ATSC Technology Group Report: DRM Guidelines

Doc. TG3-176r1
12 March 2019

Advanced Television Systems Committee
1776 K Street, N.W.
Washington, D.C. 20006
202-872-9160

The Advanced Television Systems Committee, Inc., is an international, non-profit organization developing voluntary standards and recommended practices for digital television. ATSC member organizations represent the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries. ATSC also develops digital television implementation strategies and supports educational activities on ATSC standards. ATSC was formed in 1983 by the member organizations of the Joint Committee on Inter-society Coordination (JCIC): the Electronic Industries Association (EIA), the Institute of Electrical and Electronic Engineers (IEEE), the National Association of Broadcasters (NAB), the National Cable Telecommunications Association (NCTA), and the Society of Motion Picture and Television Engineers (SMPTE). For more information visit www.atsc.org.

Note: The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. One or more patent holders have, however, filed a statement regarding the terms on which such patent holder(s) may be willing to grant a license under these rights to individuals or entities desiring to obtain such a license. Details may be obtained from the ATSC Secretary and the patent holder.

Implementers with feedback, comments, or potential bug reports relating to this document may contact ATSC at https://www.atsc.org/feedback/.

Revision History

Version	Date
TG3-170r1 approved	6 March 2019
Editorial items completed and document published	12 March 2019

Table of Contents

Index of Figures and Tables

ATSC Technology Group Report: DRM Guidelines

1. SCOPE

This is an ATSC Technology Group Report prepared by TG3. This is a document that incorporates consensus on information regarding ATSC Standards and related industry activities.

This document preserves information that was previously published related to Digital Rights Management (DRM) for the ATSC 3.0 suite of standards. This document is not intended to be a comprehensive treatment of the subject matter. See Section 1.1 for details.

1.1 Introduction and Background

ATSC is in the process of revising A/344:2017, "ATSC 3.0 Interactive Content" [10] and A/360:2018, "ATSC 3.0 Security and Service Protection" [9]. Among changes in the 2019 revisions to those documents, ATSC removed informative text that the earlier versions contained. Thus, subject to the ATSC approval process, it is anticipated that the removed informative text will not be found in the 2019 revisions of the documents. In order to preserve public access to the removed informative text, ATSC prepared this Technology Group Report. This report contains the informative text verbatim, as it appeared in the two documents. The new draft standards are published at this writing as Candidate Standards which can be found here: https://www.atsc.org/standards/candidate-standards/, and once fully approved, can be found here: https://www.atsc.org/standards/atsc-3-0-standards/.

ATSC anticipates future completion of a Recommended Practice on Security topics. Recognizing, however, that it may take significant time to develop such a Recommended Practice, ATSC is publishing this Technology Group Report to ensure that the text extracted from the earlier versions of A/344 and A/360 remains publicly accessible. Upon publication of the planned Recommended Practice, this Report likely will be withdrawn.

2. REFERENCES

All referenced documents are subject to revision. Users of this document are cautioned that newer editions might or might not be compatible.

2.1 Informative References

The following documents contain information that may be helpful in applying this Technology Group Report.

[1] ISO/IEC: ISO/IEC 23001-7:2016, "Information technology — MPEG systems technologies — Part 17: Common encryption in ISO base media file format files."

[2] W3C: "Encrypted Media Extensions," W3C Recommendation 18 September 2017, World Wide Web Consortium, https://w3c.github.io/encrypted-media/.

[3] W3C: "Media Source Extensions", W3C Recommendation 17 November 2016, World Wide Web Consortium, https://w3c.github.io/media-source/.

[4] DASH: "Guidelines for Implementation: DASH-IF Interoperability Points for ATSC 3.0", Version 1.1, DASH Industry Forum, Beaverton, OR, 12 June 2018.

[5] ATSC: "ATSC Standard: Signaling, Delivery, Synchronization and Error Protection," Doc. A/331:2017, Advanced Television System Committee, Washington, D.C., 6 December 2017.

[6] ISO/IEC: "Information technology – High efficiency coding and media delivery in heterogeneous environments – Part 1: MPEG media transport (MMT)," Doc. ISO/IEC 23008-1:2017(E), International Organization for Standardization/ International Electrotechnical Commission, Geneva Switzerland.

[7] DASH: "Guidelines for Implementation: DASH-IF Interoperability Points", Version 4.0, DASH Industry Forum, Beaverton, OR, 12 December 2016.

[8] ISO/IEC: "ISO/IEC 23009–1:2014, Information technology — Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats," International Organization for Standardization, Geneva, 2nd Edition, 15 May 2014.

[9] ATSC: "Security and Service Protection", Doc. A/360:2018, Advanced Television System Committee, Washington, D.C., 9 January 2018.

[10] ATSC: "Interactive Content", Doc. A/344:2017, Advanced Television System Committee, Washington, D.C., 18 December 2017.

[11] ISO/IEC: "ISO/IEC 14496-12:2015, "Information technology -- Coding of audio-visual objects -- Part 12: ISO base media file format," International Organization for Standardization, Geneva, 5th Edition, 15 December 2015

3. INFORMATIVE TEXT FROM A/360:2018, "ATSC 3.0 SECURITY AND SERVICE PROTECTION" [9]

5.7.1 Common Encryption

The Common Encryption (`cenc`) protection scheme specifies encryption parameters that can be applied by a scrambling system, along with key mapping methods via common key identifier (KID) for use by different DRM systems, such that the same encrypted version of a file can be handled by different DRM systems which can store proprietary information for licensing and key retrieval in designated metadata boxes of the ISO BMFF file – specifically, the Protection System Specific Header Box (`pssh`) as defined in ISO/IEC 23001-7 [1].

The key advantage of CENC is that by providing a common way to encrypt content, it decouples the content encryption from the key acquisition and thus provides support for multiple DRM systems.

