
Digital cinema (D-cinema) operations —
Part 6:
Auditorium security messages for intra-
theater communications

Opérations du cinéma numérique (cinéma D) —

*Partie 6: Messages de sécurité de salle pour les communications à
l'intérieur du théâtre*



Reference number
ISO 26430-6:2009(E)



Documents

Document Sharing Hub
© ISO 2009

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 2009

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.

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 26430-6 was prepared by the Society of Motion Picture and Television Engineers (as SMPTE 430-6-2008) 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* [equivalent to SMPTE 430-1]
- *Part 2: Digital certificate* [equivalent to SMPTE 430-2]
- *Part 3: Generic extra-theater message format* [equivalent to SMPTE 430-3]
- *Part 4: Log record format specification* [equivalent to SMPTE 430-4]
- *Part 5: Security log event class and constraints* [equivalent to SMPTE 430-5]
- *Part 6: Auditorium security messages for intra-theater communications* [equivalent to SMPTE 430-6]
- *Part 9: Key delivery bundle* [equivalent to SMPTE 430-9]

Introduction

This part of ISO 26430 comprises SMPTE 430-6-2008 and Annex ZZ (which provides equivalences between ISO standards and SMPTE standards referenced in the text).

SMPTE STANDARD

D-Cinema Operations — Auditorium Security Messages for Intra-Theater Communications



Page 1 of 18 pages

Table of Contents	Page
Foreword	2
1 Scope	3
2 Conformance Notation	3
3 Normative References	3
4 Glossary	4
5 Overview (Informative)	4
6 Message Security, RRP Structure and General Requirements	5
6.1 Message Security: Transport Layer Security (TLS)	5
6.2 Message Structure: Key-Length-Value (KLV)	5
6.3 General ASM Command Elements	6
6.4 General TLS and RRP Requirements for Auditorium Security Messages	6
7 General Purpose ASM Commands	7
7.1 BadRequest Response	8
7.2 GetTime	8
7.3 GetEventList	9
7.4 GetEventID	10
7.5 QuerySPB	10
8 Link Encryption ASM Commands	11
8.1 LEKeyLoad	12
8.2 LEKeyQueryID	13
8.3 LEKeyQueryAll	14
8.4 LEKeyPurgeID	14
8.5 LEKeyPurgeAll	15
Annex A Auditorium Security Messages Variable Length Universal Label (UL) Key (Normative)	16
Annex B Bibliography (Informative)	18

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 430-6 was prepared by Technology Committee DC28.

1 Scope

The Auditorium Security Message (ASM) specification enables interoperable communication of security-critical information (information necessary to ensure security of D-Cinema content) between devices over an intra-theater exhibition network. The specification uses Transport Layer Security (TLS) for authentication and confidentiality, and Key-Length-Value (KLV) coding for message encoding. It defines a protocol, a general purpose request-response message set and a specific message set for link encryption keying.

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 which, through reference in this text, constitute provisions of this recommended practice. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this recommended practice are encouraged to investigate the possibility of applying the most recent edition of the standards indicated below.

[336M] SMPTE 336M-2007, Data Encoding Protocol Using Key-Length-Value

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

[IANA] Internet Assigned Numbers Authority. See www.iana.org/assignments/port-numbers

[KDM] SMPTE 430-1-2006, D-Cinema Operations — Key Delivery Message

[Log] SMPTE 430-5-2008, D-Cinema Packaging — Security Log Event Class and Constraints

[TLS] "The TLS Protocol, Version 1.0" RFC 2246 See www.ietf.org/rfc/rfc2246.txt

[TLS-AES] "AES Cyphersuites for TLS" RFC 3268 See www.ietf.org/rfc/rfc3268.txt

4 Glossary

The following acronyms are used in this specification:

ASM	Auditorium Security Message
AES	Advanced Encryption Standard
BER	Basic Encoding Rules (ASN.1)
CBC	Cipher Block Chaining
IMB	Image Media Block
KLV	Key Length Value
LDB	Link Decryptor Block
LE	Link Encryption
RRP	Request Response Pair
RSA	Rivest Shamir Adleman public key encryption
SHA-1	Secure Hash Algorithm revision 1
SM	Security Manager
SPB	Secure Processing Block
TLS	Transport Layer Security
Uinx	Unsigned x bit integer
UL	Universal Label
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier (ISO 11578)

5 Overview (Informative)

Exhibition security equipment configurations which employ remote Secure Processing Blocks (SPBs) (i.e., SPBs which are remote from that which contains the Security Manager) require a secure method of communicating with such SPBs. The generic model for this is illustrated in Figure 1.

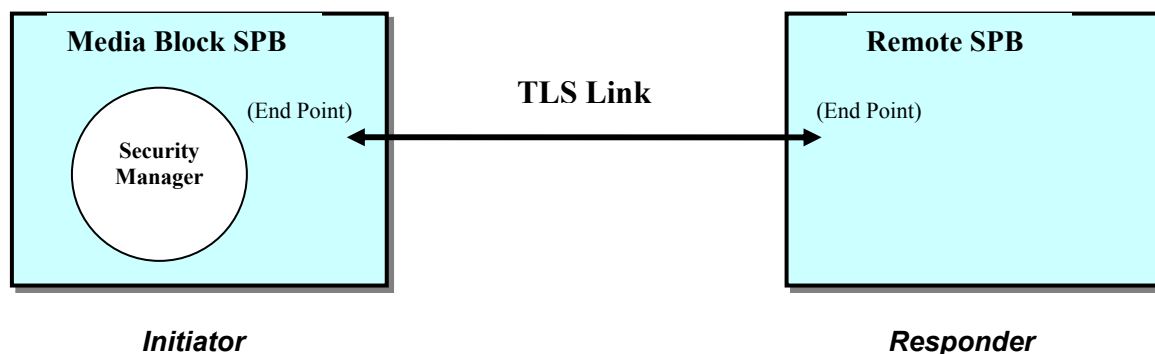


Figure 1 – Auditorium Security Message Model