INTERNATIONAL STANDARD

ISO 26430-3

First edition
2008-07-15

Digital cinema (D-cinema) operations —

Part 3: Generic extra-theater message format

Opérations du cinéma numérique (cinéma D) —

Partie 3: Format de message d'extra théâtre générique

Reference number
ISO 26430-3:2008(E)

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.

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

ISO 26430-3 was prepared by the Society of Motion Picture and Television Engineers (as SMPTE 430-3-2008) 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*

SMPTE 430-3-2008
Revision of
SMPTE 430-3-2006

SMPTE STANDARD

D-Cinema Operations — Generic Extra-Theater Message Format

Table of Contents

Approved
March 3, 2008

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 430-3 was prepared by Technology Committee DC28.

1 Scope

This standard presents a specification for a generic Extra-Theatre Message (ETM) format for use with unidirectional communications channels used in security communcations for Digital Cinema (D-Cinema) systems.

The ETM specification is a generic XML security wrapper that includes specific fields which can be extended to carry different kinds of information to meet various application-level requirements. (For example, the Key Delivery Message (KDM) is a specific instance of this format.) The ETM uses W3C Extensible Markup Language (see [XML]) to represent the information payload. It provides security using the XML encryption and signature primitives.

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

2 Conformance Notation

Normative text is text that describes elements of the design that are indispensable or contains the conformance language keywords: "shall", "should", or "may". Informative text is text that is potentially helpful to the user, but not indispensable, and can be removed, changed, or added editorially without affecting interoperability. Informative text does not contain any conformance keywords.

All text in this document is, by default, normative, except: the Introduction, any section explicitly labeled as "Informative" or individual paragraphs that start with "Note:"

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

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

The keywords "may" and "need not" indicate courses of action permissible within the limits of the document.

The keyword "reserved" indicates a provision that is not defined at this time, shall not be used, and may be defined in the future. The keyword "forbidden" indicates "reserved" and in addition indicates that the provision will never be defined in the future.

A conformant implementation according to this document is one that includes all mandatory provisions ("shall") and, if implemented, all recommended provisions ("should") as described. A conformant implementation need not implement optional provisions ("may") and need not implement them as described.

3 Normative References

The following standards contain provisions that, 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.

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

[FIPS-180-2] "Secure Hash Standard" Version 2. August 1, 2002. FIPS-180-2. See: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[FIPS-197] “Advanced Encryption Standard (AES)” November 26, 2001. FIPS-197. See: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[FIPS-198] “The Keyed-Hash Message Authentication Code (HMAC)” March 6, 2002. File updated April 8, 2002. http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

[PKCS1] “PKCS #1: RSA Cryptography Specifications Version 2.1” By B. Kaliski. February 2003. RFC 3447 See: http://www.ietf.org/rfc/rfc3447.txt

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

[RFC4051] ”Additional XML Security Uniform Resource Identifiers (URIs)” April 2005. See: http://www.ietf.org/rfc/rfc4051.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 Universially Unique Identifier (UUID) URN Namespace” July 2005. See: http://www.ietf.org/rfc/rfc4122.txt

[XML] “*XML Schema Part 1: Structures”* World Wide Web Consortium May 2001. See: http://www.w3.org/TR/2001/REC-xmlschema-1-20010502

[XML-Encrypt] ”XML Encryption Syntax and Processing” World Wide Web Consortium December 2002. See: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[XML-Sign] ”XML-Signature Syntax and Processing” World Wide Web Consortium February 2002. See: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

4 Glossary

The following paragraphs define the acronyms used in this document.

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

ASN.1: Abstract Syntax Notation 1.

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

FIPS: Federal Information Processing Standards of NIST.

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

IETF: Internet Engineering Task Force standards group.

IP: Internet Protocol. An IETF standard.

ISO: International Standards Organization.

KDM: Key Delivery Message – An instance of the ETM. See [SMPTE 430-1]

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. Defined in [PKCS1]

SE: Security Entity. Any Digital Cinema entity that performs cryptography.

SHA-1: Secure Hash Algorithm revision 1. Defined in [FIPS-180-2].

SHA-256: Secure Hash Algoritm. Defined in [FIPS-180-2].

SM: Security Manager.

S/MIME: Secure Multipurpose Internet Mail Extensions.

SPB: Secure Processing Block.

SSL: Secure Socket Layer protocol. See [TLS].

TCP: Transmission Control Protocol. IETF standard for reliable bi-directional streams.

TLS: Transport Layer Security protocol. See [Rescorla].

TMS: Theater Management System.

X.509: A widely used and supported digital certificate standard. Refer to [D-Cinema Digital Certificate]

XML: Extensible Markup Language.

