INTERNATIONAL STANDARD

ISO 26430-2

First edition
2008-09-01

Digital cinema (D-cinema) operations —

Part 2: Digital certificate

Opérations du cinéma numérique (cinéma D) —

Partie 2: Certificat numérique

Reference number
ISO 26430-2:2008(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.

ISO 26430-2 was prepared by the Society of Motion Picture and Television Engineers (as SMPTE 430-2-2006) 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 430-2-2006

SMPTE STANDARD

D-Cinema Operations — Digital Certificate

Table of Contents

Page

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 430-2 was prepared by Technology Committee DC28.

Introduction

This standard presents a specification for Digital Certificates used in a D-Cinema system. These certificates are used to help secure communications both within an exhibition facility and between business entities (Studios, Distributors and Exhibitors). This standard defines the Digital Certificate format and associated processing rules in sufficient detail to enable vendors to develop and rollout interoperable security solutions for D-Cinema.

This Digital Certificate standard is based on a constrained form of the X.509v3 format and processing rules. X.509v3 certificates have been widely used in other well-respected security standards such as SSL/TLS secure internet access, IPSec Virtual Private Networks and S/MIME secure email. The specific constraints on the X.509v3 format are chosen to reduce the amount of time and implementation effort required to achieve interoperability with high security and yet provide a robust flexible foundation that can support future enhancements. These certificates support a simple yet flexible trust model without having to introduce new business entities. Specifically, there is no need to create an industry wide certification lab, though one could be supported.

These certificates are used in several D-Cinema standards. They are used to provide authenticity and integrity for Composition Play Lists [CPL] and Packing Lists [PL]. They provide authenticity, integrity and confidentiality in Extra-Theatre Messages [ETM] such as the Key Delivery Message [KDM], and they are used with the TLS session security protocol to protect Intra-Theater Messages.

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

1 Scope

This standard presents a specification for Digital Certificates for use in D-Cinema systems. The standard defines the Digital Certificate format and associated processing rules in sufficient detail to enable vendors to develop and implement interoperable security solutions. In the D-Cinema environment, certificates have these primary applications:

- Establishing identity of security devices
- Supporting secure communications at the network layer (e.g. TLS) or application-messaging layer (e.g., Extra Theater Messages [ETM])
- Authentication and integrity requirements for Composition Play Lists (CPL) and Packing Lists (PL)

The Digital Certificate standard is based on a constrained form of the X.509v3 [X.509] format and processing rules. Only the most widely supported features of X.509v3 are used in order to give vendors a large selection of X.509v3 development toolkits and certificate issuing products. The constraints also avoid the complexity and ambiguity that often occurs in systems that use X.509v3 certificates.

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.

[ASN.1] ISO/IEC 8824-1:2002 (ITU-T X.680, Information Technology) - Abstract Syntax Notation One (ASN.1). See: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35684

[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

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

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

[RFC4055] “Additional Algorithms and Identifiers for RSA Cryptography for Use in the Internet X.509 Public Key Infrastructure” by J. Schaad, B. Kaliski, R. Housley, June 2005. See: http://www.ietf.org/rfc/rfc4055.txt

[RFC3280] “Internet X.509 Public Key Infrastructure Certificate and CRL Profile” by R. Housley, W. Ford, W. Polk, D. Solo, April 2002. See: http://www.ietf.org/rfc/rfc3280.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

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997. See: http://www.itu.int/ITU-T/asn1/database/itu-t/x/x509/1997/

3 Glossary

The following paragraphs define the acronyms used in this standard.

ASN.1: Abstract Syntax Notation 1.
BER: Basic Encoding Rules for ASN.1 structures. There are multiple BER encodings for a given value.
Base64: A printable encoding of binary data. Defined in [Base64].
CA: Certificate (issuing) Authority
DC: Digital Cinema.
DER: Distinguished Encoding Rules for ASN.1 structures. These rules create a canonical representation.
ETM: Extra Theatre Message.
FIPS: Federal Information Processing Standards of NIST.
IETF: Internet Engineering Task Force standards group.
IP: Internet Protocol. An IETF standard.
ISO: International Standards Organization.
LE: Link Encryptor.
LD: Link Decryptor.
MD: Media Decryptor.
NIST: National Institute of Standards and Technologies.
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.
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: Theatre Management System.
X.509: A widely used and supported digital certificate standard.
XML: Extensible Mark-up Language.