The CENC mechanism only encrypts media samples or parts thereof and leaves the ISOBMFF metadata such as the file and track structure boxes un-encrypted to enable players to recognize and read the file correctly and acquire any required license. CENC supports the encryption of NAL-based video encoding formats such as AVC and HEVC, thus offering sub-sample encryption capability, where only the video data of a sub-sample is encrypted, while the NAL header is not. This flexibility can be used to offer a free preview of the video, enable editing and processing of the video, or provide free access to some service components such as audio. By providing offsets to the encrypted byte ranges inside a sample in an ISOBMFF "mdat" box, players can easily process the file and pass the encrypted chunks to the decryptor for decryption and playback.

In order for decryption to work, CENC provides the following information in the ISOBMFF:

- Key Identifiers (KID): a key ID must be associated with every encrypted sample in a track. In case a single key is used for the whole track.
- Initialization Vectors (IV): the IV, a random number used to initialize an encryption function, is used for randomization and removal of semantics and is essential for strong protection. For every sample, the IV must be known in order to be able to construct the decryption key.

- License Acquisition Information: information about license acquisition is specific to each DRM system. The player needs to support at least one of the DRM systems that offer access to the encrypted stream.

CENC defines a way to store the previous information in the ISOBMFF. The Key Identifiers may be provided:

- As the default_KID in the track encryption box "tenc", when a single key applies to the whole track,
- As a key for a set of samples that share the same encryption key, provided in a sample grouping structure using the sample group description box "sgpd".

The IV for every sample is provided as part of the sample auxiliary information in the "mdat" box or in the "senc" box together with information about the position of the encrypted chunks.

The license acquisition information is provided as part of the protection system specific header box "pssh", where each DRM system is identified by a SystemID. The "pssh" box also provides a list of the provided Key Identifiers and opaque system-specific information that describes how to acquire the keys identified by the supported key ids.

Figure 5.1 depicts the encrypted track structure.

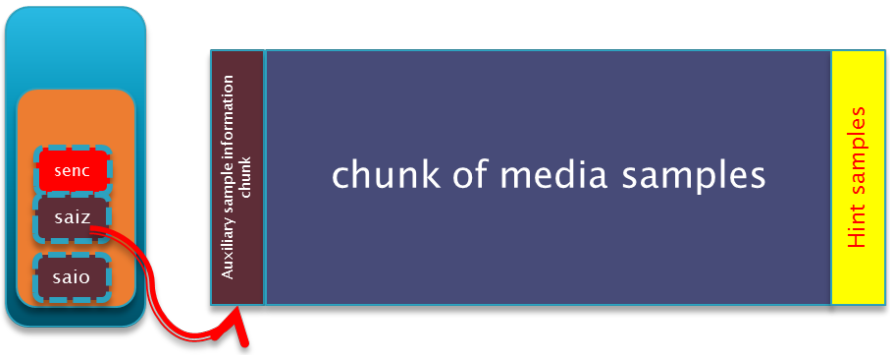

Figure 5.1 Storage of CENC related information.

5.7.2 Encrypted Media Extensions

W3C Encrypted Media Extensions (EME) [2] specifies JavaScript APIs which enable a web application to facilitate the exchange of decryption keys between a device-resident DRM system agent, referred to as the Content Decryption Module (CDM), and a key source or license server located somewhere on the network, to support the playback of encrypted audio and video media content. EME is based on the HTML5 Media Source Extensions specification [3] which enables adaptive bitrate streaming in HTML5 using, DASH-IF ATSC Profile [4] with MPEG-CENC (Common Encryption) [1] protected content. The architecture of EME is illustrated in Figure 5.2, which depicts the primary interactions of the EME workflow between the functional entities involved in the detection of encrypted content and the subsequent acquisition of license and key material, to enable content decryption and playout.

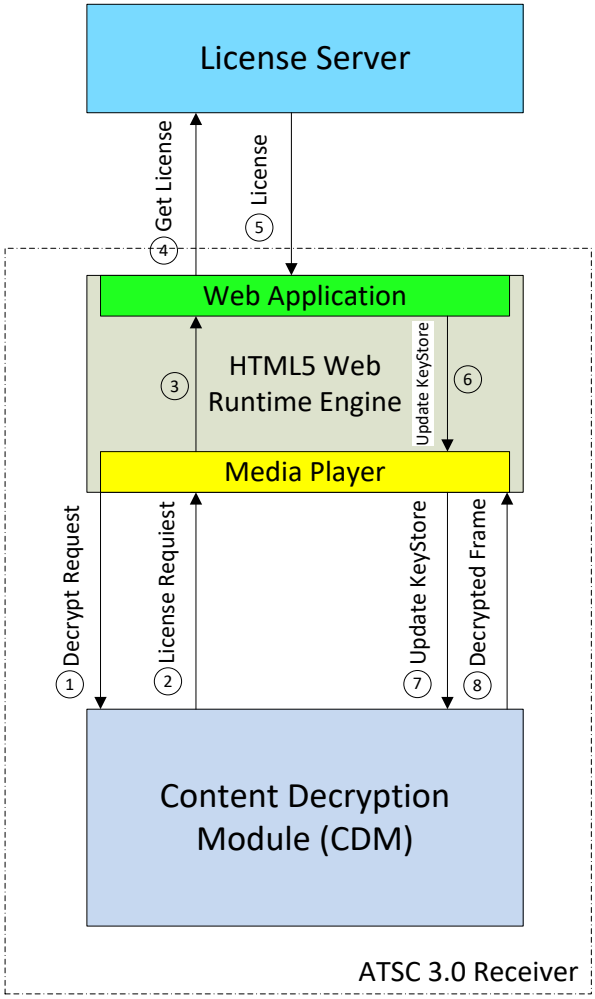

Figure 5.2 Encrypted Media Extensions workflow.

The principal objects in EME are `MediaKeySession` and `MediaKeys`. The web application creates a `MediaKeySession` object, which represents the lifetime of a license and its key(s), by calling `createSession()` on the `MediaKeys` object. The app initiates the request for a license by passing the media data obtained in the `encrypted` event handler to the CDM. In turn, the CDM for the selected DRM system will generate a data blob (license request) and deliver it back to the app, which will then send that request to the license server. The returned license from the server is then passed by the app to the CDM, by using the `update()` method of the `MediaKeySession`. The CDM and/or the browser will use keys stored in the key session to decrypt media samples as they are encountered. The CDM may be either embedded in the web browser, or run in a trusted environment, depending on the required level of security, in passing the decrypted frames to a decoder.

