FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
23001-9**

ISO/IEC JTC **1**/SC **29**

Secretariat: JISC

Voting begins on:
2016-01-13

Voting terminates on:
2016-03-13

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 FDIS 23001-9:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

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 (ISO/IEC 23001-9:2014), which has been technically revised.

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*

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

— *Part 11: Energy-efficient media consumption (green metadata)*

— *Part 12: Sample Variants in the ISO base media file format*

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.

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

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

ISO/IEC 23001-7[1)], *Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files*

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

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

Rec. ITU-T H.265 | ISO/IEC 23008-2[1)], *Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 2: High efficiency video coding*

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 encrypted access unit

Note 1 to entry: In case of Rec. ITU-T H.264 | ISO/IEC 14496-10 and Rec. ITU-T H.265 | ISO/IEC 23008-2, these are comprised of one or more NAL units.

1) To be published.

4 Abbreviated terms

AES	Advanced Encryption Standard (FIPS-197)
AU	Access Unit
CAT	Conditional Access Table (Rec. ITU-T H.222.0 | 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 (Rec. ITU-T H.222.0 | ISO/IEC 13818-1)
EAU	Encrypted Access Unit
ECM	Entitlement Control Message (Rec. ITU-T H.222.0 | 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 (Rec. ITU-T H.222.0 | ISO/IEC 13818-1)
NAL	Network Access Layer (Rec. ITU-T H.264 | ISO/IEC 14496-10, Rec. ITU-T H.265 | ISO/IEC 23008-2)
PAT	Program Association Table (Rec. ITU-T H.222.0 | ISO/IEC 13818-1)
PES	Packetized Elementary Stream (Rec. ITU-T H.222.0 | ISO/IEC 13818-1)
PID	Packet Identifier (Rec. ITU-T H.222.0 | ISO/IEC 13818-1)
PMT	Program Map Table (Rec. ITU-T H.222.0 | ISO/IEC 13818-1)
PTS	Presentation Time Stamp (Rec. ITU-T H.222.0 | ISO/IEC 13818-1)
RAP	Random Access Point
VCL	Video Coding Layer (Rec. ITU-T H.264 | ISO/IEC 14496-10, Rec. ITU-T H.265 | ISO/IEC 23008-2)

5 Overview

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 this part of ISO/IEC 23001 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 ISO/IEC 23001, and depends on the key system in question. The abstraction used in this part of ISO/IEC 23001 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, it is necessary 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.

If the value of CA_System_ID equals ‘ce’, and `transport_scrambling_control` has a value other than ‘00’, the complete transport stream packet payload contains only encrypted bytes. In the same case when the value of CA_System_ID value is ‘cf’, parts of the payload may be non-encrypted, and encrypted and non-encrypted byte ranges are signalled in an adaptation field descriptor cets_byte_range_descriptor.

NOTE 1 In the ‘ce’ CA system, if a packet has `transport_scrambling_control` value other than ‘00’, the encrypting application places only encrypted bytes into its payload; combining non-encrypted and encrypted bytes in the same packet payload is disallowed. The same applies to byte ranges in the ‘cf’ CA system.

NOTE 2 Given that common encryption is applied separately per each access unit, `transport_scrambling_control` value will most probably change with 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 `transport_scrambling_control` 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 ISO/IEC 23001, 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.

5.3 Notation

This part of ISO/IEC 23001 uses same notation as used in Rec. ITU-T H.222.0 | ISO/IEC 13818-1.

This part of ISO/IEC 23001 makes extensive use of fields with possibly different lengths. An additional short-hand notation is used to improve readability in these cases: length field names are referenced within the “number of bits” column of syntax tables. The alias name for the length field is provided in parenthesis in non-bold font at the same line as the length field, and the number of bits is given as a function of that field.

In the example below, SFL is an alias for the some_field_length_qwords field which indicates length in units of 64-bit words. As the latter can have values of 0…3, some_field can have lengths of 0, 64, 128 and 192 bits. Note that stating that some_field is a 0-bit field implies that some_field is not present (in the example below this would result in some_structure() being a 1-byte structure.

Syntax	No. bits	Mnemonic
some_structure {		
some_field_length_qwords (SFL)	2	uimsbf
reserved	6	bslbf
some_field	SFL*64	uismbf
}		

6 Encryption Parameter Signalling

6.1 CETS ECM

6.1.1 General

CETS ECM provides (a) key ID and initialization vector for each state of `transport_scrambling_control`, and (b) notification of upcoming key rotation. CETS ECM's are expected to be carried very frequently (one ECM per AU) for cases where IV or/and key are changed for each sample.

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 shall always be 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	uimsbf
next_key_id_flag	1	bslbf
reserved = 0	5	bslbf
iv_size (IVS)	8	uismbf
default_key_id	128	uismbf
for (i = 0; i < num_states; i++) {		
transport_scrambling_control	2	bslbf
num_eu	6	uismbf
for (j = 0; j < num_eu; j++) {		
key_id_flag	1	bslbf
encryption_block_start_flag	1	bslbf
reserved = 0	2	bslbf
eu_byte_offset_size (EBOS)	4	uismbf
if (key_id_flag == 1){		bslbf
key_id	128	
}		
eu_byte_offset	EBOS*8	uismbf
initialization_vector	IVS*8	bslbf
}		
if (iv_size == 0) {		
// only cf system	1	
key_id_flag	2	bslbf
constant_initialization_vector_length_qwords (CIVL)	5	bslbf
reserved = 0		bslbf