Text

Description automatically generatedISO/IEC JTC 1/SC 29/WG 03 N1624

**ISO/IEC JTC 1/SC 29/WG 03  
MPEG Systems   
Convenorship: KATS (Korea, Republic of)**

**Document type:** Output Document

**Title:** Technologies under Consideration for ISO/IEC 23001-7

**Status:** Approved

**Date of document:** 2025-10-15

**Source:** ISO/IEC JTC 1/SC 29/WG 03

**No. of pages:** 7 (with cover page)

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

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

**INTERNATIONAL ORGANIZATION FOR STANDARDIZATION**

**ORGANISATION INTERNATIONALE DE NORMALISATION**

**ISO/IEC JTC 1/SC 29/WG 03 MPEG SYSTEMS**

**ISO/IEC JTC 1/SC 29/WG 03 N1624**

**October 2025, Daejeon, KR**

|  |  |
| --- | --- |
| **Title** | **Technologies under Consideration for ISO/IEC 23001-7** |
| **Source** | **WG 03, MPEG Systems** |
| **Status** | **Approved** |
| **Serial Number** | **25598** |

# Signaling of Common Encryption Tools

ISO/IEC 23001-7 relies on ISO/IEC 14496-12 structures (e.g., boxes) for signaling various aspects of encryption. As ISO/IEC 14496-12 evolves and adds versions/flags to boxes used by ISO/IEC 23001-7, the File Format group considers improving the signaling of the exact support required. Experts’ feedback is encouraged either through [GitHub](https://github.com/MPEGGroup/FileFormat/issues) or through MPEG contributions.

# Brand definitions

The on-going amendment defines one structural brand ‘coen’ and “functional” brands are under consideration.

The following “functional” brands are defined as a restriction of Common Encryption tools for typical combinations in Table XX. 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.

|  |  |
| --- | --- |
| *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:   * AES\_256\_flag = 0 * subsample\_encryption = 0 * default\_crypt\_byte\_block = 0 * default\_skip\_byte\_block = 0   The length of encryption keys shall be 128 bits.  BytesOfClearData shall be set to 0. |
| ‘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:   * AES\_256\_flag = 0 * subsample\_encryption = 1 * default\_crypt\_byte\_block = 0 * default\_skip\_byte\_block = 0   The length of encryption keys shall be 128 bits.  BytesOfClearData shall not be set to 0. |
| ‘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:   * AES\_256\_flag = 1 * subsample\_encryption = 1 * default\_crypt\_byte\_block = 0 * default\_skip\_byte\_block = 0   The length of encryption keys shall be 256 bits  BytesOfClearData shall not be set to 0. |
| ‘cbc1’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**cb**cs’  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * AES\_256\_flag = 0 * subsample\_encryption = 1 * default\_crypt\_byte\_block shall not be 0 * default\_skip\_byte\_block shall not be 0   The length of encryption keys shall be 128 bits.  AES-CBC mode partial video NAL pattern encryption (various patterns). |
| ‘cbc2’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**cb**cs’.  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * AES\_256\_flag = 1 * subsample\_encryption = 1 * default\_crypt\_byte\_block shall not be 0 * default\_skip\_byte\_block shall not be 0   The length of encryption keys shall be 256 bits.  AES-CBC mode partial video NAL pattern encryption (various patterns). |
| ‘cb19’ | The SchemeTypeBox in the ProtectionSchemeInfoBox shall be equal to ‘**cb**cs’.  When TrackEncryptionBox has version greater than or equal to 2, the following apply:   * AES\_256\_flag = 0 * subsample\_encryption = 1 * default\_crypt\_byte\_block = 1 for video * default\_skip\_byte\_block = 9 for video   The length of encryption keys shall be 128 bits.  BytesOfClearData shall not be set to 0. |

TableXX: list of functional brands

# (informative) List of CENC features combinations

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Protection Scheme | Pattern enc.  (‘tenc’ version) | Per sample Initialization Vector (IV) | **Full or partial**  **sample** | **Allow last cipher block to be partial** | **Single / multi key** | **Key length** | Sample auxiliary information? |
| **‘cenc’**  **CTR**  (10.1) | No  (v0) | Yes | Full (non NAL) | Should avoid (10.1) | Single  (non NAL) | 128 | Yes (9.3) |
| 256 |
| Multi=N.A |  |
| Partial (NAL or as defined by derived spec) | Single | 128 | Yes (9.3) |
| 256 |
| Multi (+non NAL) | 128 |
| 256 |
| **‘cbc1’**  **CBC**  (10.2) | No  (v0) | Yes | Full (non NAL) | Yes in clear (9.4.3) | Single (non NAL) | 128 | Yes  (9.4.3) |
| 256 |
| Multi=N.A |  |
| Partial (NAL or as defined by derived spec) | Forbiden  (10.2) | Single | 128 | Yes  (9.5.1) |
| 256 |
| Multi (+non NAL) | 128 |
| 256 |
| **‘cens’ CTR**  (10.3) | Yes  (v1) | Yes | Partial (NAL or as defined by derived spec) | Forbiden (10.3) | Single | 128 | Yes (9.3) |
| 256 |
| Multi (+non NAL) | 128 |
| 256 |
| Whole block full sample (**non NAL**) | Yes (9.7)  Forbiden (10.3) | Single | 128 | Yes (9.3) |
| 256 |
|  | Multi=N.A. |  |
| **‘cbcs’ CBC**  (10.4) | Yes  (v1) | No | Partial (NAL or other) | Yes (9.5) | Single (+non NAL) | 128 | Yes (10.4) |
| 256 |
| Multi (+non NAL) | 128 |
| 256 |
| Whole block full sample  (**non NAL**) | Yes (9.7) | Single | 128 | No  (SAI size is 0) |
| 256 |
| Multi=N.A |  | Yes (10.4) |
| **‘sve1’ CTR**  (10.5) | No  (v0) | Yes (10.5) | **N.A.** | Yes (9.5) | No restrictions | 128 | Yes |
| 256 |

Table 1: CENC features versus protection schemes

# Relaxing constraints in Common Encryption

This section discusses the possibility to relax constraints written in the CENC specification, while technically feasible, for different encryption modes.

## Full Sample Encryption

CENC 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.

It would then be interesting to investigate how these restrictions could be lifted.

## Pattern encryption

CENC 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).

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.*”

# Other comments

## Comments on the ‘cens’ protection scheme

### Comments “cens\_1”

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” …)

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.

### Comments “cens\_2”

In the definition of the cens (10.3) protection scheme, the following statement:

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

should be rephrased as follows:

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

This is because “The BytesOfProtectedData size ” is meaningless in full sample encryption.

### Comments “cens\_3”

The ‘cens’ protection scheme states that

* “Constant IVs shall not be used”, and
* “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.”

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).

## On subsample encryption and CENC SAI

Section 9.5.1 (definition of subsample encryption) uses BytesOfClearData and BytesOfProtectedData. However, the CENC specification never explicitly states that CENC SAI shall be present.

This should be clarified.

As another general editorial comment, we suggest the File Format group to consider moving NAL / non NAL specific sections in dedicated Annexes to avoid “polluting” definition of protection schemes with video format.