INTERNATIONAL STANDARD

ISO/IEC 23001-7

First edition
2012-02-01

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

Reference number
ISO/IEC 23001-7:2012(E)

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

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 23001-7 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

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*

Introduction

The Common Encryption ('cenc') protection scheme specifies standard encryption and key mapping methods that can be utilized by one or more digital rights and key management systems [digital-rights management (DRM systems)] to enable decryption of the same file using different DRM systems. The scheme 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 'cenc' 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'), using one for each DRM system applied. 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.

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, the ISO base media file format.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 14496-10, *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: Advanced Video Coding (AVC) file format*

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

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

3 Definitions

3.1 Terms and definitions

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

3.1.1
ISO Base Media File
name of a file conforming to the file format described in ISO/IEC 14496-12 in which the techniques in ISO/IEC 23001-7 may be used

NOTE Adapted from ISO/IEC 14496-12, definition 3.1.8.

3.2 Abbreviated terms

For the purposes of this document, 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

AVC Advanced Video Compression as specified in ISO/IEC 14496-10

ISOAVC An ISO Base Media File containing AVC media tracks as specified in ISO/IEC 14496-15

NAL Network Abstraction Layer as specified in ISO/IEC 14496-10

4 Scheme Signalling

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 has the following additional constraints:

- The `scheme_type` field is set to a value of `'cenc'` (Common Encryption).
- 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 has the following additional constraint:

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

5 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 8.1.
- 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 8.2.
- 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 6 for further details.
- 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 7 for further details.

6 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 8.2), or (b) specifying the parameters by sample group, or (c) using a combination of these two techniques.

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 sample group description structure, `CencSampleEncryptionInformationVideoGroupEntry`, 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;
}
```

Similarly, tracks with a handler type of 'soun' shall use the sample group description structure, `CencSampleEncryptionInformationAudioGroupEntry`, 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 Groups 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 9.2 for further details.

`IV_size` is the Initialization Vector size in bytes for samples in the sample group. See the `IV_size` field in 9.2 for further details.

`KID` is the key identifier used for samples in the sample group. See the `KID` field in 9.2 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.

7 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 AVC video tracks shall conform to ISO/IEC 14496-10 and ISO/IEC 14496-15 and shall use the subsample encryption scheme specified in 9.6.2, 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: