INTERNATIONAL STANDARD

ISO 26430-1

First edition
2008-07-15

Digital cinema (D-cinema) operations —

Part 1:
Key delivery message

Opérations du cinéma numérique (cinéma D) —

Partie 1: Message de remise de clé

Reference number
ISO 26430-1:2008(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

ISO 26430-1 was prepared by the Society of Motion Picture and Television Engineers (as SMPTE 430-1-2006) and was adopted, under a special “fast-track procedure”, by Technical Committee ISO/TC 36, *Cinematography*, in parallel with its approval by the ISO member bodies.

ISO 26430 consists of the following parts, under the general title *Digital cinema (D-cinema) operations*:

— *Part 1: Key delivery message*

— *Part 2: Digital certificate*

— *Part 3: Generic extra-theater message format*

Introduction

The International Organization for Standardization (ISO) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO. Information may be obtained from:

Eastman Kodak Company
Intellectual Property Transactions
343 State Street
Rochester, NY 14650
USA

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO shall not be held responsible for identifying any or all such patent rights.

SMPTE 430-1-2006

SMPTE STANDARD

D-Cinema Operations — Key Delivery Message

Page 1 of 17 pages

Table of Contents

Page

1 Scope 3

2 Normative References 3

3 Glossary 3

4 Overview of the KDM (Informative) 4

4.1 Basic KDM Elements and D-Cinema Relationships 4

4.2 XML Overview of the KDM 6

5 Authenticated and Enencrypted Information 6

5.1 Message Type 6

5.2 RequiredExtentions 7

5.2.1 Receipt 7

5.2.2 CompositionPlaylisted 7

5.2.3 ContentTitleText 7

5.2.4 ContentAuthenticalor (Optical) 8

5.2.5 AuthorizedDeviceInfo 9

5.2.6 ContentKeysNotValidBefore 9

5.2.7 ContentKEysNotValidAfter 10

5.2.8 LeyIDList 10

5.2.9 ForensicMarkFlagList (Optional) 10

5.3 NonCriticalExtensions 11

6 Authenticated and Excrypted Information 11

6.1 EncryptedKey 12

6.1.1 KenInfo 12

6.1.2 CipherData 12

6.2 EncryptedData 13

7 Signature Information 13

Annex A Design Features and Secutiry Goals (Informative) 14

Annex B Bibliography (Informative) 15

Annex C XML Schema for KDM (Normative) 16

Copyright © 2006 by THE SOCIETY OF
MOTION PICTURE AND TELEVISION ENGINEERS
3 Barker Avenue, White Plains, NY 10601
(914) 761-1100

Approved
October 3, 2006

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 Part XIII of its Administrative practices.

SMPTE Standard 430-1 was prepared by Technology Committee DC28.

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 decryption 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 429-6-2006, D-Cinema Packaging — MXF Track File Essence Encryption

[D-Cinema Digital Certificate] SMPTE 430-2-2006, D-Cinema Operations — Digital Certificate

[ETM] SMPTE 430-3-2006, 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 decryption 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.

