SMPTE ST 430-1:2017
Revision of
SMPTE 430-1:2006

SMPTE STANDARD

D-Cinema Operations — Key Delivery Message

Table of Contents

Approved
January 12, 2017

Foreword

SMPTE (the Society of Motion Picture and Television Engineers) is an internationally recognized standards developing organization. Headquartered and incorporated in the United States of America, SMPTE has members in over 80 countries on six continents. SMPTE's Engineering Documents, including Standards, Recommended Practices and Engineering Guidelines, are prepared by SMPTE's Technology Committees. Participation in these Committees is open to all with a bona fide interest in their work. SMPTE cooperates closely with other standards-developing organizations, including ISO, IEC and ITU.

SMPTE Engineering Documents are drafted in accordance with the rules given in its Standards Operations Manual.

SMPTE ST 430-1 was prepared by Technology Committee 21DC.

Intellectual Property

SMPTE draws attention to the fact that it is claimed that compliance with this Standard may involve the use of one or more patents or other intellectual property rights (collectively, "IPR"). The Society takes no position concerning the evidence, validity, or scope of this IPR.

Each holder of claimed IPR has assured the Society that it is willing to License all IPR it owns, and any third party IPR it has the right to sublicense, that is essential to the implementation of this Standard to those (Members and non-Members alike) desiring to implement this Standard under reasonable terms and conditions, demonstrably free of discrimination. Each holder of claimed IPR has filed a statement to such effect with SMPTE. Information may be obtained from the Director, Standards & Engineering at SMPTE Headquarters.

Attention is also drawn to the possibility that elements of this Standard may be subject to IPR other than those identified above. The Society shall not be responsible for identifying any or all such IPR.

1 Scope

This specification defines a “Key Delivery Message” (KDM) for use in Digital Cinema (D-Cinema) systems. The KDM has been designed to deliver security parameters and usage rights between D-Cinema content processing centers (e.g. from post production to distribution, or from distribution to exhibition). The KDM carries fundamentally three information types:

- Content keys for a specified Composition Play List (CPL).
- Content key parameters – primarily the permitted key usage date/time window.
- The Trusted Device List (TDL) which identifies equipment permitted to use the content keys.

The KDM is based on the D-Cinema generic Extra-Theater Message (ETM) format [ETM]. It uses XML to represent the information about the content keys and TDLs, and provides security using standardized XML encryption and signature primitives. The KDM message uses X.509 digital certificates, specified in [D-Cinema Digital Certificate], to provide authentication and trust.

Note: The brackets convention “[…]” as used herein denotes either a normative or informative reference.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of the standards indicated below.

[KLV] SMPTE ST 429-6:2006, D-Cinema Packaging — MXF Track File Essence Encryption

[D-Cinema Digital Certificate] SMPTE ST 430-2:2017, D-Cinema Operations — Digital Certificate

[ETM] SMPTE 430-3:2012, D-Cinema Operations — Generic Extra Theater Message Format

[RFC2253] Lightweight Directory Access Protocol (v3):UTF-8 String Representation of Distinguished Names, December 1997. See: http://www.ietf.org/rfc/rfc2253.txt

[Time] UTC, RFC 3339: Date and Time on the Internet: Timestamps. G. Klyne and C. Newman. Informational, July 2002. See: http://ietf.org/rfc/rfc3339.txt

[UUID] “A Universally Unique Identifier (UUID) URN Namespace” July 2005. See: http://www.ietf.org/rfc/rfc4122.txt

3 Glossary

The following paragraphs define the acronyms used in this standard.

AES: Advanced Encryption Standard secret key algorithm. See [FIPS-197].

ASN.1: Abstract Syntax Notation 1.

Base64: A printable encoding of binary data. See [Base64].

DES: Data Encryption Standard. See [FIPS-46-3].

ETM: Extra Theatre Message [See ETM]

FIPS: Federal Information Processing Standards of NIST.

HMAC-SHA-1: Hash-based Message Authentication Code based on SHA-1. See [FIPS-198].

IETF: Internet Engineering Task Force standards group.

IP: Internet Protocol. An IETF standard.

ISO: International Standards Organization.
KEK: Key Encrypting Key
LE: Link Encrypter.
LD: Link Decrypter.
MD: Media Decrypter.
NIST: National Institute of Standards and Technologies.
OAEP: Optimal Asymmetric Encryption Pattern. See [PKCS1].
RO: Rights Owner.
RSA: Rivest Shamir Adleman public key algorithm.
SE: Security Entity. Any Digital Cinema entity that performs cryptography.
SHA-1: Secure Hash Algorithm revision 1. See [FIPS-180-2].
SHA-256: Secure Hash Algorithm. See [FIPS-180-2].
SM: Security Manager.
S/MIME: Secure Multipurpose Internet Mail Extensions.
SPB: Secure Processing Block.
TCP: Transmission Control Protocol. IETF standard for reliable bi-directional streams.
TDES: Triple DES. See [FIPS-43-3].
TLS: Transport Layer Security protocol. See [Rescorla].
TMS: Theater Management System.
X.509. A widely used and supported digital certificate standard.
XML: Extensible Markup Language.

