INTERNATIONAL STANDARD

ISO/IEC 23001-7

Third edition
2016-02-15

AMENDMENT 1
2019-09

Information technology — MPEG systems technologies —

Part 7: Common encryption in ISO base media file format files

AMENDMENT 1: AES-CBC-128 and key rotation

Technologies de l'information — Technologies des systèmes MPEG —

Partie 7: Cryptage commun des fichiers au format de fichier de médias de la base ISO

AMENDEMENT 1: AES-CBC-128 et rotation des clés

Reference number
ISO/IEC 23001-7:2016/Amd.1:2019(E)

COPYRIGHT PROTECTED DOCUMENT

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

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*.

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.

{"1":"1","2":"1","3":"1","4":"1","5":"1","6":"1","7":"1","8":"1","9":"1","10":"1","11":"1","12":"1","13":"1","14":"1","15":"1","16":"1","17":"1","18":"1","19":"1","20":"1","21":"1","22":"1","23":"1","24":"1","25":"1","26":"1","27":"1","28":"1","29":"1","30":"1","31":"1","32":"1","33":"1","34":"1","35":"1","36":"1","37":"1","38":"1","39":"1","40":"1","41":"1","42":"1","43":"1","44":"1","45":"1","46":"1","47":"1","48":"1","49":"1","50":"1","51":"1","52":"1","53":"1","54":"1","55":"1","56":"1","57":"1","58":"1","59":"1","60":"1","61":"1","62":"1","63":"1","64":"1","65":"1","66":"1","67":"1","68":"1","69":"1","70":"1","71":"1","72":"1","73":"1","74":"1","75":"1","76":"1","77":"1","78":"1","79":"1","80":"1","81":"1","82":"1","83":"1","84":"1","85":"1","86":"1","87":"1","88":"1","89":"1","90":"1","91":"1","92":"1","93":"1","94":"1","95":"1","96":"1","97":"1","98":"1","99":"1","100":"1","101":"1","102":"1","103":"1","104":"1","105":"1","106":"1","107":"1","108":"1","109":"1","110":"1","111":"1","112":"1","113":"1","114":"1","115":"1","116":"1","117":"1","118":"1","119":"1","120":"1","121":"1","122":"1","123":"1","124":"1","125":"1","126":"1","127":"1","128":"1","129":"1","130":"1","131":"1","132":"1","133":"1","134":"1","135":"1","136":"1","137":"1","138":"1","139":"1","140":"1","141":"1","142":"1","143":"1","144":"1","145":"1","146":"1","147":"1","148":"1","149":"1","150":"1","151":"1","152":"1","153":"1","154":"1","155":"1","156":"1","157":"1","158":"1","159":"1","160":"1","161":"1","162":"1","163":"1","164":"1","165":"1","166":"1","167":"1","168":"1","169":"1","170":"1","171":"1","172":"1","173":"1","174":"1","175":"1","176":"1","177":"1","178":"1","179":"1","180":"1","181":"1","182":"1","183":"1","184":"1","185":"1","186":"1","187":"1","188":"1","189":"1","190":"1","191":"1","192":"1","193":"1","194":"1","195":"1","196":"1","197":"1","198":"1","199":"1","200":"1","201":"1","202":"1","203":"1","204":"1","205":"1","206":"1","207":"1","208":"1","209":"1","210":"1","211":"1","212":"1","213":"1","214":"1","215":"1","216":"1","217":"1","218":"1","219":"1","220":"1","221":"1","222":"1","223":"1","224":"1","225":"1","226":"1","227":"1","228":"1","229":"1","230":"1","231":"1","232":"1","233":"1","234":"1","235":"1","236":"1","237":"1","238":"1","239":"1","240":"1","241":"1","242":"1","243":"1","244":"1","245":"1","246":"1","247":"1","248":"1","249":"1","250":"1","251":"1","252":"1","253":"1","254":"1","255":"1","256":"1","257":"1","258":"1","259":"1","260":"1","261":"1","262":"1","263":"1","264":"1","265":"1","266":"1","267":"1","268":"1","269":"1","270":"1","271":"1","272":"1","273":"1","274":"1","275":"1","276":"1","277":"1","278":"1","279":"1","280":"1","281":"1","282":"1","283":"1","284":"1","285":"1","286":"1","287":"1","288":"1","289":"1","290":"1","291":"1","292":"1","293":"1","294":"1","295":"1","296":"1","297":"1","298":"1","299":"1","300":"1","301":"1","302":"1","303":"1","304":"1","305":"1","306":"1","307":"1","308":"1","309":"1","310":"1","311":"1","312":"1","313":"1","314":"1","315":"1","316":"1","317":"1","318":"1","319":"1","320":"1","321":"1","322":"1","323":"1","324":"1","325":"1","326":"1","327":"1","328":"1","329":"1","330":"1","331":"1","332":"1","333":"1","334":"1","335":"1","336":"1","337":"1","338":"1","339":"1","340":"1","341":"1","342":"1","343":"1","344":"1","345":"1","346":"1","347":"1","348":"1","349":"1","350":"1","351":"1","352":"1","353":"1","354":"1","355":"1","356":"1","357":"1","358":"1","359":"1","360":"1","361":"1","362":"1","363":"1","364":"1","365":"1","366":"1","367":"1","368":"1","369":"1","370":"1","371":"1","372":"1","373":"1","374":"1","375":"1","376":"1","377":"1","378":"1","379":"1","380":"1","381":"1","382":"1","383":"1","384":"1","385":"1","386":"1","387":"1","388":"1","389":"1","390":"1","391":"1","392":"1","393":"1","394":"1","395":"1","396":"1","397":"1","398":"1","399":"1","400":"1","401":"1","402":"1","403":"1","404":"1","405":"1","406":"1","407":"1","408":"1","409":"1","410":"1","411":"1","412":"1","413":"1","414":"1","415":"1","416":"1","417":"1","418":"1","419":"1","420":"1","421":"1","422":"1","423":"1","424":"1","425":"1","426":"1","427":"1","428":"1","429":"1","430":"1","431":"1","432":"1","433":"1","434":"1","435":"1","436":"1","437":"1","438":"1","439":"1","440":"1","441":"1","442":"1","443":"1","444":"1","445":"1","446":"1","447":"1","448":"1","449":"1","450":"1","451":"1","452":"1","453":"1","454":"1","455":"1","456":"1","457":"1","458":"1","459":"1","460":"1","461":"1","462":"1","463":"1","464":"1","465":"1","466":"1","467":"1","468":"1","469":"1","470":"1","471":