ISO/IEC JTC 1/SC 29 N

Date: 2012-10-11

ISO/IEC CD 23001-9

ISO/IEC JTC 1/SC 29/WG 11

Secretariat:

Information technology — MPEG systems technologies — Part 9: Common Encryption of MPEG-2 Transport Streams

Technologies de l'information — Technologies des systèmes MPEG — Partie 9: Le cryptage commune de MPEG-2 Transport Stream

Document type: International Standard
Document subtype:
Document stage: (30) Committee
Document language: E

Macintosh HD:Users:xli:Downloads:29n13191t.doc STD Version 2.1c2

Contents

Page

Foreword ... iv
1 Scope ... 1
2 Normative References ... 1
3 Definitions ... 1
3.1 Terms and Definitions ... 1
3.2 Abbreviations ... 2
4 Introduction ... 3
4.1 General ... 3
4.2 Theory of Operation ... 3
5 Encryption Parameter Signalling ... 3
5.1 CETS ECM ... 3
5.1.1 General ... 3
5.1.3 Semantics ... 4
5.2 CETS EMM ... 5
5.2.1 General ... 5
5.2.2 Syntax ... 5
5.2.3 Semantics ... 5
5.3 CA_descriptor ... 5
5.3.1 General ... 5
5.3.2 Syntax ... 5
5.3.3 Semantics ... 6
6 Operation ... 6
6.1 Restrictions on Encryption ... 6
6.1.1 General ... 6
6.1.2 ISO/IEC 14996-10 and ISO/IEC 23008-2 ... 6
6.2 Multiple elementary streams ... 7

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 Part 7 of ISO/IEC 23001, Common encryption in ISO base media file format files. 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 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 and corrigenda) applies.

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

ITU-T Rec.H.262 | ISO/IEC 13818-2, *Information technology – Generic coding of moving pictures and associated audio information: Video*

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 (technically identical to ISO/IEC 15444-12)*

ISO/IEC 14496-15, Information technology – Coding of audio-visual objects – Part 15: Carriage of NAL unit structured video in the ISO Base Media File Format

ISO/IEC 23001-7, Information technology – MPEG systems technology – 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.*

3 Definitions

3.1 Terms and Definitions

Encrypted AU A part of elementary stream containing one access unit. In case of ISO/IEC 14496-10 and ISO/IEC 23008-2, these are comprised of one or more NAL units.

3.2 Abbreviations

MPEG-2 TS MPEG-2 Transport Stream (ISO/IEC 13818-1)

ISO-BMFF ISO Base Media File Format (ISO/IEC 14496-12)

ECM Entitlement Control Message (ISO/IEC 13818-1)

CENC Common Encryption (ISO/IEC 23001-7)

EAU Encrypted Access Unit

AES Advanced Encryption Standard

CBC Cipherblock Chaining

CTR Counter Mode

AU Access Unit

KID Key Identifier

IV Initialization Vector

NAL Network Access Layer

PSI Program Specific Information

PAT Program Association Table

CAT Conditional Access Table

PMT Program Map Table

CETS Common Encryption of MPEG-2 Transport Streams

EMM Entitlement Management Message

ECM entitlement control message

PES packetized elementary stream

PTS presentation time stamp

DTS decoding time stamp

RAP random access point

PID Packet Identifier

VCL Video Coding Layer

4 Introduction

4.1 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.

.

4.2 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 `scrambling_bits` field. Thus the transport stream packet payload is in the clear if the `scrambling_bits` value is 0, or encrypted with key/IV combination identified by the `scrambling_bits` value within the nearest ECM.

NOTE: as common encryption is applied separately per each access unit, scrambling_bits value will most probably change each access unit, hence ECM's will appear very frequently. Only the last ECM preceding the beginning of an access unit, and the first ECM following its start are guaranteed to contain the correct key/IV combination for a given access unit, as `scrabmling_bits` is a 2-bit field and has only 3 available 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 EMM. This does not necessarily mean that EMM 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.

