INTERNATIONAL STANDARD

ISO/IEC 23001-9

First edition
2014-06-01

Information technology — MPEG systems technologies —

Part 9: Common encryption of MPEG-2 transport streams

Technologies de l'information — Technologies des systèmes MPEG — Partie 9: Cryptage commun des flux de transport de contenu MPEG-2

Reference number
ISO/IEC 23001-9:2014(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 23001-9 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*

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

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

Information technology — MPEG systems technologies —

Part 9:
Common encryption of MPEG-2 transport streams

1 Scope

This part of ISO/IEC 23001 specifies a common media encryption format for use in MPEG-2 transport streams. This encryption format is intended to be used in an interoperable way with media encrypted using the format described by ISO/IEC 23001-7. This part of ISO/IEC 23001 allows conversion between encrypted MPEG-2 transport streams and encrypted ISO base media file format files without re-encryption.

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.

Rec. ITU-T H.222.0 | ISO/IEC 13818-1, *Information technology — Generic coding of moving pictures and associated audio information — Part 1: Systems*

ISO/IEC 13818-7, *Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC)*.

ISO/IEC 14496-10, *Information technology — Coding of audio-visual objects — Part 10: Advanced Video Coding* (technically aligned with Rec. ITU-T H.264)

ISO/IEC 14496-3, *Information technology — Coding of audio-visual objects — Part 3: Audio*

ISO/IEC 23001-7, *Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files*

ISO/IEC 23008-2, *Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 2: High efficiency video coding*

IETF RFC 1321, *The MD5 Message-Digest Algorithm* , April 1992

Advanced Encryption Standard, Federal Information Processing Standards Publication 197, FIPS-197

Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A

3 Terms and definitions

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

3.1
Encrypted AU
part of elementary stream containing one access unit

Note 1 to entry: In case of ISO/IEC 14496-10 and ISO/IEC 23008-2, these are comprised of one or more NAL units.

4 Abbreviations

AES	Advanced Encryption Standard (FIPS-197)
AU	Access Unit
CAT	Conditional Access Table (ISO/IEC 13818-1)
CBC	Cipherblock Chaining (NIST 800-38A)
CENC	Common Encryption (ISO/IEC 23001-7)
CETS	Common Encryption of MPEG-2 Transport Streams
CTR	Counter Mode (NIST SP 800-38A)
DTS	Decoding Time Stamp (ISO/IEC 13818-1)
EAU	Encrypted Access Unit
ECM	Entitlement Control Message (ISO/IEC 13818-1)
ISO-BMFF	ISO Base Media File Format (ISO/IEC 14496-12)
IV	Initialization Vector (NIST SP 800-38A)
KID	Key Identifier (ISO/IEC 23001-7)
MD5	MD5 Message-Digest Algorithm (IETF RFC 1321)
MPEG-2 TS	MPEG-2 Transport Stream (ISO/IEC 13818-1)
NAL	Network Access Layer (ISO/IEC 14496-10, ISO/IEC 23008-2)
PAT	Program Association Table (ISO/IEC 13818-1)
PES	Packetized Elementary Stream (ISO/IEC 13818-1)
PID	Packet Identifier (ISO/IEC 13818-1)
PMT	Program Map Table (ISO/IEC 13818-1)
PTS	Presentation Time Stamp (ISO/IEC 13818-1)
RAP	Random Access Point
VCL	Video Coding Layer (ISO/IEC 14496-10, ISO/IEC 23008-2)

5 Introduction

5.1 General

An interoperable container-independent encryption scheme allows container format changes for encrypted content in the network without the need for the processing node to be able to support for and interoperate with multiple DRM's. Given the need to support clients that use different container formats, such capability allows end-to-end content protection from the content preparation stage till the content consumption by the authorized end user.

If the encrypted parts of elementary streams are the same, and parameters needed to do re-encapsulation are in the clear, it is possible to do re-encapsulation without re-encryption. Partial bitstream encryption specified in ISO/IEC 23001-7 makes such re-multiplexing of ISO-BMFF files possible. ISO/IEC 23001-7

is specific to ISO-BMFF, while this part of ISO/IEC 23001 provides an MPEG-2 TS framework which provides same functionality for MPEG-2 TS. A combination of ISO/IEC 23001-7 and ISO/IEC 23001-9 allows re-encapsulation between ISO-BMFF and MPEG-2 TS content without re-encryption.

5.2 Theory of Operation

The premise of common encryption is that each access unit is encrypted separately, either completely or partially. Hence each access unit needs two parameters, key and initialization vector. Key resolution is out of scope of this part of the standard, and depends on the key system in question. The abstraction we use is that given a key identifier and a license, a key system will return a key. ECM is used to transport IVs and key identifiers. In order to make it possible to decrypt, we need to be able to identify which access unit is encrypted with which key/IV combination. MPEG-2 TS provides transport-level and PES-level functionality for this using the `transport_scrambling_control` field. Thus the transport stream packet payload is in the clear if the `transport_scrambling_control` value is '00'. Otherwise, the payload is encrypted with key/IV combination identified by the `transport_scrambling_control` value within the nearest ECM.

NOTE Given that common encryption is applied separately per each access unit, `transport_scrambling_control` value will most probably change each access unit, hence ECM's will appear very frequently. For the first encrypted MPEG-2 TS packet of a PES packet, only the immediately preceding ECM is guaranteed to contain the correct key/IV combination for a given access unit, as `scrambling_bits` is a 2-bit field and has only 3 available encryption states.

