

---

---

**Digital cinema (D-cinema) operations —**  
**Part 1:**  
**Key delivery message**

*Opérations du cinéma numérique (cinéma D) —*  
*Partie 1: Message de remise de clé*



**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](mailto:copyright@iso.org)  
Web [www.iso.org](http://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 STANDARD

SMPTE 430-1-2006

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 Encrypted Information .....                | 6    |
| 5.1 Message Type .....                                         | 6    |
| 5.2 RequiredExtensions .....                                   | 7    |
| 5.2.1 Receipt .....                                            | 7    |
| 5.2.2 CompositionPlaylisted .....                              | 7    |
| 5.2.3 ContentTitleText .....                                   | 7    |
| 5.2.4 ContentAuthenticator (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 Exrypted 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 Security Goals (Informative) ..... | 14   |
| Annex B Bibliography (Informative) .....                       | 15   |
| Annex C XML Schema for KDM (Normative) .....                   | 16   |

## **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.