4 Overview of the KDM (Informative)

4.1 Basic KDM Elements and D-Cinema Relationships

This standard presents a specification for the Key Delivery Message (KDM) for use in a Digital Cinema (D-Cinema) system. The D-Cinema Key Delivery Message is normally sent:

1. Between a post-production system and a Distributor, or
2. Between a Distributor and a Theater facility.

D-Cinema systems require that content keys, key usage time window (key parameters) and “trusted equipment” information (Trusted Device List or TDL) be communicated to exhibition facilities. The KDM carries all the critical information required to enable content decryption according to a baseline interoperable security standard. The basic form of the KDM is shown in Figure 1.

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 intended security, full KDM information access should only take place within a secure environment (e.g., within a D-Cinema Secure Processing Block). KDMs can, however, be authenticated by insecure devices if such devices have copies of the root certificate of the entity that created and signed the KDM.

The KDM uses XML to represent the information about content keys and provides security using the XML Encryption and Signature primitives. To facilitate efficient processing with hardware security chips, the KDM individually encrypts each content key (along with other information) with RSA, and is structured to allow KDMs to be processed by devices that have limited resources of physically secure memory.

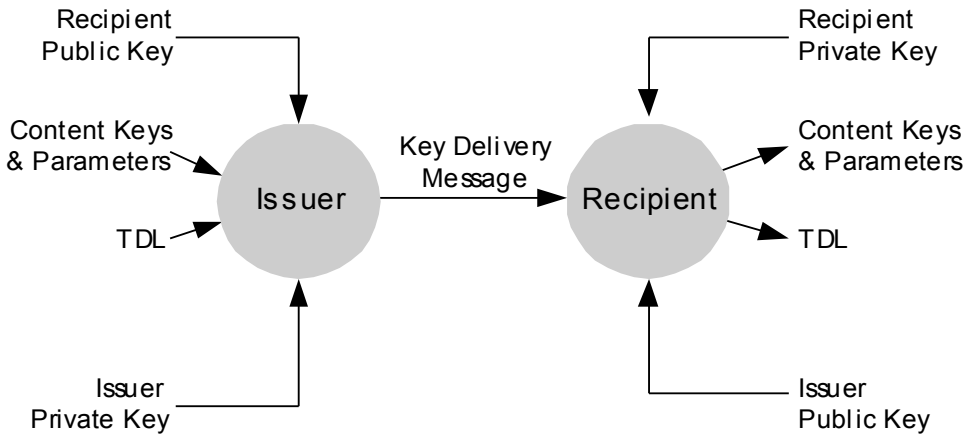

Figure 1 – KDM Information Flow

The KDM message is a particular instance of the generic XML security wrapper defined by the D-Cinema Generic Extra Theatre Message Format [ETM] and uses digital certificates defined by the D-Cinema Digital Certificate specification. This document defines the characteristics that are specific to the KDM, and should be followed in combination with [ETM], which in turn references the digital certificate specification.

The relationship between the KDM and the Composition Play List (CPL) is shown in Figure 2.

