**3GPP TSG- Meeting #**

**, , - revision of S4-241655**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  |  |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** |  |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** |  |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | DRM and Conditional Access are commonly used by third-party streaming services. However, in case streaming is done through MBS or MBMS, a more careful management of the keys needs to be checked. Scalability of key delivery is an issue. The support for -encrypted content in Unicast/Multicast and Broadcast is relevant. Integration of Content Protection interfaces in the provisioning, for example using CPIX back-end interfaces is of high relevance for the industry and should accordingly be studied. The impacts of these on media plane (reference points M2 and M4) as well as the media session handling APIs (reference points M3, M5) should also be studied. |
|  |  |
| ***Summary of change:*** | Addresses the work item objectives for this key issue* Documents the key issue in more detail, in particular how they relate to the 3GPP Media Delivery architecture and/or the MBS User Service architecture
* Studies collaboration scenarios between the Application Service Provider and the 5G System and for each of the key topics.
* Based on existing architectures, provides one or more deployment architectures that address the key topics and the collaboration models.
* Maps the key topics to basic functions and develop high-level call flows.
* Identifies the issues that need to be solved.
* Provides candidate solutions including call flows, protocols and APIs for each of the identified issues.

Identifies gaps and recommend potential normative work for stage-2 and stage-3, including which existing specifications would be impacted and/or if any new specifications would preferably be developed. |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 5.10, 6.10 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TR 26.804 CR 0014  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** | Updated scope, references and abbreviations are in CR 0014**References**[C] ETSI TS 103 799 Content Protection Information Exchange Format (CPIX) [B] DASH-IF-IOP-Part6-v5.0.0: Content protection and security[A] ETSI TS 104 002: DASH-IF Forensic A/B Watermarking**Abbrevations**:CPIX Content Protection Information eXchange formatDRM Digital Rights ManagementThis document is submitted as basis for future work. |
|  |  |
| ***This CR's revision history:*** |

|  |  |  |  |
| --- | --- | --- | --- |
| [S4-241469](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/TSGS4_129-e/Docs/S4-241469.zip) | [FS\_AMD] DRM and Conditional Access. | Qualcomm Germany | Thomas Stockhammer |

**E-mail Discussion**:

|  |  |  |
| --- | --- | --- |
| [[8.6 FS\_AMD; 1469; 20 August 1400 CEST] CR 26.804 [FS\_AMD #05] DRM and Conditional Access -> for agreement](https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG4_MBS;a137d671.2408C&S=) | Gabin, Frederic | Mon, 19 Aug 2024 11:49:06 +0000 |
| [[8.6 FS\_AMD; 1469; 20 August 1400 CEST] CR 26.804 [FS\_AMD #05] DRM and Conditional Access -> for agreement](https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG4_MBS;7fcd83ab.2408C&S=) | Richard Bradbury | Mon, 19 Aug 2024 13:09:54 +0100 |
| [[8.6 FS\_AMD; 1469; 20 August 1400 CEST] CR 26.804 [FS\_AMD #05] DRM and Conditional Access -> for agreement](https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG4_MBS;d9d59ae2.2408C&S=) | Thomas Stockhammer | Tue, 20 Aug 2024 11:05:24 +0000 |
| [[8.6 FS\_AMD; 1469; 20 August 1400 CEST] CR 26.804 [FS\_AMD #05] DRM and Conditional Access -> for agreement](https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG4_MBS;5ca304a.2408C&S=) | Rufael Mekuria | Tue, 20 Aug 2024 12:02:27 +0000 |
| [[8.6 FS\_AMD; 1469; 20 August 1400 CEST] CR 26.804 [FS\_AMD #05] DRM and Conditional Access -> for agreement](https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG4_MBS;66c8406a.2408C&S=) | Thomas Stockhammer | Tue, 20 Aug 2024 12:04:40 +0000 |
| [[8.6 FS\_AMD; 1469; 20 August 1400 CEST] CR 26.804 [FS\_AMD #05] DRM and Conditional Access -> for agreement](https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG4_MBS;6d9e081b.2408C&S=) | Rufael Mekuria | Tue, 20 Aug 2024 12:26:39 +0000 |
| [[8.6 FS\_AMD; 1469; 20 August 1400 CEST] CR 26.804 [FS\_AMD #05] DRM and Conditional Access -> for agreement](https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG4_MBS;34f920d3.2408C&S=) | Gabin, Frederic | Tue, 20 Aug 2024 12:31:49 +0000 |

