

FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/IEC
FDIS
23001-12

ISO/IEC JTC 1/SC 29

Secretariat: JISC

Voting begins
on: 2015-09-04

Voting terminates
on: 2015-11-04

Information technology — MPEG systems technologies —

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

*Technologies de l'information — Technologies des systèmes MPEG —
Partie 12: Variantes d'échantillon dans le format ISO de base pour les
fichiers médias*

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



Reference number
ISO/IEC FDIS 23001-12:2015(E)

© ISO/IEC 2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/e42d233e-df10-4ad9-b672-d733d493b717/iso-iec-23001-12-2015>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, 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	iv
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 Overview (informative)	2
5 Variant Constructors	4
5.1 Overview.....	4
5.2 Access to Variant Constructors.....	4
5.3 Encryption of Variant Constructors.....	5
6 Variant Byte Ranges	5
6.1 Overview.....	5
6.2 Access to Variant Byte Ranges.....	5
6.3 Encryption of Variant Byte range information.....	6
7 Sample Variants	6
7.1 Overview.....	6
7.2 Access to Sample Variants.....	6
7.3 Encryption of Sample Variants.....	6
8 ISO storage	6
8.1 Overview.....	6
8.2 Variant tracks.....	7
8.2.1 Definition.....	7
8.2.2 Association.....	7
8.2.3 Variant Metadata Sample Entry.....	7
8.3 Sample data.....	8
8.3.1 Variant Data.....	8
8.3.2 Variant Constructor list.....	8
8.3.3 Variant Constructor.....	9
8.3.4 Encryption.....	11
8.3.5 Association.....	12
9 Variant Processor Model and Example (Informative)	12
9.1 Variant Processor Model.....	12
9.2 Example.....	13

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, 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 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*

Information technology — MPEG systems technologies —

Part 12:

Sample variants in the ISO base media file format

1 Scope

This part of ISO/IEC 23001 defines the carriage of Sample Variants in the ISO base media file format (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*¹⁾

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

3.1.1

Double Encrypted

Sample Variant byte range data encrypted by first a Media Key (as part of the encryption of the complete Sample Variant) and then second a Variant Byte Range key

Note 1 to entry: See [6.1](#).

3.1.2

Media Key

encryption key associated with one or more media samples

3.1.3

Media KID

encryption KID associated with one or more media samples

3.1.4

Sample Variant

assembled media sample replacing an original sample

3.1.5

Variant Byte Range

location of a sequence of bytes that might constitute a portion of a Sample Variant

1) ISO/IEC 14496-12 is technically identical to ISO/IEC 15444-12.

3.1.6

Variant Constructor

Sample Variant metadata that defines how to assemble an individual Sample Variant

3.1.7

Variant Media Data

media data used to construct a Sample Variant, some of which may come from the original sample media data

3.1.8

Variant Processor

logical module that performs the processing steps that implement the process of assembling Sample Variants

3.2 Abbreviated terms

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

CENC Common ENCRyption (as specified by ISO/IEC 23001-7)

DRM Digital Rights Management

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

IV Initialization Vector

KID Key Identifier

4 Overview (informative)

This part of ISO/IEC 23001 defines a framework for the carriage of Sample Variants in the ISOBMFF. Sample Variants are typically used to provide forensic information in the rendered sample data that can, e.g. identify the DRM client. This variant framework is intended to be fully compatible with ISOBMFF and CENC, and agnostic to the particular forensic marking system used.

The Sample Variant framework uses three core constructs to define and carry Sample Variant data in ISOBMFF: Variant Constructors, Variant Byte Ranges and Variant Samples.

NOTE The Variant Process Model described in [Clause 9](#) can also assist in introducing the concepts.

[Figure 1](#) shows a scenario where a sample (Sample 2) has a number of Sample Variants. [Figure 1](#) shows 3 samples in a series left to right, the middle of which has variants. The top row is a conceptual depiction of what is encoded using ISOBMFF 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 in [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.