"1","472":"1","473":"1","474":"1","475":"1","476":"1","477":"1","478":"1","479":"1","480":"1","481":"1","482":"1","483":"1","484":"1","485":"1","486":"1","487":"1","488":"1","489":"1","490":"1","491":"1","492":"1","493":"1","494":"1","495":"1","496":"1","497":"1","498":"1","499":"1","500":"1","501":"1","502":"1","503":"1","504":"1","505":"1","506":"1","507":"1","508":"1","509":"1","510":"1","511":"1","512":"1","513":"1","514":"1","515":"1","516":"1","517":"1","518":"1","519":"1","520":"1","521":"1","522":"1","523":"1","524":"1","525":"1","526":"1","527":"1","528":"1","529":"1","530":"1","531":"1","532":"1","533":"1","534":"1","535":"1","536":"1","537":"1","538":"1","539":"1","540":"1","541":"1","542":"1","543":"1","544":"1","545":"1","546":"1","547":"1","548":"1","549":"1","550":"1","551":"1","552":"1","553":"1","554":"1","555":"1","556":"1","557":"1","558":"1","559":"1","560":"1","561":"1","562":"1","563":"1","564":"1","565":"1","566":"1","567":"1","568":"1","569":"1","570":"1","571":"1","572":"1","573":"1","574":"1","575":"1","576":"1","577":"1","578":"1","579":"1","580":"1","581":"1","582":"1","583":"1","584":"1","585":"1","586":"1","587":"1","588":"1","589":"1","590":"1","591":"1","592":"1","593":"1","594":"1","595":"1","596":"1","597":"1","598":"1","599":"1","600":"1","601":"1","602":"1","603":"1","604":"1","605":"1","606":"1","607":"1","608":"1","609":"1","610":"1","611":"1","612":"1","613":"1","614":"1","615":"1","616":"1","617":"1","618":"1","619":"1","620":"1","621":"1","622":"1","623":"1","624":"1","625":"1","626":"1","627":"1","628":"1","629":"1","630":"1","631":"1","632":"1","633":"1","634":"1","635":"1","636":"1","637":"1","638":"1","639":"1","640":"1","641":"1","642":"1","643":"1","644":"1","645":"1","646":"1","647":"1","648":"1","649":"1","650":"1","651":"1","652":"1","653":"1","654":"1","655":"1","656":"1","657":"1","658":"1","659":"1","660":"1","661":"1","662":"1","663":"1","664":"1","665":"1","666":"1","667":"1","668":"1","669":"1","670":"1","671":"1","672":"1","673":"1","674":"1","675":"1","676":"1","677":"1","678":"1","679":"1","680":"1","681":"1","682":"1","683":"1","684":"1","685":"1","686":"1","687":"1","688":"1","689":"1","690":"1","691":"1","692":"1","693":"1","694":"1","695":"1","696":"1","697":"1","698":"1","699":"1","700":"1","701":"1","702":"1","703":"1","704":"1","705":"1","706":"1","707":"1","708":"1","709":"1","710":"1","711":"1","712":"1","713":"1","714":"1","715":"1","716":"1","717":"1","718":"1","719":"1","720":"1","721":"1","722":"1","723":"1","724":"1","725":"1","726":"1","727":"1","728":"1","729":"1","730":"1","731":"1","732":"1","733":"1","734":"1","735":"1","736":"1","737":"1","738":"1","739":"1","740":"1","741":"1","742":"1","743":"1","744":"1","745":"1","746":"1","747":"1","748":"1","749":"1","750":"1","751":"1","752":"1","753":"1","754":"1","755":"1","756":"1","757":"1","758":"1","759":"1","760":"1","761":"1","762":"1","763":"1","764":"1","765":"1","766":"1","767":"1","768":"1","769":"1","770":"1","771":"1","772":"1","773":"1","774":"1","775":"1","776":"1","777":"1","778":"1","779":"1","780":"1","781":"1","782":"1","783":"1","784":"1","785":"1","786":"1","787":"1","788":"1","789":"1","790":"1","791":"1","792":"1","793":"1","794":"1","795":"1","796":"1","797":"1","798":"1","799":"1","800":"1","801":"1","802":"1","803":"1","804":"1","805":"1","806":"1","807":"1","808":"1","809":"1","810":"1","811":"1","812":"1","813":"1","814":"1","815":"1","816":"1","817":"1","818":"1","819":"1","820":"1","821":"1","822":"1","823":"1","824":"1","825":"1","826":"1","827":"1","828":"1","829":"1","830":"1","831":"1","832":"1","833":"1","834":"1","835":"1","836":"1","837":"1","838":"1","839":"1","840":"1","841":"1","842":"1","843":"1","844":"1","845":"1","846":"1","847":"1","848":"1","849":"1","850":"1","851":"1","852":"1","853":"1","854":"1","855":"1","856":"1","857":"1","858":"1","859":"1","860":"1","861":"1","862":"1","863":"1","864":"1","865":"1","866":"1","867":"1","868":"1","869":"1","870":"1","871":"1","872":"1","873":"1","874":"1","875":"1","876":"1","877":"1","878":"1","879":"1","880":"1","881":"1","882":"1","883":"1","884":"1","885":"1","886":"1","887":"1","888":"1","889":"1","890":"1","891":"1","892":"1","893":"1","894":"1","895":"1","896":"1","897":"1","898":"1","899":"1","900":"1","901":"1","902":"1","903":"1","904":"1","905":"1","906":"1","907":"1","908":"1","909":"1","910":"1","911":"1","912":"1","913":"1","914":"1","915":"1","916":"1","917":"1","918":"1","919":"1","920":"1","921":"1","922":"1","923":"1","924":"1","925":"1","926":"1","927":"1","928":"1","929":"1","930":"1","931":"1","932":"1","933":"1","934":"1","935":"1","936":"1","937":"1","938":"1","939":"1","940":"1","941":"1","942":"1","943":"1","944":"1","945":"1","946":"1","947":"1","948":"1","949":"1","950":"1","951":"1","952":"1","953":"1","954":"1","955":"1","956":"1","957":"1","958":"1","959":"1","960":"1","961":"1","962":"1","963":"1","964":"1","965":"1","966":"1","967":"1","968":"1","969":"1","970":"1","971":"1","972":"1","973":"1","974":"1","975":"1","976":"1","977":"1","978":"1","979":"1","980":"1","981":"1","982":"1","983":"1","984":"1","985":"1","986":"1","987":"1","988":"1","989":"1","990":"1","991":"1","992":"1","993":"1","994":"1","995":"1","996":"1","997":"1","998":"1","999":"1","1000":"1"}

