 ISO/IEC JTC 1/SC 29/WG 3 N1754

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

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

**Document type:** Output Document

**Title: Working Draft of ISO/IEC 23001-7:2023 AMD2: Brand definitions**

**Status:** Approved

**Date of document:** 2026-01-29

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

# Expected action: Publish

**Action due date:** 2026-01-29

**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** **01754**

**Online – January 2026**

|  |  |
| --- | --- |
| **Title** | **Working Draft of ISO/IEC 23001-7:2023 AMD2: Brand definitions** |
| **Source** | **WG 03, MPEG Systems** |
| **Status** | **Approved** |
| **Serial Number** | **25955** |

© 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 25955

Date:  2026-01-29

ISO/IEC 23001-7:2023/AMD 2:2026(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 2: Brand definitions

*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 2: Brand definitions

*In section 9.4, consider how the following restrictions could be lifted:*

Section 9.4, currently has two modes for full sample encryption:

1. one for AES-CTR (section 9.4.2) where all bytes are encrypted (even if not complete),
2. one for AES-CBC (section 9.4.3) where the last bytes are left in the clear if less than a full block (called “whole-block full sample encryption”).

It is **currently not possible to use full sample encryption** (‘cenc’ or ‘cbc1’ protection schemes) **for a NALU-based video**, for example in case the content provider does not want to expose any of the NAL structure of the stream.

The section 9.4.1 states:

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

Moreover, the definitions of the cenc (section 10.1) and cbc1 (section 10.2) protection schemes both state:

*“Encrypted video tracks or items using NAL unit structured video conforming to ISO/IEC 14496-15 shall be protected using subsample encryption specified in 9.5, …”*

The restriction only comes from the definitions of the protection schemes, and **most implementations are likely able to support full-sample encryption even for NALU-based video tracks**.

*In section 9.5.1; the definition of subsample encryption should be clarified:*

Each subsample shall have an unprotected part followed by a protected part, only one of which may be zero bytes in length (usually both are non-zero values). The total length of all of the subsamples shall be equal to the size of the sample itself, and they shall not overlap (BytesOfClearData + BytesOfProtectedData for all subsamples that make up a sample).

[Ed. Note: the specification never explicitly states that CENC SAI shall be present, this should be clarified.]

*In section 9.6, consider how the following restrictions could be lifted:*

Section 9.6 currently defines **pattern encryption** as a simple tool allowing to protect only N out of K blocks. In theory, the tool **could be applied to any protection scheme**, but is only allowed on subsample-based encryption modes in the definitions of ‘cens’ and ‘cbcs’ protection schemes, consequently mostly for NALU-based media only (except for ‘cbcs’ scheme).

[Ed. Note: It would be interesting to investigate how these restrictions could be lifted, especially considering the following statement from section 10.3:

“*Derived specifications may relax this constraint to allow usage of subsample encryption as specified in subclause 9.5, in which case pattern encryption as specified in 9.6 shall be used.*” ]

*In section 10.3, consider shall as a should:*

Section 10.3 states, for ‘cens’ AES-CTR, that:

" *The BytesOfProtectedData size shall be a multiple of 16 bytes to avoid partial cipher blocks in subsamples*”

(while the definition of cenc in 10.2 is considering a “should be a multiple of 16 bytes” …)

[Ed. Note: We need to understand why the "shall” is used in cens, as this decision is taken by the encryptor but does not impact the decryptor module]

*In section 10.3, rephrase:*

“The BytesOfProtectedData size shall be a multiple of 16 bytes to avoid partial cipher blocks in subsamples.”

*With:*

“In video tracks using subsample encryption, the BytesOfProtectedData size shall be a multiple of 16 bytes to avoid partial cipher blocks in subsamples.”

[Ed. Note: this is because “The BytesOfProtectedData size ” is meaningless in full sample encryption]

*In section 10.3, fix the contradiction:*

The ‘cens’ protection scheme states that

* “When a single key applies to each sample, encrypted tracks or items not using NAL structured video shall be protected using whole-block full-sample encryption as specified in subclause 9.7.” and
* “Constant IVs shall not be used”,

[Ed. Note: We note that the whole-block full sample encryption (9.7) is using constant IVs. The text should then be corrected to indicate usage of full sample encryption (9.4).]

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

1. The 'coeg' brand
   1. Overview

The requirements for files and readers compliant to the brand 'coeg' 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, possibly with the 'seig' sample group. It does not constrain encryption parameters.

* 1. Requirements on files

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

The brand 'coeg' requires support for all file features of the 'coen' brand. In addition, files may contain boxes for 'seig' sample group.

* 1. Requirements on readers

Readers shall support all boxes required under the 'coen' brand plus the following box.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Hierarchy of boxes** | | | | **Version** | **Flags** | **Box description** |
|  |  | seig |  | - | - | CencSampleEncryptionInformationGroupEntry |
|  |  |  |  |  |  |  |

1. The 'coe2' brand
   1. Overview

The requirements for files and readers compliant to the brand 'coe2' 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, especially the version 2 of the TrackEncryptionBox. It does not constrain encryption parameters.

