INTERNATIONAL STANDARD

ISO/IEC 23001-7

Third edition
2016-02-15

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 23001-7:2016(E)

© ISO/IEC 2016

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions, and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 2

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

5 Overview of encryption metadata **3**

6 Encryption parameters shared by groups of samples **3**

7 Common encryption sample auxiliary information **5**
7.1 Definition 5
7.2 Sample Encryption Information box for storage of sample auxiliary information 6
7.2.1 Sample Encryption Box (‘senc’) 6
7.2.2 Syntax 6
7.2.3 Semantics 6

8 Box definitions **7**
8.1 Protection system specific header box 7
8.1.1 Definition 7
8.1.2 Syntax 7
8.1.3 Semantics 8
8.2 Track Encryption box 8
8.2.1 Definition 8
8.2.2 Syntax 8
8.2.3 Semantics 9

9 Encryption of media data **9**
9.1 Field semantics 9
9.2 Initialization Vectors 10
9.3 AES-CTR mode counter operation 11
9.4 Full sample encryption 12
9.4.1 General 12
9.4.2 Full sample encryption using AES-CTR mode 12
9.4.3 Full sample encryption using AES-CBC mode 12
9.5 Subsample encryption 13
9.5.1 Definition (normative) 13
9.5.2 Subsample encryption of NAL Structured Video tracks 14
9.6 Pattern encryption 18
9.6.1 Definition 18
9.6.2 Example of pattern encryption applied to a video NAL unit 19
9.7 Whole-block full sample encryption 19

10 Protection scheme definitions **19**
10.1 ‘cenc’ AES-CTR scheme 19
10.2 ‘cbc1’ AES-CBC scheme 20
10.3 ‘cens’ AES-CTR subsample pattern encryption scheme 20
10.4 ‘cbcs’ AES-CBC subsample pattern encryption scheme 21
10.4.1 Definition 21
10.4.2 ‘cbcs’ AES-CBC mode pattern encryption scheme application (informative) 22

11 XML representation of Common Encryption parameters **22**

© ISO/IEC 2016 – All rights reserved

11.1 General 22
11.2 Definition of the XML cenc:default_KID attribute and cenc:pssh element 22
11.3 Use of the cenc:default_KID attribute and cenc:pssh element in DASH ContentProtection Descriptor elements 23
11.3.1 General 23
11.3.2 Addition of cenc:default_KID attributes in DASH ContentProtection Descriptors 23
11.3.3 Addition of the cenc:pssh element in Protection System Specific UUID ContentProtection Descriptors 24
11.3.4 Example of two Content Protection Descriptors in an MPD 24

Bibliography **26**

 © ISO/IEC 2016 – 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

This third edition cancels and replaces the second edition (ISO/IEC 23001-7:2015), which has been technically revised.

ISO/IEC 23001 consists of the following parts, under the general title *Information technology — MPEG systems technologies*:

— *Part 1: Binary MPEG format for XML*

— *Part 2: Fragment request units*

— *Part 3: XML IPMP messages*

— *Part 4: Codec configuration representation*

— *Part 5: Bitstream Syntax Description Language (BSDL)*

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

— *Part 8: Coding-independent code points*

— *Part 9: Common encryption of MPEG-2 transport streams*

— *Part 10: Carriage of timed metadata metrics of media in ISO base media file format*

— *Part 11: Energy-efficient media consumption (green metadata)*

— *Part 12: Sample variants in the ISO base media file format*

© ISO/IEC 2016 – All rights reserved

Introduction

Common Encryption specifies standard encryption and key mapping methods that can be utilized to enable decryption of the same file using different Digital Rights Management (DRM) and key management systems. It operates by defining 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 is intended to 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 Protection System Specific Header box ('`pssh`'). 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 part of ISO/IEC 23001 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.

© ISO/IEC 2016 – All rights reserved

Information technology — MPEG systems technologies —

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

1 Scope

This part of ISO/IEC 23001 specifies common encryption formats for use in any file format based on ISO/IEC 14496-12. File, 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 part of ISO/IEC 23001 does not define a DRM system.

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. 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, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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 NAL unit structured video in the ISO Base Media File Format*

© ISO/IEC 2016 – All rights reserved