INTERNATIONAL STANDARD

ISO 26429-6

First edition
2008-07-15

Digital cinema (D-cinema) packaging —

Part 6: **MXF track file essence encryption**

Emballage du cinéma numérique (cinéma D) —

Partie 6: Chiffrement de l'essence du fichier de piste MXF

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbe74a501/iso-26429-6-2008

Reference number
ISO 26429-6:2008(E)

© ISO 2008

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbe74a501/iso-26429-6-2008

COPYRIGHT PROTECTED DOCUMENT

© ISO 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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.

ISO 26429-6 was prepared by the Society of Motion Picture and Television Engineers (as SMPTE 429-6-2007) 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 26429 consists of the following parts, under the general title *Digital cinema (D-cinema) packaging*:

— *Part 3: Sound and picture track file*

— *Part 4: MXF JPEG 2000 application*

— *Part 6: MXF track file essence encryption*

— *Part 7: Composition playlist*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbe74a501/iso-26429-6-2008

© ISO 2008 – All rights reserved

Introduction

The International Organization for Standardization (ISO) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO. Information may be obtained from:

Eastman Kodak Company
Intellectual Property Transactions
343 State Street
Rochester, NY 14650
USA

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO shall not be held responsible for identifying any or all such patent rights.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbe74a501/iso-26429-6-2008

© ISO 2008 – All rights reserved

SMPTE 429-6-2006

SMPTE STANDARD

D-Cinema Packaging — MXF Track File Essence Encryption

Page 1 of 25 pages

Table of Contents

1 Scope 3
2 Normative References 3
3 Overview 4
4 Encrypted Essence Container 5
5 Cryptographic Framework 5
5.1 Cryptographic Framework Key 6
5.2 Length 6
5.3 Context SR 7
6 Cryptographic Context 7
6.1 Cryptographic Context Key 7
6.2 Length 8
6.3 Context ID 8
6.4 Source Essence Container Label 8
6.5 Cipher Algorithm 8
6.6 MIC Algorithm 8
6.7 Cryptographic Key ID 9
7 Encrypted Triplet 9
7.1 Encrypted Triplet Key 10
7.2 Length 10
7.3 Cryptographic Context Link 10
7.4 Plaintext Offset 10
7.5 Source Key 10
7.6 Source Length 10
7.7 Encrypted Source Value 11
7.8 TrackFile ID [optional] 11
7.9 Sequence Number [optional] 12
7.10 MIC [optional] 12
8 Encrypted Track File Constraints 12
8.1 Encrypted Essence Track 12
8.2 Cryptographic Framework DM Track 12
8.3 Index Tables 13
9 Reference Decryption Processing Model 13
9.1 Overall Flow 13
9.2 Modules 14

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbe74a501/iso-26429-6-2008

Copyright © 2006 by THE SOCIETY OF
MOTION PICTURE AND TELEVISION ENGINEERS
3 Barker Avenue, White Plains, NY 10601
(914) 761-1100

Approved
October 3, 2006

10 Label and Key Structures 18
10.1 Encrypted Essence Container Label 18
10.2 Cryptographic Framework Label 19
10.3 Cryptographic Framework Key 20
10.4 Cryptographic Context Key 21
10.5 Encrypted Triplet Key 22
10.6 AES-CBC with 128-bit Key UL 22
10.7 HMAC-SHA1 with 128-bit Key UL 23
Annex A Security Properties (Informative) 24
Annex B Bibliography (Informative) 25

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d40c898c-966-4d35-8e2e-
1f1dbe74a501/iso-26429-6-2008

SMPTE Engineering Documents are drafted in accordance with the rules given in Part XIII of its Administrative Practices.

Proposed SMPTE Standard 429-6 was prepared by Technology Committee DC28.

© ISO 2008 – All rights reserved

1 Scope

This standard defines the syntax of encrypted D-Cinema non-interleaved MXF frame-wrapped track files 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. The D-Cinema track file format is designed to carry D-Cinema essence for distribution to exhibition sites and is specified in the Sound and Picture Track File specification.

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 across D-Cinema distribution and exhibition environments. In addition, this document does not address, but does not preclude, the use of watermarking, fingerprinting or other security techniques to provide additional protection. The scope is limited to D-Cinema and does not define a generic MXF encryption framework.

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.

SMPTE 336M-2001, Television — Data Encoding Protocol Using Key-Length-Value

iTeh STANDARD PREVIEW

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

(standards.iteh.ai)

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

ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbe74a501/iso-26429-6-2008

IETF 2898 (September 2000). PKCS #5: Password-Based Cryptography Specification – Version 2.0.

IETF 2104 (February 1997). HMAC: Keyed-Hashing for Message Authentication

National Institute of Standards and Technology (December 1, 2001). Recommendation for Block Cipher Modes of Operation Methods and Techniques (SP 800-38A).

