INTERNATIONAL STANDARD

ISO/IEC 23001-12

Second edition
2018-12

Information technology — MPEG systems technologies —

Part 12: Sample variants

Technologies de l'information — Technologies des systèmes MPEG —

Partie 12: Variantes d'échantillon

Reference number
ISO/IEC 23001-12:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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.

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 second edition cancels and replaces the first edition (ISO/IEC 23001-12:2015), which has been technically revised.

The main changes compared to the previous edition are as follows:

— support for using sample variants for multiple alternate samples;

— support for using sample variants for multiple alternate protection schemes;

— support for carriage of sample variants in MPEG-2 transport streams.

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

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.

Information technology — MPEG systems technologies —

Part 12:
Sample variants

1 Scope

This document defines sample variants and their carriage in the ISO base media file format (ISO/IEC 14496-12) and MPEG-2 transport stream (ISO/IEC 13818-1).

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.

ISO/IEC 13818-1:2018, *Information technology — Generic coding of moving pictures and associated audio information — Part 1: Systems*

ISO/IEC 14496-12:2015, *Information technology — Coding of audio-visual objects — Part 12: ISO base media file format*

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

ISO/IEC 23001-9, *Information technology — MPEG systems technologies — Part 9: Common encryption of MPEG-2 transport streams*

3 Terms and definitions

For the purpose of this document, the terms and definitions given in ISO/IEC 13818-1, ISO/IEC 14496-12, and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
double encrypted
encrypted first by a *media key* (3.3) (as part of the encryption of the complete sample variant) and then by a variant byte range key

Note 1 to entry: See 7.2.

3.2
media data stream
track or packetized elementary stream containing audio-visual content

Note 1 to entry: Track is as specified in ISO/IEC 14496-12.

Note 2 to entry: Packetized elementary stream is as specified in ISO/IEC 13818-1.

3.3
media key
encryption key associated with one or more media *samples* (3.5)

3.4
media KID
encryption KID associated with one or more media *samples* (3.5)

3.5
sample
data of a sample or of an access unit

Note 1 to entry: Data of a sample is as specified in ISO/IEC 14496-12.

Note 2 to entry: Data of an access unit is as specified in ISO/IEC 13818-1.

3.6
sample variant
assembled media *sample* (3.5) replacing an original sample

3.7
sample variants media data stream Extractor
logical module that performs the steps that implement the process of generating a complete compliant *media data stream* (3.2) composed of *sample variants* (3.6)

3.8
variant byte range
location of a sequence of bytes that can constitute a portion of a *sample variant* (3.6)

3.9
variant constructor
sample variant (3.6) metadata that defines how to assemble an individual sample variant

3.10
variant data stream
track or packetized elementary stream for variant data

Note 1 to entry: Track is as specified in ISO/IEC 14496-12.

Note 2 to entry: Packetized elementary stream is as specified in ISO/IEC 13818-1.

3.11
variant media data
media data used to construct a *sample variant* (3.6)

Note 1 to entry: Some of the media data can come from the original media data stream.

3.12
variant processor
logical module that implements the process of assembling *sample variants* (3.6)

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

CENC Common Encryption (as specified in ISO/IEC 23001-7)

CETS Common Encryption of MPEG-2 Transport Streams (as specified in ISO/IEC 23001-9)

DRM Digital Rights Management

ISOBMFF ISO Base Media File Format (as specified in ISO/IEC 14496-12)

IV Initialization Vector

KID Key Identifier

MPEG-2 TS MPEG-2 Transport Stream (as specified in ISO/IEC 13818-1)

5 Overview

This document defines a framework for the carriage of sample variants in the ISOBMFF and MPEG-2 TS. Sample variants are alternative samples which can be used to replace the original samples in the media data stream. Sample variants can be used, for example, to provide forensic information in the rendered sample that can identify the DRM client or to provide appropriately encrypted samples with multiple protection schemes. This variant framework is fully compatible with ISOBMFF and CENC for carriage in ISOBMFF or fully compatible with MPEG-2 TS and CETS for carriage in MPEG-2 TS. The variant framework is agnostic to any particular forensic marking system or DRM system used.

The sample variant framework uses three core constructs to define and carry sample variant data: variant constructors, variant byte ranges and variant media data.

NOTE 1 The variant process model described in Clause 12 can also assist in introducing the concepts.

Figure 1 shows a scenario where a sample (sample 2) has a number of sample variants. The figure shows 3 samples in a series from left to right, the middle of which has variants. The top row is a conceptual depiction of what is encoded using ISOBMFF or MPEG-2 TS and the bottom row shows what is output after sample variant processing. Access to samples is under the control of KIDs as depicted in the top row of Figure 1. For sample variants, a hierarchy of KIDs is used to provide access to data, with the higher level KIDs providing access to sample variant metadata and the lower level KIDs providing access to media data.