Information technology — MPEG systems technologies —

Part 7:
Common encryption in ISO base media file format files

AMENDMENT 1: AES-CBC-128 and key rotation

Clause 2

Add the following new normative references:

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

ISO/IEC 23008-12, *Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 12: Image File Format (HEIF)*

3.1

Insert a new 3.1.8 and renumber current 3.1.8 as 3.1.9:

3.1.8
sample
media sample when the protection applies to media tracks, or payload of an item when the protection applies to items

Note 1 to entry: Media sample as defined in 14496-12.

Note 2 to entry: Payload of an item as defined in 14496-12.

4.2

Add the following item to the list:

e) **'sve1'** – AES-CTR content sensitive encryption, as defined in Annex A.

Clause 6

In paragraph 4, replace:

```
{
   unsigned int(8)      reserved = 0;
   unsigned int(4)      crypt_byte_block;
   unsigned int(4)      skip_byte_block;
   unsigned int(8)      isProtected;
   unsigned int(8)      Per_Sample_IV_Size;
   unsigned int(8)[16]  KID;
   if (Per_Sample_IV_Size == 0) {
      unsigned int(8)   constant_IV_size;
      unsigned int(8)[constant_IV_size] constant_IV;
   }
}
```

with

```
{
   unsigned int(1)      multi_key_flag;
   unsigned int(7)      reserved = 0;
   unsigned int(4)      crypt_byte_block;
   unsigned int(4)      skip_byte_block;
   unsigned int(8)      isProtected;
   if (multi_key_flag == 1) {
      unsigned int(16)     key_count;
   } else {
      key_count = 1;
   }
   for (i=1; i <= key_count; i++) {
      unsigned int(8)      Per_Sample_IV_Size;
      unsigned int(8)[16]  KID;
      if (Per_Sample_IV_Size == 0) {
         unsigned int(8)   constant_IV_size;
         unsigned int(8)[constant_IV_size] constant_IV;
```

```
      }
   }
}
```

Clause 6

Add a new item to the list in paragraph 5 (insert before semantics of `isProtected`):

— `multi_key_flag` indicates that the multiple key version of the sample group description is used. If this flag is set, multiple keys will be described for this sample group description entry; otherwise, a single key is described for this sample group description entry.

Add a new item to the list in paragraph 5 (insert after semantics of `isProtected`):

— `key_count` indicates the number of keys that may apply to a sample associated to this sample group description entry. It is not required that a sample associated with this sample group description entry uses all the keys described.

7.1

Replace the sample auxiliary information in paragraph 3 with:

```
aligned(8) class CencSampleAuxiliaryDataFormat
{
   if (aux_info_type_parameter==0) {
      unsigned int(Per_Sample_IV_Size*8) InitializationVector;
      if (sample_info_size > Per_Sample_IV_Size ) {
         unsigned int(16) subsample_count;
         {
            unsigned int(16) BytesOfClearData;
            unsigned int(32) BytesOfProtectedData;
         } [subsample_count ]
      }
   } else if (aux_info_type_parameter == 1) {
      unsigned int(16) multi_IV_count;
      for (i=1; i <= multi _IV_count; i++) {
         unsigned int(8) multi_subindex_IV;
         unsigned int(Per_Sample_IV_Size*8) IV;
      }
      unsigned int(32) subsample_count;
      {
```

```
         unsigned int(16) multi_subindex;
         unsigned int(16) BytesOfClearData;
         unsigned int(32) BytesOfProtectedData;
      } [subsample_count]
   }
}
```

Following the sample auxiliary information, add the following at the end of the 'where' list (after semantics of `BytesOfProtectedData`):

`multi_IV_count` indicates the number of entries in the initialization vector loop;

`multi_subindex_IV` indicates the index of the associated key entry, where value one is the first entry, in the associated list; if this data is read for the processing of a track sample, the associated list is the `'seig'` sample group description entry associated with this sample; otherwise (this data is read for the processing of an item), the associated list is the list of key definitions in the `'ienc'` item property of this item. The associated key entry shall have a `Per_Sample_IV_Size` different from 0, i.e. key entries using constant IV shall not be present in this loop. If this data is read for the processing of a track sample and `aux_info_type_parameter` is set to 1, the associated `'seig'` sample group description entry shall have the `multi_key_flag` set to 1;

`IV` indicates the initialization vector to be used for the first block of protected data for the associated key entry;

`multi_subindex` indicates the index of the associated key entry, where value one is the first entry, in the associated list (see `multi_subindex_IV`) for the following run of encrypted data.

7.2.2

Replace the content of 7.2.2 with the following:

```
aligned(8) class SampleEncryptionBox extends FullBox('senc', version, flags)
{
   unsigned int(32)  sample_count;
   {
      if (version==0) {
         unsigned int(Per_Sample_IV_Size*8) InitializationVector;
         if (flags & 0x000002) {
            unsigned int(16) subsample_count;
            {
               unsigned int(16) BytesOfClearData;
               unsigned int(32) BytesOfProtectedData;
            } [subsample_count ]
         }
```

```
      } else if (version==1) {
         unsigned int(16) multi_IV_count;
         for (i=1; i <= multi _IV_count; i++) {
            unsigned int(8) multi_subindex_IV;
            unsigned int(Per_Sample_IV_Size*8) IV;
         }
         unsigned int(32) subsample_count;
         {
            unsigned int(16) multi_subindex;
            unsigned int(16) BytesOfClearData;
            unsigned int(32) BytesOfProtectedData;
         } [subsample_count]
      }
   }[ sample_count ]
}
```

7.2.3

Add the following to the list of semantics:

— `multi_IV_count`, `multi_subindex_IV`, `IV` and `multi_subindex` SHALL conform to the definition specified in Clause 7.

8.1.1

Replace

Container: Movie (‘`moov`’) or Movie Fragment (‘`moof`’)

with

Container: Movie (‘`moov`’) or Movie Fragment (‘`moof`’) or ‘meta’ if no Movie (‘`moov`’)

8.2

Add the following new subclauses after 8.2:

8.3 Item encryption box

8.3.1 Definition

Box Type: `ienc`

Container: Item Properties Box

Mandatory (per item): Yes for protected items using schemes defined in this document

Quantity (per item): At most one associated with any item

Quantity: Zero or one

Items as defined in ISO/IEC 14496-12 may be protected using the schemes defined in this document. In this case, such items shall have an associated `ItemEncryptionBox` property and an associated auxiliary item with an `aux_info_type` matching the protection scheme used, as defined in 8.4. The payload of that auxiliary item shall be exactly one `CencSampleAuxiliaryDataFormat` as defined in 7.1.

The `ItemEncryptionBox` contains default values for the `isProtected` flag, `Per_Sample_IV_Size`, and `KID` for the item. In the case where pattern-based encryption is in effect, it supplies the pattern and when Constant IVs are in use, it supplies the Constant IV. These values are used as the encryption parameters for the item in this meta box. For files with only one key for all items, this property box allows the basic encryption parameters to be specified once for all items instead of being repeated per item.

Items sharing this property are always protected; consequently, the default value for `isProtected` field (see 9.1) is 1.

If the value `Per_Sample_IV_Size` is 0, then the `constant_IV_size` for all items that use these settings SHALL be present. A Constant IV SHALL NOT be used with counter-mode encryption.

`ItemEncryptionBox` properties shall be marked as essential in `ItemPropertyAssociation`.

NOTE The version field of the `ItemEncryptionBox` is set to a value greater than zero when the pattern encryption defined in 9.6 is used and to zero otherwise.

