INTERNATIONAL STANDARD

ISO 26430-6

First edition
2009-12-15

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)

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 430-6-2008

SMPTE STANDARD

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

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 430-6 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
Uintx	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.

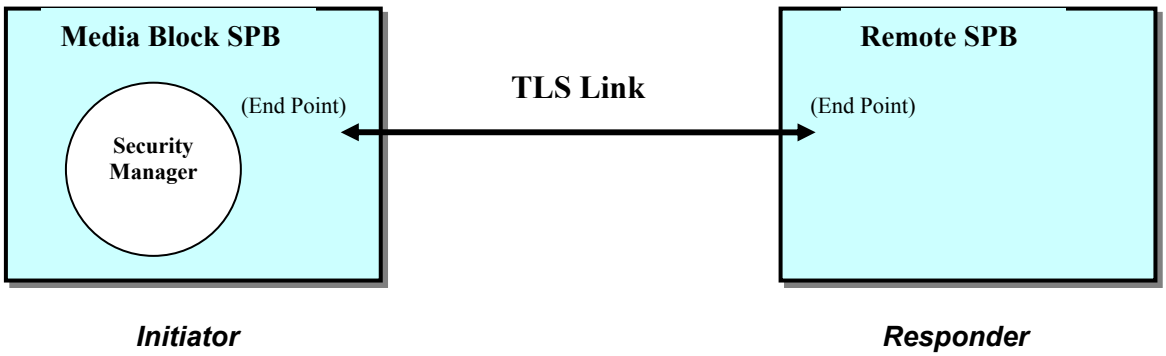

Figure 1 – Auditorium Security Message Model

The communication security protection mechanism needs to provide (1) confidentiality, (2) integrity, (3) authentication and (4) prevention of replay. In addition, the mechanism needs to be inexpensive to implement, and simple to support in secure silicon processors.

Message descriptions are given in terms of the Initiator and Responder (and this specification makes no distinction between messages emanating from the Security Manager vs. the Image Media Block that contains it). As used herein the generic name for a "block" is SPB.

6 Message Security, RRP Structure and General Requirements

The implementation of Auditorium Security Messages (ASM) shall be in the form of a "Request" from the Initiator followed by a "Response" from the Responder (recipient SPB). Each pair of messages is referred to as a Request-Response Pair (RRP).

6.1 Message Security: Transport Layer Security (TLS)

Message security shall be provided by communicating ASMs under Transport Layer Security (TLS) (see [TLS]). During TLS session establishment, the Initiator (which contains the Security Manager) and Responder exchange their X.509 certificates as part of the initial TLS handshake. This exchange shall be supported using D-Cinema compliant certificates as defined in the D-Cinema Digital Certificate specification [DCert].

The TLS protocol is constrained to simplify implementation, facilitate interoperability and ensure predictable processing:

- The protocol shall be TLS 1.0.
- 2048-bit RSA using a public exponent value of 65537 shall be the only supported public key algorithm.
- AES-CBC 128-bit shall be the only supported symmetric cipher (see [TLS-AES]).
- SHA-1 shall be the only supported hash algorithm.
- The CipherSuite shall be "TLS_RSA_WITH_AES_128_CBC_SHA" (0x00, 0x2F) (see [TLS-AES]).
- The TLS record size shall equal 512 bytes.
- The Compression Method shall be "null" (no compression).
- Other than as part of the opening handshake, the ChangeCipherSpec message shall be ignored.

6.2 Message Structure: Key Length Value (KLV)

Request and Response ASMs shall be Key Length Value (KLV) encoded using Fixed Length Pack encoding according to SMPTE 336M-2001 [336M]. The Fixed Length Universal Label (UL) Key is given in Annex A of this document. As a Fixed Length Pack, each individual item in the Value field comprises only an item value. The KLV Length field shall be a long-form BER value encoded with a fixed length of 4 bytes total.

Example: For a KLV packet having a Value field that is 12 bytes in length, the Length field would be encoded as the following 4 bytes, 0x83 0x00 0x00 0x0C (hexadecimal).

Each ASM Request-Response Pair (RRP) represents two message types and thus KLV UL "value" registration is required twice for each defined RRP (see Annex A).

Informative Note: The recipient of each RRP Request or Response command is implicit by virtue of the TLS socket (which is known at the applications level) that carries the messages.

