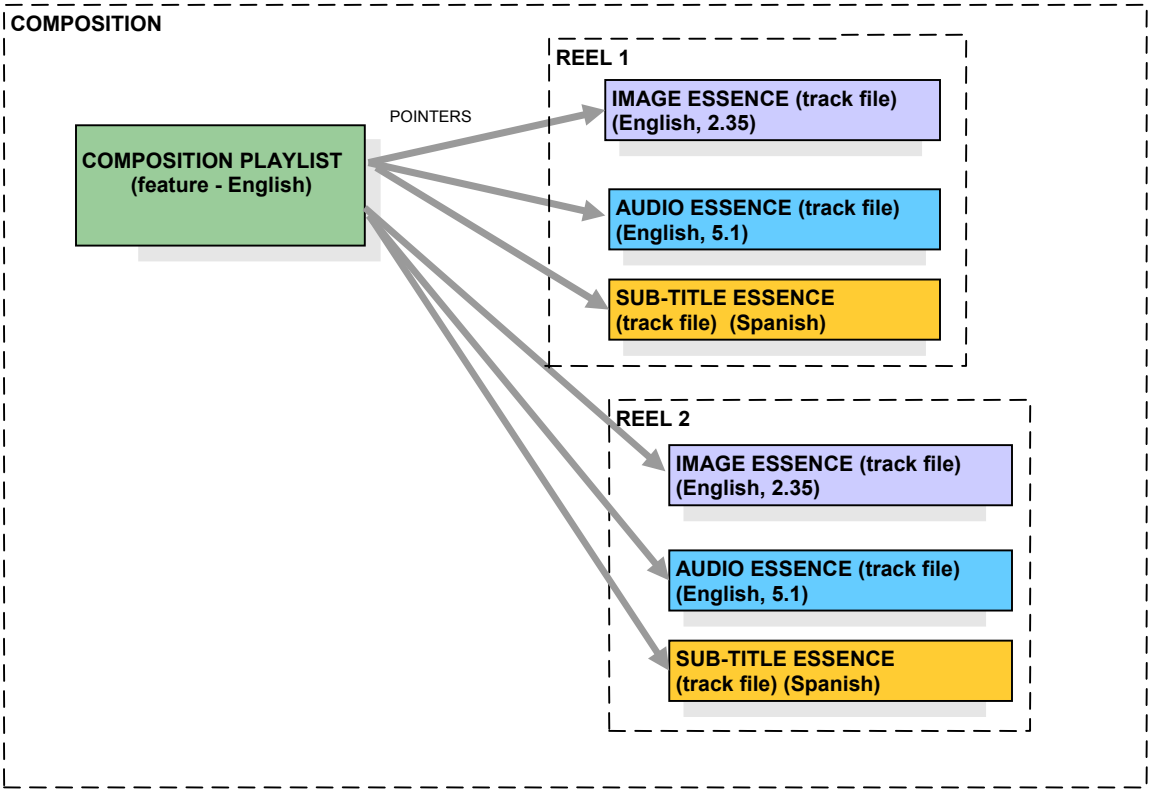

Figure 5: Example Composition Playlist

A Composition Playlist is created in the Digital Cinema mastering process to assemble a complete Composition. This Composition consists of all of the essence and metadata required for a single presentation of a feature, or a trailer, or an advertisement, or a logo. A single Composition Playlist contains all of the information on how the files are to be played, at the time of a presentation, along with the information required to synchronize the track files. A Composition Playlist could consist of one reel or many reels. *The Composition Playlist is digitally signed, such that any modification to the Composition Playlist may be reported back to the Security Manager (see Section 9.4.2.4 Security Manager (SM)).* There is a separate Composition Playlist for each version or language audio track of a motion picture/feature (composition). For example, a DCP of a feature film for the European market with French, Italian, German and Spanish audio tracks would contain four separate Composition Playlists, one for each sound track.

At the exhibition site, the Theater Management System (TMS) or Screen Management System (SMS) assembles the Show Playlist. A Show Playlist is created from individual Composition Playlists. *The Show Playlist can also be created either on-site or off-site and interchanged as a file to one or more Screen Management Systems.* One could have multiple Playlists as well. Figure 6 is an example of a Show Playlist consisting of multiple Composition Playlists.

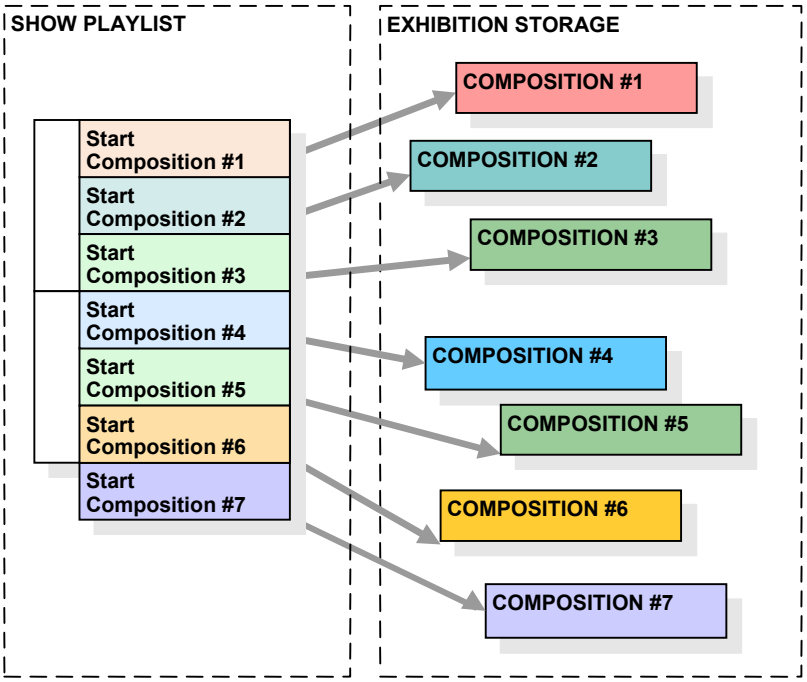

Figure 6: Example Show Playlist

The final element in the Packaging system is a Packing List for the distribution package. The Packing List contains information and identification about each of the individual files that will be delivered in a Digital Cinema Package (DCP). This allows for asset management and validation, including cryptographic integrity checking, for the received DCP. A feature can be sent in a single DCP or multiple DCPs and therefore could be listed in one or more Packing Lists. The Packing List can be sent ahead of the DCP, for asset management purposes. A diagram of a Packing List structure is shown in Figure 7.

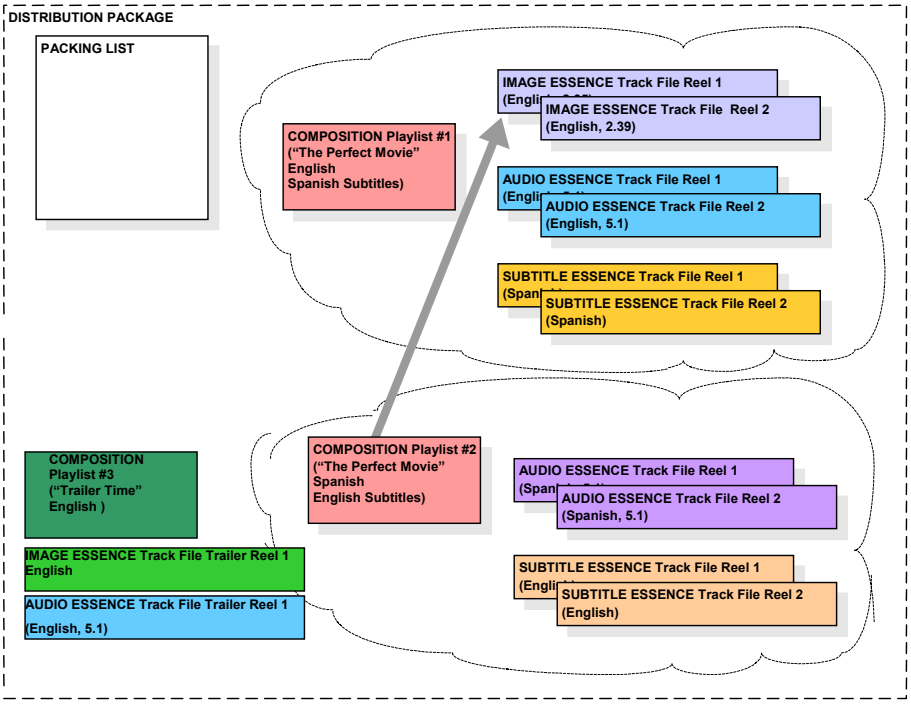

Figure 7: Example Distribution Package

5.3. Composition

5.3.1. Track File Concepts and Requirements

5.3.1.1. Introduction

The Sound and Picture Track File is the fundamental element in the Digital Cinema packaging system. The Sound and Picture Track File structure and requirements are defined by the essence or metadata that they contain. Each of these essence or metadata containers could be image, sound, subtitle (Timed Text, and/or subpicture), caption or auxiliary data. However, each track file follows the same basic file structure. A track file consists of three logical parts: the File Header, the File Body and the File Footer as shown in Figure 8.

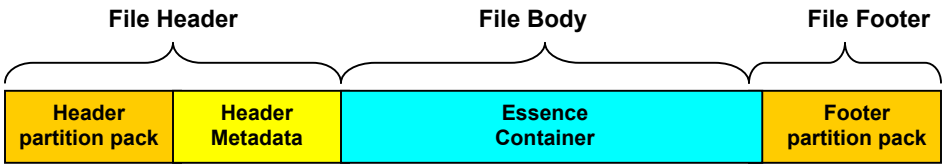

Figure 8: Example Track File Structure

The file structure is further broken down into logical data items as defined in [SMPTE 336M Data Encoding Protocol using Key-Length-Value]. The KLV Coding Protocol is composed of Universal Label (UL) identification Key (UL Key), followed by a numeric Length (Value Length), followed by the data Value as shown below in Figure 9. One or more of these data items are combined to form the logical parts shown above.

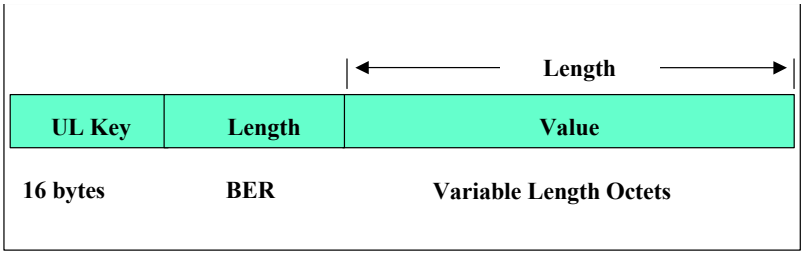

Figure 9: Example of KLV Coding

5.3.1.2. Format Information

Each track file is required to be a self-contained element, such that it's essence or metadata can be understood and presented as it was packaged by a compliant decoder. The information is required to be located in the predetermined specified area. The Track File is required to contain the following minimum information:

- Required metadata for unique asset identification
- Required metadata for decompression (optional)
- Required metadata for decryption (optional)

The following information is required to be configured in a human readable format:

- Essence physical format description. (e.g., 4096 x 2160)
- Essence title asset information. (e.g., The_Perfect_Movie_English_ R2)

5.3.1.3. Reel

A Reel is a conceptual period of time having a specific duration, as defined below:

- *Track Files are required to be associated with a particular Reel.*
- *A Track File is required to not cross over a reel boundary that is a playable portion of a track file, between the mark in and mark out points.*
- *Reels are required to be composed of one or more Track Files.*
- *The minimum duration of a Track File is required to be an integer number of frames, such that the length is greater than or equal to one (1) second.*

5.3.1.4. Track File Replacement

A Track File is the smallest unit that can be managed or replaced as a discrete file in the field. A Track File length is always equal to its associated Reel length.

5.3.1.5. Synchronization

Each Track File is required to contain the following synchronization information:

- Start of Essence Data (mark in)
- End of Essence Data (mark out)
- Track File Frame Count
- Frame Rate
- Internal Synchronization

5.3.1.6. Splicing

Track Files, of the same essence type, are required to allow for seamless or click-free splicing to create a continuous data stream for a presentation. The playback system is required to be able to perform sample accurate or click free splicing of audio track files. (See Section 7 THEATER SYSTEMS for sample accurate playback requirements.)

5.3.1.7. Key Epoch

A Key Epoch is the period of time during which a given Decryption Key is effective. The Key Epoch is one Reel.

5.3.1.8. Security

Each Track File is required to provide for encryption and methods to authenticate the data, if the content provider chooses to use such methods. In addition:

- *The essence container is required to allow encrypted data, while the rest of the Track File metadata is left unencrypted.*
- *At any point in the delivery chain, it is required to be possible to detect whether any accidental or intentional alteration has occurred.*

5.3.1.9. Integrity and Authentication

Each Track File is required to provide a method for verification of file integrity that can be easily determined at any step of the delivery process. In addition:

- *It is encouraged that missing or corrupted data be easily identified.*
- *Track Files are encouraged to be subdivided into smaller segments, which have individual authenticity/error-check codes. This facilitates a decision as to whether the file is so corrupt it cannot be played, or whether it is safe to proceed with playback while requesting a replacement Track File.*

- *Synchronization with other Track Files is encouraged to be verifiable.*

5.3.1.10. Extensibility

The Operational Pattern is required to accommodate future extensions within its original scope.

5.3.1.11. Random Access and Restarts

The Operational Pattern is required to support random access to the nearest integer minute. Random access to individual frames is neither required nor desired.

A restart occurs as a result of a stop or pause in the system while executing a Composition Playlist. *The system may be restarted at any frame prior to the frame at which it was stopped or paused. It is required that a restart be logged by the Security Manager, provided that the essence (either image, audio or subtitle) is encrypted.*

5.3.1.12. Simple Essence

A track file is required to contain essence of a single essence type (e.g., audio, image, subtitles). While a Track File can, for instance, contain all audio channels for a given language, additional languages are required to be stored in separate track file. The Composition Playlist will select the correct Track Files to play a requested version of the movie (composition).

5.3.2. MXF Track File Encryption

5.3.2.1. Introduction

The following are requirements for MXF Track File Encryption. For the purpose of this section, a frame is defined as an image frame time, for example 24 FPS or 48 FPS.

- *The encryption shall support KLV encoding as specified in [SMPTE 336M-2001 Television – Data Encoding Protocol using Key-Length-Value].*
- *The encrypted audio or image Track File shall be a valid MXF file.*
- *KLV packets shall be encrypted using the Advanced Encryption Standard (AES) block cipher algorithm using a 128 bit key operating in Cipher Block Chaining (CBC) mode, as defined in [NIST Special Publication 800-38A]. See National Institute of Standards and Technology [FIPS PUB 197] (November 26, 2001).*
- *Each shall use a single cryptographic key for all frames within the sound or picture Track File.*
- *The encryption method shall support random access to any frame of essence within the sound or picture Track File.*
- *The integrity of each frame of sound and picture essence shall be verifiable using the HMAC-SHA1 algorithm.*
- *There shall be a method for verifying that all frames within a sound and picture track are played in correct sequence.*
- *The Track File encryption method shall allow for the common header data within each frame of essence to be plain text. In other words, the encryption of each frame of essence shall have a programmable offset of "n" bytes such that common header data is left as plaintext.*
- *There shall be a method for verifying that the correct cryptographic key is used and the essence is being decrypted correctly.*
- *A reference decryption model shall be specified.*

- *Track File encryption shall not require encryption of all frames within a file.*
- *Track File encryption shall be independent of the nature of the underlying essence and associated metadata.*
- *No information shall be lost in the Track File encryption process.*

5.3.2.2. Encrypted Track File Constraints

Encrypted Track Files shall follow the same specification as plain-text Track Files, with the following additional constraints. The following are included in the Encrypted Track File Constraints:

- **Encrypted Essence Track** – *A single cryptographic key, and hence, Cryptographic Context, shall be used to encrypt any given essence track.*
- **Cryptographic Framework Descriptive Metadata Track** – *Track Files may contain one or more Descriptive Metadata Tracks in the MXF File Package that describes the essence of the Track File.*
- **Index Tables** – In a plain-text Track File, each Index Table entry locates a Triplet containing a single frame of picture essence. *Similarly, in an encrypted Track File, each Index Table entry shall point to an Encrypted Triplet wrapping a single Triplet, itself containing a single frame of picture essence.*

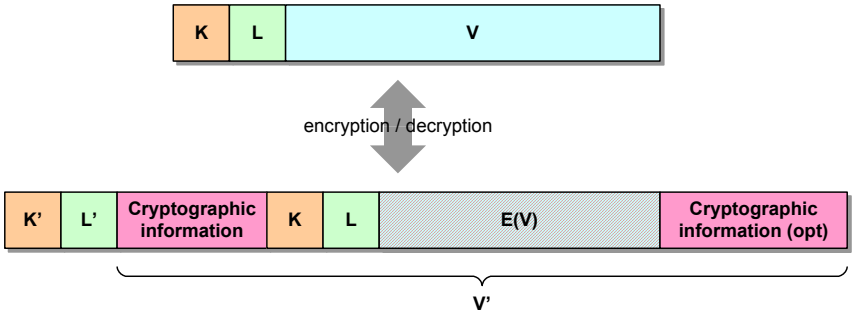

Figure 10. Correspondence between Source and Encrypted Triplets[9]

Figure 10 illustrates the correspondence between a plaintext KLV triplet and an Encrypted KLV Triplet. The value V of a source plaintext KLV Triplet is first encrypted to yield E(V). This encrypted value, E(V), along with K and L, is wrapped in a K'L'V' Encrypted Triplet. K' is a unique label common to all Encrypted KLV Triplets, independent of their content. L' refers to the full length of V'. V' consists of K, L and E(V) from the source KLV Triplet as well as cryptographic information specific to the Encrypted KLV Triplet. This cryptographic information includes, for instance, the initialization vector used in generating E(V) and the Message Integrity Code used to verify the integrity of the Triplet.

5.3.3. Image Track File

5.3.3.1. Introduction

An Image Track File contains the image essence data and its associated metadata. Each Image Track File can contain compressed and encrypted image data. The following are requirements for an Image Track File.

[9] Red hatching depicts the encrypted portion of the Encrypted Triplet. Other items are left in the clear. Only the value item of Source Triplet is encrypted, allowing the essence information to be encrypted prior to wrapping. See "Encrypted Triplet" for a description of the cryptographic information associated with each Encrypted Triplet.

5.3.3.2. Frame Boundaries

The Image Track File is required to begin and end with complete frames that allow for splicing. Frames are defined to be image frames such as 24 FPS (1/24 sec) or 48 FPS (1/48 sec). The image data within the Track File shall be wrapped using KLV on an image frame boundary.

5.3.3.3. Compression

The Track File is required to support Constant Bit Rate (CBR) compression and Variable Bit Rate (VBR) compression, within the constraints of the specified code stream for the reference decoder (see Section 4 COMPRESSION).

5.3.3.4. Metadata

The following metadata is required to be furnished with the Image Track File:

- Unique ID
- Unique ID of corresponding plaintext track if encrypted
- Track type (i.e., mage)
- Total width in pixels
- Total height in pixels
- Aspect Ratio
- Frame Rate
- Frame count number (duration)

5.3.4. Audio Track File

5.3.4.1. Introduction

An Audio Track File contains the audio essence data and its associated metadata. The following are requirements for an Audio Track File.

5.3.4.2. Frame Boundaries

The Audio Track File is required to begin and end with complete frames that are associated with its Image Track File to allow for a clean transition between reels. The audio data within the Track File shall be wrapped using KLV on an image frame boundary.

5.3.4.3. Data Packing Format

The Audio Track File is required to support uncompressed audio data.

5.3.4.4. Metadata

The following metadata is required to be furnished with the Audio Track File:

- *Unique ID*
- *Unique ID of corresponding plaintext track encrypted*
- *Track type (i.e., audio)*
- *Audio Sampling Frequency*
- *Quantization bits (sample size)*
- *Channel Count*
- *Channel Mapping Labels*

- *Data Packing Format*
- *Frame Rate*
- *Audio Frame count number (duration)*

5.3.5. Subtitle Track File

5.3.5.1. Introduction

A Subtitle Track File contains, for example, the Subtitling essence data and its associated metadata. *Each Subtitle Track File may contain any combination of text, font references, and image references*.

5.3.5.2. Frame Boundaries

The Subtitle Track File is required to have the same duration as the playable region of its associated Image Track File.

5.3.5.3. Timed Text

Any Timed Text element is required to use an Open Type font.

5.3.5.4. Subpicture

Subpicture elements are required to use the PNG file format.

5.3.5.5. Metadata

The following metadata is required to be furnished with the subpicture Track File:

- *Unique identification*
- *Track Type (i.e., Timed Text, subpicture)*
- *Total Width In Pixels of the Image Track File (PNG files only)*
- *Total Height In Pixels of the Image Track File (PNG files only)*
- *Aspect Ratio (PNG files only)*
- *Frame Rate*
- *Position*
- *Timing (Temporal)*

5.3.6. Auxiliary Track Files

5.3.6.1. Introduction

An Auxiliary Track contains, for example, the Unicode™ text data or any other data or metadata that belongs in a separate track for functional purposes. The following are requirements for an Auxiliary Track File.

5.3.6.2. Frame Boundaries

The Auxiliary Track File is encouraged to begin and end with complete frames that are associated with its Image Track File to allow for a clean transition between reels.

5.3.6.3. Metadata

The following metadata is required to be furnished with the Auxiliary Track Files:

- *Unique identification*
- *Track Type (i.e., auxiliary)*

- *Frame Count Number*
- *Text Format (If applicable)*
- *Cue Names (If applicable)*

5.4. Composition Playlists

5.4.1. Introduction

Composition Playlists (CPL) are textual lists that define how elements of Digital Cinema Compositions are played back in a presentation. The content owner creates the Composition Playlist in a post-production environment. The Composition Playlist is digitally signed, such that any unauthorized modifications can be detected by any entity (e.g., Theater Management System or Security Manager) knowing the public key of the signer. The Composition Playlist has the following requirements.

5.4.2. File Format

The Composition Playlist is required to use the secure (digitally signed) text-based XML file format.

5.4.3. Human Readable Information

The Composition Playlist is required to contain the following human readable information in English (default) but can be provided in other languages as well.

5.4.3.1. General Information

- *A Composition Playlist is required to be identified by ISAN [ISO 15706] or UMID [SMPTE 330M-2004 Television – Unique Material Identifier (UMID)].*
- Content Title in human readable text
- Content Kind (e.g., Feature, Trailer, Logo, Advertisement)
- Content Version
- Language
- Country
- Rating
- Aspect Ratio
- Image Format
- Audio Format

5.4.3.2. Image Track Information (list for each reel)

Any given image Track File is required to have exactly one and only one Entry Point within a given composition playlist.

- Unique ID encoded as a UUID
- File Authentication Code
- Entry Point (number of frames offset into the Track File)
- Duration

5.4.3.3. Audio Track Information (list for each reel)

Any given audio Track File is required to have exactly one and only one Entry Point within a given composition playlist.

- Unique ID encoded as a UUID
- File Authentication Code
- Entry Point (number of frames offset into the Track File)
- Duration

5.4.3.4. Subtitle Track Information if Present (list for each reel)

- Unique ID encoded as a UUID
- File Authentication Code
- Entry Point (number of frames offset into the Track File)
- Duration

5.4.3.5. Auxiliary Track Information if Present (list for each reel)

- Unique ID encoded as a UUID
- File Authentication Code
- Entry Point
- Duration

5.4.3.6. Digital Signature

- Encrypted hash (message digest)
- Signer identification

5.4.4. Digitally Certified

A Composition Playlist is digitally signed by its creator, and cannot be modified without detection. *Digital signatures are required to verify the authenticity of the Composition Playlist.*

5.5. Distribution Package

5.5.1. Introduction

The Distribution Package has two major components. One is the Package itself, which includes all of the Track Files and the other is the Packing List. These are all of the elements required for a complete delivery to the theater Digital Cinema system. It is technically possible to include engagement-specific licenses and keying information in a Package in the form of opaque metadata, but this is not recommended for general usage.

A Distribution Package can contain a complete feature composition or a set of compositions. Alternatively, it can carry as little as a single file to update one reel's subtitle or sound track.

5.5.2. Distribution Package

5.5.2.1. General

The Distribution Package is required to contain a Packing List and one or more Digital Cinema Track Files.

5.5.2.2. Packing for Transport

The distribution method is required to allow a DCP to be transported via physical media, satellite or network.

5.5.2.3. Security

The distribution method is required to provide digital signatures to allow the recipient to verify integrity of the Packing List and the enclosed files.

Preparation of Packing Lists is a distribution fulfillment or transport function. Therefore, the digital signatures come from these entities, not the content-owner who mastered the files. Packing List security functions do not verify the authenticity of the content, only the intent of the delivery agent. Content authenticity is verified through Playlist signatures and digital licenses.

5.5.3. Packing List

5.5.3.1. File Format

The Packing List is required to use XML data format with XML signature (digital signature). It should be in English (default) but can be provided in other languages as well.

5.5.3.2. Fields

The following data fields are required to be included in the Packing List for each file in the Package:

- *Unique identification of each file included in the DCP is encoded as urn:UUID.*
- *Annotation Text parameter (optional), if present, is a free-form, human readable annotation associated with the asset. It is meant strictly as a displayable guidance for the user.*
- *File Integrity check (hash) for each file in the distribution package*
- *Size of the file in bytes*
- *Type (e.g., Packing List, Playlist, Track File, opaque security data)*
- *Original File Name*

The following fields are required to be included in the digital signature section of the Packing List:

- *Signer parameter uniquely identifies the entity, and hence public key that digitally signs the Packing List.*
- *Signature parameter contains a digital signature authenticating the Packing List.*

THIS PAGE LEFT BLANK INTENTIONALLY

6. TRANSPORT

6.1. Introduction

Transport refers to the movement of the packaged Digital Cinema content. This can be accomplished in many ways, such as physical media, Virtual Private Network (VPN), or satellite. This section will describe any requirements for the transport of packaged content.

6.2. Transport System Overview

6.2.1. Transport Fundamental Requirements

6.2.1.1. Introduction

Digital Cinema presents unique opportunities for the transport of theatrical content. Some basic requirements are stated below.

6.2.1.2. Security

The content owner's encryption is required to not be removed during transport.

6.2.1.3. Robustness

The files are required to retain all of the data of the original files upon completion of transport of the Digital Cinema content.

6.2.2. Transport Fundamental Concepts

The transport of Digital Cinema content can be accomplished in many different ways. The Distributors will select the method that is both economical and technically robust to ship their content to the theaters. This can include the use of physical media or through transmission (e.g., satellite, fiber, copper). *Any selected method is required to provide for a secure environment for the content as well as no corruption of the data*. Segmenting of the packaged content can occur to accommodate fixed media or bandwidth constraints.

6.2.3. Ingest Interface

Independent of the transport method, the output interface of the transport system is required to be ingested into the Digital Cinema Storage in the theater.

The ingest interface is required to be Gigabit or 1000Base-T Ethernet [IEEE802.3ab (copper)] or [IEEE802.3z (fiber)] interface using a TCP/IP protocol.

THIS PAGE LEFT BLANK INTENTIONALLY

7. THEATER SYSTEMS

7.1. Introduction

Theater Systems for Digital Cinema incorporates all of the equipment required to make a theatrical presentation within an auditorium located within a Theater complex. This encompasses projectors, Media Blocks, Security Managers, storage, sound systems, DCP ingest, theater automation, Screen Management System (SMS) and Theater Management System (TMS). The Screen Management System (SMS) provides the theater manager a user interface for local control of the auditorium such as start, stop, select a Show Playlist and edit a Show Playlist. At a higher level is the Theater Management System (TMS). The TMS can control, supervise and report status on all of the equipment in the Theater as well as perform all the duties of the SMS. This section will define the requirements and interconnectivity of a TMS and multiple SMSs within a theater complex.

7.2. Theater System Overview

7.2.1. Functional Framework

For the purpose of documenting the specific requirements and specifications for a Digital Cinema Theater System, it is helpful to divide the system into a set of components. The specifications and performance requirements for each of these components will be described in the following sections:

- **Screen and Theater Management Systems** – The human interface for the Digital Cinema System
- **Theater Systems Architecture** – The equipment and interconnect within the Theater
  - Single Screen Architecture
  - Multiplex Architecture

7.2.2. Theater System Major Concepts

Theater Systems can have a wide range of responsibilities. They are required to provide a theatrical presentation in a timely manner along with controlling the environment in which it is presented. To simplify this complex system, each major component of a Digital Cinema Theater System is reviewed and shown how they interconnect. The human interface of the single screen system is the Screen Management System (SMS). *It is required that there be one SMS for each auditorium*. The Screen Management System (SMS) provides user interface to control (start, stop, pause, load playlist, etc.) a single auditorium. The Theater Management System (TMS) allows a theater manager to control many or all auditoriums within a theater complex from a central location This is the interface that allows for control, show programming, troubleshooting, asset management and status of the Digital Cinema equipment. There are many different scenarios for the implementation of the SMS and the TMS.

7.2.3. Theater System Fundamental Requirements

Digital Cinema Theater Systems have some basic requirements that are stated below.

7.2.3.1. Reliability

A key part of the Digital Cinema system is reliability. *In the realm of Digital Cinema, the presentation should not be interrupted, except in the event of a catastrophic failure of the*

Digital Cinema system (e.g., loss of power) or a natural disaster. There will be cases where equipment will fail (such as happens now with traditional 35mm film equipment). However, the time between failures, and the speed at which it is repaired, is encouraged to be no worse than those for traditional 35mm film equipment.

Each individual theater system is required to have a Mean Time Between Failure (MTBF) of at least 10,000 hours.

7.2.3.2. Mean Time to Repair

A failed or malfunctioning unit/component is required to be capable of being diagnosed and replaced within 2 hours, exclusive of the time needed to order and to deliver the replacement component(s). Design of a system is required to allow repair of any failed unit/component within two hours.

7.2.3.3. Test Shows

The system is required to allow the content to be played back for validation and verification prior to exhibition.

7.2.3.4. Monitoring and Diagnostics

The system is required to provide monitoring and diagnostic checks and provide for status, monitoring, alignment and calibration. This can be done locally or through remote control.

7.2.3.5. Easy Assembly of Content

The system is required to provide a graphical user interface (GUI) interface for the assembly of content with relative ease in a timely matter.

7.2.3.6. Movement of Content

The system is required to provide for intra-theater movement of content within a multiplex facility. Emergency moves (e.g., equipment failure) between auditoriums are required to allow playback to start within 15 minutes or less after the start of the movement.

7.2.3.7. Ease of Operation

The Digital Cinema Theater System is encouraged to require only a reasonable level of computer operation knowledge or training for the basic operation of the system. The computer-based user interfaces are required to be simple and intuitive.

7.2.3.8. Multiple Systems

There can be one Theater Management System communicating to one or more Screen Management Systems.

7.2.3.9. Environment

The theater is required to provide an adequate environment for the equipment, with an operating temperature range of 10-35°C and operating Humidity of 10% to 85% Non-Condensing.

7.2.3.10. Safety

All equipment is required to comply with applicable safety regulations.

7.2.3.11. Storage Capacity Per Screen

The central and/or local storage system is required to have the capacity to hold at least 1 TByte of usable storage per screen, where a TByte equals 1,000,000,000,000 bytes.

7.2.3.12. Persistent Security

Theater systems equipment is required to implement all the security requirements as specified in Section 9 SECURITY. These requirements enable the necessary functions and features for a reliable and persistent environment to protect content and Security Data, and support the required forensic processes that stakeholders require.

7.2.3.13. Power Failure

In the case of a power interruption, the Digital Cinema Theater System is required to be restored into a stable stop/idle condition.

7.2.3.14. Local Control

Every auditorium is required to provide the means of local control by the Screen Management System (SMS) at each projection booth.

7.3. Show Playlist

7.3.1. Introduction

The Show Playlist is the list that the Exhibitor assembles to complete a presentation in the theater. The Show Playlist has the following requirements.

7.3.2. File Format

The Show Playlist is required to use XML file format.

7.3.3. Human Readable Information

7.3.3.1. General Information

- Unique ID encoded as a urn:UUID
- Program Types (e.g., feature, trailer, logo, advertisement)
- Show Playlist Title
- Version
- Language
- Country
- Rating
- Aspect Ratio
- Image Format
- Audio Format

7.3.3.2. Sequence of Composition Playlists

- Unique ID encoded as a urn:UUID
- Composition and/or Event Playlist Filename
- Timeline Count In Point
- Timeline Count Out Point

7.3.4. Editing Show Playlist

The Show Playlist is designed to be edited in the field. The requirements for editing are listed below:

- *Shall support adding or deleting of a reference of a Composition Playlist to a Show Playlist*
- *Shall support altering of the sequence of a reference to a Composition Playlist within a Show Playlist*
- *Shall allow for show cue programming and automation*
- *Shall provide programming synchronized to a local clock (timeline)*

7.4. Theater Management System

7.4.1. Operation

7.4.1.1. Introduction

The Screen Management System (SMS) is required to allow the theater staff to function similar to traditional theater operations. The workflow does not need to radically change to support Digital Cinema presentations. Digital Cinema content will arrive at the theater via fixed media, or through other means of transport, and will be loaded into central or local storage. The staff will then assemble a Show Playlist using a computer Graphical User Interface. This Show Playlist could include advertisements, logos, previews and a main feature. The staff will then direct the show to the screen and let the SMS begin the show by local or remote control.

The Screen Management System provides a user interface to control (start, stop, pause, load playlist, etc.) a single auditorium. The Theater Management System (TMS) allows a theater manager to control many or all auditoriums within a theater complex from a central location.

At the beginning of this section, fundamental requirements were listed that would allow theaters to operate as they have been for some time. This section will elaborate on some of these and other requirements, as they affect the SMS and TMS.

7.4.1.2. Local Control

Each auditorium in a theater complex is required to allow for local control at each screen via the SMS. This will provide for at a minimum:

- Show Start
- Show Stop
- Show Pause
- Show Restart
- Show programming (single screen installation)

7.4.1.3. User Accounts

The SMS and TMS are required to support multiple levels of user accounts. The following is an example of multiple accounts: Projection, Show Manager, Super-user, and Administrator with password-protected appropriate log-ons.

A. Projection – Required to be able to perform the following functions

- Browse and activate current shows
- Play content, including starting and stopping playback

- Assemble shows

B. Show Manager – Required to have access to the following functions

- All projection functions
- Assemble or Delete Shows to/from storage
- Import/Delete Content to/from storage

C. Super-user – Required to have access to the following functions

- All Show Manager functions
- User Management
- Theater System Setup

D. Administrator – Required to have access to the following functions

- All Super-user functions
- System Setup
- Security Setup

7.4.1.4. Receipt of Content

Content can be received by physical media or via a network. The theater systems are required to allow multiple motion pictures and related content to be delivered to a theater in a timely matter. The theater systems are also required to provide a method to verify that the data is complete and whether or not it has not been corrupted.

7.4.1.5. Movement of Content

The SMS and TMS are required to allow an authorized user to search for content and provide a method for the movement and deletion of content, within a screen or multiplex facility, while the system is in operation. As an example, this would include simultaneous content load-in and playback. This movement could consist of many different examples of operation such as:

- Downloading content while playback of presentations are in progress
- Movement of content from a central storage to local storage while other content is in playback
- Deleting content while other content is in playback
  - *I. The SMS or TMS is required to warn and not allow deletion if the content is in use or part of a current Show Playlist.*
  - *II. The SMS or TMS is required to provide a deletion process that removes all of the content, key information, and playlists associated with the composition.*

7.4.1.6. Assembly of Content

An electronic method is required to assemble trailers, feature presentations and other content in the creation of shows. At a minimum, a standard method is required to electronically identify the content to the SMS, TMS and the Security Manager (SM) to allow the show to be assembled and played back. This method of identification is embedded within the packaging format as metadata. (See Section 5 PACKAGING.)

Operationally, the SMS and TMS are required to provide the user with a method of creating a Show Playlist. This method provides for the following:

- *A method of building shows is required to allow only authorized personal to build, save and transport the Show Playlist.*

- *A method is required to use the validity/expiry method, so that one can check that one has the security devices and keying parameters required for playback.*
- *A method is required to make it possible for a Show Playlist to be provided via an external source.*
- *A method is required to provide a means for inserting a black screen and silence between content. The Media Block is required to be able to transition modes without displaying a roll or similar artifacts during a transition between clips in a playlist or between playlists.*
- *Show Playlists can consist of both encrypted and non-encrypted content.*
- *The Show Playlist can be communicated in whole to the Media Block, whereupon it is then stored and subsequently executed within the Media Block (Content Data Pull Model).*
- *The Show Playlist can be executed within the SMS and communicated to the Storage and Media Block one command at a time (Content Data Push Model).*
- *A method is required to provide for the insertion of cues.* These cues allow the automation system to perform its tasks at event boundaries, such as start of feature and start of end credits.

