~~ISO/IEC JTC 1/SC 29~~

~~Date: 2021-10-29~~

~~ISO/IEC 23001-7:2021(E)~~

~~ISO/IEC JTC 1/SC 29/WG 3~~

Date: 2023-02-08

ISO/IEC FDIS 23001-7:2023(E)

ISO/IEC JTC 1/SC 29/WG 3

Secretariat: ~~JISC~~JISC

~~Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files~~

~~Élément introductif — Élément central — Partie 7: Titre de la partie~~

Document type:
Document subtype:
Document stage:
Document language:

Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files

Élément introductif — Élément central — Partie 7: Titre de la partie

Document type:
Document subtype:
Document stage:
Document language:

ISO copyright office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Email: copyright@iso.org

Website: www.iso.org

Published in Switzerland

Contents

Page

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Foreword

ISO (the International Organization for Standardization) and IEC~~-~~ (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC~~-~~ participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC~~-~~ technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.~~ In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.~~

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC~~-~~ Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC~~ Directives, Part 2 (see www.iso.org/directives~~ Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

~~Attention is drawn~~ISO and IEC draw attention to the possibility that ~~some of ~~the ~~elements~~implementation of this document may ~~be~~involve the ~~subject~~use of (a) patent~~ rights. ISO and IEC ~~(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.~~ Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).~~

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation ~~on~~of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see ~~the following URL: Foreword - Supplementary information~~www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

~~The committee responsible for this~~This document ~~is~~was prepared by Joint Technical Committee ISO/IEC~~-~~ JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

This ~~third~~fourth edition cancels and replaces the ~~second~~third edition (ISO/IEC 23001-7:~~2015~~2016), which has been technically revised.

It also incorporates the Amendment ISO/IEC 23001~~ consists of the following parts, under the general title *Information technology — MPEG systems technologies*:~~-7:2016/Amd 1:2019.

~~— Part 1: *Binary MPEG format for XML*~~

~~— Part 2: *Fragment request units*~~

~~— Part 3: *XML IPMP messages*~~

~~— Part 4: *Codec configuration representation*~~

~~— Part 5: Bitstream Syntax Description Language (BSDL)~~

~~— Part 7: Common~~The main changes are as follows:

Addition of:

— item encryption~~ in ISO base ~~, which allows image items to use protection schemes defined for media ~~file format files~~tracks,

~~— Part 8: Coding-independent code points~~

~~— Part 9: Common encryption of MPEG-2 transport streams~~

~~— Part 10: Carriage of timed metadata metrics of media~~— support for multiple keys and IVs per protected sample,

— `'sve1'` sensitive encryption scheme, a codec-specific encryption scheme for which the encrypted bitstream remains a valid decodable bitstream,

— improved selective encryption using sample groups

A list of all parts in the ISO~~ base media file format~~

~~— Part 11: Energy-efficient media consumption (green metadata)~~

~~— Part 12: Sample variants in~~/IEC 23001 series can be found on the ISO ~~base media file format~~and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Common Encryption specifies encryption and key mapping methods that enable decryption of the same file using different Digital Rights Management (DRM) and key management systems. It defines encryption algorithms and encryption related metadata necessary to decrypt the protected streams, yet it leaves the details of rights mappings, key acquisition and storage, DRM content protection compliance rules, etc., up to the DRM system or systems. For instance, DRM systems necessarily support identifying the decryption key via stored key identifiers (KIDs), but how each DRM system protects and locates the KID identified decryption key is left to a DRM-specific method.

DRM specific information such as licenses, rights, and license acquisition information can be stored in an ISO Base Media file using a `ProtectionSystemSpecificHeaderBox`. Each instance of this box stored in the file corresponds to one applicable DRM system identified by a well-known `SystemID`. DRM licenses or license acquisition information need not be stored in the file in order to look up a separately delivered key using a `KID` stored in the file and decrypt media samples using the encryption parameters stored in each track.

The second edition of this document added XML representations of Common Encryption parameters for delivery in XML documents, such as an MPEG DASH Media Presentation Description Documents (MPD). The second edition also defined the `'cbc1'` protection scheme using AES-CBC mode encryption.

The third edition added `'cbcs'` and `'cens'` protection schemes for pattern encryption, which encrypt only a fraction of the data blocks within each video subsample protected. Pattern encryption reduces the computational power required by devices to decrypt video tracks.

The additions in this fourth edition ~~added:~~are listed in the Foreword.

~~item~~

Information technology — MPEG systems technologies — Part 7: Common encryption~~, which allows image items to use protection schemes defined for~~ in ISO base media ~~tracks,~~file format files

- ~~support for multiple keys and IVs per protected sample,~~
- ~~'svc1' sensitive encryption scheme, a codec-specific encryption scheme for which the encrypted bitstream remains a valid decodable bitstream,~~
- ~~improved selective encryption using sample groups.~~

1 Scope

~~Part 7 of ISO/IEC 23001~~This document specifies common encryption formats for use in any file format based on ISO/IEC 14496-12~~, ISO Base Media File Format~~. File, item, track, and track fragment metadata is specified to enable multiple digital rights and key management systems (DRMs) to access the same common encrypted file or stream. This document does not define a DRM system.

