 ISO/IEC JTC 1/SC 29/WG 3 N1714

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

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

**Document type:** Output Document

**Title: Potential improvement of ISO/IEC 23001-7:2023 DAM 1 AES-256 Support**

**Status:** Approved

**Date of document:** 2026-01-26

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

# Expected action: Publish

**Action due date:** 2026-01-26

**No. of pages:** 10 (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** **01714**

**Online– January 2026**

|  |  |
| --- | --- |
| **Title** | **Potential improvement of ISO/IEC 23001-7:2023 DAM 1 AES-256 Support** |
| **Source** | **WG 03, MPEG Systems** |
| **Status** | **Approved** |
| **Serial Number** | **25903** |

© 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 25903

Date:  2026-01-26

ISO/IEC 23001-7:2023/AMD 1:2026(E)

ISO/IEC JTC 1/SC 29/WG 3

Secretariat:

Information Technology — MPEG Systems Technologies— Part 7: Common Encryption in ISO base media file format files — Amendment 1: Support for AES-256

*Élément introductif — Élément central — Partie 5: 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 in ISO base media file format files — Amendment 1: Support for AES-256

*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 9.4.1, replace*

“Full sample encryption may be used for all encrypted media types other than NAL structured video, which shall use Subsample encryption.”

*with*

“Full sample encryption or subsample encryption may be used for all encrypted media types. NAL structured video shall use Subsample encryption.”

*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 9.5.1, add the following paragraph after the first paragraph:*

“While subsample encryption is mandatory for NAL structured video, it may also be used for other media types”

*Add a new section 9.5.3:*

**9.5.3 Subsample encryption of other tracks and items than NAL structured video tracks**

This specification does not provide subsample definitions for non NAL structured video tracks or items and therefore does not specify subsample encryption for these tracks and items.

NOTE: Derived specifications can provide format specific definitions and thereby enable subsample encryption of such tracks or items.

*In section 8.2.1, add:*

The following 2-bits flags are defined for TrackEncryptionBox:

use\_subsample\_encryption: flag mask is 0x000003.

When (flags & 0x000003) is equal to 0, it indicates that the that for any sample associated with this ‘tenc’ box, the presence or absence of BytesOfClearData and BytesOfProtectedData is undefined.

When (flags & 0x000003) is equal to 1, it indicates that for any sample associated with this ‘tenc’ box, BytesOfClearData and BytesOfProtectedData shall be present in the structure describing the encryption parameters, i.e., either using the senc’ box or the sample auxiliary information boxes (‘saiz’ and ‘saio’ boxes).

When (flags & 0x000003) is equal to 2, BytesOfClearData and BytesOfProtectedData shall not be present,

The value 0x000003 is reserved.

Default value is 0.

use\_multi\_key: flag mask is 0x00000C.

When ((flags & 0x00000C) >> 2) is equal to 0, it indicates that for samples associated with this ‘tenc’ box, the use of multiple keys is undefined,

When ((flags & 0x00000C) >> 2) is equal to 1, it indicates that for samples associated with this ‘tenc’ box, there are multiple keys in use. If the ‘seig’ sample group is used, there shall be at least one ‘seig’ sample group description entry with multi\_key\_flag set to 1.

When ((flags & 0x00000C) >> 2) is equal to 1, it indicates that there is a single key in use per sample. If the seig’ sample group is used, the multi\_key\_flag in all ‘seig’ sample group description entries shall be set to 0.

The value 0x00000C is reserved.

Default value is 0.

use\_senc: flag mask is 0x000030.

When ((flags & 0x000030) >> 4) is equal to 0, the presence or absence of the ‘senc’ box is undefined.

When ((flags & 0x000030) >> 4) is equal to 1, it indicates, that the ‘senc’ box is used to provide sample encryption information for samples associated with this ‘tenc’ box.

When ((flags & 0x000030) >> 4) is equal to 2, there shall be no ‘senc’ box associated with samples associated with this ‘tenc’ box.

The value 0x000030 is reserved.

Default value is 0.

use\_sai: flag mask is 0x0000C0.

When ((flags & 0x0000C0) >> 6) is equal to 0, it indicates that the presence or absence of ‘saiz’ and ‘saio’ boxes is undefined.

When ((flags & 0x0000C0) >> 6) is equal to 1, it indicates that the ‘saiz’ and ‘saio’ boxes are used to sample encryption information for samples associated with this ‘tenc’ box.

When ((flags & 0x0000C0) >> 6) is equal to 2, there shall be no sample auxiliary information boxes associated for samples associated with this ‘tenc’ box.

The value 0x0000C0 is reserved.

Default value is 0.

use\_seig: flag mask is 0x000300.

When ((flags & 0x000300) >> 8) is equal to 0, it indicates that the presence or absence of a ‘seig’ sample group is undefined.

When ((flags & 0x000300) >> 8) is equal to 1, it indicates that some samples associated with this ‘tenc’ box are associated with a ‘seig’ sample group.

When ((flags & 0x000300) >> 8) is equal to 2, there shall be no ‘seig’ sample group box associated with the samples associated with this ‘tenc’ box.

The value 0x0000300 is reserved.

Default value is 0.

use\_encrypted\_slice\_header: flag mask is 0x000C00.

When ((flags & 0x000C00) >> 10) is equal to 0, the encryption or not of the slice headers of the NAL units is undefined.

When ((flags & 0x000C00) >> 10) is equal to 1, it indicates that all NAL units are encrypted, including the slice header.

When ((flags & 0x000C00) >> 10) is equal to 2, the slice headers in the NAL units are unencrypted.

The value 0x0000C00 is reserved.

Default value is 0.

*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 if (version >= 1 ){ // version is 1 or greater  
 unsigned int(4) default\_crypt\_byte\_block;  
  unsigned int(4) default\_skip\_byte\_block;  
 if (version >= 2 ){   
 unsigned int(1) use\_AES\_256; unsigned int(7) reserved\_bits;   
 }  
 }  
 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;  
 }  
}

*In section 8.2.3, Add the following semantics:*

use\_AES\_256 indicates, when equal to 1, that encrypted data in the samples associated with this ‘tenc’ box was encrypted using a 256-bit key and, when equal to 0, that a 128-bit key was used. Default value is 0.

*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' …) and only providing constraints for the boxes used for signaling encryption. It does not constrain encryption parameters.

* 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 |  |
|  | saiz |  |  | 0 | 0x000001 |  |
|  | saio |  |  | 0,1 | 0x000001 |  |
| trak  traf |  |  |  | - | - |  |
|  | senc |  |  | 0 | 0x000002 |  |