INTERNATIONAL STANDARD

ISO/IEC 23001-7

First edition
2012-02-01

AMENDMENT 1
2012-11-01

Information technology — MPEG systems technologies —

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

AMENDMENT 1: AES-CBC-128 and key rotation

Technologies de l'information — Technologies des systèmes MPEG — Partie 7: Cryptage commun des fichiers au format de fichier de médias de la base ISO

AMENDEMENT 1: AES-CBC-128 et rotation de la clé

Reference number
ISO/IEC 23001-7:2012/Amd.1:2012(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

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.

Amendment 1 to ISO/IEC 23001-7:2012 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

Information technology — MPEG systems technologies —

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

AMENDMENT 1: AES-CBC-128 and key rotation

Page 2, 3.2

Add the following abbreviated term:

AES-CBC AES Cipher-Block Chaining Mode as specified in *Recommendation of Block Cipher Modes of Operation*, NIST, NIST Special Publication 800-38A

Page 2, Clause 4

Replace the first bullet with the following:

- 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 shall be set to the value `cbc1'.

Page 2, Clause 5

Replace the introductory sentence with the following:

The encryption metadata defined by schemes conforming to this standard can be categorized as follows:

Page 4, 8.1

Replace 8.1 with the following:

8.1 Protection System Specific Header Box

8.1.1 Definition

Box Type: `pssh'
Container: Movie (`moov') or Movie Fragment (`moof')
Mandatory: No
Quantity: Zero or more

This box contains information needed by a Content Protection System to play back the content. The data format is specified by the system identified by the `'pssh'` parameter `SystemID`, and is considered opaque for the purposes of this specification. The collection of Protection System Specific Header boxes from the initial movie box, together with those in a movie fragment, shall provide all the required Content Protection System information to decode that fragment.

The data encapsulated in the Data field may be read by the identified Content Protection System client to enable decryption key acquisition and decryption of media data. For license/rights-based systems, the header information may include data such as the URL of license server(s) or rights issuer(s) used, embedded licenses/rights, embedded keys(s), and/or other protection system specific metadata.

A single file may be constructed to be playable by multiple key and digital rights management (DRM) systems, by including Protection System Specific Header boxes for each system supported. In order to find all of the Protection System Specific data that is relevant to a sample in the presentation readers shall:

- Examine all Protection System Specific Header boxes in the Movie Box and in the Movie Fragment Box associated with the sample (but not those in other Movie Fragment Boxes).

- Match the `SystemID` field in this box to the SystemID(s) of the DRM System(s) they support

- Match the KID associated with the sample (either from the `default_KID` field of the Track Encryption Box or the `KID` field of the appropriate sample group description entry) with one of the KID values in the Protection System Specific Header Box. Boxes without a list of applicable KID values, or with an empty list, shall be considered to apply to all KIDs in the file or movie fragment.

Protection System Specific Header data shall be associated with a sample based on a matching KID value in the ‘pssh’ and sample group description or default ‘tenc’ describing the sample. If a sample or set of samples is moved due to file defragmentation or refragmentation or removed by editing, then the associated Protection System Specific Header boxes for the remaining samples shall be stored following the above requirements.

NOTE Multiple Protection System Specific Header boxes may be associated with a given KID and `SystemID`.For storage efficiency, Protection System Specific Header boxes containing the same KID(s) and SystemID should not be duplicated in a movie fragment or movie box resulting from defragmentation or refragmentation.

8.1.2 Syntax


```
aligned(8) class ProtectionSystemSpecificHeaderBox extends FullBox(‘pssh’,
version, flags=0)
{
   unsigned int(8)[16]         SystemID;
   if (version > 0)
   {
      unsigned int(32)         KID_count;
      {
         unsigned int(8)[16]   KID;
      } [KID_count]
   }

   unsigned int(32)            DataSize;
   unsigned int(8)[DataSize]   Data;
}
```

8.1.3 Semantics

`SystemID` specifies a UUID that uniquely identifies the content protection system that this header belongs to.
`KID_count` specifies the number of KID entries in the following table. The value may be zero.
`KID` identifies a key identifier that the Data field applies to.
`DataSize` specifies the size in bytes of the Data member.
`Data` holds the content protection system specific data.