5.7.3.1 MMT Support for CENC and EME

MMT supports common encryption through use of the SI descriptor. For more information, see ATSC A/331 [5] and ISO/IEC 23008-1 [6] subclause 10.5.5.

5.7.3.2 ROUTE/DASH Support for CENC and EME

ROUTE/DASH support for CENC may be found in [4], Section 7. Information on the interaction of ROUTE/DASH and EME is provided in Annex A.

5.8 Backend Business Systems

It is beyond the scope of this specification to define the detailed components used in the preparation of broadcast streams that carry encrypted content. DASH Guidelines for Implementations: DASH-IF Interoperability Points [8] Section 7.8 provides an overview of the logical roles and workflow of the components of a system for the exchange of content protection information.

5.9 DRM Data Service Delivery for Broadcast-Only Devices

See A/331 for specification of delivery of DRM Data Services in the broadcast emission.

Annex A: ROUTE/DASH Client Processing for Common Encryption (CENC) and Encrypted Media Extensions (EME) (Informative)

A.1 INTRODUCTION

This Annex describes the operation of a ROUTE-enabled ATSC receiver when accessing CENC-protected media.

ROUTE/DASH supports the Common Encryption (CENC) framework for multiple DRM systems to protect DASH-formatted streaming service content. ROUTE/DASH includes protection system specific and proprietary signaling information delivered in two way: a) in predetermined locations in the MPD, and b) carried inband to the DASH content, in designated metadata boxes of the ISO BMFF format for movie fragments [1], in accordance to the usage as defined in ISO/IEC 23001-7 [1]. Most of the details can be found in the DASH-IF IOP specification [7], and are compliant to the DASH-IF Broadcast IOP specification [4].

A.1.1 Basic CENC Operation in ROUTE/DASH

This section describes the basic mechanisms of how DASH-formatted streaming content, protected by a DRM system, and delivered by the ROUTE protocol, can be decrypted and played out. It describes, in the context of CENC and EME, the required interactions within the receiver and between the receiver and a license server, for license and key acquisition and subsequent content decryption and playout.

Two alternative methods are described using message/interaction flows. In the first (see Section 0), acquisition of the DRM license and content key by the CDM occurs prior to the start of the streaming program delivery. In the second method (as described in Section 0), acquisition of the DRM license and content key by the CDM occurs during the program delivery. The first method, by bootstrapping the license and key acquisition prior to the start of the broadcast program, may be preferable over the second in reducing start-up delay for playing out of DRM-protected content, although the actual gains depend on the specific service requirements and practical license acquisition latency over the broadband network.

A.1.1.1 License Acquisition Prior to Program Delivery

Figure A.1 is an example message flow illustrating the method whereby the `ContentProtection` descriptor in the MPD is used to provide the affiliated metadata, such as license server's URL and default KID to the CDM. This triggers the CDM to request and obtain the DRM license, and associated key material prior to the media delivery. When the encrypted media content is later broadcast, the receiver has the necessary decryption keys to render the content immediately.

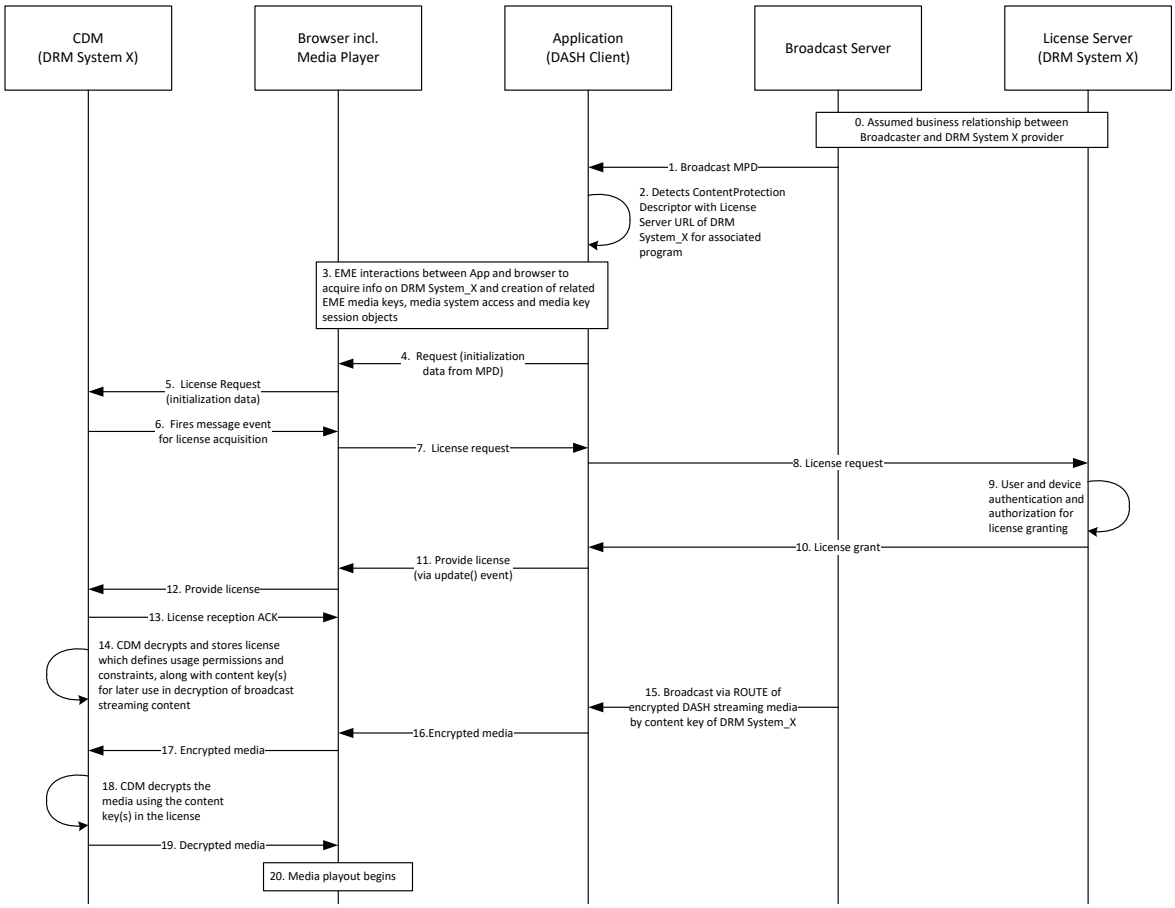

Figure A.1 DRM license and key acquisition before start of program in ROUTE/DASH.