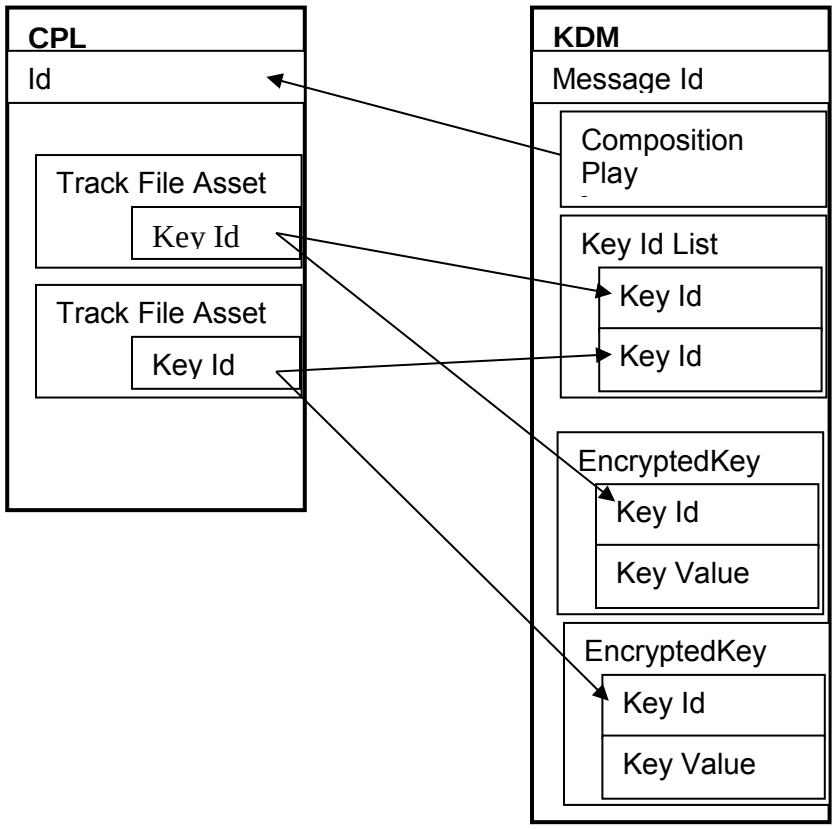

Figure 2 – Linking Between CPL and KDM Structures

Each CPL is identified by a globally unique value [UUID] that appears in the element named “Id” in the top-level XML structure for a CPL. There are other elements in the CPL that are also called “Id”, such as the identifier for a track file, though these are not the identifier of the whole CPL itself. The KDM contains an element named “CompositionPlaylistId” whose value matches the UUID of the CPL for which it carries content keys. The CPL identifies the (optional) content key associated with each track file by a UUID in an element called “KeyId”. The KDM has matching elements called KeyId. An unencrypted list of the KeyId values that are carried in the KDM appears in the first part of the KDM. The actual content key values (and their matching KeyId) appear in an encrypted portion of the KDM that can only be decrypted by the intended recipient (typically a Security Manager in an exhibition facility).

4.2 XML Overview of the KDM

Note: The XML figures shown in this specification are informative. See Annex B for the normative XML schema that defines the KDM. The XML diagrams in this document conform to the legend given in [ETM].

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 keys.

The KDMRequiredExtensions element contains information that must be visible without decryption in order to properly handle the KDM within D-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 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 [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 [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.

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.

5 Authenticated and Unencrypted Information

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.

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.

5.1 MessageType

The MessageType field is defined in [ETM]. In a KDM, this field shall contain the following URI:

http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type

Informative Note: The MessageType value "http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type" is legal and correct, but, in the event a future revision of the KDM specification requires a revision to the MessageType value, the MessageType value should follow the pattern http://www.smpte-ra.org/430-1/2006/KDM and match the target namespace of the schema.

5.2 RequiredExtentions

The RequiredExtentions element of the KDM shall contain exactly one KDMRequiredExtensions element, as defined in Annex B and illustrated in Figure 3. The KDMRequiredExtensions element shall have the following child elements:

5.2.1 Recipient

The Recipient element identifies the certificate associated with the intended recipient of this KDM. The public key identified in this certificate is used to encrypt keys and other information in the AuthenticatedPrivate element of the KDM. To uniquely identify the certificate, the Recipient element shall contain two elements — X509IssuerSerial and X509SubjectName. The X509IssuerSerial element identifies the name of the Certificate Authority (CA) that issued the certificate, called X509IssuerName, and the unique serial number assigned by the CA, called X509SerialNumber.

The X509SubjectName element shall contain the X.509 subject distinguished name found in the certificate. The X.509 distinguished name values in X509IssuerName and X509SubjectName elements shall be compliant with RFC2253 [RFC2253].

5.2.2 CompositionPlaylistId

This field contains a machine-readable identifier for the Rights Owner's content (such as a Composition Playlist). It is a 128-bit UUID represented in "urn:uuid:" format when used with XML [UUID].

This is an informational field that is a copy of the definitive value that appears in the RSA protected EncryptedKey structure. It may be ignored by mechanisms that process the EncryptedKey field.

5.2.3 ContentTitleText

The ContentTitleText parameter shall contain a human-readable title for the composition; e.g., When Pigs Will Fly II. It is strictly meant as a display hint to the user. The optional language attribute is an ISO 3166 language code and indicates the language used. If the language attribute is not present, the content of the field shall be English.