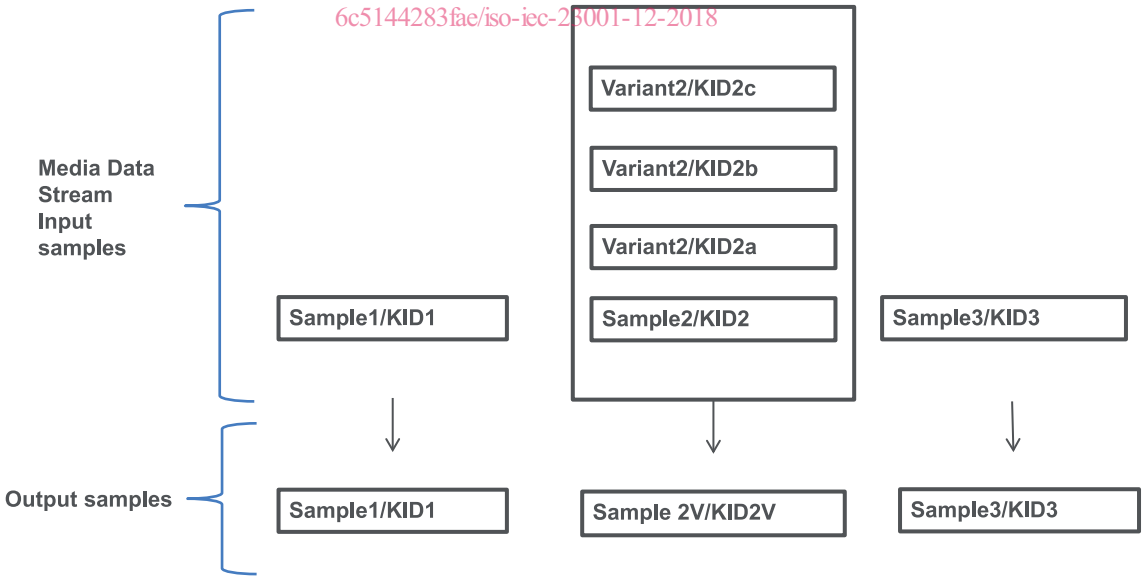

Figure 1 — Example sample variant structure for multiple alternate samples

Figure 2 shows another scenario in which a sample (sample 2) has a number of sample variants. In this case, however, only the data that differs from the original sample is carried in the samples of the variant data stream. As in Figure 1, the top row is a conceptual depiction of what is encoded using ISOBMFF or MPEG-2 TS and the bottom row shows what is output after sample variant processing, with access to samples controlled via KIDs as depicted in the top row. Under some use cases, such as subsample pattern encryption, the amount of redundant data between an original sample and a corresponding

sample variant may be relatively large. Sample variants can reference byte ranges of the original media data stream in addition to those of the current variant data stream, as well as additional variant data streams. This can enable more efficient carriage of sample variants than if sample variants had to be encoded in their entirety.