National Institute of Standards and Technology, FIPS 197 (November 26, 2001). Advanced Encryption Standard (AES).

National Institute of Standards and Technology, FIPS PUB 186-2 (+Change Notice 1) (January 27, 2000). Digital Signature Standard (DSS).

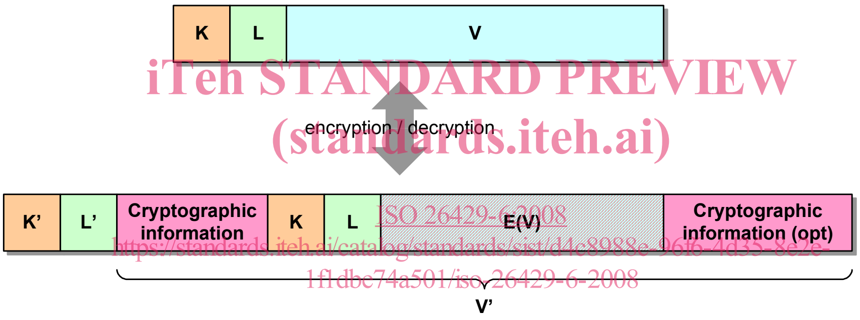
© ISO 2008 – All rights reserved

3 Overview

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[1]. It differs in the following three areas.

First, the Essence Container Label associated with the plaintext track is replaced by an Encrypted Essence Container Label. The replacement Label signals the presence of encrypted essence and allows any receiving MXF application which cannot perform decryption to “fail fast” as described in SMPTE EG 41. The Encrypted Essence Container is defined in Section 4.

Second, cryptographic information associated with the encrypted track as a whole is inserted in the MXF header metadata as a Cryptographic Framework. The Cryptographic Framework contains a link to the single cryptographic key used to encrypt the essence track. It also lists the algorithms necessary to process the encrypted essence and contains the original Essence Container Label. The latter allows implementations to determine the nature of the plaintext essence without further processing. The Cryptographic Framework is defined in Sections 5 and 5.1.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbc74a501/iso-26429-6-2008

Figure 1 – Correspondence between Source and Encrypted Triplets.

Red hatching depicts the encrypted portion of the Encrypted Triplet; other items are left as plaintext. Only the value item of Source Triplet is encrypted, allowing the essence information to be encrypted prior to wrapping. See Section 7 for a description of the cryptographic information associated with each Encrypted Triplet.

Third, the plaintext Triplets containing essence information have been replaced by Encrypted Triplets — see SMPTE 336M for details on KLV (Key-Length-Value) coding. Each Encrypted Triplet, is designed to be processed independently, allowing decryption to start anywhere within the encrypted Track File. Figure 1 illustrates the correspondence between a plaintext and an Encrypted Triplet[2]. The value *V* of a source plaintext *KLV* Triplet is first encrypted to yield *E(V)*. The encrypted value *E(V)*, along with K and L, is wrapped in a *K’L’V’* Encrypted Triplet. *K'* is a unique label common to all Encrypted Triplets, independent of their content. *L'* refers to the full length of *V'*. *V'* consists of *K*, *L* and *E(V)* from the source Triplet as well as cryptographic information specific to the Encrypted Triplet. This cryptographic information includes, for instance, the initialization vector used in generating *E(V)* and the message integrity code (MIC) used to verify the integrity of the Triplet. The structure of Encrypted Triplets is detailed in Section 7.

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

[2] This specification does not require the essence to be wrapped in a KLV Triplet to enable its encryption. In other words, essence may be encrypted prior to being wrapped in an Encrypted Triplet.

4 Encrypted Essence Container

In order to signal the presence of encrypted tracks, the Essence Container Label of any track containing Encrypted Triplets shall be replaced by the Encrypted Essence Container Label listed in Table 1. This replacement shall occur both in the Preface set and in the Partition Pack. The Essence Container Label in the File Descriptor (SMPTE 377M) shall however remain unchanged to identify the underlying plaintext essence.