**Revisions**:

|  |  |  |
| --- | --- | --- |
| [S4-241469\_BBC.docx](https://www.3gpp.org/ftp/tsg_sa/WG4_CODEC/TSGS4_129-e/Inbox/Drafts/MBS/S4-241469_BBC.docx) | 8/15/2024 15:19 | 360,5 KB |
| [S4-241469-26804-0016rev2-DRM\_huawei.docx](https://www.3gpp.org/ftp/tsg_sa/WG4_CODEC/TSGS4_129-e/Inbox/Drafts/MBS/S4-241469-26804-0016rev2-DRM_huawei.docx) | 8/20/2024 12:26 | 353,1 KB |
| [S4-241469r01.docx](https://www.3gpp.org/ftp/tsg_sa/WG4_CODEC/TSGS4_129-e/Inbox/Drafts/MBS/S4-241469r01.docx) | 8/20/2024 11:05 | 356,7 KB |

**Presenter**: Thomas Stockhammer**Online Discussion**:* r01 version presented.
* Thomas: This is a revision based on comments from Richard. I believe I addressed all of those.

**Decision**: Revised. The revision will be endorsed without presentation.[S4-241469](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/TSGS4_129-e/Docs/S4-241469.zip) is **revised to S4-241655**.This revision is provided as basis for future work and submitted for endorsement. |

## ===== 2 . Change ==========

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

…

[104] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[MovieLab] Movie labs Specification for Enchanced Content Protection

Available at: <https://movielabs.com/ngvideo/MovieLabs_ECP_v1.4.pdf>.

[W3C EME] W3C Encrypted Media Extensions

Available at: https://www.w3.org/TR/encrypted-media-2/

## ===== CHANGE =====

## 5.10 Support for DRM protected, encrypted and high-value content

### 5.10.1 Description

Content is increasingly encrypted for distribution for different reasons, e.g. Content Protection, Conditional Access, or integrity of playback. The management of keys for different use cases is a prime concern. Examples include scalable access to keys, secure storage of keys, key availabilities. It is envisioned that an MNO can provide key management and/or key distribution services for content providers. In particular, providing scalable and secure key management within 5GMS for multiple different devices needs further study.

Examples for secure media requirements are for example provided by the MovieLabs ECP [MovieLab] specification and other content providers requirements.In a specific example, a live sports service provider wants to offer a live stream. Examples include where the content needs to be delivered with low latency (typically encoder to glass in 3–10 seconds) in order to be on par with regular TV distribution means, and wether it is made available for replay and seeking in a certain time window. Other services may also be considered.

The service may require different tools and functionalities levels of security:

1. *Conditional access supported by DRM management.* As an example, users need to get a key for decrypting the secondary level keys to support key rotations.

2. *Key rotation.* As an example, these keys are changed periodically but protected by the master key.

3. multi-*DRM and multi-key management* to ensure playback rules, for example to avoid that clients attempting early playback of the content too early and have advantages in betting/wagering, skipping content, etc. In many cases multiple DRM Systems need to be supported to target different devices types. In addition multi-key can enable distinct keys to support different qualities such as UHD and HD which is a common industry requirement.

4. *Watermarking.* The content is distributed and a unique signature is added at the latest possible time (in the device, at the Edge). An example of such approach can be found here <https://learn.akamai.com/en-us/webhelp/adaptive-media-delivery/adaptive-media-delivery-implementation-guide/GUID-3F89E64C-415D-452D-9541-BB650CD783B9.html>.