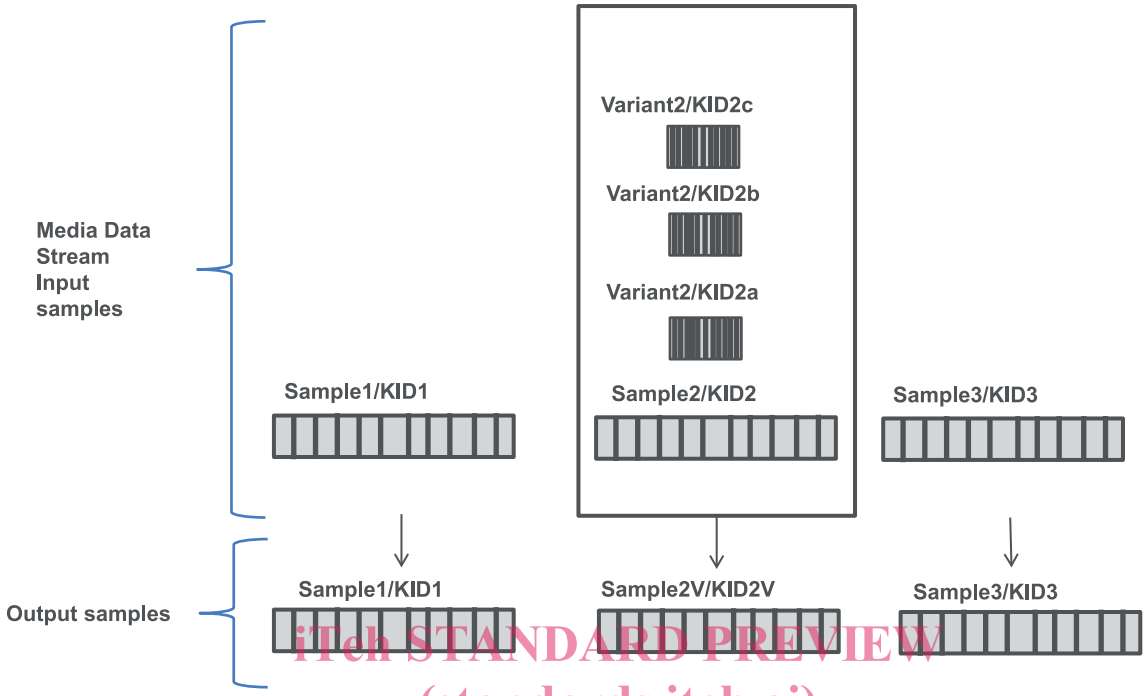

Figure 2 — Example sample variant byte range encoding for multiple alternate samples

Figure 3 further shows an example of how a media data stream prepared for one protection scheme can be efficiently adapted using sample variants to support another protection scheme. The figure shows samples in a series from left to right. The top row is made of samples from the original media data stream and the bottom row is made of sample variants from the variant media data. The sample variant may have the same KID or it may have a different KID from the samples of the original media data stream. The protection scheme can be different between samples from the original media data stream and samples from the variant media data.

The bottom two rows show the sample variant processing output samples of a single protection scheme. Access to the samples is under control of KIDs and protection scheme. It enables the application to carry media data stream with more than one protection scheme.

The control point for the use of the proposed framework is the content publisher:

— The content publisher encodes encrypted, compressed variant media data into the ISOBMFF file or MPEG-2 TS and ensures that each set of variant media data for a given sample time is encrypted with a key and signalled with a KID and protection scheme.

— The content publisher works with the DRM system to manage the release of KIDs/keys and protection scheme information such that the playback path (the actual sample data used during playback) is controlled and the player can only decrypt and render the data that it has been authorized to render.

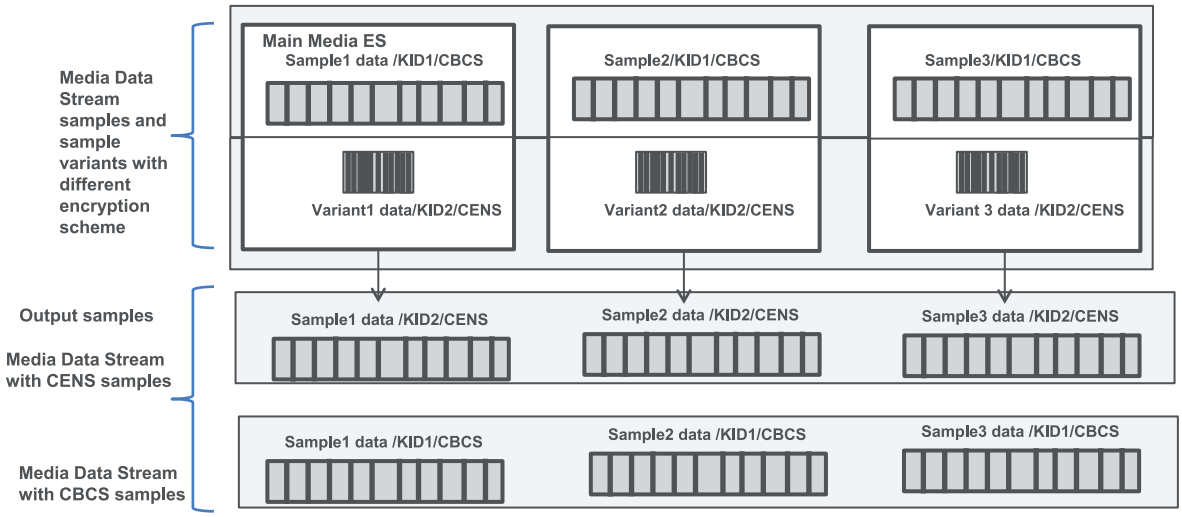

Figure 3 — Example sample variant structure for multiple protection schemes

Figure 4 shows the decoder model for the processing of files or transport streams that utilize sample variants. Critical to the sample variant decoding process is control over if and how the sample variants are processed.

