

Digital cinema (D-cinema) operations

Part 2: Digital certificate

ICS 35.040; 37.060.99

National foreword

This British Standard is the UK implementation of ISO 26430-2:2008.

The UK participation in its preparation was entrusted to Technical Committee CPW/36, Cinematography.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2009

© BSI 2009

ISBN 978 0 580 60228 3

Amendments/corrigenda issued since publication

Date	Comments

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)

AVA Documents
Document Sharing Hub
© ISO 2008

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 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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 STANDARD

D-Cinema Operations — Digital Certificate



Table of Contents	Page
1 Scope	3
2 Normative References	3
3 Glossary	3
4 Overview of Digital Certificates (Informative).....	4
5 Certificate Fields	5
5.1 Required Fields.....	5
5.2 Field Constraints	6
5.3 Naming and Roles	6
5.3.1 Public Key Thumbprint (DnQualifier)	7
5.3.2 Root Name (OrganizationName)	7
5.3.3 Organization Name (OrganizationUnitName)	8
5.3.4 Entity Name and Roles (CommonName)	8
5.4 Certificate and Public Key Thumbprint	8
6 Certificate Processing Rules.....	8
6.1 Validation Context.....	9
6.2 Validation Rules	9
6.3 Human Verification (Informative)	11
Annex A CommonName Role Descriptions (Informative).....	12
Annex B Design Features and Validation Context Considerations (Informative).....	14
Annex C Bibliography (Informative)	16
Annex D Example D-Certificate (Informative).....	17

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/x509/1997/>

3 Glossary

The following paragraphs define the acronyms used in this standard.