

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
***Intertrust Techs. Corp. v. Cinemark Holdings, Inc.* (Case No. 2:19-cv-00266-JRG)**
U.S. PATENT NO. 6,785,815: CLAIMS 42, 43¹

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
[815.42] A method for managing at least one use of a file of electronic data, the method including: ⁴	<p>Cinemark has committed and continues to commit acts of infringement of claim 42 under 35 U.S.C. § 271 through its use of DCI-compliant Digital Cinema systems to show movies and other DCI-compliant content.</p> <p>To the extent that the Court determines that the preamble of this claim is limiting, Cinemark performs the claimed method for managing at least one use of a file of electronic data. <i>See</i> [815.42]-[815.42e], <i>infra</i>.</p> <p>For example, Cinemark performs the claimed method through the use of a DCI-compliant Digital Cinema system to show DCI-compliant content. Each DCI-compliant Digital Cinema system includes one or more Media Blocks (e.g., Image Media Block (IMB), and optionally one or more Outboard Media Blocks (OMB)) and, depending on the configuration, one or more Secure Processing Blocks that manage at least one use of Track Files (one non-limiting example of "a file of electronic data") in connection with showing DCI-compliant content.</p> <p><i>See</i> DCI Digital Cinema System Specification v. 1.2 with Errata as of 30 August 2012 Incorporated ("DCI Specification"), 15-16 (discussing general objectives of Digital Cinema system).⁵⁶</p>

¹ The infringement contentions provided herein are based on information obtained to date and may not be exhaustive. Intertrust's investigation of Cinemark's infringement is ongoing. Intertrust reserves the right to supplement and/or amend these disclosures, including on the basis of discovery obtained from Cinemark and from third-parties during the course of this litigation.

² All infringement contentions set forth herein for any independent patent claims are hereby incorporated by reference into the infringement contentions alleged for any dependent patent claims that depend on such independent claims, as if fully set forth therein.

³ The citations to excerpts of documents herein are examples provided solely for illustrative purposes. The citations are not intended to be exhaustive.

⁴ Intertrust's inclusion of any claim preamble in this claim chart should not be interpreted as an admission that the preamble is limiting. Intertrust reserves the right to take the position that the claim preambles are limiting or not limiting on a claim-by-claim basis.

⁵ DCI Specification was produced at INTERTRUST00083760 – INTERTRUST00083914.

⁶ The infringement contentions herein also apply to DCI Digital Cinema System Specification v. 1.3, produced at INTERTRUST00083915 – INTERTRUST00084069.

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>9.4.2.3. Media Blocks (MBs)</p> <p>The term Media Block⁴¹ (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 contains a Security Manager (SM) and performs essence decryption, i.e., it contains at least one MD. <i>Other SE functions may also be present within a MB SPB, as described below:</i></p> <ul style="list-style-type: none">• Image Media Block (IMB) – <i>The Image Media Block (IMB) is a type 1 Secure Processing Block (SPB) that shall contain a Security Manager (SM), Image, Audio and Subtitle Media Decryptors (MD), image decoder, Image and Audio Forensic Marking (FM) and optionally Link Encryptor (LE) functions. It is encouraged for the IMB to optionally contain the content essence processing to perform the functions of the Outboard Media Block (OMB). The IMB SM is responsible for security for a single Equipment Suite, and it authenticates other SPBs that comprise the suite. Other such SPBs are referred to as remote SPBs.</i>• Outboard Media Block (OMB) – <i>The OMB is a type 1 SPB that shall contain a Security Manager (SM) and one or more Media Decryptors (MD) and associated Forensic Markers (FM) to process (only) those content essence types explicitly designated in Section 9.4.3.6.4 “Outboard Media Block (OMB)”.</i> <p>Erratum #9, Chapter 9 Replacement to DCSS Version 1.2 with Errata as of 30 August 2012 Incorporated (“Chapter 9 Replacement”)⁷, 91; <i>see also id.</i>, 82, 87.</p>

⁷ Chapter 9 Replacement was produced at INTERTRUST00084074 – INTERTRUST00084141.