7.4.1.7. Automation Programming

The Automation System is required to communicate events to and from the screen equipment. These can be light dimmers, curtains, or other systems within an auditorium. These events or cues are programmed within the TMS or the SMS, and initiated by either the SMS or the Automation depending on which unit is master and which is slave. All of the event types are pre-programmed to have certain effects on the system. *These events, at a minimum, are required to be recognized by all systems and are listed below:*

- First Frame of Content
- First Frame of Intermission
- Last Frame of Intermission
- First Frame of End Credits
- First Frame of End Credits on Black
- Last Frame of Content

7.4.1.8. Playback of Content

The system is required to provide a method to:

- *Have full content play functionality (e.g., make playlists active, stop, start, start play) at any reel break point in a playlist.*
- *Handle power interrupted while playing content. When the system is next started, it is required to inform the user that playback was abnormally interrupted during the last play, and offer the user the ability to restart playback at a point prior to the failure (see Section 5.3.1.11 Random Access and Restarts). The system should also log such events.*
- *Have no interruptions during playback (glitch-free).*
- *Adjust the delay of audio ±5 image frames in 10 msec increments of all presentation content to the image.*

7.4.2. Theater Management System Events

The following table depicts situations and events related to the Theater Management System (TMS). These events do not affect the security system and are known only to the Theater Management System. In addition, the Theater Management System has the ability to have pre-showtime knowledge of events in the security system by directing the Screen Management System to query the Security Manager.

Item, Observation or Issue	Approach
Log data collected from auditoriums	TMS controls and can check collection status
Equipment installation and locations	TMS knows about and controls installations
Auditorium scheduling	TMS knows scheduling information

Table 8: Examples of Theater Management System Events

The examples in Table 8 are outside of the knowledge or control of the security system. The Theater Management System may have the capacity to execute such functions or make records of various activities under its control. Under a private agreement between the Exhibitor and the Distributor, data collected by the Theater Management System could be made available.

7.5. Theater Systems Architectures

7.5.1. Introduction

A Digital Cinema Theater System includes several component systems: ingest, storage, Media Block, security, projection, audio system, Theater Management System, Screen Management System and automation. An example of a single screen installation is shown in Figure 11.

7.5.2. Ingest

7.5.2.1. Introduction

Ingest is the process of receiving content and security information at the theater level. These are the devices that connect to and from the outside world. The following is an example list of such devices split into two groups. The first group has to do with content while the second group is for security and control.

Content:

- Satellite receiver(s) (with cache or local storage)
- Terrestrial fiber network(s) (with cache or local storage)
- Fixed media interface(s)

Security and Control:

- Security Management Interface – Standardized Extra-Theater Message (ETM) and logging report communications interface.
- *Once a complete DCP has been ingested, the TMS or SMS is encouraged to verify that a KDM is available and displays the time window for showing the content. A TMS or SMS show schedule can display conflicts between the KDM and the scheduled showings.*
- *The TMS or SMS is encouraged to alert the user when a KDM will expire within 48 hours.*

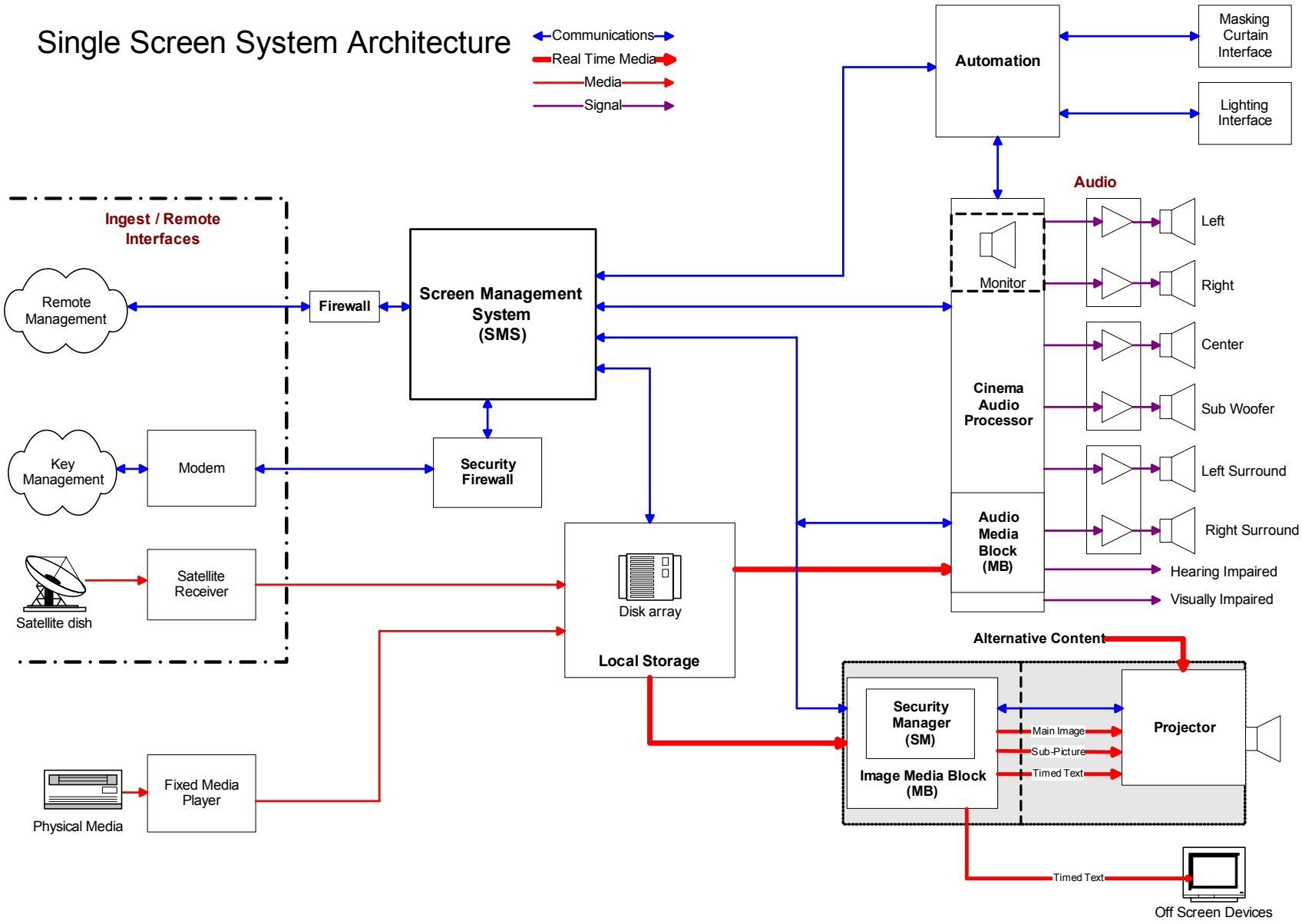

Figure 11: Single-Screen System Architecture

7.5.2.2. Ingest Interfaces

Except for security messaging, the interfaces to the outside world can use any method or physical connection. Inside the theater structure, the architecture is encouraged to break down into two types of interfaces, one for the content and one for control/status and key exchange.

- *The content ingest interface is required to be Gigabit Ethernet [IEEE802.3ab (copper)] or [IEEE802.3z (fiber)] interface.*
- *Theater facilities are required to provide a dial-up modem with a connection that will be available 24/7 for security communications (all ETM and log data reporting*). It is theater management's decision as to whether this connection is dedicated. However it will be recognized that for some operational situations (e.g., receiving new KDMs), it may be important to have priority access to this connection for security communications. Additional alternative means of security communication can be implemented by agreement between the parties.

7.5.2.3. Firewalls

Theater networks are required to protect the security system from the threat of external and internal network-born attacks by the installation of appropriate firewalls. Because there will be many variations in network designs, it is impossible to define specific solutions as part of this specification. *Exhibition operators are encouraged to solicit competent network security engineering assistance as part of their facility network design efforts.*

7.5.3. Storage

7.5.3.1. Introduction

Content storage can be arranged into two basic configurations or a combination of the two. One is known as local storage and the other is central storage. Local storage is a configuration where the storage is located at each screen. Central storage is a configuration that has all of the storage of content in a central location for all of the screens in a multiplex. There can also be combinations of central and local storage.

7.5.3.2. Storage Reliability

The most important aspect of the storage system is reliability. There are a number of RAID configurations that will provide storage redundancy and therefore storage reliability. *The storage system is required to provide redundancy such that should a single hard disc drive fail, the system will continue to play with no visible or audible interruptions or artifacts.*

7.5.3.3. Central Storage

Central Storage implies that packaged content for a multiplex may be stored in one location. Central Storage may allow for multicasting of the content.

If only Central Storage architecture is used, careful planning is required to be done to ensure that it does not have a single point of failure, including the network. In this type of implementation, the Central Storage is required to also provide the capability to sustain the peak bit rate of all screens being fed simultaneously, along with ingest.

7.5.3.4. Local Storage

Local storage implies a single storage system for each screen. Local storage is required to be able to sustain the bit rate required for the playback of all content for that screen.

7.5.3.5. Combined Central and Local Storage.

A combination of central and local storage for a multiplex can be the best solution. *The central storage can be used for ingest of material and redundancy of content, while the local storage is encouraged to hold just the content required for the immediate presentation(s).*

7.5.3.6. Bandwidth

The storage system is required to provide enough output to support a continuous stream of 307 Mbits/sec for compressed image, uncompressed audio (16 channels, 24 bit sample, 96 kHz) and subtitle data to allow for non interrupted Digital Cinema playback.

7.5.3.7. Capacity

Excluding storage necessary for redundancy, the storage system is required to provide for, at a minimum, the storage of three features (including pre-show content) per screen (one feature currently showing and a second or upcoming feature). Shown in Table 9 below, are some example storage requirements. The numbers are based on:

- One three-hour feature
- 20 minutes of pre-show material at the same resolution
- 16 channels of uncompressed audio at 48 kHz at 24 (AES3) bits
- 3,000 sub pictures in PNG file format
- 3,000 Timed Text lines
- A fixed amount of Auxiliary Data (1 MByte)

Average Bit Rate (Mbits/sec)	3 Hour Image (GBytes)	3 Hour Audio (GBytes)	20 min. pre-show (Gbytes)	Sub Picture (GBytes)	Timed Text (GBytes)	Aux Data (GBytes)	3 Hour Total (GBytes)
250	371.250	2.281	41.250	0.300	0.001	0.001	415.082
200	297.000	2.281	33.000	0.300	0.001	0.001	332.582
125	185.625	2.281	20.625	0.400	0.001	0.001	208.932
100	148.500	2.281	16.500	0.600	0.001	0.001	167.882
80	118.800	2.281	13.200	0.800	0.001	0.001	135.082

Table 9: Example of Storage Capacity for one 3-Hour Feature (12 bits @ 24 FPS)

Image size: Calculated by: {Average or max bit rate (Mbits/sec) * hours * 60 min/hour * 60 sec/min} / {8 bits/byte *1000} the results is in GBytes

Audio size: Calculated by: {32 (AES bits) * 48,000 samples/sec *16 (channels) * hours * 60 min/hour * 60 sec/min / 8 (bits/byte) = size

or

Calculated by: {32 (AES bits) * 96,000 samples/sec *16 (channels) * hours * 60 min/hour * 60 sec/min / 8 (bits/byte) = size

Sub Picture size: Calculated by: 100,000 (bytes/png file @ level 1) * 3,000 (subtitles/feature) = size

Timed Text size: Calculated by estimate of 1 MBytes per feature

Auxiliary Data size: Calculated by estimate of 1 MBytes per feature

7.5.3.8. Storage Security

It is required that image and audio essence on storage devices retains the original AES encryption, if present during ingest. It is required that decrypted plaintext (image or audio) essence is never stored on the storage system.

7.5.4. Media Block

7.5.4.1. Introduction

Another key component in the playback chain is the Media Block. One or more Media Blocks are responsible for converting the packaged, compressed and encrypted data into raw image, sound, subtitles and auxiliary data.

Depending upon implementation, both security and non-security functions take place within Media Blocks. *Security functions of Media Blocks (those functions which process plain text essence or Security Data such as decryption keys) may take place only within physically secure perimeters called Secure Processing Blocks (SPB).* The more general functions of the Media Block and variations on implementation are described here. Not all such functions are required to be within an SPB. Detailed security requirements of Media Blocks are discussed in Section 9.4 Theater Systems Security.

The Media Block can be implemented in a server configuration, as shown in Figure 12. This is where the storage and the Media Block are closely coupled. In this configuration, the content data is then pushed to the final playback device. *In this configuration, Link Encryption is required to protect the uncompressed content.*

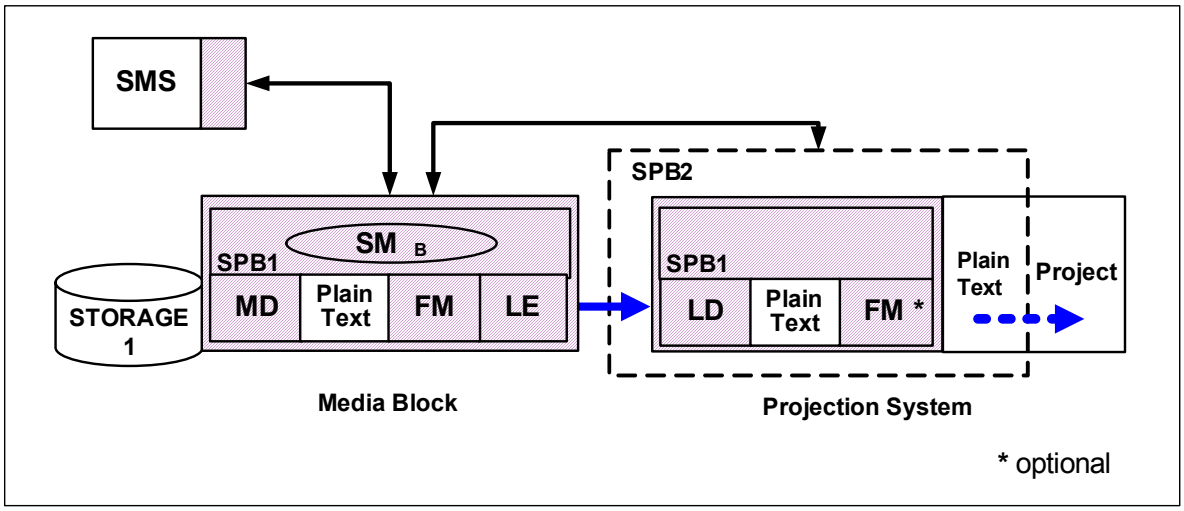

Figure 12: Media Block Server Configuration[10]

The Media Block can also be implemented as a component within the projection system. This provides the option of not requiring Link Encryption. In this configuration, the Media Block may use a push or pull method to process essence data from storage, as shown in Figure 13.

[10] The double-lined boxes of Figure 12 and Figure 13 show those processing functions required to take place within physically secure SPB type 1 perimeters

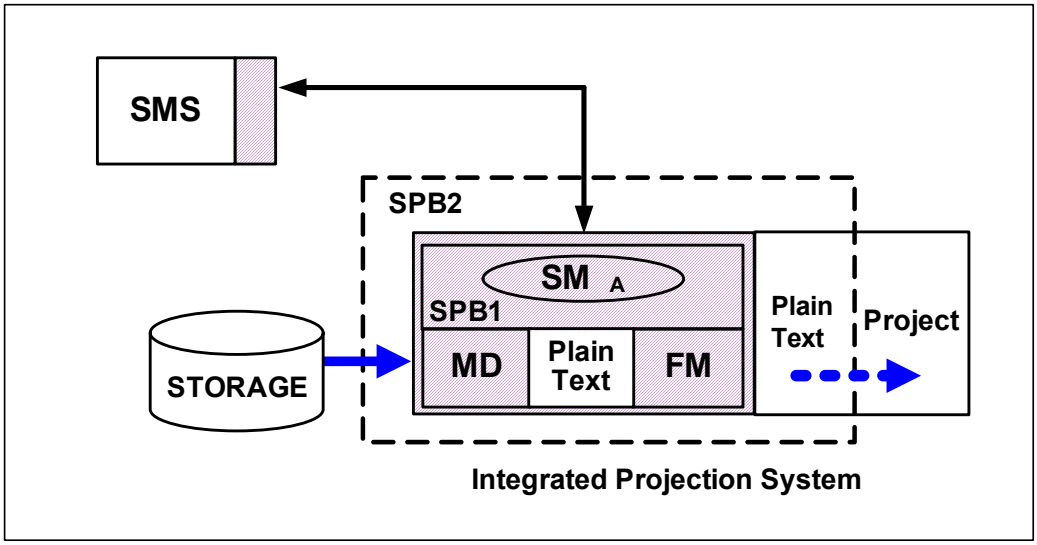

Figure 13: Media Block in Projector Configuration[10]

If both Image Media Block (IMB) and Audio Media Block exist serving a single auditorium, the Media Block processing the image is required to contain the SM for that auditorium.

Note: Due to the dynamic nature of security technology, DCI reserves the right, at some future time, to update requirements and may require changes to Digital Cinema systems as situations warrant.

7.5.4.2. Media Block Functional Requirements

7.5.4.2.1. Synchronization

The Media Block is the device that converts, in real time, the packaged content data from storage into data for playback to downstream devices. *The Media Block is required to playback the image, audio and other timed dependant content in a manner that presents a synchronized performance to the audience.*

7.5.4.2.2. Security Functions

One of the functions of a Media Block is essence decryption, which is performed by the appropriate Media Decryptor (MD) for image or audio decryption. *Image and audio decryption is required for all playback systems. Image Media Blocks (IMB) are also required to contain the Security Manager, Forensic Marker for image content and decoder. Link Encryption is also required, if the IMB is not contained within the projection system.*

Audio decryption may take place as part of the IMB, or in a separate Audio Media Block. An Audio Media Block is required to accomplish the formatting to synchronize audio and to convert to [AES3-1992 (r1997)]. It also provides Forensic Marking capability for audio.

All Media Blocks are required to provide logging functions per the requirements of Section 9.4.6.3.1 Logging Requirements.

7.5.4.2.3. Image Link Encryption and Decryptor Block

If the Image Media Block is not physically located in the same secure container as the projector, then the Image Media Block is required to provide link encryption to the

projection system to protect image essence per Section 9.4.4 Link Encryption. At the projector, a Link Decryptor Block is required to decrypt the image essence. The Link Decryptor Block is required to provide SPB type 1 physical protection for link decryption, the associated security keys and logging functions.

7.5.4.2.4. Unpackaging

Any packaged content that comes from storage is required to contain all of the content data required for the presentation and file integrity. The first job of the Media Block is to arrange the track files into their appropriate modules and to provide a timely supply of data to the next process. *The content can arrive completely unpacked or partially unpacked depending upon the system's storage method.*

7.5.4.2.5. Alpha Channel Overlay

An alpha channel overlay module, to key subtitles or open captions into the Main Image, can be located in the projector or in the Media Block.

7.5.4.2.6. Subpicture Renderer

The subpicture renderer, a module that converts the subpicture file into the DCDM image file with an alpha channel overlay, can be located in the projector or the Media Block.*

7.5.4.2.7. Timed Text Renderer

The Timed Text renderer, a module that converts Timed Text data into the image file with an alpha channel overlay, can be located in the projector or the Media Block.

7.5.4.2.8. Auxiliary Data

A module that converts auxiliary data into timed data, that is understood by its downstream devices, (e.g., time code), can be located in the projector or the Media Block.

7.5.4.3. Media Block Interfaces

The Media Block is required to interface on three levels with the rest of the system. One level deals with the packaged Digital Cinema content. The next level is the raw essence output for the projector, the audio processor and any special devices for the automation system. The third level is the control and status of the Media Block playback system. These interfaces are noted below.

- **Packaged Data** – The packaged content requires a standard data interface that could handle bandwidths up to 307 Mbits/sec for the composition data. *This may be a Gigabit or 1000Base-T Ethernet [IEEE 802.3ab (copper)] or [IEEE 802.3z (fiber)] interface.*
- **Uncompressed Essence** – The raw essence data requires a real time data interface with extremely high bandwidths. The interface will depend on the physical location of the Media Block and the type of essence that the interface carries.
    - **A. Main Image** – *This streaming data interface is required to handle data rates up to 10 Gbits/sec. (*See Section 8 PROJECTION for details.)
    - **B. Subpicture** – *This streaming data interface is required to handle data rates up to 20 Mbits/sec. This can be accomplished by the use of a standard 100Base-T Ethernet [IEEE 802.3] interface.*

C. **Timed Text** – This could be a streaming data interface depending on the buffer capability of the projector. It is expected that this interface can also use a standard 100Base-T Ethernet [IEEE 802.3] interface that can handle data rates up to 500 Kbits/sec. *It is encouraged that there be at least two of these interfaces from the Media Block, one to feed the projector and the other to feed off-screen devices.*

D. **Audio** – *This interface is required to stream multiple digital audio channels to the Cinema Audio Processor. This is required to be in an AES3 format. For worst-case audio bandwidth, 37 Mbits/sec is required (16 channels * 24 bit sample * 96 kHz = 37 Mbits/sec).*

E. **Auxiliary Data** – This interface handles any optional automation data sent to the Screen Automation. This data needs to be dealt with in real time. Current practice for this application is RS-422 and/or 100Base-T Ethernet [IEEE 802.3] interfaces.

- **Security Messaging** – *The Image Media Block is required to communicate security messaging via a standard 100Base-T Ethernet [IEEE 802.3] interface to the projector, the SMS and remote Media Blocks*. This communications facility is referred to as the intra-auditorium security network and it may physically be part of other/existing auditorium networks, which carry other types of traffic (e.g., command, control and status). *However, it is distinguished in that security messaging is required to utilize Transport Layer Security (TLS) at all times.* See Section 9.4.5 Intra-Theater Communications for security messaging requirements.

7.5.5. Projection System

7.5.5.1. Introduction

The Projection System is required to change digital image data into the light that appears on the screen. The projection system is required to support many interfaces and different Digital Cinema system architectures. One of these architectures includes the Image Media Block (described above) installed in the projector. In this type of architecture, all of the content is ported through a single data interface. *When the Image Media Block is external to the Projector, Link Encryption is required. The corresponding Link Decryption Block is required at the projector interface.*

Alternative content can come from an external interface, even when the Media Block is present inside the projector.

7.5.5.2. Projection System Interfaces

The Projection System not only provides the main image on the screen, it can provide subtitles, open captioning, and still pictures. This requires extra interfaces from the Media Block, if the Media Block is not installed in the projector. These interfaces are noted below. (For the complete interface specification refer to Section 8 PROJECTION.)

- **Subpicture** – The subpicture (bit mapped image data with alpha channel) information will need either a separate interface into the projector, or the Media Block is required to overlay the subpicture with the main image and send it through the main image interface. *A subpicture interface is required to be a 100Base-T Ethernet [IEEE 802.3] interface with enough sustained bandwidth to support subpictures at up to 24 FPS for 4K content and 24 FPS or 48 FPS for 2K content.*
- **Timed Text** – Information can also enter into the projector through a data port or

be rendered and overlaid in the Media Block. *The interface is required to be a 100Base-T Ethernet [IEEE 802.3] interface.*

- **Control and Status** – *The projection system is required to also provide a 100Base-T Ethernet [IEEE 802.3] data interface that can receive control information and send status to the Media Block and SMS.*

7.5.6. Audio System

7.5.6.1. Introduction

The Audio System delivers the sound of the theatrical presentation to the audience. It is responsible for receiving the uncompressed digital audio from the Media Block, converting it to analog and directing it to the proper speakers for translation to acoustic energy. *The system is required to provide the capability for 16 channels of audio playback. The presentation is required to provide, at a minimum, a 5.1 audio format, (Left, Center, Right, Low Frequency Effects, Left Surround and Right Surround).* An audio format of 7.1 can also be provided. The undefined channels can include a Hearing Impaired and/or a Visually Impaired channels as well.

The Cinema Audio Processor can provide the digital audio conversion and the channel mapping. Its other duties can include playing the intermission program or music (often called non-sync) and allowing for monitoring in the projection booth.

7.5.6.2. Audio System Interfaces

The Audio System requires several interfaces. The main interface deals with the digital audio and the other interfaces deal with status and control. These interfaces are noted below.

- **Digital Audio** – The digital audio is delivered from the Media Block to the Cinema Audio Processor. This is a real time digital audio link that has the capacity for delivering 16 channels of digital audio at 24-bit 48 kHz or 96 kHz. *This link is required to follow [AES3-1992 (r1997)] recommended practice for serial transmission format for two-channel linearly represented digital audio data*.
- **Control and Status** – *The Cinema Audio Processor is encouraged to also provide a 100Base-T Ethernet [IEEE 802.3] interface that can receive control information and send status to Automation and/or SMS depending on the existing Automation in the theater.*

7.5.7. Screen Automation System

7.5.7.1. Introduction

A Screen Automation System can interface with life safety, motor controlled curtains, motor controlled masking, the dimmers for the lighting, existing 35mm film projectors and possibly to other devices such as the Cinema Audio Processor, and/or special effects devices. One of the challenges of Digital Cinema is to interface with the many different Automation devices installed presently in the theaters.

7.5.7.2. Automation Interface

The automation interface is a variable that is different depending on the manufacturer of the installed system. This could range from contact closures to proprietary interfaces. *The Theater System is required to translate Digital Cinema cues into something that the automation system understands, and reciprocally, is required to translate the automation information into something the SMS understands.*

7.5.7.3. Auxiliary Data Interface

The Auxiliary Data Interface is required to provide GPIO at a minimum and may contain other interfaces. It has four main interfaces, from which it communicates information to and from the SMS, and to and from the automation system. These interfaces are listed below:

The following is required:

- **GPIO** – *Communicate to and receive contact closures to/from external equipment and/or the automation systems.*

The following are optional:

- **RS-422** – To communicate to the Media Block for time sensitive information.
- **Ethernet** – To communicate to the SMS via the Theater Management Network for non-time sensitive information, configuration and software and firmware upgrades.
- **LTC** – An output to communicate [SMPTE 12M-1999 Television, Audio and Film – Time and Control Code]

7.5.8. Screen Management System (SMS)

Each auditorium is required to have a single dedicated Screen Management System (SMS). The Screen Management System provides a user interface to theater management for local control of the auditorium, such as start, stop, select a Show Playlist and edit a Show Playlist. In addition to control, the Screen Management System can monitor and run diagnostics on equipment within the auditorium and provide such status information to the exhibitor. *The Screen Management System is required to operate in one of two modes, local or remote.*

The following table depicts situations and events related to the Screen Management System.

Item, Observation or Issue	Approach
Corrupted Movie Received	SMS can validate received DCP
Valid Composition Playlist Received	SMS can validate received CPL
Movie prepped for playback is modified	SMS can check prepped movie against CPL
Playback time associations of Trailers-Movie	SMS knows show playlists and execution statistics

Table 10: Examples of Screen Management System Events

The examples in Table 10 are outside of the knowledge or control of the security system. Under a private agreement between the exhibitor and the distributor, the Screen Management System may be required to execute functions or make records of such activities under its control.

7.5.9. Multiplex Theater System Architecture

7.5.9.1. Introduction

Many Theater Systems will be part of a larger multi-screen facility. *A single TMS for Digital Cinema operations is expected to support all multiplex configurations.*

Figure 14 Multiplex Theater System Architecture below demonstrates an example architecture of one of these systems from an interface prospective. This section will consider the requirements and interfaces of a large networked system. There are two

main interface components of this larger system. The first is the Media Network and the second is the Theater Management Network.

7.5.9.2. Media Network

The Media Network is a high bandwidth, switched interface, made up of media interfaces, Disc Arrays and Media Blocks. *The Media Network is required to support sustained rate of 307 Mbits/sec for compressed image (250 Mbits/sec), audio (37.87 Mbits/sec - 16 channels, 24 bit sample, 96 KHz) and subtitle data (subpicture 20 MBits/sec) for each screen.* Additional data bandwidth is needed for ingesting new content and control/monitoring.

7.5.9.3. Theater Management Network

7.5.9.3.1. Introduction

Not all multi-screen complexes will have Theater Management Networks. When present, the Theater Management Network is a low bandwidth, shared interface, made up of Theater System devices and an Ethernet distribution system. *This is required to be accomplished using 100Base-T Ethernet [IEEE 802.3]. This network is required to support all of the control, configuration, security, software upgrades, testing and status of the Theater Systems.*

The Theater Management Network can be sub-divided into two main categories of communications:

- Operational communications – The sending of commands and data to the Theater System devices and receiving status back form those devices. *TCP/IP is required to be the protocol to send commands and configuration. SNMP/UDP/IP (Simple Network Management Protocol over User Datagram Protocol over Internet Protocol) can be used for status of the equipment.*
- Security communications – This messaging supports pre-playback, playback and post playback operations and thus interfaces with the security subsystem(s). *Such communications may take place over the same networks as above. However, security communications are required to employ Transport Layer Security (TLS) per the security requirements of Section 9* SECURITY*.*

The following is a list of devices and examples of typical communications:

7.5.9.3.2. Screen / Theater Management System (SMS/TMS)

- **Playback** – Commands and Status, Material IDs, Asset Management
- **Configuration** – Installation Values, Audio Channel Mappings, Automation Behavior, Equipment Behaviors, Equipment Diagnostics
- **Security** – Playability queries, SM Time adjusting, delivery of Key Management messages
- **Software/Firmware Upgrade** – Software Upgrade Mode/Status, Firmware Upgrade Mode/Status messages to Security Managers (SMs), collection of log reports from Security Managers (SMs)
- **Faults** – Equipment ID, Timestamp, Errors
- **Reports** – Equipment Histories, User Logs, Security Events

7.5.9.3.3. Storage

- **Playback** – Commands And Status, Material IDs, Asset Management

- **Configuration** – Installation Values, Equipment Behaviors, Equipment Diagnostics
- **Software/Firmware Upgrade** – Software Upgrade Mode/Status, Firmware Upgrade Mode/Status
- **Faults** – Equipment ID, Timestamp, Errors, Disk Error Logs
- **Reports** – Equipment History

7.5.9.3.4. Media Block

- **Playback** – Commands And Status
- **Configuration** – Installation Values, Audio Channel Mappings, Automation Behavior, Equipment Behaviors, Equipment Diagnostics
- **Security** – Contains Exhibition Security Manager performing Authentication, Key Exchange, Key Management
- **Software/Firmware Upgrade** – Software Upgrade Mode/Status, Firmware Upgrade Mode/Status
- **Faults** – Equipment ID, Timestamp, Errors
- **Reports** – Equipment History, Security Events, Playback

7.5.9.3.5. Projection System

- **Playback** – Commands And Status
- **Configuration** – Installation Values, Equipment Behavior, Equipment Diagnostics
- **Security** – Link Encryption Key Exchange with SM, log record delivery to SM
- **Software/Firmware Upgrade** – Software Upgrade Mode/Status, Firmware Upgrade Mode/Status
- **Faults** – Equipment ID, Timestamp, Errors
- **Reports** – Equipment History, Security Events

7.5.9.3.6. Cinema Audio Processor

- **Playback** – Commands And Status
- **Configuration** – Installation Values, Audio Channel Mappings, Equipment Behavior, Equipment Diagnostics
- **Software/Firmware Upgrade** – Software Upgrade Mode/Status, Firmware Upgrade Mode/Status
- **Faults** – Equipment ID, Timestamp, Errors
- **Reports** – Equipment History

7.5.9.3.7. Auxiliary Data Interface

- **Playback** – Commands And Status
- **Configuration** – Installation Values, Automation Behavior, Equipment Behaviors, Equipment Diagnostics
- **Software/Firmware Upgrade** – Software Upgrade Mode/Status, Firmware Upgrade Mode/Status
- **Faults** – Equipment ID, Timestamp, Errors
- **Reports** – Equipment History

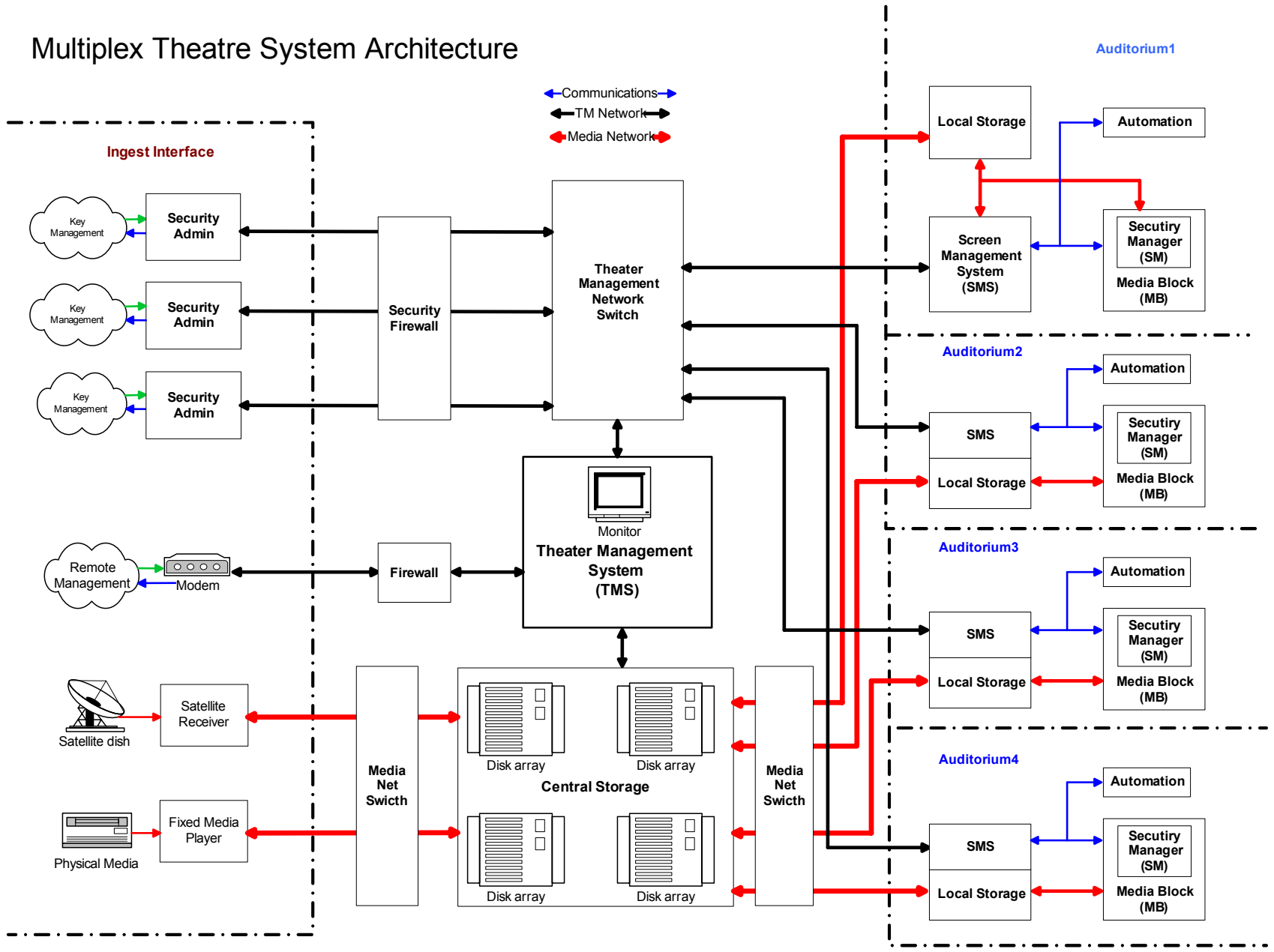

Figure 14: Multiplex Theater System Architecture

THIS PAGE LEFT BLANK INTENTIONALLY

8. PROJECTION

8.1. Introduction

The Projection System is an essential part of the Digital Cinema System. Its job is to change digital image data into light that appears on the screen. This section is broken into parts to help define the requirements, interfaces and performance specifications.

8.2. Projection System Overview

8.2.1. Functional Framework

For the purpose of documenting the specific requirements and standards for a Digital Cinema Projection system, it is helpful to divide the system into a set of components. The specifications and performance requirements for each of these components will be described in the following sections:

- **Colorimetry** – The method for color conversion (see Section 3.2.1.4 Colorimetry)
- **Performance Parameters** – Performance specifications and requirements
- **Interfaces** – The physical connections to and from the projector (see Section 8.4 Projector Interfaces)

8.2.2. Projection Fundamental Requirements

8.2.2.1. Introduction

Digital Cinema presents a challenge to create a versatile projection system. Throughout this system, some basic requirements are needed and are stated below.

8.2.2.2. Interfaces

The projector is required to have the following interfaces:

- For control and status, 100Base-T Ethernet [IEEE 802.3] interface.

The projector can have:

- Graphics and/or Text Interface (could be the same as Control and Diagnostics, e.g., Ethernet Interface)

The projector is required to have either an:

- Uncompressed image interface (with Link Encryption), or a
- Media Block Interface (if the Media Block is installed in the projector)

The projector is required to not have any test, utility or output interface that provides unencrypted content in the clear.

8.2.2.3. Alternative Content

The projector is required to not preclude the ability to present alternative content. The projector can also provide an auxiliary content input.

8.2.2.4. Single Lens

The projection system is required to provide either a single lens solution or an unattended changeover if more than one lens is required.

8.2.2.5. Color Space Conversion

The projection system is required to convert the incoming DCDM color space to its native color space.*

8.2.2.6. Pixel Count

The sampling structure of the displayed picture array (pixel count of the projector) is required to be equal to or greater than that of the specified image containers (either 4096 x 2160 or 2048 x 1080).

8.2.2.7. Spatial Resolution Conversion

The projector is required to display either a native resolution of 4096 x 2160 or 2048 x 1080. If the projector's native resolution is 4096 x 2160, and the incoming spatial resolution of the content is 2048 x 1080, then the projection system is required to perform the up-conversion of 2048 x 1080 content to 4096 x 2160. All spatial conversions are required to be done at an exact ratio of 2:1 in each axis; i.e., a projector with a horizontal pixel count of slightly higher than the image container is required to not convert the projected image beyond the image container to fill the array, nor is an image required to be converted to something less than the 4096 x 2160 or 2048 x 1080 image container size.

