INTERNATIONAL STANDARD

ISO/IEC 23001-7

Second edition
2015-04-01

Information technology — MPEG systems technologies —

Part 7: Common encryption in ISO base media file format files

Technologies de l'information — Technologies des systèmes MPEG —

Partie 7: Cryptage commun des fichiers au format de fichier de médias de la base ISO

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50312cd968f/iso-iec-23001-7-2015

Reference number
ISO/IEC 23001-7:2015(E)

© ISO/IEC 2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50312cd968f/iso-iec-23001-7-2015

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested 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

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50312cd968f/iso-iec-23001-7-2015

© ISO/IEC 2015 – All rights reserved

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. 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 the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

This second edition cancels and replaces the first edition which has been technically revised.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e5031b2ed968f/iso-iec-23001-7-2015

ISO/IEC 23001 consists of the following parts, under the general title *Information technology — MPEG systems technologies*:

— *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 encryption in ISO base media file format files*

— *Part 8: Coding-independent code points*

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

The following parts are under preparation:

— *Part 10: Carriage of timed metadata metrics of media in ISO base media file format*

— *Part 11: Green metadata*

© ISO/IEC 2015 – All rights reserved

Introduction

The common encryption protection scheme specifies standard encryption and key mapping methods that can be utilized to enable decryption of the same file using different digital rights management (DRM) and key management systems. The schemes operates by defining a common format for the encryption related metadata necessary to decrypt the protected streams, yet leaves the details of rights mappings, key acquisition and storage, DRM compliance rules, etc., up to the DRM system or systems supporting the common encryption scheme. For instance, DRM systems supporting the 'cenc' protection scheme must support identifying the decryption key via 'cenc' key identifier (KID) but how the DRM system locates the identified decryption key is left to a DRM-specific method. DRM specific information such as licenses or rights and license/rights acquisition information can be stored in an ISO Base Media file using a Protection System Specific Header box ('pssh'). Each instance of this box stored in the file corresponds to one applicable DRM system. DRM licenses/rights need not be stored in the file in order to look up a key using KID values stored in the file and decrypt media samples using the encryption parameters stored in each track. The second edition of this part of ISO/IEC 23001 also describes XML representation of common encryption parameters in MPEG DASH Media Presentation Description Documents.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50312cd968f/iso-iec-23001-7-2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50312cd968f/iso-iec-23001-7-2015

Information technology — MPEG systems technologies —

Part 7:
Common encryption in ISO base media file format files

1 Scope

This part of ISO/IEC 23001 specifies a common encryption format for use in any file format based on ISO/IEC 14496-12.

2 Normative references

The following documents, in whole or in part, are normatively referenced in 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.

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 ISO base media file format*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50312ed968f/iso-iec-23001-7-2015

3 Terms and definitions

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

NOTE Words used as defined terms and normative terms (SHALL, SHOULD, MAY) are written in upper case to distinguish them from the same word intending its dictionary definition.

3.1
ISO Base Media File
file conforming to the file format described in ISO/IEC 14496-12 in which the techniques in ISO/IEC 23001-7 can be used

3.2
network abstraction layer
NAL
NAL syntax element specified by a network abstraction layer specification such as AVC or HEVC

3.3
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

3.4
NAL structured video
video sample description format specified by ISO/IEC 14496-15

© ISO/IEC 2015 – All rights reserved

4 Abbreviated terms

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

AES	Advanced Encryption Standard as specified in Federal Information Processing Standards Publication 197, FIPS-197
AES-CTR	AES Counter Mode as specified in *Recommendation of Block Cipher Modes of Operation*, NIST, NIST Special Publication 800-38A
AES-CBC	AES Cipher-Block Chaining Mode as specified in *Recommendation of Block Cipher Modes of Operation*, NIST, NIST Special Publication 800-38A
AVC	Advanced Video Coding as specified in ISO/IEC 14496-10
HEVC	High Efficiency Video Coding as specified in ISO/IEC 23008-2
NAL	Network Abstraction Layer, as specified in ISO/IEC 14496-10 and ISO/IEC 23008-2
URN	Unique Resource Name
UUID	Universally Unique Identifier

5 Scheme Signaling

Scheme signaling SHALL conform to ISO/IEC 14496-12. As defined in ISO/IEC 14496-12, the sample entry is transformed and a Protection Scheme Information Box (`sinf') is added to the standard sample entry in the Sample Description Box to denote that a stream is encrypted. The Protection Scheme Information Box SHALL contain a Scheme Type Box (`schm') so that the scheme is identifiable. The Scheme Type Box SHALL have the following additional constraints:

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50912cd968f/iso-iec-23001-7-2015

— The scheme_type field is set to a value of `cenc' (Common Encryption). As an optional alternative, AES-CBC may be used in which case the scheme_type field is set to the value `cbc1'.

