SMPTE ST 430-1:2017
Revision of
SMPTE 430-1:2006

SMPTE STANDARD

D-Cinema Operations — Key Delivery Message

Table of Contents

Approved
January 12, 2017

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 its Standards Operations Manual.

SMPTE ST 430-1 was prepared by Technology Committee 21DC.

Intellectual Property

SMPTE draws attention to the fact that it is claimed that compliance with this Standard may involve the use of one or more patents or other intellectual property rights (collectively, "IPR"). The Society takes no position concerning the evidence, validity, or scope of this IPR.

Each holder of claimed IPR has assured the Society that it is willing to License all IPR it owns, and any third party IPR it has the right to sublicense, that is essential to the implementation of this Standard to those (Members and non-Members alike) desiring to implement this Standard under reasonable terms and conditions, demonstrably free of discrimination. Each holder of claimed IPR has filed a statement to such effect with SMPTE. Information may be obtained from the Director, Standards & Engineering at SMPTE Headquarters.

Attention is also drawn to the possibility that elements of this Standard may be subject to IPR other than those identified above. The Society shall not be responsible for identifying any or all such IPR.

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 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 ST 429-6:2006, D-Cinema Packaging — MXF Track File Essence Encryption

[D-Cinema Digital Certificate] SMPTE ST 430-2:2017, D-Cinema Operations — Digital Certificate

[ETM] SMPTE 430-3:2012, 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.

IP: Internet Protocol. An IETF standard.