INTERNATIONAL ORGANISATION FOR STANDARDISATION
ORGANISATION INTERNATIONALE DE NORMALISATION
ISO/IEC JTC1/SC29/WG11
CODING OF MOVING PICTURES AND AUDIO

ISO/IEC JTC1/SC29/WG11 MPEG2016/m39153
October 2016, Chengdu, China

Source	**Thales, IETR-INSA, Telecom ParisTech**
Status	**Input Document**
Title	**Adding new scheme in Common Encryption**
Author	Cyril Bergeron, Wassim Hamidouche, Jean Le Feuvre, Cyril Concolato

1 Introduction

During the 115th MPEG meeting, we presented contribution m38535 [1] in which we described a way of managing region encryption in the scope of Visual Identity Privacy management [2]. We propose to add new functionalities in ISO/IEC 23001-7 (Common encryption in ISO base media file format files) [3] for managing several key identifier inside a sample group.
This contribution first describes example of use cases not addressed by the existing standard and then suggest extending the syntax of ‘seig’

2 Use cases not addressed by Common Encryption

In ISOBMFF, the internal file organization can be different for application purposes (Figure 1): non-fragmented, fragmented or segmented. So these organizations may contain in different way the video track with multiple regions (independent tiles) or with multiple scalable layers (for example: SVC or SHVC). In some applications, we can consider that we want to have a conditional access for different part of this organization. In this contribution we present two uses cases:

- Tiled video, (example: mosaic with multiple TV channel or one ROI and background tiles) where each tile can be decoded independently with an associated encryption scheme.
- Multi-layer Scalable video, where each quality (or spatial) layer can have a different encryption scheme to provide several quality according to various paid subscription.

