 ISO/IEC JTC 1/SC 29/WG 3 N1288

**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:** 2024-07-19

**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** **01288**

**Sapporo – July 2024**

|  |  |
| --- | --- |
| **Title** | **WD of ISO/IEC 23001-7:2023 AMD 1 AES-256 Support** |
| **Source** | **WG 03, MPEG Systems** |
| **Status** | **Approved** |
| **Serial Number** | **24134** |

© 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 24134

Date:   2024-07-19

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. 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.*

*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].”