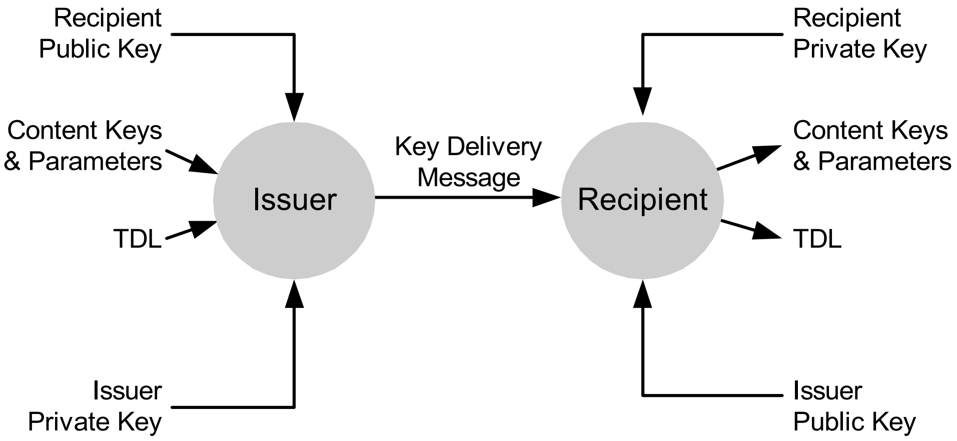

Figure 1 – KDM Information Flow

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.

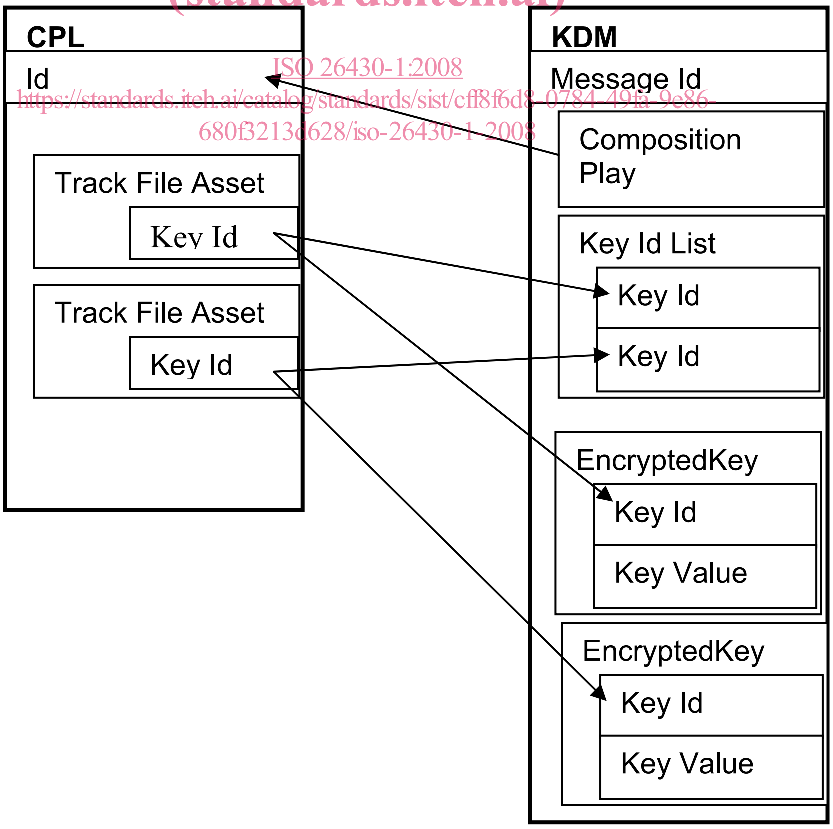

Figure 2 – Linking Between CPL and KDM Structures

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 keys. The CPL identifies the (optional) 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 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 C 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 encryption 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 decryption keys each encrypted in an EncryptedKey element. These RSA encrypted elements also include the KeyId and validity dates for each content key. The optional EncryptedData element defined in [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 decryption keys for the same content (the same CompositionPlaylistId), and a Composition Play List may require 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 C. 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

5.2 RequiredExtentions

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

5.2.1 Recipient

The Recipient field shall identify the intended certificate/subject of this KDM. The public key identified in this certificate is used to encrypt the keys found in the AuthenticatedPrivate portion of the KDM message. An X.509 certificate is identified by the name of the Certificate Authority (CA) that issued it, called IssuerName, and the unique serial number assigned by the CA, called SerialNumber. To aid in routing of KDMs, the X.509 SubjectName that is found in the certificate shall also be placed in the Recipient element. The Distinguished Name value in the X509IssuerName element shall be compliant with RFC 2253 [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.