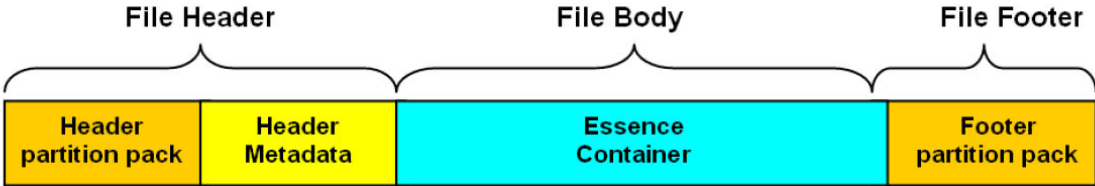
Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>The Media Block can be implemented in a server configuration, as shown in Figure 11. 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. <i>In this configuration, Link Encryption is required to protect the uncompressed content.</i></p> <p style="text-align: center;">Figure 11: Media Block Server Configuration⁴</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>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 12.</p> <p>Figure 12: Media Block in Projector Configuration⁵</p> <p>DCI Specification, 64.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p style="text-align: center;">5.3.1.1. Introduction</p> <p>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) or caption 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.</p> <div style="text-align: center;"><p>The diagram illustrates the structure of a track file. It is divided into three main sections: File Header, File Body, and File Footer. The File Header section contains two sub-sections: 'Header partition pack' and 'Header Metadata'. The File Body section contains a single sub-section: 'Essence Container'. The File Footer section contains a single sub-section: 'Footer partition pack'. Brackets above the boxes group them into the three main sections.</p></div> <p style="text-align: center;">Figure 8: Example Track File Structure</p> <p>DCI Specification, 39.</p> <ul style="list-style-type: none">• <i>Each MB/SM shall be provided with the appropriate DCP track files for the media essence to be processed by the respective MB. (This could be the entire DCP or portions of it according to where DCP track file parsing takes place.)</i> <p>Chapter 9 Replacement, 94.</p>
[815.42a] receiving a request to use the file in a predefined manner;	<p>Cinemark performs the claimed step of receiving a request to use the file in a predefined manner.</p> <p>For example, the user interface of a Screen Management Systems (SMS) or Theater Management System (TMS) receives a request from the theater manager to start a Show Playlist created from individual Composition Playlists (CPLs), where each CPL references one or more reels having one or more Track Files (e.g., Image Track File, Audio Track File, Sub-title Track</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>File, Caption Track File) that contain the essence (image, audio, captions, sub-titles) of the Composition. The Security Manager subsequently receives a request from the SMS/TMS to perform playback of the file consistent with the defined Composition.</p> <p style="text-align: center;">7.1. Introduction</p> <p>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.</p> <p>DCI Specification, 51.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<div><p>Show Playback Overview</p><pre>graph TD; A[Screen Management System commands to prepare for playback] --> B[Security Manager checks that all Security Entities are valid and that all necessary cryptographic Keys are available]; B -- "OK?" --> C[KDM conditions are satisfied]; C -- "Yes/No" --> B; B -- "OK?" --> D[Confirm if logging sub-system operative]; D -- "Yes/No" --> B; B --> E[Issues keys to Media Decryptors]; B --> F[Generates keys to Link Encryptor/ Decryptor]; B --> G[Enables Forensic Marking (if required)]; E --> H[Show Starts]; F --> H; G --> H; H --> I[Essence Streams, and Security System monitors/ logs all security activity];</pre><p>Figure 18: Show Playback Overview</p><p>Chapter 9 Replacement, 98.</p></div>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<div><p>Digital Cinema Auditorium Security Implementations</p><p>Abbreviations: DCP = Digital Cinema Package FM = Forensic Marker LD = Link Decryptor LE = Link Encryptor MD = Media Decryptor SM = Security Manager SMS = Screen Management System SPB = Secure Processing Block TMS = Theater Management System</p><p>Standardized Messages: ① Extra-Theater Messages ② Intra-Theater Messages</p><p>Notes:</p><ul style="list-style-type: none">• Double-lined components are hard-security SPB1 containers• Dashed components are SPB2 containers• Circled numbers are the "security interfaces"• Components filled with red diagonal lines are Security Entities• Auditorium storage is not denoted in this diagram</div> <p style="text-align: center;">THEATER</p> <p style="text-align: center;">Figure 15: Digital Cinema Auditorium Security Implementations</p>

Chapter 9 Replacement, 89.

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<div><p style="text-align: center;">Single Screen System Architecture</p><p style="text-align: center;">Figure 10: Single-Screen System Architecture</p></div> <p>DCI Specification, 60.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>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.</p> <div><div>SHOW PLAYLIST</div><div><div>Start Composition #1</div><div>Start Composition #2</div><div>Start Composition #3</div><div>Start Composition #4</div><div>Start Composition #5</div><div>Start Composition #6</div><div>Start Composition #7</div></div><div>EXHIBITION STORAGE</div><div><div>COMPOSITION #1</div><div>COMPOSITION #2</div><div>COMPOSITION #3</div><div>COMPOSITION #4</div><div>COMPOSITION #5</div><div>COMPOSITION #6</div><div>COMPOSITION #7</div></div></div> <p style="text-align: center;">Figure 6: Example Show Playlist</p> <p>DCI Specification, 38.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5.2.3. Packaging Concepts</p> <p>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. <i>This concept of reels is required to be supported with Digital Cinema content.</i></p> <p>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.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<div><p>COMPOSITION</p><p>COMPOSITION PLAYLIST (feature - English)</p><p>POINTERS</p><p>REEL 1</p><p>IMAGE ESSENCE (track file) (English, 2.35)</p><p>AUDIO ESSENCE (track file) (English, 5.1)</p><p>SUB-TITLE ESSENCE (track file) (Spanish)</p><p>REEL 2</p><p>IMAGE ESSENCE (track file) (English, 2.35)</p><p>AUDIO ESSENCE (track file) (English, 5.1)</p><p>SUB-TITLE ESSENCE (track file) (Spanish)</p></div> <p>Figure 5: Example Composition Playlist</p> <p>DCI Specification, 37.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
[815.42b] retrieving at least one digital signature and at least one check value associated with the file;	<p>Cinemark performs the claimed step of retrieving at least one digital signature and at least one check value associated with the file.</p> <p>For example, the Security Manager receives the CPL and retrieves therefrom the CPL's digital signature. The CPL is digitally signed so that modifications to the CPL and the associated Composition can be detected.</p> <p style="padding-left: 40px;">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. <i>For encrypted essence, the Composition Playlist shall be digitally signed such that modifications to the Composition Playlist (and/or the associated composition) can be detected.</i> 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.</p> <p>DCI Specification, 37-38.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5.4.3.6. Digital Signature</p> <ul style="list-style-type: none">• Encrypted hash (message digest)• Signer identification <p>5.4.4. Security of the CPL</p> <p><i>For encrypted essence, the Composition Playlist shall be digitally signed such that modifications to the Composition Playlist (and/or the associated composition) can be detected. In support of this, the CPL assets "KeyID" and "Hash" elements shall be present in the CPL track file asset structure.</i></p> <p>DCI Specification, 46.</p> <hr/> <p>6.13 Signature [optional]</p> <p>The <code>Signature</code> element shall contain a digital signature authenticating the Composition Playlist. If the <code>Signature</code> element is present, then the <code>Signer</code> element (6.12 above) shall also be present. The <code>Signature</code> element shall be an instance of the <code>ds:Signature</code> element defined in [XML-Signature Syntax and Processing]. The digital signature shall be <i>enveloped</i> and apply to the entire Composition Playlist. An enveloped signature is one that is attached to the document being signed. The signature is generated by the signer, as identified by the <code>Signer</code> element, using the signer's private key.</p> <p>SMPTE ST⁸ 429-7-2006, D-Cinema Packaging – Composition Playlist ("SMPTE 429-7-2006"), 11.⁹</p>

⁸ DCI-compliant Digital Cinema systems that follow the "Interop" DCP documentation practice the asserted claims in the same or substantially the same way as DCI-compliant Digital Cinema systems that follow the SMPTE standards.

⁹ SMPTE 429-7-2006 was produced at INTERTRUST00084967 – INTERTRUST00084996.

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³				
	<p>4. <i>Validate Composition Playlists (CPL), and log results as a prerequisite to the associated composition playback. For encrypted content, validation shall be by cross checking that the associated KDM's ContentAuthenticator element matches a certificate thumbprint of one of the certificates in the CPL's signer chain (see item 1 above), and that such certificate indicate only a “Content Signer” (CS) role per Section 5.3.4, “Naming and Roles” of the certificate specification (SMPTE430-2 D-Cinema Operation - Digital Certificate).</i></p> <p>Chapter 9 Replacement, 100.</p> <ul style="list-style-type: none">• Composition Playlist (CPL) and Key Delivery Message (KDM) check(s) – <i>Composition Playlists (CPL) and Key Delivery Messages (KDM) shall be validated by the Security Manager(s) participating in the respective composition playback.</i> <p>Chapter 9 Replacement, 95.</p> <table><tr><th>Message Category</th><th>Function</th></tr><tr><td>1. SMS to SM StartSuite StopSuite CPLValidate KDMValidate TimeAdj</td><td><i>Suggested operational messages</i> Commands SM to establish TLS sessions with remote SPBs Commands SM to terminate TLS sessions with remote SPBs Requests that the SM perform a CPL validation check Requests that the SM perform a KDM validation check Adjusts time at SM (within annual limits)</td></tr></table> <p>Chapter 9 Replacement, 113.</p> <p>The Security Manager also retrieves hashes of the Track Files from the CPL and HMAC values associated with the Track Files.</p>	Message Category	Function	1. SMS to SM StartSuite StopSuite CPLValidate KDMValidate TimeAdj	<i>Suggested operational messages</i> Commands SM to establish TLS sessions with remote SPBs Commands SM to terminate TLS sessions with remote SPBs Requests that the SM perform a CPL validation check Requests that the SM perform a KDM validation check Adjusts time at SM (within annual limits)
Message Category	Function				
1. SMS to SM StartSuite StopSuite CPLValidate KDMValidate TimeAdj	<i>Suggested operational messages</i> Commands SM to establish TLS sessions with remote SPBs Commands SM to terminate TLS sessions with remote SPBs Requests that the SM perform a CPL validation check Requests that the SM perform a KDM validation check Adjusts time at SM (within annual limits)				

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<div><p style="text-align: center;">Figure 10 – Track File Asset Structure (Dotted lines denote an optional element)</p></div> <p>SMPTE 429-7-2006, 15.</p> <p>8.2.2 Hash [optional]</p> <p>The <code>Hash</code> element shall contain the hash (message digest) of the underlying track file computed using the SHA-1 message digest algorithm [RFC 3174]. When authenticated by the digital signature in the Composition Playlist (see 6.13), it may be used to verify the integrity and authenticity of the underlying track file. The resulting 160-bit integer shall be encoded using Base64 representation [RFC 2045].</p> <p>SMPTE 429-7-2006, 16.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<ul style="list-style-type: none">• <i>At any point in the delivery chain, it is required to be possible to detect whether any accidental or intentional alteration has occurred.</i> <p>5.3.1.9. Integrity and Authentication</p> <p><i>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:</i></p> <ul style="list-style-type: none">• <i>It is encouraged that missing or corrupted data be easily identified.</i>• <i>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.</i> <p>DCI Specification, 41.</p> <ul style="list-style-type: none">• <i>The integrity of each frame of sound and picture essence shall be verifiable using the HMAC-SHA1 algorithm. The optional Message Integrity Code (MIC) element of SMPTE 429-6 shall be present.</i> <p>DCI Specification, 42; <i>see also</i> DCI Digital Cinema System Specification v. 1.3 (June 2018) ("DCI Specification 1.3"), 42.</p> <p><i>The following role(s) shall be included for the IMB and OMB, as applicable:</i></p> <ul style="list-style-type: none">▪ <i>KDM-borne Message Integrity Code key capable MB – MIC</i> <p>DCI Specification 1.3, 134.</p> <p>As another example, the Security Manager receives a Key Delivery Message associated with the file of electronic data and retrieves therefrom the KDM's digital signature. The KDM is digitally signed so that modifications to the KDM and its contents can be detected.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p style="text-align: center;">Key Delivery Message (KDM) – The Extra Theater Message (ETM) for delivering content keys and Trusted Device List (TDL) to exhibition locations.</p> <p>Chapter 9 Replacement, 82.</p> <p>The Signature element defined in [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). The Signature section is not authenticated, though it is believed if an attacker made any beneficial modifications to the Signature section, then the authentication of the other sections would fail.</p> <p>A single KDM can carry multiple content keys for the same content (the same CompositionPlaylistId), and a Composition Play List may require content keys that are carried in multiple KDMs. For example, a separate KDM could be used to deliver content keys for region-specific dialog tracks.</p> <p>5 Authenticated and Unencrypted Information</p> <p>The KDM extends the ETM by including the KDMRequiredExtensions element (see Figure 4 below) in its RequiredExtensions element. The normative schema is defined in Annex B. 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.</p> <p>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.</p> <p>SMPTE ST 430-1:2017, D-Cinema Operations - Key Delivery Message ("SMPTE 430-1:2017"), 6.¹⁰</p>