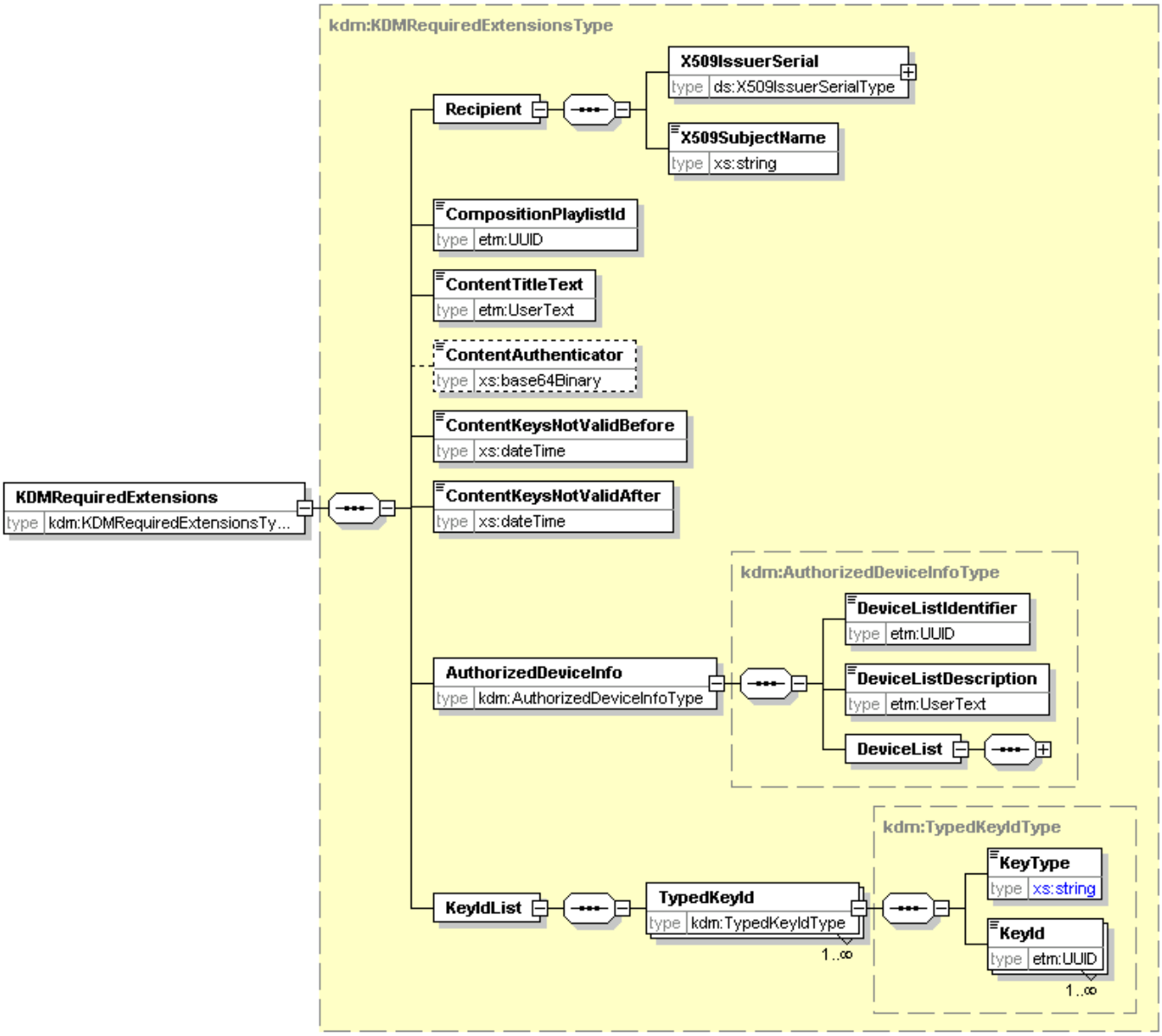

Figure 3 – KDMRequiredExtensions Element (Informative)

5.2.4 ContentAuthenticator (Optional)

This field, if present, shall contain a certificate thumbprint (defined in [D-Cinema Digital Certificate]) that supports authentication of the content as an authorized version (e.g. through a Composition Playlist [CPL]). This field may be absent at the discretion of the KDM creator (who acts on behalf of the rights owner), but it is part of the RequiredExtentions elements because compliant receiving equipment is required to understand and process it when present.

Informative Notes:

1 If this field is present, then it is intended that the recipient crosscheck the certificate chain for the signer of the CPL against this value. Specifically, one of the certificates in the signer chain of the CPL should have a certificate thumbprint that matches this field in the KDM.

2 This field facilitates the business requirement of allowing an exhibitor to show content produced by a wide range of studios without needing to have a business relationship with all those studios (e.g., without needing to know the root certificates for all studios). The exhibitor has a relationship with a set of distributors (and knows their root certificates), and the distributors in turn have relationships with studios. To support business flexibility, the ContentAuthenticator is not necessarily the thumbprint of the studio's root certificate.

3 Of course, nothing precludes an exhibitor from knowing the root certificates of specific studios and using those certificates as part of validating CPL.

5.2.5 AuthorizedDeviceInfo

This item contains three elements as described below.

Informative Note: This field is intended to support authorization of devices which process content keys delivered by the KDM, or perform other security services related to content protected by those content keys. The AuthorizedDeviceInfo field does not play any role in validating the KDM itself. This field facilitates the dual business requirements of (a) allowing exhibition equipment to be implemented as multiple secure devices (e.g. image media block, sound media block, projector) and (b) allowing a rights owner to limit delivery of his content or keys to specific trustworthy devices.

5.2.5.1 DeviceListIdentifier

This field shall contain a value uniquely identifying a list of trusted equipment. It is a required member of the AuthorizedDeviceInfo structure.

Informative Note: This field is an aid to management of device lists and tracking of updates to them.

5.2.5.2 DeviceListDescription (Optional)

The DeviceListDescription parameter, where present, shall contain a human-readable title description of the device list, e.g. "Bigtown Multiplex facility equipment list updated June 20, 2006". It is strictly meant as a display hint to the user. The optional language attribute is an ISO 3166 language code and indicates the language used. If the language attribute is not present, the content of the field shall be English.

5.2.5.3 DeviceList

The DeviceList item shall contain a set of one or more certificate thumbprints [See D-Cinema Certificate].

Informative Note: Each entry typically represents a specific device which is authorized for use in connection with some of the keys in this KDM. However, the normative behavior of receiving equipment is outside the scope of this standard.