8.3.2 Syntax

```
aligned(8) class ItemEncryptionBox extends ItemFullProperty('ienc', version, flags=0)
{
      unsigned int(8) reserved = 0;
      if (version==0) {
            unsigned int(8) reserved = 0;
      } else { // version is 1 or greater
            unsigned int(4) crypt_byte_block;
            unsigned int(4) skip_byte_block;
      }
      unsigned int(8) num_keys;
      for (i=1; i<= num_keys; i++) {
         unsigned int(8) Per_Sample_IV_Size;
         unsigned int(8)[16] KID;
         if (Per_Sample_IV_Size == 0) {
            unsigned int(8) constant_IV_size;
            unsigned int(8)[ constant_IV_size] constant_IV;
         }
      }
}
```


8.3.3 Semantics

`version` SHALL be zero unless pattern-based encryption is in use, whereupon it SHALL be 1.

`crypt_byte_block` specifies the count of the encrypted blocks in the protection pattern, where each block is of size 16-bytes, for items associated with this key entry. See 9.1 for further details.

`skip_byte_block` specifies the count of the unencrypted blocks in the protection pattern for items associated with this key entry. See the `skip_byte_block` field in 9.1 for further details.

`num_keys` indicates the number of key definition entries.

`Per_Sample_IV_Size` is the initialization vector size in bytes for items associated with this key entry. See the `Per_Sample_IV_Size` field in 9.1 for further details.

`KID` is the key identifier used for items associated with this key entry. See the `KID` field in 9.1 for further details.

`constant_IV_size` is the size of a initialization vector for items associated with this key entry.

`constant_IV`, if present, is the initialization vector for items associated with this key entry. See the `constant_IV` field in 9.1 for further details.

8.4 Item auxiliary information box

8.4.1 Definition

Box Type: `` `iaux' ``

Container: Item Properties Box

Mandatory (per item): Yes for protected items using schemes defined in this document

Quantity (per item): At most one associated with any item

Quantity: Zero or one

An item may have some auxiliary information associated, similarly to sample of a track having auxiliary sample information. This information is usually declared through item properties and associations; it can also be declared through auxiliary information items, to allow sharing the auxiliary info between items and samples through the extent construction method of the item.

Auxiliary information items shall be declared with an `item_type` value of `` `auxi' ``. Items shall indicate their auxiliary information items through an item reference of type `` `auxr' `` from the item to the auxiliary information item(s).

Auxiliary information item may have an `ItemAuxiliaryInformationBox` property associated, indicating the type of auxiliary information and its parameter type (`aux_info_type` and `aux_info_type_parameter`).

If no `ItemAuxiliaryInformationBox` is present for an auxiliary information item, then the implied value of `aux_info_type` is either (a) in the case of protected content, the `scheme_type` included in the `ProtectionSchemeInfoBox` of the referring item or otherwise (b) the `item_type` of the referring item. The default value of the `aux_info_type_parameter` is 0. The `ItemAuxiliaryInformationBox` shall be present when the referring item is not protected and is not defined using version 2 or higher of `ItemInfoEntry`.

There shall be at most one auxiliary information item with a given `aux_info_type` and `aux_info_type_parameter` associated with an item.

When present, the `ItemAuxiliaryInformationBox` property shall be marked as essential in `ItemPropertyAssociation`.

8.4.2 Syntax

```
aligned(8) class ItemAuxiliaryInformationBox extends ItemFullProperty('iaux', version=0,
flags=0)

{

      unsigned int(32) aux_info_type;

      unsigned int(32) aux_info_type_parameter;

}
```

8.4.3 Semantics

`aux_info_type`: same semantics as sample auxiliary information in ISO/IEC 14496-12.

`aux_info_type_parameter`: same semantics as sample auxiliary information in ISO/IEC 14496-12.

9.1

In 9.1, replace the semantics of BytesOfProtectedData by:

`BytesOfProtectedData` specifies the number of bytes of protected data following the clear data (this value may be zero if no protected bytes exist for this Subsample). The Subsample encryption entries SHALL NOT include an entry with a zero value in both the `BytesOfClearData` field and in the `BytesOfProtectedData` field unless a `'tref'` box is found for this track with one or more track references of type `'scal'` pointing to one or more tracks with sample entry code `'encv'`, in which case 9.5.2.6 applies. The total length of all `BytesOfClearData` and `BytesOfProtectedData` in a sample SHALL equal the length of the sample. Subsample encryption entries SHOULD be as compactly represented as possible. For example, instead of two entries with {15 clear, 0 protected}, {17 clear, 500 protected} use one entry of {32 clear, 500 protected}. If pattern-based encryption is used, then the pattern applies to the protected byte range, `BytesOfProtectedData`; otherwise all protected bytes are encrypted.

9.5

Add the following text after 9.5.2.5:

9.5.2.6 Subsample encryption applied to NAL structured video with extractors

In this clause, "sample auxiliary information for cenc" refers to the size of the block of clear data and the size of the block of protected data, regardless whether this is stored as sample auxiliary information pointed to by 'saiz' and 'saio' boxes or included in a 'senc' box.

In this clause, "extractor track with cenc" refers to a track with sample entry code 'encv' with original format, as indicated by the 'frma' box in the 'sinf' box, in which extractors, as defined in ISO/IEC 14496-15:—[1)], Annex A, may be present.

When a 'tref' box is found in an extractor track with cenc which refers to one or more tracks with sample entry code 'encv', the following restrictions apply in addition to restrictions defined in 9.5.2.2:

— Extraction process SHALL take place before the decryption process.

— Extractors NAL units SHALL NOT be encrypted.

1) Under preparation.

— The following applies to the sample auxiliary information for cenc found in an extractor track with cenc.

  — When both values of `BytesOfClearData` and `BytesOfProtectedData` are 0, it is a placeholder for the sample auxiliary information for cenc of the NAL Structured Video samples that result from resolving the constructors within the extractor NAL unit as defined in ISO/IEC 14496-15:—, A.7.

  — Otherwise, the values of `BytesOfClearData` and `BytesOfProtectedData` apply to the extracted sub_sample.

— The sample auxiliary information for cenc SHALL be present for each referenced track in 'tref' with sample entry code 'encv'.

— When an extractor NAL unit as defined in ISO/IEC 14496-15:—, A.7 with associated sample auxiliary information for cenc contains a value of 0 for both `BytesOfClearData` and `BytesOfProtectedData` points to a track with sample entry code 'encv':

  — Exactly one VCL NAL unit SHALL be encrypted in each subsample of the referenced track.

  — Let `RefBytesOfClearData` and `RefBytesOfProtectedData` be the sample auxiliary information for cenc associated with the subsample of which the byte range is extracted, then the sample auxiliary information for cenc for the resolved VCL NAL unit is SHALL be replaced by the following values:

    ```
    BytesOfClearData = RefBytesOfClearData - SampleConstructor.sample_offset + InlineConstructor.length

    BytesOfProtectedData = RefBytesOfProtectedData
    ```

    The value `SampleConstructor.sample_offset` is the value of `sample_offset` in the SampleConstructor in the extractor that is processed.

    The value `InlineConstructor.length` is the sum of the values in the length fields inside the `InlineConstructor`, if any are found in the extractor that is processed, else 0.