¹⁰ SMPTE 430-1:2017 was produced at INTERTRUST00085093 – INTERTRUST00085110.

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>6 Authenticated and Encrypted Information</p> <p>The AuthenticatedPrivate element is normatively defined in [ETM]. It is described here only to illustrate the use of this element for carrying encrypted keys in a KDM. This portion of the KDM is authenticated by the signature, and encrypted for the recipient before being transmitted. The word “private” appears in the XML label for this portion, though this does not mean that the information is proprietary or vendor-specific. It means that through encryption only a specified recipient is allowed to view this information. The recipient performs standard XML decryption operations to recover the private information.</p> <p>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.</p> <p>For the KDM, the ETM's EncryptedData element shall be omitted and each EncryptedKey element shall carry one content key and its associated information. The KDM shall only have a single recipient. The following sections describe how the KDM message uses the EncryptedKey element.</p> <p>SMPTE 430-1:2017, 12-13.</p> <div><p>The diagram illustrates the Key Delivery Message process. It features two central nodes: 'Issuer' and 'Recipient'. The Issuer node receives three inputs: 'Recipient Public Key' (top left), 'Content Keys & Parameters' (middle left), and 'TDL' (bottom left). The Issuer node outputs 'Issuer Private Key' (bottom left). The Recipient node receives three inputs: 'Recipient Private Key' (top right), 'Content Keys & Parameters' (middle right), and 'TDL' (bottom right). The Recipient node outputs 'Issuer Public Key' (bottom right). A central arrow labeled 'Key Delivery Message' connects the Issuer node to the Recipient node.</p></div> <p>SMPTE 430-1:2017, 5.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
[815.42c] verifying the authenticity of the at least one check value using the digital signature;	<p>Cinemark performs the claimed step of verifying the authenticity of the at least one check value using the digital signature.</p> <p>For example, the CPL's digital signature envelops and applies to the entire CPL including the hash values of the underlying Track Files. Consequently, verification of the CPL's digital signature is used to verify the authenticity of the hash values.</p> <div><p>6.13 Signature [optional]</p><p>The <code>Signature</code> element shall contain a digital signature authenticating the Composition Playlist. If the <code>Signature</code> element is present, then the <code>Signer</code> element (6.12 above) shall also be present. The <code>Signature</code> element shall be an instance of the <code>ds:Signature</code> element defined in [XML-Signature Syntax and Processing]. The digital signature shall be <i>enveloped</i> and apply to the entire Composition Playlist. An enveloped signature is one that is attached to the document being signed. The signature is generated by the signer, as identified by the <code>Signer</code> element, using the signer's private key.</p></div> <p>SMPTE 429-7-2006, 11.</p> <p>4. <i>Validate Composition Playlists (CPL), and log results as a prerequisite to the associated composition playback. For encrypted content, validation shall be by cross checking that the associated KDM's ContentAuthenticator element matches a certificate thumbprint of one of the certificates in the CPL's signer chain (see item 1 above), and that such certificate indicate only a “Content Signer” (CS) role per Section 5.3.4, “Naming and Roles” of the certificate specification (SMPTE430-2 D-Cinema Operation - Digital Certificate).</i></p> <p>Chapter 9 Replacement, 100.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<ul style="list-style-type: none">• Composition Playlist (CPL) and Key Delivery Message (KDM) check(s) – <i>Composition Playlists (CPL) and Key Delivery Messages (KDM) shall be validated by the Security Manager(s) participating in the respective composition playback.</i> <p>Chapter 9 Replacement, 95.</p> <p>6.1.5. Restriction of Keying to Valid CPLs</p> <p>Objective</p> <p>Verify that the SM validates CPLs and logs results as a prerequisite to preparing the suite for the associated composition playback.</p> <p>Procedures</p> <ol style="list-style-type: none">1. Supply the CPL <i>DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)</i>, keyed with KDM for DCI <i>Malformed Test 6: CPL with incorrect track file hashes (Encrypted)</i>, to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.2. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.3. Extract a security log from the Test Subject and using a <i>Text Editor</i>, identify the CPLCheck event associated with the above operation and:<ol style="list-style-type: none">a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the <code>contentId</code> element contains the Id of the CPL. Verify that the value of the <code>SignerID</code> parameter contains the Certificate Thumbprint of the certificate used to sign the CPL. Verify that <code>ReferencedIDs</code> element contains a <code>CompositionID</code> parameter with a value that is the Id of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.b. Confirm the presence of a <code>AssetHashError</code> exception in the CPLCheck log record. Record any additional parameters associated with the exception. A missing <code>AssetHashError</code> exception shall be cause to fail this test.4. Supply the CPL <i>DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)</i>, keyed with KDM for DCI <i>Malformed Test 7: CPL with an Invalid Signature (Encrypted)</i> to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.5. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>Digital Cinema System Specification – Compliance Test Plan v. 1.2 (Oct. 10, 2012) ("DCSS CTP"), 220.¹¹</p> <p>As another example, the KDM's digital signature applies to the contents of the KDM, including, but not limited to, the content keys and the message integrity code (MIC) keys. Thus, verification of the KDM's digital signature also verifies the authenticity of the keys (content or MIC) that are associated with hashes of the Track File contents.</p> <p style="padding-left: 40px;">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.</p> <p style="padding-left: 40px;">For the KDM, the ETM's EncryptedData element shall be omitted and each EncryptedKey element shall carry one content key and its associated information. The KDM shall only have a single recipient. The following sections describe how the KDM message uses the EncryptedKey element.</p> <p>SMPTE 430-1:2017, 12-13.</p>

