INTERNATIONAL ISO/IEC

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 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

Contents

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.

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.