5 Overview of Generic Extra Theater Message (informative)

Extra-Theater Messages (ETM) may be used generally between any two D-Cinema Security Entities (SE), however an ETM is particularly appropriate where a unidirectional rather than a bi-directional communications channel is employed. Such channels would be typical of those between a Distributor and an Exhibitor, or between a Studio and a Distributor. The ETM format defined in this document provides a basic message structure having a useful set of known security properties. It is intended that all D-Cinema extra-theatre messaging requirements utilize this structure in order to minimize the risk that introduction of new security messages will undermine the integrity of the security system.

The following diagram presents an overview of the generic security wrapper. The top-level XML element indicates that this structure is a D-Cinema Extra-Theatre security Message. It contains three elements (segments) for data: 1) authenticated and public (viewable by anyone who receives the message), 2) authenticated and private (viewable by the intended recipients only), and 3) authentication (signature and trust) information.

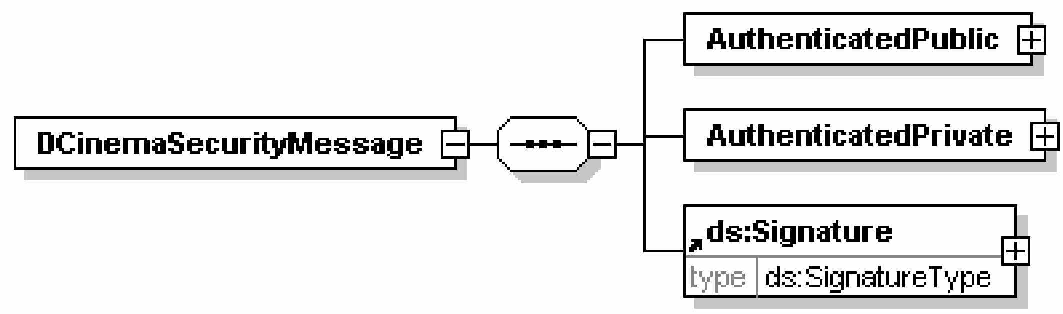

Figure 1 – XML Diagram for Generic Extra Theater Message

The AuthenticatedPublic segment includes standard message header information and a place to put required standard extension elements for the particular message type, and a place for proprietary extensions that are not critical to the baseline interoperability standard.

The single signer of the ETM is identified in the AuthenticatedPublic segment, and any entity that receives the message is able to read and authenticate the information in the AuthenticatedPublic segment. For ETMs that carry encrypted information in the AuthenticatedPrivate segment, the identity of the recipient of this private information (as specified by the issuer name and serial number of a certificate) appears in a standard field (KeyInfo) of the standard XML EncryptedKey element of the AuthenticatedPrivate segment. To avoid redundancy, the recipient information is not also carried in the AuthenticatedPublic segment.

The AuthenticatedPrivate segment includes zero or more blocks of information encrypted by RSA (called EncryptedKey) and an optional block of information encrypted by AES (called EncryptedData). The use of the EncryptedKey and EncryptedData fields is application-dependent. For example, the KDM message uses the RSA blocks in a special way and does not use the AES block. Other instances of the ETM may use the AuthenticatedPrivate segment to carry data that is hidden from all but the intended recipients. The data in this segment is encrypted with a fresh random AES key (in the EncryptedData segment), and that AES key is made available to the desired recipient in one or more EncryptedKey elements by encrypting the AES key with the public key of the recipient. The recipient has the matching private key, and so can decrypt the RSA block and recover the AES key.

The Signature segment includes 1) the value of the signer's certificate chain (note that the identity of the signer appears in the AuthenticatedPublic segment), 2) a SignedInfo segment that separately specifies the expected hash of the AuthenticatedPublic and AuthenticatedPrivate parts (this allows any entity that handles this message to detect tampering, even if it is not the intended recipient), and 3) an RSA signature on the SignedInfo element, which thus authenticates the two expected hash values that in turn authenticate the AuthenticatedPublic and AuthenticatedPrivate portions. The Signature segment is not itself authenticated, though it is believed if an attacker made any modifications to the Signature section, then the authentication of the other sections would fail.

To facilitate parsing, the ETM is represented with the UTF-8 character set. All strings intended for human display include a language attribute that is used to select an appropriate character set to display the UTF-8 string contents. All date-time values are expressed in UTC format. The cryptographic mechanisms and structures are from the XML standards for encryption and digital signatures.

6 Authenticated and Public (Unencrypted) Information

The information in this segment of the ETM shall be digitally signed, and trust in the signature can be verified using the certificate chain in the Signature portion. This segment shall not be 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 portion means that any entity that receives the message can view this portion.