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

The Protection Scheme Information Box SHALL also contain a Scheme Information Box ('schi'). The Scheme Information Box SHALL have the following additional constraint:

— The Scheme Information Box SHALL contain a Track Encryption Box ('tenc'), describing the default encryption parameters for the track.

6 Overview of Encryption Metadata

The encryption metadata defined by the 'cenc' Common Encryption Scheme can be categorized as follows:

— Protection System Specific Data – this data is opaque to the 'cenc' Common Encryption Scheme. This gives protection systems a place to store their own data using a common mechanism. This data is contained in the ProtectionSystemSpecificHeaderBox described in 9.1.

— Common encryption information for a media track – this includes default values for the key identifier (KID), initialization vector size, and encryption flag. This data is contained in the TrackEncryptionBox described in section 9.1.

— Common encryption information for groups of media samples – this includes overrides to the track level defaults for key identifier (KID), initialization vector size, and encryption flag. This allows groups of samples within the track to use different keys, a mix of clear and encrypted content, etc. This data is contained in a SampleGroupDescriptionBox (`sgpd') that is referenced by a SampleToGroupBox (`sbgp'). See 7 for further details.

© ISO/IEC 2015 – All rights reserved

— Encryption information for individual media samples – this includes initialization vectors and, if required, sub sample encryption data. This data is sample auxiliary information, referenced by using a SampleAuxiliaryInformationSizesBox ('saiz') and a SampleAuxiliaryInformationOffsetsBox ('saio'). See 8 for further details.

7 Encryption Parameters shared by groups of samples

Each sample in a protected track SHALL be associated with an IsEncrypted flag, IV_Size, and KID. This can be accomplished by (a) relying on the default values in the TrackEncryptionBox (see 9.2, or (b) specifying the parameters by sample group, or (c) using a combination of these two techniques. Encryption parameters defined at sample group level override the corresponding default parameter values defined in the TrackEncryptionBox.

When specifying the parameters by sample group, the SampleToGroupBox in the sample table or track fragment specifies which samples use which sample group description from the SampleGroupDescriptionBox. The format of the sample group description is based on the handler type for the track.

Tracks with a handler type of 'vide' SHALL use the CencSampleEncryptionInformationVideoGroupEntry sample group description structure, which has the following syntax:

```
aligned(8) class CencSampleEncryptionInformationVideoGroupEntry
    extends VisualSampleGroupEntry( 'seig' )
{
    unsigned int(24)      IsEncrypted;
    unsigned int(8)       IV_size;
    unsigned int(8)[16]   KID;
}
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7f11-4f00-9648-e50312cd968f/iso-iec-23001-7-2015

Similarly, tracks with a handler type of 'soun' SHALL use the CencSampleEncryptionInformationAudioGroupEntry sample group description structure, which has the following syntax:

```
aligned(8) class CencSampleEncryptionInformationAudioGroupEntry
    extends AudioSampleGroupEntry( 'seig' )
{
    unsigned int(24)      IsEncrypted;
    unsigned int(8)       IV_size;
    unsigned int(8)[16]   KID;
}
```

NOTE Sample Group Entries with identical structure should be defined if protection of other media types is needed.

These structures use a common semantic for their fields as follows:

IsEncrypted is the flag which indicates the encryption state of the samples in the sample group. See the IsEncrypted field in 10.2 for further details.

IV_size is the Initialization Vector size in bytes for samples in the sample group. See the IV_size field in 10.2 for further details.

KID is the key identifier used for samples in the sample group. See the KID field in 10.2 for further details.

In order to facilitate the addition of future optional fields, clients SHALL ignore additional bytes after the fields defined in the CencSampleEncryption group entry structures.

8 Common Encryption Sample Auxiliary Information

Each encrypted sample in a protected track SHALL have an Initialization Vector associated with it. Further, each encrypted sample in protected NAL structured video tracks SHALL conform to ISO/IEC 14496-15 and SHALL use the subsample encryption scheme specified in 10.6.2, which requires subsample encryption data. Both initialization vectors and subsample encryption data are provided as Sample Auxiliary Information with `aux_info_type` equal to 'cenc' and `aux_info_type_parameter` equal to 0. For tracks protected using the 'cenc' scheme, the default value for `aux_info_type` is equal to 'cenc' and the default value for the `aux_info_type_parameter` is 0 so content MAY be created omitting these optional fields. Storage of sample auxiliary information SHALL conform to ISO/IEC 14496-12.

The format of the sample auxiliary information for samples with this type SHALL be:

```
aligned(8) class CencSampleAuxiliaryDataFormat
{
   unsigned int(IV_size*8) InitializationVector;
   if ( sample_info_size > IV_size )
   {
      unsigned int(16) subsample_count;
      {
        unsigned int(16) BytesOfClearData;
        unsigned int(32) BytesOfEncryptedData;
      } [ subsample_count ]
   }
}
```

Where:

`InitializationVector` is the initialization vector for the sample. See the `InitializationVector` field in 10.2 for further details.

`subsample_count` is the count of subsamples for this sample. See the `subsample_count` field in 10.2 for further details.

`BytesOfClearData` is the number of bytes of clear data in this subsample. See the `BytesofClearData` field in 10.2 for further details.

`BytesOfEncryptedData` is the number of bytes of encrypted data in this subsample. See the `BytesofEncryptedData` field in 10.2 for further details.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50312ed968f/iso-iec-23001-7-2015

If sub-sample encryption is not used (sample_info_size equals IV_size), then the entire sample is encrypted (see 10.5 for further details). In this case, all auxiliary information will have the same size and hence the `default_sample_info_size` of the SampleAuxiliaryInformationSizes box will be equal to the `IV_Size` of the initialization vectors.

Note, however, that even if subsample encryption is used, the size of the sample auxiliary information MAY be the same for all of the samples (if all of the samples have the same number of subsamples) and the `default_sample_info_size MAY be` used.

8.1 Sample Encryption Information Box for Storage of Sample Auxiliary Information

An optional storage location for Sample Auxiliary Information is the Sample Encryption Information Box (`'senc'`) specified below.

8.1.1 Sample Encryption Box ('senc')

Box Type `'senc'`

Container Track Fragment Box (`'traf'`) or Track Box (`'trak'`)

Mandatory No

Quantity Zero or one

The Sample Encryption Box contains sample auxiliary information, including the initialization vector for each sample, and clear and encrypted byte ranges of partially encrypted video samples (“subsample encryption”). It MAY be used when samples in a track or track fragment are encrypted. Storage of ‘senc’ in a Track Fragment Box makes the necessary Sample Auxiliary Information accessible within the movie fragment for all contained samples in order to make each track fragment independently decryptable; for instance, when movie fragments are delivered as DASH Media Segments.

8.1.2 Syntax

```
aligned(8) class SampleEncryptionBox
   extends FullBox(‘senc’, version=0, flags=0)
{
   unsigned int(32)  sample_count;
   {
      unsigned int(IV_size*8)  InitializationVector;
      if (flags & 0x000002)
      {
         unsigned int(16)  subsample_count;
         {
            unsigned int(16)  BytesOfClearData;
            unsigned int(32)  BytesOfEncryptedData;
         } [ subsample_count ]
      }
   }[ sample_count ]
}
```

8.1.2.1 Semantics

- `flags` is inherited from the `FullBox` structure. The `SampleEncryptionBox` currently supports the following bit values:
  - 0x2 – `UseSubSampleEncryption`
  - If the `UseSubSampleEncryption` flag is set, then the track fragment that contains this Sample Encryption Box SHALL use the sub-sample encryption as described in Section 9.6. When this flag is set, sub-sample mapping data follows each `InitilizationVector`. The sub-sample mapping data consists of the number of sub-samples for each sample, followed by an array of values describing the number of bytes of clear data and the number of bytes of encrypted data for each sub-sample.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 23001-7:2015
https://standards.iteh.ai/catalog/standards/sist/e5883567-7b11-4f00-9648-e50312cd968f/iso-iec-23001-7-2015

- `sample_count` is the number of encrypted samples in the containing track or track fragment. This value SHALL be either zero (0) or the total number of samples in the track or track fragment.
- `InitializationVector` SHALL conform to the definition specified in Section 10.2. Only one `IV_size` SHALL be used within a file, or `IV_size` SHALL be zero when a sample is unencrypted. Selection of `InitializationVector` values SHOULD follow the recommendations of Section 10.3.
- `subsample_count` SHALL conform to the definition specified in Section 10.2.
- `BytesOfClearData` SHALL conform to the definition specified in Section 10.2.
- `BytesOfEncryptedData` SHALL conform to the definition specified in Section 10.2.

9 Box Definitions

9.1 Protection System Specific Header Box

9.1.1 Definition

Box Type: `pssh’

© ISO/IEC 2015 – All rights reserved