Should electronic image resizing or scaling be used to support a constant height projection or constant width projection theater environment, then it is required that the image resizing or scaling does not introduce visible image artifacts.

8.2.2.8. Refresh Rate

If the incoming frame rate is not the projection system native refresh rate, then the projector is required to convert it to its native refresh rate.

8.2.2.9. Forensic Marking

A Forensic Mark is required to be inserted in real time into the content at the earliest point after decryption and prior to the content data being present on any data bus outside the Media Block (see Section 9.4.6.1 Forensic Marking).

8.2.2.10. Media Block

In the preferred implementation, the projector is required to provide an area for a Media Block to be installed. If the Media Block is installed external to the projector, then a link encrypted interface is required to ensure that no Digital Cinema content is in the clear.

8.2.3. Projection Concepts

The Digital Cinema projector is one of the principal elements in the system. It is perceived that projector technology will continue to change and develop with time. There are several items affecting the projection system: color space, resolution, brightness, contrast and interfaces. *The projector is required to convert from the incoming X'Y'Z' color space to its native color space. The projector is required to support more than one spatial resolution and frame rate.*

A Reference Projector is used in the mastering process for creating the Digital Cinema Distribution Master (DCDM), with the target performance parameters and tolerances included in this chapter described below. Test patterns and measurement procedures are defined for measuring these performance parameters. It also describes a controlled environment for the mastering of projected images. The goal is to provide a means for achieving consistent and repeatable color quality.

8.3. Projected Image and Viewing Environment for Digital Cinema Content

8.3.1. Introduction

This section provides requirements defining the reference input to a Digital Cinema projector, the viewing environment, and output display characteristics for mastering and theatrical environments. These requirements are provided to ensure a single inventory distribution will be input compatible with any brand projector and that the projector output will be predictable, based on the standard format input. Nominal reference points plus tolerances are provided.

8.3.2. Input

The projector is required to support the image structures, aspect ratios, file formats, and frame rates as specified in Section 3.2 Image Specification. The projector can support other image structures, aspect ratios, file formats, and frame rates as determined by the individual manufacturer.

8.3.3. Environment

8.3.3.1. Initial Conditions

The projector is required to be turned on (including the lamp house) and allowed to thermally stabilize for 20 to 30 minutes prior to all measurements except Ambient Level. The room lights in screening room are required to be turned off, with the exception of the minimal lighting provided for working or safety reasons. For a theatrical environment room, the room lights are required to be normal theatrical lighting environment.

The projector is required to be set to calibrated mode[11], such that incoming code values are interpreted in accordance with Section 3.2 Image Specification.

8.3.3.2. Ambient Level

Stray light on the screen is required to be minimized. The use of black non-reflective surfaces with recessed lighting is encouraged.

With the projector turned off or with the lamp-house doused, measure the luminance off the center of the screen. *The ambient light level of a mastering environment reflected by the screen is required to be less than 0.01 cd/m^2 (.0029 ft-L).*

For theatrical environments, the ambient light level reflected by the screen is encouraged to be less than 0.03 cd/m^2 (.01 ft-L). Safety regulations and the placement of exit lights or access lights can result in a higher ambient light level. But, it is noted that this will reduce the contrast of the projected image.

8.3.3.3. Screen Characteristics

The screen is required to be non-specular and equally reflective over the entire visible spectrum. The screen is required to have variable black masking, adjustable to tightly frame the projected image. This is required to minimally include 1.85:1 or 2.39:1 image formats. Masking for other formats is optional.

[11] In this mode, a pure primary input code value will not generally result in projection of a pure optical primary.

8.3.4. Image Parameters

8.3.4.1. Introduction

All image parameters are required to be measured off of the screen from the center of the normal seating area in an exhibition theater. The nominal (reference) parameters and the tolerances for review rooms and theaters are summarized in Table 11.

8.3.4.2. Pixel Structure

For the exhibition theater, the sampling structure of the displayed image is required to be compliant with the image and aspect ratio specifications in Section 3.2 Image Specification.

The device structure (mesh) of the projector picture array is required to be invisible at the reference viewing distance.

8.3.4.3. Peak White Luminance

Using the white field test pattern (X'=3794, Y'=3960, Z'=3890), adjust the peak white luminance, as measured at screen center, to 48 cd/m^2 (14 ft-L), with the measurement made at the reference viewing position.

8.3.4.4. Luminance Uniformity

Using the white field test pattern (X'=3794, Y'=3960, Z'=3890), align the lamp house to minimize luminance fall-off from center to corners. *The measured luminance of the corners and sides in a 3 x 3 grid shall be at least 75% of the center, as measured from the reference viewing position.*

Follow manufacturer's recommendations for digital uniformity correction (if applicable).

Measure center to corner uniformity as described in [SMPTE 196E].

8.3.4.5. White Point Chromaticity

Using the white field test pattern (X'=3794, Y'=3960, Z'=3890), measure the white point chromaticity coordinates of the center of the screen with a spectroradiometer.

8.3.4.6. Color Uniformity of White Field

Using the white field test pattern (X'=3794, Y'=3960, Z'=3890), measure the chromaticity coordinates of the center points of a 3 x 3 grid with a spectroradiometer.

8.3.4.7. Sequential Contrast

The sequential contrast ratio is computed by dividing the white luminance (of a peak white field) by the black luminance (of a black field). *The nominal (reference) value is required to have a minimum sequential contrast of 2000:1*. The tolerances for mastering and exhibition are shown in Table 11. In order to eliminate unwanted detail or discoloration in near blacks, it is critical that Mastering Projectors have an equal or higher sequential contrast than all exhibition projectors.

Note that this is a measurement of the sequential contrast of the system. It includes the projector and the ambient light on the screen.

Image Parameters	Nominal (Projected Image)	Tolerances (Review Rooms)	Tolerances (Theatrical)
Pixel Count	2048 x 1080 or 4096 x 2160	N/A	N/A
Luminance Uniformity, corners and sides	85% of center	80% to 90% of center	70% to 90% of center
Calibrated White Luminance, center	48 cd/m² (14 fL)	±2.4 cd/m² (± 0.7 fL)	±10.2 cd/m² (± 3.0 fL)
Calibrated White Chromaticity, center from code values [3794 3960 3890]	x=.3140, y=.3510	±.002 x, y	±.006 x, y
Color Uniformity of White Field, corners	Matches center	±.008 x, y Relative to center	±.010 x, y Relative to center
Sequential Contrast	2000:1 minimum	1500:1 minimum	1200:1 minimum
Intra-frame Contrast	150:1 minimum	100:1 mininum	100:1 mininum
Grayscale Tracking	No visible color shading	No visible color shading	No visible color shading
Contouring	Continuous, smooth ramp, with no visible steps	(same)	(same)
Transfer Function	Gamma 2.6	± 2%[12] Per component	± 5%[12] Per component
Color Gamut	Minimum Color Gamut enclosed by white point, black point[13] and Red: 0.680 x, 0.320 y, 10.1 Y Green: 0.265 x, 0.690 y, 34.6 Y Blue: 0.150 x, 0.060 y, 3.31 Y	(same)	(same)
Color Accuracy	Colorimetric Match	+/- 4 delta E[14]	+/- 4 delta E[14]

Table 11: Reference Image Parameters and Tolerances

8.3.4.8. Intra-frame (Checkerboard) Contrast

With the spot meter placed at the reference viewing position, measure the luminance levels of each of the patches in the checkerboard test pattern. Intra-frame contrast is computed by summing the luminance of the white patches and dividing by the sum of the luminance of the black patches. Infra-frame contrast is reduced by many factors including projection lens flare, port glass flare, ambient light spilling on the screen and back-reflections from the room itself. Note that this measurement is made with the projector in situ, with the screening room or theater in full operating mode.

8.3.4.9. Grayscale Tracking

Using the black-to-white gray step-scale test pattern described in Table 12, the entire step-scale should appear neutral without any visible color non-uniformity or non-

[12] Least squares fit of slope of a log/log plot of measured luminance vs. input code value, using a range from peak white luminance down to 5% of peak white.
[13] The luminance of the black point is limited by the sequential contrast ratio of the projector plus the ambient light falling on the screen.
[14] Delta E is color error, defined as the geometric sum of delta u' and delta v' (square root of sum of squares).

monotonic luminance steps in the test pattern. The black-to-white gray step-scale test pattern shall be centered on the screen and occupy a rectangle sized 20% of the screen height by 80% of the screen width. The background shall be defined by code values [1565 1633 1604], which define a luminance of 4.80 cd/m^2 and chromaticity coordinates x = 0.3140 y= 0.3510. Each step shall be 8% of the screen width and shall be defined by the code values in Table 12.

Step Number	Input Code Values			Output Chromaticity Coordinates		Output Luminance
	X'	Y'	Z'	x	y	Y
1	379	396	389	0.3140	0.3510	0.12
2	759	792	778	0.3140	0.3510	0.73
3	1138	1188	1167	0.3140	0.3510	2.10
4	1518	1584	1556	0.3140	0.3510	4.43
5	1897	1980	1945	0.3140	0.3510	7.92
6	2276	2376	2334	0.3140	0.3510	12.72
7	2656	2772	2723	0.3140	0.3510	18.99
8	3035	3168	3112	0.3140	0.3510	26.87
9	3415	3564	3501	0.3140	0.3510	36.50
10	3794	3960	3890	0.3140	0.3510	48.00

Table 12: Black-to-White Gray Step-Scale Test Pattern Code Values, Luminance Values, and Chromaticity Coordinates

Using the second black-to-dark gray step-scale test pattern described in Table 13, the entire step-scale should appear neutral without any visible color non-uniformity or non-monotonic luminance steps in the test pattern. The black-to-dark gray step-scale test pattern shall be centered on the screen and occupy a rectangle sized 20% of the screen height by 80% of the screen width. The background shall be defined by code values [122 128 125], which define a luminance of 0.0064 cd/m^2 and chromaticity coordinates x = 0.3140 y= 0.3510. Each step shall be 8% of the screen width and shall be defined by the code values in Table 13.

Step Number	Input Code Values			Output Chromaticity Coordinates		Output Luminance
	X'	Y'	Z'	x	y	Y
1	122	128	125	0.3140	0.3510	0.0064
2	245	255	251	0.3140	0.3510	0.0386
3	367	383	376	0.3140	0.3510	0.1107
4	490	511	502	0.3140	0.3510	0.2339
5	612	639	627	0.3140	0.3510	0.4178
6	734	766	753	0.3140	0.3510	0.6712
7	857	894	878	0.3140	0.3510	1.0022
8	979	1022	1004	0.3140	0.3510	1.4182
9	1101	1150	1129	0.3140	0.3510	1.9263
10	1224	1277	1255	0.3140	0.3510	2.5333

Table 13: Black-to-Dark Gray Step-Scale Test Pattern Code Values, Luminance Values, and Chromaticity Coordinates

8.3.4.10. Contouring

Contouring is the appearance of steps or bands where only a continuous or smooth gradient should be seen. Because contouring is a function of many variables, it is important to look at a series of test patterns with shallow gradations to simulate naturally occurring gradations in images. Examples include horizons, particularly at sunset or sunrise, and the natural falloff around high intensity spotlights, particularly if diffused by atmosphere or lens filtration. *These test pattern ramps should be placed on a background equal to the minimum value in the ramp, so that the eye is adapted for maximum sensitivity.*

Each image shall be viewed under normal viewing distance and operating condition, and shall not exhibit any contouring (step in luminance), or color deviation from the neutral gray.

8.3.4.11. Transfer Function

The encoding transfer function is defined in terms of output-referred CIE XYZ tristimulus values. The inverse equations are:

$$X = P * \left(\frac{X'}{4095} \right)^{2.6}$$

$$Y = P * \left(\frac{Y'}{4095} \right)^{2.6}$$

$$Z = P * \left(\frac{Z'}{4095} \right)^{2.6}$$

Where P = 52.37 cd/m^2

Note: In practice, luminance at the bottom end of the transfer function is skewed by ambient light input and finite projector sequential contrast. Linearity of the photometer is critical for a useful measurement here.

Note: If the data is transported over [SMPTE 372M Link 1.5 Gb/s Digital Interface for 1920 × 1080 and 2048 × 1080 Picture Formats], code values 0-15 and 4080-4095 are reserved (illegal) code values and these code values will be clipped. For example, code values 0 thru 15 will be forced to 15 and code values 4080 thru 4095 will be forced to 4080.

8.3.4.12. Color Gamut

In an additive display, the color gamut is defined by the chromaticity coordinates and luminance values of the three primaries, the white point, and the black point. *A projector may have a larger gamut by placing the primaries anywhere where this minimum gamut is enclosed within the gamut of the projector.*

8.3.4.13. Color Accuracy

Within the minimum color gamut, all colors shall be accurately reproduced within the tolerances shown in Table 14. Table 14 gives a set of colors that can be used to verify the color accuracy.

Step Number	Input Code Values			Output Chromaticity Coordinates		Output Luminance
	X'	Y'	Z'	x	y	Y, cd/m²
Red-1	2901	2171	100	0.6800	0.3200	10.06
Green-1	2417	3493	1222	0.2650	0.6900	34.64
Blue-1	2014	1416	3816	0.1500	0.0600	3.31
Cyan-1	2911	3618	3890	0.2048	0.3602	37.94
Magenta-1	3289	2421	3814	0.3424	0.1544	13.36
Yellow-1	3494	3853	1221	0.4248	0.5476	44.69
Red-2	2738	2171	1233	0.5980	0.3269	10.06
Green-2	2767	3493	2325	0.2884	0.5282	34.64
Blue-2	1800	1416	3203	0.1664	0.0891	3.31
Cyan-2	3085	3590	3756	0.2409	0.3572	37.19
Magenta-2	3062	2421	3497	0.3382	0.1838	13.36
Yellow-2	3461	3777	2065	0.3973	0.4989	42.46

Table 14: Color Accuracy Color Patch Code Values, Luminance Values, and Chromaticity Coordinates[15]

8.3.4.14. Temporal Artifacts

Temporal artifacts, such as flicker and lag on moving highlights, can significantly impair the quality of a projected image. Although it is difficult to measure and quantify these parameters, the goal shall be to minimize the visibility of flicker and lag, such that they do not distract from the presentation.

8.3.5. Projected Image Tolerances

The reference image parameters and tolerances for the projected image in mastering rooms and exhibition theaters, as measured off the screen and including the room ambient light, are summarized in Table 11. *Where the nominal parameters are specified as minimums, these parameters shall not be constrained from future improvements as the technology improves.*

8.4. Projector Interfaces

8.4.1. Introduction

Projection systems will likely have many input/output interfaces to support the various signals that are required to send and receive data between projector, Media Block (MB) and Screen Management System (SMS). Any security aspect of the use of these interfaces is described under Section 9 SECURITY.

[15] The accuracy with which these colors (in the above tables) shall be displayed is shown in Table 11

8.4.2. Image Media Block Interface

The preferred implementation of a Digital Cinema system would locate the Image Media Block in the projector. *At a minimum, the Image Media Block is required to decrypt, decompress and forensically mark the image and provide this to the internal projector interface. The Security Manager is required to be notified in the event of tampering or removal of any Media Block. If the Image Media Block is external to the projector, then a secure interface, utilizing Link Encryption, is required between the Image Media Block and the projector.*

8.4.3. Uncompressed Image Interface

8.4.3.1. Introduction

For the mastering environments, an uncompressed image interface is required. Since mastering environments are considered trusted environments, it is not required that these interfaces support link encryption.

*For theatrical environments, the preferred solution is for the Media Block to be located inside the projector. The Forensic Mark is required to be inserted at the point of the internal interface between the Media Block and the projector. In the case where the Media Block is external to the projector, it is required that the projector uncompressed interface provide a robust Link Decryption. In this case, the Forensic Mark is required to be inserted within the Image Media Block at the output of decoding and prior to Link Encryption (*See Section 9.4.4 Link Encryption)*.*

8.4.3.2. Dual-Dual (Quad) Link HD-SDI

For mastering environments, the interface can be a dual-Dual Link HD-SDI [SMPTE 372M Link 1.5 Gb/s Digital Interface for 1920 × 1080 and 2048 × 1080 Picture Formats].

*When used in theatrical environments, it is required that the dual-Dual Link HD-SDI [SMPTE 372M Link 1.5 Gb/s Digital Interface for 1920 × 1080 and 2048 × 1080 Picture Formats] be encrypted. The encryption specification is required to be an open international standard. The encryption is required to use AES with a 128-bit key. (*See Section 9.4.4 Link Encryption).

Note: dual-Dual Link HD-SDI is to accommodate 2K 48 FPS, 12-bit.

8.4.3.3. Dual Link HD-SDI

The interface can be Dual Link HD-SDI [SMPTE 372M Link 1.5 Gb/s Digital Interface for 1920 × 1080 and 2048 × 1080 Picture Formats]. However, this interface is only compliant if provisions are made for 2K 48 FPS support (see Section 2.1.1.4 Digital Cinema Package (DCP)).

When used in theatrical environments, it is required that the Dual Link HD-SDI be encrypted. The encryption specification is required to be an open international standard. The encryption is required to use AES with a 128 bit key. (See Section 9.4.4 Link Encryption.)

8.4.3.4. 10 Gigabit Fiber

For mastering environments, 10 Gigabit fiber, also known as [IEEE 802.3ae], may be adapted for a point-to-point interface. The goal for this interface would be to use the same physical layer and adopt a protocol for streaming image data. Listed below are some of the requirements:

- Dual SC Fiber Connector (back haul status/handshake)

- Multi Mode
- Point-to-point
- Matrix Switch and/or Patchable
- Up to 100 meter runs
- Physical Interface established (Layer 1)
- Electrical Interface established (Layer 1)
- 10 Gbit/sec link bandwidth to accommodate up to DCDM in real-time

8.4.4. Graphics and Timed Text Interface

Timed Text and subpicture interfaces are required to use a 100Base-T Ethernet [IEEE 802.3] interface. This may be the same interface that is used for control and status.

8.4.5. Control and Status Interface

These signals allow the SMS, TMS, the projector and the theater automation system to communicate. The physical implementation is required to be 100Base-T Ethernet [IEEE 802.3]. The protocol used is required to be the same as the Theater Management Network. (See Section 7 THEATER SYSTEMS*)*

8.4.5.1. Control

The following is an example list of control messages that can be sent to the projector:

- Local / Remote
- Power On / Off
- Douser On / Off
- Input Select
- Test Signal On / Off
- Test Signal Selection
- User Memory Recall 1 to n
- Zoom In / Out
- Focus + / -
- Lens Shift Up / Down
- Lamp Mode Full, Half
- Lamp Hours Reset
- Keystone + / -

8.4.5.2. Status

The following is an example list of status messages that can be sent from the projector:

- Projector On / Off
- Projector Standby Mode
- Projector Cool Down Mode
- Douser On / Off
- Lamp off due to Power Management
- Temperature Readings
- Temperature Warning

- Temperature Sensor Failure
- Temperature Shut down
- Current Input selection
- Input Signal Status
- Test Signal On / Off
- Test Signal Selection
- Lamp Hours Total
- Lamp Hours Bulb Life
- Lamp Mode
- Image Format – Aspect Ratio
- Power Failure

THIS PAGE LEFT BLANK INTENTIONALLY

9. SECURITY

9.1. Introduction

This section defines the requirements for Digital Cinema security. Though security is an end-to-end process, these specifications are focused on the exhibition environment. The high level business requirements for security are:

- Enable the decryption and playback of feature films, based upon business rules agreed upon by Exhibition and Distribution.
- Provide persistent security protection against unauthorized access, copying, editing, or playback of feature films.
- Provide records of security-related events.

The high level technical requirements for security are:

- Meet the above business requirements.
- Define an open security architecture.
- Provide a minimum set of standards around which the exhibition security infrastructure can be implemented by multiple equipment suppliers.

Security is provided primarily through the application of encryption technology and the management of content key access. When content is transported and received in an encrypted fashion, it is necessary to establish standardized methods of delivering and utilizing decryption keys to unlock the content. This is known as key management. Associated with key exchange is DRM (Digital Rights Management), which establishes the rules for using content. The management of DRM is known as security management. DRM requirements include logging of content access and other security event information.

In the security architecture defined herein, security management functions are entrusted to a Security Manager (SM), a logically separable and functionally unique component of the architecture. The security system is referred to as the infrastructure that provides security features, and the Security Manager is at the heart of this infrastructure. At exhibition, each Digital Cinema auditorium shall have its own dedicated security system, which is comprised of multiple subsystems under the supervision of the Security Manager. The security system architecture is defined to provide open and standardized security operation and enable interoperability between an exhibition SM and the rest of the exhibition security infrastructure.

Section 9 SECURITY is organized as follows:

- **Fundamental Security Requirements** (Section 9.2) – System-level goals, which security implementations are required to meet.
- **Security Architecture Overview** (Section 9.3) – Definitions and description of the basic security architecture, security messaging, and role of the Security Manager.
- **Theater Systems Security** (Section 9.4) – Security and equipment functions, behavior requirements and security operations at exhibition.
- **Implementation Requirements** (Section 9.5) – Requirements for equipment implementation, physical and logical robustness and certification.
- **Security Features and Trust Management** (Section 9.6) – The requirements and implementation of security policy and trust infrastructures.
- **Essence Encryption and Cryptography** (Section 9.7) – Cryptographic requirements for essence encryption and related cryptography.

- **Digital Certificates, Extra-Theater Message and Key Delivery Message Requirements** (Section 9.8) – Detailed requirements for Digital Certificates, Extra-Theater Message and Key Delivery Message.

The following acronyms are introduced and used extensively in Section 9 SECURITY:

SM	Security Manager
KDM	Key Delivery Message
ETM	Extra-Theater Message
ITM	Intra-Theater Message
TDL	Trusted Device List
FM	Forensic Marking (Marker)
SE	Security Entity
SPB	Security Processing Block
RRP	Request-Response Pairs

9.2. Fundamental Security System Requirements

This section describes the goals for the security system. Cryptographic security requires communications connectivity between Distribution and Exhibition, above what is required for 35mm film. However, at no time do security requirements mandate continuous on-line connectivity to an exhibition facility.

Note: Due to the dynamic nature of security technology, DCI reserves the right, at some future time, to update requirements and may require changes to Digital Cinema systems as situations warrant.

9.2.1. Content Protection and Piracy Prevention

The security system shall provide a means for the securing of content against unauthorized access, copying, editing, and playback. Protection shall be standardized primarily through the application of encryption technology, management of content key access and robust logging.

9.2.2. Single Inventory and Interoperability

The security system shall support a single inventory Digital Cinema Package (DCP) delivered to every compliant theater installation. The security system architecture shall support file interoperability for both the Digital Cinema Package (DCP) and the Key Delivery Message (KDM). The security system architecture shall require system inoperability between Security Manager (SM) and Screen Management System (SMS).

9.2.3. Reliability

The security system shall recognize that the show must go on" except in extreme circumstances. The model shall support intelligent means to locate failures expeditiously, and support field replaceable security devices.

9.2.4. Support Forensics and Attack Detection

- *The security system shall produce records of the access to secured content at authorized facilities.*
- *The security system shall support techniques to expose security attacks in process prior to an actual loss.*

- *The security system shall support techniques (e.g., Forensic Marking) to implant evidence of origin of the content for use in tracing unauthorized copies of the content to the source.*
- *The security system shall support the interface(s) and operation of anti-camcorder devices.* This may include, but is not limited to, the ability to log the results of an anti-camcorder (detection of a camcorder event) or a non-functional anti-camcorder-ing system.

9.2.5. Resist Threats

The security system shall support prevention and detection of the following threats:

- *Content theft (piracy) – as noted above*
- *Unauthorized exhibition (e.g., at wrong facility)*
- *Manipulation of content (e.g., editing)*
- *Un-logged usage of content*
- *Denial of Service*

9.3. Security Architecture Overview

This section describes the architectural elements and fundamental operation of the Digital Cinema security system.

9.3.1. Definitions

- **Content** – The digital representation of a visual, audio or subtitled program. Content exists in several forms (encrypted/plaintext, compressed/uncompressed, etc) at various stages of the process in the Digital Cinema system.
- **Digital Cinema Package (DCP)** – The standardized form of content intended for delivery to theatrical exhibition facilities. DCP content components are selectively encrypted by the Rights Owner.
- **Equipment Suite (Suite)** – A set of security devices (including one Security Manager) that collectively support playback for a single auditorium.
- **Extra-Theater Message (ETM)** – One-way information packet that passes into or out of, the exhibition facility. The ETM is a generic message container.
- **Forensic Mark** – The generic term used in this specification for any or all of the following: watermarking, fingerprinting, and/or forensic watermarking functions used at the time of playback.
- **Intra-Theater Message (ITM)** – The data packet that passes between SEs assigned to a single auditorium. ITM(s) operate on two-way channels.
- **Key Delivery Message (KDM)** – The Extra Theater Message (ETM) for delivering content keys and Trusted Device List (TDL) to exhibition locations.
- **Log Data** – The data produced and stored as a result of security system activity.
- **Media Block (MB)** – A type of security device that performs media decryption.
- **Rights Owner** – The generic term used to describe the party having authority over content to negotiate terms of engagements (e.g., a studio or distributor).
- **Screen Management System (SMS)** – A (non-secure) Security Entity (SE) that directs security functions for a single auditorium on behalf of exhibition management.
- **Security Data** – The keys and associated parameters required for access to content, and managed by Security Managers.

- **Security Entity (SE)** – A logical processing device which executes a distinct security process or function. SEs are not distinguished from other theater equipment by being physically secure, but by the specific security function that they perform (see Section 9.3.3 Security Messaging and Security Entities).
- **Security Interface** – A standardized point of interoperability for security messaging.
- **Security Management** – The process of securely distributing, storing and utilizing Security Data in order to access content.
- **Security Manager (SM)** – A conceptual device Security Enitity (SE) that controls Security Data according to a defined policy. Wherever this term is used, it shall be understood that an SM is installed in each auditorium, and each reference is to an auditorium SM.
- **Stakeholder** – A party involved in a business agreement relating to distribution and exhibition of specific Content.
- **Trusted Device List (TDL)** – A list of specified security devices which are approved to participate in playback of a particular composition at the exhibition facility.

9.3.2. Security Management Approach to Security

The security architecture described herein distinguishes security management from content management. Once content is encrypted, it is "purpose neutral and safe" and can be allowed to take any path desired at any time to any destination. Thus, content management (physical distribution) can be implemented along lines that are oriented towards business needs, commercial cost effectiveness, and convenience. "Purpose neutral and safe" means once content is encrypted, its purpose has been neutralized (as to the content type, information contained, etc.) and it is safe (one does not care where it goes, how it gets there or who has access to it).

Access to encrypted content is controlled by the security management function. That is, content access is enabled or denied through control of Security Data. This function is entrusted to a Security Manager (SM), a logically separable and functionally unique component of the architecture. At exhibition, the SM controls Security Data, and consequently, access to content.

In the theater, Digital Cinema systems will have an SM assigned to each auditorium/projector. For each playback, each SM will require, and be delivered, one or more unique keys to unlock encrypted content files. All distributors will share this SM.

Each key is delivered in a Key Delivery Message (KDM) with a specified play period. That is defined as the time window when the key is authorized to unlock the content. There is a start time/date and a stop time/date associated with each key. The authorized window for each key will be part of the normal engagement negotiation between Exhibition and Distribution. The Security Manager will authenticate the identity and integrity of the auditorium security equipment for each showing, and thereafter enable the use of the appropriate keys during the authorized play window.

9.3.3. Security Messaging and Security Entities

The security system described herein implements a standardized open architecture in which equipment used at exhibition facilities can be sourced from multiple, competing suppliers. In order to achieve interoperable security operation, the security system design for Exhibition, specifies a standard message set for interoperable communications between standardized security devices (Security Entities).

9.3.3.1. Security Messages

There are two classes of messages in the architecture:

- **Extra-theater Messages (ETM)** – These are self-contained one-way messages that move Security Data and information outside or within the theater. These specifications have defined a fundamental message structure for a generic ETM, the requirements for which are normative and given in Section 9.8.2 Generic Extra-Theater Message (ETM).
- **Intra-theater Message (ITM)** – Messages that move security information within the auditorium over a real-time two-way channel. Requirements for the ITM infrastructure are given in Section 9.4.5 Intra-Theater Communications.

Figure 15 shows typical locations of SM functions[16], ETM[17] and ITM message interfaces. ETM message types are labeled with a black 1 and ITM messages with a red 2. Security Entities (SE) are filled with red diagonal lines (not all SE types are shown in this figure; see Figure 16 for more detail).

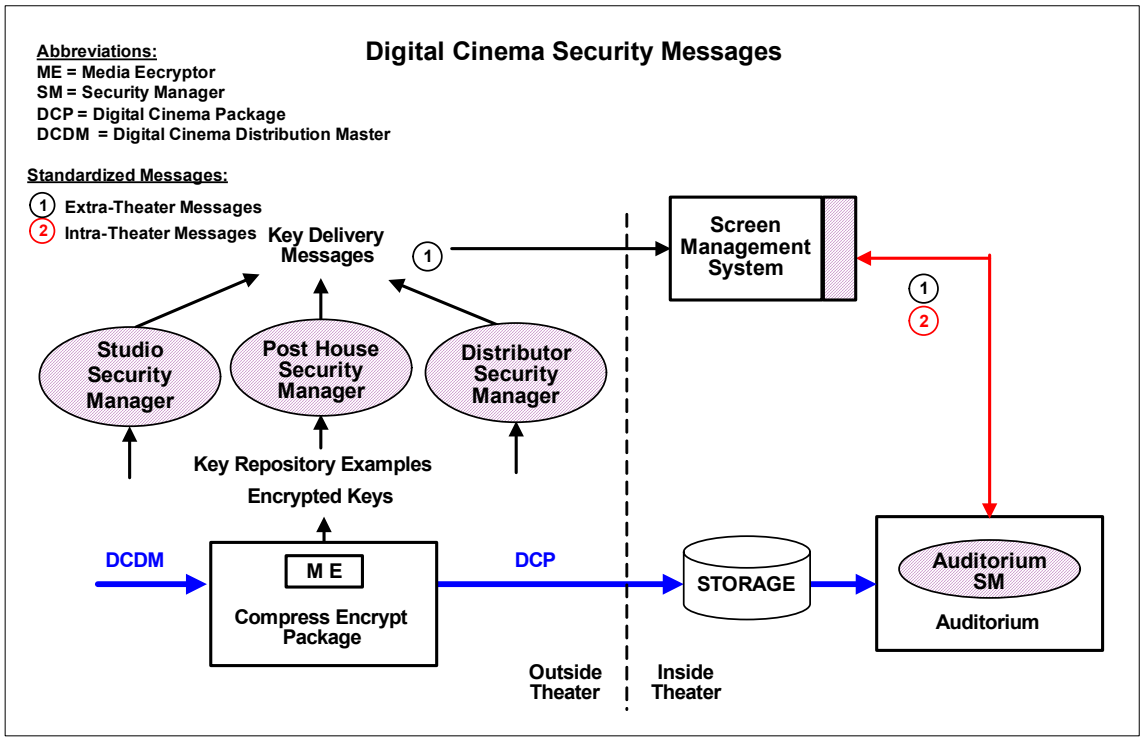

Figure 15: Digital Cinema Security Message Flow

9.3.3.2. Security Entities

Security Entities (SE) are characterized by executing in a narrowly defined security function, and having a role defined for them in a digital certificate with which they are associated. The seven defined SE(s) are as follows (these are developed more fully in Section 9.4 Theater Systems Security):

[16] There may be various types of SM functions. These specifications are focused on the auditorium SM and its security management roles. SM functional and behavioral requirements are specified in Section 9.4.3 Theater Security Operations.
[17] The KDM is a type of ETM, and its creation location may vary. The KDM is normatively specified in Section 9.8.3 Key Delivery Message (KDM).

1. *Screen Management System (SMS) – The SMS is not a secure device and therefore is not trusted to handle Security Data (keys). The SMS is trusted to send/receive commands to/from the auditorium SM, such as those required to prepare an equipment suite for playback.*
2. *Security Manager (SM) – Responsible for Security Data (keys) and Digital Rights Management within a defined sphere of control (see Section 9.6.2.1 Trust Domains)*
3. *Media Decryptor (MD) – Transforms encrypted (image, sound, etc.) content to its original plaintext form*
4. *Link Encryptor (LE) – Encrypts content transmission over links between physical devices in exhibition*
5. *Link Decryptor (LD) – Decrypts content encrypted by a Link Encryptor (LE)*
6. *Forensic Marker (FM) – Inserts markings (data indicating time, date and location of playback) in both image and audio essence in realtime at time of playback (i.e., a fingerprint or watermark inserter)*
7. *Secure Processing Block (SPB) – A Security Entity (SE) whose security function is to provide physical protection to other SEs contained within it. A Media Block is an example of a SPB. These specifications define two types of SPB physical protection perimeters (see Section 9.4.2.2 The Secure Processing Block (SPB)).*

Security Entity Notes:

- The term Security Entity should not be confused with secure entity. The term secure entity is not normatively defined or used in these specifications, as the SPB function serves this purpose, and is normatively defined.
- The Link Encryptor and Link Decryptor Security Entities exist only when Link Encryption is used.
- The SMS is not a secure device, and is sometimes viewed as part of the media server, or as part of the TMS. These security specifications focus on the SMS as the auditorium controlling device, independently of its scope or totality of other functions it may provide (see Section 9.4.2.5 Screen Management System (SMS)).

9.4. Theater Systems Security

9.4.1. Theater System Security Architecture

The Theater System is comprised of those components, at an Exhibition location, that are required by the security system to support playback of a show. Once in possession of the complete DCP and its associated KDMs, the theater security system can independently enable playback of the composition.

Theater System Security requirements are:

1. *Each auditorium shall have one authenticating Media Block, containing an auditorium SM that Rights Owners will share. The authenticating MB shall be the Image Media Block (IMB).*
2. *The auditorium SM shall have knowledge of the projector it enables, by being able to authenticate that the projector has been certified to meet content protection requirements. Authentication shall be assured via a projector certificate, which shall be associated with the projector's SPB type 2 (see Section 9.5.1 Digital Certificates and Section 9.7.3 Subtitle Encryption).*

3. *Every auditorium shall be capable of image, audio and subtitle decryption. If the Audio Media Block is separate from the Image Media Block (IMB), it shall be authenticated to the IMB SM.*
4. *Every IMB shall include image Forensic Marking (FM) capability. Every audio decryption process shall have associated audio Forensic Marking, contained within the audio MB.*
5. *If Link Encryption (LE) exists, the Link Decryptor (LD) Block shall be authenticated to the IMB SM. Forensic Marking within an LD Block shall be optional.*
6. *Image, Audio and LD Blocks shall be of the SPB type 1 (see Section 9.4.2.2 The Secure Processing Block (SPB)), and shall be field replaceable, but non-field serviceable[18].*
7. *Secure Processing Block (SPB) devices (and the SEs contained within them) shall have normative security and operational behavior requirements specified. Security Managers shall monitor the functioning of all SPB/SE devices and invoke controls to prevent use of improperly operating security equipment. To the extent possible, all security devices shall be designed with self-test capability to announce failures and take themselves out of service.*

Figure 16 presents the two fundamental auditorium security system architectures, with and without Link Encryption, and the security message types ETM and ITM. This diagram does not attempt to detail functions that are unrelated to security (e.g., decoding), but does anticipate such functions by noting where plain text content exists.

Though not shown in Figure 16, but as indicated in the requirements above, every auditorium shall support image, audio, and subtitle decryption[19], and image and audio Forensic Marking. Sound decryption and Forensic Marking may take place in the IMB or in a separate Media Block for audio. Subtitle decryption may take place in the IMB or server.

9.4.1.1. Architecture Description and Comments

The security architecture descriptions and requirements revolve around two embodiments: the SPB and the SE. As defined in Section 9.3.3 Security Messaging and Security Entities, SEs are logical devices that perform specific security functions. They are logical because these specifications do not dictate how SEs are actually designed, and more than one type of SE may be implemented within a single circuit.

All functional Security Entities (*SEs) (except the SMS) shall be contained within SPBs, which provide physical protection for the Security Entities (SEs).* The SPB is itself a literal SE Type – its security function is physical protection. The Security Entities (SEs) and SPB type 1 and type 2 containers are depicted in Figure 16. This figure shows that there are only three permitted physical protection scenarios:

- No physical protection required – Screen Management System (SMS)
- SPB type 1 protection required – All Media Blocks and Link Decryptor Blocks
- SPB type 2 protection required – Content essence entering the projector from an IMB or LD Block.

These requirements are more fully defined in the SM and SPB functional requirements below (see Section 9.5 Implementation Requirements).

[18] "Non-field serviceable" means not serviceable by other than the equipment vendor or his authorized and supervised service repair depot (see Section 9.5.2.3 Repair and Renewal).

[19] Subtitle encryption is directed primarily against interception during transport, and cryptographic protection within the theater is not required. For example, plaintext subtitle content may be transmitted from a server device to a projection unit. It is preferred, but not required, that subtitle content be maintained in encrypted form except during playback.

