 ISO/IEC JTC 1/SC 29/WG 3 N1428

**ISO/IEC JTC 1/SC 29/WG 3**

**MPEG Systems   
Convenorship: KATS (Korea, Republic of)**

**Document type:** Output Document

**Title: WD of ISO/IEC 23001-7:2023 AMD 1 AES-256 Support**

**Status:** Approved

**Date of document:** 2025-01-24

**Source:** ISO/IEC JTC 1/SC 29/WG 3

# Expected action: None

**Action due date:** None

**No. of pages:** 2 (with cover page)

**Email of Convenor:** young.L@samsung.com

**Committee URL:** <https://isotc.iso.org/livelink/livelink/open/jtc1sc29wg3>

**INTERNATIONAL ORGANISATION FOR STANDARDISATION**

**ORGANISATION INTERNATIONALE DE NORMALISATION**

**ISO/IEC JTC 1/SC 29/WG 3**

**CODING OF MOVING PICTURES AND AUDIO**

**ISO/IEC JTC 1/SC 29/WG 3 N** **01428**

**Geneva – January 2025**

|  |  |
| --- | --- |
| **Title** | **WD of ISO/IEC 23001-7:2023 AMD 1 AES-256 Support** |
| **Source** | **WG 03, MPEG Systems** |
| **Status** | **Approved** |
| **Serial Number** | **24728** |

© ISO/IEC 2017 – All rights reservedISO/IEC 14496-5:2001/PDAM 43:2017(E) 63Part 5: Reference software, AMENDMENT43: New levels of ALS simple profileInformation Technology — Coding of audio-visual objectsÉlément introductif — Élément central — Partie 5: Élément complémentaireInformation Technology — Coding of audio-visual objects — Part 5: Reference software, AMENDMENT43: New levels of ALS simple profileE2017-01-18(30) CommitteeISO/IECISO/IEC J200143AmendmentInternational Standard2017 ISO/IEC 14496‑ISO/IEC 14496‑5ISO/IEC 14496-5/PDAM 43:2017    11291 2見出し 2見出し 1     0 STD Version 2.8f30   4C:\WorkD\Standards\ISO-IEC\_14496-5\_2001\_A43\_(E).docx             ISO/IEC JTC 1/SC 29 N 24728

Date:   2025-01-24

ISO/IEC 23001-7:2023/AMD 1:2024(E)

ISO/IEC JTC 1/SC 29/WG 3

Secretariat:

Information Technology — MPEG Systems Technologies— Part 7: Common Encryption, AMENDMENT1: AES-256 Support

*Élément introductif — Élément central — Partie 14: Élément complémentaire*

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

**Copyright notice**

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

[Indicate the full address, telephone number, fax number, telex number, and electronic mail address, as appropriate, of the Copyright Manager of the ISO member body responsible for the secretariat of the TC or SC within the framework of which the working document has been prepared.]

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Information Technology — MPEG Systems Technologies— Part 7: Common Encryption, AMENDMENT1: AES-256 Support

*Editor's note: the following changes aims at supporting AES-256 and define a brand for Common Encryption. There is an open question about possible impacts on Common encryption scheme types in section 4.2. 2 options are considered:*

*1. Either define new 4CCs to distinguish modes for AES-128 from modes for AES-256,*

*2. Or keep the same 4CCs and consider that each applies to both AES-128 and AES-256*

*3. Another option has been considered at MPEG#149:*

* *No new protection scheme for the moment*
* *Rather useTrackEncryptionBox to indicate actual CENC features in use in an encrypted file.*

*In section 1 Scope, replace*

" The AES-128 symmetric block cipher is incorporated by reference to encrypt elementary stream data contained in media samples. Both AES counter mode (CTR) and Cipher Block Chaining (CBC) are specified in separate protection schemes."

*with*

" The AES-128 or AES-256 symmetric block cipher is incorporated by reference to encrypt elementary stream data contained in media samples. Both AES counter mode (CTR) and Cipher Block Chaining (CBC) are specified in separate protection schemes.”

*In section 3.1.1 block, replace*

"16-byte extent of sample data that may be encrypted or decrypted by the AES-128 block cipher, in which case, a cipher block. "

*with*

"16-byte extent of sample data that may be encrypted or decrypted by the AES-128 or AES-256 block cipher, in which case, a cipher block.

*In section 9.3, replace*

" Counter-mode schemes shall use the Advanced Encryption Standard, specified in Federal Information Processing Standards Publication 197, FIPS-197 published by the United States National Institute of Standards and Technology (NIST) using 128-bit keys in Counter Mode (AES-CTR), as specified in Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A.

AES-128 CTR mode is a 16 byte block cipher that can encrypt an arbitrary sized byte stream without need for padding or leaving a clear remainder when the last block of sample data is a partial block (1 to 15 bytes in size). "

*with*

" Counter-mode schemes shall use the Advanced Encryption Standard, specified in Federal Information Processing Standards Publication 197, FIPS-197 published by the United States National Institute of Standards and Technology (NIST) using 128-bit or 256-bit keys in Counter Mode (AES-CTR), as specified in Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A.

AES-128 CTR or AES-256 CTR mode is a 16 byte block cipher that can encrypt an arbitrary sized byte stream without need for padding or leaving a clear remainder when the last block of sample data is a partial block (1 to 15 bytes in size). “

*In section 9.4.3, replace*

“Full sample AES-CBC mode shall use the Advanced Encryption Standard specified by AES [FIPS197] using 128-bit keys in Cipher Block Chaining mode (AES-CBC-128), as specified in Block Cipher Modes [NIST 800-38A].”