5. *Content encryption.* This makes sure content cannot be used by users that are not in possession of the key. The encryption is usually applied on the content when packaging or encoding the content.

6. *A secure implementation* (use of TEE, Secure Media Path).

In addition, DASH-IF has defined workflows for managing protected content as follows:

- Content Protection Information Exchange Format (CPIX) as specified in ETSI TS 103 799 [C].

- DASH-IF Interoperability Points; Part6-v5.0.0: Content protection and security [B].

- DASH-IF Forensic A/B Watermarking as specified in ETSI TS 104 002 [A].

Integration of Content Protection interfaces in the provisioning, for example using CPIX back-end interfaces, is of high relevance for the industry and should accordingly be studied. The impacts of these on the media plane (reference points M2 and M4) as well as on the media session handling APIs (reference points M3, M5) should also be studied.

In addition, W3C has developed the encrypted media extensions, enabling browser platforms to support secure encrypted media playback using different DRM solutions [W3C EME].

### 5.10.2 Collaboration scenarios

It is assumed that the content provider provides DRM protections for the content. However, beyond this different collaboration models between the content provider and 5G System operator/MNO exist.

As examples, the MNO provides infrastructure to the content service provider in order to support security related functions.

- The service provider may want to provide scalable access to the content and in particular the key distribution. Hence it uses 5G Media streaming servers to support secure key distribution.

- The streaming service provider wants to rule playback, for example to avoid that the situation whereby users can see the streamed content too early while at the same time, the streaming service provider does not want to delay the distribution artificially either and want to give the clients the ability to download the main content (without buffer underruns).

- The service provider asks for fairness in the client, but the client cannot be trusted to act fairly. Hacked clients are possible. Clients may have DRM systems that the service providers will use.

- The service provider asks for a watermarking solution from the MNO.

Encryption (as already defined in TS 26.511 [96]) and secure keys may be used for other purposes, for example for conditional access or DRM systems. In some cases, keys are also provided in hierarchically, depending on business rules, security levels and deployment scenarios.

In an extension of the above use case, the content is distributed via multiple operators network. In this case, the encryption may be done by the service provider and the service provider provides the keys to the MNO. In another case, the service is offered by the MNO and the MNO does encryption and key management. In another context, DRM-protected encrypted content may also be distributed when using 5G Media Streaming over MBMS or MBS as documented in clauses 4.6 and 4.9 respectively in TS 26.501 [26501].

### 5.10.3 Deployment architectures

The core components of a DRM workflow are provided in figure 5.10.3-1 based on DASH-IF-IOP-Part5-v5.0.0 [B]. Similar work flows apply also for other streaming technologies but DASH is used for the analysis.



Figure 5.10.3-1: Core elements in content protection according to DASH-IF-IOP-Part5-v5.0.0 [B]

The definition of the functions is as follows:

- **Authorization Server**: provides authorization tokens that may be required for requesting a license from a license server.

- **DASH client**: a function using the Media platform and the DRM system to playback encrypted content.

- **DASH Presentation**: A server hosting DASH resources, i.e. MPDs and Segments primarily, and includes information on the used DRM System.

- **License Server**: A license server provides licenses that are data structures in a DRM system specific format that contains one or more content keys and associates them with a policy that governs the usage of the content keys (e.g. expiration time).

- **Media Platform**: enables playback of encrypted content while protecting the decrypted samples and content keys against potential attacks

- **DRM System**: an implementation of content keys management cooperating with the device’s media platform to enable playback of encrypted content while protecting the decrypted samples and content keys against potential attacks, consisting of two main components: a license server and a DRM client.

- **DRM Client:** processes licenses and enforcing the associated policies. Either the DRM client handles the decryption of samples, or the DRM client interacts with the hardware elements that address the decryption.