Note: The security network is shown (in red) in Figure 16. This is described below as operating under Transport Layer Security (TLS), a readily available and well known protocol standard for providing protection between application layer processes that must communicate between devices, in this case between auditorium devices (Secure Processing Blocks) performing security functions.[20]

As part of TLS session establishment, each party to the session presents its digital certificate to the other. In this fashion, the IMB Security Manager identifies the other SPBs in the auditorium, and mutual authentication is accomplished (see Section 9.4.3.1 Transport Layer Security (TLS) Establishment and Secure Processing Block (SPB) Authentication, and Section 9.4.5.1 Transport Layer Security Sessions, End Points and Intra-Theater Messaging). Although the SM may establish secure TLS communications with an SPB, it will not "trust" (approve) that SPB for content playback functions until the identity of such SPB appears on the appropriate Trusted Device List (TDL) for the particular composition (see Section 9.6.2 "Trust" and the Trusted Device List (TDL)).

The playback processes begins and ends with the SMS, under the control of Exhibition. Thus, the SMS is viewed as the initiator of security functions, and the window into the exhibition security system. Protection over cryptographic processes begins by requiring the SMS to communicate, in a secure fashion (i.e., under TLS), with the Security Managers (SM) under its control. The security system takes advantage of these secure command and control features to protect itself, as well as the exhibition operator, from several forms of attacks, including SMS imposters and Denial of Service.

While it is true that the security system places no physical protection requirements on the SMS, the extent to which the SMS is vulnerable to being tampered with, or its functions subverted, is a result of exhibition implementation and policy (e.g., who gets access to the SMS, how it is physically protected by room locks, operator access). The security system requires the SMS and SMS operator to identity itself to the Security Manager. The extent to which this information is reliable is subject to issues outside the scope of the security system and this specififcation. But the security system structure and standards requirements are appropriately specified to enable policies to regiment these aspects according to any particular security needs, without needing to change or enhance SE device operations or features.

[20] Transport Layer Security (TLS) can be viewed as an extension of the SPB physical protection container, but for communications, a "steel pipe" that surrounds the wire between devices. Thus, these specifications define both physical and logical protection mechanisms for all security and playback processes.

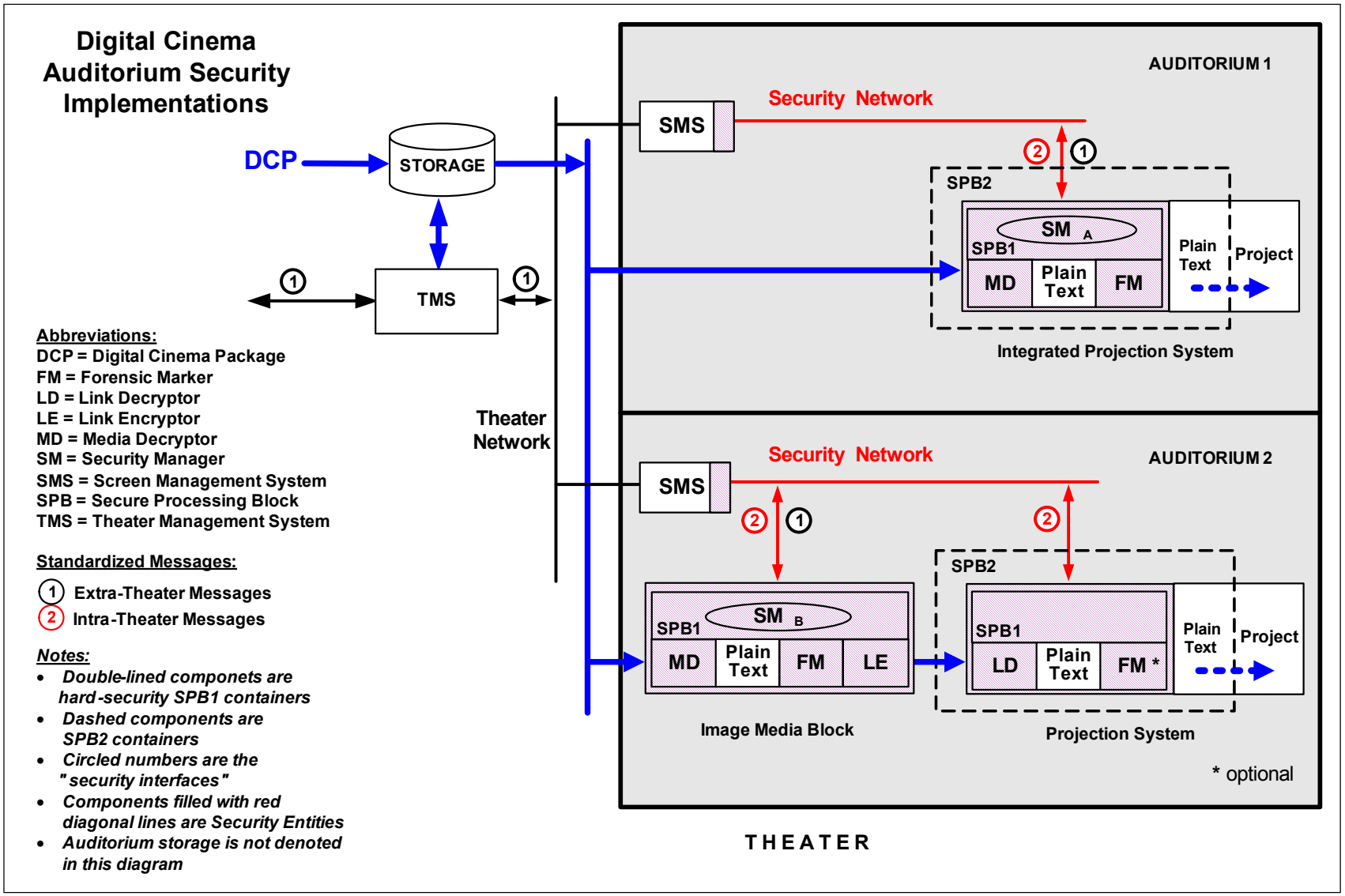

Figure 16: Digital Cinema Auditorium Security Implementations

9.4.2. Theater System Security Entities (SE)

Although SEs are not distinctly visible outside of the SPB that contains them, SEs exist logically, and their normative behavior is specified in conjunction with the requirements defined below for SPB systems (see Section 9.4.3.5 Functions of the Security Manager (SM) and Section 9.4.3.6 Functional Requirements for Secure Processing Block Systems). This is accomplished using a traditional Applications Programming Interface (API) approach, where the focus of the interoperability point is the SPB (logical) interface, and associated messaging and operational behavior at the interface.

9.4.2.1. Equipment Suites

Several SPBs may be grouped to support an auditorium. Security requirements do not define an auditorium per se, but instead refer to a collection of equipment in the display chain as an equipment suite. A playback of a show will be associated with an equipment suite, and that suite must be set up (prepared) by the requisite IMB SM ahead of the show for each playback (see Section 9.4.3.6.3 Normative Requirements: Image Media Block (IMB)). This takes place for each showing by command of the SMS.

The installation and configuration of equipment that comprises suites is an exhibition management function.

9.4.2.2. The Secure Processing Block (SPB)

The SPB is defined as a container that has a specified physical perimeter, within which one or more SE and/or other plaintext processing functions are placed (e.g., decryptor, decoder, Forensic Marker). The SPB exists to enclose SEs and other devices in the content path, impede attacks on those SEs, and to protect signal paths between the SEs.

There are two normatively defined SPB types:

- **Secure Processing Block type 1** – An SPB type 1 provides the highest level of physical and logical protection. *Image, sound and Link Decryptor Blocks shall be contained within a type 1 SPB.* (These are shown as double-lined boxes filled with diagonal lines in Figure 16.)
- **Secure Processing Block type 2** – An SPB type 2 provides a lesser perimeter of protection, for content or security information that does not require the full SPB type 1 protection. *SPB type 2 protection shall be provided by projectors as shown as the dotted line around the SPB type 1 devices as shown in Figure 16.*

Secure Processing Blocks (*SPBs) shall provide security perimeters that meet minimum security requirements as defined in Section 9.5.2* Robustness and Physical Implementations*. Both SPB types are considered a Security Entity (SE), and shall carry a digital certificate with their SPB role, such that they may be authenticated to the SM (see Section 9.5.1 Digital Certificates and Section 9.8.1.3 Naming and Roles).*

9.4.2.3. Media Blocks (MBs)

The term Media Block[21] (MB) has been used by the Digital Cinema industry in a number of ways. In this Section 9 SECURITY, it has a very narrow scope: An MB is an SPB that performs essence decryption, i.e., it contains at least one MD. *Other SE functions may also be present within a MB SPB, as described below:*

[21] In Section 7 THEATER SYSTEMS, Media Blocks are also discussed. The terminology used there is not strictly security focused, because other important equipment requirements such as storage and server functions are discussed. Depending upon a particular design, server functions may well be part of what is in a MB, when viewed in its entirety. Since other such functions are invisible to security, they need not be discussed within the security arena, and are not addressed in this security chapter.

- **Image Media Block** (IMB) – The Image Media Block (IMB) is a type of Secure Processing Block (SPB) that contains an SM, Image Media Decryptor (MD), decoder, Forensic Marking (FM) and optionally Link Encryptor (LE) functions. The IMB SM is responsible for security for a single auditorium, and it authenticates other SPBs that are required to participate in showings. Other such SPBs are referred to as remote or external SPBs.
- **Remote Media Block** – A remote Media Block is a remote SPB that contains other types of MDs, such as those used for audio or subtitles, but does not contain an SM. An Audio Media Block is an example of a Remote Media Block.

9.4.2.4. Security Manager (SM)

The SM controls Security Data and content access in a manner consistent with the policies agreed upon by the Stakeholders who rely upon it. *There is one* SM *for each auditorium, and it shall be contained within the IMB. The Rights Owners (Distribution) shall share this* SM *for their security needs.*

Security Manager functions shall conform to the requirements as given in Section 9.4.5.3 Intra-Theater Message Details and Section 9.6.1 Digital Rights Management. The Security Manager is a self-contained system with an embedded processor and real-time operating system. *SM functions shall not be implemented outside of the secure environment of the Image Media Block (IMB) SPB.*

The Security Manager is a self-contained processor running a real-time operating system. The operating environment shall be limited to the FIPS 140-2 limited operational environment category (Section 9.5.2.5 FIPS 140-2 Requirements for Type 1 Secure Processing Blocks), meaning that the SM's operation shall not be modifiable in the field. The only security communication with systems (processors) external to the SM's SPB shall be by Transport Layer Security (TLS) over a network interface per Section 9.4.5.1 Transport Layer Security Sessions, End Points and Intra-Theater Messaging. The preferred real time operating system would use the National Security Agency (NSA) kernel and would be specifically designed for secure operations. The Security Manager software shall use all appropriate security features of the operating system.

Security Manager software changes and upgrade requirements are given in Section 9.5.2.7 SPB Firmware Modifications.

9.4.2.5. Screen Management System (SMS)

Theater management controls auditorium security operations through the Screen Management System (SMS). Because the SMS interacts and communicates directly with the security system, it is also considered to be part of the Security Entity (SE)[22]. The SM responds to the directives that Theater Management System (TMS) issues via the SMS. For purposes of simplicity, and subject to the TMS constraint below, this specification uses the term SMS to mean either/both Theater Management System (TMS) or Screen Management System (SMS).

SMS Requirements:

- *The SMS shall carry a DCI compliant digital certificate (see Section 9.8.1 Digital Certificates) to identify the SMS entity to the SM. The SMS certificate shall indicate only the SMS role unless the SMS is contained within a SPB meeting the protection requirements for any other designated roles.*
- *As the SMS is not required to be physically secure, the SMS's private key shall be contained within a physically secure device associated with the SMS. Such*

[22] The Screen Management System (SMS) is part of the Security Entity (SE) but is not a secure device.

devices shall meet the requirements for secure silicon (see Section 9.5.2.2 Physical Security of Sensitive Data). For simplicity, it is encouraged that this be accomplished using a secure integrated circuit, smart card, dongle, etc.

- *In the event that Exhibition command and control designs include the TMS as a device that interfaces with the SMs, such a TMS shall be viewed by the security system as an SMS, and it shall contain a secure private key, carry a digital certificate and follow all other SMS behavior, Transport Layer Security (TLS) and Intra-Theater Message (ITM) communications requirements.*
- *Exhibition management shall designate, via the "StartSuite" ITM command, the identity of the particular SMS under whose command each auditorium SM operates.*
- *In the case of a fully integrated stand alone projection system, an SMS Security Entity (SE) proxy shall exist within the system, which fulfills the SMS function.*

SM interaction with the SMS[23] is normatively defined (see Section 9.4.3.5 Functions of the Security Manager (SM)). These include the requirements that:

- The SMS's identity appears on the KDM Trusted Device List (TDL).
- The SM provides log records to the SMS for which it operates, as well as the operator "AuthorityID" field (Section 9.4.5.2.4 Request-Response Pairs (RRP)) of the SMS.

9.4.3. Theater Security Operations

This section describes how equipment conforming to the security system is used in normal theater operations. The show, expressed in a Show Playlist, consists of exhibition-arranged sequences of compositions, any of which may be encrypted. One or more Rights Owners may supply Key Delivery Message(s) (KDMs) to provide all the content keys required for the Show Playlist.

With respect to security, theater operations break down into four categories:

1. Secure communications establishment and Secure Processing Block (SPB) device authentication
2. Pre-show preparations
3. Playback
4. Post playback

The SMS is generally responsible for initiating activity within each category, except the last.

9.4.3.1. Transport Layer Security (TLS) Establishment and Secure Processing Block (SPB) Authentication

Exhibition has the liberty to power their equipment up and down as desired. However, the Security Managers (SM) must authenticate the equipment within their respective suites, and establish secure Transport Layer Security (TLS) sessions with each remote SPB with each power-on.

- *For each equipment suite, an SM initiated power-on initialization process shall establish secure TLS sessions between the Image Media Block (IMB) SM and the Screen Management System (SMS), and between the Image Media Block (IMB) SM and the remote SPBs.*

[23] SMS-to-SM Intra-Theater Message (ITM) commands (see Section 9.4.5.3.1 Screen Management System to Security Manager Messages) include means to carry SMS operator identification via the "AuthorityID" field. The specific operational policies used at exhibition that surround operator identification, empowerment or enforcement are outside the scope of this specification.

- *The IMB SM shall authenticate the SMS and the remote SPBs as part a of TLS session establishment.* A remote Secure Processing Block is any SPB separated from that which contains an SM, and for which the SM has security control over, i.e., those SPBs in its equipment suite.

Note that the establishment of each TLS session enables the SM to authenticate the other party (SPB or SMS) to the session and provides for secure ITM communications within the auditorium. The SM does not "trust" such party for security functions related to content playback, unless the identity of the party appears on the Trusted Device List (TDL) delivered in the Key Delivery Message (KDM) for that particular Composition Playlist (CPL) (see Section 9.4.3.5 Functions of the Security Manager (SM) and Section 9.8.3 Key Delivery Message (KDM)). Thus, device authentication and secure communications occurs independently of "trust"; the former being an exhibition equipment/infrastructure security issue, the latter being specific to a Rights Owner and a composition. Where content is not encrypted and no KDM/TDL exists, the SM does not invoke trust control.

The flow chart in Figure 17 is an example of how a system start-up may occur. This flow chart is informative. There are other designs that may have different steps or different sequences that will accomplish the same result and meet the requirements of this specification.

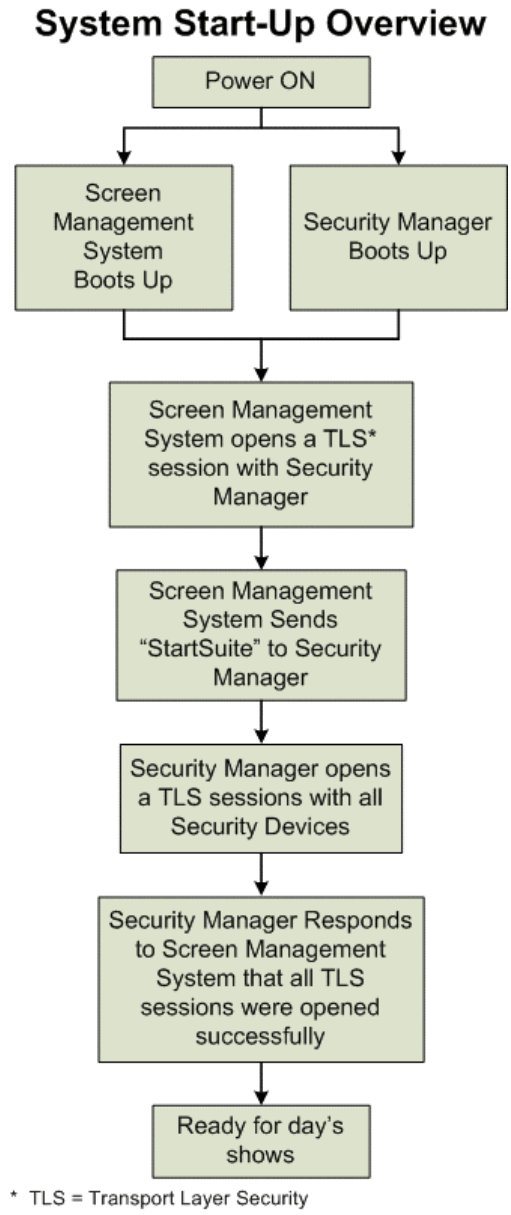

Figure 17: System Start-Up Overview

9.4.3.2. Pre-show Preparations

Pre-show preparations include tasks to be performed (well) in advance of show time to ensure adequate lead-time to resolve any issues that might impact the composition showing. These preparations do not prepare an auditorium for a showing, but are designed to provide assurance that all prerequisites for a specific showing have been satisfied.

- **Composition Playlist (CPL) check(s)** – *Composition Playlists (CPL) shall be validated by the Security Manager participating in the respective composition playback.*
- **Composition decryption preparations** – Each encrypted composition will have associated with it one or more Key Delivery Message(s) (KDMs), carrying time window constraints, decryption keys, and a Trusted Device List (TDL). *The SMS, working with the security infrastructure, shall verify that the content keys required*

for playback are available and valid for scheduled exhibitions, and the suite equipment to be used for playback (including the SMS) is on the TDL.

- **Show playback preparations** – Exhibitors will assemble Show Playlists specific to each exhibition event, containing various compositions (including advertising, trailers, movies, etc.). *Because the final Show Playlists may involve many content keys and/or consist of content from different Rights Owners, show preparations should ensure the auditorium SM has confirmed possession of all necessary* Key Delivery Message(s) (*KDMs) for the Show Playlist. In addition, FM devices may require configuration (keying) by the* SM.

The flow chart in Figure 18 is an example of how a system may prepare to execute a Show Playlist. This flow chart is informative. There are other designs that may have different steps or different sequences that will accomplish the same result and meet the requirements of this specification.

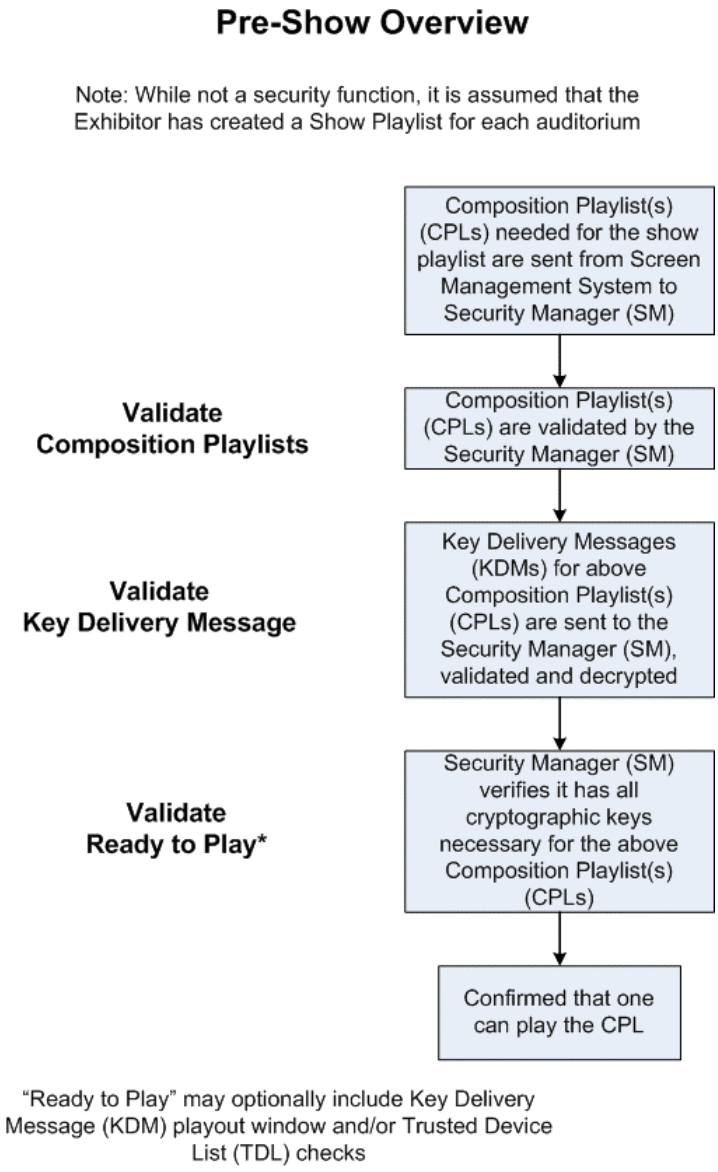

Figure 18: Pre-Show Overview

9.4.3.3. Show Playback

Show playback processes include auditorium preparations for the playback of a specific Show Playlist, and the actual run-time security functions that include content decryption at the Media Decryptor(s), link encryption/decryption, forensic marking, and recording of log data.

- **Equipment suite preparations** – *The* SM *shall prepare the suite for playback prior to each composition showing. This shall include validation of the authenticity and "trust status" of the SMS and suite SPBs, and delivery of all necessary keys per Section 9.4.3.5 Functions of the Security Manager (SM). SMs shall obtain trust status by confirming that the SMS and SPBs are listed in the TDL delivered as part of each KDM required for the entire Show Playlist. Different compositions may have different requirements.* The "PrepSuite" RRP command (see Section 9.4.5.3.1.5 PrepSuite) facilitates these functions.
- **Streaming media decryption** – Playback of a show consists of a concatenation of compositions that require serial or (separately) parallel decryption. *One or more Media Decryptors (e.g., for image, audio or subtitle) may be involved.*
- **Link Encryption (LE) and Link Decryption (LD)** – *If Link Encryption is used, the* SM *shall support keying of LE and LD Security Entities.*
- **Forensic Marking** – *Each MB shall apply Forensic Marking to image and audio data during playback.*
- **Log data recording** – *The SEs shall capture and transfer log records of playback events to the Image Media Block (IMB) SMs as specified in Section 9.4.6.3 Logging Subsystem.*

The flow chart in Figure 19 is an example of how a system may execute a Show Playlist. This flow chart is informative. There are other designs that may have different steps or different sequences that will accomplish the same result and meet the requirements of this specification.

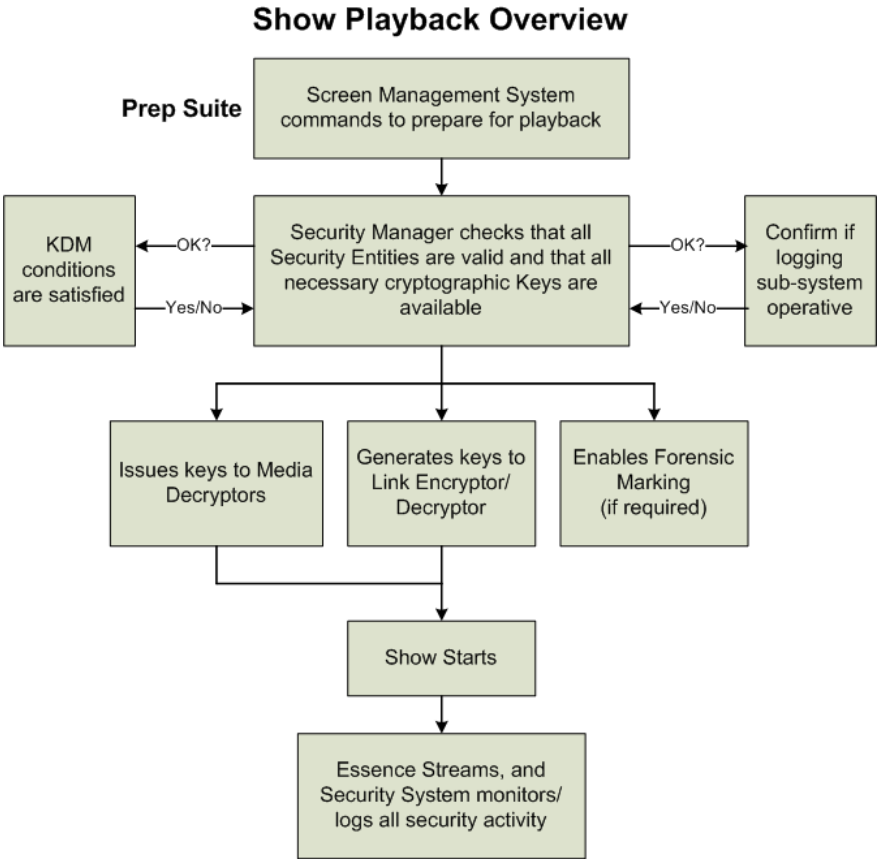

Figure 19: Show Playback Overview

9.4.3.4. Post Playback

Post playback activity primarily includes cleansing SPBs of sensitive data and collection of log data.

- **Media Decryptor and Link Decryptor content key zeroing** – *MDs and LDs shall honor a validity duration period supplied with the keys provided by the SM, after which playback keys shall be purged*[24] *from the respective SE.*
- **Collection of log data** – *The Image Media Block* SM *shall be responsible for collection of all playback event log data from SPBs within the playback suite it supports per Section 9.4.6.3 Logging Subsystem.*
- **Purge Suite** – *The SMS shall be able to invoke a process that cleanses a suite of specific KDM content keys and suite preparations.* This would be used as a last minute decision to change auditoriums, and/or to recover SPB memory storage, for example.

There are no end of engagement requirements placed on the security system. Exhibition may cleanse Screen Management System (SMS) or Theater Management System (TMS) devices, content storage devices, Key Delivery Message(s) (KDMs), etc. according to their own operational needs. Defined security system behavior places controls on Security Data, keys, etc. such that security interests are maintained.

The flow chart in Figure 20 is an example of those items a system performs following a completed Show Playlist. This flow chart is informative. There are other designs that

[24] As used above and elsewhere in these specifications, the term purge shall mean the data is permanently erased or overwritten such that it is unusable and irrecoverable (also known as "zeroization" in FIPS 140-2).

may have different steps or different sequences that will accomplish the same result and meet the requirements of the specification.

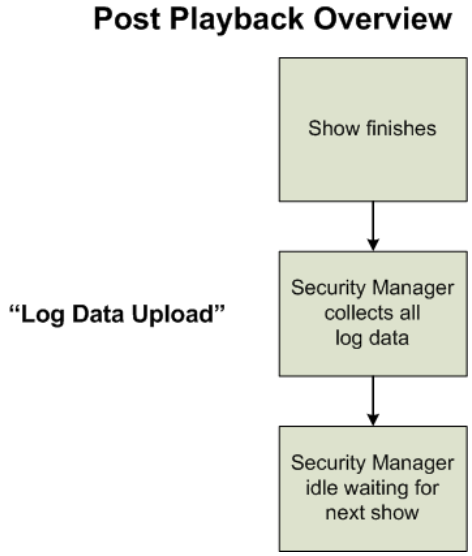

Figure 20: Post Playback Overview

9.4.3.5. Functions of the Security Manager (SM)

Auditorium Security Managers (SMs) are responsible for overseeing the security aspects of the auditorium they are assigned to (installed in). Each SM operates independently from other SMs in responding to the auditorium's Screen Management System (SMS) to enable playback of content. The required SM functions are described below.

In listing these functions the approach is that of a reference model for SM behavior, meaning that these specifications do not define required implementation methods. A standards-compliant implementation must, however, have the same input/output behavior as the reference model.

Security Manager (SM) Functions:

1. *Receive, store, decrypt, and validate signatures on Key Delivery Message(s) (KDMs) that are targeted at the SM.*
2. *Enforce the playback time window specified in the KDM by:*
    a. *Delivering content keys to Media Decryptors along with usage periods fully contained within the KDM time window,*
    b. *Deleting expired Key Delivery Message(s) (KDMs) and associated keys from (its) storage.*
3. *Reject ETM messages that are not recognized as DCI compliant standardized messages.*
4. *Validate Composition Playlists (CPL), and log results as a prerequisite to preparing the suite for the associated composition playback.*
5. *Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Log information necessary to detect deviations (including restarts, see Section 9.4.5.3.1.1 StartSuite) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:*
    a. *Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.*

b. *Audio – Process integrity pack information, including the hash (HMAC).*

6. *Maintain a list of certificates required to authenticate CPLs and ETM, as applicable[25].*
7. *Perform remote Secure Processing Block (SPB) and Screen Management System (SMS) authentication through Transport Layer Security (TLS) session establishment, and maintain the certificate lists so collected.*
   a. *Associate certificate lists with TDLs delivered in KDMs to support the identification of security devices that are trusted/not trusted.*
   b. *Maintain TLS sessions open for not more than 24 hours between complete restarts (i.e., forces periodic fresh TLS keys).*
8. *Support TLS-protected ITM standards per Section 9.4.5.2 Intra-Theater Message Definitions. ITM functions shall include:*
   a. *Maintain TLS sessions with suite SPBs (including the SMS),*
   b. *Querying/receiving status of other SPBs external to the SM's Media Block,*
   c. *ITM usage and operational behavior means with respect to (a) and (b) sufficient to detect any equipment substitutions,*
   d. *Reporting status on CPL playability, suite readiness and other SM and SPB conditions to the SMS,*
   e. *Movement of security (or security related) information (e.g., content and LE keys, logging data, secure time).*
9. *Prepare and issue protected content keys to external Media Decryptor (MD) and Forensic Marking (FM) SEs as may require keying per the CPL. Constrain issuance of keys to:*
   a. *Suite preparation command (see Section 9.4.5.3.1.5 PrepSuite) received from an SMS that appears on the Trusted Device List (TDL) for the composition being prepared for playback.*
   b. *Usage validity periods of six (6) hours for remote SPBs. Do not allow the six hour period to extend beyond the playback time window of (2).*
   c. *Authenticated and trusted Secure Processing Blocks (SPBs) per (7).*
   d. *Media Decryptors (e.g., image, sound, subtitle, link encryption) in SPBs which meet status requirements of (14).*
   e. *Specific MDs matching the key type IDs as designated the KDM.*
   f. *Receipt by the SM of a valid CPL for the composition being prepared for playback per (4).*
10. *Support Link Encryption (LE) keying (if link encryption is used) by:*
    a. *Generating unpredictable keys per Section 9.7.6 Key Generation and Derivation and having a usage validity period on a per-showing basis (i.e., each showing requires a fresh LE key), which is generated per item (11).*
    b. *Transferring LE keys only to an authenticated and trusted (7) Link Decryptor Block installed in an authenticated and trusted (7) projector.*
    c. *Support link encryption operational processes for combinations of clear and encrypted content according to Section 9.4.4 Link Encryption.*
11. *Perform suite playback preparations (via SMS "PrepSuite" command) per (9) and (10) for each showing, within 30 minutes prior to showtime. Though (9) establishes key validity periods of six hours, security equipment integrity checks*

[25] Certificate management is out of scope.

shall be executed, and suite re-keying should be executed, prior to each showing.

12. *Maintain secure time for a specific auditorium, including SPB time synchronization requirements per Section 9.4.3.7 Theater System Clocks and Trustable Date-Time.*
13. *Execute log duties for the assigned auditorium per Section 9.4.6.3 Logging Subsystem.*
14 *Execute Forensic Marking (FM) control operations per Section 9.4.6.2 Forensic Marking Operations*
15. *During all normal operating conditions, continuously monitor and log integrity status of all security components ("QuerySPB" command) so as to detect attacks, and preclude delivery of keys/content to, or playback on, compromised or improperly operating security equipment.*
16. *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).*
17. *Secure Processing Block behavior and suite implementations shall permit the SM to prevent or terminate playback upon the occurrence of a suite SPB substitution or addition since the previous suite authentication and/or ITM status query. The SMs shall respond to such a change by immediately purging all content and link encryption keys, terminating and re-establishing: a) TLS sessions (and re-authenticating the suite), and b) suite playability conditions (KDM prerequisites, SPB queries and key loads). "Prepsuite" command(s) shall be issued per (9) prior to the next playback.*
18. *Perform and log all the above functions under the operational (not security) control of the particular SMS designated by the exhibition operator per Section 9.4.2.5 Screen Management System (SMS). The designation shall be authenticated to the SMS's certificate, and may include identities of system operator(s) and equipment installer(s).*
19 *The use of multiple KDMs for any CPL is allowed. In cases where KDM playback time windows do not overlap, each KDM shall be treated as unique and its contents applied. In cases where the time windows overlap:*
    a. *The SM shall honor any valid* playback *time window.*
    b. *Should inconsistencies in the TDL exist during the time window overlap, the SM shall attempt to enable playback using the sum of the TDLs (i.e., "trust" the union set of the two or more TDLs). The SM shall otherwise follow the TDL information for non-overlapping time window periods. Under no circumstances shall the SM disrupt any single showing because of an overlap condition.*

9.4.3.6. Functional Requirements for Secure Processing Block Systems

Each type 1 Secure Processing Block (SPB) can be considered an SPB system, since it operates as a collection of SEs. Similarly, the projector also has its associated type 2 SPB, which does not contain SEs, but fulfills security functions as described below. (Secure Processing Block types are defined in Section 9.4.2.2 The Secure Processing Block (SPB).) In order to facilitate a composition playback, SPBs constituting the suite must work in a coordinated fashion under control of the suite's SM, contained within the Image Media Block (IMB).

Functional requirements of the SM are defined in Section 9.4.3.5 Functions of the Security Manager (SM). This section defines the functions and operational requirements for the following SPB systems:

- Projector Secure Processing Block (SPB)
- Link Decryptor Block (LDB) Secure Processing Block (SPB)
- Image Media Block (IMB) Secure Processing Block (SPB)
- Remote Audio Media Block Secure Processing Block (SPB)

9.4.3.6.1. Normative Requirements: Projector Secure Processing Block

From a security perspective, a projection system consists of the projector Secure Processing Blocks (SPB) type 2 and its companion SPB, which will be either the Link Decryptor Block (LDB) or Image Media Block (IMB).

The following are the normative requirements for the projector Secure Processing Block (SPB):

1. *The projector's companion SPB (Link Decryptor Block or Image Media Block) shall be physically inside of, or otherwise mechanically connected to, the projector Secure Processing Block (SPB).*
2. The projector and Link Decryptor Block (LDB) *Secure Processing Blocks (*SPBs) shall be authenticated to the *SM*. *However, authentication does not ensure that the two SPBs are mechanically connected to each other or ensure that an IMB/projector system is mechanically connected.* Therefore, an electronic marriage shall take place upon installation of an IMB or LDB projector pair. This physical/electrical connection shall be battery-backed and monitored 24/7 by the companion SPB and, if broken, shall require a re-installation (re-marriage) process.

   Breaking the marriage shall not zero the projector SPB long term identity keys (RSA private), see item (7).
3. *To support projector maintenance, the projector SPB may be serviceable, but access is security-sensitive because of the possibility of tampering during service access. The projector SPB shall implement a "projector SPB access door open" event signal to the companion SPB. Playback shall not be permitted and shall terminate if the projector SPB access door is open.*

   The projector SPB is not required to perform security logging functions or contain a clock counter or battery for logs, since access openings will be logged by the companion SPB via the marriage connection (per LDB and IMB requirements below).
4. *Projector SPB designs shall not allow physical access to signals running between the companion SPB and the projector SPB without breaking the marriage, in which case a re-installation shall be required and tampering will be observed by the authorized installer (see Section 9.5.2.5 FIPS 140-2 Requirements for Type 1 Secure Processing Blocks).*
5. *The projector SPB shall accept the decrypted streaming image signal from either the Image Media Block (IMB) or Link Decryptor Block (LDB) SPB and process accordingly.*
6. *The projector SPB shall provide at least a type 2 image signal path and tamper/access protection container.*

7. *The projector SPB shall include a secure silicon host device (see Section 9.7.3 Subtitle Encryption) to support an identity key pair (private key), and appropriate intelligence for support of the following:*
    - Authentication per implementation options in Section 9.4.3.6.5 SPB Systems Implementation and Standards Options
    - Electronic marriage and SPB "open" signal
    - SPB access door opening event detection
    - Secure silicon device operational status (e.g., keys zeroed, etc.)