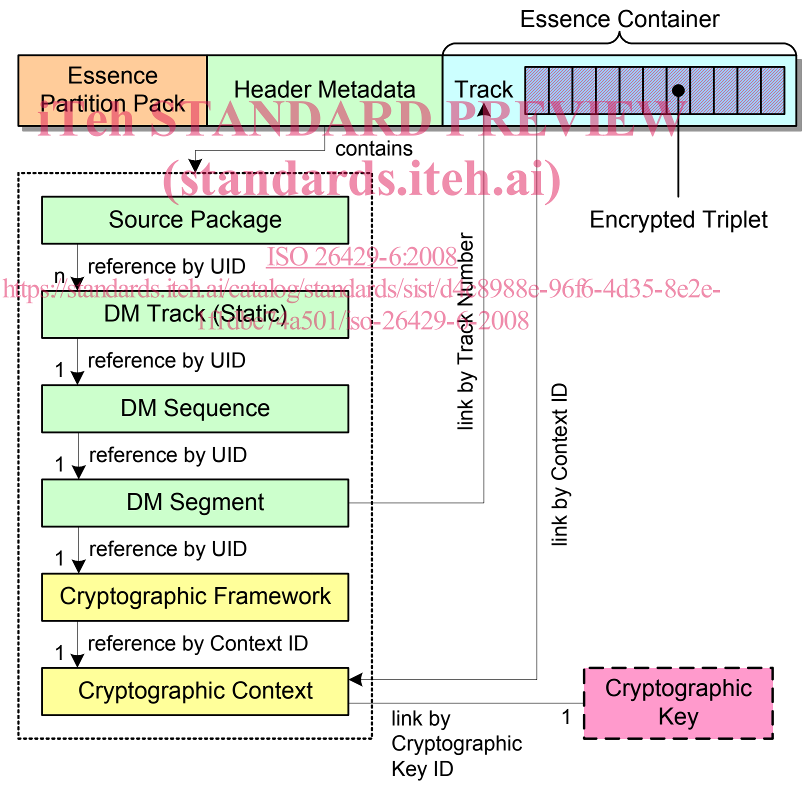
Table 1 – Encrypted Essence Container Label

(See Section 10.1 for the complete structure of the Label.)

060e2b34 04010107 0d010301 020b0100

5 Cryptographic Framework

As depicted in Figure 2, the Cryptographic Context shall be carried in encrypted Track Files as an MXF Descriptive Metadata (DM) Framework[3]. Specifically, Track Files may contain one or more Descriptive Metadata Tracks containing each a single Cryptographic Framework[4]. The Cryptographic Framework structure is detailed in Table 3.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4e8988e-96f6-4d35-8e2e-f1fdbe74a501/iso-26429-6-2008

Figure 2 – Cryptographic Framework

The DM Track is static since in encrypted Track Files a single cryptographic key is associated with any given track. Each Encrypted Triplet within a Track must refer to the same Cryptographic Context.

[3] DM frameworks are defined in SMPTE 377M under Plug-in Mechanism and follow the principles described in SMPTE EG 42.

[4] (Informative) The Cryptographic Framework is specified as a subclass of the DM Framework abstract superclass (see SMPTE 380M).

© ISO 2008 – All rights reserved

The Cryptographic Framework forms a Cryptographic DM Scheme. The Cryptographic Framework Label listed in Table 2 shall be included in the Preface set as the identifier of the Cryptographic DM Scheme.

Table 2 – Cryptographic Framework Label

(See Section 10.2 for the complete structure of the Label.)

```
060e2b34 04010107 0d010401 02010100
```

The Cryptographic Framework does not contain actual cryptographic information and instead references a single Cryptographic Context, which is defined in Section 6. Its purpose is to provide compatibility with other MXF Descriptive Metadata, allowing the Cryptographic Context to be exposed in a consistent manner.

The following defines the items contained in the Cryptographic Framework Set. With the exception of InstanceID and GenerationUID, which are already defined in SMPTE 377M, all Local Tag values for the descriptor shall be dynamically allocated as defined in SMPTE 377M section 8.2.2 (Local tag values). The translation from each dynamically allocated local tag value to its full UL value can be found using the Primer Pack mechanism defined in SMPTE 377M section 8.2 (Primer Pack).

Table 3 – Cryptographic Framework Set (Lengths are in bytes)

Item Name	Type	Len	UL	Req ?	Meaning
Cryptographic Framework Key	Set Key	16	060e2b34 02530101 0d010401 02010000	Req	Defines the Cryptographic Framework Set
Length	BER Length	var	n/a	Req	Set length
InstanceID	UUID	16	060e2b34 01010101 01011502 00000000	Req	Unique identifier for the framework.
GenerationUID	UUID	16	060e2b34 01010102 05200701 08000000	Opt	Optional Generation Identifier
Context SR	Strong Ref (Descriptive Set)	16	060e2b34 01010109 06010104 020d0000	Req	Strong reference to the associate Cryptographic Context (see Section 6)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2c-1f1dbe74a501/iso-26429-6-2008

5.1 Cryptographic Framework Key

The Cryptographic Framework Key uniquely identifies the Set as a Cryptographic Framework being subject to this specification.

Table 4 – Cryptographic Framework Key

(See Section 10.3 for the complete structure of the Key.)

```
060e2b34 02530101 0d010401 02010000
```

5.2 Length

The Length item specifies the length of the Cryptographic Framework encoded using Basic Encoding Rules (BER) per SMPTE 336M.