A.1.1.2 License Acquisition During Program Delivery

Figure A.2 is an example message flow illustrating the method whereby the protection system related metadata carried in the DASH Segments, specifically the '`pssh`' box in the '`moov`' or '`moof`' box is used to provide the affiliated metadata, such as license server's URL and default KID to the CDM. During the interval that it takes for the CDM to request and obtain the DRM license, and associated key material, the program cannot be rendered. Due to the greater start-up delay associated with this method, it is suggested that the alternative method in Section 0 be employed by the broadcaster.

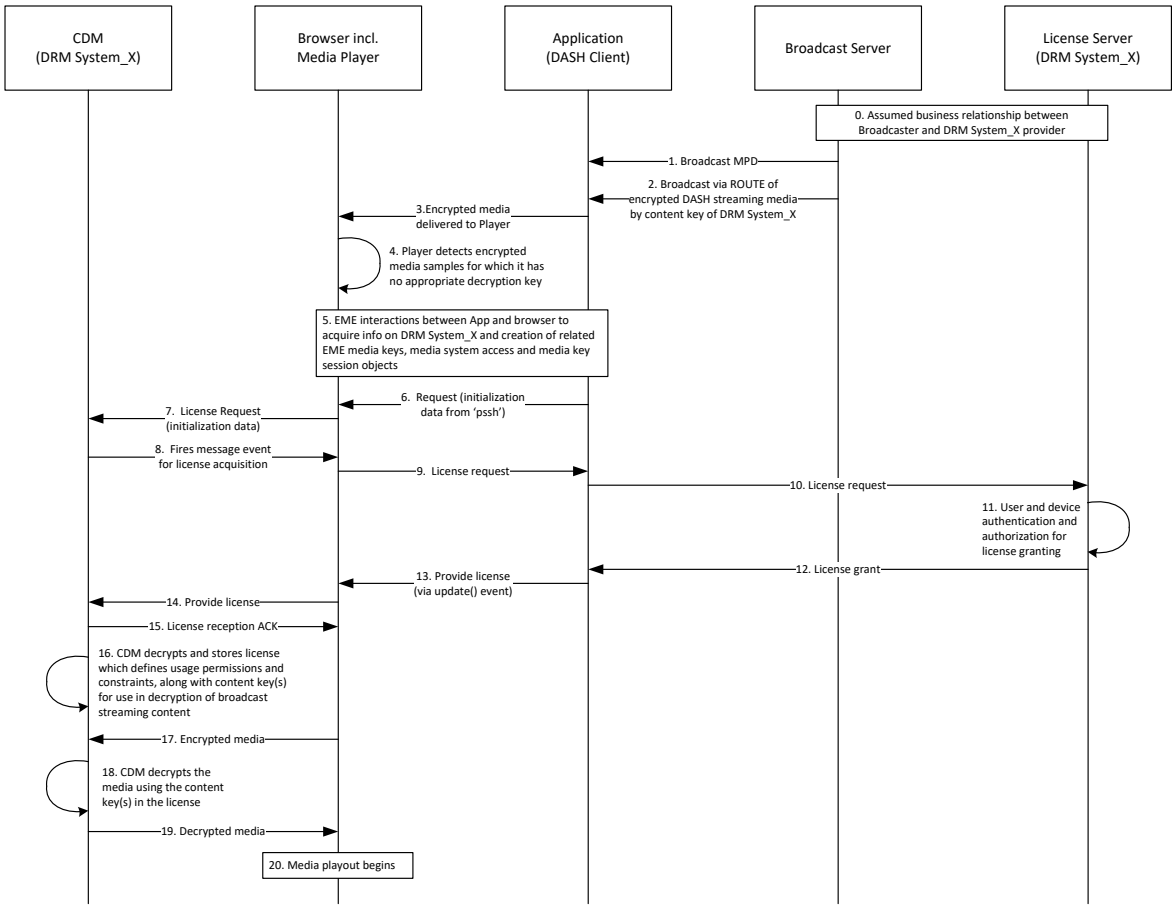

Figure A.2 DRM license and key acquisition during program delivery in ROUTE/DASH.

A.1.2 Solution Framework for DRM and CENC

ISO-IEC 23001-7 [1] represents the normative standard for common encryption in conjunction with ISO BMFF [11], and includes the following technology components used for DRM protection of streaming media carried by ROUTE/DASH:

- Common encryption of NAL structure video and other media with AES-128 CTR mode
- Support for decryption of individual Representations by one or more DRM systems
- Key rotation to enable the change of the content encryption keys over time
- Extension of the `ContentProtection` descriptor to enable the signaling of `default_KID` and '`pssh`' parameters in the MPD

The primary DRM related signaling components and tools available for use in ROUTE/DASH are as follows:

1) The `ContentProtection` descriptor in the MPD which contains the URI for signaling of the use of Common Encryption or the specific DRM scheme being used.