5 Encryption Parameter Signalling

5.1 CETS ECM

5.1.1 General

At the very basic level, CETS ECM provides (a) key ID and IV's for each `scrambling_bits` state, 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.

5.1.2 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
current_key_id	128	uismbf
for (i = 0; i < num_states; i++) {		
scrambling_bits	2	bslbf
num_au	6	uismbf
for (j = 0; j < num_au; j++) {		
key_id_flag	1	bslbf
au_byte_offset_size	3	uismbf
reserved	4	bslbf
if (key_flag == 1) {		
key_id	128	uismbf
}		
if (au_byte_offset_flag == 1) {		
au_byte_offset	N	uismbf
}		
initialization_vector	8*iv_size	uismbf
}		
}		
if (next_key_id_flag == 1) {		
countdown_sec	4	
reserved	4	
next_key_id	128	
}		
}		

5.1.3 Semantics

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

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

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

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

num_samples: number of samples (access units) that share the same `scramble_bits` state and PID.

key_id: key identifier used for key acquisition

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.

initialization_vector initialization vector used in this key/IV combination.

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 current_key_id and key_id fields of CETS ECM

5.2 CETS EMM

5.2.1 General

EMM carries the complete payload of a `pssh` message, as defined in ISO/IEC 23001-7

The first packet of CETS EMM shall have `payload_units_start_indicator` set to 1.

5.2.2 Syntax

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

5.2.3 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).This means that the box length is a 32-bit word at offset of 4 bytes, and if the latter has the value of 1, the length is given by a 64-bit word at 12-byte offset. If length is zero, the box continues till the next packet on this PID that has `payload_unit_indicator set`. This is conceptually identical to PES packet length in ISO/IEC 13818-1.

Alex Giladi 10/19/2012 4:46 AM
Comment [1]: Unclear what is the length – maybe add a different explanation

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

5.3 CA_descriptor

5.3.1 General

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

5.3.2 Syntax

Syntax	No. of bits	Format
CA_descriptor(){		

Syntax	No. of bits	Format
descriptor_tag	8	bslbf
descriptor_length	8	bslbf
CA_SystemID //'ce'	16	bslbf
reserved	3	bslbf
CA_PID	13	uismbf
scheme_type	32	baslbf
scheme_version	32	uismbf
num_system_id	8	bslbf
encryption_algorithm	24	uismbf
for (i = 0; i < num_system_id; i++) {		
system_id	128	bslbf
}		
for (i=0; i<N;i++) {		
private_data_byte	8	uismbf
}		
}		

5.3.3 Semantics

CA_SystemID: system identifier of this system, as defined in ISO/IEC 13818-1. Shall be 'ce' in this part of ISO/IEC 23001.

CA_PID: as defined in ISO/IEC 13818-1

scheme_type: same as `schm`.scheme_type field.

scheme_version: same as `schm`.scheme_version field

num_system_id: number of 128-bit system ID's is provided below.

encryption_algorithm: specifies the encryption algorithm, same as `tenc`.IsEncrypted

system_id: same as `pssh`.SystemID

6 Operation

6.1 Restrictions on Encryption

6.1.1 General

Same key and initialization vector shall be used only on one access units

Only one key and one initialization vector shall be necessary for decrypting a payload of a TS packet.

6.1.2 ISO/IEC 14996-10 and ISO/IEC 23008-2

Start codes and NAL headers shall not be encrypted; moreover non-VCL access units shall not be encrypted. : It is recommended not to encrypt slice headers as well.

> NOTE: this means that the implementer is guaranteed to have the ability to parse these: e.g. irrespective of the value of scrambling bits it can reliably parse PTS, DTS, AUD and SPS/PPS. With that said, the implementer should not assume that start code emulation prevention was applied to packets with a non-zero value of scrambled_bits.

<< ed: need to check which parts of audio stream need to be in the clear>>

6.2 Multiple elementary streams

Key/IV information for every encrypted PID shall be carried in a separate ECM PID.