© ISO 2008 – All rights reserved

5.3 Context SR

The Context SR item contains a strong reference to the Cryptographic Context associated with the Cryptographic Framework.

6 Cryptographic Context

The Cryptographic Context Set[5] contains cryptographic information that applies to encrypted essence tracks as a whole. The following defines the items contained in the Cryptographic Context Set. With the exception of InstanceID and GenerationUID, which are already defined in SMPTE 377M, all Local Tag values for the descriptor shall be dynamically allocated as defined in SMPTE 377M section 8.2.2 (Local tag values). The translation from each dynamically allocated local tag value to its full UL value can be found using the Primer Pack mechanism defined in SMPTE 377M section 8.2 (Primer Pack).

Table 5 – Cryptographic Context Set (Lengths are in bytes)

Item Name	Type	Len	UL	Req ?	Meaning
Cryptographic Context Key	Set Key	16	060e2b34 02530101 0d010401 02020000	Req	Defines the Cryptographic Context Set
Length	BER Length	var	n/a	Req	Set length
InstanceID	UUID	16	060e2b34 01010101 01011502 00000000	Req	Unique identifier for the context used by Cryptographic Framework to refer to the Context.
GenerationUID	UUID	16	060e2b34 01010102 05200701 08000000	Opt	Optional Generation Identifier
Context ID	UUID	16	060e2b34 01010109 01011511 00000000	Req	Unique identifier used by Encrypted Triplets to refer to the Context.
Source Essence Container Label	UL	16	060e2b34 01010109 06010102 02000000	Req	Essence Container Label for the source essence, prior to encryption
Cipher Algorithm	UL or zero	16	060e2b34 01010109 02090301 01000000	Req	Algorithm used for Triplet encryption, if any.
MIC Algorithm	UL or zero	16	060e2b34 01010109 02090302 01000000	Req	Algorithm used for Triplet integrity, if any.
Cryptographic Key ID	UUID	16	060e2b34 01010109 02090301 02000000	Req	Unique identifier for the cryptographic key.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbe74a501/iso-26429-6-2008

6.1 Cryptographic Context Key

The Cryptographic Context Key item uniquely identifies the Set as a Cryptographic Context being subject to this specification.

[5] (Informative) The Cryptographic Context is a subclass of an InterchangeObject (see SMPTE 380M Annex C)

© ISO 2008 – All rights reserved

Table 6 – Cryptographic Context Key

(See Section 10.4 for the complete structure of the Key.)

`060e2b34 02530101 0d010401 02020000`

6.2 Length

The Length item specifies the length of the Cryptographic Context value encoded using Basic Encoding Rules (BER) per SMPTE 336M.

6.3 Context ID

The Context ID item uniquely identifies this particular Cryptographic Context. It is represented by a UUID. This value is referenced by Encrypted Triplets.

6.4 Source Essence Container Label

The Source Essence Container Label item contains the original Label of the Essence Container to which the Encrypted Triplet belongs. This allows the type of essence contained in the Encrypted Container to be readily determined.

6.5 Cipher Algorithm

The Cipher Algorithm ID item identifies the algorithm and mode used to encrypt the Encrypted Triplets associated with this Cryptographic Context. It shall contain one of the values listed in Table 7.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26429-6:2008
https://standards.iteh.ai/catalog/standards/sist/d4c8988e-96f6-4d35-8e2e-1f1dbe74a591/iso-26429-6-2008

Table 7 – Cipher Algorithms

Description	Value
No cipher algorithm used.	`00000000 00000000 00000000 00000000`
AES-CBC with 128-bit key.	`060e2b34 04010107 02090201 01000000`

The first row of Table 7 is a special value that shall be used to indicate that no cipher algorithm is necessary to process the Encrypted Triplets associated with the Cryptographic Context. The second row identifies the sole permitted value of the cipher algorithm — Section 10.6 defines the complete structure of this label.

6.6 MIC Algorithm

The MIC Algorithm ID item identifies the algorithm used to compute the (optional) message integrity code contained in the Encrypted Triplets associated with this Cryptographic Context. It shall contain one of the values listed in Table 8.

Table 8 – Message Integrity Code Algorithms

Description	Value
No MIC algorithm used.	`00000000 00000000 00000000 00000000`
HMAC-SHA1 with 128-bit key.	`060e2b34 04010107 02090202 01000000`

The first row of Table 8 is a special value that shall be used to indicate that no MIC algorithm is necessary to process the Encrypted Triplets associated with the Cryptographic Context. The second row identifies the sole permitted value of the MIC algorithm — Section 10.7 defines the complete structure of this label.

© ISO 2008 – All rights reserved