2) Parameters of the 'tenc' box, carried as part of protection scheme information in the movie box ('moov') of the Initialization Segment, which specify encryption parameters and default_KID. The default_KID information may also be carried out-of-band in the MPD.
3) Signaling of common encryption sample auxiliary information in the form of initialization vectors and subsample encryption ranges, if applicable, using the 'senc box as defined in ISO/IEC 23001-7 [1], or via the SampleAuxiliaryInformationSizesBox ('saiz') and a SampleAuxiliaryInformationOffsetsBox ('saio').
4) 'pssh' license acquisition data or keys for each DRM system in a format that is protection system specific. 'pssh' refers to the Protection System Specific Header box as defined in ISO/IEC 23001-7 [1], and which may be stored in the Initialization Segment or in Media Segments. It may also be present in a **cenc:pssh** element in the MPD. Note that while the presence of **cenc:pssh** information in the MPD increases the MPD size, it may allow faster parsing, earlier access, and addition of DRM systems without content modification.
5) Key rotation to enable modification over time in the entitlement for access to continuous live content. Details on how key rotation operates in the protection of broadcast DASH streaming content can be found in the DASH-IF Interoperability Points documents [7], [4] (*nb.* Section 7.5 of [7] and Section 7.4 of [7]).

A graphical representation of the box structure pertaining to encryption metadata support for video-on-demand (VoD) content is shown in Figure A.3.

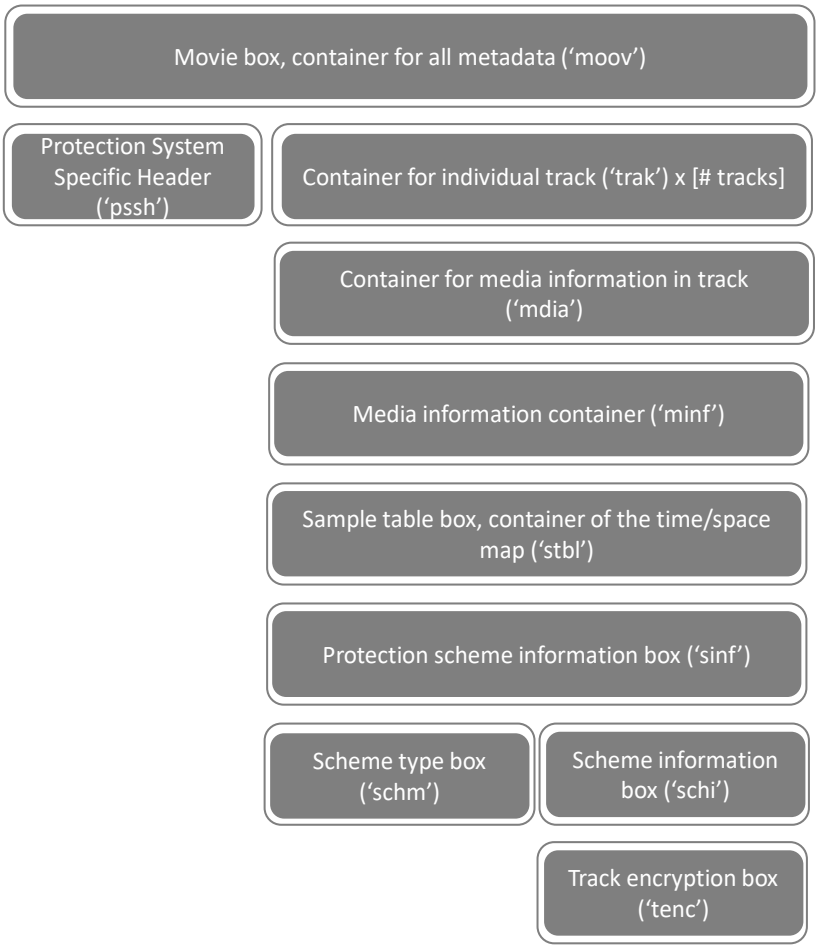

Figure A.3 CENC-related metadata structure for protection of VoD content by a single key.

A graphical representation of the box structure pertaining to encryption metadata support for live streaming content is shown in Figure A.4.

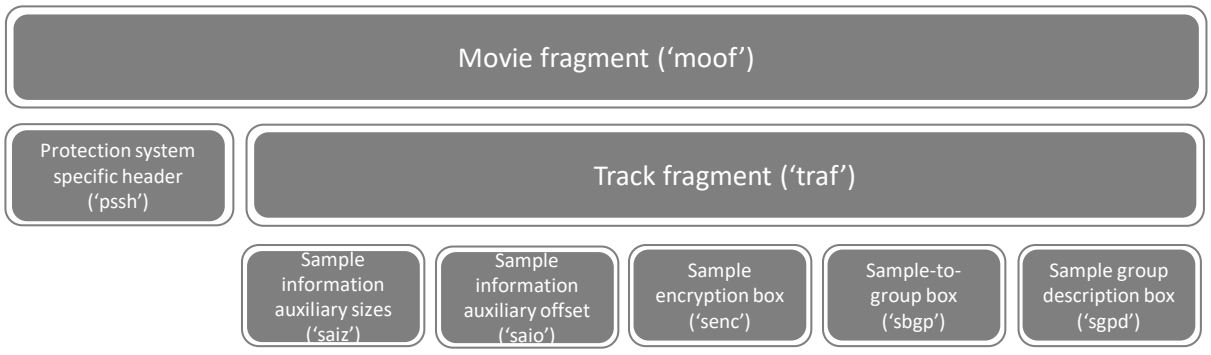

Figure A.4 CENC-related metadata structure for protection of live streaming content.

A.1.3 MPD Support for Encryption and DRM Signaling

The MPD contains signaling of the content encryption and key management methods used to enable the DRM client to determine whether it is capable to play out the content. That information is contained in the **ContentProtection** descriptor, of which at least one instance must be present in each **AdaptationSet** element describing encrypted content.

A.1.3.1 Use of the Content Protection Descriptor for mp4 Protection Scheme

As specified by MPEG-DASH [8], a **ContentProtection** descriptor with @schemeIdUri value of "urn:mpeg:dash:mp4protection:2011" indicates that the content is encrypted with the scheme as indicated in the @value attribute. The file structure of content protection schemes is specified in MPEG-DASH [8], Section 5.8.5.2, and the @value is 'cenc' in denoting the Common Encryption scheme. Such value for the @schemeIdUri of the **ContentProtection** descriptor along with @cenc:default_KID as defined within the "urn:mpeg:cenc:2013" extension namespace may be sufficient for the receiver to acquire a DRM license, or identify a previously acquired license that can be used to decrypt the Adaptation Set.