¹¹ DCSS CTP was produced at INTERTRUST00084142 – INTERTRUST00084797.

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5. <i>Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Integrity pack deviations (including HMAC, as applicable) detected during playback shall be logged; however, per Section 9.6.1.2 "Digital Rights Management: Security Manager" Table 21, playback should not be prevented or interrupted. For clarity purposes, integrity pack metadata is defined as Track File ID, Frame Sequence and calculated Message Integrity Code (MIC) information to be compared against the reference data contained in the associated CPL. Log information necessary to detect deviations (including restarts) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:</i></p> <p class="list-item-l1"><i>a. Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.</i></p> <p class="list-item-l1"><i>b. Audio – Process integrity pack information, including the hash (HMAC). The SM shall prevent playout of encrypted content for which the image and sound integrity pack metadata is not present per the requirements of Section 5.3.2.1.</i></p> <p>Chapter 9 Replacement, 100.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5. <i>Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Integrity pack deviations (including HMAC, as applicable) detected during playback shall be logged; however, per Section 9.6.1.2 Digital Rights Management: Security Manager (SM) Table 21, playback should not be prevented or interrupted. For clarity purposes, integrity pack metadata is defined as Track File ID, Frame Sequence and calculated Message Integrity Code (MIC) information to be compared against the reference data contained in the associated CPL. Log information necessary to detect deviations (including restarts) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:</i></p> <p style="margin-left: 40px;"><i>a. Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.</i></p> <p style="margin-left: 40px;"><i>b. Audio – Process integrity pack information, including the hash (HMAC).</i></p> <p>DCI Specification 1.3, 103-104.</p> <p>6. <i>As of January 1, 2016, Federal Information Processing Standards (FIPS) compliance requirements disallow use of the random number generator (RNG) as specified in [SMPTE ST429-6 D-Cinema Packaging - MXF Track File Essence Encryption]. Additionally, a KDM key type is needed to support encryption of generic Auxiliary Data (AD) essence per [SMPTE ST429-14 D-Cinema Packaging - Aux Data File]. These are addressed by the following requirements for support of KDMs carrying "MIC" and "Aux Data" key types:</i></p> <p style="margin-left: 40px;"><i>a. Media Block (MB) SMs shall support the receipt and processing of KDMs carrying the MIC and Aux Data (AD) key types. (See [SMPTE ST430-1 D-Cinema Operations - Key Delivery Message].)</i></p> <p style="margin-left: 40px;"><i>b. MB SMs shall perform the content hash (HMAC) integrity check of above item 5 using the KDM-borne MIC keys if present (and shall not derive the MIC key from KDM content keys).</i></p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p><i>c. MB SMs capable of processing KDM-borne MIC keys shall indicate so by including "MIC" in their digital certificate roles (see role definitions of Section 9.5.1.1 Single Certificate Implementations).</i></p> <p><i>d. MB SMs shall not implement the Random Number Generator (RNG) defined (for the purpose of MIC key derivation) in [SMPTE ST429-6: D-Cinema Packaging - MXF Track File Essence Encryption].</i></p> <p><i>e. When receiving a KDM type that does not contain a MIC key, MB SMs shall perform all the content integrity checks specified in above item 5 except the hash (HMAC) check.</i></p> <p>DCI Specification 1.3, 104.</p>
[815.42d] verifying the authenticity of at least a portion of the file using the at least one check value; and	<p>Cinemark performs the claimed step of verifying the authenticity of at least a portion of the file using the at least one check value.</p> <p>For example, the Security Manager verifies the authenticity of the Track Files by using the validated hashes associated with the underlying Track Files.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>6.1.5. Restriction of Keying to Valid CPLs</p> <p>Objective</p> <p>Verify that the SM validates CPLs and logs results as a prerequisite to preparing the suite for the associated composition playback.</p> <p>Procedures</p> <ol style="list-style-type: none">1. Supply the CPL <i>DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)</i>, keyed with <i>KDM for DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)</i>, to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.2. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.3. Extract a security log from the Test Subject and using a <i>Text Editor</i>, identify the CPLCheck event associated with the above operation and:<ol style="list-style-type: none">a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the <code>contentId</code> element contains the Id of the CPL. Verify that the value of the <code>SignerID</code> parameter contains the Certificate Thumbprint of the certificate used to sign the CPL. Verify that <code>ReferencedIDs</code> element contains a <code>CompositionID</code> parameter with a value that is the Id of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.b. Confirm the presence of a <code>AssetHashError</code> exception in the CPLCheck log record. Record any additional parameters associated with the exception. A missing <code>AssetHashError</code> exception shall be cause to fail this test.4. Supply the CPL <i>DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)</i>, keyed with <i>KDM for DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)</i> to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.5. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test. <p>DCSS CTP, 220.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5. <i>Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Integrity pack deviations (including HMAC, as applicable) detected during playback shall be logged; however, per Section 9.6.1.2 "Digital Rights Management: Security Manager" Table 21, playback should not be prevented or interrupted. For clarity purposes, integrity pack metadata is defined as Track File ID, Frame Sequence and calculated Message Integrity Code (MIC) information to be compared against the reference data contained in the associated CPL. Log information necessary to detect deviations (including restarts) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:</i></p> <p class="list-item-l1"><i>a. Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.</i></p> <p class="list-item-l1"><i>b. Audio – Process integrity pack information, including the hash (HMAC). The SM shall prevent playout of encrypted content for which the image and sound integrity pack metadata is not present per the requirements of Section 5.3.2.1.</i></p> <p>Chapter 9 Replacement, 100.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5. <i>Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Integrity pack deviations (including HMAC, as applicable) detected during playback shall be logged; however, per Section 9.6.1.2 Digital Rights Management: Security Manager (SM) Table 21, playback should not be prevented or interrupted. For clarity purposes, integrity pack metadata is defined as Track File ID, Frame Sequence and calculated Message Integrity Code (MIC) information to be compared against the reference data contained in the associated CPL. Log information necessary to detect deviations (including restarts) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:</i></p> <p style="margin-left: 40px;"><i>a. Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.</i></p> <p style="margin-left: 40px;"><i>b. Audio – Process integrity pack information, including the hash (HMAC).</i></p> <p>DCI Specification 1.3, 103-104.</p> <p>6. <i>As of January 1, 2016, Federal Information Processing Standards (FIPS) compliance requirements disallow use of the random number generator (RNG) as specified in [SMPTE ST429-6 D-Cinema Packaging - MXF Track File Essence Encryption]. Additionally, a KDM key type is needed to support encryption of generic Auxiliary Data (AD) essence per [SMPTE ST429-14 D-Cinema Packaging - Aux Data File]. These are addressed by the following requirements for support of KDMs carrying "MIC" and "Aux Data" key types:</i></p> <p style="margin-left: 40px;"><i>a. Media Block (MB) SMs shall support the receipt and processing of KDMs carrying the MIC and Aux Data (AD) key types. (See [SMPTE ST430-1 D-Cinema Operations - Key Delivery Message].)</i></p> <p style="margin-left: 40px;"><i>b. MB SMs shall perform the content hash (HMAC) integrity check of above item 5 using the KDM-borne MIC keys if present (and shall not derive the MIC key from KDM content keys).</i></p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p><i>c. MB SMs capable of processing KDM-borne MIC keys shall indicate so by including "MIC" in their digital certificate roles (see role definitions of Section 9.5.1.1 Single Certificate Implementations).</i></p> <p><i>d. MB SMs shall not implement the Random Number Generator (RNG) defined (for the purpose of MIC key derivation) in [SMPTE ST429-6: D-Cinema Packaging - MXF Track File Essence Encryption].</i></p> <p><i>e. When receiving a KDM type that does not contain a MIC key, MB SMs shall perform all the content integrity checks specified in above item 5 except the hash (HMAC) check.</i></p> <p>DCI Specification 1.3, 104.</p>
[815.42e] granting the request to use the file in the predefined manner.	<p>Cinemark performs the claimed step of granting the request to use the file in the predefined manner.</p> <p>For example, the Security Manager grants the request to play the Show Playlist and the referenced Track Files in a manner consistent with the Composition Playlist ("use the file in the predefined manner").</p> <p>9.4.3.2. Pre-show Preparations</p> <p>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.</p> <ul style="list-style-type: none">• Composition Playlist (CPL) and Key Delivery Message (KDM) check(s) – <i>Composition Playlists (CPL) and Key Delivery Messages (KDM) shall be validated by the Security Manager(s) participating in the respective composition playback.</i> <p>Chapter 9 Replacement, 95.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
***Intertrust Techs. Corp. v. Cinemark Holdings, Inc.* (Case No. 2:19-cv-00266-JRG)**