9.4.3.6.2. Normative Requirements: Link Decryptor Block (LDB)

The following requirements are normative where Link Encryption is used:

1. *As part of the installation (mechanical connection to projector and electrical initiation), perform electrical and logical marriage with the projector SPB. Electrical connection integrity between the Link Decryptor Block and the projector SPB shall be monitored 24/7. Should the integrity of the connection be broken, log the event and require a re-installation process before becoming active again.*

   Breaking of the LDB/projector SPB marriage shall not zero the LDB SPB long-term identity keys (RSA private keys).
2. *Perform content link decryption, and pass the decrypted streaming image to the appropriate circuitry inside the projector SPB.*
3. *Respond to the Security Manager's (SM's) initiatives in establishing a Transport Layer Security (TLS) session and Link Decryptor Block authentication. Maintain this session until commanded to terminate.*
4. *Link Decryptor Blocks (LDBs) shall not establish security communications with more than one SM at a time.*
5. *Accept and track time information from the Image Media Block (IMB) SM over the Transport Layer Security (TLS) link. While powered, maintain time synchronism with the SM. When not powered, maintain a battery powered clock counter that shall be used to time stamp log record events.*
6. *Respond to SM "status" queries, and other Intra-theater Messages (ITMs) and SM commands as necessary to support SM behavior requirements.*
7. *Accept and store link decryption keys, and associated parameters, provided by the SM. The LDB shall have the capacity to store at least 64 key/parameter sets.*
8. *Purge LD keys upon expiration of the SM designated validity period, SM "purge" command, Link Decryptor Block SPB tamper detection, break of projector LDB SPB electrical connection, or change in TLS network parameters suggestive of an attack or equipment substitution.*
9. *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.*
10. *Monitor Link Decryptor Block SPB 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 Critical Security Parameters (CSP)). Do not purge log records. If the intrusion takes place while communication with the SM is possible, issue an "alert" message to the SM.*

11. *Monitor projector SPB marriage and operational status 24/7 and create log records and/or alert messages accordingly.*

9.4.3.6.3. Normative Requirements: Image Media Block (IMB)

The following are normative requirements for the Image Media Block:

1. *Perform all SM functions as defined under Section 9.4.3.5 Functions of the Security Manager (SM).*
2. *As part of the installation (mechanical connection to the projector and electrical initiation), perform electrical and logical marriage with the projector Secure Processing Block (SPB). Electrical connection integrity shall be monitored 24/7, and should the integrity of the connection be broken, log the event and require a re-installation process before becoming active again.*
3. *Monitor IMB SPB 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 Critical Security Parameters (CSP)). If communication with the SMS is available, issue an alert message. Do not purge log records.*
4. *When connected directly to the projector SPB (i.e., no link encryption used), monitor the projector SPB marriage and operational status 24/7 and create log records accordingly. Upon break of the marriage or projector SPB open event, if communication with the Screen Management System (SMS) is available, issue an alert message. Do not purge log records.*

   Breaking of the IMB/projector Secure Processing Block (SPB) marriage shall not zero the IMB Secure Processing Block (SPB) long-term identity keys (RSA private keys).
5. *Perform Media Decryption for image essence.*
6. *Perform Forensic Marking for image essence.*
7. *After image decryption and Forensic Marking (and other non-security plain text functions as appropriate by design), pass the image signal to the projector SPB or Link Decryptor Block, as appropriate.*
8. *If included as part of the IMB Secure Processing Block (SPB) design, perform streaming Media Decryption and Forensic Marking for audio, and pass the decrypted audio essence to external components. If not part of the IMB Secure Processing Block (SPB), perform support functions for the remote Audio Media Block Secure Processing Block (SPB) per the requirements given in (1).*

9.4.3.6.4. Normative Requirements: Audio Media Block

The existence of the Audio Media Block SPB depends upon implementation choice (the audio decryption function may alternatively be contained within the Image Media Block SPB). In the case where audio decryption takes place in its own remote SPB, the following requirements shall be met:

1. *Respond to the Security Manager's (SM's) initiatives in establishing a Transport Layer Security (TLS) session (and Audio Media Block authentication). Maintain this session until commanded to terminate.*
2. *Audio Media Blocks shall not establish security communications with more than one SM at a time.*
3. *Accept and track time information from the Image Media Block (IMB) SM over the TLS link per Section 9.4.3.6.6 Permanently Married Implementations. When not*

powered, maintain a battery powered clock capability that shall be used to time stamp log record events.

4. *Respond to SM "status" queries, and other Intra-Theater Messages (ITMs) and SM commands as necessary to support SM Section 9.4.3.5 Functions of the Security Manager (SM) requirements.*
5. *As required, accept and store audio Forensic Marking and decryption keys (including associated parameters) provided by the SM. The Audio Media Block shall have enough capacity to store at least audio 512 key/parameter sets.*
6. *Perform streaming Media Decryption and Forensic Marking for audio essence, and pass the decrypted essence to external components as designed.*
7. *Purge audio keys upon expiration of the SM designated validity period, SM "purge" command, Audio Media Block SPB tamper detection, or change in the TLS network parameters suggestive of an attack or equipment substitution.*
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 Logging Subsystem.*
9. *Monitor Audio Media Block SPB 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 Critical Security Parameters (CSP)). Do not purge log records. If the intrusion takes place while communication with the SM is possible, issue an alert message to the SM.*

9.4.3.6.5. SPB Systems Implementation and Standards Options

The following are considerations for implementation details, and standardization.

- 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. *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.
- *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.*
- 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.

9.4.3.6.6. Permanently Married Implementations

This section assumes that the LDB and IMB are implemented as field replaceable SPB modules. It is not mandatory, however, that they be implemented in this fashion. It is allowed, for example, for the LDB to be permanently married to a projector, and not field replaceable. In such a case where the projector and its companion SPB (LDB or IMB) are not field separable, there is no marriage event, and thus no reason to monitor whether the marriage connection is broken. This relieves the companion SPB from marriage monitoring duties, but does not change the requirement for IMB or LDB equivalent SPB functions, and the projector SPB, to meet the respective SPB type 1 and type 2 physical and logical protection requirements of Section 9.5 Implementation Requirements, and the normative requirements as specified above,

except as the latter requirements relate to marriage event and connection monitoring.

Implementations that do not meet the marriage functions, per the normative requirements of this section, shall not permit field replacement of the IMB or LDB security function as appropriate according to which function is the companion SPB to the projector, and shall require the projector SPB and companion SPB system to be replaced in the event of an SPB failure.

A deviation from these requirements shall be considered non-compliant and a "Security Function Failure" (see Section 9.5.5 Compliance Testing and Certification).

9.4.3.7. Theater System Clocks and Trustable Date-Time

To ensure playback times and event log time stamps are time-accurate, means must exist to distribute and maintain proper security system time. *Time shall mean UTC (Coordinated Universal Time).* See ASN.1 standard syntax for transferring time and date data "GeneralizedTime" and "UTCTime".

Security Managers shall each be responsible for maintaining secure and trusted time for the auditorium to which they are assigned (installed). The security system clock requirements are:

- *The Image Media Block (IMB) SM shall be responsible for establishing and maintaining time for the auditorium equipment suite it supervises.*
- *Each Image Media Block (IMB) SM clock shall be set by the SM vendor to within one second of a national time standard (such as WWV). It shall be tamper-proof and thereafter may not be reset*[26]*.*
- *In order to maintain synchronism between auditoriums, Exhibition shall be able to adjust a Security Manager's clock offset a maximum of +/- five minutes within any calendar year. Time adjustments shall be logged events.*
- *Remote SPBs type 1 shall maintain their time-awareness under both powered and un-powered conditions. "Time awareness" shall either be by knowing absolute time according to the suite's IMB SM clock, or via a time duration (relative time) counter. Other requirements:*
  - *SPB clocks shall have a battery life of a minimum of 5 years.*
  - *The SM shall establish and confirm proper operation of time with each remote SPB via a standardized Intra-Theater Message (ITM) communication at least once per day.*
- *The industry is encouraged to standardize upon either an absolute or relative time clock implementation for remote SPBs. In any event, log records and associated time stamps reported for the suite by the SM shall indicate UTC time and the local time zone where events are being recorded.*
- *The IMB Security Manager (SM) clock shall have the following capabilities:*
  - *Resolution to one second*
  - *Stability to be accurate +/- 30 seconds/month*
  - *Date-Time range at least 20 years*
  - *Battery life of at least 5 years*
  - *Battery can be changed without losing track of proper time*

[26] A limited-magnitude adjustable time offset to this clock is described in the subsequent point.

9.4.4. Link Encryption

Link Encryption shall be used at all times (i.e., for encrypted and clear text content) where image content is carried on interconnecting cables, which are exposed (i.e., outside of an SPB) downstream from image media decryption.

Where Link Encryption is used (i.e., Auditorium 2 of Figure 16), the Image Media Block (IMB) SM *shall provide link encryption keys for use with the Link Encryptor (LE) and Link Decryptor (LD) Security Entities (SE) located within the IMB and Link Decryptor Block (LDB) SPBs respectively. Authentication of the LDB by the IMB SM (see Security Manager and LDB requirements of Section 9.4.3.5 Functions of the Security Manager (SM) and Section 9.4.3.6.2 Normative Requirements: Link Decryptor Block (LDB)) shall be performed to ensure that link keys are provided only to legitimate devices which appear on the KDM Trusted Device List (see Section 9.6.2 "Trust" and the Trusted Device List (TDL))*

In the case of playback of clear text content (as indicated by the CPL), no KDM is required, and in such a case no TDL will exist. Recognizing that combinations of clear text and encrypted content must be accommodated, the following rules define normative Link Encryption functionality:

- *In any instance where content is not encrypted and no KDM for this content exists, the SM shall automatically assume "trust" in the LDB and projector SPBs for purposes of keying the LDB and enabling playback for (only) that CPL. All logging processes shall take place normally, recognizing that some logging events (e.g., no logging of content key use) will not be recorded.*
- In instances where combinations of encrypted and non-encrypted content constitute a Show Playlist, the SM shall require the LDB and projector to appear on the TDL prior to enabling keying Link Encryption functions and enabling playback for any CPL having encrypted content.

It is encouraged that the industry standardizes the content encryption processing employed for Link Encryption. *However these specifications only dictate that such protection shall select one of the TDES [FIPS (46-3) and ANSI standard X9.32*] *or AES algorithm applied in a NIST approved fashion. Link Encryption keys shall be 112 bits in length for TDES or 128 bits in length for AES, and such keys shall be generated according to the requirements of Section 9.7.6 Key Generation and Derivation.*

It is mandatory that a fresh Link Encryption key be used for each movie showing, and that such keys be delivered by the Image Media Block (IMB) SM with a single-showing duration period. Multiple Link Encryption keys may be used for showings, and in such cases, it is encouraged that different LE keys be distinguished by (used according to) the CPL (where different Composition Playlists constitute a showing). In the case where multiple LE keys are used, it will be necessary for the industry to standardize on a single technique to identify which LE key is to be used for which portion(s) of any given showing.

9.4.5. Intra-Theater Communications

This Section discusses requirements for communications necessary to support security functions in each auditorium. Depending upon facility communications network designs, there may be both intra-auditorium as well as theater-wide networks and these may be physically one network. The security system requires and addresses only the intra-auditorium network, over which Intra-Theater (security) Messages (ITM) are employed.

Intra-Theater Message(s) (ITMs) are described for communications between the SMS and SM, and between the SM and remote Secure Processing Blocks (SPBs). Note that, depending upon SPB designs, the numbers of SPBs used, and the mix of Security Entities (SEs) within them may vary.

9.4.5.1. Transport Layer Security Sessions, End Points and Intra-Theater Messaging

The Transport Layer Security (TLS) standard has been selected to provide protection for ITMs within the theater. As part of establishing TLS communications sessions, both parties, to the connection, present their digital certificates to achieve mutual authentication. *The authentication shall utilize digital certificates as defined in Section 9.8.1 Digital Certificates, which facilitate a cryptographic process that identifies the SMS and each SPB device to the* SM*.*

The SM and SMS shall both conduct their intra-theater security messaging under TLS protection (IETF RFC 2246). In the case of a fully integrated stand alone projection system (i.e., an auditorium projection system without a distinct SMS device), an SMS proxy shall exist within the projection system, which fulfills the SMS security-related functions.

All TLS end points shall be within the physical protection perimeter of the associated SPB. No SPB requirements are placed on the SMS.

9.4.5.2. Intra-Theater Message Definitions

This section identifies the set of Inter-Theater Message Request Response Pairs (RRPs) to be standardized. These are required to support interoperability and normative operational and security behavior of SPB systems. *The following shall be normative for DCI compliance:*

- *The RRP approach and TLS operations described herein*
- *The* Intra-Theater Messages **(***ITM) of Categories 2 and 3 in Table 15 below, developed in compliance with the message function details of Section 9.4.5.3 Intra-Theater Message Details, or their equivalent.*

9.4.5.2.1. Intra-theater Message Hierarchy

The following hierarchy for Intra-Theater Messaging (ITM) is defined:

- Transactions – Describe the interactions between exhibition components (Security Entities) and the system state changes that occur as a result of the transaction.
- Request/Response Pairs (RRP) – Describes a single interaction between the SEs. At least one RRP is required to implement a transaction.
- Messages – A data structure that passes between SEs. An RRP consists of a request message and a resultant response message.

A transaction consists of sequences of RRPs, and RRPs are pairings of messages. A transaction is an interaction, or series of interactions (RRPs) that change the state in one or more participating SEs in a consistent manner. Transactions need not be standardized. *In assembling transactions, the sequences of RRPs used may vary according to the equipment vendor or facility configuration. Transactions shall be "idempotent" (such a transaction may be repeated without changing its outcome).* Thus, if the initiator of a transaction does not receive evidence of satisfactory completion, it may safely initiate the transaction again without fear of unexpected consequences.

RRP standards do not apply inside of Secure Processing Blocks (SPBs), however RRP concepts are developed assuming that a Security Entity (SE) will exist logically within a SPB, even if not distinctly in hardware. *The SPB is allowed to proxy for any SE (within it) in the support of security messaging.*

9.4.5.2.2. Terms and Abbreviations

The following abbreviations and terms are used in this ITM section:

- Requester = initiator of an RRP
- Responder = answers the RRP
- UDP & TCP = IP protocols for delivering blocks of bytes (UDP) or stream of bytes (TCP)

9.4.5.2.3. General RRP Requirements

1. *Only the SMS or SM shall set up Transport Layer Security (TLS) sessions TLS session establishment between SMS and SM may be initiated by either party. Except where noted, only the SMS or SM shall initiate RRPs.*
2. *Security Managers (SMs) shall not communicate with SPBs other than those in its suite, and SPBs shall not communicate with SMs other than the one assigned to their suite.*
3. *Secure Processing Blocks (SPBs) shall maintain their TLS communications sessions with the SM open and active at all times.*
4. *Absence of a response after an RRP is directed to a SPB over an active TLS session represents a network failure or SPB fault condition. Playback shall continue under network failure conditions to the extent possible.*
5. *Unless otherwise noted, an RRP response is allowed to be busy or an unsupported message type, and such a response shall not be an error event.*
6. *No broadcast RRP commands shall be used or required.*
7. *Except where noted, non-TLS security communications shall not be allowed, and production Digital Cinema security equipment shall have no provisions for* performing security functions *in a TLS "bypass" mode.*
8. *RRP protocols shall be synchronous: Each pairing shall be opened and closed before a new RRP is opened between any two devices. Nested transactions (in which one end point must communicate with another end point while the first waits) are allowed.*
9. *Standardized security messages (both TLS TCP and non-TLS UDP RRP connections) shall use, and have exclusive use of, well-known port 1173 (which has been reserved for SMPTE from the Internet Assigned Numbers Authority [IANA]). (UDP and TCP have different port number address spaces, but IANA assigns both to the same organization when either is requested.)*
10. *Equipment suppliers may implement proprietary ITM, however such ITM shall not communicate over TCP or UDP port 1173 (i.e., any non-standardized ITM shall use a different port).*
11. *Equipment suppliers shall define and describe their respective security designs surrounding the use of port 1173 per the requirements of FIPS 140-2 per Section 9.5.2.5 FIPS 140-2 Requirements for Type 1 Secure Processing Blocks.*

9.4.5.2.4. Request-Response Pairs (RRP)

Table 15 describes the RRPs by outgoing message. The messages in category 1 are considered operational. Categories 2 and 3 are messages that directly impact SM security operation and behavior. To support generalized interoperability for theater security operations, all ITM message categories are encouraged to be developed as a unified group.

- *It shall be mandatory that* ITM *categories 2 and 3 be developed and functionally supported as a set of standardized security messages.*
- *It shall be mandatory that ITM category 1 messages be functionally supported by Security Managers*
- ITMs *of categories 2 and 3 shall be used only between SPBs as specified in Section 9.4.5.3 Intra-Theater Message Details.*
- *Category 1 messages (or their equivalent) shall carry an "AuthorityID" field which is intended to indicate the SMS operator. As indicated in Section 9.4.2.5, policies for the information that the SMS places in this field shall be by business agreement, and are out of scope of these standards.*
- *It is encouraged, but does not mandated that XML be used in the implementation of Intra-theater Messages.*

Message Category	Function
1. SMS to SM	***These define interoperable behavior requirements for SMs***
StartSuite	Commands SM to establish TLS sessions with specific SPBs
CPLValidate	Passes CPL to SM and requests validation check
KDMValidate	Passes KDM to SM and requests validation check
Playok	Query SM if OK to play CPL(id) at (time) on (suite equipment)
PrepSuite	SM to prep SPBs for CPL(id) (load keys, etc.)
PurgeSuite	Purges prep'd suite for CPL(id) (and makes room for new keys)
TimeAdj	Adjusts time at SM (within annual limits)
LogUpload	Request from SMS to IMB SM to report available log data
LogGetNext	Request for specified log block (RRPs are normally chained)
2. IMB SM to SPB	***Intra-suite ITMs***
QuerySPB	Query status of SPB, and serves as TLS heartbeat
KeyLoad	SM key load to remote SPBs (MD/LD/FM/ST)
KeyPurge	Command for SPB to purge keys (makes room for new keys)
LogUpload	Command from SM to SPB to report available log data
LogGetNext	Request for specified log block (RRPs are normally chained)
3. Housekeeping	
Alert	UDP/IP: SPB to SM and TMS for alert or TLS reconnect request.
Abort	Terminates open RRP(id)
TermTLS	Command from SMS or SM for SPB to terminate TLS session

Table 15: Intra-theater Message (ITM) Request-Response Pairs (RRP)

9.4.5.3. Intra-Theater Message Details

This section describes the general functions of each RRP. The tables after each message pair describes the state of the requester and respondent after a successful or unsuccessful RRP. A blank indicates no state change. If the unsuccessful field is error event, it means that there is no reason the command should not have been successful, unless something is wrong with one of the RRP endpoints or the network.

9.4.5.3.1. Screen Management System to Security Manager Messages

These messages are aimed at the SM, and they result in subsequent SM action(s).

9.4.5.3.1.1. StartSuite

This command, StartSuite, tells the SM to initialize its suite. The SM will initiate Transport Layer Security (TLS) sessions with remote Secure Processing Blocks

(SPBs) thereby authenticating them, and issue QuerySPB to SPBs specified in the request.

RRP	Requester	Respondent
Successful	SMS confirms suite is operational	SM records “start” event data
Unsuccessful	SMS is aware of suite problems	SM records “start” failure data

Table 16: RRP State: StartSuite

Notes:

- This RRP identifies to the SM the SMS and remote SPBs that are in the suite.
- This command should be designed to start or restart the suite (takes time), or “query suite status” (without restarting, and takes no time).

9.4.5.3.1.2. CPLValidate

This command, CPLvalidation, will request validation that the CPL signature matches the contents of CPL and the CPL signer cert meets authentication criteria. The CPL list is passed in the message.

RRP	Requester	Respondent
Successful	Confirms SM’s validation of the CPL	Now knows/has CPL
Unsuccessful	Indicates a problem with the CPL	

Table 17: RRP State: CPLValidate

Notes:

- Packing List validation check is assumed to be performed by the Theater Management System (TMS) or Screen Management System (SMS).
- A successful ValidateCPL operation results in the SM retaining the CPL, and subsequent messages may refer to the CPL by the Composition ID [CPL(id)].

9.4.5.3.1.3. KDMValidate

This command, KDMValidate, asks the SM to validate a specific KDM. The KDM is passed to the SM in this RRP. If validated, the SM retains the contents of the KDM.

RRP	Requester	Respondent
Successful	Confirms SM validation of the KDM	SM now has KDM(id)
Unsuccessful	Informs SM has rejected KDM (why)	

Table 18: RRP State: Key Delivery Message KDMValidate

Notes:

- Normal method used to deliver a KDM to the SM if not received directly by an ETM.

9.4.5.3.1.4. PlayOK

This command, PlayOK, asks the SM whether playback of CPL(id) is OK at (time) on (suite equipment list). The suite and time window fields are optional, so this RRP can be used before the suite or showtimes are established (SMs will enforce these tests before allowing playback).

RRP	Requester	Respondent
Successful	SMS is aware of playability pass/fail for the specified playback conditions	
Unsuccessful	SMS is aware of playback prohibitions	

Table 19: RRP State: PlayOK

Notes:

- KDM and CPL validations should precede this RRP.
- A negative response from an SM shall indicate the reason.
- The SMS must perform a series of the above if the Show Playlist uses multiple CPLs.
- This RRP does not indicate preparation status of the suite as it is a permissions query.

9.4.5.3.1.5. PrepSuite

This command, PreSuite, instructs the SM to prepare the suite for playback of the CPL(id). PrepSuite results in a series of SM transactions that check KDM conditions for playback, confirms SMS and Secure Processing Blocks (SPBs) against TDL, confirms Transport Layer Security (TLS) and queries SPBs for status, loads all required MD, FM and LE/LD key caches, and alerts of any problems.

PrepSuite is the only category 1 RRP that requires the SMS to appear on a TDL. The SMS identity shall appear on the TDL associated with the CPL being prepared for playback (see Section 9.4.3.5 Functions of the Security Manager (SM) (9)a).

Once this command has been successfully executed, the suite is ready for playback and will do so upon the order of the SMS.

RRP	Requester	Respondent
Successful	SMS knows that the CPL will play when instructed	SM enters “suite is prepped” state and logs all relevant prep events
Unsuccessful	SMS is aware of issues prohibiting playback	SM records the prep failure and associated security issues

Table 20: RRP State: PrepSuite

Notes:

- In the case of multiple CPLs per show, or different shows per auditorium, this setup must be done for all CPLs and each Show Playlist.
- Security Manager behavior requires “PrepSuite” prior to each movie playback.

9.4.5.3.1.6. PurgeSuite

This command, PurgeSuite, instructs the SM to clear/purge all previous preparations made for the suite to play CPL(id). Purge results in an SM scenario that clears all key caches, and collects all log data for the particular Composition Play List (CPL).

RRP	Requester	Respondent
Successful	SMS knows suite has been cleared for CPL(id) playability	SM records purge event and collects all suite log data for CPL(id)
Unsuccessful	Error event	

Table 21: RRP State: PurgeSuite

Notes:

- This command should be used whenever the SMS wishes to terminate an engagement, or to clear key caches to make room for more keys.
- This command should not cause the SM to purge a KDM (SM behavior shall cause it to purge expired KDMs).

9.4.5.3.1.7. TimeAdj

This command, TimeAdj, adjusts the Security Managers (SMs) clock offset (within limits as specified).

RRP	Requester	Respondent
Successful	SMS is able to keep suites in sync	SM adjusts clock and logs event
Unsuccessful	Adjustment refused by SM	SM logs reason for refusal

Table 22: RRP State: TimeAdj

9.4.5.3.1.8. LogUpload

This command, LogUpload, requests information about the next available log data in a sequence. This RRP is used as a precursor to the transfer of log information. The response indicates available log records, including their time stamp(s), and the LogGetNext RRP manages the actual data transfers.

RRP	Requester	Respondent
Successful	SMS knows available log data	SM sends record information to SMS
Unsuccessful	Error event	

Table 23: RRP State: LogUpload

Notes:

- Log data requests should be by class per the log specifications.
- This RRP set should support the LogGetNext note below regarding requesting log event data by time.

9.4.5.3.1.9. LogGetNext

This command, LogGetNext, this request identifies which log data (by class) is desired, and the response delivers a block of log data. This RRP is normally part of a chained set of RRPs.

RRP	Requester	Respondent
Successful	SMS receives requested block of data	SM sends requested block of data; counters, hashes, etc. are incremented
Unsuccessful	Error event	

Table 24: RRP State: LogGetNext

Notes:

- It is desirable that this RRP set be designed such that the request may include a time or time window for the return of log data events within (around) such window
- Chained RRPs may be interrupted by other RRPs. The requestor should remember states so data transfers may resume. The LogUpload RRP may be sent again if states are lost.

9.4.5.3.2. Image Media Block SM to Remote SPB Messages

RRP message(s) that contain the SM's current time (to which the SPBs shall be slaved) shall be specified.

It is recommended that the Security Alert field of the QuerySPB response be replicated in each of the below SM RRP responses. It should indicate functional health and tampering status of the SPB.

9.4.5.3.2.1. QuerySPB

This command, QuerySPB, instructs the SM to query and collect status information about the Secure Processing Block (SPB). The primary use of this RRP is for security monitoring of the remote Secure SPB. This RRP doubles as a heartbeat RRP, and shall be sent to each SPB at least every five (5) seconds whenever TLS sessions are open, including during a showing, unless other SM-driven RRPs are in process.

Other suggested response items:

- "RRP(id) to me is open" (not this RRP)
- "I am currently doing (task, playback status, or not busy)"

RRP	Requester	Respondent
Successful	SM collects status data	
Unsuccessful	Error Event	

Table 25: RRP State: QuerySPB

Notes:

- *It shall not be legal for an SPB to Abort a QuerySPB issued by the SM.*
- The SMS may issue a QuerySPB if direct SPB communications exist.
- Failed QuerySPB RRP indicates either a SPB or network failure.
- To avoid SE overhead, the "request" does not carry data/information.
- The currently doing "task/not busy" flag can be used by the requester as an indication of SE availability to respond to future desired transactions.

9.4.5.3.2.2. KeyLoad

This command, KeyLoad, is used by the SM to deliver keys and associated parameters (keyIDs) to Media Decryptors, Forensic Markers or Link Decryptors

located in remote Secure Processing Blocks (SPBs). This RRP will be issued in response to the Screen Management System (SMS) ordering a PrepSuite, but only after the SM is satisfied with SPB queries and prerequisites of a validated KDM & CPL.

RRP	Requester	Respondent
Successful	Suite is prepared for playback of a specified CPL	SE is prepared to utilize keys on demand until the validation time expires
Unsuccessful	Error event	

Table 26: RRP State: KeyLoad

Notes:

- The key validation period is delivered by the SM in the request.
- KeyLoads are used for image, audio, LE, FM or subtitle keys, as applicable.
- The KeyLoad RRP communicates the “no FM mark” state to remote FM SEs.

9.4.5.3.2.3. KeyPurge

This command, KeyPurge instructs the SEs holding keys and key information associated for a given CPL to purge themselves of those keys. The response confirms the purge, and both the SM and SE log the event.

RRP	Requester	Respondent
Successful	SM is aware of purge	SE is rendered unable to play CPL(id)
Unsuccessful	Error event	

Table 27: RRP State: KeyPurge

Notes:

- This RRP may be ordered by the SMS at any time (via PurgeSuite), or by the SM in the event it is responding to an attack.
- This RRP can eliminate keys by CPL to avoid cache overloads prior to play.

9.4.5.3.2.4. LogUpload

This command, LogUpload, generates an RRP from the Security Manager (SM) to Secure Processing Block (SPB) requesting information about the next available log data in a sequence. This RRP is used by the SM as a precursor to the transfer of log information. The response indicates available log records, and the LogGetNext RRP manages the actual data transfers.

RRP	Requester	Respondent
Successful	SM knows available log data	SE sends record information to SM
Unsuccessful	Error event	

Table 28. RRP State: LogUpload

Notes:

- The SM may request log data by class per the Log Requirements Specifications.

9.4.5.3.2.5. LogGetNext

This command, LogGetNext, generates an RRP request that identifies which log data the Security Manager wishes to receive, and the response delivers a block of log data. This RRP may be part of a chained set of RRPs.

RRP	Requester	Respondent
Successful	SMS receives requested block of data	SE sends requested block of data; counters, hashes, etc. are incremented
Unsuccessful	Error event	

Table 29: RRP State: LogGetNext

Notes:

- The SM should remember chain sequence states between log uploads. The LogUpload RRP may be sent again if states are lost.

9.4.5.3.3. Intra-Theater Network Housekeeping Messages

9.4.5.3.3.1. TermTLS

This command, TermTLS, generates an RRP from SM to Secure Processing Block (SPB) commanding termination of the Transport Layer Security (TLS) session. The RRP is executed under TLS, after which the SPB zeros all TLS session parameters.

RRP	Requester	Respondent
Successful	TLS session terminated	TLS session terminated; resources freed
Unsuccessful	Error event	

Table 30: RRP State: TermTLS

Notes:

- Transport Layer Security (TLS) layer termination process closes the underlying TCP/IP connection.

9.4.5.3.3.2. Alert

This command, Alert, is a Non-TLS UDP/IP RRP from an Secure Processing Block (SPB) to an SM, or from Security Manager to Screen Management System, issued in the event of a security alarm under circumstances when (for whatever reason) a Transport Layer Security (TLS) session and normal RRP responses are not available to deliver the alarm.

The need for this command may arise from the failure of a device, power, or network. Recognizing that UDP/IP does not guarantee reliable delivery, the requester should send the command at least three times. If there is no response, a network problem should be assumed. The responder should respond identically to each request it receives.

RRP	Requester	Respondent
Successful	SE receives response and knows SM received request	SM is aware of alert, (but unaware if response received)
Unsuccessful	SE is unaware whether SM is aware of error condition	SM may or may not be aware of request
Unsuccessful after repeats	Follow error procedures	SM may or may not be aware of request

Table 31: RRP State: Alert

Notes:

- If the need for this RRP is caused by a network problem, lower level TCP communications may have knowledge about the error conditions. These need to be woven into the ITM problem discovery/recovery process.
- Conditions/protections for the issuance of this command must include:
  - Protection of the network from being jammed if the problem is with the SPB.
  - SPBs TLS recovery expectations, and behavior if recovery doesn't happen.
  - Behavior of SPBs prior to being communicated to (e.g., power-up).
- This RRP can be used by the SMS to direct an SM to initiate a TLS (re)connect, though this may be done also at the TCP layer.

9.4.5.3.3.3. Abort

This command, Abort, terminates an open RRP that is: 1) instigated by the original recipient's lack of response, or 2) forced by the original recipient.

The Abort command interrupts an open RRP by interjecting the abort before the original recipient responds. The recipient of any RRP can issue this command response in place of the originally requested response. No parameters are sent in either the request or response.

RRP	Requester	Respondent
Successful	SM (or SMS) no longer is waiting for RRP(id) response	SE (or SM) aborts its RRP(id) response ambitions
Unsuccessful	Error event	

Table 32: RRP State: Abort

Notes:

- It shall not be permitted for an SE to abort a QuerySPB RRP.
- The responder must respond to the Abort request, even if the original RRP(id) response happens to have been sent (race condition is OK).

9.4.6. Forensics

Forensics do not prevent content theft or other compromises, but rather, it provide methods for their detection and investigation. Forensic features deter attackers who are aware that their actions would be logged and/or reported in considerable detail.

Forensic features fall into two classes: Forensic Marking (FM) and logging. Forensic Marking embeds tracking information into content itself, to be carried into subsequent legitimate or stolen copies. Logging creates records of both normal and abnormal events in the Distribution and Exhibition process. *During a content theft investigation, both FM and logging information may be combined to establish the details of the security compromise.*

Industry terminology for watermarking and Forensic Marking is not consistent. For these security specification purposes, stakeholders have agreed to use the term Forensic Marking for all content marks.

9.4.6.1. Forensic Marking

These specifications require that Forensic Marking (FM) capability be included in each Image and Audio Media Block. The security system identifies content marking devices (e.g., Forensic Marking embedders) as the "FM" Security Entity (SE) type. *To support FM processes, standardized Intra-Theater Messaging (ITM) may be used where needed for communications between such* SEs *and Security Managers (SMs).* Such communications and associated FM behavior is outside of this specification. However the requirements of ITM Section 9.4.5 Intra-Theater Communications shall be mandatory where such theater messaging employs the intra-auditorium security network. Forensic Marking does not require interoperability between detection systems, as the detection operation is usually performed "off line" as part of a security investigation.

Multiple solutions may be qualified and will allow Media Block solutions providers to select the solution of their choice. Candidate providers should meet with individual studios to discuss RAND and technical suitability of their approach.

Note: DCI reserves the right, at some future time, to require a specific Forensic Marking insertion solution for Digital Cinema systems.

At a minimum, Forensic Marking systems are required to meet the following:

9.4.6.1.1. General Requirements

- *The Forensic Marking data payload is required to be a minimum of 35 bits and must contain the following information:*
    - *Time stamp every 15 minutes (four per hour), 24 hours per day, 366 days/year the stamp will repeat annually. There are 35,136 time stamps needed, therefore allocate a 16 bit unsigned number (65,536).*
    - *Location (serial number) information, allocated 19 bits (524,000 possible locations/serial numbers)*
- *All 35-bits are required to be included in each five minute segment.*
- *Forensic Marking insertion is required to be a real-time (i.e., show playback time), in-line process performed in the associated media block, and is required to have a reasonable computational process.*
- *Recovery can up to a 30-minute content sample for positive identification.*
- *Support of a single distribution inventory is required.*
- *Terms and conditions of use are required to be reasonable and non-discriminatory (RAND).*
- *Detection can be performed by the vendor or the Rights Owner at the Rights Owner's premises.*
- DCI will entertain development of a generic Forensic Mark inserter architecture. *Any FM technology utilizing pre-processing is required to use a generic inserter architecture that meets the criteria outlined below.* Additionally, a full understanding of the intellectual property terms and conditions will need to be reached.
    - *Standardized Metadata Format – Any pre-processing solution is required to be able to utilize a single, industry standardized metadata transport format and a generic inserter solution.*

- *Title (Composition) Single Inventory – For each composition, the system is required to support the use of a single image or audio FM technology that generates one set of metadata. This metadata is required to be compatible with all deployed compliant generic inserters. At the distributor's discretion, multiple sets of metadata can be used to mark the same composition.*
- *Generic Inserter Compatibility – For the initial generic inserter deployment, the generic inserter in final product form is required to be openly demonstrated and independently tested to demonstrate compatibility with a minimum of three independent metadata-based forensic marking solutions.*
- *Forensic Mark and Generic Inserter Backwards Compatibility – After initial deployment, any subsequent metadata-based FM solutions or generic inserters are required to function correctly with all deployed compliant systems.*
- *Forensic Mark Pre-Processing Speed – The Forensic Mark processing steps needed to generate and insert metadata are required to be real time or faster and are required to occur in a single pass.*

- *As a matter of implementation, recognizing business and post-production constraints, it is encouraged that a generic inserter implementation minimizes the metadata payload needed to provide forensic mark data to the generic inserter.* A reasonable target would be less than two percent of the compressed image and sound data payload.

9.4.6.1.2. Image/Picture Survivability Requirements

- *Image Forensic Marking is required to be visually transparent to the critical viewer in butterfly tests for motion image content.*
- *Is required to survive video processing attacks, such as digital-to-analog-digital conversions (including multiple D-A/A-D conversions), re-sampling and re-quantization (including dithering and recompression) and common signal enhancements to image contrast and color.*
- *Is required to survive attacks, including resizing, letterboxing, aperture control, low-pass filtering and anti-aliasing, brick wall filtering, digital video noise reduction filtering, frame-swapping, compression, scaling, cropping, overwriting, the addition of noise and other transformations.*
- *Is required to survive collusion, the combining of multiple videos in the attempt to make a different fingerprint or to remove it.*
- *Is required to survive format conversion, the changing of frequencies and spatial resolution among, for example, NTSC, PAL and SECAM, into another and vice versa.*
- *Is required to survive horizontal and vertical shifting.*
- *Is required to survive arbitrary scaling (aspect ratio is not necessarily constant).*
- *Is required to survive camcorder capture and low bit rate compression (e.g. 500 Kbps H264, 1.1 Mbps MPEG-1).*

9.4.6.1.3. Audio Survivability Requirements

- *Audio Forensic Mark is required be inaudible in critical listening A/B tests.*
- *The embedded signal is required to survive multiple Digital/Analog and Analog/Digital conversions.*
- *Is required to survive radio frequency or infrared transmissions within the theater.*
- *Is required to survive any combination of captured channels.*
- *Is required to survive resampling and down conversion of channels.*
- *Is required to survive time compression/expansion with pitch shift and pitch preserved.*
- *Is required to survive linear speed changes within 10% and pitch-invariant time scaling within 4%.*
- *Is required to survive data reduction coding.*
- *Is required to survive nonlinear amplitude compression.*
- *Is required to survive additive or multiplicative noise.*
- *Is required to survive frequency response distortion such as equalization.*
- *Is required to survive addition of echo.*
- *Is required to survive band-pass filtering.*
- *Is required to survive flutter and wow.*
- *Is required to survive overdubbing.*

9.4.6.2. Forensic Marking Operations

There may be differing circumstances surrounding the desire by a Rights Owner to forensically mark content. To accommodate these variations, it is necessary to be able to independently control the activation of both the audio and the image Forensic Marking (FM). *The following rules shall be normative for Forensic Marking operations:*

1. *The SM shall be solely responsible for control of FM marking processes (i.e., "on/off") for the auditorium it is installed in, and, subject to (2), command and control of this function shall be only via the KDM indicator per (3).*
2. *Forensic Marking shall not be applied to non-encrypted audio or image content. If portions of a composition are encrypted and other portions are not, FM shall not be applied to those Track Files that are not encrypted.*
3. *Forensic Marking shall otherwise be applied to all encrypted content, except as follows.*
    a. The KDM contains fields for carriage of FM keys and key IDs. *A single default FM key value indicating a "no FM mark" state shall be defined and standardized. Lacking an industry standard, an "all one's key" shall indicate the "no FM mark" state for the associated composition.*
    b. *Upon receipt of the "no FM mark" default key in the KDM, the Security Manager (SM) shall indicate to the targeted image or sound FM Security Entity (SE) (see (3)) that a "no FM mark state" has been commanded.*
    c. *Upon receipt of the SM's "no FM mark" command, the FM device shall enter a full bypass mode, and not impose any mark onto the image essence for the associated CPL/composition.*

2. *"No FM mark" states shall be capable of being independently commanded for audio or image compositions via appropriate use of the KDM FM key for audio or image Track Files*[27]*.*
3. *Audio and image Forensic Marking SEs shall recognize the "no FM mark" state commanded by the SM, whether or not their specific technologies are normally keyed via the KDM.*
4. *When used, the FM default key, and thus the "no FM mark" state, shall apply to the entire CPL/composition, according to the associated KDM. The "no FM mark" state shall not apply to any other composition, even if the other composition is part of the same showing (i.e., same Show Playlist).*
5. *In the event that valid overlapping KDMs exist for a particular CPL (i.e., KDMs that have overlapping time windows), and such KDMs conflict with respect to their contained "no FM mark" states, the SM shall maintain Forensic Marking in the "mark" state for the portion of time that the time windows overlap. Outside of the time overlap the SM shall follow the respective KDM FM key indicator.*
6. *SM control of the Forensic Marking "no FM mark" state in remote SPBs shall be via the "KeyLoad' Intra-Theater Message (ITM) (see Section 9.4.5.3.2.2 KeyLoad).*
7. *The SM and FM Security Entities shall log the occurrence of all "no FM mark" states and associated KDMs/keys.*

9.4.6.3. Logging Subsystem

In the Exhibition environment, the preparations for and execution of a movie showing creates information that has security and forensic implications. The capturing and storage of such information is the responsibility of the logging subsystem. In order to realize a "control lightly/audit tightly" end-to-end security environment, the security system includes a secure logging subsystem.