The formal XML definition is given in Annex C. Figure 2 is an informative illustration of the appropriate code section from that annex.

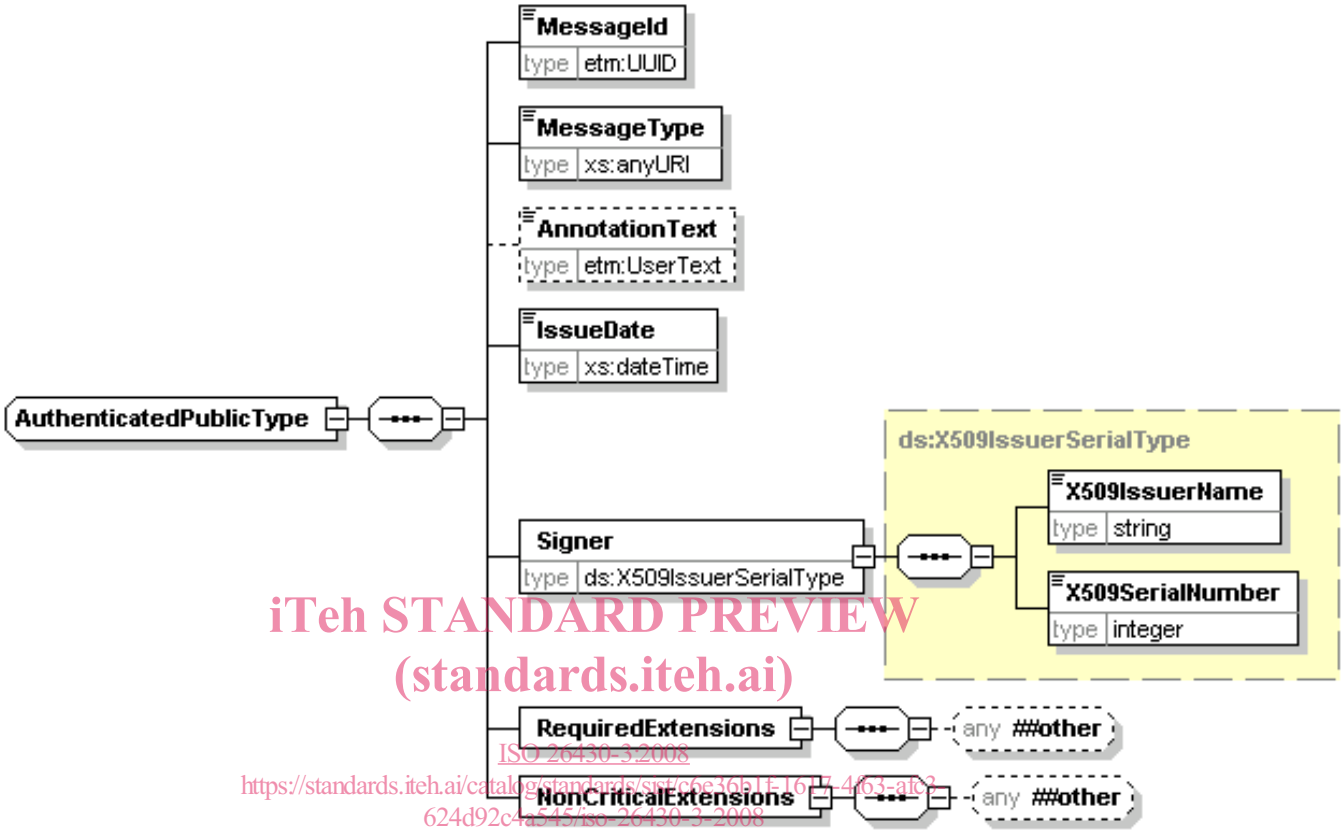

Figure 2 – Authenticated and Public Portion of ETM (Informative)

6.1 MessageId

The MessageId field shall be a globally unique identifier for a given ETM that is chosen by the creator of the message. In other words, no two otherwise different messages shall share the same Id. This value is helpful for logging, tracking and indexing ETM messages. It is in the “urn:uuid” format that is also used with the D-Cinema packing list and composition play list standards.

6.2 MessageType

The MessageType field identifies the specific version and type of the message. It is a URI string that identifies the namespace for the particular ETM instance specification being represented.

6.3 AnnotationText

The optional AnnotationText field contains a human-readable description of the message. It is not used in any security-related process and is only meant as a display hint to human users. Unless the optional xml:lang attribute is specified, the content of the field shall be en. If humans need to troubleshoot a problem related to