A DRM system cooperates with the device’s media platform to enable playback of encrypted content while protecting the decrypted samples and content keys against potential attacks. The same encrypted DASH presentation can be decrypted by different DRM systems if a DASH client is provided the DRM system configuration for each DRM system, either in the MPD or at runtime. A content key is a key used by a DRM system to make content available for playback. A content key and its identifier can be shared between all DRM systems, whereas the mechanisms used for key acquisition and content protection are largely DRM system specific. DASH adaptation sets are often protected by different content keys. The encapsulated content keys are typically encrypted and only readable by the DRM system. A more detailed DRM workflow is provided in Figure 5.10.3-2 based on ETSI TS 103 799 [C] on Content Protection Information Exchange Format (CPIX). It complements DASH-IF-IOP-Part6 [B] by putting more emphasis on the back-end aspects. The following additional functions are defined:

- **Content Provider**: A publisher who provides the rights and rules for delivering protected media, also possibly source media (mezzanine format, for transcoding), asset identifiers, key identifiers (KID), content key values, encoding instructions, and content description metadata.

- **Encoder**: A function that encodes media in a specified set of formats with different bitrates and resolutions etc., possibly determined by the publisher.

- **Packager / Encryptor**: A function that who encrypts and packages media, inserting DRM Signaling and metadata into the media files.

- **Manifest Creator**: A function that generates the media manifests which group the various media files into a coherent presentation. These manifest files may contain DRM signaling information.

- **DRM Client**: It gets information from different sources: media manifest files, media files, and DRM licenses.

An example architecture is provided in figure 5.10.3-2.



Figure 5.10.3-2: Example backend architecture and workflow for encrypted live content
based on ETSI TS 103 799 [C]

In this case, content is continuously received, transcoded in the desired format and encrypted if any type of protectionis required. One or multiple content keys can be used regardless if key rotation is used or not. Keys are generated by the encryption engine or the DRM system and are available to all DRM systems and the encryption engines to support multi DRM with a shared key. The MPD Generator requests to the DRM systems their specific signalling, if any, to be added in the MPD. Encrypted segments and the media manifest can be uploaded on a CDN making it available to users.

Figure 5.10.3-3 illustrates the usage of the encrypted content in a realistic workflow comprising multiple cooperating components. In ETSI TS 103 799 [C], a standardised data format for content protection information exchange is defined, collected in a document that can be signed.



Figure 5.10.3-3 Incremental update and extension of the document based on ETSI TS 103 799 [C]

Also, in ETSI TS 103 799 [C] a workflow is presented for which multiple producers are included. This workflow is shown in figure 5.10.3-4.



Figure 5.10.3-4: Multiple producer example steps based on ETSI TS 103 799 [C]

A typical example workflow of encrypted content is shown in figure 5.10.3-5.



Figure 5.10.3-5 Typical workflow for generating, distributing and playing back encrypted content

The following call flow is provided:

*Initialization:*

1. The Encryptor/Packager (ENP), License Server (LS), and Authorization Server (AUS) exchange public keys.

*Content Protection Information construction:*

2. The Packager constructs content protection information.

3. The Encryptor encrypts keys and adds them to the content protection information.

*Content Protection Information distribution:*

4. The Encryptor/Packager sends the content protection information to the Authorization Server.

5. The Authorization Server decrypts the keys and adds data to the content protection information.

6. The Authorization Server sends the updated content protection information to the License Server.

7. The License Server decrypts the keys and adds data to the content protection information.

8. The License Server sends the updated content protection information to the Encryptor/Packager and the Manifest Creator.