When the @cenc:default_KID is present for each Adaptation Set, it allows a player to determine if a new license needs to be acquired for each Adaptation Set by comparing their default_KIDs with each other, and with the default_KIDs of stored licenses. A player can simply compare these KID strings and determine what unique licenses are necessary without interpreting license information specific to each DRM system.

A.1.3.2 Use of Content Protection Descriptor for uuid Scheme

A UUID **ContentProtection** descriptor in the MPD may indicate the availability of a particular DRM scheme for license acquisition. An example is shown below:

```
<ContentProtection
schemeIdUri="urn:uuid:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
value="DRMNAME version"/>
```

The schemeIdUri uses a UUID URN with the UUID string equal to the registered SystemID for a particular DRM system. This is specified in MPEG DASH [8], Section 5.8.5.2. A list of known DRM System IDs can be found in the DASH identifier repository at: http://www.dashif.org/identifiers/content-protection.

A.1.3.3 Protection System Specific Header Box in the MPD

A 'pssh' box is defined by each DRM system for use with their registered SystemID, and is nominally stored in the movie box ('moov') and additionally may be present in the movie fragment box ('moof'). The same box can also be stored in the MPD within a **ContentProtection** Descriptor for a UUID scheme using the extension element **cenc:pssh** in the "urn:mpeg:cenc:2013" namespace, as defined by ISO/IEC 23001-7 [1]. Carrying the **cenc:pssh** element and also the cenc:default_KID attribute as defined by the same "urn:mpeg:cenc:2013" extension namespace, in the MPD, can be useful in supporting key identification, license evaluation, and license retrieval before the availability of Initialization Segments for live content. This enables ATSC receivers, via the broadband network, to be able to acquire license requests prior to the start of the program. Also, spreading out over time license requests avoids potential overloading of the license server due to a high volume of simultaneous license requests from many viewers, starting when at an

Initialization Segment containing license acquisition information in 'pssh' becomes available. With **cenc:default_KID** indicated in the mp4protection **ContentProtection** descriptor for each Adaptation Set, the DRM client in the receiver can determine whether

- the associated decryption key for the program is available to the viewer (e.g., without purchase or subscription),
- if the key is already downloaded, or
- which license the client may download before the @availabilityStartTime of the program, based on the default_KID of each Adaptation Set element selected.

4. INFORMATIVE TEXT FROM A/344:2017, "ATSC 3.0 INTERACTIVE CONTENT" [10]

(*begins on next page*)

Annex C: DRM API Examples

C.1 EXAMPLE USE CASE #1 – CONNECTED RECEIVER

The following use case is an example showing how the DRM APIs defined in ATSC A/344, [10] may be used by the RMP in the case that a broadcast Service uses SHVC and only the enhancement layer of spatial scalable video codec is encrypted. In this case, the Receiver has internet connectivity, and it has no pre-cached license to decrypt the enhancement layer of the Service. Figure C.1.1 describes the process.

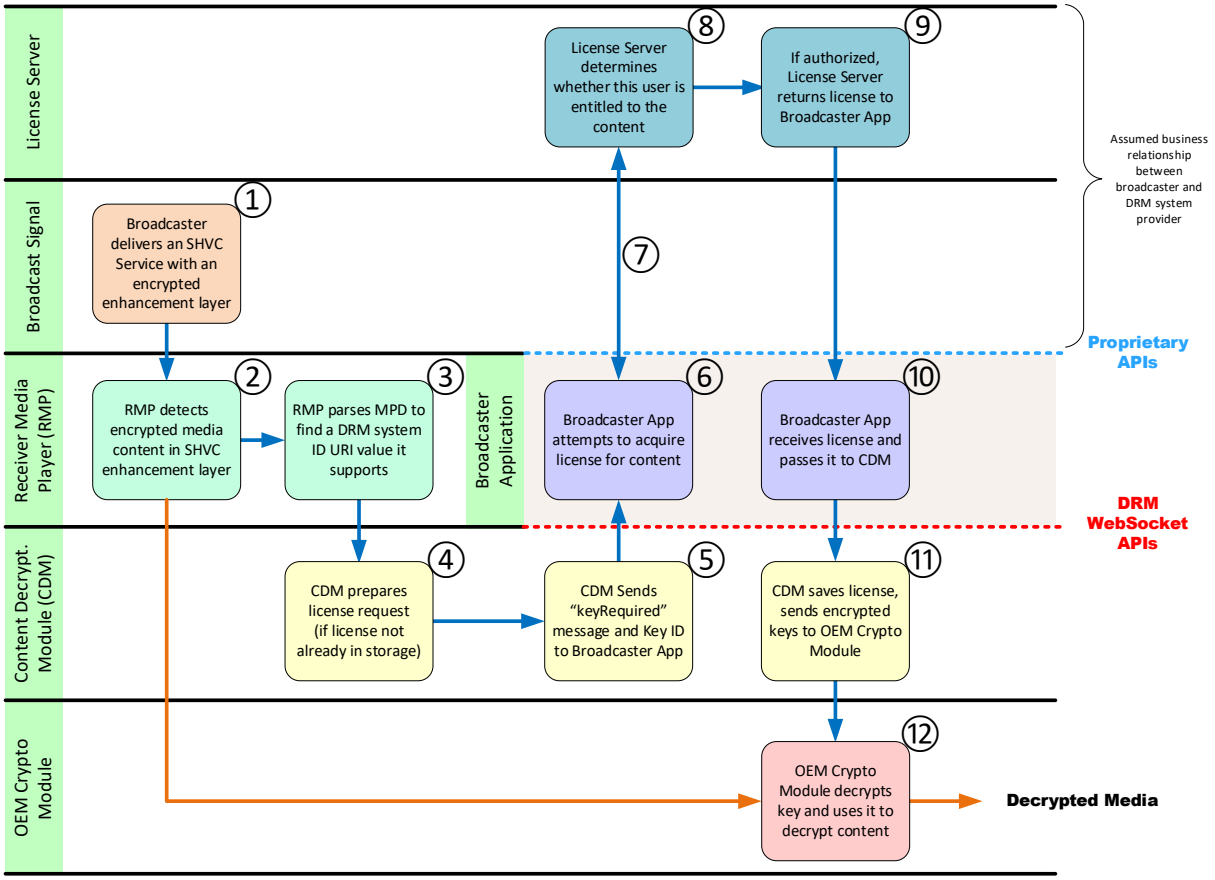

Figure C.1.1 Example use case – Connected Receiver.