— The resulting subsample information SHALL be conformant to CENC, and the decrypted version of every sample in the extractor track SHALL comply with the file and/or track brand and track description entry type.

9.7

Add the following subclauses after 9.7, and renumber subsequent figures:

9.8 Content sensitive encryption

9.8.1 Definition

Content sensitive encryption is a bitstream syntax aware scrambling scheme that modifies media bitstream in such a way that an unauthorized receiver (i.e. a standard decoder) can normally decode the ciphered stream, while the displayed content is made non-intelligible by the encryption. This scheme is currently applicable to AVC and HEVC and defined in Annex A. The scheme can be applied to both media tracks and image items, in which case media tracks shall be in accordance with ISO/IEC 14496-15 and image items shall be in accordance with ISO/IEC 23008-12.

The scheme operates in compressed domain based on entropic coder, by identifying the elements of the stream that can be ciphered without disrupting a standard decoding process. The bits to be encrypted are chosen with respect to the considered video standard to ensure full compatibility, achieved by selecting the bits (generally parts of code-words) for which each of the encrypted configurations modifies the decoding process context but does not create de-synchronization nor lead to non-compliant bitstream.

The selected elements will depend on the video coding specification used:

— A.1 gives the list of elements and possible bit encryption for AVC|H264 CAVLC

— A.2 gives the list of elements and possible bit encryption for AVC|H264 CABAC

— A.3 gives the list of elements and possible bit encryption for HEVC|H265

NOTE For CABAC entropic coding (i.e. in A.2 and A.3), the bits considering as cipherable regarding to Content Sensitive encryption process are listed as bins since the considered codewords are first binarized before the bypassed Coded Engine.

9.8.2 Content sensitive encryption applied to a video NAL unit

In content sensitive encryption, 16 bytes block cypher cannot be used directly on the payload. Consequently, a video parser shall be used to locate bits to cipher/decipher. These bits, listed in Annex A, depend on the coding standard and potentially the entropic coding mode used.

Content sensitive encryption scheme shall use the AES-CTR mode for its cipher.

The encryption and decryption processes are performed with a simple XOR operation between the identified bits in the syntax and the cypher blocks, as shown in Figure 10.

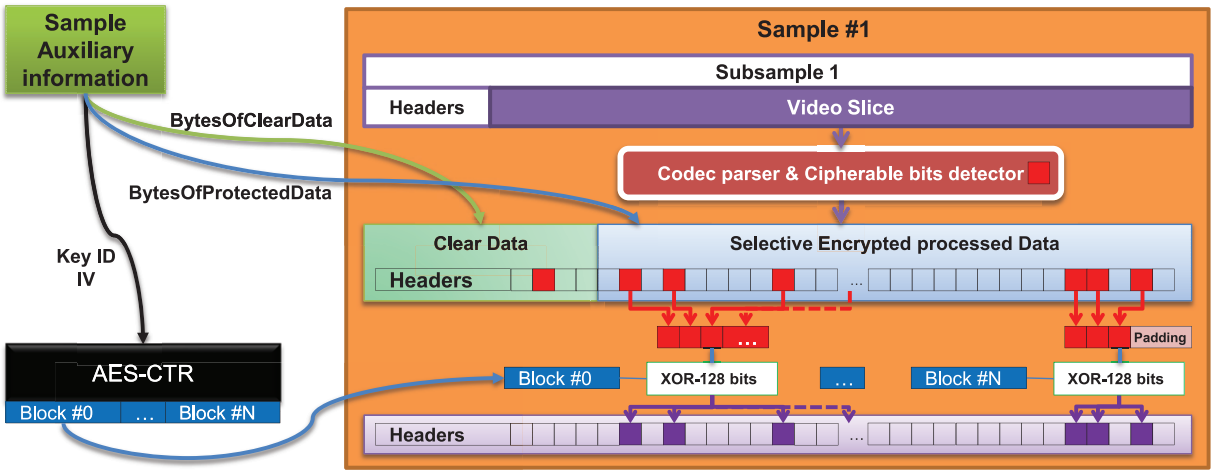

Figure 10 — Content Sensitive Encryption scheme

Samples protected with content sensitive scheme shall follow subsample encryption of NAL Structured Video tracks as defined in 9.5.2. The samples shall be divided into one or more contiguous subsamples. Each subsample consists of an unprotected part of `BytesOfClearData`, potentially 0, followed by a protected part. Bits contained in the clear part of the subsample shall not be selected for the decryption process. The first bit selectable for the encryption process in the range of protected data shall be XORed with the first bit of the first encrypted cipher block.

The AES-CTR counter shall be incremented after each completely used encrypted cipher block (128 bits) or at the subsample boundaries; this implies that if not all bits were consumed on the last cipher block of a subsample, the block shall be considered as consumed and the counter shall be incremented before processing any subsequent subsample associated with that cipher.

10.1, 10.2, 10.3 and 10.4.1

Replace all uses of

“Encrypted video tracks using NAL”

with

“Encrypted video tracks or items using NAL”

10.1 and 10.2

Replace

“The version of the `TrackEncryptionBox (‘tenc’)` SHALL be 0.”

with

“For tracks, the version of the `TrackEncryptionBox (‘tenc’)` SHALL be 0. For items, the version of the `ItemEncryptionBox (‘ienc’)` SHALL be 0.”

10.1

Replace

"Non-video encrypted tracks SHALL be protected using a full sample encryption as specified in section 9.4."

with

“When a single key applies to each sample, encrypted tracks or items not using NAL structured video conforming to ISO/IEC 14496-15 SHALL be protected using full sample encryption as specified in 9.4. When multiple keys apply to samples, encrypted tracks or items not using NAL structured video conforming to ISO/IEC 14496-15 SHALL be protected using subsample encryption as specified in 9.5.1.”

10.2

Replace

“Other tracks SHALL be protected using full sample encryption as specified in section 9.4.”

with

“When a single key applies to each sample, other tracks or items SHALL be protected using full sample encryption as specified in 9.4. When multiple keys apply to samples, other tracks or items SHALL be protected using subsample encryption as specified in 9.5.1.”

10.3 and 10.4

Replace

“The version of the `TrackEncryptionBox (‘tenc’)` SHALL be 1.”

with

“For tracks, the version of the `TrackEncryptionBox (‘tenc’)` SHALL be 1. For items, the version of the `ItemEncryptionBox (‘ienc’)` SHALL be 1.”

10.3

Replace

"Tracks other than video are protected using whole-block full-sample encryption as specified in 9.7, and hence `skip_byte_block` SHALL be 0."

with

“When a single key applies to each sample, encrypted tracks or items not using NAL structured video conforming to ISO/IEC 14496-15 SHALL be protected using whole-block full-sample encryption as specified in 9.7, and hence `skip_byte_block` SHALL be 0. When multiple keys apply to samples, encrypted tracks or items not using NAL structured video conforming to ISO/IEC 14496-15 SHALL be protected using subsample encryption as specified in 9.5.1.”

