**A black and white logo

Description automatically generated** **ISO/IEC JTC 1/SC 29/WG 03 N1531**

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

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

**Document type:** Output Document

**Title: Technologies under consideration on CMAF**

**Status:** Approved

**Date of document:** 2025-04-04

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

**Expected action:** ACT

**Action due date:**

**No. of pages:** 4 (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 N1531**

**Virtual – April 2025**

|  |  |
| --- | --- |
| **Title** | **Technologies under consideration on CMAF** |
| **Source** | **WG 03, MPEG Systems** |
| **Status** | **Approved** |
| **Serial Number** | **25121** |

# Introduction

This document captures the technologies under consideration for future amendments of the Common Media Application Format (CMAF), ISO/IEC 23000-19 specification.

The current technologies under consideration include:

* On subsample encryption of CMAF tracks.
* Support for AES-256 in encrypted profiles.

# On subsample encryption of CMAF tracks

# 2.1 Abstract

Proposal to explicitly allow partial encryption for non-video tracks

# 2.2 Introduction

Media encryption in ISOBMFF can be applied either as full sample encryption (where an entire media sample is encrypted) or subsample encryption (where only portions of a sample are encrypted). Subsample encryption is particularly useful when certain parts of the media sample need to remain in the clear for processing, such as frame headers, while still protecting the actual media content. This allows for more efficient processing while maintaining content protection.

# 2.3 Motivation

Subsample encryption is useful when configuration and format information is embedded in the stream and needs to be available in the clear even when the content is protected.

In the context of video, this information is often carried in separate NAL units, or other packetized formats (e.g. OBUs with AV1).

# 2.4 Problem Description

The current CMAF specification (ISO/IEC 23000-19:2024) appears to disallow subsample encryption for non-video content through the following requirement:

"Encrypted *non-video* tracks *shall use* the schemes specified in ISO/IEC 23001-7, which define a *full media sample encryption* method for each scheme."

This wording can lead to confusion among implementers and potentially unnecessary restrictions in deployments. It is unclear whether it requires that non-video (e.g. audio) tracks use full sample encryption, or whether it requires that encryption uses one of the schemes specified in ISO/IEC 23001-7 but only those schemes that describe full sample encryption. In either case, implementers might conclude that partial encryption is disallowed for audio. It seems unlikely that this was the original intention.

# 2.5 Proposal

*In clause 8.2.1, replace the following sentence:*

Encrypted non-video tracks shall use the schemes specified in ISO/IEC 23001-7, which define a full media sample encryption method for each scheme.

*with:*

Encrypted non-NAL structured tracks shall use the schemes specified in ISO/IEC 23001-7. These tracks may use either full sample encryption or subsample encryption as defined in ISO/IEC 23001-7.

NOTE Examples of formats that may benefit from subsample encryption include those with frame headers that need to remain in the clear for processing, similar to how NAL headers remain in the clear for NAL structured video content.

This change would clarify that subsample encryption is permitted for audio content while maintaining alignment with CENC's security model.

# 2.6 Alternatives

If there are concerns with a retroactive bugfix, the fix could be conditional for the new “cmfm” profile. Alternatively, the fix could be introduced only into some, not all, of the existing profiles.

# 2.7 Other Specifications

Even for video, the current CENC specification (ISO/IEC 23001-7:2023) raises questions about use of subsample encryption for video that is not based on NAL structures as defined in ISO/IEC 14496-15. The CENC spec puts enough emphasis on describing NAL structured video encryption that it is difficult to determine if that means subsample encryption may *only* be used with NAL structured video, or if NAL structured video is just used as an example of the kind of bitstreams that subsample encryption can be applied to.

* For 'cenc' scheme: It requires full sample encryption for non-NAL structured content. However, it allows derived specifications to relax this constraint.
* For 'cbcs' scheme: It allows pattern encryption for non-NAL content, which implicitly requires subsample encryption, yet also contains language about "relaxing constraints" for subsample encryption.
* Only the AV1 ISOBMFF specification [1] has extended subsample encryption support to OBU-based structures, setting a precedent for extending beyond NAL-only structures.

It is advised to review this contribution in conjunction with contribution [m72214](https://dms.mpeg.expert/doc_end_user/current_document.php?id=98542&id_meeting=202) (“On subsample encryption”) addressing this issue in CENC.

# 2.8 References

[1] AV1 Codec ISO Media File Format Binding,  
<https://aomediacodec.github.io/av1-isobmff/>

# Support for AES-256 in encrypted profiles

# 3.1 Introduction

This contribution asks CMAF experts to consider the support of AES-256 support in CMAF profile. The File Format group is developing an amendment addressing this support in Common Encryption [1] and there is a need from the industry to have this support also available in CMAF. The need comes from evolution of regulation in the US [2], as explained below.

We would like to hear experts’ advices and recommendations on how to support AES-256 in CMAF.

# 3.2 Context and requirements

**Regulation**

The NSA is defining security requirements for future “quantum-resistant” products in the Commercial National Security Algorithm Suite (CNSA) 2.0 [2]. In particular, **for** **symmetric-key algorithms, using 256-bit keys will become mandatory**. The NSA set a milestone in 2030 from which IP products not compliant to CNSA 2.0 could not be sold anymore in the US.

**Impact on the market**

The market of video surveillance will be impacted by this new regulation. Standardisation organizations or industrial consortia have concerns about this. For example, ONVIF (Open Network Video Interface Forum) defines specifications that makes mandatory the support of **MPEG Common Encryption** and **CMAF** for devices supporting the recording of encrypted content [3]. To keep on using MPEG standards, to guarantee interoperability, there is a need for CMAF to consider AES-256.

**On-going work in Common Encryption**

In July 2024, the MPEG File Format group started an amendment to Common Encryption considering the support of AES-256 [1].

The support for 256-bit keys has been added in the specification text as well as means to indicate which length is actually in use in the encrypted file but also in MIME types [4]. It is proposed to extend the TrackEncryptionBox and use its flags to indicate whether some Common Encryption features are in use or not; for example: 128 or 256 key-length, single of multiple keys, full or subsample encryption, pattern mode or not…. The only new feature compared to previous edition of Common Encryption is the variable length for encryption keys.

# 3.3 Possible support in CMAF

A quick look at CMAF specification lets us think that while nothing is said about the length of the encryption keys, considering different key lengths would not break the CMAF encrypted tracks. (it was the same situation in MPEG Common Encryption). CMAF section 8 defines “encryption constraints” but a priori none prevents using longer encryption keys than 128-bits.

The CMAF presentation profiles (CMFHDc and CMFHDs) in Annex A.1 are respectively referencing the ‘cenc’ and ‘cbcs’ protection schemes. No mention about the length of encryption keys is given. We may assume that it can be any length, or we may interpret that it is 128-bit only as defined in Common Encryption 4th edition.

The question we ask to CMAF experts is then:

* Should we have an **explicit CMAF presentation profile for encrypted tracks using AES-256**? Or
* Should we keep on using existing ones and consider the signaling introduced by the AMD to Common Encryption to determine the key length in use?
  + In this case, we may want to update the section 8 to indicate the 128 or 256-bit keys can be used.

# 3.4 Conclusion

We explained the need for AES-256 support in CMAF, after introducing its support in Common Encryption.

We would like CMAF experts to consider how AES-256 can be supported in CMAF.

# 3.5 References

1. MDS24728\_WG03\_N01428, “*WD of ISO/IEC 23001-7:2023 AMD 1 AES-256 Support”*, MPEG#149, January 2025

1. [CNSA Suite 2.0 and Quantum Computing FAQ](https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF)  (.pdf)

1. [ONVIF Recording Control Service Specification](https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.onvif.org%2fspecs%2fsrv%2frec%2fONVIF-RecordingControl-Service-Spec.pdf&c=E,1,f0jEn7_W1yp4cllXC4h6H1XnZ32AximpEYVxvym5XU4K3jUlvLx2Jh6gQBAFA6B5EZ0SUULp60VpFXt-BjWbXORQaGuy72hxHUVaZw82&typo=1), v24.12 Dec. 2024 (.pdf)
2. m72413, “*On MIME types for encrypted content*”, MPEG#150, April 2025