**SMPTE ST 430-2:2017**
Revision of
SMPTE 430-2-2006

# SMPTE STANDARD

# D-Cinema Operations — Digital Certificate



## Table of Contents

**Page**



Copyright © 2017 by THE SOCIETY OF
MOTION PICTURE AND TELEVISION ENGINEERS
3 Barker Avenue, White Plains, NY 10601
(914) 761-1100

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 430-2 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.

## Introduction

This standard presents a specification for Digital Certificates. This standard defines the Digital Certificate format and associated processing rules in sufficient detail to enable vendors to develop and rollout interoperable security solutions.

This Digital Certificate standard is based on a constrained form of the X.509v3 format and processing rules. X.509v3 certificates have been widely used in other well-respected security standards such as SSL/TLS secure internet access, IPSec Virtual Private Networks and S/MIME secure email. The specific constraints on the X.509v3 format are chosen to reduce the amount of time and implementation effort required to achieve interoperability with high security and yet provide a robust flexible foundation that can support future enhancements. These certificates support a simple yet flexible trust model without having to introduce new business entities. Specifically, there is no need to create an industry wide certification lab, though one could be supported.

These certificates are used in several D-Cinema standards. They are used to provide authenticity and integrity for Composition Play Lists [CPL] and Packing Lists [PL]. They provide authenticity, integrity and confidentiality in Extra-Theatre Messages [ETM] such as the Key Delivery Message [KDM], and they are used with the TLS session security protocol to protect Intra-Theater Messages.

Note: The brackets convention "[…]" as used herein denotes either a normative or informative reference.

# 1 Scope

This standard presents a specification for Digital Certificates. The standard defines the Digital Certificate format and associated processing rules in sufficient detail to enable vendors to develop and implement interoperable security solutions.

The Digital Certificate standard is based on a constrained form of the X.509v3 [X.509] format and processing rules. Only the most widely supported features of X.509v3 are used in order to give vendors a large selection of X.509v3 development toolkits and certificate issuing products. The constraints also avoid the complexity and ambiguity that often occurs in systems that use X.509v3 certificates.

In the D-Cinema environment, certificates have these primary applications:

- Establishing identity of security devices
- Supporting secure communications at the network layer (e.g. TLS) or application-messaging layer (e.g., Extra Theater Messages [ETM])
- Authentication and integrity requirements for Composition Play Lists (CPL) and Packing Lists (PL)

# 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.

[ASN.1] ISO/IEC 8824-1:2002 (ITU-T X.680, Information Technology) - Abstract Syntax Notation One (ASN.1). See: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35684

[Base64] MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies. See: http://www.ietf.org/rfc/rfc1521.txt

[FIPS-180-2] “Secure Hash Standard” Version 2. August 1, 2002. FIPS-180-2. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[PKCS1] “PKCS #1: RSA Encryption Version 2.1” By B. Kaliski. February 2003. IETF RFC 3447. See: http://www.ietf.org/rfc/rfc3447.txt

[RFC4055] “Additional Algorithms and Identifiers for RSA Cryptography for Use in the Internet X.509 Public Key Infrastructure” by J. Schaad, B. Kaliski, R. Housley, June 2005. See: http://www.ietf.org/rfc/rfc4055.txt

[RFC3280] “Internet X.509 Public Key Infrastructure Certificate and CRL Profile” by R. Housley, W. Ford, W. Polk, D. Solo, April 2002. See: http://www.ietf.org/rfc/rfc3280.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

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology — Open Systems Interconnection — The Directory: Authentication Framework, June 1997. See: http://www.itu.int/ITU-T/asn1/database/itu-t/x/x509/1997/

# 3 Glossary

The following paragraphs define the acronyms used in this standard.