* 1. Requirements on files

Files containing the brand 'coe2' in the compatible brands array of the FileTypeBox shall conform to the constraints defined in this subclause.

The brand 'coe2' requires support for all file features of the 'coen' brand. In addition, files may contain TrackEncryptionBox with a version 2.

* 1. Requirements on readers

Readers shall support all boxes required under the 'coen' brand plus the following versions of the TrackEncryptionBox.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Hierarchy of boxes** | | | | **Version** | **Flags** | **Box description** |
|  |  |  | tenc | 0,1, **2** | Defined flags | TrackEncryptionBox |
|  |  |  |  |  |  |  |

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

1. Functional brands
   1. Overview

The following “functional” brands are defined as a restriction of Common Encryption tools for typical combinations summarized in Table XX (below). These brands are expected to be used by derived specifications to clearly indicate what Common Encryption tools are supported. Derived specifications can define how the brand is used. Care should be taken when these brands are used in the file especially when multiple tracks are present.

In particular, derived specifications should:

- Select structural brand (one or more)

- Select functional brands (one or more)

- Define the restrictions, if any, on the remaining free parameters; e.g. the actual pattern for ‘cbcs’ (for example the 1:9 pattern).

|  |  |  |  |
| --- | --- | --- | --- |
| **Protection scheme** | **Full sample**  **or subsample encryption** | **Key length**  **(in bits)** | **Functional brand** |
| ‘cenc’ | Full sample | 128 | ‘ce1f’ |
| 256 | ‘ce2f’ |
| Subsample | 128 | ‘ce1s’; ‘co1s’ |
| 256 | ‘ce2s’ |
| ‘cbc1’ | Full sample (non NAL) | 128 | ‘cb1f’\* |
| 256 | Not needed |
| Subsample | 128 | Not needed |
| 256 |
| ‘cens’ | Full sample  (whole block for non NAL) | 128 | Not needed |
| 256 |
| Subsample | 128 |
| 256 |
| ‘cbcs’ | Full sample  (whole block for non NAL) | 128 | ‘cb1f’\* |
| 256 | ‘cb2f’ |
| Subsample | 128 | ‘cb1s’ |
| 256 | ‘cb2s’ |
| ‘sve1’ | Not applicable | 128 | Not needed |
| 256 |

Table XX: list of functional brands

\*about ‘cb1f’: multiple protection schemes are not encouraged: for example, as ‘cbcs’ whole block full sample and ‘cbc1’ full sample are equivalent according to sections 9.7 and 9.4.3, only one, common, brand is defined.

* 1. Definitions

|  |  |
| --- | --- |
| *Brand value* | *Requirements* |
| ‘ce1f’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**ce**nc’.  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 0 * use\_subsample\_encryption = 0x02 * default\_crypt\_byte\_block = 0 * default\_skip\_byte\_block = 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |
| ‘ce2f’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**ce**nc’.  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 1 * use\_subsample\_encryption = 0x02 * default\_crypt\_byte\_block = 0 * default\_skip\_byte\_block = 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |
| ‘ce1s’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**ce**nc’.  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 0 * use\_subsample\_encryption = 0x01 * default\_crypt\_byte\_block = 0 * default\_skip\_byte\_block = 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |
| ‘co1s’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**ce**nc’.  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 0 * use\_subsample\_encryption = 0x01 * use\_encrypted\_slice\_header = 0x100 * default\_crypt\_byte\_block = 0 * default\_skip\_byte\_block = 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |
| ‘ce2s’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**ce**nc’,  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 1 * use\_subsample\_encryption = 0x01 * default\_crypt\_byte\_block = 0 * default\_skip\_byte\_block = 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |
| ‘cb1f’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**cb**cs’or ‘cbc1’  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 0 * use\_subsample\_encryption = 0x02 * default\_crypt\_byte\_block shall not be 0 * default\_skip\_byte\_block shall not be 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |
| ‘cb2f’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘cbc1’  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 1 * use\_subsample\_encryption = 0x02 * default\_crypt\_byte\_block shall not be 0 * default\_skip\_byte\_block shall not be 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |
| ‘cb1s’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**cb**cs’  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 0 * use\_subsample\_encryption = 0x01 * default\_crypt\_byte\_block shall not be 0 * default\_skip\_byte\_block shall not be 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |
| ‘cb2s’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**cb**cs’.  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * use\_AES\_256 = 1 * use\_subsample\_encryption = 0x01 * default\_crypt\_byte\_block shall not be 0 * default\_skip\_byte\_block shall not be 0   When TrackEncryptionBox has version 0 or 1, the semantics of TrackEncryptionBox version 2 still apply. |

Table YY: definitions of functional brands