The AES-128 symmetric block cipher is used to encrypt elementary stream data contained in media samples. Both AES counter mode (CTR) and Cipher Block Chaining (CBC) are specified in separate protection schemes. Partial encryption using a pattern of encrypted and clear blocks is also specified in separate protection schemes. The identification of encryption keys, initialization vector storage and processing is specified for each scheme.

Subsample encryption is specified for NAL structured video, such as AVC and HEVC, to enable normal processing and editing of video elementary streams prior to decryption.

An XML representation is specified for important common encryption information so that it can be included in XML files as standard elements and attributes to enable interoperable license and key management prior to media file download.

2 Normative references

The following documents~~,~~ are referred to in ~~whole~~the text in such a way that some or ~~in part, are normatively referenced in~~all of their content constitutes requirements of this document~~ and are indispensable for its application~~. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ITU-T Rec.H.264 | ISO/IEC 14496~~-~~-10, *Information technology* — Coding of audio-visual objects — Part 10: Advanced Video Coding

ISO/IEC 14496~~-~~-12, *Information technology — Coding of audio-visual objects — Part 12: ISO Base Media File Format*

ISO/IEC 14496~~-~~-15, *Information technology — Coding of audio-visual objects — Part~~-~~ 15: Carriage of network abstraction layer (NAL) unit structured video in the ISO ~~Base Media File Format~~base media file format*

ISO/IEC 23008~~-~~-2, *Information technology* – Coding of audio-visual objects – Part 2: High Efficiency Video Coding (HEVC)

ISO/IEC~~—~~ 23008~~-~~-12, *Information technology ~~–~~— High efficiency coding and media delivery in heterogeneous ~~environments –~~— Part 12: Image File Format (HEIF)*

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*

FIPS-197, *Advanced Encryption Standard*, Federal Information Processing Standards Publication 197, ~~FIPS-197, http://www.nist.gov/~~https://www.nist.gov/

NIST Special Publication 800-38A, *Recommendation of Block Cipher Modes of Operation*, ~~NIST, NIST Special Publication 800-38A, http://www.nist.gov/~~https://www.nist.gov/

~~IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*, July 2005~~

3 Terms, definitions and abbreviated terms

3.1 -Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1.1
block
16-byte extent of sample data that may be encrypted or decrypted by AES-128 block cipher

Note 1 to entry: This is commonly known as a cipher block**.**

3.1.2
CENC SAI

sample auxiliary information associated with a sample and containing cryptographic information such as initialization vector or subsample information

Note 1 to entry: The sample auxiliary information is defined in ISO/IEC 14496-12**,** and is not part of the sample data**.**

3.1.3
constant IV
initialization vector specified in a sample entry or sample group description that applies to all samples and subsamples under that sample entry or mapped to that sample group

3.1.4
initialization vector
8 or 16-byte value used in combination with a key and a block to create the first cipher block in a chain, and derive subsequent cipher blocks in a cipher block chain

3.1.5
NAL unit
syntax structure containing an indication of the type of data to follow and bytes containing that data in the form of an RBSP interspersed as necessary with emulation prevention bytes

3.1.6
NAL structured video
video streams composed of NAL Units

Note 1 to entry: The carriage of NAL Units is specified in ISO/IEC 14496-15

3.1.7

protection scheme
encryption algorithm and information identified by the `scheme_type` in a `SchemeTypeBox` in a `ProtectionSchemeInfoBox`

3.1.8

sample
media sample when the protection applies to media tracks, or the payload of an item when the protection applies to items

Note 1 to entry: Media sample as defined in ISO/IEC 14496-12.

Note 2 to entry: Payload of an item as defined in ISO/IEC 14496-12.

3.1.9

selective encryption
change in the `isProtected` value of samples associated with the same sample description entry

Note 1 to entry: ~~this~~ This is achieved using `CencSampleEncryptionInformationGroupEntry` sample groups.

3.1.10

subsample
byte range within a sample consisting of an unprotected part immediately followed by a protected part

3.2 Abbreviated terms

~~For the purposes of this International Standard, the following abbreviated terms apply.~~

AES	Advanced Encryption Standard
AES-CTR	AES Counter
AES-CBC	AES Cipher-Block Chaining
AVC	Advanced Video Coding as specified in ISO/IEC 14496-10
CENC	Common ENCryption
DRM	Digital Rights Management
HEVC	High Efficiency Video Coding as specified in ISO/IEC 23008-2
IV	Initialization vector
NAL	Network Abstraction Layer, as specified in ISO/IEC 14496-10 and ISO/IEC 23008-2
UUID	Universally Unique Identifier

4 Protection schemes

4.1 Scheme type signalling

Scheme signalling shall conform to ISO/IEC 14496-12. For media tracks, as defined in ISO/IEC 14496-12, the sample entry is transformed and a `ProtectionSchemeInfoBox` is added to the standard sample entry in the `SampleDescriptionBox` to denote that a stream is protected. The

ProtectionSchemeInfoBox shall contain a SchemeTypeBox so that the scheme is identifiable. The SchemeTypeBox shall obey the following additional constraints:

— The scheme_type field shall be set to a value equal to a four-character code defined in Clause ~~10.~~ 10.