Cryptographic technology as applied to essence and key delivery, together with agreed upon usage rules provides the "control lightly" characteristics. The function of a logging subsystem is to respond to the "audit tightly" requirement. Logging is therefore observed as a critical component of security, and secure logging information and surrounding processes are subject to the same fundamental cryptographic requirements as the front end control components: cryptographic protection of critical functions and data components related to integrity, data loss, confidentiality and movement.

This section sets requirements for generating log files appropriate for reliable reporting of security event data. *These specifications require that standardized mechanisms shall be available to extract log information from a single point (the Image Media Block* Security Manager*) in each auditorium.*

Definitions related to logging:

- Log Event – Any event that has security implications or forensic value. Such an event results in the recording of log data.
- Log Data – Security event information that is recorded and stored within the Security Entity (SE), where such an event took place or was observed.
- Log Record – Standardized XML structure representing a discrete logged event.
- Log Report – Standardized XML structure containing one or more log records spanning a continuous sequence in time. *The log record content in a report is*

[27] While the KDM contains key identification fields indicating whether keys are for image, audio, FM, etc., there is no distinction between image or audio FM keys. In order to meet the above requirements, a method for such distinction may need to be defined by the industry.

intended to be organized by class, and may be filtered prior to delivery according to specified criteria (Rights Owner, CPL, etc.).

- Log Message – Standardized Intra-Theater Message (ITM) for moving log reports from an SE to the SM, or from an SM to the SMS.

Following the above definitions, a basic logging process is described:

- Surrounding a showing will be a number of security events that result in logged data. *Discrete logged event data shall be placed in an XML structure called a record.*
- A number of records are collected in sequence and by class to make up log reports.
- A complete (unfiltered) report is useful for transferring entire sets of log data for archiving or post-processing outside of the security system.
- A "filtered" report is useful for responding to a request for log data according to specified bounds (e.g., report the SE key usage records for CPL(id) for specific date(s) and time(s)).
- *Reports may be delivered via the theater network using log messages (*Intra-theater Messages*), or simply transferred to a physical device (e.g., USB removable flash memory).*

9.4.6.3.1. Logging Requirements

1. *Logging subsystem implementations shall not affect the ability of Exhibition to operate their projection systems in a standalone fashion.*
2. *Security Entities (SE) shall have normative requirements for the specific log data to be recorded for each record (see Section 9.4.6.3.7 Log Record Classes and Section 9.4.6.3.8 Log Record Information).*
3. *Log records and reports shall be protected from undetected alteration (integrity and authentication) or deletion (continuity).*
4. *Log records and reports shall be non-repudable and traceable back to the source SE device (i.e., where the logged event took place).*
5. *Log records and reports shall carry proof of authenticity, which does not rely on the trustworthiness of the systems and channels they pass through. Systems or devices which communicate, handle or store log messages (or records) need not be trusted or secure.*
6. *The content of log records shall be protected from exposure to parties other than the intended recipient (see Section 9.4.6.3.6 Secondary Log Distribution and Log Filtering).*
7. *Each Rights Owner shall be able to cryptographically confirm the integrity and continuity of log records and their log data independently of other Rights Owners (see Section 9.4.6.3.6 Secondary Log Distribution and Log Filtering).*
8. *Image Media Block SMs shall collect log information from all remote Secure Processing Blocks in the suite it enables at the earliest equipment idle time between scheduled showings. To assure timely collection, TLS sessions shall not be terminated prior to collection of all remote SPB log data, and in no event shall more than 24 hours pass between the recording of log data by a remote SPB and the collection of such data by the IMB Security Manager.*
9. *The Image Media Block SM shall be capable of storing at least 12 months of typical log data accumulation for the auditorium in which it is installed.*

10. *Remote Secure Processing Blocks (SPBs) shall have sufficient secure storage to hold log data to accommodate at least two days worth of typical operation.*
11. *Log records stored in SPBs shall be stored in non-volatile memory and are not be purge-able. Data shall be over-written beginning with the oldest data as new log data is accumulated.*
12. *An SE shall author its own log records, or utilize the services of a proxy within the same secure SPB.*
13. *SEs or their SPB proxy shall have an asymmetric identity key pair and Digital Cinema certificate for signing log records.*
14. *SEs or their proxy shall time stamp log records, with date/time synchronized with the auditorium SM's secure clock.*
15. *SEs or their proxy shall sequence log records with a secure and persistent counter.*
16. *An Image Media Block Security Manager (SM) shall associate (identify) all suite log records with the SMS under which it operates.*
17. *Any use of a proxy in the above, shall produce log records compliant to these requirements.*

9.4.6.3.2. Log Record and Report Format

The following describes the XML structure for log records. A log report contains at least one sequence of log records. *In the case of reports covering multiple* SEs*, records shall consist of a separate sequence for each SE. Each record shall contain the following three XML nodes: Header, Content, and Signature.* This structure was developed specifically to allow efficient authentication, while supporting the removal (filtering, explained below) of confidential information.

- **Header** – *The Header node shall contain control information, notably record type (class), sequence number, time stamp, origin, and integrity control data. The Header node is essential to authentication and shall be present in every log record.*
- **Content** – *The Content node shall contain the detailed log information (payload), dependent on the log record type. Content node information should not be encrypted, as it is necessary for Exhibition to have visibility over log data. Confidential information should be placed in the Content node, since deletion of the Content node is permissible.*
- **Signature** – *The Signature node shall directly authenticate only the Header node.* The Signature node is optional for any given record, but required periodically in order to create authentication checkpoints in the sequence of log records. Requirements for how often Signature nodes must be created are unspecified. Authentication of unsigned nodes is provided indirectly by hashing.

9.4.6.3.3. Log Integrity Controls

Protection from unauthorized log data alteration or deletion is a mandatory requirement of stored or delivered log data. Conventional methods of integrity control would require computationally intensive private key operations on the part of a log record originator. Since many SEs are envisioned as lightweight devices, such processing could impact performance or increase the cost of the device. Alternatively, a hash-chain method (Figure 21) is recommended to provide integrity control at significantly reduced overhead and storage.

The log record structure shall contain the following information to ensure integrity of each record and the continuity of the overall log.

- **Content Node Hash** – *The Header node shall contain a hash of the Content node. This hash may be used to authenticate the Content node.*
- **Log Sequence Number** – *The Header nodes shall contain a serial number.* Each SE must sequence its logs to facilitate detection of deleted log records.
- **Prior Record Hash** – *The Header node shall contain a hash of the Header node from the previous log record from the same SE.* This data permits chain signing such that once a log record is authenticated, all prior log records can be authenticated simply by verifying that the Prior Record Hash in each header matches a computed hash of the Header from the prior record.
- **Digital Signature** – *The Digital Signature shall be computed using the private key of the originating SE and verified using the public key in the SE's certificate.* Using the recommended hash chaining method, a signature is optional for a given log record. However, *the SE shall sign the last record in a sequence of log records uploaded to the* SM *(or from* Security Manager *to Screen Management System).* Unsigned log records are validated using the chain of hash values in the Header node.

Figure 21 illustrates this method of ensuring log integrity.

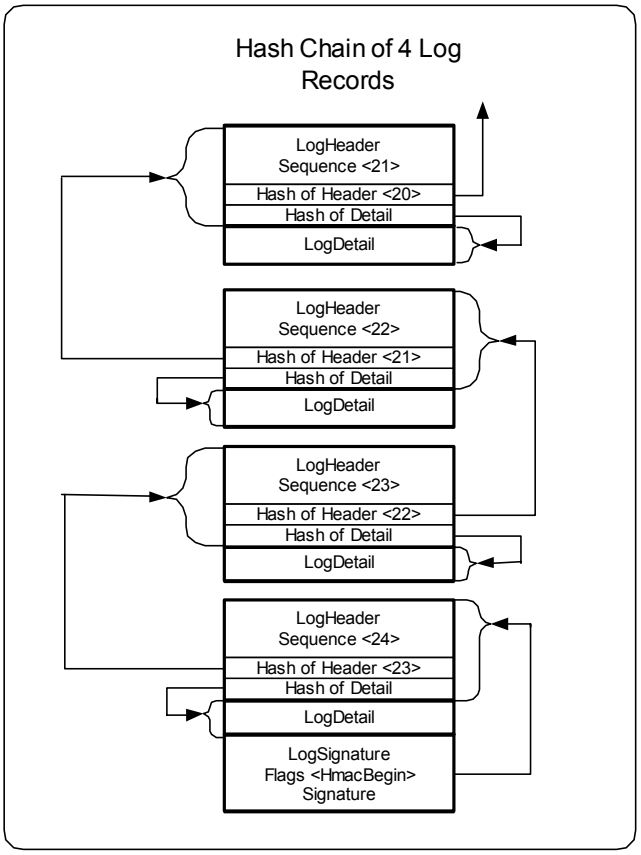

Figure 21: Log Record Chaining Example

The above hash chaining method is not required, however in the absence of this approach, signatures shall be used on log records and reports.

9.4.6.3.4. Security of Log Record Sequencing

It is mandatory to enable validation of logging stream continuity. *To ensure continuity, the log message originating SE shall maintain a secure and persistent counter to provide a unique sequential number to each log record it creates.* Log records are to be stored by class (see Section 9.4.6.3.7 Log Record Classes). It is presumed that SEs will sequence by class. This sequencing technique permits the storage and distribution of the log records on or over non-secure media, without danger of undetected deletions.

The sequence number shall appear in the log record Header node. While Content nodes may be deleted from the log (see filtering), all headers shall be present in the log record stream to preserve the ability to authenticate the stream.

9.4.6.3.5. Log Upload Protocol over Theater Networks

For non-integrated (multi-Secure Processing Blocks) suite equipment architectures, log records shall be formatted as log reports and transferred from their originating SE to the Image Media Block (IMB) SM, by use of standardized ITM log messages. *The dialog shall take place over the bidirectional Transport Layer Security (TLS) session on the intra-suite network within the auditorium.* For fully integrated suite equipment architectures (i.e., where no Link Encryption is used and all Security Entities are within the Image Media Block), the IMB SM will inherently have all of the auditorium's log data. *Subsequent log report message transfers may take place from the IMB* SM *to the SMS, or via physical connection to the IMB.*

Log message transfers begin with a request by the recipient specifying the next log record sequence numbers expected. The response is a log report containing the requested log records, or an end-of-log indication. Depending on whether the messages are going from Security Entity to SM, or SM to Screen Management System (SMS), the recipient will be either the Security Manager (SM) or the Screen Management System (SMS). The protocol is the same.

9.4.6.3.5.1. Option for Log Uploads to the Image Media Block SM

Recognizing that TLS protection exists between the IMB SM and remote SPBs and SM authentication is in place, the following option may reduce processing and/or storage requirements in remote SPBs.

It shall be allowed for the log record protocol of the transfer of log data from a remote SPB to the IMB SM to avoid the overhead of signing. In such case all normal log record nodes, hashes and sequencing shall be maintained as specified above. The SM shall sign log records or reports for uploads from the SM, and provide the identity of the remote SPB for which it is signing.

9.4.6.3.6. Secondary Log Distribution and Log Filtering

This section describes log filtering. The locations where log data filtering takes place (e.g., in an the Image Media Block (IMB) vs. external theater-controlled/supplied process) is an implementation decision. This is not a security issue, as the processes described above ensure the integrity of log records. The description below assumes log data filtering, the removal of Content nodes from records, takes place at the SMS.

The descriptions above relate to how log records are collected by the Image Media Block (IMB) SM within the auditorium suite, or by the SMS from the auditorium SM. Subsequent log data movement (e.g., SMS to the Theater Management System (TMS) or to a Distributor) is referred to herein as secondary log distribution. Log records will be a mixture of data types, some of which will be Rights Owner-specific

(e.g., CPL key id was used), and some of which will not be (e.g., SPB(id) TLS session established (time/date)). For secondary distribution, it will be necessary to filter log content such that reports can be generated, which supply log record content selectively to the appropriate recipients.

To facilitate filtering, the SMS may delete Content Nodes from records before forwarding them to a secondary recipient. The structure of the log record allows a secondary recipient to authenticate the record, even though Content nodes are missing (the hash of the Content node remains in the Header, the Digital Signature covers only the Header node). *Since all log record Header nodes remain present, the secondary recipient can determine whether all log content is accounted for even though they may have only portions of it.*

To facilitate accurate filtering and secondary distribution of log data to the appropriate recipient(s), it is recommended that a CompositionID (e.g., UUID) be placed in the Content node. This allows the SMS to easily identify log records associated with specific content or Rights Owners, which will be eliminated by the filtering function except for those Rights Owners who are selected as recipients.

To facilitate rapid access to log data specific to a particular Rights Owner, title, date, etc, it is recommended that a CompositionID plus log event Time/Date field be placed in the header, such that secondary recipients can easily search through raw records for specific information. *Since all Rights Owners have access to all Header information, to avoid broadcasting content-showing information (i.e., what movies played how many times), this field should be encrypted with a key that the Rights Owner will have (e.g., the hash of a content key). The Time/Date portion may be selected in advance to be fine or coarse-grained, depending upon the Rights Owner's fast search desires that are enabled by this feature.*

To facilitate log record requests related to the time of logged events, it is recommended that the "LogUpload" and "LogGetNext" Intra-Theater Messages (the messages that manage and transfer log data, see Section 9.4.5.3.2.4 LogUpload) accommodate a time window capability indicating the desired time segment for which a particular class of log data is desired. This will provide a convenient method for stakeholders to request log information surrounding a particular time window.

9.4.6.3.7. Log Record Classes

Log records shall be categorized by class. These classes shall denote the specific types of event data to be recorded. Additional information shall be associated with and stored for each record (e.g., SMS, SM or SE(s) involved, time stamps, certificate thumbprints, CPL(id), etc), sufficient to explicitly and unambiguously complete the record (see Section 9.4.6.3.8 Log Record Information). The following tables describe logged event by class:

1. *The use of the descriptor SE includes SPB, as appropriate.*
2. *Certain facility operational procedures are logged events. The failure or refusal of many such functions to execute is also a logged event.*
3. *The Request-Response Pair (RRP) nature of security messages results in many companion records (i.e., where both the request and response are logged by the respective SEs). This will assist in forensic investigations on suspect equipment.*
4. *Log classes have been selected to be useful for troubleshooting both security operations and infrastructure, and content security issues.*
5. *Re-organizing these classes by SPB type rather than as shown may be beneficial towards SPB storage or processing requirements, or record or*

report generation. This is considered an implementation detail, but the industry is encouraged to standardize on a single approach.

Operational – The table below illustrates normal Security Entity operational events.

Event	Description
PowerDown	SPB shutdown (may not exist for a system crash)
PowerUp	SPB startup
StartSuite	SM records command to establish TLS with specified SPBs
TLSInitiated	SM and SE record TLS session initiation event and parameters
TLSTerminated	SM and SE record TLS session termination event and parameters
TLSRefused	SM rejects TLS session establishment (reason)
TimeAdjust	SM or SPB has its internal time clock adjusted
Alert	SM or SPB record issuance of UDP alert command and reason
MaintBegin	SPB had maintenance (type) performed (as applicable).
MaintEnd	SPB maintenance (type) is complete.
FailureDetect	SPB has detected a failure (type: internal or TLS/network)
SMCertLoad	SM certificate (type) load event
CodeEvent	Records of modification of SM or SPB code

Table 33: Log Record Class: Operational

Log Messages/Management – The table below illustrates messages that implement the actual delivery of log data to designated recipients, and information that is recorded *about* the recording, transmission, collection or reception of log records.

Event	Description
LogRequest	SMS or SM generated LogRequest (sequence) message
LogUpload	SPB or SM generated LogUpload (sequence) message
LogUploadRecord	Information about the generation of a LogUpload sequence record
LogAcknowledge	SPB or SM received a LogAcknowledge record

Table 34: Log Record Class: Log Messages/Management

Playback Management – The table below illustrates events regarding suite playback management, and information describing the delivery and receipt of Content and Link Encryption keys, and their usage to decrypt content.

Event	Description
PrepSuite	SM records command to prep for playback of CPL(id)
PurgeSuite	SM records command to purge playback prep of CPL(id)
PlayOK	Query/response for playability acknowledgment
KeyUsage	SPB used a content or LE key to decrypt content
KeyExpire	SPB acknowledges key timeout purge
KeyPurge	SM commands SE to purge a key
NoFMMark	SM & FM records receipt and execution of “no FM mark” state

Table 35: Log Record Class: Playback Management

Validations & Exceptions – The table below illustrates events regarding operational or playback exceptions, and information about various SM validation checks, as may be requested or required behavior.

Event	Description
ContentCheck	Results of SM pre-show content hash integrity check
CPLCheck	Results of SM pre-show CPL validation check
PLCheck	Results of SM Packing List validation check
KDMCheck	Results of SM KDM receipt and validation check
QuerySPB	Record of failed SPB status query (includes TLS anomalies)
LogFail	Event that may result in (or indicate) unreported SE or SM log data
IntegCheck	Records of run-time image and audio essence integrity checks

Table 36: Log Record Class: Validations/Exceptions

9.4.6.3.8. Log Record Information

The logging subsystem shall record the events as shown in the above Table 34, Table 35, and Table 36 classes. The following are given to show examples of the additional parametric information necessary to fully complete log records (time is a UTC time stamp):

- Time of playback and CPL identifier of each showing of each composition.
- Identity of each SE, SM, SMS involved in a playback. Logged SMS information shall include the ITM “AuthorityID” field per Section 9.4.5.2.4 Request-Response Pairs (RRP).
- Identification of all content keys (key IDs) utilized for playback, including time and duration for each key use.
- The generation, time of use (duration) and associated CPL ID for each Link Encryption Key shall be logged.
- Identification of the KDM by which content keys were delivered.
- As applicable, necessary records for the applied Forensic Marking processes (i.e., any data required in support of the FM detection/audit processes), and

the receipt and/or execution of any “no FM mark” state commands (Section 9.4.6.2 Forensic Marking Operations).

- Time and detail noted of any incomplete or non-contiguous playback (e.g., restarts, Section 9.4.5.3.1.1 StartSuite).
- Time and detail of a projection system marriage or maintenance event (e.g., establishment or breakage of the marriage, opening of projector SPB access door, maintenance AuthorityID figure).
- Details of any anomalous security conditions (e.g., issuance of Alert, Query anomalies, TLS or ITM network failures).

9.4.6.3.9. FIPS 140-2 Audit Mechanism Requirements

FIPS 140-2 requirements (see Section 9.5.2.5 FIPS 140-2 Requirements for Type 1 Secure Processing Blocks) require audit (logging) mechanisms for certain modifiable operating system environments for cryptographic modules. These specifications restrict the SBP operating environment to non-modifiable modes of implementation. Thus there are no additional FIPS 140-2 related logging requirements for Exhibition security devices for normal Digital Cinema operations.

Logging requirements for SPB firmware code changes shall be implemented per Section 9.5.2.7 SPB Firmware Modifications. These device-change log records shall be accessible using the log record specifications as given in this section.

9.4.6.3.10. Logging Failures

The secure logging subsystem is required to be operable as a prerequisite to playback. Security Managers (SMs) shall not enable for playback (i.e., key) any suite for which it has not collected log records from Secure Processing Blocks (SPBs) per Section 9.4.6.3.1 Logging Requirements item (8), or if there is any indication that a next playback will not record and report log records as required. Behavior of security devices (SPB or SE) 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 and SEs shall not be purgeable except by authorized repair centers, which are capable of securely recovering such log records.

9.5. Implementation Requirements

9.5.1. Digital Certificates

Digital Certificates are the means by which the Security Manager identifies other security devices, and is also used in establishing Transport Layer Security (TLS) connections. *Each* Secure Processing Block (*SPB) shall carry at least one Digital Cinema specification-compliant certificate, and each SBP certificate shall designate via its role table (see Section 9.8.1.3 Naming and Roles) the specific Security Entities (SEs) that are contained within the SPB. SEs within an SPB may have their own certificate, however exactly one certificate shall designate the SPB role for any SPB*[28].

The make, model, device UUID (if available) and serial number of each certificated device shall be carried in the appropriate fields of the assigned certificate. This information shall also be placed on the exterior of each device in a manner that is easily read by a human.

Digital Cinema certificates shall use the X.509, Version 3 ITU standard (see [ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection

[28] These specifications do not address ITM and/or TLS conflicts that may arise should manufacturers decide to implement SPBs with multiple certificates. In such event, the vendor shall be responsible for meeting all ITM, TLS and robustness requirements as specified herein.

– *The Directory: Authentication Framework, June 1997, and RFC2459]).* This certificate standard for Digital Cinema applications has been constrained in order to reduce the complexity and ambiguity that can occur in systems that use X.509 certificates.

Detailed requirements for Digital Cinema Digital Certificates are given in Section 9.8.1 Digital Certificates.

9.5.2. Robustness and Physical Implementations

This security system protects Digital Cinema content during transport and storage through the use of secret keys. Key secrecy is maintained in normal operations by cryptographic techniques dependent upon other secret keys. The physical protection afforded secret keys, and the content itself once decrypted, determine the robustness of the security implementation.

Robustness is required for all modes of operation, both normal and abnormal. Robustness is a function of the quality of the implementation of security devices, Exhibition operational procedures, and the security system itself.

9.5.2.1. Device Perimeter Issues

Security equipment design must provide physical perimeters around secrets not cryptographically protected. Secure Processing Block (SPB) security perimeter requirements shall meet the following characteristics:

- **Tamper evident** – Penetration of the security perimeter results in permanent alterations to the equipment that are apparent upon inspection. This is the least robust perimeter, since it only reveals an attack after-the-fact, and depends on a specific inspection activity.
    - *SPB type 1 and SPB type 2 shall be tamper evident.*
- **Tamper resistant** – The security perimeter is difficult to penetrate successfully. Compromise of effective tamper resistant designs require the attacker to use extreme care and/or expensive tooling to expose secrets without physically destroying them and the surrounding perimeter(s).
    - *SPB type 1 and SPB type 2 secure silicon (see Section 9.5.2.2 Physical Security of Sensitive Data) shall be tamper resistant.*
- **Tamper detecting and responsive** – The security perimeter and/or access openings are actively monitored. Penetration of the security perimeter triggers erasure of the protected secrets.
    - *SPB type 1 and SPB type 2 secure silicon (see Section 9.5.2.2 Physical Security of Sensitive Data) shall be tamper responsive.*
    - *SPB type 1 shall be permitted to have maintenance access doors or panels, provided that their designs and tamper protections do not permit access (penetration) other than as specified in Section 9.5.2.3 Repair and Renewal.*

9.5.2.2. Physical Security of Sensitive Data

Sensitive data critical to the security of the Secure Processing Block (SPB) or SE (e.g., private keys, LE/LD or content keys) is generically referred to as a Critical Security Parameter (see Section 9.5.2.6 Critical Security Parameters (CSP)). The security system defines levels of protection appropriate to each type of CSP as well as plain text content. The levels of protection are described as follows:

- **Secure Silicon** – Sensitive data can only be compromised by a physical attack on a secure Integrated Circuit storing the data.

a. *Secure integrated circuits used for Digital Cinema security applications shall be of the type designed to resist physical and logical attacks, and shall ensure that a physical attack destroys CSPs prior to exposure. Devices meeting the "secure silicon" level of protection shall be of the FIPS 140-2 Physical Security Single-Chip Cryptographic Module type, and meet FIPS 140-2 level 3 specifications, per the requirements of Section 9.5.2.5 FIPS 140-2 Requirements for Type 1 Secure Processing Blocks.*

b. *Secure silicon level protection shall be used within both SPB type 1 and SPB type 2, with such protection continuously provided (including if powered down) for all SE and Secure Processing Block (SPB) private keys and content image keys.*

c. *Image keys may be stored outside of the secure silicon that performed KDM decryption, provided that such storage meets the requirements of Section 9.7.4 Protection of Content Keys. Device private keys, whether encrypted or not, shall not exist outside of the secure silicon device.*

- **Secure Processing Block** (**SPB) Hardware Module** – Sensitive data will only be exposed by penetration of a physical barrier, which surrounds the electronics.

  a. *All Secure Processing Block (SPB) module designs shall implement hardware module perimeter protection that prevents access to internal circuitry and detects opening of the module perimeter. Further protection of keys and clear text content should use techniques such as burying sensitive traces, applying tamper resistant integrated circuit coverings, and tamper responsive circuitry. Detailed SPB type 1 and SPB type 2 physical protection requirements are defined below in Section 9.5.2.4 Specific Requirements for Type 2 Secure Processing Blocks and Section 9.5.2.5 FIPS 140-2 Requirements for Type 1 Secure Processing Blocks.*

  b. *Other than the SMS, no Security Entity (SE) shall exist outside the protection of a SPB type 1.*

- **Software** – Protection implemented in software can be compromised through modifications to the software, inspection of memory, or monitoring of bus signals.

  a. *Software protection methods shall not be used to protect Critical Security Parameter or content essence.*

9.5.2.3. Repair and Renewal

The following address restrictions on repair and renewal of Secure Processing Blocks (SPBs) and associated cryptographic parameters:

- *Type 1 SPBs may be field replaceable (as an entire SPB module) by Exhibition, but shall not be field serviceable (e.g., SPB type 1 maintenance access doors shall not be open-able in the field).*
- *The secure silicon device, contained within a SPB type 2, shall not be field serviceable, but may be field replaceable. It shall not be accessible during normal SPB type 2 operation or non-security-related servicing.*
- *Repair and renewal processes for an SPB type 1 and SPB type 2 shall be performed under the supervision of the security equipment vendor. Maintenance of the SPB type 2 (projector) is permitted for non-security components accessible via maintenance openings.*

Repair and renewal is limited to failed devices, or devices which have lost or zeroed their secrets (e.g., private keys or digital certificates). Such maintenance does not effect the device's FIPS 140-2 certification or compliance, as long as Section 9.5.2.5 FIPS 140-2 Requirements for Type 1 Secure Processing Blocks requirements are met. Requirements for firmware changes to SPBs are given in of Section 9.7.4 Protection of Content Keys.

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 probably 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.

This SPB is anticipated to surround two fundamental functional environments:

1. *A security environment consisting of a secure silicon chip, input/output signals to the chip and projector SPB perimeter open detection signals and circuits.*
2. *A projector image signal processing environment, that prepares the image signal for light production.*

The latter environment may require field maintenance, and therefore the projector SPB is allowed to have access doors available to Exhibition personnel. The logical relationship and electrical connectivity between the companion and projector SPB was defined in Section 9.4.3.6 Functional Requirements for Secure Processing Block Systems. In addition to these and the requirements of Section 9.5.2.1 Device Perimeter Issues and Section 9.5.2.2 Physical Security of Sensitive Data, additional projector SPB requirements are as follows:

- Table 37 FIPS 140-2 level 3 requirements shall be followed for area (row) number 2, with Transport Layer Security (TLS) security as defined in these specifications providing input/output logical separation protection if TLS is used for projector authentication. The operational environment of the secure chip shall follow Nr 6 of the Limited Operational Environment of Table 37 (also see Section 9.5.2.7 SPB Firmware Modifications).
- The projector SPB silicon chip and associated input/output signals shall not be accessible via the SPB's maintenance door or other openings (i.e., there shall be a partition that separates the chip and signals from the maintenance accessible areas).
- The physical environment surrounding the connected (married) companion and projector SPBs shall be designed such that access to the projector SPB secure silicon chip, input/output signals to the chip, and signals going between the SPBs is not possible without causing permanent and easily visible damage to either or both of the SPBs.

In summary, a tamper detecting/responding secure silicon chip provides protection for CSPs. Protection for image essence (and the silicon chip) is provided by the projector's SPB' physical perimeter. An SPB type 2 intrusion detection/response is minimally provided by the access door open detection, and Exhibition visual inspection is relied upon to detect physical abuse that might allow compromise of, or access to, decrypted image essence.

9.5.2.5. FIPS 140-2 Requirements for Type 1 Secure Processing Blocks

Robustness requirements for Digital Cinema Secure Processing Blocks (SPBs) shall follow the guidelines of the Federal Information Processing Standards [FIPS PUB 140-2][29]*.* A summary of these requirements is shown in the table below.

FIPS 140-2 specifies eleven areas for evaluation against a rating, which shall be performed by US government recognized independent laboratories.

All SPB type 1 shall meet and be certified for the requirements of FIPS 140-2 Level 3 in all areas except those subject to the following exceptions or additional notes (the Nr indicators refer to the table items by row):

- Nr 2 – Logical data port separation requirements shall be supported by the use of Transport Layer Security (TLS) protection on well known port 1173 as defined in Section 9.4.5.2.3 General RRP Requirements.
- Nr 3 – *The* Screen Mana*gement System (SMS) (Section 9.4.2.5 Screen Management System (SMS)) shall support role-based authentication with the* Security Manager(s) *via their certificates and Transport Layer Security (TLS) authentication. The security system shall support SMS operator and authorized equipment installer Identity-based authentication with the* Security Manager(s)SMs (see the "AuthorityID" Intra-Theater Message field, Section 9.4.5.2.4 Request-Response Pairs (RRP)).
- Nr 6 – *The software operating environment of* Secure Processing Blocks (*SPBs) shall be restricted to the Limited Operational Environment.* This eliminates the requirements for Common Criteria (CC) and Evaluation Assurance Level (EAL) testing, and any additional FIPS140-2-specific logging/audit processes other than those specified in Section 9.5.2.7 SPB Firmware Modifications for firmware modifications.
- Nr 7 – *Section 9.7 Essence Encryption and Cryptography of these Digital Cinema requirements shall supersede any conflicts with Nr 7.*
- Nr 8 – Secure Processing Blocks (*SPBs) shall only be required to meet Security Level 2 business use A FCC class requirements.*
- Nr 10 – Design Assurance requirements may meet Security Level 2 requirements.
- Nr 1 and Nr 11 – *Vendor-specified Security Policy specifications shall be in alignment with and fully support the requirements of this Digital Cinema specification, in addition to vendor-specific policies.*

[29] Readers unfamiliar with [FIPS PUB 140-2] will need to refer to the standards text to fully understand the table and exceptions.

Nr	Section	Security Level 1	Security Level 2	Security Level 3	Security Level 4
1	**Cryptographic Module Specification**	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
2	**Cryptographic Module Ports And Interfaces**	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically separated from other data ports.	
3	**Roles, Services And Authentication**	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
4	**Finite State Model**	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
5	**Physical Security**	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detect & response. EFP and EFT.
6	**Operational Environment**	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
7	**Cryptographic Key Management**	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, & key zeroization.			
		Secret and private keys established using manual methods may be entered or output in plaintext form.		*Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.*	
8	**EMI/EMC**	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
9	**Self-Tests**	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.		Statistical RNG tests. Callable on demand	Statistical RNG tests performed at power-up.
10	**Design Assurance**	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Pre/post conditions.
--	**Mitigation of Other Attacks**	Specification of mitigation of attacks for which no testable requirements are currently available.			

Table 37: Summary of FIPS 140-2 Security Requirements[30]

[30] From Section 4 of [FIPS PUB 140-2]

9.5.2.6. Critical Security Parameters (CSP)

A requirement of FIPS-140-2 is to list the Critical Security Parameters (CSP) that are important for the security of Digital Cinema cryptographic module(s) (Secure Processing Block) and its functions. The following CSPs shall receive Secure Processing Block (SPB) type 1 protection, whenever they exist outside of their originally encrypted state.

1. *Device Private Keys – RSA private key that devices use to prove their identity and facilitate secure Transport Layer Security (TLS) communications.*
2. *Content Encryption Keys – KDM AES keys that protect content.*
3. *Content Integrity Keys – HMAC-SHA-1 keys that protect the integrity of compressed content (integrity pack check parameters).*
4. *Control Message Encryption and Integrity Keys – AES, HMAC-SHA-1/SHA-256 keys/parameters that protect the privacy and/or integrity of Composition Play Lists, Track File Lists, Key Delivery Messages and other ETMs.*
5. *Link Encryption Keys – Keys that protect the privacy and integrity of uncompressed content for link encryption.*
6. *Watermarking or Fingerprinting command and control – Any of the parameters or keys used in a particular Forensic Marking process.*
7. *Transport Layer Security (TLS) secrets – These are transient keys/parameters used or generated in support of TLS and Intra-Theater Messaging (ITM).*
8. *Logged Data – All log event data and associated parameters constituting a log record or report.*
9. *The FIPS-140-2 rule for Critical Security Parameter delivery to/from the secure module is that all CSPs must be input and output from the device via a trusted, private, tamper detecting path. The ITM and TLS security methods required in this specification provide such a path.*

9.5.2.7. SPB Firmware Modifications

The Limited Operational Environment operating system requirement of FIPS 140-2 Section 9.5.2.5 FIPS 140-2 Requirements for Type 1 Secure Processing Blocks restricts SPBs type 1 and the secure silicon chip of SPB type 2 from having their operating system or firmware modified in the field. The following defines the requirements for making firmware[31] changes to these security devices. FIPS 140-2 constrained devices shall:

- *Be designed such that their firmware cannot be modified without the knowledge and permission of the original manufacturer.*
- *Require a Digital Cinema compliant certificate that authenticates and confirms the identity of the authority figure responsible for making a firmware change.*
- *Not undergo firmware changes without informing potentially affected information bases that support Digital Cinema equipment operations (e.g., databases used by stakeholders for facility lists, KDM and TDL creation), and the owner of the device.*
- *Log the firmware change event by meeting FIPS 140-2 Operational Environment (row 6 of Table 37) audit/recording requirements of the Operating System Requirements subsection Security Level 3, except that Common Criteria (CC) and Evaluation Assurance Level (EAL) certification mandates shall not be required.*

[31] The term firmware shall mean all operating system, software, firmware or ROM based code within the SPB type 1 SPB type 2 silicon chip.

- *Enable the extraction of the above firmware change related log records using standard log record messages per Section 9.4.6.3 Logging Subsystem. For the delivery of these log records, it shall be mandatory that the records be signed, and the TLS-dependent alternative of Section 9.4.6.3.5.1 not be used.*
- *Follow FIPS 140-2 certification body change notification requirements regarding modifications to security devices. Undergo re-certification if required.*

9.5.3. Screen Management System (SMS)

There are no physical constraints or requirements imposed on the SMS by the security system (i.e., no SPB requirements), other than the requirement for the SMS's private key to be contained within a secure silicon device (see Section 9.4.2.5 Screen Management System (SMS)). The SMS implementation shall not otherwise weaken or effect the security operations of other Security Entities or SPBs.

9.5.4. Subtitle Processing

Subtitle encryption is directed primarily against interception during transport, and cryptographic protection within the theater is not required. There are no physical constraints or requirements imposed on subtitle decryption processing by the security system, other than it's implementation shall not weaken or otherwise effect the security operations of other Security Entities or SPBs.

9.5.5. Compliance Testing and Certification

Compliance Testing is the process of qualifying Secure Processing Blocks (SPBs) and their Security Entities for use in Digital Cinema systems. *All SPBs shall be subject to qualifying criteria in the following areas:*

- Compliance to Intra-Theater Messaging (ITM) specifications – *The SPB and internal logical* SEs *shall interpret and respond to the standard ITM message set according to the appropriate Section 9.4.5.2.4 Request-Response Pairs (RRP) category as specified herein.*
- *Image Media Blocks shall support compliance with standardized Extra-Theater Messaging (ETM) specifications, in addition to the above compliance requirement for ITMs.*
- *The SM and Secure Processing Block systems shall meet the functional requirements as specified in Sections 9.4.3.5 Functions of the Security Manager (SM) and 9.4.3.6 Functional Requirements for Secure Processing Block Systems, respectively.*
- Compliance to SPB physical and logical requirements – *Each SPB shall be evaluated against physical and logical requirements based on the SPB type per Section 9.5.2 Robustness and Physical Implementations, including FIPS 140-2 requirements as applicable.*

Device vendors shall issue Digital Cinema certificates only to devices that comply with this specification. Such issuance enables the devices to become certified.