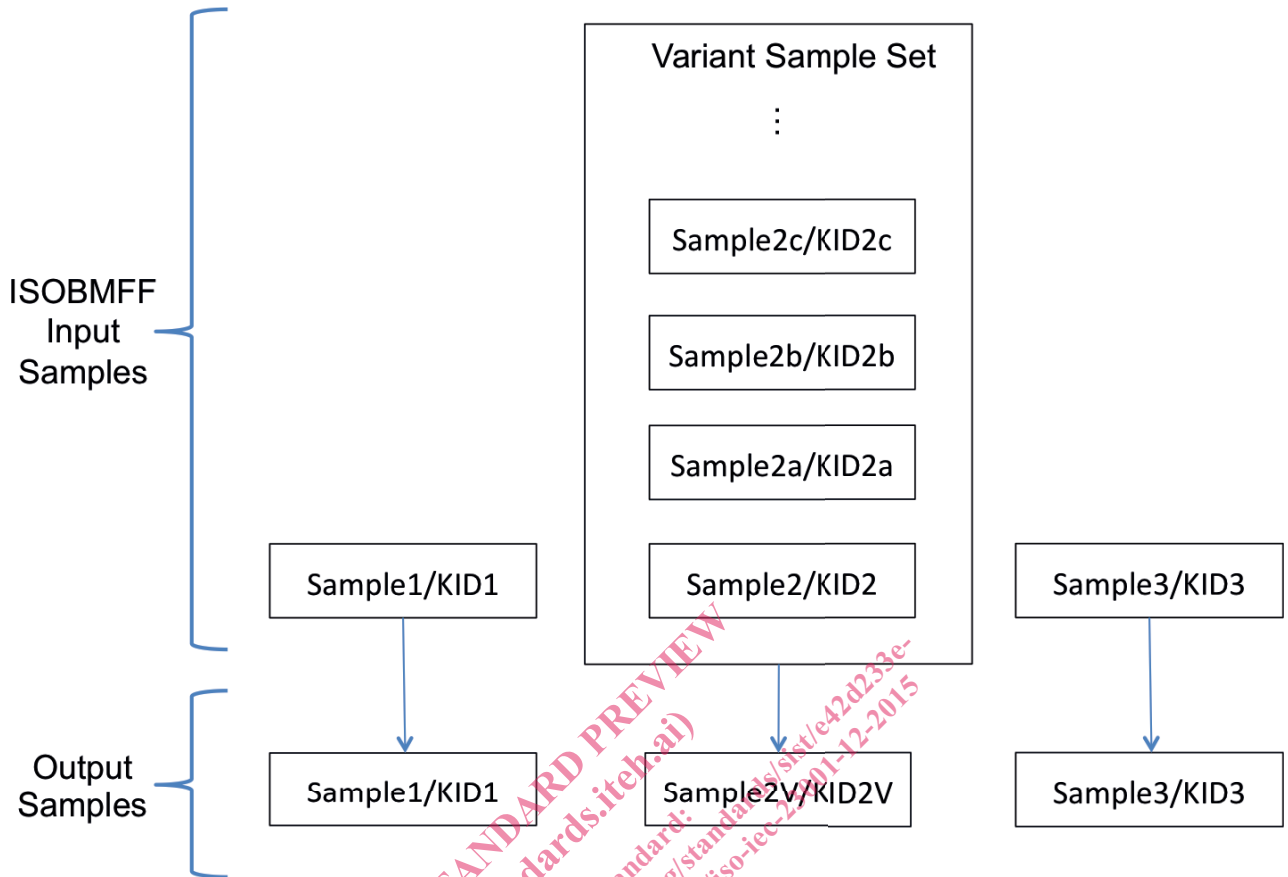


Figure 1 — Sample Variant structure

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

- the content publisher will encode encrypted, compressed Sample Variant data into the ISOBMFF file and ensure that each set of Sample Variant data for a given sample time is encrypted with a different key and signalled with a different KID.
- the content publisher will work with the DRM to manage the release of KIDs/keys 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.

The decoder model for the processing of the file is shown in [Figure 2](#). Critical to the Sample Variant decoding process is control over if and how the Sample Variants are processed.

NOTE The decrypt and decode steps are standard operations as they would be for any CENC-enabled decoder.