*with*

" Full sample AES-CBC mode shall use the Advanced Encryption Standard specified by AES [FIPS197] using 128-bit or 256-bit keys in Cipher Block Chaining mode (AES-CBC-128 or AES-CBC-256), as specified in Block Cipher Modes [NIST 800-38A].”

*In section 8.2.1, add :*

The following flags are defined for TrackEncryptionBox:

AES\_256\_flag: flag mask is 0x000001. This flag indicates, when set, that 256-bit key length is in use and, when not set that 128-bit length is used for the encryption keys. Default value is 0.

full\_sample\_encryption: flag mask is 0x000002. This flag indicates, when set, that full sample encryption is in use and when not set that subsample encryption is in use. Default value is 0.

multi\_key: flag mask is 0x000004. This flag indicates whether there is a single key in use (value 0) of multiple keys (value 1). Default value is 0.

use\_senc: flag mask is 0x000008. This flag indicates, when set, that the ‘senc’ box is used to provide CENC SAI and, when not set, that sample auxiliary information is used to provide CENC SAI. Default value is 0.

allow\_partial\_last\_block: flag mask is 0x000010. This flag indicates, when set, that the last cipher block in a sample may be a partial cipher block (less than 16 bytes). When not set, it indicates that there are no partial cipher blocks (no cipher blocks less than 16 bytes).

pattern\_mode: flag mask is 0x000020. This flag indicates, whether pattern encryption mode is in use (value 1) or not (value 0).

*[Ed. Note: we encourage experts to comment on the above proposed flags: are some relevant features missing?, are some of the proposed ones not so relevant? …]*

*In section 8.2.2, Replace the section with :*

**8.2.2. Syntax**

aligned(8) class TrackEncryptionBox extends FullBox('tenc', version, flags)  
{  
 unsigned int(8) reserved = 0;  
 if (version==0) {  
 unsigned int(8) reserved = 0;  
 }  
 else { // version is 1 or greater  
 unsigned int(4) default\_crypt\_byte\_block;  
 unsigned int(4) default\_skip\_byte\_block;  
 }  
 unsigned int(8) default\_isProtected;  
 unsigned int(8) default\_Per\_Sample\_IV\_Size;  
 unsigned int(8)[16] default\_KID;  
 if (default\_isProtected ==1 && default\_Per\_Sample\_IV\_Size == 0) {  
 unsigned int(8) default\_constant\_IV\_size;  
 unsigned int(8)[default\_constant\_IV\_size] default\_constant\_IV;  
 }  
}

*Add a new Annex B – (normative) Common Encryption Brands*

1. The 'coen' brand
   1. Overview

The requirements for files and readers compliant to the brand 'coen' are defined in the following subclause. It is meant to be independent of the actual protection schemes ('cenc', 'cens', 'cbc1', 'cbcs' …).

* 1. Requirements on files

Files containing the brand 'coen' in the compatible brands array of the FileTypeBox shall conform to the constraints defined in this subclause.

The following boxes are required in a file under the 'coen' brand. The Version column in the following table lists the versions of the boxes allowed by this brand. Other versions of the boxes shall not be present. The Flags column in the following table lists the flags that may be present in files of this brand and are required to be supported by the readers of this brand. If other flags of the boxes have been specified, they may be present but are not required to be supported by the readers of this brand.

NOTE A '-' in the Version and Flags column indicates that the box is a container box or does not support versioning.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Hierarchy of boxes** | | | | **Version** | **Flags** | **Box description** |
| enca  encf  encm  encp  encs  enct  encu encv  enc3 |  |  |  | - | - | Protected Sample Entry. At least one of these entry needs to be present. |
|  | sinf |  |  | - | - |  |
|  |  | frma |  | - | - |  |
|  |  | schm |  | 0 | 0x000001 |  |
|  |  | schi |  | - | - |  |
|  |  |  | tenc | 0,1 | Defined flags |  |

* 1. Requirements on readers

Support for the following boxes is required under the 'coen' brand. The Version column in the following table specifies the versions of the boxes that shall be supported by the readers of the 'coen' brand.

NOTE A '-' in the Version and Flags column indicates that the box is a container box or does not support versioning nor flagging.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Hierarchy of boxes** | | | | **Version** | **Flags** | **Box description** |
| enca  encf  encm  encp  encs  enct  encu encv  enc3 |  |  |  | - | - | Readers may support only some Protected Sample Entry types. Derived specifications may require specific support. |
|  | sinf |  |  | - | - |  |
|  |  | frma |  | - | - |  |
|  |  | schm |  | 0 | 0x000001 |  |
|  |  | schi |  | - | - |  |
|  |  |  | tenc | 0,1 | Defined flags |  |
| moov  moof |  |  |  | - | - |  |
|  | pssh |  |  | 0,1 | 0 |  |
| sbtl  traf |  |  |  | - | - |  |
|  | sbgp |  |  | 0,1 |  |  |
|  | sgpd |  |  | 0,1,2 | 0 |  |
|  |  | seig |  | - | - |  |
|  | saiz |  |  | 0 | 0x000001 |  |
|  | saio |  |  | 0,1 | 0x000001 |  |
| trak  traf |  |  |  | - | - |  |
|  | senc |  |  | 0 | 0x000002 |  |

*[Ed. Note: Open question => Is one brand sufficient to represent today’s support of “old tools”?*

* *For example, some devices only support ‘saio’/’saiz’, others only support ‘senc’. Should we define 2 different brands?*
* *Similarly, use of ‘seig’ is specific to some use cases (e.g. multi-key support). Should this be in a separate brand?*

*]*