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<div data-bbox="1400 316 2032 1192"> <pre> graph TD A["Composition Playlist(s) (CPLs) needed for the show playlist are sent from Screen Management System to Security Manager (SM)"] --> B["Composition Playlist(s) (CPLs) are validated by the Security Manager (SM)"] B --> C["Key Delivery Messages (KDMs) for above Composition Playlist(s) (CPLs) are sent to the Security Manager (SM), validated and decrypted"] C --> D["Security Manager (SM) verifies it has all cryptographic keys necessary for the above Composition Playlist(s) (CPLs)"] D --> E["Confirmed that one can play the CPL"] </pre> <p>Validate Composition Playlists</p> <p>Validate Key Delivery Message</p> <p>Validate Ready to Play*</p> <p>*"Ready to Play" may optionally include Key Delivery Message (KDM) playout window and/or Trusted Device List (TDL) checks</p> </div> <p data-bbox="1540 1214 1892 1248">Figure 17: Pre-Show Overview</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<div style="text-align: center;"><p>Show Playback Overview</p><pre>graph TD; A[Screen Management System commands to prepare for playback] --> B[Security Manager checks that all Security Entities are valid and that all necessary cryptographic Keys are available]; B -- "OK?" --> C[KDM conditions are satisfied]; C -- "Yes/No" --> B; B -- "OK?" --> D[Confirm if logging sub-system operative]; D -- "Yes/No" --> B; B --> E[Issues keys to Media Decryptors]; B --> F[Generates keys to Link Encryptor/ Decryptor]; B --> G[Enables Forensic Marking (if required)]; E --> H[Show Starts]; F --> H; G --> H; H --> I[Essence Streams, and Security System monitors/ logs all security activity];</pre></div> <p style="text-align: center;">Figure 18: Show Playback Overview</p> <p>Chapter 9 Replacement, 98.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5. <i>Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Integrity pack deviations (including HMAC, as applicable) detected during playback shall be logged; however, per Section 9.6.1.2 "Digital Rights Management: Security Manager" Table 21, playback should not be prevented or interrupted. For clarity purposes, integrity pack metadata is defined as Track File ID, Frame Sequence and calculated Message Integrity Code (MIC) information to be compared against the reference data contained in the associated CPL. Log information necessary to detect deviations (including restarts) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:</i></p> <p class="list-item-l1"><i>a. Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.</i></p> <p class="list-item-l1"><i>b. Audio – Process integrity pack information, including the hash (HMAC). The SM shall prevent playout of encrypted content for which the image and sound integrity pack metadata is not present per the requirements of Section 5.3.2.1.</i></p> <p>Chapter 9 Replacement, 100.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5. <i>Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Integrity pack deviations (including HMAC, as applicable) detected during playback shall be logged; however, per Section 9.6.1.2 Digital Rights Management: Security Manager (SM) Table 21, playback should not be prevented or interrupted. For clarity purposes, integrity pack metadata is defined as Track File ID, Frame Sequence and calculated Message Integrity Code (MIC) information to be compared against the reference data contained in the associated CPL. Log information necessary to detect deviations (including restarts) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:</i></p> <p style="margin-left: 40px;"><i>a. Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.</i></p> <p style="margin-left: 40px;"><i>b. Audio – Process integrity pack information, including the hash (HMAC).</i></p> <p>DCI Specification 1.3, 103-104.</p> <p>6. <i>As of January 1, 2016, Federal Information Processing Standards (FIPS) compliance requirements disallow use of the random number generator (RNG) as specified in [SMPTE ST429-6 D-Cinema Packaging - MXF Track File Essence Encryption]. Additionally, a KDM key type is needed to support encryption of generic Auxiliary Data (AD) essence per [SMPTE ST429-14 D-Cinema Packaging - Aux Data File]. These are addressed by the following requirements for support of KDMs carrying "MIC" and "Aux Data" key types:</i></p> <p style="margin-left: 40px;"><i>a. Media Block (MB) SMs shall support the receipt and processing of KDMs carrying the MIC and Aux Data (AD) key types. (See [SMPTE ST430-1 D-Cinema Operations - Key Delivery Message].)</i></p> <p style="margin-left: 40px;"><i>b. MB SMs shall perform the content hash (HMAC) integrity check of above item 5 using the KDM-borne MIC keys if present (and shall not derive the MIC key from KDM content keys).</i></p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p><i>c. MB SMs capable of processing KDM-borne MIC keys shall indicate so by including "MIC" in their digital certificate roles (see role definitions of Section 9.5.1.1 Single Certificate Implementations).</i></p> <p><i>d. MB SMs shall not implement the Random Number Generator (RNG) defined (for the purpose of MIC key derivation) in [SMPTE ST429-6: D-Cinema Packaging - MXF Track File Essence Encryption].</i></p> <p><i>e. When receiving a KDM type that does not contain a MIC key, MB SMs shall perform all the content integrity checks specified in above item 5 except the hash (HMAC) check.</i></p> <p>DCI Specification 1.3, 104.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>6.1.5. Restriction of Keying to Valid CPLs</p> <p>Objective</p> <p>Verify that the SM validates CPLs and logs results as a prerequisite to preparing the suite for the associated composition playback.</p> <p>Procedures</p> <ol style="list-style-type: none">1. Supply the CPL <i>DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)</i>, keyed with <i>KDM for DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)</i>, to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.2. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.3. Extract a security log from the Test Subject and using a <i>Text Editor</i>, identify the CPLCheck event associated with the above operation and:<ol style="list-style-type: none">a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the <code>contentId</code> element contains the Id of the CPL. Verify that the value of the <code>SignerID</code> parameter contains the Certificate Thumbprint of the certificate used to sign the CPL. Verify that <code>ReferencedIDs</code> element contains a <code>CompositionID</code> parameter with a value that is the Id of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.b. Confirm the presence of a <code>AssetHashError</code> exception in the CPLCheck log record. Record any additional parameters associated with the exception. A missing <code>AssetHashError</code> exception shall be cause to fail this test.4. Supply the CPL <i>DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)</i>, keyed with <i>KDM for DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)</i> to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.5. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test. <p>DCSS CTP, 220.</p>
[815.43] A method as in claim 42, in which the at	Cinemark has committed and continues to commit acts of infringement of claim 43 under 35 U.S.C. § 271 through its use of

