**3GPP TSG-SA4 Meeting #130 *S4-241883***

**Orlando, United States, 18th Nov 2024 - 22nd Nov 2024 revision of S4aI240188**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **26.804** | **CR** | **0016** | **rev** | **6** | **Current version:** | **18.1.0** |  |
|  |
| *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:***  | [FS\_AMD] DRM and Conditional Access. |
|  |  |
| ***Source to WG:*** | Qualcomm Germany |
| ***Source to TSG:*** |  |
|  |  |
| ***Work item code:*** | FS\_AMD |  | ***Date:*** | 2024-11-11 |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***Release:*** | Rel-19 |
|  | *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:*** | 2, 5.10, 6.10 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TR 26.804 CR 0014 |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  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, but expected to be completed during this meeting. |
|  |  |
| ***This CR's revision history:*** |

|  |  |  |  |
| --- | --- | --- | --- |
| [**S4aI240152**](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Docs/S4aI240152.zip) | [FS\_AMD] DRM and Conditional Access. | Qualcomm Germany | Thomas Stockhammer |

**E-mail Discussion**:

|  |  |  |
| --- | --- | --- |
| [240152 DRM & conditional access](https://list.etsi.org/scripts/wa.exe?A2=3GPP_TSG_SA_WG4_MBS;dc104126.2410C&S=) | Rufael Mekuria | Tue, 15 Oct 2024 11:38:05 +0000 |

**Revisions**:

|  |  |  |
| --- | --- | --- |
| [S4aI240152-26804-0016rev4-DRM\_huawei.docx](https://www.3gpp.org/ftp/tsg_sa/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Inbox/Drafts/S4aI240152-26804-0016rev4-DRM_huawei.docx) | 2024/10/15 11:33 | 356 KB |
| [S4aI240152r01-26804-0016rev4-DRM.docx](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Inbox/Drafts/S4aI240152r01-26804-0016rev4-DRM.docx) | 2024/10/18 12:51 |  |

**Presenter**: Thomas Stockhammer**Online Discussion**: October 18, 2024* Thomas presents [\_huawei](https://www.3gpp.org/ftp/tsg_sa/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Inbox/Drafts/S4aI240152-26804-0016rev4-DRM_huawei.docx)
	+ Comments acceptable
	+ We getting towards a solution

**Decision**:* October 18, 2024: huawei version acceptable with small online edits as basis for future work. Needs a revision. Revision is endorsed.

[S4aI240152](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Docs/S4aI240152.zip) is **revised** to [S4aI240188](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Docs/S4aI240188.zip).

|  |  |  |  |
| --- | --- | --- | --- |
| [S4aI240188](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Docs/S4aI240188.zip) | [FS\_AMD] DRM and Conditional Access. | Qualcomm Germany | Thomas Stockhammer |

 [S4aI240188](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Docs/S4aI240188.zip)  is **endorsed.**This document addresses comments received from BBC here <https://www.3gpp.org/ftp/tsg_sa/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Inbox/Drafts/S4aI240188_BBC.docx> and Aside from adding missing references and fixing editorial nits, the substantive point is that I think the architectural mapping and call flows in clause 5.10.4 should be couched in terms of **downlink media streaming** specifically since that is the focus of this Key Issue. I don't think there is much point in generalising it further at this point.<https://www.3gpp.org/ftp/tsg_sa/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Inbox/Drafts/S4aI240188_BBC.docx>An additional question: the **candidate solution** in clause 5.10.6 suggests the use of **CPIX** at reference point M2d and the use of the **DASH-IF Part 6 Interoperability Points** at reference point M4d to support content hosting scenarios where the 5GMSd AS needs to re-encrypt content (because it needs to perform content preparation requiring access to the content in unencrypted form). But there is no mention of how the necessary decryption/re-encryption tasks would be configured in the 5GMSd AS via reference point M3d. I'm assuming this would be just a couple of extra steps in the content preparation pipeline description. Isn't there a significant specification gap here too that would need to be addressed by SA4? Shouldn't this Key Issue propose a candidate solution for this aspect too? |

# ===== 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".

[MovieLabs‑ECP] 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/

[Akamai-AMDIG] Akamai: "Welcome to Adaptive Media Delivery", in *Adaptive Media Delivery Implementation Guide*, available at: <https://learn.akamai.com/en-us/webhelp/adaptive-media-delivery/adaptive-media-delivery-implementation-guide/GUID-3F89E64C-415D-452D-9541-BB650CD783B9.html>

[C] ETSI TS 103 799: "Content Protection Information Exchange Format (CPIX)".