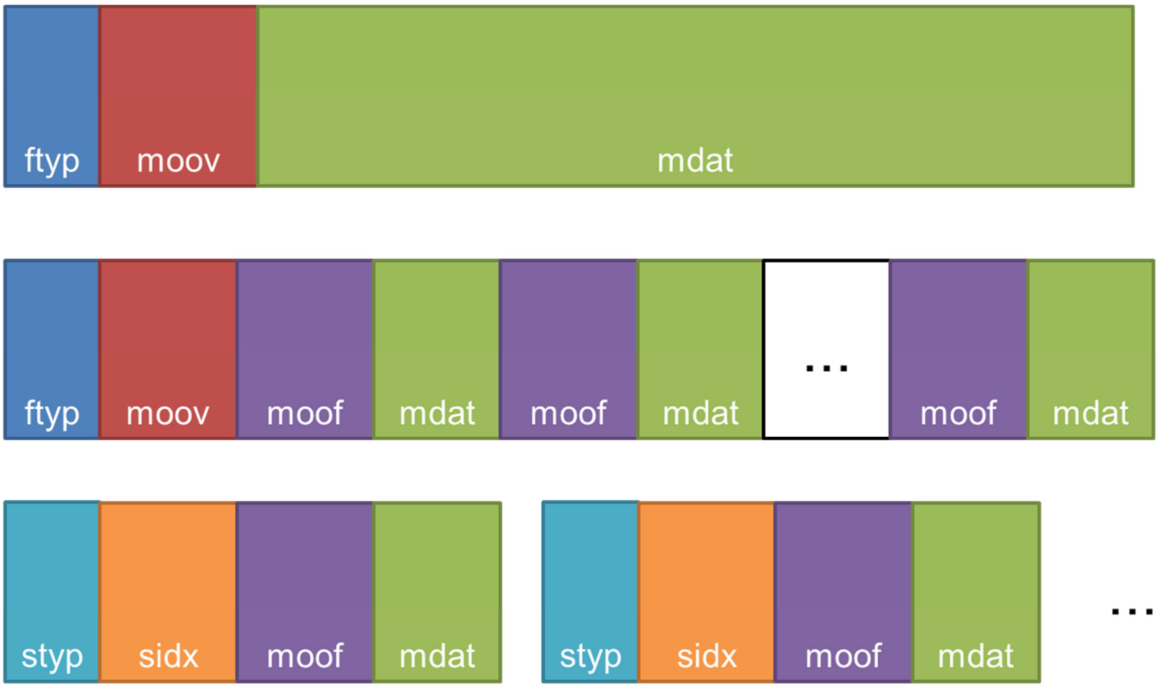

Figure 1 - ISOBMFF file organizations

Common Encryption ('cenc') protection scheme enables multiple Key Systems to decrypt the same media content. Each key is identified by a keyID and each encrypted sample is associated with the keyID of the key needed to decrypt it. This association is signaled either through the specification of a default key ID in the track encryption box ('tenc') or by assigning the sample to a Sample Group, the definition of which specifies a key ID. Files may contain a mixture of encrypted and unencrypted samples. But it is not possible to have different keyIDs for a given sample when we want to recompose a tile track based file, or multi-track hierarchically coded bitstream file into a single-track file.

3 Proposal: new scheme in common encryption

```
aligned(8) class CencSampleEncryptionInformationGroupEntry
extends SampleGroupDescriptionEntry( ‘seig’)
{
unsigned int(1) multi_key_flag;
unsigned int(7) reserved=0;
unsigned int(4) crypt_byte_block = 0;
unsigned int(4) skip_byte_block = 0;
unsigned int(8) isProtected;
if (multi_key_flag == 1){
      unsigned int(8) count;
      for (i=1; i <= count; i++){
            unsigned int(8) Per_Sample_IV_Size[i];
            unsigned int(8)[16] KID[i];
            if (isProtected ==1 && Per_Sample_IV_Size[i] == 0) {
                  unsigned int(8) constant_IV_size[i];
                  unsigned int(8)[constant_IV_size] constant_IV[i];
                  }
            }
      }
else
      {
      unsigned int(8)[16] KID;
      if (isProtected ==1 && Per_Sample_IV_Size == 0) {
            unsigned int(8) constant_IV_size;
            unsigned int(8)[constant_IV_size] constant_IV;
            }
      }
}
```

Each protected sample in a protected track shall have an Initialization Vector associated with it. Both Initialization Vectors and Subsample encryption information may be provided as Sample Auxiliary Information with `aux_info_type` equal to the scheme and `aux_info_type_parameter` equal to 0. This implies that traditional CENC will only have one saiz/saio of type “cenc”. However, if different keys are used to protect different parts of the samples, this is not enough.

3.1 Approach 1

We would like to reuse the CENC sai format without modification for implementation simplicity (single format used). This implies that we need a way to associate a given sai data with one of the key assigned to the current sample. We propose to use ‘`aux_info_type_parameter`’ as a parameter to indicate the keyID from the seig Sample Group Description entry that applies to the sample.

If a sample has two runs of data encrypted with key1 and key2, the track/fragment will have two sai, one with `aux_info_type_parameter=1` indicating key index #1 in the seig entry, the other with `aux_info_type_parameter=2` indicating key index #2 in the seig entry,

The advantage of this method is its backward compatibility with existing cenc/sai processors, but it implies as many saiz/saio as there are keys involved in the protection of a sample.

3.2 Approach 2

Another approach would be to use the `aux_info_type_parameter` to extend the current sai for cenc by indicating a list of keys

The proposed format of the sample auxiliary information for samples with this type could be as follows:

```
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{
  for (i=1; i <= aux_info_type_parameter; i++)
  {
   unsigned int(8) seig_subindex;
   if (seig_subindex) {
    unsigned int(Per_Sample_IV_Size*8) InitializationVector[i];
    unsigned int(16) subsample_count;
    {
     unsigned int(16) BytesOfClearData[i];
     unsigned int(32) BytesOfProtectedData[i];
    } [subsample_count]
   }
  }
 }
}
```

seig_subindex: is the 1-based index of the Key ID from the list in `'seig' entry`. If 0, this means the key is not used for this sample.

Figure 2 is a Subsample encryption example showing two samples, each containing three Subsamples, with two different Key ID applied on different subsample, with an associated per-sample Initialization Vector and a logically continuous sequence of 16-byte cipher blocks interspersed with unencrypted byte ranges.