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
<p>least one check value comprises one or more hash values, and in which verifying the authenticity of at least a portion of the file using the at least one check value includes: hashing at least a portion of the file to obtain a first hash value; and comparing the first hash value to at least one of the one or more hash values.</p>	<p>DCI-compliant Digital Cinema systems to show movies and other DCI-compliant content.</p> <p>Cinemark performs the claimed method of claim 42. <i>See supra</i> [815.42]-[815.42e]. In addition, Cinemark performs the claimed method in which the at least one check value comprises one or more hash values.</p> <p>For example, on information and belief, verification of the authenticity of at least a portion of the Track Files is performed by hashing the at least a portion of the Track Files to obtain a first set of hash values and then comparing these first set of hash values to the hashes validated by information provided in the KDM and CPL.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>6.1.5. Restriction of Keying to Valid CPLs</p> <p>Objective</p> <p>Verify that the SM validates CPLs and logs results as a prerequisite to preparing the suite for the associated composition playback.</p> <p>Procedures</p> <ol style="list-style-type: none">1. Supply the CPL <i>DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)</i>, keyed with <i>KDM for DCI Malformed Test 6: CPL with incorrect track file hashes (Encrypted)</i>, to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.2. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test.3. Extract a security log from the Test Subject and using a <i>Text Editor</i>, identify the CPLCheck event associated with the above operation and:<ol style="list-style-type: none">a. Confirm that all required elements have correctly formatted parameters as defined in [SMPTE-430-5]. Verify that the <code>contentId</code> element contains the Id of the CPL. Verify that the value of the <code>SignerID</code> parameter contains the Certificate Thumbprint of the certificate used to sign the CPL. Verify that <code>ReferencedIDs</code> element contains a <code>CompositionID</code> parameter with a value that is the Id of the CPL. Missing required elements or incorrect parameters shall be cause to fail this test.b. Confirm the presence of a <code>AssetHashError</code> exception in the CPLCheck log record. Record any additional parameters associated with the exception. A missing <code>AssetHashError</code> exception shall be cause to fail this test.4. Supply the CPL <i>DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)</i>, keyed with <i>KDM for DCI Malformed Test 7: CPL with an Invalid Signature (Encrypted)</i> to the SM. Verify that the SM rejects the CPL. If the SM accepts the CPL, this is cause to fail this test.5. Attempt to start playback and verify that it is not possible. If playback starts, this is cause to fail this test. <p>DCSS CTP, 220.</p>