Page 6, 9.2

In 9.2, replace:

`IsEncrypted` is the identifier of the encryption state of the samples in the track or group of samples. This flag takes the following values:

0x0: Not encrypted
0x1: Encrypted using AES 128-bit in CTR mode
0x000002 – 0xFFFFFF: Reserved

with:

`IsEncrypted` is the identifier of the encryption state of the samples in the track or group of samples. This flag takes the following values:

0x0: Not encrypted
0x1: Encrypted (as signalled by the scheme_type field of the scheme type box ‘schm’, e.g. for ‘cenc’ this is AES-CTR)
0x000002 – 0xFFFFFF: Reserved

And replace:

`InitializationVector` specifies the initialization vector (IV) needed for decryption of a sample. For an `IsEncrypted` flag of 0x0, no initialization vectors are needed and the auxiliary information should have a size of 0, i.e. not be present.

For an `IsEncrypted` flag of 0x1 (AES-CTR), if the IV_size field is 16 then `InitializationVector` specifies the entire 128-bit IV value used as the counter value. If the `IV_size` field is 8, then its value is copied to bytes 0 to 7 of the counter value and bytes 8 to 15 of the counter value are set to zero. The `IV_size` field shall not be 0 when the `IsEncrypted` flag is 0x1 (AES-CTR).

For an `IsEncrypted` flag of 0x1 (AES-CTR), counter values shall be unique per `KID`. If an `IV_size` of 8 is used, then the `InitializationVector` values for a given `KID` shall be unique for each sample in all tracks and samples shall be less than 2^{64} blocks in length. If an `IV_size` of 16 is used, then initialization vectors shall have large enough numeric differences to prevent duplicate counter values for any encrypted block using the same `KID`.

with:

`InitializationVector` specifies the initialization vector (IV) needed for decryption of a sample. For an `IsEncrypted` flag of 0x0, no initialization vectors are needed and the auxiliary information should have a size of 0, i.e. not be present.

For an `IsEncrypted` flag of 0x1
if the IV_size field is 16 then `InitializationVector` specifies the entire 128-bit IV value
If the `IV_size` field is 8, then its value is copied to bytes 0 to 7 of the InitializationVector and bytes 8 to 15 of the Initialization Vector are set to zero. The `IV_size` field shall not be 0 when the `IsEncrypted` flag is 0x1.

For an `IsEncrypted` flag of 0x1 where the scheme_type field of the scheme type box is ‘cenc’ (i.e. AES-CTR), counter values shall be unique per `KID`. If an `IV_size` of 8 is used, then the `InitializationVector` values for a given `KID` shall be unique for each sample in all tracks and samples shall be less than 2^{64} blocks in length. If an `IV_size` of 16 is used, then initialization vectors shall have large enough numeric differences to prevent duplicate counter values for any encrypted block using the same `KID`.

Page 10

Add the following clause after Clause 9:

10 AES 128-bit Cipher Block Chaining (CBC-128) Encryption of Media Data

10.1 Introduction to AES 128-bit Cipher-Block Chaining (CBC-128) Mode

Media data using 'cbc1' Protection Scheme uses the Advanced Encryption Standard specified by AES [FIPS-197] using 128-bit keys in Cipher-block chaining mode (AES-CBC-128), as specified in Block Cipher Modes [NIST 800-38A], with IVs stored as described in 6 and 9.2. Encrypted AVC Video Tracks shall follow the scheme outlined in10.2.4, which defines a NAL unit based encryption scheme to allow access to NAL units and unencrypted NAL unit headers in an encrypted AVC stream. All other types of tracks must follow the scheme outlined in 10.2.5, which defines a simple sample-based encryption scheme.

NOTE Support for 'cbc1' scheme is not mandatory in the common encryption mechanism, however implementations that process the 'cbc1' scheme are also required to process the 'cenc' scheme so that files using the 'cenc' scheme may be processed on all implementations of this standard.

10.2 AES-CBC-128 Mode

The scheme_type field of the scheme Type Box (`schm') shall be set to 'cbc1' to signal AES-CBC-128 Mode. The AES-CBC-128 mode shall follow the same mechanisms as defined in Clauses 4 to 9.3 except for Initialization Vector creation, 9.5 and 9.6.2, but using the 'cbc1' rather than 'cenc', and with additional constraints as detailed in 10.2.1 to 10.2.5.

10.2.1 Field Semantics for AES-CBC-128 Mode

`IV_size` (as defined in 9.2) shall be 16 which specifies 128-bit initialization vectors.

10.2.2 Creation of Initialization Vectors (Informative)

There are no constraints on the values used for initialization vectors when applying encryption. However, security may be improved if the first initialization vector used for encryption is randomly selected and no duplicate values are used with the same KID value. Decryption efficiency may be improved if subsequent initialization vectors use the value of the last cipher block at the end of the previous sample so that multiple samples may be decrypted as a continuous chain.