A vendor-specific license is necessary for any practical DRM operation. In ISO/IEC 23001-7, this is carried for each DRM in one or more `pssh` boxes. In this part of ISO/IEC 23001, same information is carried in a private CETS PSSH PID (one PID per each DRM system). This does not necessarily mean that `pssh` data has to be carried inband – this is a decision left to the implementer.

Algorithm-related parameters are signalled via the `CA_descriptor` descriptor.

In ISO/IEC 23001-7 each track has its own `tenc` box and sample-specific IV's. In this part of the standard it is implemented as separate ECM PID. If same key/IV combination is used for more than one PID (e.g., same combination for both audio and video), it is possible to use same ECM PID for all PIDs sharing the same key/IV combination. However, this practice may increase the complexity and fragility of the system.

6 Encryption Parameter Signalling

6.1 CETS ECM

6.1.1 General

At the very basic level, CETS ECM provides (a) key ID and initialization vector for each state of `transport_scrambling_control`, and (b) notification of upcoming key rotation. In case where IV or/and key are changed per each sample, therefore CETS ECM's are expected to appear very frequently (ECM per AU)

As it is possible to have a key and/or IV change in the middle of a PES packet (e.g. in case PES carries several access units, which is a common practice for audio), CETS ECM also indicates byte offsets into the beginning of encrypted bytes that are encrypted with different key/IV pair.

CETS ECM is always contained in a single MPEG-2 TS packet, therefore the size of `cets_ecm` shall not exceed 184 bytes. Adaptation field stuffing shall be used for smaller `cets_ecm` sizes.

6.1.2 Syntax

Syntax	No. of bits	Format
cets_ecm(){		
num_states	2	uimbsf
next_key_id_flag	1	bslbf
reserved	3	bslbf
iv_size	8	uismbf
default_key_id	128	uismbf
for (i = 0; i < num_states; i++) {		
transport_scrambling_control	2	bslbf
num_au	6	uismbf
for (j = 0; j < num_au; j++) {		
key_id_flag	1	bslbf
reserved	3	uismbf
au_byte_offset_size	4	bslbf
if (key_id_flag == 1) {		
key_id	128	uismbf
}		
if (au_byte_offset_size > 0) {		
au_byte_offset	N1	uismbf
}		
initialization_vector	N2	uismbf
}		
}		
if (next_key_id_flag == 1) {		
countdown_sec	4	uismbf
reserved	4	bslbf
next_key_id	128	bslbf
}		
}		

6.1.3 Semantics

num_states: number of key/IV combinations described in this ECM

next_key_id_flag: if 1, `next_key_id` is provided in this ECM

iv_size: size of initialization vectors, in bytes. 8-byte and 16-byte initialization vectors shall be supported.

transport_scrambling_control: value of the `transport_scrambling_control` field that corresponds to this key/IV combination

default_key_id: default key ID used with the access units listed in this CETS ECM.

num_au number of samples (access units) that share the same `transport_scrambling_control` state and key ID.

key_id_flag: if 1, explicit key ID will be provided. If 0, default key ID is used.

au_byte_offset_size: size of `au_byte_offset`, in bytes.

key_id: key identifier used for key acquisition for this sample (access unit)

au_byte_offset: in case of multiple access units packed in one PES packets, byte offset from the first byte of PES payload till the first byte encrypted using the current key/IV combination. Field length is given by `au_byte_offset_size`.

NOTE Offsets are relative to the first byte of PES packet payload, hence the first access unit of each PES packet will have a zero offset. Non-zero offsets correspond to the additional access units within the same PES packet. The access unit loop is over an integer number of PES packets, and every zero value of au_byte_offset corresponds to the start of a PES packet.

initialization_vector: initialization vector used in this key/IV combination. Field length is given by `iv_size`.

countdown_sec: seconds left till the nearest key rotation

next_key_id: key ID that is expected be used first in `countdown_sec` seconds in the future

NOTE The upcoming key ID's are added in order to allow the client pre-fetch them in time for the key rotation;, hence countdown value should be non-zero, i.e. a key rotation notification should be sent at least 1 sec. ahead of time. Countdown is imprecise and non-binding – it only provides an early warning. Moreover, there is no guarantee that the indicated key will be used at the indicated time. A mandatory notification of key use is in `default_key_id` and `key_id` fields of CETS ECM.

6.2 CETS PSSH

6.2.1 General

A CETS PSSH packet carries the complete payload of a `pssh` box, as defined in ISO/IEC 23001-7. Each packet uses private syntax and carries a `pssh` box along with an MD5 hash for integrity.

The first transport stream packet of a CETS PSSH shall have `payload_units_start_indicator` set to 1.

6.2.2 Syntax

Syntax	No. of bits	Format
`cets_pssh_packet(){`		
`md5_flag`	1	bslbf
`reserved`	31	bslbf
`pssh_box()`		FullBox
`if (md5_flag == 1)`		
`md5sum`	128	bslbf
`}`		
`}`		

6.2.3 Semantics

md5_flag: if true, MD5 hash will appear after the `pssh` box

pssh_box: complete `pssh` box, as defined in ISO/IEC 23001-7.

NOTE The message length is derived from fields inherited by `pssh` from the `Box` class. See ISO/IEC 14496-12 for details on box structure.

md5_sum: MD5 hash of the CETS PSSH packet, starting from `md5_flag` and continuing till the last byte of the `pssh` box

6.3 CA_descriptor

6.3.1 General

`CA_descriptor` is used to indicate properties of the content protection scheme.

NOTE It is recommended that `CA_descriptor` size be set such that PMT and CAT sections can fit into a single transport stream packet.