INTERNATIONAL STANDARD

ISO/IEC 23001-7

Second edition
2015-04-01

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 23001-7:2015(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 second edition cancels and replaces the first edition 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*

The following parts are under preparation:

- *Part 10: Carriage of timed metadata metrics of media in ISO base media file format*
- *Part 11: Green metadata*

Introduction

The common encryption protection scheme 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. The schemes operates by defining a common format for the encryption related metadata necessary to decrypt the protected streams, yet leaves the details of rights mappings, key acquisition and storage, DRM compliance rules, etc., up to the DRM system or systems supporting the common encryption scheme. For instance, DRM systems supporting the 'cenc' protection scheme must support identifying the decryption key via 'cenc' key identifier (KID) but how the DRM system locates the identified decryption key is left to a DRM-specific method. DRM specific information such as licenses or rights and license/rights 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. DRM licenses/rights need not be stored in the file in order to look up a key using KID values 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 also describes XML representation of common encryption parameters in MPEG DASH Media Presentation Description Documents.

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 a common encryption format for use in any file format based on ISO/IEC 14496-12.

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 network abstraction layer (NAL) unit structured video in ISO base media file format*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE Words used as defined terms and normative terms (SHALL, SHOULD, MAY) are written in upper case to distinguish them from the same word intending its dictionary definition.

3.1
ISO Base Media File
file conforming to the file format described in ISO/IEC 14496-12 in which the techniques in ISO/IEC 23001-7 can be used

3.2
network abstraction layer
NAL
NAL syntax element specified by a network abstraction layer specification such as AVC or HEVC

3.3
NAL unit
syntax structure containing an indication of the type of data to follow and bytes containing that data in the form of an RBSP interspersed as necessary with emulation prevention bytes

3.4
NAL structured video
video sample description format specified by ISO/IEC 14496-15