**3GPP TSG-SA4 Meeting #129-e *S4-241469***

**Online, , 19th Aug 2024 - 23rd Aug 2024 revision of S4aI240099**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **26.804** | **CR** | **0016** | **rev** | **2** | **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:*** | S4 |
|  |  |
| ***Work item code:*** | FS\_AMD |  | ***Date:*** | 2024-08-12 |
|  |  |  |  |  |
| ***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:*** | 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-Part5-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:*** |

|  |  |  |  |
| --- | --- | --- | --- |
| [**S4aI240099**](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Docs/S4aI240099.zip) | [FS\_AMD] DRM and Conditional Access. | Qualcomm Germany | Thomas Stockhammer |

**Revisions**: none**Presenter**: Thomas Stockhammer**Online Discussion**:Rufael: Multi-key and multi-DRM is not very explicitly explained. And second question you are mapping all from the CPIX document, right?Thomas: We could say everything is external. I think we should see what would happen if we internalise the 5GMS architecture. Rufael: so this is like, after the encryption part, right? **Decision**: endorsed [S4aI240099](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/3GPP_SA4_AHOC_MTGs/SA4_MBS/Docs/S4aI240099.zip) is **Endorsed**. |

## ===== CHANGE (Updates in clause 5.10.3 and 5.10.4 w/o rev marks) =====

## 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 specification are for example provided by the MovieLabs ECP requirements 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. 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. This includes management for supporting multiple DRM systems at the same time

2. *Key rotation in order to support live streaming.* As an example, these keys are changed periodically but protected by the master key.

3. *DRM and 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. Another case might be multi-key, where different quality levels are encrypted with different keys.

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.*

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

In addition, DASH-IF has defined workflows for managing protected content.

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

- DASH-IF-IOP-Part5-v5.0.0: Content protection and security [B]

- ETSI TS 104 002: DASH-IF Forensic A/B Watermarking [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 media plane (reference points M2 and M4) as well as the media session handling APIs (reference points M3, M5) should also be studied.

### 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 TS 26.501.

### 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].



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 are 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.

In even more details, a 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-Part5-v5.0.0 [B] by putting more emphasis on the backend 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 entitlement is required. One or several content keys can be used 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 (in case multi-DRM is used there are multiple DRM systems) and the encryption engine at the right moment depending on how these keys are used. The MPD generator requests to the DRM systems their specific signaling, if any, to be added in the MPD. Encrypted segments and the media manifest are uploaded on a CDN making it available to users.

Figure 5.10.3-3 illustrates the usage of the encrypts in a realistic workflow comprising multiple cooperating components. In ETSI TS 103 799, a standardized data format for content protection information exchange is defined, collected in a document that is 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 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 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 (MC).

MPD and Segment Generation:

9. The Manifest Creator generates the MPD (Media Presentation Description) and adds the content protection information.

10. The Manifest Creator uploads the MPD to the DASH Presentation Hosting (DP).

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

12. The Manifest Creator uploads the encrypted segments to the DASH Presentation Hosting.

Client Requests and Authorization:

13. The DASH Client (DC) requests the MPD from the DASH Presentation Hosting.

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

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

16. The DASH Client provides the license to the DRM System (DRMS).

Content Delivery and Decryption:

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

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

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

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 M12 of the Media Delivery architecture as shown 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 TS 26.501 [15]

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 |  |  |  |
| DASH Presentation |  | 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 is running all DRM and packaging related functions, and the Media AS only acts as hosting the DASH Presentation as a CDN. For DRM acquisition, the UE contacts the Media Application Provider.

Option 2: the mobile network operator runs a DRM and packaging service, including a license server on the Media AS. Content is ingest to the Media AS and all operations functions of license hosting, encoding, encryption and so on is running in the Media AS.

Option 3: the mobile network operator runs encoding and packaging service, but the license server is external in the Media AP. The Media AS needs to communicate with the license server for encoding and packaging.

Option 4: the mobile network operator runs manifest generation, but the encoding/packager/encryptor are external in the Media AP. The Media AS needs to acquire relevant information for manifest generation.

Option 5: this is similar to option 2, but the licensing server as being quite specific in operation is handed to the Media AF. The main communication is between Media AS and Media AF.

Option 6: this is similar to option 5, but only the licensing server is offered by the MNO in the Media AF. The main communication is between application provider and Media AF for content encoding.

Based on current deployments, license acquisition is a user plane communication and no APIs in the media access client exist to delegate the license acquisition to a third-party function, such as the 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 | 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 F | Media Access F | Media Access F | Media Access F |
| 17 | M4 | M4 | M4 | M4 |
| 18 | Media Access F | Media Access F | Media Access F | Media Access F |
| 19 | Media Access F | Media Access F | Media Access F | Media Access F |
| 20 | Media Access F | Media Access F | Media Access F | Media Access F |
| 21 | Media Access F | Media Access F | Media Access F | Media Access F |

Based on the analysis in Table 5.10.4-2, for different deployment options, functional updates are necessary for Media AS and Media Access Functions, and additional information may be exchanged through interfaces M2, M4 and M8.

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

### 5.10.5 Potential open issues

Editor’s Note: Identify the issues that need to be solved.

### 5.10.6 Candidate Solutions

Editor’s Note: Provide candidate solutions (including call flows) for each of the identified issues.

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

## 6.10 Support for encrypted and high-value content

No conclusion has yet been reached for this key issue.

Initial considerations are provided in clause 5.10. It is recommended to study it further at an appropriate time.