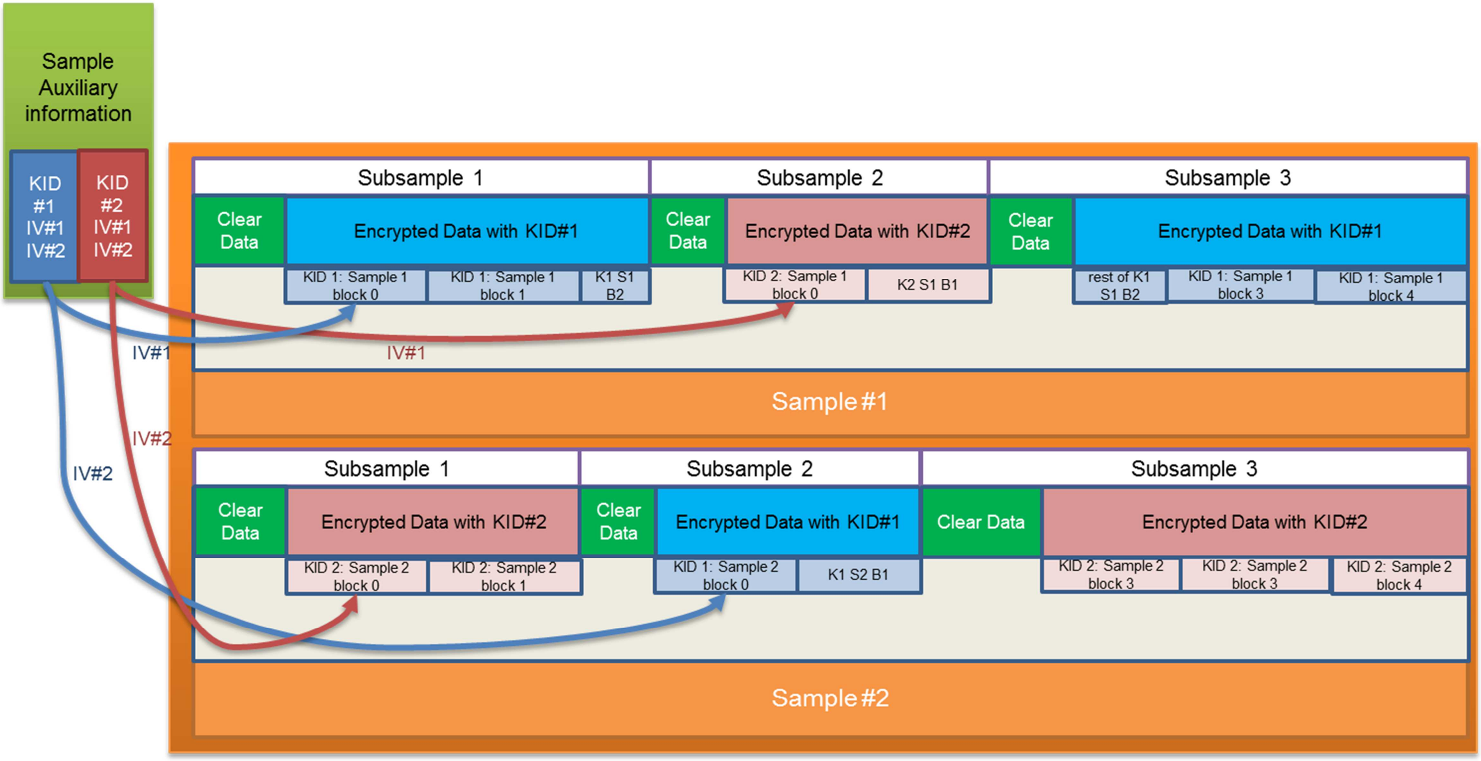

Figure 2 - subsample encryption with different keys

4 Conclusions

This contribution presented a way of extending common encryption signaling to address those presented use cases. We recommend that MPEG experts take into consideration this solution for adding it in the scope of CENC.

5 References

[1] m389535 - Uses of Selective Encryption for Visual Identity Management AF (June 2016, Geneva,CH)

[2] w16226 - Use cases and requirements on Visual Identity Management AF (June 2016, Geneva,CH)

[3] ISO/IEC 23001-7:2015, Information technology — MPEG systems technologies — Part 7: Common encryption in ISO Base Media File Format files - 2nd Edition. *International Standard.*