5.2.6 ContentKeysNotValidBefore

This field specifies the time before which the content keys contained in this KDM are not valid. The time shall be 25 characters in the form of a Universal Coordinated Time timestamp as specified in RFC 3339 [Time] Section 5.6 date-time. Timestamps shall not include fractional seconds (RFC 3339 time-secfrac). Timestamps shall not use 'Z' ('Zulu') time zone offset notation. It is possible for a separate KDM to provide a different time window for the same content keys (e.g., to allow a pre-view showing, or to extend an engagement).

This is an informational field that is a copy of the definitive value that appears in the RSA protected EncryptedKey structure. It may be ignored by mechanisms that process the EncryptedKey field. The time windows of all content keys shall be the same in the RSA protected blocks.

5.2.7 ContentKeysNotValidAfter

This field specifies the time after which the content keys contained in this KDM are not valid. The time shall be 25 characters in the form of a Universal Coordinated Time timestamp as specified in RFC 3339 [Time] Section 5.6 date-time. Timestamps shall not include fractional seconds (RFC 3339 time-secfrac). Timestamps shall not use 'Z' ('Zulu') time zone offset notation. It is possible for a separate KDM to provide a different time window for the same keys (e.g., to allow a pre-view showing, or to extend an engagement).

This is an informational field that is a copy of the definitive value that appears in the RSA protected EncryptedKey structure. It may be ignored by mechanisms that process the EncryptedKey field. The time windows of all content keys shall be the same in the RSA protected blocks.

5.2.8 KeyIdList

This field shall contain 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 (see Section 6.1). It may be ignored by mechanisms that process the EncryptedKey field.

5.2.8.1 KeyId

KeyIds are 128-bit UUIDs that shall be represented in “urn:uuid:” format when they appear as an XML value [UUID]. The KeyId parameter uniquely identifies the content key. All keys shall be for use with the assets referenced by the Composition Playlist identified by the CompositionPlaylistId field. As shown below, it shall be used to identify the content key used in encrypting d-cinema assets, as defined by [KLV]. It shall be represented by a UUID [UUID].

5.2.8.2 TypedKeyId

A TypedKeyId is a compound element consisting of a KeyType field and a KeyId. The KeyType shall be a string of characters, further constrained as described below. The KeyType distinguishes keys targeted to different types of devices (e.g. image media decryptor, sound media decryptor). The KeyID shall be as defined in Section 5.2.8.1. Binding a KeyType to each KeyId assists in defending against cross-system attacks.

The KeyType element shall contain a symbol composed of four (4) characters from the set of 52 upper and lower case ASCII letters *A-Z* (0x41-0x5A) and *a-z* (0x61-0x7A).

The KeyType element shall have an optional “scope” attribute, which shall be a URI value identifying the normative reference which defines the four character key type identifier contained within the element. The default value of the scope attribute shall be the URI value “http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type”. Associated with this URI is the following set of key type identifiers:

Byte String (hexadecimal notation)	Character String	Description
4D.44.49.4B	“MDIK”	Image essence key
4D.44.41.4B	“MDAK”	Sound essence key
4D.44.53.4B	“MDSK”	Subtitle essence key
46.4D.49.4B	“FMIK”	Image forensic marking key
46.4D.41.4B	“FMAK”	Sound forensic marking key

Informative Note 1: Receiving equipment is contemplated to use the information in this field to restrict delivery of key information to devices which serve the intended D-Cinema roles. However, the normative behavior of receiving equipment is outside the scope of this document.

The scope attribute with the value "http://www.smpte-ra.org/430-1/2017/KDM#kdm-key-type" shall be associated with the following KeyType values::

Byte String (hexadecimal notation)	Character String	Description
4D.44.58.31	"MDX1"	Aux Data Type 1 key
4D.44.58.32	"MDX2"	Aux Data Type 2 key

Informative Note 2: The MDX1 and MDX2 values allow two distinct sets of security policies to be associated with essence carried in Aux Data Track Files (see [ADTF]), based on the nature of this essence. Specifically, MDX1 is intended to signal that the plaintext essence (potentially forensically marked unless forensic marking is disabled per Section 5.2.9.1) is transmitted without restrictions within the exhibition environment. In contrast, MDX2 is intended to signal that the plaintext essence (potentially forensically marked unless forensic marking is disabled per Section 5.2.9.1) is transmitted over encrypted links within the exhibition environment. Conformance to these security policies is not specified here, and is left to other documents.

The scope attribute with a value that conforms to the syntax "http://www.smpte-ra.org/430-1/2017/KDM#mic-key-type-{ID}", where {ID} conforms to the lowercase UUID string representation specified in [UUID], shall be associated with the following KeyType value:

Byte String (hexadecimal notation)	Character String	Description
4D.44.4D.4B	"MDMK"	MIC key

The {ID} shall be equal to a KeyId value within the KeyIdList element.

Informative Note 3: The MDMK key is intended to define the MICKey (see [KLV]) to be used in conjunction with the content key identifier by the UUID embedded in the scope attribute.