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

[A] ETSI  TS 104 002: "DASH-IF Forensic A/B Watermarking".

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

## 5.10 Support for distributing 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 ofof secure media requirements are, for example, capturedcaptured in the MovieLabs ECP specificationspecification [MovieLabs‑ECP] and elsewhere by other content providers. 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, to support key rotation, users need to get a master key for decrypting the secondary level keys.

2. *Key rotation.* As an example, contentcontent decryption 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 device 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 in [Akamai-AMDIG].

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

6. *A secure implementation.* The client implements a Trusted Execution Environment (TEE), such as 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 API [W3C-EME], enabling browser platforms to support secure encrypted media playback using different DRM solutions.

### 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.

- The service provider want the 5GMS to do re-encryption as part of content preparation feature.

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 [15].

### 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-6Part6-v5.0.0 [B]. Similar workflows apply also for other streaming technologies, but DASH is used inin the below analysis for illustrative purposes.



Figure 5.10.3-1: Core elements in content protection according to DASH-IF-IOP-6Part6-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 bebe 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.

AA more detailed DRM workflow is provided in figure 5.10.3-2 based on the Content Protection Information Exchange Format (CPIX) as specified in ETSI TS 103 799 [C]. It complements Part 6 of the DASH-IF Interoperability Points specification [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 of whether 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 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 for use with CPIX 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 retrieves 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 downlinkmsdownlink media streaming and high-level call flows

Based on the generalised Media Delivery architecture from TS 26.501 [15], as reproduced in figure 5.15.1-1 below, different mapping options of the components of the above DRM architecture to the downlinkdownlink media streaming architecture are provided in table 5.10.4-1.



NOTE SinceNOTE: Since this Key IssueIssue deals only with downlink media streaming, figure 4.2.1-2 from TS 26.501 may be applicable as well, withwith "5GMSd" instead of "Media" throughout.

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

Table 5.10.4-1 provides different deployment options on how the DRM network functions are mapped to the downlinkdownlink media streaming functions.

Table 5.10.4-1 Possible deployment options to map DRM network functions
to downlinkdownlink media streaming functions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DRM Function | 5GMSd5GMSd Application Provider | 5GMSd5GMSd AS | 5GMSd5GMSd AF | Media PlayerPlayer | 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 5GMSd Application Provider runs all DRM and packaging related functions, and the 5GMSd AS only caches the DASH Presentation as a CDN. For DRM acquisition, the UE contacts the 5GMSd Application Provider.

NOTE: This option corresponds to downlink media streaming in Release 18 in which DRM is external to the 5GMSd AS. Other options address the internalization of certain DRM-related functions.

Option 2: The 5GMSd5GMSd System runs a DRM and packaging service, including a License Server, on the 5GMSd AS. Content is ingested by the 5GMSd AS and all functions of licence hosting, content encoding, content encryption and so on run in the 5GMSd AS.

Option 3: The 5GMSd System runs a content encoding and packaging service, but the License Server is external in the 5GMSd Application Provider. The 5GMSd AS needs to communicate with the License Server for content encoding and packaging.

Option 4: The 5GMSd System generates the presentation manifest, but content encoding, content packaging and content encryption are external in the 5GMSd Application Provider. The 5GMSd 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 5GMSd AF alongside the Authorization Server. The main communication is between 5GMSd AS and 5GMSd AF at reference point M3d.

Option 6: This is similar to option 5, but only the License Server is offered by the 5GMSd System, hosted in the 5GMSd 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 5GMSd Provider and the 5GMsd AF at reference point M1d for the exchange of Content 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.