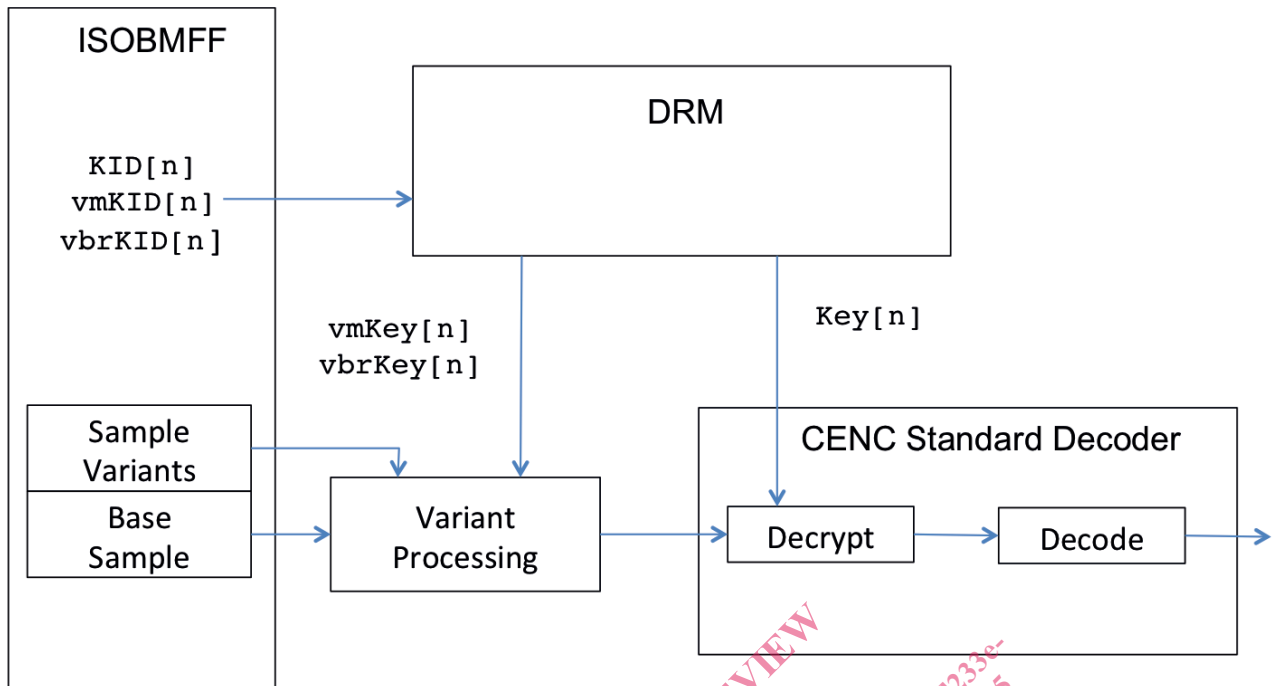


Figure 2 — Variant Decoder Model

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

5 Variant Constructors

5.1 Overview

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 ISOBMFF 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 and initialization vector for decrypting the Sample Variant.

5.2 Access to Variant Constructors

If the decoder is given access to the Media Key for the sample defined by the ISOBMFF media track, Sample Variant processing will not occur for this sample. If the decoder does not have access to the original Media Key for the sample defined by the ISOBMFF media track, the Variant Processor shall be given access to one Variant Constructor associated with the sample.

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. 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 defined in the Variant Constructor.

If the Variant Processor has access to more than one KID/Key associated with Variant Constructor for a given sample, the Variant Processor utilizes the first Variant Constructor that it has access to in data encoding order. The Variant Processor uses exactly one Variant Constructor to assemble a Sample Variant.

5.3 Encryption of Variant Constructors

Each Variant Constructor shall be encrypted with a “Variant Constructor key”.

As a Variant Processor is provided only with the Variant Constructor keys for the 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.

6 Variant Byte Ranges

6.1 Overview

Each Variant Constructor defines a sequence of one or more Variant Byte Ranges. Each Variant Byte Range defines the location of a sequence of bytes that might constitute bytes in a Sample Variant. Variant Byte Ranges can contain unused data.

The sequence of Variant Byte Ranges defined in a Variant Constructor are grouped into one or more Variant Byte Range groups. Each Variant Byte Range group shall define one or more Variant Byte Ranges. An individual Variant Byte Range within a Variant Byte Range group:

- May reference bytes of data that constitute bytes in a Sample Variant that is made available to certain Variant Processors (“real Variant Byte Range”).
- May reference bytes of data that are not made available to any Variant Processor (“fake Variant Byte Range”).

A “fake Variant Byte Range” can be used to hide the amount of actual “real Variant Byte Ranges” defined within a Variant Constructor. The Variant Processor uses all Variant Byte Ranges that it has access to. In addition to the presence of the Variant Byte Range, “access” includes cryptographic access.

