**Agenda item:** 9.8

**Source:** Qualcomm Incorporated

**Title:** [5MBUSA] Security Aspects

**Document for** Discussion andAgreement

# Introduction

This document addresses issues around transport and content security in 5MBS.

# Security in MBMS

The following summarizes some clauses from TS 26.346 on security in MBMS.

4.4.3 MBMS Session and Transmission Function

…

MBMS user services data may be integrity and/or confidentiality protected as specified within 3GPP TS 33.246 [20], and protection is applied between the BM-SC and the UE. This data protection is based on symmetric keys, which are shared between the BM-SC and the UEs accessing the service.

…

5.2.2.4 Security Description

The Security Description fragment contains the key identifiers and procedure descriptions for one delivery method. Multiple delivery methods, each via an instance of the *deliveryMethod* element, may reference the same Security Description fragment.

The Security Description fragment contains key identifiers and the server address to request the actual key material. To avoid overload situations, the same load balancing principles as in the associated delivery procedures are used. The key management server shall be selected as defined in sub-clause 9.3.5. The back-off time shall be determined as defined in sub-clause 9.3.4.

The XML schema for the Security Description fragment is defined in sub-clause 11.3.

5.5 MBMS Protocols

Figure 9 illustrates the protocol stack used by MBMS User services for Streaming and Download delivery. The grey-shaded protocols and functions are outside of the scope of the present document. MBMS security functions and the usage of HTTP-digest and SRTP are defined in 3GPP TS 33.246 [20], and 3GP-DASH is defined in TS 26.247 [98].

NOTE: The asterisk(\*) mark after the box labelled "HTTP(S)" in the left side of Figure 9 means that although the box is unshaded, the use of HTTP(S) for unicast delivery of Service Announcement & Metadata is outside the scope of this document, and is defined by the OMA Push OTA specification [79].

****

**Figure 9:** **Protocol stack view of the MBMS User Services for Streaming and Download Delivery**

5.6 DASH and MBMS

…

Clause 4.4.3 of this specification enables integrity and/or confidentiality protection of MBMS user services data according to 3GPP TS 33.246 [20]. In this case each DASH formatted file is protected using the Protection of Download Data as described in [20].

As this protection mechanism is performed in the underlying layer of the DASH client it is transparent to 3GP-DASH client and not reflected in the MPD associated to the DASH representation.

…

7.2.9 Signalling of Parameters with FDT Instances

…

These optional FDT Instance data elements may or may not be included for FLUTE in MBMS:

- Complete (the signalling that an FDT Instance provides a complete, and subsequently unmodifiable, set of file parameters for a FLUTE session may or may not be performed according to this method).

- Content-Encoding.

- Content-MD5: represents a digest of the transport object. The file server should indicate the MD5 hash value whenever multiple versions of the file are anticipated for the download session.

- IndependentUnitPositions: represents a list of byte position in the file, at which the handler assigned to the Content-Type for the file may access the file.

- File-ETag: represents the value of the ETag, or entity-tag as defined in RFC 2616 [18] which mays also serve as the version identifier of the file object described by the FDT Instance.

NOTE 6: The values for each of the above data elements are calculated or discovered by the FLUTE sender.

The FEC-OTI-Scheme-Specific-Info FDT Instance data element contains information specific to the FEC scheme indicated by the FEC Encoding ID encoded using base64.

7.2.15 Decryption key indicating of protected download data

A MBMS download service may indicate relevant decryption key file for protected download file in FLUTE FDT instance. A new attribute "Decryption-KEY-URI" is created within element "file" of the FDT to indicate the association between protected download file and relevant decryption key file. The value of "Decryption-KEY-URI" in "file" element shall be equal to the content-location of the MIKEY file that contains the decryption key file.

When the server delivers a protected download file, the server should set a "Decryption-KEY-URI" field in the corresponding file element in the FLUTE FDT instance. When a UE receives a protected file, the UE may instruct its FLUTE receiver to download the relevant decryption key file according to "Decryption-KEY-URI" field in file element of FDT instance.

The XML syntax of the "Decryption-KEY-URI" attribute within the FLUTE FDT is the following.

<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns="urn:3GPP:metadata:2009:MBMS:FLUTE:FDT\_ext"

xmlns:xs="http://www.w3.org/2001/XMLSchema"

targetNamespace="urn:3GPP:metadata:2009:MBMS:FLUTE:FDT\_ext"

elementFormDefault="qualified">

<xs:attribute name="Decryption-KEY-URI" type="xs:anyURI"/>

</xs:schema>

A service protection method is described in TS 26.346, clause 11.3 to 11.7. However, this security mechanism is not referenced in Annex L for the deployment profiles.

# Security in 5MBS

In TS 23.247, security is not mentioned.

In TR 23.757, some statements of security are mentioned

* For "Content security protection", it is assumed to be achieved on application layer which is out of SA2 scope.
* Handling of the security for MBS traffic is determined by SA3. SA2 specifications will align with SA3 as needed.

