SMPTE ST 429-6:2006
Amendment 1:2018

SMPTE STANDARD

D-Cinema Packaging – MXF Track File Essence Encryption

Table of Contents

Approved December 27, 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. This SMPTE Engineering Document 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 Engineering Document. 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.

Introduction

This section is entirely informative and does not form an integral part of this Engineering Document. The purpose of this document is to address a request from 35PM50 to modify the standard to facilitate their referencing by IMF. The changes shall not require modifications to D-Cinema implementations.

Amendment

Upon approval of this amendment, ST 429-6:2006 shall be revised as follows:

General

References to:

SMPTE ST 377M

are replaced with:

SMPTE ST 377 or SMPTE ST 377-1

Section 1 Scope

Replace Section 1 Scope in its entirety with:

This standard defines a syntax for encrypted Track Files, i.e. MXF files containing a single Essence Track, and specifies a matching reference decryption model. It uses the AES cipher algorithm for essence encryption and, optionally, the HMAC-SHA1 algorithm for essence integrity.

This standard assumes that the cryptographic keys necessary to decrypt and verify the integrity of encrypted Track Files will be available upon demand. More precisely, it does not specify the fashion with which cryptographic keys and usage rights are managed.

In addition, this document does not address, but does not preclude, the use of watermarking, fingerprinting or other security techniques to provide additional protection.

Section 2 Normative References

Remove the following normative reference:

SMPTE 429-3-2006, D-Cinema Packaging — Sound and Picture Track File

Replace the following normative reference:

SMPTE 377M-2004, Television — Material Exchange Format (MXF) — File Format Specification

with:

SMPTE ST 377:2004, Material Exchange Format (MXF) — File Format Specification

SMPTE ST 377-1:2012, Material Exchange Format (MXF) — File Format Specification

Note: The reference to SMPTE ST 377:2004 (http://dx.doi.org/10.5594/S9781614827689) is intentional and reflects ongoing uses of this specification.

Section 3 Overview

Add the text below as the first paragraph:

A Track File is an indexed, randomly-accessible MXF container for a single clip of a single essence track, e.g. SMPTE ST 429-3 or SMPTE ST 429-5.

Replace

> *This specification defines the encryption of the sensitive essence information contained in D-Cinema Track Files using the Advanced Encryption Standard (AES) cipher algorithm in Cipher Block Chaining (CBC) mode as defined in NIST SP 800-38A. As an option, it also allows the integrity of the same essence to be verified using the HMAC-SHA1 algorithm. More specifically this specification allows any individual track contained within a plaintext Track File to be encrypted using a single cryptographic key. The resulting encrypted Track File is extremely similar to a plaintext Track File, which is itself a constrained version of the MXF OP-ATOM operational pattern. It differs in the following three areas.*

With

> *This specification defines the encryption of the sensitive essence information contained in Track Files using the Advanced Encryption Standard (AES) cipher algorithm in Cipher Block Chaining (CBC) mode as defined in NIST SP 800-38A. As an option, it also allows the integrity of the same essence to be verified using the HMAC-SHA1 algorithm. More specifically this specification allows any individual track contained within a plaintext Track File to be encrypted using a single cryptographic key. The resulting encrypted Track File is extremely similar to a plaintext Track File[1]. It differs in the following three areas.*

Section 4 Encrypted Essence Container

Replace Table 1 – Encrypted Essence Container Label with the table below:

Frame Wrapped	060e2b34 04010107 0d010301 020b0100
Clip Wrapped	060e2b34 0401010d 0d010301 020b0200

[1] This specification assumes that the reader is familiar with the MXF and Track File formats.

Section 7.8 Trackfile ID [optional]

Replace

The optional TrackFile ID item uniquely identifies the Track File to which the Encrypted Triplet belongs. It shall be present if and only if the MIC item is present. This item is a UUID and shall have the same value for all Encrypted Triplets within a given Track File.

INFORMATIVE NOTE – Use of this identifier is described under Package IDs in [Sound & Picture Track File]; RP205 gives guidance on assignment of UMIDs.

with

The optional TrackFile ID item shall reference the Package UID of the Track File to which the Encrypted Triplet belongs. This item is a UUID and shall have the same value for all Encrypted Triplets within a given Track File.

INFORMATIVE NOTE – The TrackFile ID references the Package UID of the Track File, and can therefore be used only when the construction of the Package UID is such that a mapping to and from a UUID is unambiguous.

