**3GPP TSG SA WG4 Meeting 132S4-250792**

**Fukuoka, JP, 19 - 23 May 2025**

**Source: Qualcomm Incorporated**

**Title: [FS\_MeMe] DRM-protected Media Messages**

**Type: pseudo Change Request**

**Spec: 3GPP TR26.841v1.2.0**

**Agenda item: 8.6**

**Document for: Decision**

**1. Introduction and Discussion**

The key issue on DRM and encrypted content was not yet sufficiently progressed.

**2. Reason for Change**

This progresses the work.

Note that this document assumes that S4-250791 is accepted.

**3. Conclusions**

Please accept.

**4. Proposal**

It is proposed to agree the following changes to 3GPP TR26.841v1.2.0.

**5. Revision**

This revision takes into account the comments made during the presentation during SA4#132.

|  |  |
| --- | --- |
| TDoc | [S4-250792](https://www.3gpp.org/ftp/tsg_sa/WG4_CODEC/TSGS4_132_Fukuoka/Docs/S4-250792.zip) |
| Title | [FS\_MeMe] DRM-protected Media Messages |
| Source | Qualcomm Sweden |
| Contact | Thomas Stockhammer |
| Agenda Item | 8.6 |
| E-mail Discussion | No e-mail discussion. |
| Revisions | No revisions available. |
| Minutes | 21/05/25Presented by Thomas.* Thomas: It is not TR 25, I probably wanted to say 26.804.
 |
| Disposition |  |
| Status |  parked |

\* \* \* First Change \* \* \* \*

## 5.4 Key Topic #4: DRM and encrypted content

### 5.4.1 Description

While typical messaging services including IETF MIMI support end-to-end encryption of the messages, in some cases the content itself needs to be content protected, for example if high-value content is shared in messaging services, if copying of the content needs to be prevented and so on. In this case, the content may be encrypted, and the service needs to be integrated in a key management environment. Providing proper functionality for this purpose needs to be studied.

### 5.4.2 Gap Analysis and Requirements

No content protection is available in TS 26.143 [26143].

### 5.4.3 Potential Solutions

#### 5.4.3.1 General

A manifest based solution as documented in clause 5.3 is most suitable. Extension to support content protection are straightforward. The combination with a license server workflow is following 5G Media streaming as discussed in TR 26.804.

#### 5.4.3.2 Example

The example in Listing 5.3.3.2.4-2 is extended to add content protection elements in Listing 5.4.3.2-1.

Listing 5.4.3.2-1 Example MPD container to include richer content offering with Content Protection

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?><MPD  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="urn:mpeg:DASH:schema:MPD:2011" xsi:schemaLocation="urn:mpeg:DASH:schema:MPD:2011" type="static" mediaPresentationDuration="PT3256S" minBufferTime="PT1.2S" profiles="urn:mpeg:dash:profile:isoff-on-demand:2011, urn:3GPP:org:26143:baseline"> <BaseURL>http://cdn1.example.com/</BaseURL> <BaseURL>http://cdn2.example.com/</BaseURL> <Period> <!-- English Audio --> <AdaptationSet mimeType="audio/mp4" codecs="mp4a.0x40" lang="en" subsegmentAlignment="true"> <ContentProtection schemeIdUri="urn:uuid:706D6953-656C-5244-4D48-656164657221"/> <Representation id="1" bandwidth="64000"> <BaseURL>7657412348.mp4</BaseURL> </Representation> <Representation id="2" bandwidth="32000"> <BaseURL>3463646346.mp4</BaseURL> </Representation> </AdaptationSet> <!-- French Audio --> <AdaptationSet mimeType="audio/mp4" codecs="mp4a.40.2" lang="fr" subsegmentAlignment="true"> <ContentProtection schemeIdUri="urn:uuid:706D6953-656C-5244-4D48-656164657221"/> <Role schemeIdUri="urn:mpeg:dash:role" value="dub"/> <Representation id="3" bandwidth="64000"> <BaseURL>3463275477.mp4</BaseURL> </Representation> <Representation id="4" bandwidth="32000"> <BaseURL>5685763463.mp4</BaseURL> </Representation> </AdaptationSet> <!-- Timed text --> <AdaptationSet mimeType="text/mp4" codecs="3gp.text" lang="fr" lang="de"> <Role schemeIdUri="urn:mpeg:dash:role" value="subtitle"/> <Representation id="5" bandwidth="256"> <BaseURL>796735657.mp4</BaseURL> </Representation> </AdaptationSet> <!—Video AVC --> <AdaptationSet mimeType="video/mp4" codecs="avc1.4d0228" subsegmentAlignment="true" selectionPriority="2"> <ContentProtection schemeIdUri="urn:uuid:706D6953-656C-5244-4D48-656164657221"/> <Representation id="6" bandwidth="256000" width="320" height="240"> <BaseURL>8563456473.mp4</BaseURL> </Representation> <Representation id="7" bandwidth="512000" width="320" height="240"> <BaseURL>56363634.mp4</BaseURL> </Representation> <Representation id="8" bandwidth="1024000" width="640" height="480"> <BaseURL>562465736.mp4</BaseURL> </Representation> <Representation id="9" bandwidth="1384000" width="640" height="480"> <BaseURL>41325645.mp4</BaseURL> </Representation> <Representation id="A" bandwidth="1536000" width="1280" height="720"> <BaseURL>89045625.mp4</BaseURL> </Representation> <Representation id="B" bandwidth="2048000" width="1280" height="720"> <BaseURL>23536745734.mp4</BaseURL> </Representation> </AdaptationSet> <!—Video HEVC --> <AdaptationSet mimeType="video/mp4" codecs="hev1.1.6.L150.90" subsegmentAlignment="true" selectionPriority="1"> <ContentProtection schemeIdUri="urn:uuid:706D6953-656C-5244-4D48-656164657221"/> <Representation id="C" bandwidth="128000" width="320" height="240"> <BaseURL>8563456473-h.mp4</BaseURL> </Representation> <Representation id="D" bandwidth="256000" width="320" height="240"> <BaseURL>56363634-h.mp4</BaseURL> </Representation> <Representation id="E" bandwidth="512000" width="640" height="480"> <BaseURL>562465736-h.mp4</BaseURL> </Representation> <Representation id="F" bandwidth="695000" width="640" height="480"> <BaseURL>41325645-h.mp4</BaseURL> </Representation> <Representation id="G" bandwidth="760000" width="1280" height="720"> <BaseURL>89045625-h.mp4</BaseURL> </Representation> <Representation id="H" bandwidth="1024000" width="1280" height="720"> <BaseURL>23536745734-h.mp4</BaseURL> </Representation> </AdaptationSet> </Period></MPD> |

#### 5.4.3.3 Potential Open Issues

While discussed solution in this clause provides opportunities to support this feature, some potential open issues are documented in the following:

- How does DRM relate to envelope end-to-end encryption if the message body? Is this mutually exclusive?

- How would the license key management work in a messaging environment? Would the messaging server connect to a license server and also the messaging client?

- Is it really needed to use a commercial DRM or is the expectation to use clear-key protection only?

### 5.4.4 Summary and Conclusions

Based on the discussion in this clause, it is recommended to address Content Protection for richer content formats in media messaging. The following additions to TS 26.143 are recommended:

1. Address all extensions documented in clause 5.3.4.

2. Permit Content Protection to be signalled in the manifest.

3. Address the potential open issues documented in clause 5.4.3.3

\* \* \* End of Changes \* \* \* \*