4 Overview of Digital Certificates (Informative)

Digital certificates provide a way for a D-Cinema device to start with a small amount of trustworthy information and use that to verify the trustworthiness of additional information. Certificates also support the privacy, integrity and authenticity of communications.

The certificate for a security device is a statement signed by the vendor of the device saying “If you speak to an entity that can prove that it has current access to the private key that matches the public key in this certificate, then I, the vendor of the device, state that the entity has the following attributes.” The body of the certificate lists attributes such as the make, model and serial number of the device, and the D-Cinema roles supported by the device.

For reasons of scaling and security, equipment vendors need not directly sign the certificates of devices. Instead there may be one or more intermediate certificates in a chain. The vendor’s primary certificate is the “root” of this chain (called the root certificate), and the device’s certificate is the “leaf-end” of the chain. The

public key in the vendor's root certificate (which is self-signed) may be used to verify the attributes in an intermediate certificate. Those attributes include the public key of the intermediate Certificate issuing Authority (CA), which is then used to verify the next certificate in the chain, and so forth. Eventually, the public key from the last CA certificate in the chain is used to verify the device's certificate, and thus establish the trustworthiness of the attributes in the certificate (including the device's public key).

Devices that perform certificate chain validation assume that the vendor has established good policies and procedures for securely operating the CAs in the chain, which should make it unlikely that an attacker will be able to create fraudulent certificates. The name of the organization that owns the root certificate appears in all the certificates in the chain and this serves as an indication of the quality of the policies and procedures.

5 Certificate Fields

D-Cinema certificates shall use the standard X.509 (version 3) (see [X.509]) format in constrained ways defined in this standard in order to reduce the complexity and ambiguity that often occurs in systems that used X.509 certificates. This section defines those constraints.

5.1 Required Fields

This section specifies the required fields in D-Cinema certificates. The following table summarizes the required fields. Table 1 describes the detailed constraints for each field. The certificate shall be encoded (converted to bytes) using the ASN.1 DER rules (see [ASN.1], [Kaliski]), which produce a unique representation for the certificate.

Table 1 – Required X.509v3 fields for Digital Cinema Certificates

Field	Description
The first two fields shall appear outside of the signed portion of the certificate.	
SignatureAlgorithm	Identifier of the algorithm used to sign this certificate. Must be same as signature field inside the certificate.
SignatureValue	Value of the signature for the certificate.
The following fields are inside the signed portion of the certificate. The fields after the SubjectPublicKeyInfo field shall appear in the "extensions" part of the signed portion.	
Version	Indicates X.509 Version 3 format certificates.
SerialNumber	Serial number of certificate that is uniquely chosen by the Issuer.
Signature	Identifier of the signature algorithm. It appears inside the signed portion of the certificate and must match the algorithm identified on the outside in the SignatureAlgorithm field.
Issuer	Name of entity that issued and signed this certificate.
Subject	Name of the entity that is the subject of this certificate and thus controls access to the private key that corresponds to the public key that appears in this certificate.
Validity	Date/Time range when the certificate is valid.
SubjectPublicKeyInfo	Information about the subject's public key including the algorithm type, any algorithm parameters and the set of values that makes up the public key, such as modulus and public exponent for RSA.
AuthorityKeyIdentifier	This field identifies the issuer's certificate.
KeyUsage	Collection of flag bits that identify all the operations that are authorized to be performed with the public key in this certificate, and thus imply what can be done with the corresponding private key.
BasicConstraint	This field indicates whether certificate signing is allowed and specifies the maximum number of certificate signing certificates that can appear in the chain below this one.

D-Cinema certificates may contain other extension fields that are meaningful to equipment from specific vendors. All implementations shall ignore extensions (i.e. fields other than the above specified required fields) that they do not understand.

5.2 Field Constraints

Table 2 describes the constraints on the required fields.