EXAMPLE: <KeyType scope="http://www.smpte-ra.org/430-1/2017/KDM#mic-key-type-e5421139-0f4a-445e-bc1f-3018a2a858ab">MDMK</KeyType> identifies a MIC key associated with the content key with KeyId "e5421139-0f4a-445e-bc1f-3018a2a858ab".

5.2.9 ForensicMarkFlagList (Optional)

When present, this element shall contain an unordered list of one or more ForensicMarkFlag elements, which are defined below. Each ForensicMarkFlag element in the list shall have a distinct value.

5.2.9.1 ForensicMarkFlag

A ForensicMarkFlag element shall contain a single URI value indicating whether forensic marking is to be used in conjunction with a particular KeyType contained in the KDM. The following table lists the forensic marking requirements defined by this standard:

Forensic Mark Flags	
URI value	**Requirement**
http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-picture-disable	Disable forensic marking in connection with keys of KeyType “MDIK”
http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-audio-disable	Disable forensic marking in connection with keys of KeyType “MDAK”
http://www.smpte-ra.org/430-1/2017/KDM#mrkflg-mdx1-{ID}-disable	Disable forensic marking in connection with key with KeyId equal to {ID} and of KeyType equal to "MDX1"
http://www.smpte-ra.org/430-1/2017/KDM#mrkflg-mdx2-{ID}-disable	Disable forensic marking in connection with key with KeyId equal to {ID} and of KeyType equal to "MDX2".

{ID} in the table above shall conform to the lowercase UUID string representation specified in [UUID] and shall be equal to a KeyId value of the key to which the Forensic Mark Flag applies.

EXAMPLE: http://www.smpte-ra.org/430-1/2017/KDM#mrkflg-mdx1-dfc4c132-c318-44fd-a515-d2a8075f4c5a-disable

5.3 NonCriticalExtensions

This field is defined in [ETM].

Informative Note: This element may contain proprietary extensions. Conforming implementations should ignore the contents of this element.

6 Authenticated and Encrypted Information

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.

The normative schema is defined in Annex B and the schema code snippet is illustrated in Figure 4.

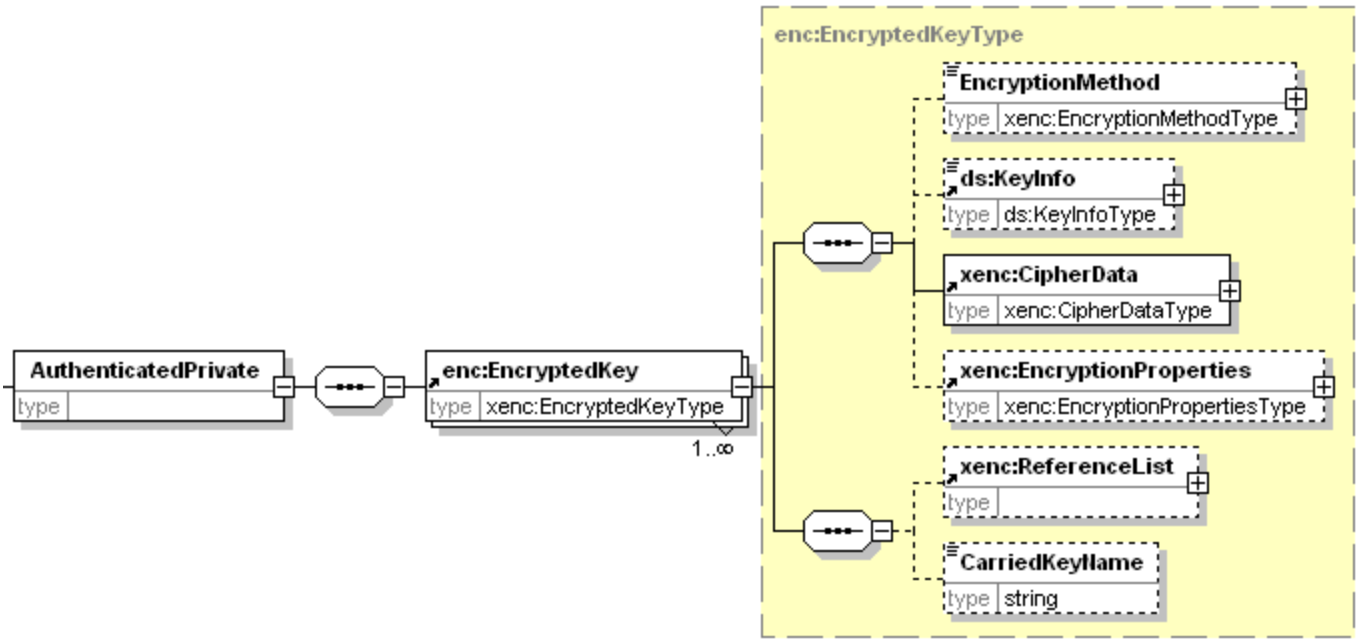

Figure 4 – Authenticated and Private Portion of KDM (Informative)

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.

