INTERNATIONAL STANDARD

ISO/IEC 23001-9

First edition
2014-06-01

Information technology — MPEG systems technologies —

Part 9: Common encryption of MPEG-2 transport streams

Technologies de l'information — Technologies des systèmes MPEG —

Partie 9: Cryptage commun des flux de transport de contenu MPEG-2

Reference number
ISO/IEC 23001-9:2014(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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 23001-9 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

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 in MPEG-2 transport streams*

Information technology — MPEG systems technologies —

Part 9:
Common encryption of MPEG-2 transport streams

1 Scope

This part of ISO/IEC 23001 specifies a common media encryption format for use in MPEG-2 transport streams. This encryption format is intended to be used in an interoperable way with media encrypted using the format described by ISO/IEC 23001-7. This part of ISO/IEC 23001 allows conversion between encrypted MPEG-2 transport streams and encrypted ISO base media file format files without re-encryption.

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.

Rec. ITU-T H.222.0 | ISO/IEC 13818-1, *Information technology — Generic coding of moving pictures and associated audio information — Part 1: Systems*

ISO/IEC 13818-7, *Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC)*.

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

ISO/IEC 14496-3, *Information technology — Coding of audio-visual objects — Part 3: Audio*

ISO/IEC 23001-7, *Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files*

ISO/IEC 23008-2, *Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 2: High efficiency video coding*

IETF RFC 1321, *The MD5 Message-Digest Algorithm* , April 1992

Advanced Encryption Standard, Federal Information Processing Standards Publication 197, FIPS-197

Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A

3 Terms and definitions

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

3.1
Encrypted AU
part of elementary stream containing one access unit

Note 1 to entry: In case of ISO/IEC 14496-10 and ISO/IEC 23008-2, these are comprised of one or more NAL units.