

Digital Video Broadcasting (DVB) CBMS Service Purchase and Protection Open Framework Content Encryption Specification

European Broadcasting Union



Union Européenne de Radio-Télévision

THIS IS A PROVISIONAL DVB DOCUMENT. IT MAY BE CHANGED BEFORE FINAL ADOPTION BY DVB. THIS PROVISIONAL DOCUMENT IS FOR DISCUSSION PURPOSES ONLY. IMPLEMENTERS ARE NOT ENTITLED TO RELY ON THIS PROVISIONAL DOCUMENT. WHERE POSSIBLE, ITEMS FOR WHICH CONSENSUS HAS NOT BEEN REACHED ARE SUITABLY MARKED, FOR EXAMPLE BY SQUARE BRACKETS. IMPLEMENTERS SHOULD ALSO NOTE THAT ONLY FINAL SPECIFICATIONS ADOPTED BY DVB ARE (SUBJECT TO THE "NEGATIVE DISCLOSURE" RIGHTS OF MEMBERS) ENTITLED TO THE IPR LICENSING TERMS OF DVB'S MEMORANDUM OF UNDERSTANDING.



Reference

REN/JTC-DVB-102

Keywords

broadcasting, digital, DVB, MPEG, service, TV,
video, AVC

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <http://www.etsi.org/tb/status/>

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2000.
© European Broadcasting Union 2000.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword	4
1 Scope	5
2 References	5
3 Definitions and abbreviations.....	5
3.1 Definitions	5
3.1.1 Parameter Set	6
3.1.2 Parameter Set Elementary Stream	6
3.1.3 Video Elementary Stream	6
3.2 Abbreviations.....	6
4 Introduction	6
4.1 Audio-visual content (streamed content)	6
4.2 Generic content (file download)	7
5 AVC Content Encryption	7
5.1 Encryption System.....	7
5.1.1 Introduction	7
5.1.2 Encryption unit	8
5.1.3 Access Unit format	8
5.1.4 Content Encryption.....	8
5.2 RTP payload format.....	8
5.3 SDP signalling	9
5.3.1 Encryption specific additional signaling.....	9
5.3.2 AVC specific additional signaling	9
5.4 MP4 storage.....	9
5.4.1 Salt signaling	9
6 Encrypted File Download	10
6.1 OMA DCF adaptation.....	10
Bibliography	13
History	14

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://www.etsi.org/ipr>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by the Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELEctrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACCONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

Founded in September 1993, the DVB Project is a market-led consortium of public and private sector organizations in the television industry. Its aim is to establish the framework for the introduction of MPEG-2 based digital television services. Now comprising over 200 organizations from more than 25 countries around the world, DVB fosters market-led systems, which meet the real needs, and economic circumstances, of the consumer electronics and the broadcast industry.

National transposition dates
<p>Date of adoption of this EN:</p> <p>Date of latest announcement of this EN (doa):</p> <p>Date of latest publication of new National Standard or endorsement of this EN (dop/e):</p> <p>Date of withdrawal of any conflicting National Standard (dow):</p>

1 Scope

The present document specifies the encryption method used for content broadcast in DVB-CBMS systems.

More specifically, it specifies encryption for visual content encoded with the ISO-IEC 14496-10 [1] codec, also known as AVC and H.264, when this content is carried over an RTP [3] stream and when it is stored in MP4 files.

This document also specifies encryption of non-audio-visual downloaded content.

This specification should be read in conjunction with :

- ETSI EN xxx xx1 DVB CBMS Service Purchase and Protection Open Framework, System Architecture.
- ETSI EN xxx xx3 DVB CBMS Mobile Device Security Framework.