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.

6.1 EncryptedKey

The RSA public key algorithm shall be used to carry the EncryptedKey data. This element (see Figure 5) contains information encrypted with the RSA public key algorithm, along with all the parameters and information needed to extract that information. It is normatively defined in [ETM] Section 6.1. Child elements of EncryptedKey not listed below shall be unchanged from their [ETM] definition.

6.1.1 KeyInfo

This field is defined in [ETM]. This field is optional for 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.

6.1.2 CipherData

The CipherData field is generally defined in [ETM]. 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 the table.

Length	Field Description
16	Structure ID. A 128-bit identifier for this structure. The value of the Structure ID shall be f1.dc.12.44.60.16.9a.0e.85.bc.30.06.42.f8.66.ab (hexadecimal).
20	Certificate Thumbprint in binary form as specified in “Certificate and Public Key Thumbprint” of [D-Cinema Digital Certificate].
16	CompositionPlaylistId, a UUID in binary form as specified in RFC 4122.
4	KeyType, a byte string of length four bytes (see Section 5.2.8.2 table).
16	KeyId, a UUID in binary form as specified in RFC 4122.
25	Not Valid Before, a UTC date-time encoded as specified in Section 5.2.6, e.g. “2004-05-01T13:20:00-00:00”.
25	Not Valid After - a UTC date-time encoded as specified in per Section 5.2.7, e.g. “2004-06-30T13:20:00-00:00”.
16	Content Key
138	**Total**

Informative Notes:

1 The “Structure ID” is a unique value within the scope of the XML namespace name declared in Section 5 above. By including a known unique plaintext value in the structure, the system is protected in the event that an attacker attempts compromise by substituting the expected encrypted key block by other data encrypted with the same public key.

2 The D-Cinema system uses 2048-bit RSA keys [D-Cinema Digital Certificate], so the ciphertext is 256-bytes long. Due to the 42-byte header that is part of the OAEP padding, the plaintext can be at most 214-bytes long.

The following three KDM validity checks are informative:

(1) The KDM recipient should check that the thumbprint of the signer’s certificate matches the signer of the KDM. If it is not correct, the KDM should be rejected. This prevents cut and paste attacks that would allow a rogue distributor to sign a KDM using the RSA blocks from the real distributor.

(2) The KDM recipient should check the Structure ID. If it is not correct, the KDM should be rejected. This prevents an RSA block that was created for a different type of message (not a KDM) from being used in a KDM.

(3) The KDM recipient 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 may choose to reject the KDM if the CompositionPlaylistId does not match in all places that it occurs in the KDM.

6.2 EncryptedData

This EncryptedData element defined in [ETM] Section 6.2 shall not be present in KDM instances.

7 Signature Information

This portion of the KDM message is defined in [ETM].

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).

Annex A Design Features and Security Goals (Informative)

This section summarizes the main design features and security goals of the KDM. Additional considerations appear in [ETM].

- A unique identifier, the KeyId is associated with each content key, allowing each encrypted D-Cinema asset, e.g. track file, to uniquely reference the key used in its encryption. A single content key can be used to protect multiple track files.

- A single message may contain multiple content keys that refer to the same content (same CompositionPlaylistId). A KeyId identifies each content key. This allows a single message to contain all the keys needed to decrypt media that uses multiple keys.

- The only standard information associated with the use of the content keys is a validity date range. All the content keys shall have the same validity range. More complex expression of licensing rights is intentionally left out of this baseline message, though it could be added in the NonCriticalExtension parameters.

- To provide extra protection for the content keys, and to enable implementations that are based on a low-end cryptographic chip that may only have 4 kilobytes of secure internal memory, the RSA public key of the recipient wraps each content key. To avoid the overhead of decrypting RSA wrapping, implementations may unwrap the content keys when the KDM is first processed and then keep the content keys locally encrypted by AES or TDES using a local (Security Manager) device key that has at least 112 bits of entropy.

- A unique identifier for the issuer, the content, and the content keys is collectively bound to the value of the content keys. This makes it harder to splice the encrypted portions of one message into another message or to take an encrypted portion that is part of some other message and make it look like a valid KDM. This can prevent an attacker who has figured out the value of one content key from forcing a component of the system to reuse that known content key.

