

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



| Table of Contents                                                                               | Page |
|-------------------------------------------------------------------------------------------------|------|
| Foreword .....                                                                                  | 2    |
| Intellectual Property .....                                                                     | 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 .....                     | 7    |
| 7 General Purpose ASM Commands .....                                                            | 7    |
| 7.1 BadRequest Response .....                                                                   | 8    |
| 7.2 GetTime .....                                                                               | 9    |
| 7.3 GetEventList .....                                                                          | 9    |
| 7.4 GetEventID .....                                                                            | 10   |
| 7.5 QuerySPB .....                                                                              | 11   |
| 7.6 GetProjCert .....                                                                           | 12   |
| 8 Link Encryption ASM Commands .....                                                            | 12   |
| 8.1 LEKeyLoad .....                                                                             | 13   |
| 8.2 LEKeyQueryID .....                                                                          | 14   |
| 8.3 LEKeyQueryAll .....                                                                         | 14   |
| 8.4 LEKeyPurgeID .....                                                                          | 15   |
| 8.5 LEKeyPurgeAll .....                                                                         | 16   |
| Annex A Auditorium Security Messages Variable Length Universal Label (UL) Key (Normative) ..... | 17   |
| Annex B Bibliography (Informative) .....                                                        | 19   |
| Annex C Explanation of TLS Length Constraints .....                                             | 20   |

## 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 ST 430-6 was prepared by Technology Committee 21DC.

## Intellectual Property

At the time of publication no notice had been received by SMPTE claiming patent rights essential to the implementation of this Standard. However, attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. SMPTE shall not be held responsible for identifying any or all such patent rights.

## 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](http://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](http://www.ietf.org/rfc/rfc2246.txt)

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

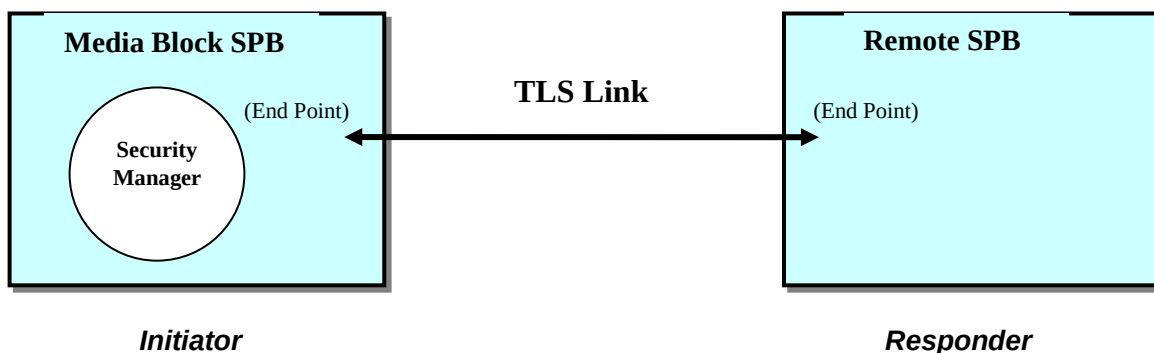


**Figure 1 – Auditorium Security Message Model**

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 shall be TLS 1.0 [TLS] constrained as follows to simplify implementation, facilitate interoperability and ensure predictable processing:

1. 2048-bit RSA using a public exponent value of 65537 shall be the only supported public key algorithm.
2. AES-CBC 128-bit shall be the only supported symmetric cipher (see [TLS-AES]).
3. SHA-1 shall be the only supported hash algorithm.
4. The CipherSuite shall be “TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA” (0x00, 0x2F) (see [TLS-AES]).
5. The TLSCiphertext.length ([TLS] section 6.2.3.) shall be less than or equal to 512 bytes (see Annex C).
6. The Compression Method shall be “null” (no compression).
7. Other than as part of the opening handshake, the ChangeCipherSpec message shall be ignored.
8. When performing TLS handshake mutual authentication, it shall be permissible for the TLS client and server devices to exchange only the respective SPB device leaf certificate.

### 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).

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.
- “Event ID” shall be a 32-bit value divided into two components:
  - o A 13 bit “Event Log” component:  
The Event Log shall be generated in a sequential (increasing) manner in order to match the Associated log records time sequence. Event Log values shall begin at 0x0000 and end at 0x1FFF. Once 0x1FFF is reached, the next Event Log value shall be 0x0000.  
These 13 bits are the 13 least significant bits (LSB) of the 32 bits.
  - o A 19 bit “User Defined Value” component:  
The definition of these 19 bits is out of the scope of this document and may vary from one implementation to the other.  
These 19 bits are the 19 most significant bits (MSB) of the 32 bits.

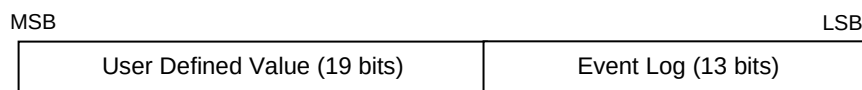


**Figure 2 – Event ID Structure**

Note: The Event ID as defined above and as used through this document is different from the Event ID defined in SMPTE 430-4, despite the fact that they share the same name. This Event ID is a Uint32, the Event ID in SMPTE 430-4 is a UUID.

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):