10.4

Replace

"Tracks other than video MAY be protected using whole-block full-sample encryption as specified in 9.6 or 9.7, and hence `skip_byte_block` SHALL be 0."

with

“When a single key applies to each sample, encrypted tracks or items not using NAL structured video conforming to ISO/IEC 14496-15 MAY be protected using whole-block full-sample encryption as specified in 9.6 or 9.7, and hence `skip_byte_block` SHALL be 0. When multiple keys apply to samples, encrypted tracks or items not using NAL structured video conforming to ISO/IEC 14496-15 SHALL be protected using subsample encryption as specified in 9.5.1.”

10.4

Add the following subclause after 10.4:

10.5 `'sve1'` AES-CTR sensitive encryption scheme

Support for the ‘sve1’ scheme is optional.

The `scheme_type` field of the scheme Type Box (`'schm'`) SHALL be set to the four-character code `'sve1'`.

Tracks or items carrying media coding types for which no sensitive encryption mode is defined in Annex A shall not use this protection scheme.

Encrypted video tracks or items using NAL unit structured video conforming to ISO/IEC 14496-15 SHALL be protected using Subsample encryption specified in 9.5 and SHALL use sensitive encryption as specified in 9.8. The NAL unit header should be left in the clear part of the subsample.

NOTE In AVC CAVLC, the slice header can be encrypted but can still be parsed.

Pattern encryption SHALL NOT be used. As a result, the fields `crypt_byte_block` and `skip_byte_block` SHALL be 0 and the version of the Track Encryption Box (`'tenc'`) SHALL be 0.

Non-video encrypted tracks SHALL be protected using full-sample encryption as specified in 9.4 and SHALL use sensitive encryption as specified in 9.8.

For tracks, the version of the `TrackEncryptionBox ('tenc')` SHALL be 0. For items, the version of the `ItemEncryptionBox ('ienc')` SHALL be 0.

Constant IVs SHALL NOT be used; `Per_Sample_IV_Size` SHALL NOT be 0, except for unencrypted sample groups.

11.3.4

Following 11.3.4, add the following annex:

Annex A
(normative)

Content sensitive encryption scheme

A.1 Code-words containing bits selected for encryption for MPEG-4/AVC CAVLC

A.1.1 General

This annex gives the list of all VLC tables and code words that shall be encrypted by the content sensitive encryption process for AVC|H264 CAVLC mode (i.e. entropy_coding_mode is equal to 0 in ISO/IEC 14496-10 in Picture Parameter set RBSP syntax).

A.1.2 Slice QP Delta

In ISO/IEC 14496-10:2014, 7.3.3 (Slice header syntax), **slice_qp_delta** is coded in se(v) (i.e. signed Exponential-Golomb code-word), and the value is given in Table A.1. But the value of slice_qp_delta shall be limited such that $SliceQP_Y$ is in the range of $-QpBdOffset_Y$ to +51, inclusive. So this code-word is eligible to be cyphered if, and only if, its absolute value is less than:

$$2^{Floor\left(Log2\left(Min\left(QpBdOffset_Y+26+pic\_init\_qp\_minus26\ ,\ 25-pic\_init\_qp\_minus26\right)\right)\right)} \quad (1)$$

Then, the suffix bits (i.e. the bits following the first '1'), as illustrated by the bold font in Table A.1, shall be selected for Content Sensitive encryption.

Table A.1 — Slice_QP_delta code-words table

Index	Slice_QP_Delta value	Code-word
0	0	1
1	1	01**0**
2	−1	01**1**
3	2	001**00**
4	−2	001**01**
5	3	001**10**
6	−3	001**11**
7	4	0001**000**
8	−4	0001**001**
…	….	**…**

A.1.3 Macroblock type

In ISO/IEC 14496-10:2014, 7.3.5 (Macroblock layer syntax), **mb_type** specifies the macroblock type is coded in ue(v) (i.e. unsigned Exponential-Golomb code-word) but the semantics of mb_type depend on the slice type:

— If slice_type is I, the bits in bold font in Table A.2 shall be selected for CONTENT SENSITIVE ENCRYPTION. Moreover, blocks located on the border of the video slice shall not be selected for Content Sensitive encryption.

Table A.2 — mb_type with I slice

Index	Symbol	Code-word
0	I_NxN	1
1	I_16x16_0_0_0	01**0**
2	I_16x16_1_0_0	01**1**
3	I_16x16_2_0_0	0010**0**
4	I_16x16_3_0_0	0010**1**
5	I_16x16_0_1_0	0011**0**
6	I_16x16_1_1_0	0011**1**
7	I_16x16_2_1_0	000100**0**
8	I_16x16_3_1_0	000100**1**
9	I_16x16_0_2_0	0001**010**
10	I_16x16_1_2_0	0001**011**
11	I_16x16_2_2_0	0001**100**
12	I_16x16_3_2_0	0001**101**
13	I_16x16_0_0_1	000111**0**
14	I_16x16_1_0_1	000111**1**
15	I_16x16_2_0_1	00001000**0**
16	I_16x16_3_0_1	00001000**1**
17	I_16x16_0_1_1	00001**010**
18	I_16x16_1_1_1	00001**011**
19	I_16x16_2_1_1	00001**100**
20	I_16x16_3_1_1	00001**101**
21	I_16x16_0_2_1	00001**110**
22	I_16x16_1_2_1	00001**111**
23	I_16x16_2_2_1	00001**1000**
24	I_16x16_3_2_1	00001**1001**
25	I_PCM	000011010

— If slice_type is P, the bits in bold font in Table A.3 shall be selected for Content Sensitive encryption.

Table A.3 — mb_type for P slice

Index	Symbol	Code-word
0	P_L0_16x16	1
1	P_L0_L0_16x8	01**0**
2	P_L0_L0_8x16	01**1**
3	P_8x8	00100
4	P_8x8ref0	00101
...	...	...

A.1.4 PCM sample Luma and Chroma

In ISO/IEC 14496-10:2014, 7.3.5 (Macroblock layer syntax), **pcm_sample_luma** and **pcm_sample_chroma** are sample values in the raster scan within the macroblock and are coded Fixe-length coding. Therefore, all bits shall be selected for Content Sensitive encryption.

A.1.5 Macroblock QP Delta

In ISO/IEC 14496-10:2014, 7.3.5 (Macroblock layer syntax), **mb_qp_delta** is coded in ue(v) (i.e. unsigned Exponential-Golomb code-word). But the value of mb_qp_delta shall be in the range of −(26 + $QpBdOffset_Y$ / 2) to +(25 + $QpBdOffset_Y$ / 2), inclusive. So this code-word is eligible to be cyphered if, and only if, its absolute value is less than:

$$2^{Floor\left(Log2\left(25+QpBdOffsetY/2\right)\right)} \tag{2}$$

Then, the suffix bits (i.e. the bits following the first '1'), as illustrated by the bold font in Table A.4, shall be selected for Content Sensitive encryption.

Table A.4 — Mb_qp_delta

Index	Mb_QP_Delta value	Code-word
0	0	1
1	1	01**0**
2	–1	01**1**
3	2	00**100**
4	–2	00**101**
5	3	00**110**
6	–3	00**111**
7	4	0001**000**
8	–4	0001**001**
...	....	...