Annex B XML Schema for KDM (Normative)

The XML Schema document presented in this appendix normatively defines the structure of a Key Delivery Message using a machine-readable language. While this schema is intended to faithfully represent the structure presented in the normative prose portions (Sections 5 and 6) of this document, conflicts in definition may occur. In the event of such a conflict, the normative prose shall be the authoritative expression of the standard.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    targetNamespace="http://www.smpte-ra.org/schemas/430-1/2006/KDM"
    xmlns:kdm="http://www.smpte-ra.org/schemas/430-1/2006/KDM"
    xmlns:etm="http://www.smpte-ra.org/schemas/430-3/2006/ETM"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xs:import namespace="http://www.smpte-ra.org/schemas/430-3/2006/ETM"
schemaLocation="./etm.xsd"/>
    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd"/>
    <xs:element name="KDMRequiredExtensions" type="kdm:KDMRequiredExtensionsType"/>

    <xs:complexType name="KDMRequiredExtensionsType">
       <xs:sequence>
          <!-- Identifies the certificate of the entity receiving the KDM. -->
          <xs:element name="Recipient">
             <xs:complexType>
                <xs:sequence>
                   <xs:element name="X509IssuerSerial" type="ds:X509IssuerSerialType"/>
                   <xs:element name="X509SubjectName" type="xs:string"/>
                </xs:sequence>
             </xs:complexType>
          </xs:element>

          <xs:element name="CompositionPlaylistId" type="etm:UUID"/>
          <xs:element name="ContentTitleText" type="etm:UserText"/>
          <xs:element name="ContentAuthenticator" type="xs:base64Binary" minOccurs="0"/>
          <xs:element name="ContentKeysNotValidBefore" type="xs:dateTime"/>
          <xs:element name="ContentKeysNotValidAfter" type="xs:dateTime"/>
          <xs:element name="AuthorizedDeviceInfo" type="kdm:AuthorizedDeviceInfoType"/>

          <xs:element name="KeyIdList">
             <xs:complexType>
                <xs:sequence>
                   <xs:element name="TypedKeyId" type="kdm:TypedKeyIdType"
maxOccurs="unbounded"/>
                </xs:sequence>
             </xs:complexType>
          </xs:element>

          <xs:element name="ForensicMarkFlagList" minOccurs="0">
             <xs:complexType>
                <xs:sequence>
                   <xs:element name="ForensicMarkFlag" type="xs:anyURI"
maxOccurs="unbounded"/>
```

```
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>

    <xs:complexType name="AuthorizedDeviceInfoType">
      <xs:sequence>
        <xs:element name="DeviceListIdentifier" type="etm:UUID"/>
        <xs:element name="DeviceListDescription" type="etm:UserText" minOccurs="0"/>
        <xs:element name="DeviceList">
          <xs:complexType>
            <xs:sequence>
<xs:element name="CertificateThumbprint" type="ds:DigestValueType" minOccurs="1"
maxOccurs="unbounded"/>                </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>

    <xs:complexType name="TypedKeyIdType">
      <xs:sequence>
        <xs:element name="KeyType">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:string">
                <xs:attribute name="scope" type="xs:anyURI" use="optional"
                    default="http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type" />
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
        <xs:element name="KeyId" type="etm:UUID"/>
      </xs:sequence>
    </xs:complexType>

</xs:schema>
```

Bibliography (Informative)

This section contains informative references that provide helpful background information.

[ASN.1] For a collection of useful links to ASN.1 resources, see:
http://www.cs.columbia.edu/~hgs/internet/asn.1.html

[CPL] SMPTE ST 429-7:2006, D-Cinema Packaging — Composition Playlist

[Base64] MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies. See: http://www.ietf.org/rfc/rfc1521.txt

[Ferguson] "Practical Cryptography" 2003 By Neils Ferguson and Bruce Schneier. Wiley Publishing, Indianapolis Indiana

[FIPS-140-2] "Security Requirements for Cryptographic Modules" Version 2, May 25, 2001. FIPS-140-2.
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[Gutmann] "X.509 Style Guide" By Peter Gutmann. See:
http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt

[IPSec] "Security Architecture for the Internet Protocol." By S. Kent, R. Atkinson. November 1998. RFC 2401. See:
http://www.ietf.org/rfc/rfc2401.txt

[NIST-KMG] "Key Management Guideline" Draft of June 3, 2002. NIST. See:
http://csrc.nist.gov/encryption/kms/guideline-1.pdf

[Rescorla] Eric Rescorla. SSL and TLS: Designing and Building Secure Systems. Addison Wesley Professional. ISBN 0201615983. October 2000

[RFC2459] "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" by R. Housley, W. Ford, W. Polk, D. Solo, January 1999. See: http://www.ietf.org/rfc/rfc2459.txt

[RFC2693] "SPKI Certificate Theory" by C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, September 1999. See: http://www.ietf.org/rfc/rfc2693.txt

[Schneier] Applied Cryptography by Bruce Schneier. Second Edition. 1996. John Wiley & Sons. ISBN 0-471-11709-9

[TLS] "The TLS Protocol Version 1.0." by T. Dierks and C. Allen. January 1999.
IETF RFC 2246. See: http://www.ietf.org/rfc/rfc2246.txt

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology — Open Systems Interconnection — The Directory: Authentication Framework, June 1997

[XML_KMS] "XML Key Management Specification (XKMS)" World Wide Web Consortium Draft April 2003.
See: http://www.w3.org/TR/xkms2/

[ISO 3166] Codes for the Representation of Names of Countries (ISO 3166-1993 (E)). See:
http://www.iso.org/iso/en/prods-services/iso3166ma/index.html

[ADTF] SMPTE ST 429-14:2014, D-Cinema Packaging — Aux Data Track File