2 References

The following documents are used either as normative or informative reference in support of the present specification:

- [1] ISO/IEC 14496-10 – “Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding”
- [2] ISO/IEC 14496-15 - Information technology — Coding of audio-visual objects — Part 15: AVC File Format
- [3] IETF RFC 3550 – “RTP: A Transport Protocol for Real-Time Applications”
- [4] ISMA 1.0 – “Internet Streaming Media Alliance Implementation Specification V 1.0”
- [5] IETF RFC 3984 – “RTP payload Format for H.264 Video”
- [6] IETF RFC 2327 – “SDP: Session Description Protocol”
- [7] IETF RFC 3711 – “SRTP: Secure Real Time Protocol”
- [8] OMA-DRM-DCF-V2_0-20041213-C – “DRM Content Format V2.0”
- [9] IETF RFC 2396 – “Uniform Resource Identifier”
- [10] ETSI EN xxx xx1 DVB CBMS Service Purchase and Protection Open Framework, System Architecture
- [11] ETSI EN xxx xx3 DVB CBMS Mobile Device Security Framework
- [12] ETSI TR 101 154 v1.7.1 DVB Implementation guidelines for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

3.1.1 Parameter Set

A parameter set is either a sequence parameter set or a picture parameter set. This term is used to refer to both types of parameter sets.

3.1.2 Parameter Set Elementary Stream

An elementary stream containing samples made up of only sequence and picture parameter set NAL units synchronized with the video elementary stream.

3.1.3 Video Elementary Stream

An elementary stream containing access units made up of NAL units for coded picture data.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AU	Access Unit
AVC	Advanced Video Codec, see [1]
DVB	Digital Video Broadcasting
FEC	Forward Error Correction
ISO	International Organization for Standardization
LSB	Least Significant Bit
MPEG	Moving Pictures Expert Group
NAL	Network Abstraction Layer
NALU	NAL Unit
RTP	Real Time Protocol, see [3]
SDP	Session Description Protocol, see [6]
uimsbf	unsigned integer most significant bit first
VCL	Video Coding Layer

4 Introduction


In the context of DVB-CBMS, content confidentiality is provided by encryption. Two categories of contents are considered: audio-visual content and generic content. This document specifies how to perform content encryption for both categories.

4.1 Audio-visual content (streamed content)

In the audio-visual category, this document concentrates on encryption of AVC [1] content. Other types of content are covered by the ISMACryp specification [4].

The goal of this specification is to provide a standard way of encrypting AVC content while it is carried over an RTP stream or stored in an ISO Base Media File Format (MP4) file. The intent is to concentrate on encrypting the content itself rather than the transport, thus providing implicit better security by minimizing the processing distance between the decryption process and the decoding process. Reduction of this processing distance also opens the way for hardware implementation of both the decryption and decoding in the same chipset without the content being exposed outside the chipset (or even to the CPU of the chipset) in its clear compressed form.

Another goal of content encryption as opposed to transport encryption is to allow content to be transposed from one transport (e.g. RTP) to another (e.g. MP4 file) without requiring decryption and re-encryption, which would expose the content and require knowledge of the decryption key from the device operating the transposition.

In a similar fashion, content encryption should allow the storage of content (on a PVR style device) without requiring its decryption. To assist this, signalling is required outside the encrypted content of certain events within the content, such as the start and type of an encoded frame. This signalling should be comparable with the existing DVB mechanisms such as those in .

4.2 Generic content (file download)

In the generic content category, this document specifies an encryption method and generic container for encrypting and carrying any kind of data. This encryption system MAY be used for any finite-length content that is to be considered as a whole by the receiver and for which a complete and error-less reception is required prior to consumption. It SHOULD NOT be used to encrypt audio-visual content for which a dedicated encryption standard has been defined, even if this content is of finite length and meant to be downloaded in its entirety prior to consumption (e.g. AVC content that needs to be stored encrypted in a file and broadcast as a whole rather than streamed over RTP SHOULD NOT be encrypted as generic content, but SHOULD instead be encrypted using the specification described in chapter “5 AVC Content Encryption”).

5 AVC Content Encryption

This section specifies how AVC content shall be encrypted and how this encryption shall be signalled at the transport layer for two transports: RTP streaming and MP4 file storage.