— The scheme_version field shall be set to 0x00010000 (Major version 1, Minor version 0).

The ProtectionSchemeInfoBox shall also contain a SchemeInformationBox. For media tracks, the SchemeInformationBox shall contain a TrackEncryptionBox, describing the default encryption parameters for the track.

The schemes identify general classes of algorithms used to encrypt data. Implementations should not rely solely on scheme_type and scheme_version to determine if they can process a file and should also take into account:

— parameters associated with the scheme (e.g. the pattern in case of pattern encryption, or the size of initialization vectors),

— use of CencSampleEncryptionInformationGroupEntry and the associated parameters (e.g. change in isProtected, change in number and/or values of keys, change in size of initialization vectors),

— value of the field aux_info_type_parameter associated with CENC SAI,

— versions and flags of the SampleEncryptionBox box if present,

— versions of the ProtectionSystemSpecificHeaderBox and TrackEncryptionBox,

— support for, and values of versions and flags, of ItemEncryptionBox and ItemAuxiliaryInformationBox.

This document does not define brands nor profiles to restrict or recommend combinations of these parameters. Derived specifications may restrict some of these aspects.

~~4.3~~4.2 Common encryption scheme types

Five protection schemes are specified in this edition of Common Encryption. Each scheme uses syntax and algorithms specified in Clause ~~5~~ 5 to Clause ~~9,~~ 9, as constrained in Clause ~~10.~~ 10. They are the following:

a) '**cenc**' – AES-CTR mode full sample and video NAL subsample encryption; see ~~10.1.~~10.1.

b) '**cbc1**' – AES-CBC mode full sample and video NAL subsample encryption; see ~~10.2.~~10.2.

c) '**cens**' – AES-CTR mode partial video NAL pattern encryption; see ~~10.3.~~10.3.

d) '**cbcs**' – AES-CBC mode partial video NAL pattern encryption; see ~~10.4.~~10.4.

e) '**sve1**' – AES-CTR content sensitive encryption, as defined in ~~Annex A.~~Annex A.

5 Overview of encryption metadata

The encryption metadata defined by Common Encryption can be categorized as follows:

- Protection system specific data – this data is opaque to Common Encryption. This gives protection systems (i.e. key and DRM systems) a place to store their own data using a common mechanism. This data is contained in the `ProtectionSystemSpecificHeaderBox` described in ~~8.1.~~8.1.

- Common encryption information for a media track – this includes default values for the key identifier (`KID`), initialization vector and vector size, protection pattern, and protection flag. This data is contained in the `TrackEncryptionBox` described in ~~8.2~~8.2 or in the `ItemEncryptionBox` described in ~~8.3.~~8.3.

- Common encryption information for groups of media samples – this includes overrides to the track level defaults defined above. This allows groups of samples within the track to use different keys, a mix of clear and protected content, share a constant IV (for some schemes), etc. This data is contained in a `SampleGroupDescriptionBox` that is referenced by a `SampleToGroupBox`. See Clause ~~6~~ 6 for further details.

- CENC SAI, containing cryptographic information for individual media samples such as initialization vectors and subsample encryption data. CENC SAI data is sample auxiliary information as defined in ISO/IEC 14496-12. CENC SAI may reference bytes in a `SampleEncryptionBox`. See Clause ~~7~~ 7 for further details.

6 Encryption parameters shared by groups of samples

Each sample in a protected track shall be associated with an `isProtected` flag, optional subsample information and, for each key involved in the sample protection, a `Per_Sample_IV_Size, KID`, and an optional `constant_IV`. This can be accomplished by using the default values in the `TrackEncryptionBox` (see ~~8.2),~~8.2), and optionally by specifying parameters by sample group. Encryption parameters specified in a sample group override the corresponding default parameter values for the samples in that group defined in the `TrackEncryptionBox`. Samples not mapped to any sample group use the default parameters established in the `TrackEncryptionBox`.

When specifying the parameters by sample group, samples are mapped using the `SampleToGroupBox` to sample group descriptions in the `SampleGroupDescriptionBox` of type `CencSampleEncryptionInformationGroupEntry` as defined below.

The syntax of `CencSampleEncryptionInformationGroupEntry` is the same for all track types (i.e., is independent from the handler type of the track).

For fragmented files, it may be necessary to store both the mappings and descriptions in each track fragment to make them accessible for decryption of the samples they describe, e.g. when movie fragments are separately stored and delivered.

```
aligned(8) class CencSampleEncryptionInformationGroupEntry
   extends SampleGroupEntry( 'seig' )
~~{~~
{
   unsigned int(1)     multi_key_flag;
   unsigned int(7)     reserved = 0;
   unsigned int(4)     crypt_byte_block;
```