*Presentation manifest and segment generation:*

9. The Manifest Creator generates the presentation manifest (e.g. DASH MPD) and adds the content protection information.

10. The Manifest Creator uploads the presentation manifest to the Content Hosting.

11. The Encryptor/Packager generates encrypted segments and adds the content protection information.

12. The Manifest Creator uploads the encrypted segments to the Content Hosting.

*Client requests and authorisation:*

13. The DASH Client requests the presentation manifest from the Content Hosting.

14. The DASH Client requests authorisation tokens from the Authorization Server.

15. The DASH Client requests a license from the License Server, possibly using the authorisation tokens.

16. The DASH Client provides the license to the DRM Client.

*Content delivery and decryption:*

17. The DASH Client requests encrypted segments from the Content Hosting.

18. The DASH Client provides the encrypted segments to the Media Platform.

19. The Media Platform provides the encrypted samples to the DRM Client.

20. The DRM System decrypts the samples using the license and content keys.

21. The DRM System provides the decrypted samples to the Media Platform.

### 5.10.4 Mapping to 5G Media Streaming and High-Level Call Flows

Based on the Media Delivery architecture as reproduced in figure 5.15.1-1, different mapping options of the components of the above DRM architecture to the Media Delivery architecture are provided in table 5.10.4-1.



Figure 5.10.4-1 Media Delivery architecture as defined in figure 4.1.2.2-1 of TS 26.501 [15]

NOTE: As this only deals with 5GMS downlink streaming, figure 4.2.1-2 from TS 26.501 and use "5GMSd" instead of "Media" throughout may be applicable as well.

Table 5.10.4-1 provides different deployment options on how the DRM network functions are mapped to the Media Delivery functions.

Table 5.10.4-1 Possible deployment options to map DRM network functions
to Media delivery functions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DRM Function | Media Application Provider | Media AS | Media AF | Media Access Function | Media Session Handler |
| Authorization Server | 1, 3, 4 | 2 | 5, 6 |  |  |
| License Server | 1, 3, 4 | 2 | 5, 6 |  |  |
| Encoder | 1, 4, 6 | 2, 3, 5 |  |  |  |
| Encryptor/packager | 1, 4, 6 | 2, 3, 5 |  |  |  |
| Manifest Creator | 1, 6 | 2, 3, 4, 5 |  |  |  |
| Content Hosting |  | 1, 2, 3, 5, 6 |  |  |  |
| DRM Client |  |  |  | 1, 2, 3, 4, 5, 6 |  |
| DASH Client |  |  |  | 1, 2, 3, 4, 5, 6 |  |
| Media Platform |  |  |  | 1, 2, 3, 4, 5, 6 |  |

The following different deployment options are discussed:

Option 1: The Media Application Provider runs all DRM and packaging related functions, and the Media AS only caches the DASH Presentation as a CDN. For DRM acquisition, the UE contacts the Media Application Provider.

Option 2: The Media Delivery System runs a DRM and packaging service, including a License Server, on the Media AS. Content is ingested by the Media AS and all functions of licence hosting, content encoding, content encryption and so on run in the Media AS.

Option 3: The Media Delivery System runs a content encoding and packaging service, but the License Server is external in the Media Application Provider. The Media AS needs to communicate with the License Server for content encoding and packaging.

Option 4: The Media Delivery System generates the presentation manifest, but content encoding, content packaging and content encryption are external in the Media Application Provider. The Media AS needs to acquire relevant information for presentation manifest generation.

Option 5: This is similar to option 2 but, being quite specific in operation, the License Server is handed to the Media AF to sit alongside the Authorization Server. The main communication is between Media AS and Media AF at reference point M3.

Option 6: This is similar to option 5, but only the License Server is offered by the Media Delivery Service, hosted in the Media AF. Similar to option 4, content encoding, content packaging and content encryption are external in the Media Application Provider. The main communication is between the Media Application Provider and the Media AF at reference point M1 for the exchange of Cotnent Protection Information.

Based on current deployments, licence acquisition is a user plane communication and no APIs in the media access client exist to delegate the licence acquisition to a third-party function, such as the Media Access Function (e.g. Media Player). Hence, option 5 and 6 are not further discussed.

Now for the different options 1-4, table 5.10.4-2 maps the steps in figure 5.10.3-5 to components and/or interfaces defined in the media delivery architecture as shown in figure 5.10.4-1.

. i.e. DRM is external. Other options address the internalization of certain DRM-related functions.