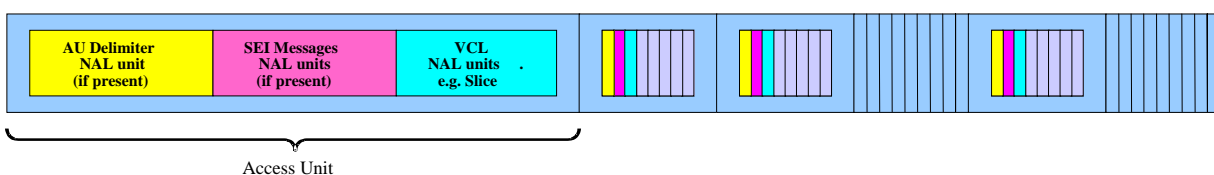
5.1 Encryption System

5.1.1 Introduction

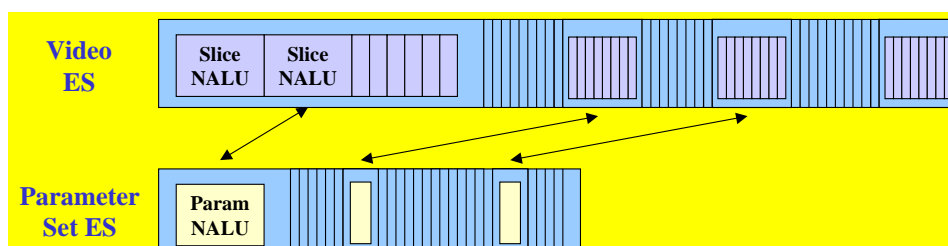
The AVC specification [1] fully describes the bitstream of an AVC video stream and introduces basic concepts:

- The Video Coding Layer (VCL), which contains the signal processing functionality of the codec.
- The Network Abstraction Layer (NAL), which encapsulates the VCL bitstream into NAL units suitable for the transmission over packet networks.
- The Access Unit (AU), the smallest piece of a bitstream that can be associated with a single presentation timestamp. It consists of a set of NAL Units of various types.
- The Parameter Set, which is a set of information used by multiple Access Units and is itself contained in a NAL Unit. Parameter Sets can change over time and may thus require a separate elementary stream for their distribution.

The following diagram illustrates these concepts:

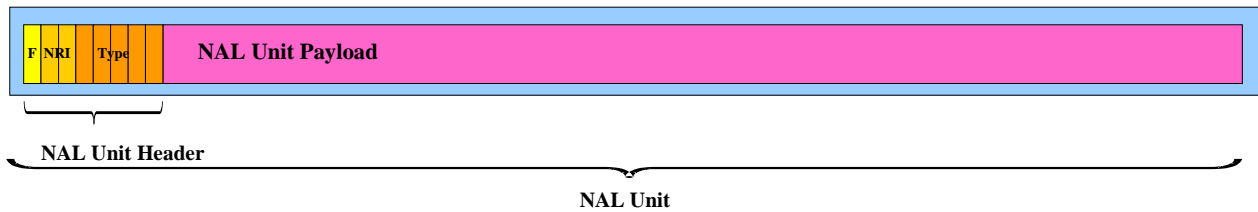


(a) Single Video Elementary Stream containing NAL Units



(b) Synchronized Video and Parameter Sets with arrows denoting synchronization between streams.

A NAL Unit is a block of bytes of variable size preceded by a one-byte header:



Note that a NAL Unit is framed externally, in the sense that it does not include information about its length, which must be signaled by other means (typically the transport layer).

5.1.2 Encryption unit

The NAL introduced by AVC is intended to provide fine grained flexibility and implicit fragmentation rules for efficient carriage of AVC content on any type of transport. Indeed, this flexibility is used extensively in the definition of the RTP payload for AVC in [5] where NAL units of a single Access Unit may be sent in multiple RTP packets and not necessarily in the canonical order. In the RTP packet payload, access units are framed by not only their size but also additional information that allows the receiver to reorder the NALUs for consistent feeding to the decoder.

Storage in an MP4 file on the other hand is more conventional in that all NALU making up a single AU are stored together and in canonical order in a single Sample with a simple signaling scheme for the framing of NALUs: each NALU is preceded by its size encoded on a configurable number of bytes.

This difference in handling AUs means that there is in fact no standard and unique way of encoding a full AU, that encoding depends on the transport.

For the sake of simplicity, this specification defines such an encoding to be used in both the RTP and the MP4 transport and considers this standardized AU as the basic unit of encryption.