SA3 has initiated a work item on this matter in [SP-210420](http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGs_92E_Electronic_2021_06/Docs/SP-210420.zip). The objective of this work item is to specify the security aspects of 5MBS services to support solution(s) in TS 23.247 and related WIs in RAN groups. Another objective of this WID is to align with SA2 and RAN group’s work item on MBS for R17 by providing the necessary security requirements, architecture enhancement and security solutions in order to support MBS in 5G. The security aspects to be considered are as follows:

* Security protection between AF and 5GC.
* Other security and privacy issues raised from other WG’s work related to 5MBS services, if there is any.

NOTE: Additional objectives will be included if additional conclusions are reached within TR 33.850 that require normative work.

As a pre-cursor, SA3 has a draft TR 33.850 on “Study on Security Aspects of Enhancements for 5G Multicast-Broadcast Services (MBS)”. Unfortunately, conclusions on security are not yet provided. However, at least certain solutions consider protecting MBS traffic on service layer and involve key distribution through MBSF and MBSTF.

# Security in 5GMS

5GMS provides the ability to use HTTPS for transport security.

In addition, TS 26.501 as well as TS 26.511 and TS 26.247 provide clear instructions in content protection

- **DRM Client** (optional): When present, the DRM client might or might not be a part of the Media Player. It provides a content protection mechanism with its unique key management and key delivery system, authentication/‌authorization, policy enforcement and entitlement check. The DRM Client is not defined within 5G Media Streaming specifications.

- **Media Decryption** (optional): When present, media decryption is responsible to decrypt the media samples using the keys provided in the DRM license, and further passing to the Media Decoder to enable playback of encrypted media. The media decryption and media decoding could be implemented on a general-purpose processor in software or hardware or, for a more secure and robust architecture, the decryption, decoding and rendering could be implemented on the hardware of secure processors.

# Discussion and Principles

Based on the findings, it is obvious that the service layer may be involved in transport security aspects for 5MBS. However, SA3 is still working on potential solutions. It is proposed to await progress in SA3, but potentially communicate with SA3 on any needs that they see arising in the design of the 5MB User Service.

Secondly, encryption and content protection are important functionalities for media services and require attention for 5MBS.

A few key observations

* Common encryption (CENC) (as defined in TS 26.511) enables multiple DRM systems with a common content format
  + Standard encryption and encryption metadata to assist in decrypt
  + Key mapping (key exchange out of scope)
* DRM systems may still be differentiated through
  + Rights management
  + Key retrieval/rotation and storage
* On the latter, DASH-IF just recently specified Enhanced Clear Key Protection (ECCP) to address greater protection than Transport Layer Security (TLS) [13] delivery, token authentication or Clear Key used individually.
  + TLS protects content in transit from client to server but the media content is stored and processed in the clear.
  + Token authentication schemes will authenticate a client, but the media content again is processed in the clear.
  + Clear Key protects the content at rest and while it is being processed in an inaccessible pipeline within the client, however it provides no authentication as the key is given to any client that requests it.
  + By combining TLS delivery with token authentication and Clear Key, it is ensured cryptographic enforcement of that token authorization, leading to a class of access control which provides stronger protection than the contributing schemes applied individually.
  + ECCP is therefore a collective set of restrictions placed on content preparation, manifest preparation, license server behavior and segment authentication.

For encrypted content we believe the following assumptions are important.

1. It is reasonable to expect that 5MBS receivers that make use of CENC-based DRM systems are unicast connected. They can create MediaKeySessions (W3C terminology) and can refresh licenses.
2. It is reasonable to expect that delivered media services are included in containers that are CENC compatible, in particular in combination with ISO BMFF, CMAF and TS 26.511.
3. Key rotation critical for ensuring continued content encryption in the case that key material has leaked. Key rotation may be addressed as part of the DASH/CMAF delivery.

Overall, it is considered that a content protection-based approach for content layer security is sufficient for any object delivery mode in 5MBS. This applies for FLUTE and ROUTE based delivery of content.

Key exchange and key rotation for 5MBS needs to be carefully checked in terms of scalability, but it is considered to be sufficient.

However, content security alone may not be sufficient to satisfy all service layer security requirements. There are some aspects of service layer security (e.g. user privacy) that may only be met by robust transport layer security mechanisms.

# Proposal

Based on the discussion it is proposed to

1. to await progress in SA3 transport security aspects, but potentially communicate with SA3 on any needs that they see arising in the design of the 5MB User Service.
2. Start collecting requirements and considerations and reach out to SA3. We may need to think also about file delivery, such as MCData.
3. To defer content layer security to the 5MBS Application. As an example, the Common encryption (CENC) approach for content security (as defined in TS 26.511) enables different service/content protection modes and multiple DRM systems with a common content format and may be used as a reference for other applications as well.
4. In consequence of the above, also agree that the exchange with the key management/DRM system happens over unicast and no specific measures are needed in 5MBS content security
5. Analyze potential aspects on unicast scalability for key exchange in the context of 5GMS-EXT key issues.
6. Analyse other aspects of service layer security (e.g. user privacy) that may only be met by robust transport layer security mechanisms and identify if SA4 or other 3GPP groups define such functionalities.

Once these basic principles are agreed, we are supportive to provide normative text on this matter and possibly communicate with SA3 (CC SA2 on the first matter).