Intertrust’s P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5. <i>Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Integrity pack deviations (including HMAC, as applicable) detected during playback shall be logged; however, per Section 9.6.1.2 "Digital Rights Management: Security Manager" Table 21, playback should not be prevented or interrupted. For clarity purposes, integrity pack metadata is defined as Track File ID, Frame Sequence and calculated Message Integrity Code (MIC) information to be compared against the reference data contained in the associated CPL. Log information necessary to detect deviations (including restarts) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:</i></p> <p class="list-item-l1">a. <i>Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.</i></p> <p class="list-item-l1">b. <i>Audio – Process integrity pack information, including the hash (HMAC). The SM shall prevent playout of encrypted content for which the image and sound integrity pack metadata is not present per the requirements of Section 5.3.2.1.</i></p> <p>Chapter 9 Replacement, 100.</p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p>5. <i>Process essence (i.e., Track File frame) integrity pack metadata for image and sound during show runtime. Integrity pack deviations (including HMAC, as applicable) detected during playback shall be logged; however, per Section 9.6.1.2 Digital Rights Management: Security Manager (SM) Table 21, playback should not be prevented or interrupted. For clarity purposes, integrity pack metadata is defined as Track File ID, Frame Sequence and calculated Message Integrity Code (MIC) information to be compared against the reference data contained in the associated CPL. Log information necessary to detect deviations (including restarts) from the actual playback sequence from the Track File ID and reel sequence specified in the CPL as follows:</i></p> <p style="margin-left: 40px;"><i>a. Image – Process integrity pack information, with the exception that the frame hash (HMAC) check is encouraged but optional.</i></p> <p style="margin-left: 40px;"><i>b. Audio – Process integrity pack information, including the hash (HMAC).</i></p> <p>DCI Specification 1.3, 103-104.</p> <p>6. <i>As of January 1, 2016, Federal Information Processing Standards (FIPS) compliance requirements disallow use of the random number generator (RNG) as specified in [SMPTE ST429-6 D-Cinema Packaging - MXF Track File Essence Encryption]. Additionally, a KDM key type is needed to support encryption of generic Auxiliary Data (AD) essence per [SMPTE ST429-14 D-Cinema Packaging - Aux Data File]. These are addressed by the following requirements for support of KDMs carrying "MIC" and "Aux Data" key types:</i></p> <p style="margin-left: 40px;"><i>a. Media Block (MB) SMs shall support the receipt and processing of KDMs carrying the MIC and Aux Data (AD) key types. (See [SMPTE ST430-1 D-Cinema Operations - Key Delivery Message].)</i></p> <p style="margin-left: 40px;"><i>b. MB SMs shall perform the content hash (HMAC) integrity check of above item 5 using the KDM-borne MIC keys if present (and shall not derive the MIC key from KDM content keys).</i></p>

Intertrust's P.R. 3-1 Disclosures: Exhibit 3
Intertrust Techs. Corp. v. Cinemark Holdings, Inc. (Case No. 2:19-cv-00266-JRG)

'815 Patent Claim ²	Where Each Claim Element Is Found Within The Accused Instrumentalities ³
	<p><i>c. MB SMs capable of processing KDM-borne MIC keys shall indicate so by including "MIC" in their digital certificate roles (see role definitions of Section 9.5.1.1 Single Certificate Implementations).</i></p> <p><i>d. MB SMs shall not implement the Random Number Generator (RNG) defined (for the purpose of MIC key derivation) in [SMPTE ST429-6: D-Cinema Packaging - MXF Track File Essence Encryption].</i></p> <p><i>e. When receiving a KDM type that does not contain a MIC key, MB SMs shall perform all the content integrity checks specified in above item 5 except the hash (HMAC) check.</i></p> <p>DCI Specification 1.3, 104.</p>