Table 2 – Field Constraints for Digital Cinema Certificates

X.509 Field	Description
SignatureAlgorithm	Shall be sha256WithRSAEncryption, which is the algorithm identifier for encrypting a SHA-256 (see [FIPS-180-2]) digest of the certificate body with RSA using PKCS #1 v1.5 signature padding (see [PKCS1]).
SignatureValue	This field is an ASN.1 Bit String that contains a PKCS #1 signature block. It shall contain a SHA-256WithRSA signature (see [RFC4055]).
Version	Shall indicate X.509 Version 3 format certificates.
SerialNumber	Unique number assigned by Issuer. Shall be an unsigned integer value that is 64-bits in length or less.
Signature	Shall be sha-256WithRSAEncryption algorithm identifier.
Issuer	Globally unique name of entity that issued and signed this certificate. See section on Naming and Roles, for further constraints.
Subject	Globally unique name of the entity that controls access to the private key that corresponds to the public key of this certificate. See section on Naming and Roles, for further constraints.
Validity	The issuer shall always encode certificate validity dates through the year 2049 as UTCTime (two digit years); certificate validity dates in 2050 or later shall be encoded as GeneralizedTime (four digit years). ([Time])
SubjectPublicKeyInfo	This shall describe an RSA public key. The RSA public modulus shall be 2048-bits long. The public exponent shall be 65537. The same public key may appear in multiple certificates. Certificate issuers should try to ensure that when a public key appears in multiple certificates, those certificates correspond to the same entity or device.
AuthorityKeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	Shall be present in all certificates, including root certificates. These attributes are the unique identifier for the issuer's certificate. They name the issuer of the issuer's certificate and the serial number assigned by the issuer's issuer.
KeyUsage	Shall be present in all certificates, including root certificates. For certificate signing certificates, only the KeyCertSign flag shall be true. For leaf certificates the DigitalSignature and KeyEncipherment flags shall be true. Other flags may be true.
BasicConstraint	This field shall be present in all certificates. When present, the CA attribute shall be true only for certificate signing certificates. For D-Cinema security devices in theatres, the CA attribute shall be false, and the PathLenConstraint shall be absent (or zero). See example in 6.2.5.

5.3 Naming and Roles

This section defines the semantics of the attributes that appear in the Issuer name field and the Subject name field of D-Cinema certificates.

Each entity that is the subject or issuer of a D-Cinema certificate is unambiguously identified by a number of attributes. In order to enable the mapping of these attributes into the X.509 name structure, this specification overloads the semantics of the X.509 name attributes, as summarized in Table 3. Overloading was chosen rather than defining new attribute types in order to facilitate implementation with widely available services and toolkits.

Table 3 – Mapping of D-Cinema Identity Attributes to X.509 Name Attributes

D-Cinema Attribute	X.509 Name Attribute	Description
Public Key Thumbprint	dnQualifier	Unique thumbprint of the public key of the entity issuing the certificate or being issued the certificate.
n/a	CountryName	This X.509 name attribute shall not appear in D-Cinema certificates.
Root Name	OrganizationName	Name of the organization holding the root of the certificate chain.
Organization Name	OrganizationUnitName	Name of the organization to which the issuer or subject of the certificate belongs. This field does not identify the end owner or facility; rather it identifies the device maker.
Entity Name	CommonName	Entity issuing the certificate or being issued the certificate. See Entity Name and Roles section.

5.3.1 Public Key Thumbprint (DnQualifier)

Exactly one instance of the DnQualifier attribute shall be present in the Subject name and the Issuer name. It is a Base64 PrintableString encoding of a Public Key Thumbprint described in section 5.4.

When the DnQualifier appears in the Subject name field, it is the thumbprint of the subject public key that appears in this certificate. When the DnQualifier appears in the Issuer name field, it is the thumbprint of the public key that is used to verify the signature on this certificate (i.e., the thumbprint of the public key that appears in the issuer's certificate).

This field is included to solve various security problems that can arise in an architecture that supports multiple root certificates.

5.3.2 Root Name (OrganizationName)

The specification in this document implies that there will be multiple roots of trust for naming entities. The OrganizationName identifies the entity that is responsible for the root of trust for this certificate.

Exactly one instance of the OrganizationName attribute is required in the Subject name and the Issuer name. It shall be a PrintableString. It should be a meaningful (to humans) name of the organization that is providing the root of trust for all certificates in this chain. There may be multiple roots of trust. The OrganizationName in the Issuer field shall match the OrganizationName in the Subject field. This means that the OrganizationName shall be the same in all certificates that chain back to the same root.

The OrganizationName attribute shall be unique. Vendors can choose their own value for this field as long as it does not match that of another vendor. The values of this field should be chosen to be sufficiently distinct that a human would not confuse two similar names. This name actually identifies the root of trust for the system that issues certificates for D-Cinema entities, so it is more specific than the name of the organization that owns the issuing system. For example, a name like "DC.CA.BigBlue.Com" would be a better name than