10.2.3 AES-CBC-128 Mode Encryption of AVC Video Tracks

AES-CBC-128 encryption of AVC Video Tracks follow the principles set out in 9.6.2.2 using partial encryption as signalled by the common encryption sample auxiliary information described in 7. The size of clear data (BytesOfClearData) at the beginning of each NAL Unit shall be set such that the size of encrypted NAL data (BytesOfEncryptedData) be an integral number of 16 bytes blocks terminating at the end of each subsample. Figure 5 below shows AES-CBC-128 handing of AVC tracks.

NOTE There are no clear partial blocks at the end of the NAL Unit Payload as shown in Figure 5.

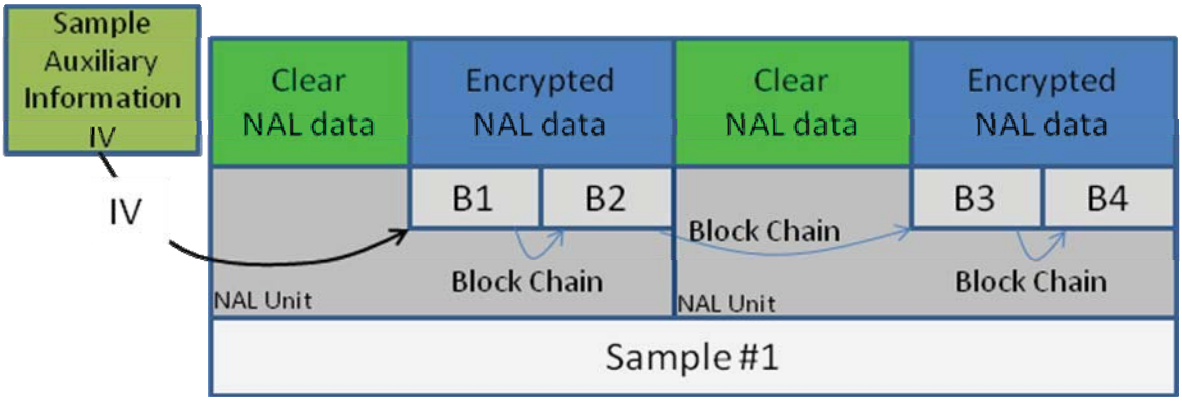

Figure 5 — Subsample Encryption Applied to AVC using AES-CBC-128

10.2.4 Full Encryption in AES-CBC-128 Mode

For full encryption in AES-CBC-128 Mode, residual block (i.e. when the last block in the chaining is less than 16 bytes) shall be left in the clear as shown in Figures 6 below. If a sample size is smaller than 16 bytes, then the sample shall be treated as a solitary block and left in the clear,

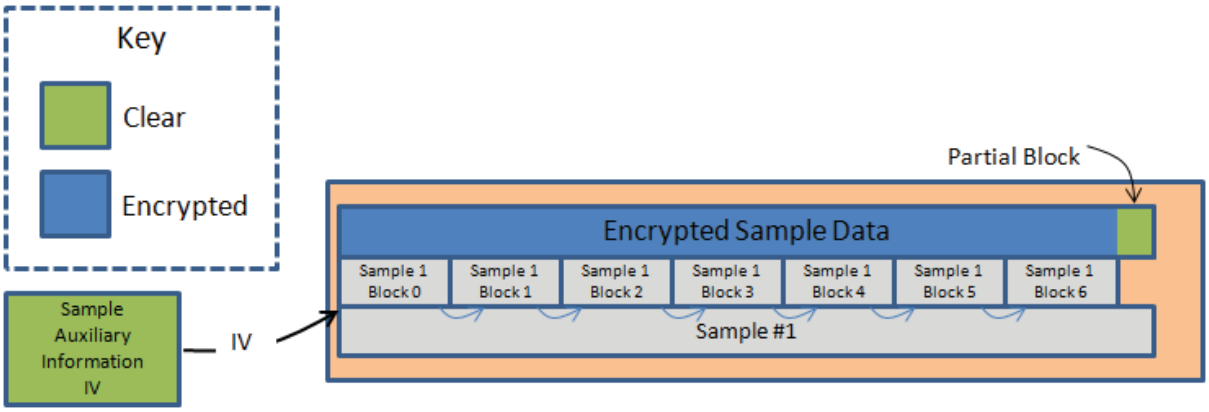

Figure 6 — Sample-based Encryption for AES-CBC-128