INTERNATIONAL STANDARD

ISO/IEC 23001-7

Fourth edition
2023-08

Information technology — MPEG systems technologies —

Part 7: Common encryption in ISO base media file format files

Technologies de l'information — Technologies des systèmes MPEG —

Partie 7: Cryptage commun des fichiers au format de fichier de médias de la base ISO

Reference number
ISO/IEC 23001-7:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **2**
3.1 Terms and definitions 2
3.2 Abbreviated terms 3

4 Protection schemes **3**
4.1 Scheme type signalling 3
4.2 Common encryption scheme types 4

5 Overview of encryption metadata **4**

6 Encryption parameters shared by groups of samples **4**

7 Common encryption sample auxiliary information **6**
7.1 Definition 6
7.2 Sample encryption information box for storage of sample auxiliary information 7
7.2.1 Sample encryption box — Definition 7
7.2.2 Syntax 8
7.2.3 Semantics 8

8 Box definitions **9**
8.1 Protection system specific header box 9
8.1.1 Definition 9
8.1.2 Syntax 10
8.1.3 Semantics 10
8.2 Track Encryption box 10
8.2.1 Definition 10
8.2.2 Syntax 11
8.2.3 Semantics 11
8.3 Item encryption box 11
8.3.1 Definition 11
8.3.2 Syntax 12
8.3.3 Semantics 12
8.4 Item auxiliary information box 13
8.4.1 Definition 13
8.4.2 Syntax 13
8.4.3 Semantics 13

9 Encryption of media data **14**
9.1 Field semantics 14
9.2 Initialization vectors 15
9.3 AES-CTR mode counter operation 16
9.4 Full sample encryption 16
9.4.1 General 16
9.4.2 Full sample encryption using AES-CTR mode 16
9.4.3 Full sample encryption using AES-CBC mode 17
9.5 Subsample encryption 17
9.5.1 Definition 17
9.5.2 Subsample encryption of NAL structured video tracks 18
9.6 Pattern encryption 23
9.6.1 Definition 23
9.6.2 Example of pattern encryption applied to a video NAL unit 24
9.7 Whole-block full sample encryption 24
9.8 Content sensitive encryption 24

© ISO/IEC 2023 – All rights reserved

9.8.1 Definition 24
9.8.2 Content sensitive encryption applied to a video NAL unit 25

10 Protection scheme definitions 26
10.1 'cenc' AES-CTR scheme 26
10.2 'cbc1' AES-CBC scheme 26
10.3 'cens' AES-CTR subsample pattern encryption scheme 27
10.4 'cbcs' AES-CBC subsample pattern encryption scheme 27
10.4.1 Definition 27
10.4.2 `'cbcs'` AES-CBC mode pattern encryption scheme application 28
10.5 `'sve1'` AES-CTR sensitive encryption scheme 29

11 XML representation of Common Encryption parameters 29
11.1 General 29
11.2 Definition of the XML `cenc:default_KID` attribute and `cenc:pssh` element 29
11.3 Use of the cenc:default_KID attribute and cenc:pssh element in DASH ContentProtection Descriptor elements 30
11.3.1 General 30
11.3.2 Addition of cenc:default_KID attributes in DASH ContentProtection Descriptors 30
11.3.3 Addition of the cenc:pssh element in Protection System Specific UUID ContentProtection Descriptors 31
11.3.4 Example of two Content Protection Descriptors in an MPD 31

Annex A (normative) **Content sensitive encryption scheme 33**

Bibliography 42

© ISO/IEC 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

This fourth edition cancels and replaces the third edition (ISO/IEC 23001-7:2016), which has been technically revised. It also incorporates the Amendment ISO/IEC 23001-7:2016/Amd 1:2019.

The main changes are as follows:

Addition of:

— item encryption, which allows image items to use protection schemes defined for media tracks,

— support for multiple keys and IVs per protected sample,

— `'sve1'` sensitive encryption scheme, a codec-specific encryption scheme for which the encrypted bitstream remains a valid decodable bitstream,

— improved selective encryption using sample groups

A list of all parts in the ISO/IEC 23001 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Introduction

Common Encryption specifies encryption and key mapping methods that enable decryption of the same file using different Digital Rights Management (DRM) and key management systems. It defines encryption algorithms and encryption related metadata necessary to decrypt the protected streams, yet it leaves the details of rights mappings, key acquisition and storage, DRM content protection compliance rules, etc., up to the DRM system or systems. For instance, DRM systems necessarily support identifying the decryption key via stored key identifiers (KIDs), but how each DRM system protects and locates the KID identified decryption key is left to a DRM-specific method.

DRM specific information such as licenses, rights, and license acquisition information can be stored in an ISO Base Media file using a `ProtectionSystemSpecificHeaderBox`. Each instance of this box stored in the file corresponds to one applicable DRM system identified by a well-known `SystemID`. DRM licenses or license acquisition information need not be stored in the file in order to look up a separately delivered key using a `KID` stored in the file and decrypt media samples using the encryption parameters stored in each track.

The second edition of this document added XML representations of Common Encryption parameters for delivery in XML documents, such as an MPEG DASH Media Presentation Description Documents (MPD). The second edition also defined the `'cbc1'` protection scheme using AES-CBC mode encryption.

The third edition added `'cbcs'` and `'cens'` protection schemes for pattern encryption, which encrypt only a fraction of the data blocks within each video subsample protected. Pattern encryption reduces the computational power required by devices to decrypt video tracks.

The additions in this fourth edition are listed in the Foreword.

© ISO/IEC 2023 – All rights reserved

Information technology — MPEG systems technologies —

Part 7:
Common encryption in ISO base media file format files

1 Scope

This document specifies common encryption formats for use in any file format based on ISO/IEC 14496-12. File, item, track, and track fragment metadata is specified to enable multiple digital rights and key management systems (DRMs) to access the same common encrypted file or stream. This document does not define a DRM system.

The AES-128 symmetric block cipher is used 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. Partial encryption using a pattern of encrypted and clear blocks is also specified in separate protection schemes. The identification of encryption keys, initialization vector storage and processing is specified for each scheme.

Subsample encryption is specified for NAL structured video, such as AVC and HEVC, to enable normal processing and editing of video elementary streams prior to decryption.

An XML representation is specified for important common encryption information so that it can be included in XML files as standard elements and attributes to enable interoperable license and key management prior to media file download.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ITU-T Rec.H.264 ISO/IEC 14496-10, *Information technology — Coding of audio-visual objects — Part 10: Advanced Video Coding*

ISO/IEC 14496-12, *Information technology — Coding of audio-visual objects — Part 12: ISO Base Media File Format*

ISO/IEC 14496-15, *Information technology — Coding of audio-visual objects — Part 15: Carriage of network abstraction layer (NAL) unit structured video in the ISO base media file format*

ISO/IEC 23008-2, *Information technology – Coding of audio-visual objects – Part 2: High Efficiency Video Coding (HEVC)*

ISO/IEC 23008-12, *Information technology — High efficiency coding and media delivery in heterogeneous — Part 12: Image File Format (HEIF)*

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*

FIPS-197, *Advanced Encryption Standard*, Federal Information Processing Standards Publication 197, https://www.nist.gov/

NIST Special Publication 800-38A, *Recommendation of Block Cipher Modes of Operation*, https://www.nist.gov/

© ISO/IEC 2023 – All rights reserved