Table 5.10.4-2: Mapping of steps in Figure 5.10.3-5 to components and/or interfaces defined in the media delivery architecture as shown in Figure 5.10.4-1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Steps | Option 1(External DRM and packaging) | Option 2(Internal DRM and packaging) | Option 3(Internal packaging, external DRM) | Option 4(only manifest internal) |
| 1 | Media AP | Media AS | M2 (CPI) | Media AP |
| 2 | Media AP | Media AS | Media AP | Media AP |
| 3 | Media AP | Media AS | Media AP | Media AP |
| 4 | Media AP | Media AS | Media AP | Media AP |
| 5 | Media AP | Media AS | Media AP | Media AP |
| 6 | Media AP | Media AS | Media AP | Media AP |
| 7 | Media AP | Media AS | Media AP | Media AP |
| 8 | Media AP | Media AS | M2 (CPI) | M2 (CPI) |
| 9 | Media AP | Media AS | Media AS | Media AS |
| 10 | M2 (Ingest) | Media AS | Media AS | Media AS |
| 11 | Media AP | Media AS | Media AS | Media AP |
| 12 | M2 (Ingest) | Media AS | Media AS | M2 (Ingest) |
| 13 | M4 | M4 | M4 | M4 |
| 14 | M8 | M4 | M8 | M8 |
| 15 | M8 | M4 | M8 | M8 |
| 16 | Media Access Fn | Media Access Fn | Media Access Fn | Media Access Fn |
| 17 | M4 | M4 | M4 | M4 |
| 18 | Media Access Fn | Media Access Fn | Media Access Fn | Media Access Fn |
| 19 | Media Access Fn | Media Access Fn | Media Access Fn | Media Access Fn |
| 20 | Media Access Fn | Media Access Fn | Media Access Fn | Media Access Fn |
| 21 | Media Access Fn | Media Access Fn | Media Access Fn | Media Access Fn |

Of the options documented in Table 5.10.4-2, obviously option 1 is most prominent as it is the default option in Rel-18. Of the remaining options, in particular option 3 is expected to be of interest for 5G Media Streaming deployments, as it addresses the scenario for which a specific encoding or transcoding for 5G Media Streaming is carried out by the Application Server. Option 4 is a subset of option 3, and hence not discussed explicitly. We also exclude option 2 for now, as DRM servers are generally handled outside MNO networks.

Editor’s Note: The mapping to 5GMS via MBS/MBMS is for further study

### 5.10.5 Potential open issues

would be Based on the discussion in clause 5.10.4, option 3 is considered in more details and the following open issues are identified:

1. Support for public key exchange between the Encryptor/Packager (ENP) on the Media AS as well as the external License Server (LS), and Authorization Server (AUS) via M2.

2. Support for the delivery of updated content protection information from an external to the Encryptor/Packager and the Manifest Creator on the Media AS via M2.

3. The delivery of content protection related information in the manifest and the content via M4.

4. Explicit support for encrypted sample entries ‘encv’ etc, in TS 26 511 to support encrypted media formats

### 5.10.6 Candidate Solutions

In order to support the open issues 1 and 2 in clause 5.10.5, the support for Content Protection Information Exchange Format (CPIX) as specified in ETSI TS 103 799 [C] on interface M2 addresses the issue.

In order to support the open issue 3 in clause 5.10.5, the support for the DASH-IF Interoperability Points; Part6-v5.0.0: Content protection and security [B] on interface M4 addresses the issue for both, DASH and HLS.

## ===== CHANGE =====

## 6.10 Support for encrypted and high-value content

Based on the considerations in clause 5.10, it is recommended to:

- support for Content Protection Information Exchange Format (CPIX) as specified in ETSI TS 103 799 [C] on interface M2 and provide the necessary extensions in stage-2 and stage-3.

- support for the DASH-IF Interoperability Points; Part6-v5.0.0: Content protection and security [B] on interface M4 to address the issue for both, DASH and HLS and provide the necessary extensions in stage-2 and stage-3.