1) A user selects a Service with an SHVC-encoded video component having an in-the-clear base layer and an encrypted enhancement layer. A Broadcaster Application is also present in the definition of the Service, and the Receiver downloads and executes it when the package containing it has been retrieved and validated.

2) The RMP starts playing by decoding and presenting only the base layer (HD Quality) since the enhanced layer is encrypted. The RMP discovers that the enhancement layer is encrypted.
3) The RMP parses the MPD in the Service Layer Signaling (SLS), specifically the `ContentProtection` element, to discover whether or not it lists a DRM System ID it supports. One is found, so processing continues.
4) The Content Decryption Module (CDM) in the Receiver associated with the DRM System ID checks to see whether the license key required to decrypt the enhancement layer is already in storage. In this example, the CDM determines that no pre-existing license for this content is available and prepares a license request for the key.
5) The CDM notifies the Broadcaster Application using the DRM Notification API, passing the DRM system ID and a message understood by Broadcaster Applications which support that system ID. The message in the notification would typically include the Key ID associated with this content, and a request for a license.
6) The Broadcaster Application executes a process to retrieve a license for the requested content. This process involves interaction with the user, and interaction with a Web Server operated by the broadcaster and a License Server associated with the DRM system employed.
7) Interaction between the Broadcaster Application and the License Server includes information the Broadcaster Application needs to create a user interface to present to the user. It presents the user with an option to acquire the rights to view the UHD version of the content. The user accepts and provides the necessary payment or information.
8) The License Server determines that the user is entitled to access the requested content.
9) The License Server delivers the license to the Broadcaster Application using proprietary messaging.
10) The Broadcaster Application issues the DRM Operation API with the DRM system ID and a message including the license for the content.
11) The CDM receives the license, saves it, and uses it to derive the key needed to decrypt the content, sending that key to the OEM Crypto Module.
12) The OEM Crypto Module decrypts the enhancement layer and the user enjoys watching the service in UHD video quality.

C.2 EXAMPLE USE CASE #2 — UNCONNECTED RECEIVER

The following use case is an example showing how the DRM APIs defined in A/344 [10] are used in the case that a broadcast Service is encrypted, and the Receiver does not have Internet access. In this case, the Receiver interacts with a License Server externally from the Receiver, resulting in the necessary DRM license being delivered in the broadcast emission. Figure C.2.1 describes the process.

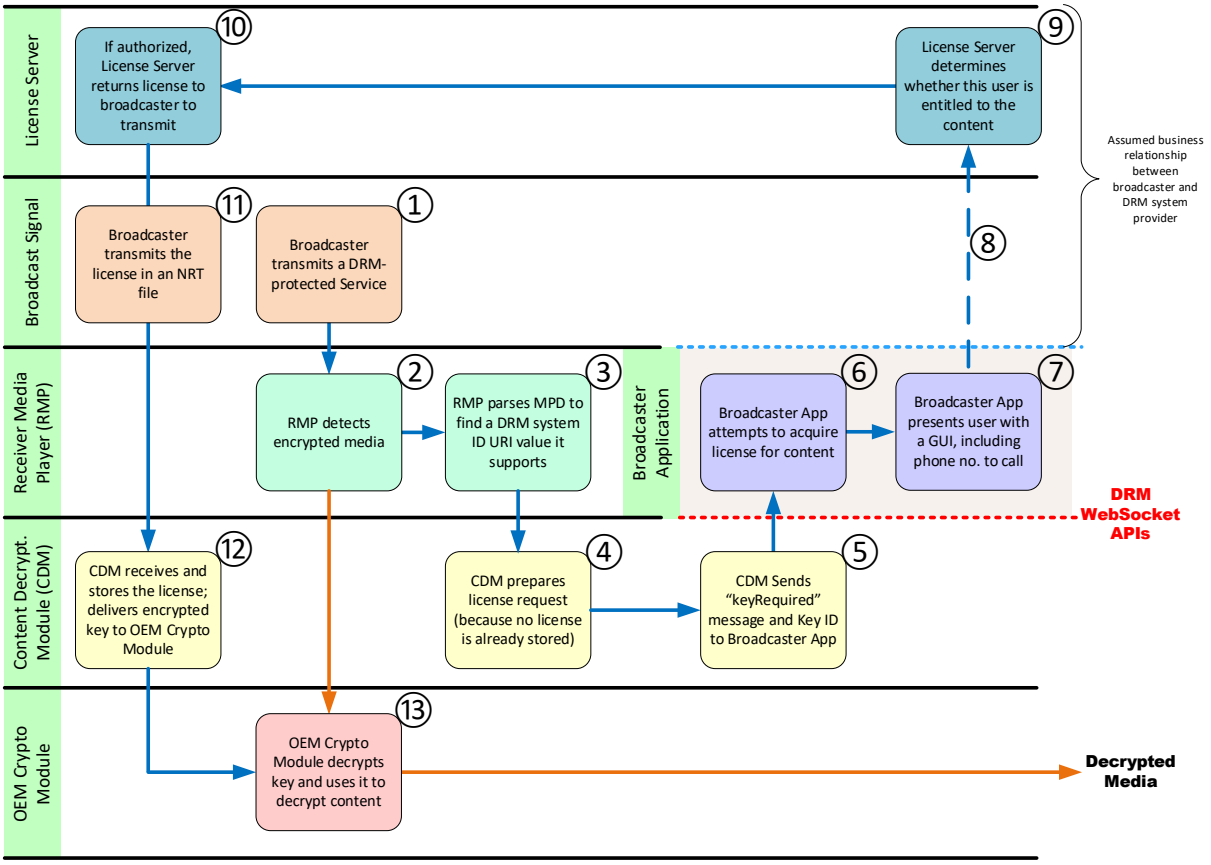

Figure C.2.1 Use case – Unconnected Receiver.