A.1.6 Prediction Intra Luma

In ISO/IEC 14496-10:2014, 7.3.5.1 (Macroblock prediction syntax), **rem_intra4x4_pred_mode** and **rem_intra8x8_pred_mode** are coded in Fixed length coding. Therefore, all bits shall be selected for Content Sensitive encryption. Moreover, blocks located on the border of the video slice shall not be selected for Content Sensitive encryption.

A.1.7 Prediction Intra Chroma

In ISO/IEC 14496-10:2014, 7.3.5.1 (Macroblock prediction syntax), **intra_chroma_pred_mode** is coded in ue(v) (i.e. unsigned Exponential-Golomb code-word). The bits in bold font in Table A.5, shall be selected as for Content Sensitive encryption. Blocks located on the border of the video slice shall not be selected for Content Sensitive encryption.

Table A.5 — intra_chroma_pred_mode table

Index	Direction	code-word
0	DC	0
1	Horizontal	01**0**
2	Vertical	01**1**
3	Plan	00100

A.1.8 Motion prediction reference

In ISO/IEC 14496-10:2014, 7.3.5.1 and 7.3.5.2 (Macroblock prediction syntax and Sub-macroblock prediction syntax), **ref_idx_l0** is coded in te(v) (i.e. truncated Exponential-Golomb code-word) and specifies the index in reference picture list 0 of the reference picture to be used for prediction.

The eligibility for Content Sensitive encryption depends on the maximum range of ref_idx_l0, so let *max_ref_l0* be equal to:

— num_ref_idx_l0_active_minus1+1, if MbaffFrameFlag is equal to 0 or mb_field_decoding_flag is equal to 0.

— 2 * num_ref_idx_l0_active_minus1 + 2, otherwise (MbaffFrameFlag is equal to 1 and mb_field_decoding_flag is equal to 1).

When *max_ref_l0* is equal to 1, ref_idx_l0 is inferred to be equal to 0 and cannot be selected for Content Sensitive encryption.

When *max_ref_l0* is equal to 2, ref_idx_l0 is coded on one bits and shall be selected for Content Sensitive encryption.

When *max_ref_l0* is greater than 2, ref_idx_l0 is coded in ue(v). The suffix bits (i.e. the bits following the first '1') as illustrated by the bold font bits in Table A.6 shall be selected as for Content Sensitive encryption. But this code-word is eligible to be cyphered if, and only if, its value is less than $2^{Floor(Log2(\text{max\_ref\_10}))}$.

Table A.6 — ref_idx_lX code-words table

Index	ref_idx_lX	Code-word
0	0	1
1	1	01**0**
2	2	01**1**
3	3	001**00**
4	4	001**01**
…	…	**…**

In ISO/IEC 14496-10:2014, 7.3.5.1 and 7.3.5.2 (Macroblock prediction syntax and Sub-macroblock prediction syntax), **ref_idx_l1** is coded in te(v) (i.e. truncated Exponential-Golomb code-word), and specifies the index in reference picture list 1 of the reference picture to be used for prediction. It has the same semantics as ref_idx_l0, with l0 and list 0 replaced by l1 and list 1, respectively.

A.1.9 Motion prediction vector

In ISO/IEC 14496-10:2014, 7.3.5.1 and 7.3.5.2 (Macroblock prediction syntax and Sub-macroblock prediction syntax), **mvd_l0** and **mvd_l1** are coded in ue(v) (i.e. unsigned Exponential-Golomb code-word), and specify the difference between a vector component to be used and its prediction.

The suffix bits (i.e. the bits following the first '1'), as illustrated by the bold font bits in Table A.7, shall be selected as for Content Sensitive encryption.

Table A.7 — Mvd_lX table

Index	Mvd_lX	Code-word
0	0	1
1	1	01**0**
2	–1	01**1**
3	2	001**00**
4	–2	001**01**
5	3	001**10**
6	–3	001**11**
7	4	0001**000**
8	–4	0001**001**

Table A.7 *(continued)*

Index	Mvd_lX	Code-word
...	...	...

A.1.10 Trailing ones

In ISO/IEC 14496-10:2014, 7.3.5.3.2 (Residual block CAVLC syntax), **trailing_ones_sign_flag** is coded in Fixed length coding. Therefore, all bits shall be selected for Content Sensitive encryption.

A.1.11 Level Suffix

In ISO/IEC 14496-10:2014, 7.3.5.3.2 (Residual block CAVLC syntax), **level_suffix** is coded in Fixed length coding. Therefore, all bits shall be selected for Content Sensitive encryption.

A.1.12 Total zeros

In ISO/IEC 14496-10:2014, 7.3.5.3.2 (Residual block CAVLC syntax), **total_zeros** is coded in ce(v) (i.e. coded Exponential-Golomb code-word). The bits in bold font in Table A.8 and Table A.9 shall be selected for Content Sensitive encryption Table A.5 only if total_coeff=1.

Table A.8 — Total_zeros table for Block 2x2 and if total_coeff=1

Index	Total_zeros values	Code-word
0	0	0
1	1	01
2	2	01**0**
3	3	01**1**

Table A.9 — Total_zeros table for Block 4x4 and if total_coeff=1

Index	Total_zeros values	Code-word
0	0	1
1	1	01**0**
2	2	01**1**
3	3	001**0**
4	4	001**1**
5	5	0001**0**
6	6	0001**1**
7	7	00001**0**
8	8	00001**1**
9	9	000001**0**
10	10	000001**1**
11	11	0000001**0**
12	12	0000001**1**
13	13	00000001**0**
14	14	00000001**1**
15	15	00000000

A.1.13 Run Before

In ISO/IEC 14496-10:2014, 7.3.5.3.2 (Residual block CAVLC syntax), **run_before** is coded by a specific table (Table A.10) and specifies the number of consecutive transform coefficient levels in the scan with

zero value before a non-zero valued transform coefficient level. The bits in bold font in Table A.10 shall be selected as for Content Sensitive encryption, if and only if the codeword run_before was preceded by (Totalcoeff-2) codewords run_before in the same block.

Table A.10 — Tables for run_before

run_before	zerosLeft						
	1	2	3	4	5	6	>6
0	**1**	1	**11**	1**1**	1**1**	11	1**11**
1	**0**	0**1**	**10**	1**0**	1**0**	0**00**	1**10**
2	—	0**0**	**01**	01	0**11**	0**01**	1**01**
3	—	—	**00**	00**1**	0**10**	0**11**	1**00**
4	—	—	—	00**0**	0**01**	0**10**	01**1**
5	—	—	—	—	0**00**	10**1**	01**0**
6	—	—	—	—	—	10**0**	001
7	—	—	—	—	—	—	0001
8	—	—	—	—	—	—	00001
9	—	—	—	—	—	—	000001
10	—	—	—	—	—	—	0000001
11	—	—	—	—	—	—	00000001
12	—	—	—	—	—	—	000000001
13	—	—	—	—	—	—	0000000001
14	—	—	—	—	—	—	00000000001

A.2 Code-words containing bins selected for encryption for MPEG-4/AVC CABAC

A.2.1 General

This clause gives the list of all VLC tables and code words that shall be encrypted by the Content Sensitive encryption process for AVC|H264 CABAC mode (i.e. entropy_coding_mode is equal to 1 in ISO/IEC 14496-10 in Picture Parameter set RBSP syntax).