A device that does not meet all of the above criteria shall not be installed in a DCI compliant Digital Cinema system. A device that does not continue to meet all the above criteria shall be declared a Security Function Failure, and shall be taken out of service until repaired.

9.5.6. Communications Robustness

The following are required for the exhibition of content and security communications, and communications networks:

- *Theater networks shall protect security system(s) from the threat of external and internal network-borne attacks by the use of appropriate firewalls. At a minimum, each auditorium shall have such firewall protection for any communications interface(s) connecting to the intra-auditorium security network.*
- *Digital Cinema security messages and content shall not be carried over a wireless network, but shall be carried over wire or optical cables.*
- *The portions of the network used to carry any security messages or content shall be logically or physically separated from any wireless network device. At a minimum, a properly configured firewall shall separate the wired network that carries security messages or content from any wireless network operated at the same facility.*
- *The network cabling or cabling trough should not be publicly accessible on the premises.*

9.6. Security Features and Trust Management

This section describes the standardized Digital Cinema security operational features, and how "trust" is communicated and enforced to ensure security features are reliably executed. A security policy is what results once the variables that develop, from the overall security system design and implementation, are constrained according to desired operational characteristics. An open architecture security system should not dictate any specific policy, but enable stakeholders to agree on one more policies that support business needs. Once policy has been decided, it can be described operationally as the security feature set.

9.6.1. Digital Rights Management

This section identifies various features and functions that describe the operation of the security system. For each auditorium equipment suite, the security system consists of three types of components involved in Digital Rights Management (DRM):

1) The Screen Management System (SMS)
2) The Security Manager (SM)
3) The associated security equipment (e.g., Media Block, Link Decryption Block)

The last two components have access to, and process, Digital Cinema security information (secrets), such as content keys or plain text content. They are the primary subject of these security specifications. The Screen Management System does not have access to such secrets. But because the Screen Management System initiates security-related activity, it is considered a participant in security events.

The basic business philosophy is to "control lightly, audit tightly." Per this philosophy, a movie will fail to playback only under four circumstances:

1) Wrong location see Table 38
2) Wrong date and time (outside the engagement window) see Table 38
3) Unauthorized device (equipment is not accepted by the content owner) see Table 38
4) Failure of, or tampering, with security equipment see Table 39

Compliance to security system logging requirements ensures that all events having security implications will generate associated log records that are stored in the Image Media Block. These log records can be accessed by the exhibitor's Screen Management System, and reports can be provided to appropriate distributors under contractual obligations.

All three types of security system components (Screen Management System, Security Manager, security equipment) have defined roles and responsibilities (e.g., to perform their security functions and generate log records), and overall security depends upon their proper operation. The descriptions below detail the three types of security system components.

Included in the Security Manager and security equipment description are tables showing possible security system operational scenarios and how the system responds to a particular issue.

The tables are also designed to be informative to parties interested in understanding business issues in relation to the Digital Cinema security system. It shows that the security system's reach is limited to only those areas necessary for ensuring persistent protection of content and security data (keys), enabling content to play within a designated time window, and the provisioning of reliable log data (Table 38 and Table 39).

9.6.1.1. Digital Rights Management: Screen Management System

The Screen Management System is responsible for managing Exhibition functions such as showtime movie playback, and is under the control of the Exhibitor. The Screen Management System manages playback functions via the Security Manager, however the Security Manager is at all times in control of and responsible for security functions and events. The full compliment of Exhibition operational events therefore consists of those under the control of the Security Manager and those under the control of the Screen Management System.

9.6.1.2. Digital Rights Management: Security Manager (SM)

The Security Manager is the executor of Digital Rights Management for each auditorium. It controls content keys and the delivery of such keys to the appropriate security equipment to enable playback of encrypted content.

Each Security Manager (and the Image Media Block it is part of) is assigned to a single projector. Keys are considered active for the business defined play period. Subject to security equipment authentication, proper operation, and integrity checks (see Section 9.4.3 Theater Security Operations), the Security Manager exercises no control over playback, other than content key delivery during the valid play period. Under private business negotiations, a Distributor may provide keys for selected or all Security Managers (i.e., projectors) in a complex.

Item, Observation or Issue	Approach
Authorized auditorium	KDM (keys) is sent to authorized auditorium SM
Engagement Play-out Window	KDM contains designated key use time/date window
Only known & trusted devices are enabled	SM authenticates equipment prior to key delivery
Modified Movie File	At playback, SM checks and logs movie against CPL

Table 38: Examples of Security Manager Events

The above table depicts events related to the Security Manager and the system's behavior. A film will not play-out if there is a failure in any of the items in rows 1, 2 and 3 due to wrong location (row 1), wrong date/time (row 2), or the attempted use of an unauthorized device (row 3). In the event of modification in a movie file (row 4), the file should be replaced, but there are no Security System controls preventing an Exhibitor from playing-out a modified file. This event, like all security events, will be logged.

9.6.1.3. Digital Rights Management: Security Entity (SE) Equipment

Security Entity equipment must perform to specified standards and function as designed. The Security Manager will continuously test for proper Security Entity identification (authentication), operation and physical integrity (tampering). Content playback is restricted to passing all security tests at all times.

Item, Observation or Issue	Approach
Security equipment tampering or failure	A tampered or failed device is non-functional until replaced
Auditorium (intra-suite) Security Network	Network must be operative to initiate playback

Table 39: Examples of Failure or Tampering of Security Equipment

The above table depicts tampering or failure of security equipment. Security equipment that has been tampered with or is malfunctioning (row 1) shall not continue operation and must be replaced before playback can commence (or continue). An example of malfunctioning security equipment is a Media Block that no longer performs one of its security functions (e.g., decryption, Forensic Marking, logging). If the auditorium security network is inoperative (row 2), playback cannot start. However, the security system will not cause playback to stop upon failure of the network during a show.

9.6.2. "Trust" and the Trusted Device List (TDL)

In a "trust" relationship, it is said "A trusts B regarding X". More specifically, the relying party A believes that B will behave in certain predictable ways under a certain range of conditions. This behavior-based definition can apply both to business relationships and to the more formalized regime of standardized security devices. And in fact, a useful Digital Cinema trust system must bridge the former to the latter.

When a Distributor trusts a piece of equipment, his level of confidence in its behavior is based on several factors such as those in Table 40.

	Factor	Root of Trust
1	Robust equipment design	Manufacturer and certification organization
2	Reliable manufacturing process	Manufacturer
3	Properly installed	Installer and organization operating device
4	Properly maintained (e.g., required firmware or security updates)	Organization operating device, manufacturer and certification organization
5	Properly managed (configured, inspected and operated in accordance with expectations during operational life)	Organization operating device
6	Has not been tampered with before or after installation	Organization operating device, certification organization

Table 40: Factors Supporting Trust in a Security Device

Protecting the content keys under a full range of potential situations can be a complex task, representing a set of behaviors involving rules and policy that meet the requirements of these specifications and (optionally) the particular business relationship. To simplify trust issues for the Digital Cinema environment, the TDL approach to equipment trust communications has been defined. In this approach, Rights Owners will indicate their approval of specific trusted equipment to be used in conjunction with an engagement by placing the identification of trusted equipment (Secure Processing Blocks and projectors) into the Key Delivery Messages (KDMs) that are sent to Security Managers. Security

Managers will trust and accept devices so listed for all security functions subject to the device's certificate declared roles (see Section 9.5.1 Digital Certificates).

The content of TDLs (e.g., facility-wide, auditorium-specific, inclusive of spares) shall be according to business party agreement, and is out of scope of these specifications.

9.6.2.1. Trust Domains

The SM Security Domain is represented by the collection of security devices associated with a single SM that work together to perform a security function. In this system, the SM Security Domain and its Trust Domain[32] are equal, and in the theater these domains are a single auditorium equipment suite. Multiple trust domains are typically used (chained) together to achieve overall security management objectives (e.g., distributing content keys from post-production to Distribution and Exhibition via multiple KDMs).

The SM functions as an anchor for a given Trust Domain. For convenience, this specification uses descriptors such as Distributor SM, Auditorium SM, etc., but it will be recognized that the security system does not mandate any particular topology for Security Managers (SMs) other than requiring that the Image Media Block contain a Security Manager.

The security system must be sufficiently flexible to support complex groupings and relationships between the Rights Owners, Distributors and Exhibitors. Trust Domains represent the essence of these relationships. The required flexibility is achieved through trust communications that supports the existence of simultaneous multiple overlapping domains, as opposed to force-fitting them into a single domain. In practice, this is implemented via the Digital Certificate chains and TDL that is part of the KDM. Digital Certificate chaining and TDL management is out of scope of these standards.

9.6.2.2. Authenticating Secure Processing Blocks and Linking Trust Through Certificates

A Digital Cinema Certificate is a declaration by a trusted organization, such as a manufacturer, that the security device is a particular make and model and is certified (i.e., found compliant to this specification) to perform identified DC roles (e.g., perform Image or Sound Decryption or provide SPB physical protection functions). The certificate is cryptographically bound to the security device it represents, in such a way that the authenticity of the device is easy to verify. The Certificate is also cryptographically bound to the entity that issued it. This latter binding can be authenticated by knowing and trusting another certificate, that of the certificate issuing entity, called the issuing authority or Certificate Authority. Certificates of issuing authorities are called root certificates.

The design of the certificate includes a technique called chaining, which is an elegant and cryptographically strong method of linking certificates back to the root certificate owned by its issuing authority. Thus, where required an entity can authenticate end entity leaf certificates by knowing just the (set of) root certificates it needs.

The use of certificates to authenticate Secure Processing Blocks (SPB) or Security Entites (SEs) prevents the theft of content by substituting a rogue device for a legitimate Secure Processing Block (SPB) or Security Entity (SE) *The security system requires (only) Image Media Block Security Managers to perform authentication functions, permitting the SM to safely extend trust to encompass those SPBs and SEs, thus forming its trust domain.*

[32] Trust Domain areas also exist for post-production and distribution, but are out of scope.

9.6.2.3. Identity vs. "Trust"

In the theater, the SM uses certificates for two primary functions: 1) authenticating a Secure Processing Block's (SPB's) identity and roles, and 2) establishing the secure Transport Layer Security (TLS) session for Intra-Theater Messaging communications with that Secure Processing Block (SPB). These two functions are performed simultaneously when the SM and Secure Processing Block (SPB) set up their Transport Layer Security (TLS) session, during which, the Secure Processing Block (SPB) presents its certificate chain to the SM. This process opens secure communications between security devices in each auditorium suite, and allows the SM to identify suite equipment.

However, decisions that the SM makes regarding its "trust" in accepting the remote Secure Processing Blocks (SPBs) as capable of playing content (receiving content keys, etc.) is independent of the above identity/authentication process. Trust decisions are made on a Rights Owner by Rights Owner basis, and communicated via the TDL in the KDM (see Section 9.4.3.1 Transport Layer Security (TLS) Establishment and Secure Processing Block (SPB) Authentication and Section 9.4.3.5 Functions of the Security Manager (SM), item 7).

9.6.2.4. Revocation and Renewal of Trust

The use of TDLs in the KDM allows a simple and effective way for Distributors to communicate trust in exhibition equipment to the responsible Security Managers. However, the source (database) of equipment lists, from which TDL information is derived must be managed with respect to revocation and renewal issues per Table 40 above.

In routine operation, trusted equipment remains trusted indefinitely. However there may be situations in which trust in a security device needs to be terminated or restored. Controlling change in trust relationships is an important aspect of trust management.

Database references for TDL creation must be managed with respect to trust issues. However, these are outside the scope of this specification.

9.7. Essence Encryption and Cryptography

The security system employs widely used and rigorously tested ciphers for use in Digital Cinema. The following are requirements pertaining to Digital Cinema applications for ciphers and associated security parameters.

9.7.1. Content Transport

Content security is transport agnostic, and can be accomplished by either electronic or physical means. Other than as authorized and intended by Rights Owners (e.g., to support Distribution practices or requirements), content shall only be decrypted at playback time at the exhibition site under the policy of the SM.

9.7.2. Image and Sound Encryption

The AES cipher, operating in CBC mode with a 128 bit key, shall be used for Digital Cinema content encryption. See [FIPS-197 "Advanced Encryption Standard (AES)" November 26, 2001. FIPS-197] and Section 5.3.2 MXF Track File Encryption for MXF track file encryption details.

The content Rights Owner shall determine which, if any, of the essence types in the composition are encrypted for distribution.

9.7.3. Subtitle Encryption

The Subtitle List element shall be encrypted using xmlenc-core. The AES-128 CBC symmetric cipher shall be used. The cryptographic key shall be identified using a unique KeyID value and delivered using the Key Delivery Message (see Section 9.8.3 Key Delivery Message (KDM)).

Subtitle encryption is directed primarily against interception during transport, and cryptographic protection within the theater is not required. For example, plaintext subtitle content may be transmitted from a server device to a projection unit. It is preferred, but not required, that subtitle content be maintained in encrypted form, except during playback.

9.7.4. Protection of Content Keys

The RSA Public Key Cipher (with 2048-bit key) shall be used to protect keys for distribution. This is accomplished by the requirements of the Key Delivery Message.

The above RSA asymmetric protection, AES (with 128-bit keys) or TDES (with 112-bit key) symmetric ciphers, may be used to protect the storage of keys once decrypted from the KDM within a Media Block (e.g., where off-secure-chip memory is used for key caching within a Media Decryptor, for example).

9.7.5. Integrity Check Codes

Data integrity signatures (hash values) shall be generated/calculated according to the PKCS-1 Digital Signature Standard, as specified in [IETF RFC 3447 (RSA and SHA-256)]. All signatures shall use SHA-256. Digital Certificates in X.509v3 format as constrained according to Section 9.8.1.2 Field Constraints, shall be used to authenticate signatures. Signature element definitions and other signature details are available in the specification for each signed data structure.

Cryptographic data integrity checksums shall be ensured according to the HMAC-SHA-1 algorithm, as specified in [FIPS PUB 198a "The Keyed-Hash Message Authentication Code."]

9.7.6. Key Generation and Derivation

Keys shall be generated as specified in [IETF RFC 3447]. A vendor that pre-loads an RSA private key into a device (e.g., secure silicon per Section 9.5.2.2 Physical Security of Sensitive Data) shall ensure that these pre-loaded keys are unique to each device made by that vendor. The vendor shall not keep any record of the preloaded private keys, though they can keep records of the matching public keys. RSA keys shall be 2048 bits in length, and may 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 (unpredictability).

A vendor that pre-loads an AES or TDES symmetric key into a device shall generate each key with a high quality random number generator with at least 128 bits of entropy (112 bits for TDES). The vendor may not keep any records of these symmetric keys.

9.7.7. Numbers of Keys

No more than 256 keys should be used to encrypt the essence of a single composition (i.e., Composition Playlist). To support multiple shows, Media Decryptors should be capable of securely caching at least 512 keys. The Show Playlists may be comprised of multiple compositions.

9.8. Digital Certificate, Extra-Theater Messages (ETM), and Key Delivery Messages (KDM) Requirements

This section gives the detailed requirements for Digital Cinema Digital Certificates, ETM and KDM.

9.8.1. Digital Certificates

Digital Cinema certificates shall use the X.509, Version 3 ITU standard (see [ITU-T Recommendation X.509 (1997 E): Information Technology — Open Systems Interconnection – The Directory: Authentication Framework, June 1997, and RFC2459]). This standard is developed for Digital Cinema applications in constrained ways, in order to reduce the complexity and ambiguity that can occur in systems that use X.509 certificates. This section describes those constraints.

9.8.1.1. Required Fields

Table 41 below summarizes the required fields. Additonally, Table 42 describes the detailed constraints for each field. *The certificate shall be encoded using the ASN.1 DER rules, which produce a unique representation for the certificate.*

Field	Description
The first two fields appear outside of the signed portion of the certificate.	
SignatureAlgorithm	Identifier of the algorithm used to sign this certificate. Must be same as signature field inside the certificate.
SignatureValue	Value of the signature for the certificate.
The following fields are inside the signed portion of the certificate. The fields after the SubjectPublicKeyInfo field appear in the extensions part of the signed portion.	
Version	Indicates X.509 Version 3 format certificates.
SerialNumber	Serial number of certificate that is uniquely chosen by the Issuer.
Signature	Identifier of the signature algorithm. It appears inside the signed portion of the certificate and must match the algorithm identified on the outside in the SignatureAlgorithm field.
Issuer	Name of entity that issued and signed this certificate.
Subject	Name of the entity that is the subject of this certificate and thus controls access to the private key that corresponds to the public key that appears in this certificate.
SubjectPublicKeyInfo	Information about the subject's public key including the algorithm type, any algorithm parameters and the set of values that makes up the public key, such as modulus and public exponent for RSA.
Validity	Date/Time range when the certificate is valid.
AuthorityKeyIdentifier	This field identifies the issuer's certificate.
KeyUsage	Collection of flag bits that identify all the operations that are authorized to be performed with the public key in this certificate, and thus imply what can be done with the corresponding private key.
BasicConstraint	This field indicates whether certificate signing is allowed and specifies the maximum number of certificate signing certificates that can appear in the chain below this one.

Table 41: Required X.509v3 fields for Digital Cinema Certificates

Digital Cinema certificates may contain other extension fields that are meaningful to equipment from specific vendors. Implementations shall ignore non-critical extensions they do not understand, and shall reject the certificate if it contains a critical extension field that they do not understand.

9.8.1.2. Field Constraints

The following table describes the constraints on the required fields.

X.509 Field	Description
SignatureAlgorithm	Shall be sha256WithRSAEncryption, which is the algorithm identifier for encrypting a SHA-256 (see [FIPS 180-2]) digest of the certificate body with RSA using PKCS #1 v1.5 signature padding (see [PKCS1]). Multi-Prime private keys are allowed as explained below.
SignatureValue	This field is an ASN.1 Bit String that contains a PKCS #1 signature block. It shall contain a SHA256WithRSA signature.
Version	Shall indicate X.509 Version 3 format certificates.
SerialNumber	Unique number assigned by Issuer. Shall be a non-negative integer that is 160-bits long or shorter.
Signature	Shall be sha256WithRSAEncryption[33] algorithm identifier.
Issuer	Globally unique name of entity that issued and signed this certificate. See section on Naming and Roles, for further constraints.
Subject	Globally unique name of the entity that controls access to the private key that corresponds to the public key this certificate. See section on Naming and Roles, for further constraints.
SubjectPublicKeyInfo	This shall describe an RSA public key. The RSA public modulus shall be 2048-bits long. The public exponent shall be 65537. The same public key may appear in multiple certificates. Certificate issuers should try to ensure that when a public key appears in multiple certificates, those certificates correspond to the same entity or device.
Validity	The issuer shall always encode certificate validity dates through the year 2049 as UTCTime (two digit years); certificate validity dates in 2050 or later shall be encoded as GeneralizedTime (four digit years). ([Time])
AuthorityKeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	Shall be present in all certificates, including root certificates. These attributes are the unique identifier for the issuer's certificate. They name the issuer of the issuer's certificate and the serial number assigned by the issuer's issuer.
KeyUsage	Shall be present in all certificates, including root certificates. For certificate signing certificates, only the KeyCertSign flag shall be true. For leaf certificates the DigitalSignature and KeyEncipherment flags shall be true. Other flags may be true.
BasicConstraint	This field shall be present in all certificates. When present, the certificate authority attribute shall be true only for certificate signing certificates. For Digital Cinema Security Entities in theaters, the certificate authority attribute shall be false, and the PathLenConstraint shall be absent (or zero).

Table 42: Field Constraints for Digital Cinema Certificates

[33] The value of "sha256WithRSAEncryption" can be found in [IETF RFC 3447].

9.8.1.3. Naming and Roles

Each entity that is the subject or issuer of a Digital Cinema certificate is unambiguously identified by a number of attributes. In order to enable the mapping of these attributes into the X.509 name structure, this specification overloads (gives further meaning to) the existing semantics of the X.509 name attributes, as summarized in Table 43.

Digital Cinema Attribute	X.509 Name Attribute	Description
Public Key Thumbprint	DnQualifier	Unique thumbprint of the public key of the entity issuing the certificate or being issued the certificate.
n/a	CountryName	This X.509 name attribute shall not appear in Digital Cinema certificates.
Root Name	OrganizationName	Name of the organization holding the root of the certificate chain.
Organization Name	OrganizationUnitName	Name of the organization to which the issuer or subject of the certificate belongs. For non-SM SE devices, this field does not identify the end owner or facility; rather it identifies the device maker.
Entity Name	CommonName	Entity issuing the certificate or being issued the certificate. See Entity Name and Roles section.

Table 43: Mapping of Digital Cinema Identity Attributes to X.509 Name Attributes

9.8.1.3.1. Public Key Thumbprint (DnQualifier)

Exactly one instance of the DnQualifier attribute shall be present in the Subject name and the Issuer name. When the DnQualifier appears in the Subject name field, it is the thumbprint of the subject public key that appears in this certificate (see Section 9.8.1.4 Certificate and Public Key Thumbprint for thumbprint definition). When the DnQualifier appears in the Issuer name field, it is the thumbprint of the public key that is used to verify the signature on this certificate (i.e., the thumbprint of the public key that appears in the issuer's certificate).

9.8.1.3.2. Root Name (OrganizationName)

The OrganizationName identifies the entity that is responsible for the root of trust for this certificate. *Exactly one instance of the OrganizationName attribute shall be in the Subject name and the Issuer name. The OrganizationName in the Issuer field shall match the OrganizationName in the Subject field. This means that the OrganizationName shall be the same in all certificates that chain back to the same root. The OrganizationName attribute shall be unique.*

9.8.1.3.3. Organization Name (OrganizationUnitName)

There shall be one instance of the OrganizationUnitName attribute. When the OrganizationUnitName appears in the Subject name field, it is the name of the organization to which the certificate has been issued and supplements the vendor information found in the CommonName attribute. When the OrganizationUnitName appears in the Issuer name field, it is name of the organization that issued the certificate.

9.8.1.3.4. Entity Name and Roles (CommonName)

Exactly one instance of this attribute shall appear in the Subject name and the Issuer name fields. It expresses the Digital Cinema role(s) performed by the entity and expresses the physical identification of the entity (make, model, and serial number for devices). *The Role shall be present in all leaf (Security Entity) certificates.*

Role types shall include SMS, SM, Secure Processing Block (both SPB type 1 and SPB type 2 projector), Image Media Decryptor, Audio Media Decryptor, Subtitle Media Decryptor, Forensic Marker, Link Encryptor and Link Decryptor.

9.8.1.4. Certificate and Public Key Thumbprint

The Public Key Thumbprint is a statistically unique identifier of a public key, and thus also an identifier of the matching private key.

A Public Key Thumbprint shall be the SHA-1 hash (see [FIPS-180-2]) of the contents of the SubjectPublicKey BIT STRING in the SubjectPublicKeyInfo field (excluding the DER tag, length, and number of unused bits count in the DER header for the BIT STRING).

9.8.1.4.1. Certificate Processing Rules

This section describes the rules for validating certificates and chains of certificates.

9.8.1.4.1.1. Validation Context

Certificates are always validated in a context. The context consists of the following components, any of which may be empty except for the first, which shall be present:

1. *A chain containing the certificate being validated*
2. *A minimum chain length (number of certificates)*
3. *A desired role*
4. *An effective time (i.e., time and date)*
5. *A set of trusted root certificates*
6. *A set of invalid certificate identifiers (issuerName-serialNumber pairs)*
7. *A set of invalid public key values*

9.8.1.4.1.2. Validation Rules

To validate a certificate chain, the SE performs at least the following steps:

1. *Parse the certificate with the ASN.1 DER (Distinguished Encoding Rules) decoding rules and reject the certificate if there are syntax errors or it is not in DER encoded. This avoids the need to re-code certificates that were received in BER (Basic Encoding Rules) format in order to verify the signature.*
2. *If the version field is not X.509v3, reject it.*
3. *If any unrecognized extensions in the certificate are marked Critical, reject it.*
4. *If any required fields are missing, reject it.*
5. *If the Certificate Authority attribute of the BasicConstraint field is True, check that the PathLenConstraint value is present and is either zero or positive. This disallows certificate chains of unbounded length. If the certificate authority attribute of the BasicConstraint field is False, check that the PathLenConstraint field is absent (or zero).*

6. *Check that the KeyUsage field is present. If the certificate authority attribute of the BasicConstraint field is True, then only the KeyCertSign flag shall be set, otherwise the keyCertSign cannot be set and at least the DigitalSignature and the KeyEncipherment flags shall be set. Reject certificates that violate this rule.*
7. *If the OrganizationName in the subject and issuer fields do not match, reject it. This is the only name subordination rule that is enforced.*
8. *If the certificate is a leaf certificate (one where the certificate authority attribute of the BasicConstraint field is False), check that there is at least one role specified in the CommonName. It is permitted for non-leaf certificates, those with BasicConstraint. Certificate authority is set to True, to have an empty list of roles, in which case the first character of the CommonName shall be the period character, which marks the end of the role field within the CommonName. If the validation context includes a desired role, check that this role appears.*
9. *If the validation context includes a desired time[34], check that the desired time is within the validity dates.*
10. *Check that the signature algorithms specified inside and outside of the certificate body match and that both equal sha256WithRSAEncryption. (see Table 42)*
11. *Check that the subject's Public Key is an RSA key with the expected length and exponent.*
12. *Reject the certificate if the subject's public key is on the list of invalid public keys, or the issuer and serial number of this certificate is on the list of revoked certificates. If invalid keys or certificates are absent from the validation context, the respective test is not performed.*
13. *Check that the computed subject's Public Key Thumbprint after Base64 encoding matches the value of the DnQualifier attribute in the Subject name field.*
14. *Look up the issuer's certificate using the value of the AuthorityKeyIdentifier attribute. If it is not found, reject the certificate.*
15. *Validate the SignatureValue in the certificate using the issuer's public key. If not valid, reject the certificate.*

To validate a chain of certificates, validate each certificate using the steps above, and also perform the following steps on each pairing of the parent (issuer) certificate and the direct child (subject) certificate.

1. *Check that the certificate chain contains at least the number of different certificates specified in the validation context.*

   Note: A minimum chain length of three certificates is (encouraged) recommended for equipment identity applications.
2. *Check that the issuer field in the child certificate matches the subject name of the parent certificate. This check provides the important security assurance that the hash of the public keys as expressed in the DnQualifier attributes has the expected value.*
3. *Check that the validity dates of the child certificate are completely contained in the validity dates of the parent certificate. This step does not*

[34] In most cases the desired time is the current time, but a different time might be used to examine historical or future information. Applications executed by devices, that do not need to know the current time in order to otherwise comply with these specifications typically will not include a desired time in the validation context and therefore will skip this step.

require a real-time clock. It is just a consistency check between data in the parent and child certificate. Failing this check indicates a problem with a Certificate Authority, and thus it is important that all SE perform this check.

4. *Check that the root of this certificate chain appears in the list of trusted root certificates that have been included in the context for this validation.*

9.8.2. Generic Extra-Theater Message (ETM)

The ETM specification addresses unidirectional messaging, in the sense that the protocol does not require a real-time bi-directional channel. The primary benefit of a standardized format is to facilitate extensions to the security system without the risk that new types of messages might introduce security flaws. The Extra-Theater Messages **(**ETM) employs cryptography to restrict access to sensitive parts of the message to the intended recipients, and to ensure the integrity and authenticity of the message.

Currently, it is envisioned that there will be Extra-Theater Messages for:

- Delivering content decryption keys and Trusted Device Lists (TDL) to theaters (in the Key Delivery Message).

Vendors of security equipment may implement additional Extra-Theater Message types. Such messages shall conform to the generic ETM *format.*

The ETM specification is a generic XML security wrapper in the sense that it includes specific fields that can be extended to carry different kinds of information to meet various application-level requirements. For example, the KDM is a specific extension of this format to deliver content decryption keys to an Exhibition facility. The ETM uses the W3C Extensible Markup Language to represent the information payload and provides security using the XML Encryption and Signature primitives.

9.8.2.1. Overview of Generic Extra-Theater Message

Figure 22 below presents an overview of the generic security wrapper. The top-level XML element indicates that this structure is a Digital Cinema Extra-Theater security Message. It contains three elements (segments) of data: 1) authenticated and public (viewable by anyone who receives the message), 2) authenticated and private (viewable by the intended recipients only), and 3) authentication information (signature and trust).

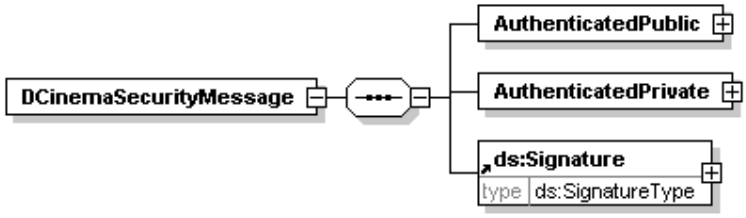

Figure 22: XML Diagram for Generic Extra-Theater Message

The AuthenticatedPublic segment shall include standard message header information and a place to put required standard extension elements for the particular message type, and a place for proprietary extensions that are not critical to the baseline interoperability standard. The single signer of the ETM shall be identified in the AuthenticatedPublic segment, and any entity that receives the message shall be able to read and authenticate the information in the AuthenticatedPublic segment.

The AuthenticatedPrivate segment includes zero or more blocks of information encrypted by RSA (called EncryptedKey) and an optional block of information encrypted

by AES (called EncryptedData). The use of the EncryptedKey and EncryptedData fields is application-dependent.

The Signature segment includes: 1) the value of the signer's certificate chain (note that the identity of the signer appears in the AuthenticatedPublic segment), 2) a SignedInfo segment that separately specifies the expected hash of the AuthenticatedPublic and AuthenticatedPrivate parts and 3) an RSA signature on the SignedInfo element, which thus authenticates the two expected hash values, that in turn authenticate the AuthenticatedPublic and AuthenticatedPrivate portions.

9.8.2.2. Authenticated and Public (Unencrypted) Information

The information in this segment of the ETM is digitally signed, and trust in the signature can be verified using the certificate chain in the Signature portion. This segment is not encrypted, so any entity that has access to the message can extract this information. The information in this segment is shown in Figure 23 below.

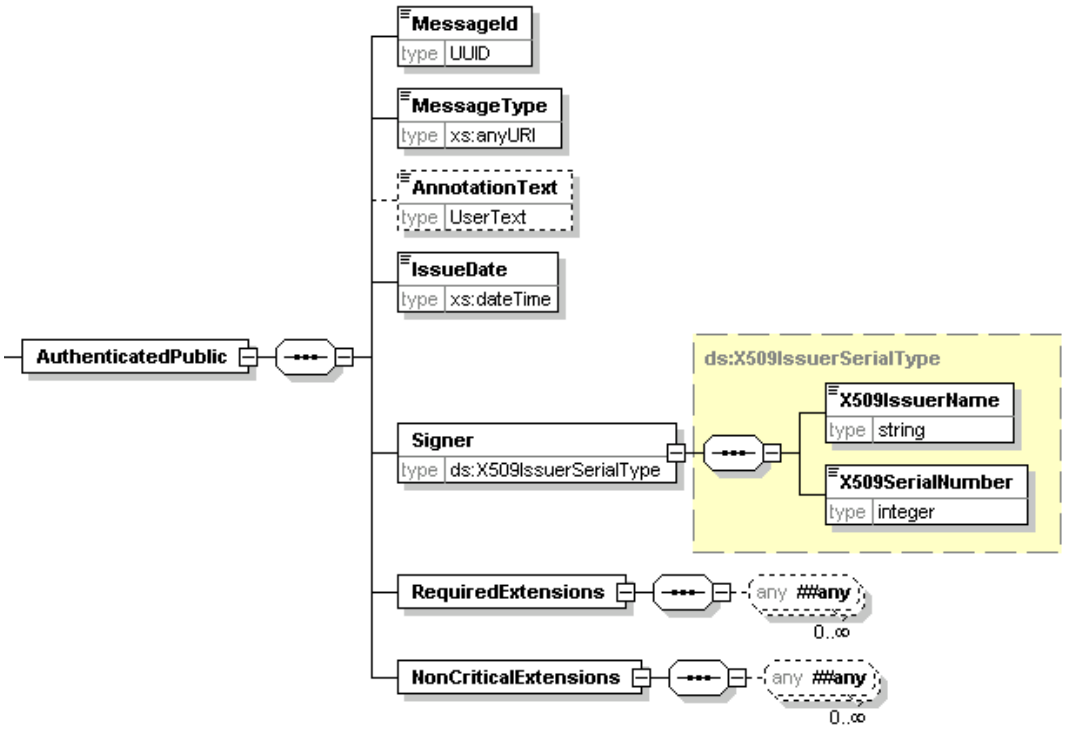

Figure 23: Authenticated and Public Portion of Extra-Theater Messages

9.8.2.2.1. MessageId

The MessageId field shall be a globally unique identifier for a given ETM that is chosen by the creator of the message.

9.8.2.2.2. MessageType

The MessageType field identifies the specific version and type of the message (e.g., this is a KDM message). The recipient shall recognize that the ETM is of a known type.

9.8.2.2.3. AnnotationText

The optional AnnotationText field contains a human-readable description of the message. It is not used in any security-related process.

9.8.2.2.4. IssueDate

The IssueDate field indicates the time and date when the message was issued. The signer's certificate chain shall be valid at this time. It is a UTC timestamp.

9.8.2.2.5. Signer

The Signer field identifies the certificate that should be used to validate the signature on this message.

9.8.2.2.6. RequiredExtentions

The RequiredExtentions field contains zero or more opaque elements that are required for the proper interpretation and usage of a specific ETM. It provides a place for adding information that can be visible to all entities that receive this message.

9.8.2.2.7. NonCriticalExtensions

The NonCriticalExtensions field contains zero or more opaque elements that are not required for the proper interpretation and usage of a specific ETM. It provides a place for information that is outside the scope of normative interoperability specifications to be carried along in the ETM.

9.8.2.3. Authenticated and Private (Encrypted) Information

This segment of the ETM is digitally signed, and trust in the signature can be verified using the certificate chain in the Signature portion. This portion is encrypted for the recipients before being transmitted. Only an entity that knows the private key of one of the recipients can decrypt this portion of the message.

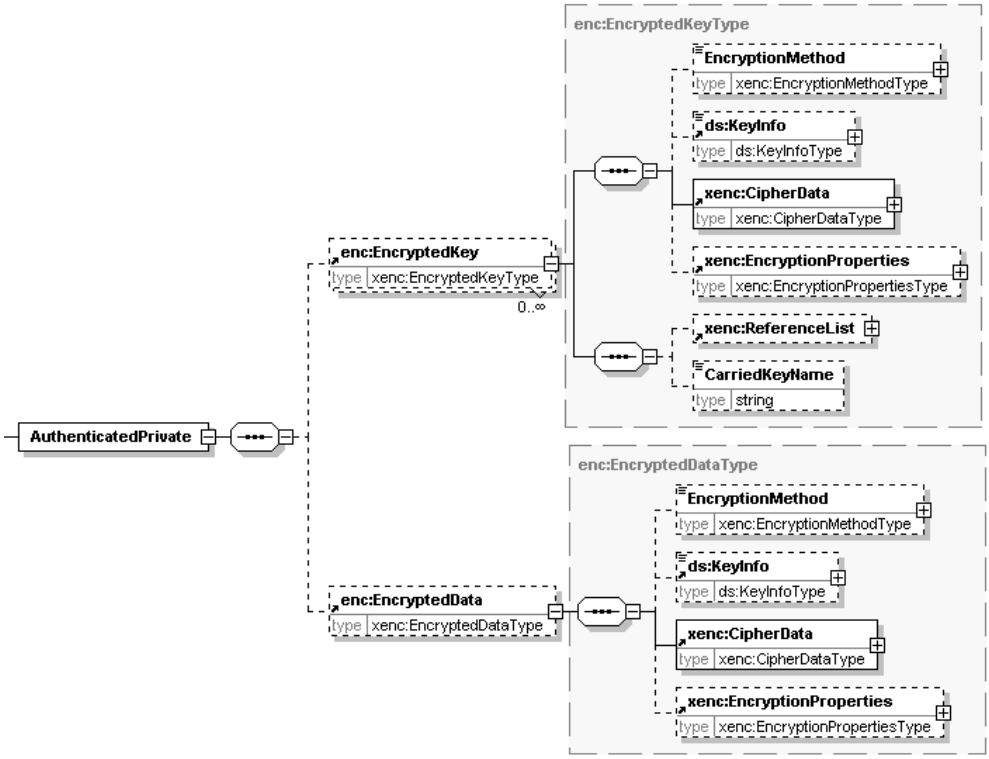

Figure 24: Authenticated and Private Portion of Extra-Theater Messages

This segment contains zero or more EncryptedKey fields and at most one EncryptedData field. The information in the segment is shown in Figure 24 above.