Data for different Sample Variants can be stored non-contiguously as referenced by different Variant Constructors. Data for a particular Sample Variant can also be stored non-contiguously using a sequence of two or more Variant Byte Ranges.

6.2 Access to Variant Byte Ranges

If a Variant Byte Range within a Variant Byte Range group signals that the data referenced by the Variant Byte Range is unencrypted (and the Variant Processor has access to the Variant Constructor), then the Variant Processor has access to the Variant Byte Range and the associated unencrypted bytes.

If the Variant Byte Range defined within a Variant Byte Range group signals that the data referenced by the Variant Byte Range is encrypted, then access to the Variant Byte Range and the associated bytes is controlled by the KID/Key associated with each Variant Byte Range, either the Media Key defined by the Variant Constructor if no Variant Byte Range key is defined for the particular Variant Byte Range group or by the Variant Byte Range key if one is defined. Access to the Variant Byte Range and the associated data referenced by a Variant Byte Range is therefore a function of the set of KID/Key value pairs made available to the Variant Processor by the DRM. Only one Variant Byte Range within a Variant Byte Range group should be made available to the Variant Processor.

If the Variant Processor has access to more than one KID/Key associated with Variant Byte Ranges within the same Variant Byte Range group for a given sample, the Variant Processor uses the first Variant Byte Range that it has access to in data encoding order. The Variant Processor uses at most one Variant Byte Range within a Variant Byte Range group to assemble a Sample Variant.

Variant Byte Ranges can be used to efficiently encode only the (typically small) differences in Sample Variants for a given presentation time without repeating non-difference data or exposing Sample Variant differences to the Variant Processor. This is achieved through Double Encryption, where the difference data is first encrypted by the Media Key and then encrypted by the Variant Byte Range key. The Variant Processor requires access to the Variant Byte Range key to decrypt such difference data and

therefore access to the difference data can be controlled via the Variant Byte Range key. This enables reuse of common data and preserves Sample Variant compatibility with CENC, which requires that only one Media Key be applied to a given sample. If Variant Byte Ranges did not provide this capability, then it would be necessary to repeat all data for each Sample Variant, including difference and non-difference data, so as to protect difference data with a different key; this is inefficient.

6.3 Encryption of Variant Byte range information

Variant Byte Range definitions are not individually encrypted (they are encrypted as part of the Variant Constructor).

7 Sample Variants

7.1 Overview

The data used for rendering a sample is defined by either a Variant Constructor (if the Variant Processor has access to the Variant Constructor for the sample per 8.3.3), or by the media data defined by ISOBMFF. When Variant Constructors are used, the actual data used for reconstructing the sample is obtained by assembling, in the order of appearance in the Variant Constructor, the byte data referenced by the Variant Byte Ranges made available to the Variant Processor per Clause 6 and this construction shall result in a valid encrypted sample for the signalled underlying encryption system; this sample is a Sample Variant.

7.2 Access to Sample Variants

Once the Sample Variant is assembled from the Variant Byte Ranges, access to the sample data is controlled by the Media Key defined in the Variant Constructor and is therefore a function of the set of KID/Key value pairs made available to the Variant Processor by the DRM.

7.3 Encryption of Sample Variants

Sample Variants shall always be encrypted according to the scheme signalling of the associated media track. Variant Byte Ranges of a Sample Variant may be unencrypted, or may be encrypted with a Media Key. The Media Key is associated with one or more samples.

When bytes in a Sample Variant are encrypted with a Media Key, one or more byte ranges of the encrypted Variant Media Data may be further encrypted (Double Encrypted) according to the common encryption signalling with a "Variant Byte Range key" per 8.3.4.

As a Variant Processor is provided only with the Variant Byte Range keys for Double Encrypted Variant Media Data that are to be used by that particular Variant Processor, Double Encrypted Variant Media Data not used by that Variant Processor are not exposed by a compromise of that Variant Processor.

8 ISO storage

8.1 Overview

Variant data is stored in an ISOBMFF metadata tracks (variant track). An ISOBMFF media track (media track) or variant track may be associated with one or more variant tracks as defined in 8.2.2.

- When an association is established between a media track and a variant track, Sample Variant processing will occur whenever a decoder does not have access to the KID/key defined for a sample in the media track as defined in 5.2.
- When an association is established from a variant track (original variant track) to another variant track (other variant track), variant data contained in the other variant track can be utilized by the original variant track.