A.2.2 PCM sample Luma and Chroma

In ISO/IEC 14496-10:2014, 7.3.5 (Macroblock layer syntax), **pcm_sample_luma** and **pcm_sample_chroma** are sample values in the raster scan within the macroblock and are coded Fixe-length coding. Therefore, all bits shall be selected for Content Sensitive encryption.

A.2.3 Absolute value of coefficient level

In ISO/IEC 14496-10:2014, 7.3.5.3.3 (Residual block CABAC syntax), **coeff_abs_level_minus1** is the absolute value of a transform coefficient level minus 1.

coeff_abs_level_minus1 is coded in UEG0 bin string (i.e. concatenated unary/0th order Exp-Golomb bin string), as specified in ISO/IEC 14496-10:2014, 9.3.2.3. The Unary prefix is obtained by invoking TU binarization process with cmax=14 as specified in ISO/IEC 14496-10:2014, 9.3.2.2.

The bins in bold font in Table A.11 shall be selected as for Content Sensitive encryption, i.e. the UEG0 suffix bit string when Coeff_abs_level_minus1>14.

Table A.11 — Coeff_abs_level_minus1 table

Coeff_abs_level_minus1	Unary Prefix	Exp-Golomb	
		Prefix	Suffix
0	0		
1	1		
2	10		
3	110		
…	…		
12	1111111111110		
13	11111111111110		
14	11111111111111	0	
15	11111111111111	10	**0**
16	11111111111111	10	**1**
17	11111111111111	110	**00**
18	11111111111111	110	**01**
19	11111111111111	110	**10**
20	11111111111111	110	**11**
21	11111111111111	1110	**000**
…	…	…	…

NOTE Only Bypass decoding process is applied on the bins selected as for Content Selective Encryption.

A.2.4 Motion prediction vector

In ISO/IEC 14496-10:2014, 7.3.5.1 and 7.3.5.2 (Macroblock prediction syntax and Sub-macroblock prediction syntax), **mvd_l0** and **mvd_l1** specify the difference between a vector component to be used and its prediction.

mvd_l0 and mvd_l1 are coded in UEG3 bin string (i.e. concatenated unary/3th order Exp-Golomb bin string) as specified in ISO/IEC 14496-10:2014, 9.3.2.3. The Unary prefix is obtained by invoking TU binarization process with cmax=9 as specified in ISO/IEC 14496-10:2014, 9.3.2.2.

The bits in bold font in Table A.12 shall be selected as for Content Sensitive encryption, i.e. the UEG3 suffix bit string when Abs(Mvd_lX)>32, and the sign bits.

Table A.12 — Mvd_lX table

Mvd_lX	Unary Prefix	3th order Exp-Golomb		sign
		Prefix	Suffix	
0	0			
1	10			**0**
–1	10			**1**
2	110			**0**
–2	110			**1**
…	…			**…**
8	111111110			**0**
–8	111111110			**1**

Table A.12 *(continued)*

Mvd_lX	Unary Prefix	3th order Exp-Golomb		sign
		Prefix	Suffix	
9	111111111	0	000	**0**
–9	111111111	0	000	**1**
10	111111111	0	001	**0**
–10	111111111	0	001	**1**
…	…	0	…	**…**
16	111111111	0	111	**0**
–16	111111111	0	111	**1**
17	111111111	10	0000	**0**
–17	111111111	10	0000	**1**
18	111111111	10	0001	**0**
–18	111111111	10	0001	**1**
…	…	…	…	**…**
32	111111111	10	1111	**0**
–32	111111111	10	1111	**1**
33	111111111	110	**00000**	**0**
–33	111111111	110	**00000**	**1**
34	111111111	110	**00001**	**0**
–34	111111111	110	**00001**	**1**
35	111111111	110	**00010**	**0**
–35	111111111	110	**00010**	**1**
…	…	…	**…**	**…**

NOTE Only Bypass decoding process is applied on the bins selected as for Content Sensitive encryption.

A.2.5 Sign of coefficient level

In ISO/IEC 14496-10:2014, 7.3.5.3.3 (Residual block CABAC syntax), **coeff_sign_flag** is the sign of a transform coefficient level and is coded in Fixed length coding. Therefore, all bins shall be selected as for Content Sensitive encryption.

A.3 Code-words containing bins selected for encryption MPEG-H/HEVC

A.3.1 General

This clause gives all possible encrypted syntax elements in ISO/IEC 23008-2 in format compliant (i.e. providing HEVC compliant bitstream).

A.3.2 Motion vector difference

The absolute value of MV differences minus 2 is binarization in EG1 code and then bypass coded. Thus, only the suffix part of MV difference is encrypted in format compliant and without impacting the compression ratio. Thus, the suffix of MV difference shall be selected for Content Sensitive encryption.

The EGk code is a concatenation of prefix and suffix. For an unsigned integer Y, the prefix part of the EGk code is the Unary representation of $l(Y)=\left\lfloor log_2\left(\frac{Y}{2^k}+1\right)\right\rfloor$. The suffix part is the Fixed Length code of $Y + 2^k(1 - 2^{l(y)})$ with $cMax = k + l(Y)$. Table A.13 gives an example of the binarization of the MV syntax element minus 2 with using EG1 code as defined in ISO/IEC 23008-2. All bins of the suffix part shall be selected for Content Sensitive encryption.

Table A.13 — Binarization of the MV minus 2 syntax element with EG1 code

MV difference minus2	Prefix	Suffix
2	10	**00**
3	10	**01**
4	10	**10**
5	10	**11**
6	110	**000**
7	110	**001**
8	110	**010**
9	110	**011**
10	110	**100**
11	110	**101**
12	110	**111**

A.3.3 Motion vector difference sign

The signs of MV difference (**mvd_sign_flag** defined in ISO/IEC 23008-2) shall be selected for Content Sensitive encryption since they are binarized in FL code with cMax = 1 and bypassed.

A.3.4 Delta QP sign syntax element

The sign of Delta QP (**cu_qp_delta_sign_flag** defined in ISO/IEC 23008-2) is binarized in FL code with cMax = 1 and bypassed. This shall be selected for Content Sensitive encryption.

A.3.5 Transform coefficient sign

Transform coefficient sign (**sig_coeff_flag** defined in ISO/IEC 23008-2) is binarized in FL code with cMax = 1 and bypassed. This shall be selected for Content Sensitive encryption.

Bibliography

Remove Reference [2].

For Reference [5], add the date of publication: 2014.

ICS 35.040.40

Price based on 22 pages