9.8.2.3.1. EncryptedKey

This optional element contains information encrypted with a public key algorithm, specifically RSA, along with all the parameters and information needed to extract that information.

9.8.2.3.1.1. EncryptionMethod

This field of EncryptedKey specifies the encryption algorithm and parameters. All Extra-Theater Message(s) **(**ETM) shall use the mode for RSA called Optimal Asymmetric Encryption Padding (OAEP).

9.8.2.3.1.2. KeyInfo

This field identifies the RSA public key used to encrypt the EncryptedKey CipherData by naming the certificate that contains the public key that was used to create the ciphertext. The matching RSA private key is needed to decrypt the key. The recipient's certificate shall be named by its IssuerName and Issuer Serial Number.

9.8.2.3.1.3. CipherData

This field is an RSA encrypted block of data that can be decrypted using the private key indirectly specified in the KeyInfo field.

9.8.2.3.1.4. EncryptionProperties

This field shall not be present.

9.8.2.3.1.5. ReferenceList

This field shall not be present.

9.8.2.3.1.6. CarriedKeyName

This field is required when the EncryptedData field is included in the Extra-Theater Message (ETM), otherwise it shall be absent. This field is used to assign an identifying name to the AES key carried in the EncryptedKey element. The EncryptedData element, if present, has a KeyName field as part of the KeyInfo element that matches this field.

9.8.2.3.2. EncryptedData

This section describes the use of the optional EncryptedData element in Extra-Theater Message (ETM). A diagram of this element is shown below in Figure 25. This field shall not be present if there are no EncryptedKey fields.

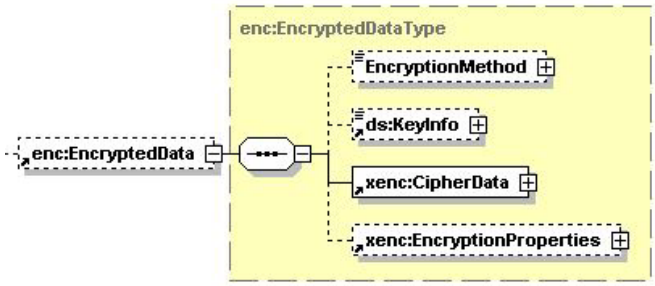

Figure 25: EncryptedData in Extra-Theater Message (ETM)

The EncryptionMethod shall specify that the data be encrypted using the AES cipher with a 128-bit key operating in CBC mode.

The KeyName field of the KeyInfo element specifies the name of the AES key needed to decrypt the ciphertext. This name shall match the CarriedKeyName value in all of the EncryptedKey elements. The EncryptionProperties shall not be present. The CipherData shall be present.

9.8.2.4. Signature Information

This segment of the Extra-Theater Message (ETM) provides authentication for the other sections using the primitives from the XML Digital Signature standard. *Digital certificates and associated data shall use the X.509 certificate form specified for Digital Cinema in the Digital Cinema Digital Certificate (specified in Section 9.8.1 Digital Certificates). Figure 26 below illustrates the Signature segment.*

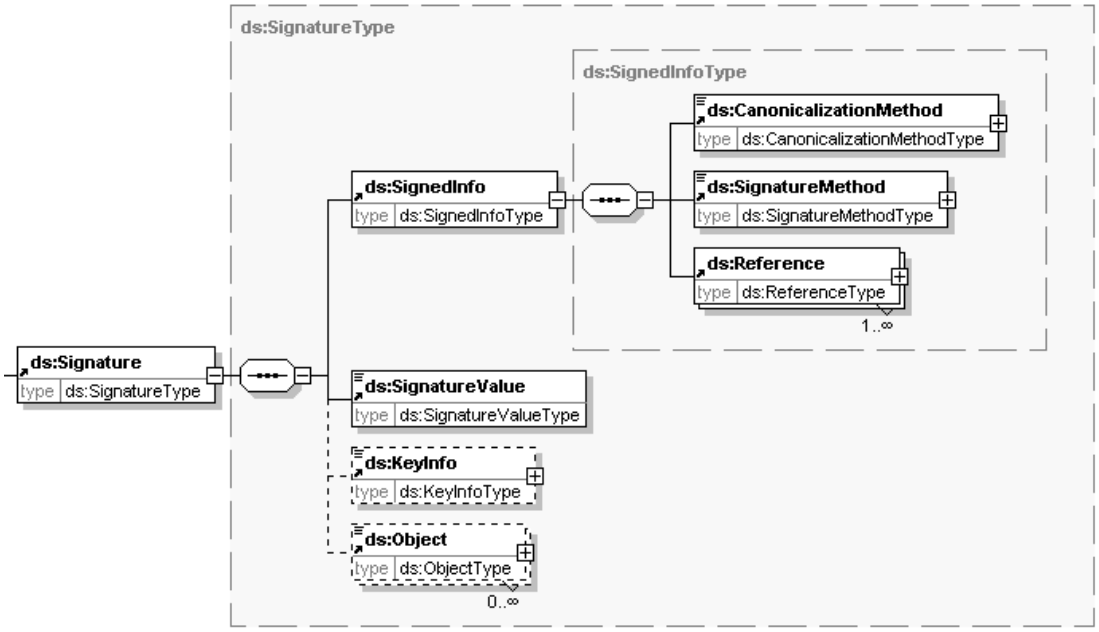

Figure 26: Signature Section of Extra-Theater Message (ETM)

The Signature primitive that is defined in the XML Digital Signature standard shall be used as specified in this section.

9.8.2.4.1. XML Embedding

Each signed data structure to be embedded should have a native or original form in which it is a complete document. The contents of the document header (prolog) shall be completely specified by the controlling standards document. During the embedding process only the prolog is stripped and the remainder of the document is embedded intact.

9.8.2.4.2. SignedInfo

The XML Digital Signature standard defines a two-step process for checking signatures. First the actual hash values of different portions of the Extra-Theater Message (ETM) are computed and compared against the expected values that appear in the Reference elements of the SignedInfo. Next, the SignedInfo element is canonicalized and then hashed and finally verified against the SignatureValue.

For all Extra-Theater Message(s) (ETM), the SignedInfo shall contain at least two Reference fields. The first is the hash of the AuthenticatedPublic element and the second is the hash of the AuthenticatedPrivate element. There may be a third Reference field that specifies the hash value for the plaintext decrypted from the EncryptedData element.

9.8.2.4.3. SignatureValue

The SignatureValue element shall be the output of the operation that is used to generate the signature.

9.8.2.4.4. KeyInfo Certificate Chain

The signer's certificate shall be identified by its IssuerName and SerialNumber in the Signer element in the AuthenticatedPublic segment of the message. It shall not be similarly (specifically) identified in this KeyInfo element.

The entire certificate chain of the signer, including the root certificate, shall be carried in the KeyInfo element as a sequence of X509Data elements. Each of the X509Data elements shall correspond to one certificate in the chain, and contain one X509IssuerSerial element and one X509 Certificate element.

9.8.2.4.5. Object Information

The Object field of the Signature element shall not be present.

9.8.3. Key Delivery Message (KDM)

The KDM provides the mechanism by which content keys, key usage permission time window (parameters) and optional TDL are exchanged between an issuer and a recipient (see Figure 27 below). *The model supports a tiered process, whereby a Rights Owner may provide* Key Delivery Message(s) *(KDMs) to a Distributor, which subsequently creates* Key Delivery Message(s) *(KDMs) for multiple Exhibitors.* Individual Key Delivery Message(s) (KDMs) are essentially entitlement messages that provide permissions and necessary information for a particular theater to play the content during the specified time window.

The TDL is used by the auditorium Security Managers (SMs) to confirm that the equipment it enables within its equipment suite is trusted and approved for use with the KDM information.

A single KDM *may be created with multiple content keys, and such keys may apply to image, audio or other content types.* A key identifier field is provided in the KDM such that the SM can direct content keys to the appropriate Media Block. The KDM is addressed and cryptographically bound to a single intended recipient, the so-called targeted SM.

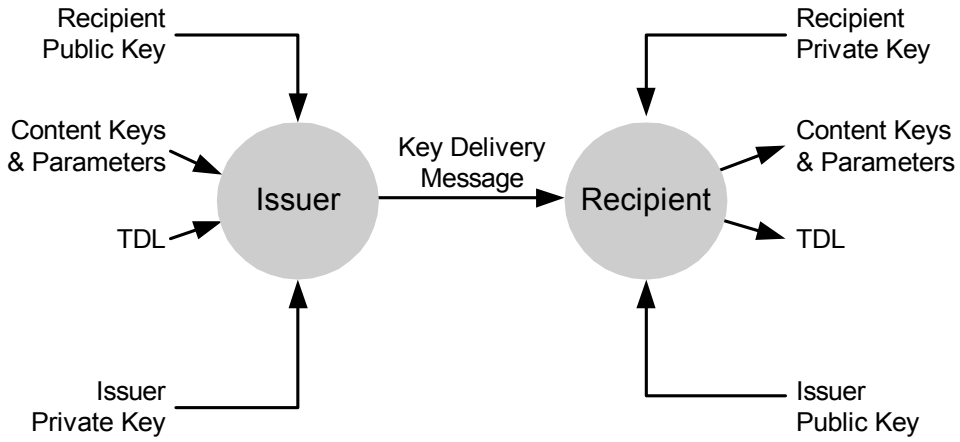

Figure 27: Key Delivery Message (KDM) Information Flow

Access to the full information payload of the KDM requires knowledge of the targeted recipient's private key. Having this key, the legitimate recipient may unlock and validate both encrypted and plain text information contents carried. As is explained further in the appropriate sections of this document, the structure of the KDM has been designed to allow this without the recipient having stores of root certificates. *To preserve the intended security, full KDM information access may only take place within a secure environment (e.g., within a Digital Cinema Security Manager).* Key Delivery Message(s) (KDMs) may be authenticated by insecure devices, if such devices have copies of the root certificate of the entity that created and signed the KDM.

To help meet stringent physical security requirements for protecting content keys, the KDM design details enable (but do not require) an implementation that is on a single chip that can: 1) perform RSA private and public key and SHA-256 hashing operations, 2) hold at least 4 kilobytes of data in physically secure memory, and 3) create and manage (store) a set of content keys, perhaps protected by a chip-specific key-encrypting-key (KEK). The security goal of such chips is to ensure that plaintext keys never pass over the wires in a circuit board, and thus are much harder for an attacker to intercept.

The KDM message is a particular instance of the generic XML security wrapper defined by the Digital Cinema Generic Extra-Theater Message (ETM) format and uses digital certificates defined by the Digital Cinema Digital Certificate specification. *The KDM specification defines the characteristics that are specific to the KDM, and should be followed in combination with the Extra-Theater Message (ETM) specifications (see Section 9.8.2 Generic Extra-Theater Message (ETM)), which in turn reference the Digital Certificate specification (see Section 9.8.1 Digital Certificates).* The following requirements address only the extensions to the ETM. Data fields not specifically addressed below are defined normatively in ETM Section 9.8.2 Generic Extra-Theater Message (ETM).

9.8.3.1. Overview of the Key Delivery Message (KDM)

A KDM is an ETM instance which has in the RequiredExtensions element a child element named KDMRequiredExtensions (defined below), and which also makes use of the AuthenticatedPrivate element of the ETM to store content encryption keys.

The KDMRequiredExtensions element contains information that must be visible without decryption in order to properly handle the KDM within Digital Cinema systems. The information made available in this element includes a list of the Content Key Ids (but not the value of those keys) in the message.

The AuthenticatedPrivate portion contains a collection of content decryption keys each encrypted in an EncryptedKey element. These RSA encrypted elements also include the KeyId and validity dates for each content key. The optional EncryptedData element, defined in the ETM, is not used by the KDM. A KDM has a single recipient, so all the EncryptedKey elements can be decrypted with the same RSA private key.

The Signature element defined in the ETM carries the signer's certificate chain and protects the integrity and authenticity of the AuthenticatedPublic portion and the AuthenticatedPrivate portion (both plaintext and ciphertext versions).

9.8.3.2. Authenticated and Unencrypted Information

The KDM extends the ETM by including the KDMRequiredExtensions element (see Figure 28 below) in its RequiredExtensions element. The information in the AuthenticatedPublic element of the ETM (and thus, KDM) is digitally signed, and trust in the signature can be verified using the certificate chain in the Signature portion. This element is not encrypted, so any entity that has access to the message can extract this information. The word public that appears in the XML label for this element means that any entity that receives the message can view this portion.

The certificate chain is part of the information that is protected by the digital signature, which reduces the risk of an attacker who is able to create a small number of legitimate certificates (e.g., through social engineering). The following sections describe the elements in this portion.

9.8.3.2.1. MessageType

In a KDM, this field shall contain the following URL:

`http://www.smpte-ra.org/414/2005/KDM#kdm-key-type`

9.8.3.2.2. RequiredExtentions

The RequiredExtentions field of the KDM shall contain exactly one KDMRequiredExtensions element. The form of element is shown in Figure 28 below.

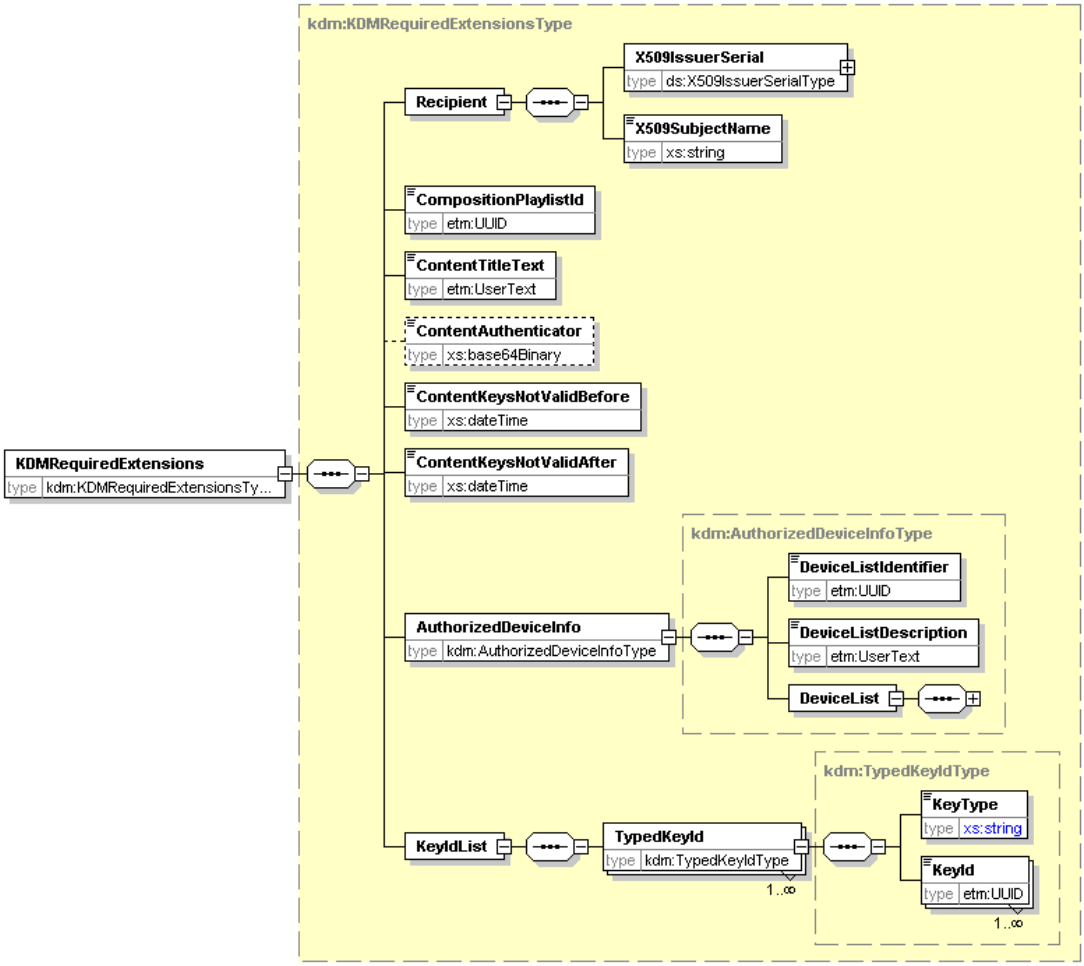

Figure 28: KDMRequiredExtensions element

The KDMRequiredExtensions element shall have the following child elements:

9.8.3.2.2.1. Recipient

The Recipient field identifies the intended certificate/subject of this KDM. The public key identified in this certificate is used to encrypt the keys found in the AuthenticatedPrivate portion of the KDM message. To aid in routing of Key Delivery Message(s) (KDMs), the X.509 SubjectName that is found in the certificate shall also be placed in the Recipient element.

9.8.3.2.2.2. CompositionPlaylistId

This field contains a machine-readable identifier for the Rights Owner's content. It matches an identifier in the bulk content packaging file(s) and in the Composition Playlist (CPL). This is an informational field that is a copy of the definitive value that appears in the RSA protected EncryptedKey structure. The CompositionPlaylistId values should be globally unique (i.e., have at least 128 bits of entropy (unpredictability)).

9.8.3.2.2.3. ContentTitleText

The ContentTitleText parameter contains a human-readable title for the composition. The optional language attribute is an ISO 3166 language code and indicates the language used.

9.8.3.2.2.4. ContentAuthenticator

This field, if present, contains a certificate thumbprint (see Section 9.8.1.4 Certificate and Public Key Thumbprint) that supports authentication of the content as an authorized version (e.g., through a Composition Playlist). This field may be absent at the discretion of the KDM creator, but it is part of the RequiredExtentions elements because compliant receiving equipment is required to understand and process it when present.

Notes:

1. *If this field is present, then it is intended that the recipient crosscheck the certificate chain for the signer of the Composition Playlist (CPL) against this value.*
2. *This field facilitates the business requirement of allowing an Exhibitor to show content produced by a wide range of studios without needing to know the root certificates for all studios.*
3. *Nothing precludes an Exhibitor from knowing the root certificates of specific studios and using those certificates as part of validating Composition Play List (CPL).*

9.8.3.2.2.5. AuthorizedDeviceInfo

This field is intended to support authorization of devices which process keys delivered by the KDM. If the AuthorizedDeviceInfo item is absent from a KDM, the intention is that no devices external to the recipient's Media Block are to utilize the secrets of the KDM.

This item contains three elements described below.

- **DeviceListIdentifier** – Contains a value uniquely identifying a list of trusted equipment. It is a required member of the AuthorizedDeviceInfo structure. This field is an aid to the management of device lists and the tracking of updates to them.
- **DeviceListDescription (optional)** – Contains a human-readable description of the device list.
- **DeviceList** – Contains a set of certificate thumbprints (see Section 9.8.1.4 Certificate and Public Key Thumbprint). Each entry represents a specific device that is authorized for use in connection with the keys in this KDM.

9.8.3.2.2.6. ContentKeysNotValidBefore

This field specifies the UTC time before which the content keys contained in this KDM are not valid. This is an informational field that is a copy of the definitive value that appears in the RSA protected EncryptedKey structure. *The time windows of all content keys shall be the same as those in the RSA protected blocks.*

9.8.3.2.2.7. ContentKeysNotValidAfter

This field specifies the UTC time after which the content key contained in this KDM are not valid. This is an informational field that is a copy of the definitive value that appears in the RSA protected EncryptedKey structure. *The time windows of all content keys shall be the same as those in the RSA protected blocks*.

9.8.3.2.2.8. KeyIdList

This field contains an unordered list of one or more TypedKeyId elements, which are defined below. This is an informational field that is a copy of the definitive values that appear in the RSA protected EncryptedKey structures.

- **KeyId** – Parameter that uniquely identifies the content decryption key. All keys are for use with the same content (identified by the CompositionPlaylistId field). It is represented by a UUID. To avoid operational problems, the KeyId values shall be globally unique (i.e., have at least 128 bits of entropy (unpredictability)).
- **TypedKeyId** – A compound element consisting of a KeyType field and a KeyId. The KeyType distinguishes keys targeted to different types of devices (e.g., image media decryptor, audio media decryptor).

  Each byte of the KeyType field represents one of the limited set of characters permitted for role identifiers in the CommonName field in the DC-Cert. If an implementation does not wish to use key types, the Character String NULL shall be used to show this.

9.8.3.2.3. NonCriticalExtensions

This field is defined in Section 9.8.2.2.7 NonCriticalExtensions. It shall be an empty element in the KDM.

9.8.3.3. Authenticated and Encrypted Information

This portion of the KDM is authenticated by the signature, and encrypted for the recipient before being transmitted. Anyone can verify the signature on the KDM and validate the certificate chain to decide whether the message has been modified and whether it was created by a trusted entity. However, only an entity that knows the private key of the recipient can decrypt this portion of the message. This is shown in Figure 29 below.

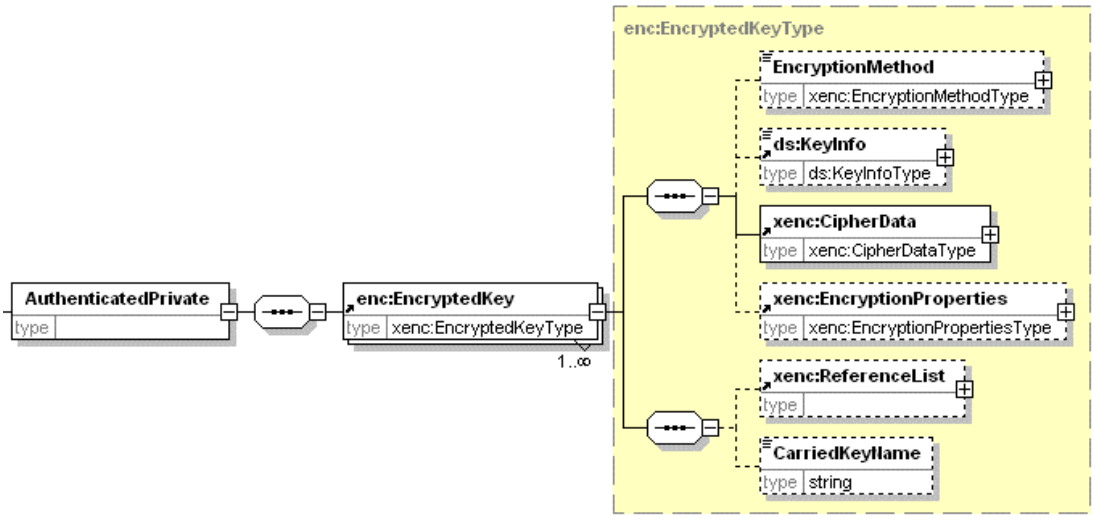

Figure 29: Authenticate and Private Portion of KDM

For the KDM, the EncryptedData element shall be omitted and each EncryptedKey element carries one content decryption key and its associated information. The KDM shall only have a single recipient.

9.8.3.3.1. EncryptedKey

This element contains information encrypted with the RSA public key algorithm, along with all the parameters and information needed to extract that information. Child elements of EncryptedKey not listed below shall be unchanged from their ETM definition (see Section 9.8.2 Generic Extra-Theater Message (ETM)).

9.8.3.3.1.1. KeyInfo

This field is optional for Key Delivery Message(s) (KDMs), since the Recipient's certificate is identified in the Recipient element of the RequiredExtensions element of the KDM. It identifies the certificate that contains the public key that was used for the RSA encryption. If this element is supplied, the certificate identified by the KeyInfo element shall be the same for all EncryptedKey elements in the KDM.

9.8.3.3.1.2. CipherData

The CipherData field is generally defined in the ETM section. For the KDM message, the CipherData field carries a specially formatted plaintext payload. The plaintext consists of the following fixed length fields concatenated together with the most significant byte first starting with the first item in Table 44 below.

Length	Field Description
16	Structure ID. A 128-bit unique identifier for this structure. Its binary value corresponds to the XML value "urn:uuid:01010000-9783-af89-bc5a-e7e9123abe52", which includes the 32 character hexadecimal representation of the Structure ID[35] value (MSB first).
20	Thumbprint of signer's certificate[36].
16	CompositionPlaylistId[37], a UUID in binary form.
2	KeyType, a byte string of length four bytes.
16	KeyId, a UUID in binary form.
25	Not Valid Before as UTC date-time such as "2004-05-01T13:20:00-05:00"
25	Not Valid After as UTC date-time such as "2004-06-30T13:20:00-05:00"
16	AES Content Decryption or Forensic Marking Key[38]
136	**Total**

Table 44: CipherData Fields

9.8.3.3.2. EncryptedData

This field shall not be present for KDM messages.

[35] The SM shall check the Structure ID. If it is not correct, the KDM shall be rejected.
[36] The SM shall check that the thumbprint of the signer's certificate matches the signer of the KDM. If it is not correct, the KDM shall be rejected.
[37] The SM should check that the CompositionPlaylistId in the RSA block matches the CompositionPlaylistId in the other portions of the KDM. The information in the RSA block is considered authoritative. The recipient should reject the KDM if the CompositionPlaylistId does not match in all places that it occurs in the KDM.
[38] The SM shall execute the "no FM mark" state requirements upon receipt of the default FM key per Section 9.4.6.1 Forensic Marking.

9.8.3.4. Signature Information

Since the EncryptedData element is not used in the KDM, the Signature element shall only contain two Reference fields, one for the AuthenticatedPublic and one for the AuthenticatedPrivate (covering the ciphertext form of the EncryptedKey elements).

THIS PAGE LEFT BLANK INTENTIONALLY

10. GLOSSARY OF TERMS

AES	Acronym for Advanced Encryption Standard
AES	Acronym for Audio Engineering Society
AES3	Audio Engineering Society - Recommended Practice for Digital Audio Engineering Serial transmission format for two-channel linearly represented digital audio data
ANSI	Acronym for American National Standards Institute
Answer Print	A color-corrected film print made directly from the cut film negative. It is also the culmination of the creative color timing process, where final creative approval is granted before the film is duplicated for release
API	Acronym for Application Programming Interface
BER	Acronym for Basic Encoding Rules
Broadcast Wave	Digital Audio file format developed and standardized by the EBU (European Broadcast Union, a standardization organization)
Burned-In	Where visual data that is normally supplemental to a motion picture is irrevocably added to the motion-picture image by compositing the data with the underlying image
Captions	Text that is a representation, often in the same language, of dialog and audio events occurring during scenes of a motion picture. (Generally associated with a dialog and audio event translation for the deaf and hard of hearing.)
CBC	Acronym for Cipher Block Chaining mode
CBR	Acronym for Constant Bit Rate for image compression
Central Storage	A central location where the packaged Digital Cinema content is stored for a multiple screen installation
Chunk	A section of a PNG file. Each chunk has a type indicated by its chunk type name. Most types of chunks also include some data. The format and meaning of the data within the chunk are determined by the name.
CIE	Acronym for International Commission on Illumination (Commission Internationale de l'Eclairage)
Closed	Referring to visual data that is supplemental to a motion picture being displayed off-screen
COC	Acronym for Coding style Component – see JPEG 2000 specification [ISO/IEC 15444-1]
COD	Acronym for Coding style Default – see JPEG 2000 specification [ISO/IEC 15444-1]
Composition	A motion picture, or a trailer, or an advertisement, etc. Composition consists of a metadata Composition Playlist along with the essence and other metadata track files that define the work.

Container Level	Metadata that indicates the size of the image/structure container and the frame rate of the images – this does not indicate the image structure or resolution
CPL	Acronym for Composition Playlist, the definitive Playlist for specifying how a Composition is played and what track files are required
CPRL	Acronym for Component Position Resolution Layer – see JPEG 2000 specification [ISO/IEC 15444-1]
CSP	Acronym for Critical Security Parameter
D/HOH	Acronym for Deaf and Hard Of Hearing
DCDM	Acronym for Digital Cinema Distribution Master. A master set of files that have not been compressed, encrypted, or packaged for Digital Cinema distribution. The DCDM contains essentially all of the elements required to provide a Digital Cinema (DC) presentation.
DCDM*	Acronym for Digital Cinema Distribution Master*. When the DCP is unpackaged, decrypted and decompressed, it is refered to as the DCDM*. The DCDM* is visually indistinguishable from the original DCDM.
DCI	Acronym for Digital Cinema Initiatives, LLC
DCP	Acronym for a Digital Cinema Package, the set of files that are the result of the encoding, encryption and packaging process
DER	Acronym for Distinguished Encoding Rules
DES	Acronym for Data Encryption Standard. DES was adopted as a federal standard in 1976 [FIPS (46-3)] and [ANSI standard X9.32]
Distribution Package	The collection of files delivered by the distributor to the exhibitor. A Distribution Package may contain pieces of a Composition or several compositions, a complete Composition, replacement/update files, etc.
DM	Acronym for Descriptive Metadata
DRM	Acronym for Digital Rights Management
DSM	Acronym for Digital Source Master, a digital master created in post-production from which different versions and duplication masters may be created.
e.g.	Abbrevation for the Latin phrase exempli gratia, meaning “for example”
End Credits	A credit sequence generally shown at the end of a motion picture
Essence	Image, audio, subtitles, or any content that is presented to a human being in a presentation
ETM	Acronym for Extra-Theater Message
Event Playlist	A playlist of Compositions, describing an assembly of Compositions in sequence. An Event Playlist is typically created by a content distributor and transferred to exhibition.
Fingerprint	Dynamic playback or distribution watermark
FIPS	Acronym for Federal Information Processing Standards
FM	Acronym for Forensic Marking

Forensic Marking	Data embedded in essence to provide forensic tracking information in the event of content theft. Such marking can be visible or non-visible, audible or non-audible.
FPS	Acronym for Frames Per Second
Generic Forensic Mark Inserter	In this architecture, metadata is first created at authoring that contains: 1) locations within the title where forensic marking may be inserted, and 2) commands that set the type of steganographic marking to be used to encode the actual forensic information. In the theater, at the time of playback, the metadata is used to instruct the inserter in the Media Block how, where, and when the required information will be hidden within the sound and/or picture.
GPIO	Acronym for General Purpose Input or Output
GUI	Acronym for Graphical User Interface
HMAC	Acronym for Hashing Message Authentication Codes
HVS	Acronym for the Human Visual System
Hz	Abbreviation for Hertz, a unit of frequency expressed in cycles per second
IANA	Acronym for Internet Assigned Numbers Authority
i.e.	Abbreviation for the Latin phrase id est, meaning “that is”
ICT	Acronym for Irreversible Color Transformation – see JPEG 2000 specification [ISO/IEC 15444-1]
IEC	Acronym for Internation Electrotechnical Commission
IMB	Acronym for Image Media Block
IP	Acronym for Intellectual Property
ISAN	Acronym for International Standards Audiovisual Number
ISO	Acronym for International Organization for Standardization
ITM	Acronym for Intra-Theater Message
JPEG	Acronym for Joint Photographic Experts Group, the international body that developed the JPEG 2000 standard
KDM	Acronym for Key Delivery Message
KEK	Acronym for Key-Encrypting Key
Key	Electronic data used to allow data encryption and decryption
Key Epoch	The period of time during which a given decryption key is valid. The key epoch defines a minimum practical time period for use of encrypted track files.
kHz	Acronym for kilo Hertz, one thousand cycles per second, a measure of frequency
KLV	Acronym for Key Length Value – used by the MXF to parse binary data
LD	Acronym for Link Decryption
LDB	Acronym for Link Decryption Block

LE	Acronym for Link Encryption
LED	Acronym for Light Emitting Diode
Local Storage	A storage device that is associated with an individual playback device
Localizations	Text on screen representing either non-source language dialog or information pertinent to the story such as time and place. This is specifically the text that is absent in text-less masters. This text is localized or translated for various markets either through subtitles or entire image replacement.
LTC	Acronym for Linear Time Code
Main Titles	A credit sequence generally shown near the beginning of a motion picture
MB	Acronym for Media Block
MD	Acronym for Media Decryptor, the device located in the Media Block that decrypts the compressed content.
ME	Acronym for Media Encryptor
Metadata	Data about data or data describing other data. Information that is considered ancillary to or otherwise directly complementary to essence. Information that is useful or of value when associated with the essence being provided.
MTBF	Acronym for Mean Time Between Failure
MXF	Acronym for Material eXchange Format
NIST	Acronym for National Institute of Standards and Technology
NSA	Acronym for National Security Agency
NTSC	Acronym for National Television System Committee, which developed the NTSC television broadcasting standard
OAEP	Acronym for Optimal Asymmetric Encryption Padding
Open	Referring to visual data that is supplemental to a motion picture being displayed on-screen
Operational Pattern	An MXF construct to define file structures
Packing List	A list describing the files and providing a means for authentication of the files as delivered in a package
PAL	Acronym for Phase Alternation by Line, a television broadcasting standard.
Perceptual Coding	Exploiting limitations in the HVS for data compression
Playlist	Conceptually, the format and structure of the various lists used to define the playback of content in Digital Cinema
PNG	Acronym for Portable Network Graphics, an extensible file format for the lossless, portable, well-compressed storage of raster images defined by the PNG Development Group.
POC	Acronym for Progression Order Change – see JPEG 2000 specification [ISO/IEC 15444-1]
PPM	Acronym for Packed Packet headers, Main header – see JPEG 2000 specification [ISO/IEC 15444-1]

PPT	Acronym for Packed Packet headers, Title-part header – see JPEG 2000 specification [ISO/IEC 15444-1]
QCC	Acronym for Quantization Component – see JPEG 2000 specification [ISO/IEC 15444-1]
QCD	Acronym for Quantization Default – see JPEG 2000 specification [ISO/IEC 15444-1]
RAID	Acronym for Redundant Array of Inexpensive Disks
RAND	Acronym reasonable and nondiscriminatory
Reel	A conceptual period of time having a specific duration. A Reel is associated with track files. From a temporal view, the files making up a Reel are in parallel and are to be synchronized in their playback.
Renewable	A software component is renewable if it can be remotely, smoothly and possibly automatically upgraded or replaced without significantly disturbing system operations. A system shutdown and normal restart is acceptable, provided that after the restart, the system can be operated as before.
Replaceable	A component is said to be replaceable if it can be upgraded or replaced without significantly disturbing system operations. A system shutdown and restart is acceptable, provided that after the replacement, the system can be operated as before.
RGN	Acronym for Region of Interest – see JPEG 2000 specification [ISO/IEC 15444-1]
RO	Acronym for Rights Owner
ROM	Acronym for Read Only Memory
RRP	Acronym for Request Response Pairs
SE	Acronym for Security Entity, not to be confused with secure entity
SECAM	Acronym for System Electronique Couleur Avec Memoire, a television broadcasting standard
Security Manager	The controlling device of the security system in either the encoding, distribution or the theater playback process
SHA1	Acronym for Secure Hashing Algorithm 1
Show	The presentation that the audience sees and hears in the theater auditorium
Show Playlist	A Playlist of Composition Playlists and Event Playlists, describing a sequence that occurs at a particular screen. A Show Playlist is typically created by exhibition and transferred to the equipment controlling a particular screen.
SM	Acronym for Security Manager
SMD	Acronym for Subtitle Media Block
SMPTE	Acronym for Society of Motion Picture and Television Engineers
SMS	Acronym for Screen Management System
SNMP/UDP/IP	Acronym for Simple Network Management Protocol Over User Datagram Protocol Over Internet Protocol

SPB	Acronym for Secure Processing Block
SPL	Acronym for Show Playlist
SPL	Acronym for Sound Pressure Level
Subpicture	A multiple-image file format for the transport of visual data supplemental to a motion picture that is intended only for graphic overlay with the main image output of a digital projector
Subtitle	Text that is a representation, in a different language, of dialog occurring during scenes of a motion picture. Generally associated with dialog translation for localization of a motion picture in a particular territory.
TCP/IP	Acronym for Transmission Control Protocol / Internet Protocol
TDES or 3DES	Acronym for Triple Data Encryption Standard. TDES or 3DES was adopted as a federal standard in 1998 [FIPS (46-3)] and [ANSI standard X9.32]
TDL	Acronym for Trusted Device List
Timed Text	Render text data onto a graphics overlay with the main image output of a digital projector
TLM	Tile-part Length, Main Header– see JPEG 2000 Specification [ISO/IEC 15444-1]
TLS	Acronym for Transport Layer Security
TMS	Acronym for Theater Management System
Track File	The smallest element of a package that can be managed or replaced as a distinct asset. A track file may contain essence and/or metadata, and its duration matches an associated Reel.
UDP	Acronym for User Datagram Protocol
UL	Acronym for Universal Lable used in MXF
Unicode™	The Universal Multiple-Octet Coded Character set, the [ISO/IEC 10646:2003] standard that defines a single code for representation, interchange, processing, storage, entry and presentation of the written form of the world's major languages
urn	Acronym for uniform resource name
USB	Acronym for Universal Serial Bus, standardized serial communications connection found on computers
UTC	Acronym for Universal Coordinated Time
UUID	Acronym for Universal Unique IDentifier
Visually Lossless	An image compression method is considered visually lossless when the processed image is indistinguishable from the unprocessed image under normal theatrical viewing conditions.
VPN	Acronym for Virtual Private Network.
VBR	Acronym for Variable Bit Rate
W3C	Acronym for The World Wide Web Consortium, the organization responsible for the development of Internet protocols

WWV	Callsign of NIST's shortwave radio station in Fort Collins, Colorado. WWV's main function is the continuous dissemination of official United States government time signals
XML	Acronym for eXtensible Markup Language
X'Y'Z'	Tristimulus values defined by CIE in 1931 to represent colors. Prime indicates gamma corrected coordinates.

THIS PAGE LEFT BLANK INTENTIONALLY