Section 8 Encrypted Track File Constraints

Replace

> *Encrypted Track Files shall follow the same specification as plaintext Track Files per SMPTE 429-3, with the following additional constraints.*

with

> *Encrypted Track Files shall conform to the following constraints.*

Section 8.3 Index Tables

Replace Section 8.3 in its entirety with

> *In a plaintext Track File, each Index Table entry locates a Triplet. Similarly, in an encrypted Track File, each Index Table entry shall point to an Encrypted Triplet wrapping a single Triplet.*
>
> *INFORMATIVE NOTE – As Index Tables for encrypted and plaintext Track Files point into different data streams, their contents can differ. KLV Fill packets can be used, as defined in SMPTE ST 377 or SMPTE ST 377-1, to support any KAG requirements and/or allow for identical Index Tables in encrypted and plaintext representations, or Index Tables using a non-zero EditUnitByteCount value (see SMPTE ST 377 or ST 377-1 at Index Table Segments).*

Section 10.1 Encrypted Essence Container Label

Replace the body of section 10.1 in its entirety with:

Byte No.	Description	Value (hex)	Meaning
1	Object Identifier	06h	
2	Label size	0Eh	
3	Designator	2Bh	ISO, ORG
4	Designator	34h	SMPTE
5	Registry Category Designator	04h	Labels
6	Registry Designator	01h	Labels Registry
7	Structure Designator	01h	Labels Structure
8	Version Number	07h	Registry Version at the point of registration of this label
9	Item Designator	0Dh	Organizationally Registered
10	Organization	01h	AAF Association
11	Application	03h	Essence containers
12	Structure Version	01h	Version 1
13	Essence Container Kind	02h	MXF Generic Container
14	Mapping Kind	0Bh	Encrypted Essence Container
15	Locally Defined	01h 02h	Frame Wrapped Clip Wrapped
16	Reserved	00h	

NOTE – Bytes 1-12 of this label are defined by the essence container label (see SMPTE ST 379 or SMPTE ST 379-1).

Annex A (informative) Security Properties

Replace the body of Annex A in its entirety with:

This specification has the following security properties:

- *The standard allows the first part of the essence KLV Triplet value to be unencrypted. The size of this part can be set independently for each KLV Triplet.*
- *The second part of each essence KLV Triplet is encrypted using a strong algorithm (AES) in an appropriate and well-understood mode (Cipher Block Chaining).*
- *The proposal provides partial integrity protection (tamper detection). Assuming that the 44-byte sequence consisting of the TrackFile ID, Sequence Number, and MIC items is delivered to a secure processing device along with the Encrypted Source Value, some types of manipulation may be detected.*
- *An attack which changes the order of essence KLV Triplets in the Track File will be detectable, based on sequence numbers.*
- *An attack which deletes or repeats complete KLV Triplets will be detectable, based on sequence numbers.*
- *An attack which inserts or substitutes KLV Triplets from a different Track File will be detectable, even if that Track File uses identical encryption and MAC keys, based on TrackFile ID.*
- *An attack which deletes, adds, or changes any bits of the ciphertext will be detectable.*
- *An attack which splices together parts of different KLV Triplets will be detectable.*
- *Certain types of tampering are not detectable using the Integrity Check Pack.*
- *An attacker is free to change the length of KLV Fill items.*
- *An attacker is free to change all the metadata in the file including the Key and Length of any triple and most of the fields within the Value portion of the triples (e.g., the Plaintext Offset or Cryptographic Context Link, but not the Integrity Check Pack), and all the fields in the Cryptographic Context and the Cryptographic Framework.*
- *The derived MIC key may be computed in a secure environment and delivered to a less secure integrity-checking device without risking the exposure of the Cipher Key encrypting the content itself.*
- *Only an entity that knows the decryption key can tell whether the file will decrypt properly. For example, an attacker could interfere with cryptographic key delivery or synchronization (e.g., by modifying the Cryptographic Context Pack while it is on the server), and only during playback will the problem be noticed.*

Annex B (informative) Bibliography

Add the following reference to Annex B:

SMPTE ST 2067-5:2013 Interoperable Master Format – Essence Component

SMPTE ST 379:2004, Material Exchange Format (MXF) — MXF Generic Container

SMPTE ST 379-1:2009, Material Exchange Format (MXF) — MXF Generic Container

NOTE: The reference to SMPTE ST 379:2004 (http://dx.doi.org/10.5594/S9781614828068) is intentional and reflects ongoing uses of this specification.