5.1.3 Access Unit format

The format of the Access Unit shall be compliant to the AVCSample structure defined in [2] (copied here for the reader's convenience):

```

aligned(8) class AVCSample
{
    unsigned int PictureLength = sample_size; //Size of AVCSample from SampleSizeBox
    for (i=0; i<PictureLength; ) // to end of the picture
    {
        unsigned int((AVCDecoderConfigurationRecord.LengthSizeMinusOne+1)*8) NALUnitLength;
        bit(NALUnitLength * 8) NALUnit;
        i += (AVCDecoderConfigurationRecord.LengthSizeMinusOne+1) + NALUnitLength;
    }
}
  
```

Note that PictureLength is a virtual field used to express the structure of the AVCSample, it does not actually appear in the encoded data.

5.1.4 Content Encryption

Encryption of the content shall be compliant to [4].

5.2 RTP payload format

Transport of encrypted AVC content shall be compliant to [4]. The 'mpeg4-video' mode shall be used for AVC content.

Prior to encryption, each AU carried in this mode shall be encoded as specified by the AVCSample structure above. An RTP packet shall carry exactly one AU or AU fragment. Access Units that need to be fragmented may be split anywhere.

Such signalling as is required to support PVR functionality will be supported outside the encrypted portion of the RTP packet.

5.3 SDP signalling

5.3.1 Encryption specific additional signaling

The configurable aspects of the encryption scheme are signaled at the session level in the SDP [6] text announcing the media streams. The signaling is as specified by [4], with the addition of the new `ISMACRYP_SALT` parameter defined below.

Parameter	Defined Values	Default
<code>ISMACRYP_SALT</code>	base64 encoded 64-bits number	None

`ISMACRYP_SALT` provides the salt value to use for this particular media stream. It is a randomly generated 64 bits integer encoded in base64. This parameter is MANDATORY.

5.3.2 AVC specific additional signaling

Carriage of AVC content over RTP may require some additional signaling at the SDP level for proper decoder setup. Three parameters are defined:

Parameter	Defined Values
<code>avc-nalu-length-size</code>	1, 2 or 4
<code>profile-level-id</code>	See [5], chapter 8.1
<code>sprop-parameter-sets</code>	See [5], chapter 8.1

`avc-nalu-length-size` indicates the length in bytes of the `NALUnitLength` field in an AVC video sample (see 5.1.3 Access Unit format, `avc-nalu-length-size == LengthSizeMinusOne+1`) of the associated stream. The value of this field SHALL be one of 1, 2, or 4, no other values are allowed. This parameter is MANDATORY.

Both `profile-level-id` and `sprop-parameter-sets` are OPTIONAL and their semantic is defined in [5], chapter 8.1.

Example:

```
m=video 49230 RTP/AVP 96
a=rtpmap:96 enc-mpeg4-generic/90000
a=fmtp:96 streamtype=4; mode=mpeg4-video; profile-level-id=42A01E; sprop-parameter-sets=Z0IACpZTBYmI,aMljiA==; avc-nalu-length-size=2; ISMACRYP_IV_LENGTH=4; ISMACRYP_KEY_INDICATOR_LENGTH=2; ISMACRYP_SALT=base64,AoIAE8BAQ8BAQOBSgABQKxkYXRhOmFwc
```

5.4 MP4 storage

Storage of encrypted AVC content shall be compliant to [2] with modifications as specified by [4].

Signalling of encrypted AVC content shall be compliant to [4].

5.4.1 Salt signaling

The salt for each encrypted media stream is signalled with a `ISMACrypSaltBox` defined below:

```
aligned(8) class ISMACrypSaltBox extends Box('islt') {
    unsigned int(64) salt;
}
```

This box is located in the `SchemeInformationBox` defined in [4].