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 | 5GMSd AP | 5GMSd AS | M2d (CPI) | 5GMSd AP |
| 2 | 5GMSd AP | 5GMSd AS | 5GMSd AP | 5GMSd AP |
| 3 | 5GMSd AP | 5GMSd AS | 5GMSd AP | 5GMSd AP |
| 4 | 5GMSd AP | 5GMSd AS | 5GMSd AP | 5GMSd AP |
| 5 | 5GMSd AP | 5GMSd AS | 5GMSd AP | 5GMSd AP |
| 6 | 5GMSd AP | 5GMSd AS | 5GMSd AP | 5GMSd AP |
| 7 | 5GMSd AP | 5GMSd AS | 5GMSd AP | 5GMSd AP |
| 8 | 5GMSd AP | 5GMSd AS | M2d (CPI) | M2d (CPI) |
| 9 | 5GMSd AP | 5GMSd AS | 5GMSd AS | 5GMSd AS |
| 10 | M2 (Ingest) | 5GMSd AS | 5GMSd AS | 5GMSd AS |
| 11 | 5GMSd AP | 5GMSd AS | 5GMSd AS | 5GMSd AP |
| 12 | M2 (Ingest) | 5GMSd AS | 5GMSd AS | M2d (ingest) |
| 13 | M4d | M4d | M4d | M4d |
| 14 | M8d | M4d | M8d | M8d |
| 15 | M8d | M4d | M8d | M8d |
| 16 | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer |
| 17 | M4d | M4d | M4d | M4d |
| 18 | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer |
| 19 | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer |
| 20 | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer |
| 21 | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer | Media PlayerPlayer |

Of the options documented in table 5.10.4-2, Option 1 is most prominent because it is the default option for downlink media streaming in Release 18. Of the remaining options:

- In particular Option 3 is expected to be of interest for 5G Media Streaming deployments, because 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.

NOTE: The mapping to 5GMS via MBS/MBMS is for further study

### 5.10.5 Potential open issues

Based on the analysis in table 5.10.4-2, for different deployment options, functional updates to the 5GMSd AS and Media Player would be needed, and additional information may be exchanged through reference points M2d, M4d and M8d. Based on the discussion in clause 5.10.4, Option 3 is considered in more detail, and the following open issues are identified:

1. Support for public key exchange between the Encryptor/Packager (ENP) on the 5GMSd AS, as well as the external License Server (LS), and Authorization Server (AUS) via reference point M2d.

2. Support for the delivery of updated content protection information (for example new key information) from an external entity to the Encryptor/Packager and the Manifest Creator deployed in the 5GMSd AS via reference point M2d.

3. The delivery of modified content protection information in the presentation manifest and the content via reference point M4d.

4. Explicit support for encrypted sample entries 'encv' etc, in 3GPP TS 26.511 [96] to support encrypted media formats.

An additional question arises whether encryption needs to be part of the content preparation template and configuration via in the 5GMSd AS via reference point M3d is needed. This aspect is not included in the call flow, but should be considered as a potential open issue.

### 5.10.6 Candidate solutions

In order to address the open issues documented in clause 5.10.5, the following aspects address a solution to the topics:

- Support for Content Protection Information Exchange Format (CPIX) as specified in ETSI TS 103 799 [C] at reference point M2d addresses open issues 1 and 2 identified in clause 5.10.5.

- Support for the DASH-IF Interoperability Points; Part 6 [B] at reference point M4d addresses open issue 3 identified in clause 5.10.5 for both DASH and HLS.

- Support for decryption and (re-)encryption tasks in the content preparation template tasks in the 5GMSd AS, specified using a Content Preparation Template provisioned in the 5GMSd AF via M1d and configuration in the 5GMSd AS via reference point M3d.

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

## 6.10 Support for distributing encrypted and high-value content

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

- Support the Content Protection Information Exchange Format (CPIX) as specified in ETSI TS 103 799 [C] at reference point M2d by specifying the necessary stage-2 and stage-3 extensions in TS 26.501 [15] and TS 26.512 [16] respectively.

- Support the DASH-IF Interoperability Points specified in [B] at reference point M4d for both DASH and HLS by specifying the necessary stage-2 and stage-3 extensions in TS 26.501 [15] and TS 26.512 [16], respectively.

- Specification of a Content Preparation Template format in TS 26.512 [16] or TS 26.510 [26510] that can configure content decryption and (re-) encryption content preparation tasks in the 5GMS AS.

NOTE: Maintaining functional symmetry with uplink media streaming (where applicable) is important.

In particular, stage 2 extensions are needed to address the open issues:

- Functional updates to the definition of the 5GMS AS to support:

- Ingest, delivery, contribution and egest of encrypted content

- Content preparation tasks for:

- Decrypting content ingested at reference point M2d or contributed at reference point M4u.

- (Re-)encrypting content prior to distribution at reference point M4d or egest at reference point M2u.

- Updates to the definitions of reference points to support:

- Carriage of Content Protection information at reference point M2d and M4u.

- Delivery of Content Protection information in presentation manifests at reference point M4d and M2u.

 Stage 3 aspects are provided above.