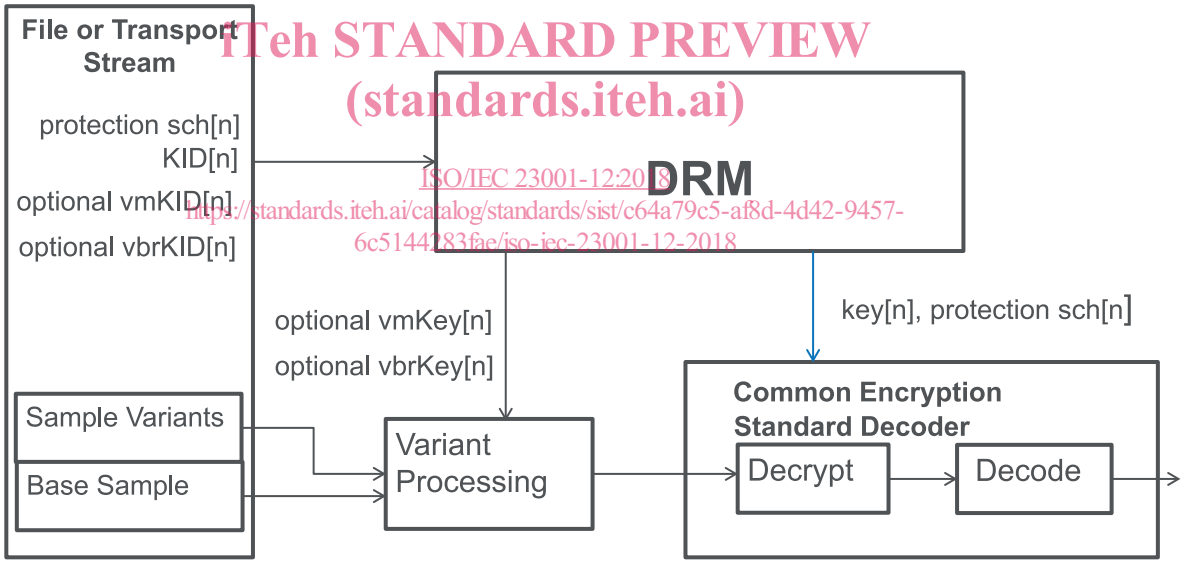

Figure 4 — Variant decoder model

NOTE 2 The decrypt and decode steps are standard operations as they would be for any common encryption enabled decoder.

By operating in the encrypted/compressed domain, secure baseband link operation (e.g. dedicated, secure video pathways) is preserved and is fully compatible with CENC or CETS.

As an alternative to the sample variants processing by the decoder, an extractor can also be used to pre-process the sample variants to generate a new media data stream and associated metadata for ISOBMFF or MPEG-2 TS. Clause 13 provides a high-level informative description of the extractor model.

6 Variant constructors

6.1 General

A variant constructor defines which bytes are used to assemble a sample variant. There may be one or more variant constructors defined for a given sample.

The variant processor may use a variant constructor if the variant processor has access to the variant constructor. In addition to the presence of the variant constructor, "access" includes cryptographic access. A variant constructor defines which data is used to assemble a sample variant and the associated media KID, protection scheme and initialization vector for decrypting the sample variant.

6.2 Access to variant constructors

If the decoder is given access to the media key, based on media KID and protection scheme, for the sample defined by the media data stream, sample variant processing does not occur for this sample. If the decoder does not have access to the original media key for the sample defined by the media data stream, e.g. due to mismatch of media KID or protection scheme, the variant processor shall be given access to one variant constructor associated with the sample. The variant constructor may be either unencrypted or encrypted.

NOTE Some application use cases, such as forensic watermarking, require that all variant constructors be encrypted to protect the integrity of the use case.

If a variant constructor is encrypted, a KID is associated with the variant constructor that identifies the key with which that variant constructor has been encrypted. The KID/key associated with the variant constructor controls access to a particular variant constructor and is therefore a function of the set of KID/key value pairs made available to the variant processor by the DRM system. Only one variant constructor per sample should be made available to the variant processor. If the variant processor is given access to a variant constructor, the decoder shall also be given access to the media key associated with the media KID and protection scheme defined in the variant constructor.

For a given variant data stream, all the variant constructors are either encrypted with the same protection scheme or all the variant constructors are unencrypted.

If the variant processor has access to more than one KID/key associated with encrypted variant constructors for a given sample, the variant processor utilizes the first variant constructor that it has access to in data encoding order.

If the variant processor has access to more than one unencrypted variant constructors for a given sample, the variant processor utilizes the first variant constructor that has matching media KID/key and protection scheme.

The variant processor uses exactly one variant constructor to assemble a sample variant.

6.3 Encryption of variant constructors

An encrypted variant constructor shall be encrypted with a "variant constructor key".

As a variant processor is provided only with the variant constructor keys for the encrypted variant constructor that is to be used by that particular variant processor, any variant constructors not used by that variant processor are not exposed by a security compromise of that variant processor.