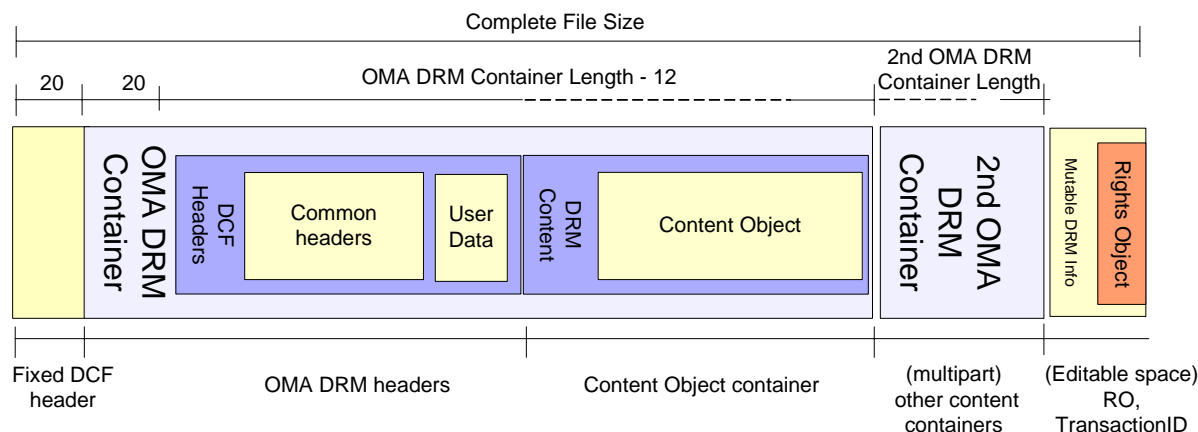
6 Encrypted File Download

In the context of DVB-CBMS, a generic encryption method is required to support protection of downloaded files. This specification provides such a method and is applicable to any type of file, independently of its internal format. It supports the use of different encryption keys for different parts of the file and it supports the access control to the keys by multiple entities (Simulcrypt).

This specification is based on the OMA DRM v2.0 DCF [8] specification which SHALL be followed, except for differences specified in this document.

The high-level overview of the DCF format is depicted in the following figure. The mandatory parts of the format include the file header (File Type box with brand number and minor version fields), immediately followed by an OMA DRM Container box. The OMA DRM Container box MUST include a DCF headers box and a Protected Content box.

The design principles for the format include that the DCF headers box is located at a fixed offset from the beginning of the file, and thus, the OMA DRM Container box MUST be the first box after the file header of 20 octets and the DCF headers box MUST be the first box in the OMA DRM Container.



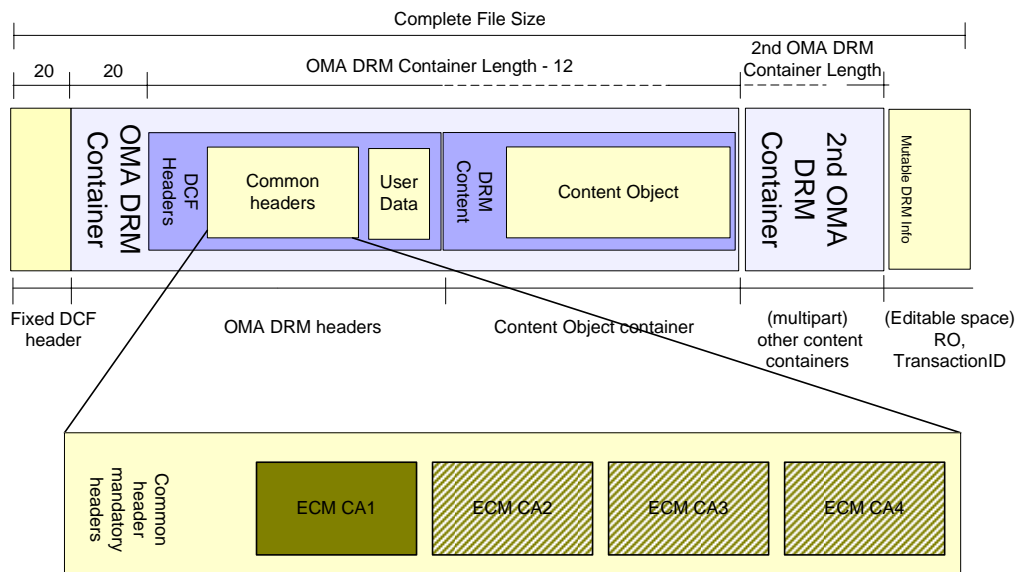
An OMA DRM DCF file MAY include more than one OMA DRM Container. Each of these containers MUST conform to the definition of the OMA DRM Container, and MUST be placed sequentially on the top level (i.e. nesting them is not allowed). The media type of the first OMA DRM Container is considered to be the default media type of the DCF's content.

6.1 OMA DCF adaptation

This document defines several extensions and deviations to OMA DRM v2.0 DCF. They are:

The value of the `RightIssuerURL[]` MUST be empty and `RightIssuerURLLength` MUST be set to 0.