6.3 General ASM Command Elements

For each message type, the following shall apply:

- The command type is denoted within the opening KLV “Key” field (16 bytes).
- “Length” is a BER-encoded four byte field which describes the length of the message in bytes.
- “Request_ID” shall be an application level tag for the Request, which shall be echoed by the corresponding Response. A non-zero Request_ID value shall be set by the SM, which should select unique values (e.g. a sequencing counter) for each TLS connection it manages. (Request_ID generation means is left to implementers and is out of scope of this specification.)
- Multi-byte integer values shall be sent as big-endian data, meaning most significant byte first.

General “Response” elements for each Response command are defined as follows:

General Response Elements

Element	Meaning	UInt8 Value	
RRP successful	Request successfully processed	0	
RRP failed	Responder unable to process Request	1	
RRP Invalid	Invalid parameter or command structure	2	
ResponderBusy	Responder too busy to process Request	3	

Messages defined in this document may contain batches. A batch is a compound data type that is created from combinations of simple data types. It is usually preceded by a name (e.g. an EventIDBatch is an unordered batch of Event ID values):

Batch: A compound type comprising multiple individual elements. The elements are unordered, the type is defined, the count of elements is explicit and the size of each element is fixed and explicit.

xxxBatch: A batch of zero or more individual elements of name “xxx” preceded by a header of 8 bytes. The first 4 bytes of the header define the number of elements to follow and the second 4 bytes define the length of each element, both represented as UInt32.

Item Name	Type	Len	UL	Meaning	Default
Number of Items	Uint32	4	n/a	The number of Items in the Batch	n
Item Length	Uint32	4	n/a	The length of each Item	L
First component of first instance of xxx	...	...		First of one or more components describing element ‘xxx’ and having a total length of L	...

6.4 General TLS and RRP Requirements for Auditorium Security Messages

This section defines implementation constraints for security assurance, interoperability, RRP contention management and serendipity with other exhibition subsystems which may use network resources shared by these security functions.

1. TLS sessions shall be established by the Initiator following the standard applications level TLS handshake protocol using mutual authentication mode (see [TLS]). Mutual authentication shall exchange both TLS client (Initiator) and server (Responder) D-Cinema compliant certificates.

   Informative Note: Certificate utility at each TLS end point is out of scope of this specification; however the purpose of mutual authentication is to enable the Responder (remote SPB) to receive the Initiator's (Image Media Block) certificate to record its thumbprint for logging purposes.

2. RRP protocols shall be synchronous (i.e., each pairing shall be opened and closed before a new RRP is opened between the same two SPBs). To avoid hang-ups, RRP Responder implementations should be designed to support maximum round-trip Request-to-Response latencies as specified in the message definition sections below. Latency shall be measured from the end of the "Request" message receipt to the start of the "Response" message transmission. Responders unable to transmit the Response within the specified limit because of a "busy" condition should close that RRP duple by issuance of a BadRequest Response with the general Response element indicating "busy" per the General Response Elements table in Section 6.3.

   Informative Note: Should the Responder fail to respond (at all) after the specified time limit, the Initiator may consider this a communications failure condition and may, for instance, close and restart the TLS session.

3. SMPTE standardized ASM security messages shall use well-known port 1173, which has been reserved for D-Cinema "security" RRPs by the Internet Assigned Numbers Authority (see [IANA]).

   Informative Note: Non-standardized, or non-security related RRPs may exist to support other functionality, however such RRPs should use a different port.

7 General Purpose ASM Commands

This section defines ASM commands which support remote SPBs generally (i.e. independently of the specific type of SPB or contained security functions). Table 1 shows these commands together with the names as recorded in the SMPTE UL metadata registries.

Request-Response round trip latency – Per item (2) of Section 6.4, Responder implementations should support a maximum round-trip Request-to-Response latency of 2 seconds for general purpose ASM commands.

Table 1 – General Purpose ASM Command Types

General Purpose ASM Commands	SMPTE Metadata General Purpose ASM Command UL Name
BadRequest Request	Bad Request Response
GetTime_ Request	Time Request
GetTime Response	Time Response
GetEventList Request	Event List Request
GetEventList Response	Event List Response
GetEventID Request	Event ID Request
GetEventID Response	Event ID Response
QuerySPB Request	Secure Processing Block Query Request
QuerySPB Response	Secure Processing Block Query Response