1) A user selects an encrypted Service. A Broadcaster Application is also present in the definition of the Service, and the Receiver downloads and launches it as soon as the package containing it has been retrieved and validated.
2) The Receiver acquires the Service and determines that the content is encrypted.
3) The RMP parses the MPD in the Service Layer Signaling (SLS) and discovers a DRM system it supports. The RMP interacts with the CDM to request the necessary license.
4) The CDM determines that no pre-existing license for this content is available.
5) The CDM notifies the Broadcaster Application using the DRM Notification API, passing the DRM system ID and a message understood by Broadcaster Applications which support that system ID. The message in the notification would typically include the Key ID associated with this content, and a request for a license. In this case, because there is no internet connectivity, the notification also includes information the Broadcaster Application will need to create the desired user interface: a string containing the Device ID and a string containing the telephone number the user can call to gain access to the content.
6) The Broadcaster Application attempts to acquire the license for the content.
7) The Broadcaster Application creates a user interface describing the content (synopsis, clips, stills, etc.) and informing them that to watch the content on this Service, they can call the number shown and provide the indicated information to the operator.
8) The user calls the number and interacts with a Service Provider.

9) The user fulfills the requirements for access to the content (in this case, agreeing to pay $3.99).
10) The Service Provider delivers a message to the broadcaster including the DRM license for the content for inclusion in the broadcast emission.
11) The broadcaster transmits the DRM license in the broadcast emission.
12) The Receiver receives the license and passes it to the CDM.
13) The CDM derives the key and uses it to decrypt the content, and the user begins to enjoy the content she paid for.

C.3 EXAMPLE USE CASE #3 – PRE-EXISTING LICENSE

The following use case illustrates the case that a broadcast Service is encrypted, and the Receiver has a pre-cached license to decrypt the Service. Neither the Broadcaster Application nor the DRM APIs are involved. Figure C.3.1 describes the process.

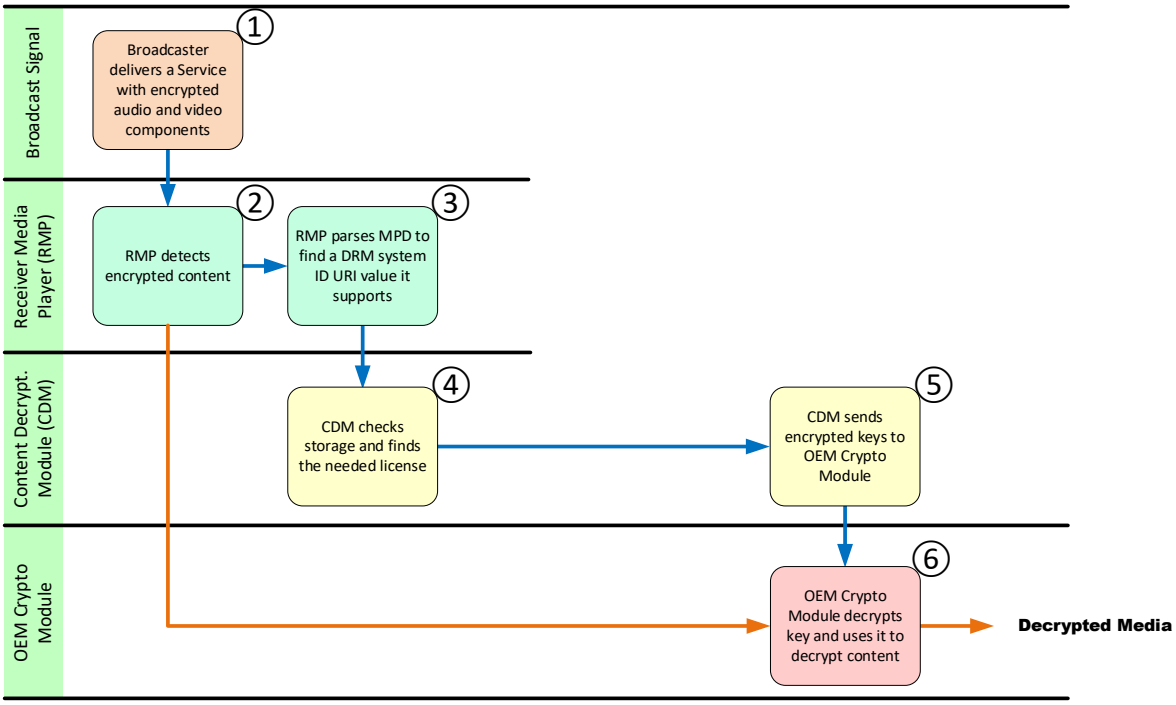

Figure C.3.1 Example use case – pre-existing license.

1) A broadcaster transmits an encrypted Service and the user selects that Service.
2) The Receiver tunes in the Service and discovers it is encrypted.
3) The RMP parses the Service Layer Signaling (SLS) to discover what DRM systems may be used to decrypt the enhancement layer. The RMP chooses the first one in the list which matches a DRM system supported by the Receiver.
4) The RMP passes information from the broadcast (for example, a `ContentProtection` descriptor from the MPD) to the CDM of the chosen DRM system. The CDM determines that a pre-existing license for this content is available.

5) The CDM retrieves the license from storage, decrypts the key needed to decrypt the content, sends it to the OEM Crypto Module which begins to render the enhanced layer. The user enjoys watching the Service.

End of Document