At least one additional ECM box **MUST** be added in the Common header box as shown in the following figure. Additional ECM boxes **MAY** be added to support Simulcrypting of the protected content.



The syntax of the ECM box is:

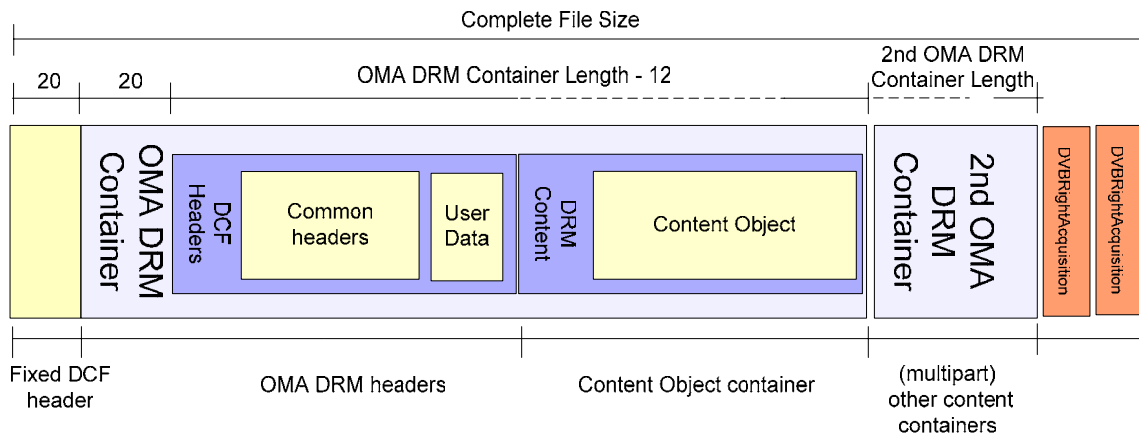
```
aligned(8) class ECM extends FullBox('ECM ', version, 0) {
    bit(16) CAS_ID;
    bit(16) Operator_ID;
    byte[] ECM;          // the actual value of the ECM
}
```

CAS_ID identifies the Key Management System applicable for the associated ECM, as defined in ISO/IEC 13818-1.

Operator_ID identifies the operator using the associated ECM. Allocations of the values of this field is under the control of the KMS identified by **CAS_ID** and allows differentiating between operators using the same KMS.

ECM contains the actual ECM data for the corresponding Key Management System and valid for the associated DRM content (stored in the DRM Container following the DCF Headers).

Additional RightAcquisitionBox Boxes MAY be added after all mandatory boxes as shown in the following figure. Each box contains the necessary information to obtain corresponding rights for the file.



The syntax of this box is:

```
aligned(8) class DVBRightAcquisition extends FullBox('dria',
version, 0) {
    bit(16)          CAS_ID;
    bit(16)          Operator_ID;
    unsigned int(16) RightAcquisitionURLLength;
    char             RightAcquisitionURL[];
    Box              Extensions[];
}
```

CAS_ID identifies the Key Management System applicable for this box, as defined in ISO/IEC 13818-1.

Operator_ID identifies the operator applicable for this box.

RightAcquisitionURLLength gives the length in bytes of the following RightAcquisitionURL field.

RightAcquisitionURL defines the Right Acquisition URL. It MAY be used by the device to obtain rights for the protected content stored in this file. The mechanism by which these rights are obtained is outside the scope of this specification. The value of RightAcquisitionURL MUST conform to [9].

The Extensions field MAY be used to provide additional information relative to the protected file and the associated Key Management System.

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

- ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems".
- Implementation guidelines for use of telecommunications interfaces in the Digital Broadcasting systems (DVB Project Office).

History

Document history		
Jan 4, 2005	G. Moreillon	Initial version
Jan 13, 2005	G. Moreillon	Revised RTP payloads, integrated downloaded file support
Jan 17, 2005	G. Moreillon	Editorial changes
Mar 16, 2005	G. Moreillon	Simplified adaptation of ISMACryp to AVC
Apr 12, 2005	G. Moreillon	Finalized document for publication
May 30, 2005	G. Moreillon	Added Operator identification
June 10, 2005	J. Cunningham/ Kevin Murray	Minor editorial changes.