Title:	**Scope of MBMS security**
Source:	**Ericsson**
Document for:	**Discussion and decision**
Agenda Item:	
Work Item:	**MBMS**

1 Introduction

In various discussions in previous SA3 meetings two issues have not been clear:

1. Is MBMS security regarded as part of MBMS User Service or MBMS Transport Service activity? In other words, is MBMS security access independent?

2. What is the scope of MSBS protection? In the current TS 33.246 one can get the understanding that MBMS security provides protection for MBMS transport bearers.

We foresee that clear common understanding of these issues helps finalise MBMS security mechanisms.

2 Discussion

SA4 is responsible for MBMS User Service architecture. In section 4.1 an 4.2 of TS 26.346 [1] SA4 has specified the following functional layers for MBMS[1]:

---

[1] Clauses 4.1 and 4.2 of TS 26.346 are added as an annex to this contribution
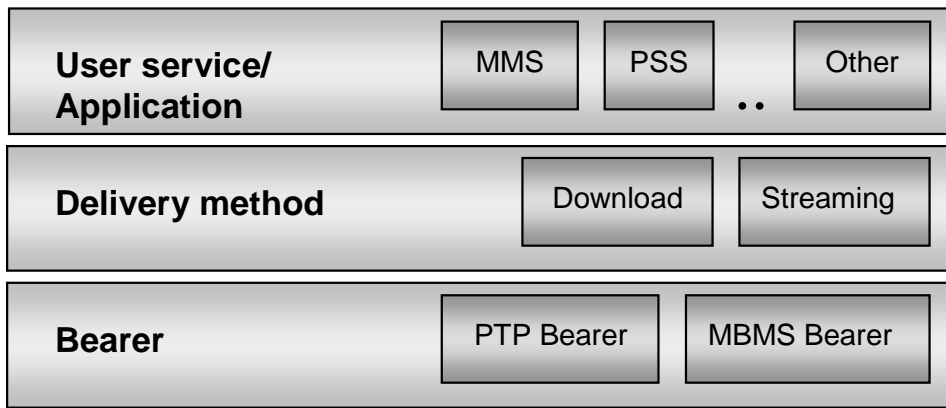
Figure 1: Functional Layers for MBMS User Service

In 4.1 of TS 26.346 MBMS security in placed on delivery method layer:

- *As an example a messaging application such as MMS would use the download delivery method while a streaming application such as PSS would use the streaming delivery method.*

- *The delivery layer <u>provides functionality such as security and key distribution</u>, ...*

- *Bearers provide the mechanism by which IP data is transported.... MBMS bearers may be used jointly with unicast PDP contexts in offering complete service capabilities*
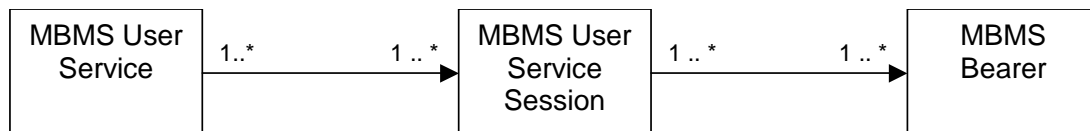
In 4.2 the following extract it is stated:

Figure 1: Entities and Relations

- *A single [user service] service entity can contain multiple distinct multimedia objects or streams, which may need to be provided over various MBMS download or MBMS streaming sessions....*

- *A set of one or more MBMS bearers can be used for delivering data as part of an MBMS download or streaming session. As an example, the audio and visual part of video stream can be carried on separate MBMS bearers. A download session or a streaming session is associated with its MBMS bearers and a set of delivery method parameters specifying how content is to be received on the mobile side.*

- ***An MBMS bearer*** *(identified by IP group address and APN) might be used in providing data to* ***more than one*** *MBMS download or streaming* ***session***.

Because SA3 MBMS security mechanisms will protect the *application layer* flows, i.e. protection of MBMS streaming sessions (with SRTP) and MBMS download sessions (with yet to be defined mechanism for FLUTE), and because several MBMS streaming or MBMS download sessions may be carried in one MBMS bearer (*which is IP layer concept*), it seems clear that the MBMS bearer is not the scope of MBMS

protection. Instead the **scope of MBMS protection should be based on MBMS Streaming / Download Sessions level as defined by SA4**. According to section 4.1 of TS 26.346 this is also the view of SA4.

This also means that **MBMS security should be independent of Transport Service and should therefore be regarded as User Service level activity**. According to this MBMS protected flow (streaming or download) could be delivered over other transport than MBMS bearer, like PTP bearer or even WLAN.

3 Conclusions and proposal

It can be concluded that

- the scope of MBMS protection should be based on MBMS User Service Sessions level/ Delivery method layer as defined by SA4. This means for example that the finest granularity of protection can be smaller a transport service, e.g. if two SRTP streams are carried in one transport service.

- MBMS security should be independent of Transport Service and should therefore be regarded as User Service level activity

It is proposed that

- SA3 aligns the scope of MBMS security with SA4 and adopts the understanding presented in conclusions

- Needed clarifications and changes are made in TS 33.246 [2]

A CR from Ericsson to this meeting proposes needed changes in TS 33.246.

4 References

[1]   TS 26.346, MBMS, Protocols and codecs

[2]   TS 33.246, Security of MBMS

5 Annex A Text from TS 26.346

4.1 MBMS Functional Layers

Delivering MBMS-based services 3 distinct functional layers are identified – Bearers, Delivery method and User service. Figure 1 depicts these layers with examples of bearer types, delivery methods and applications.
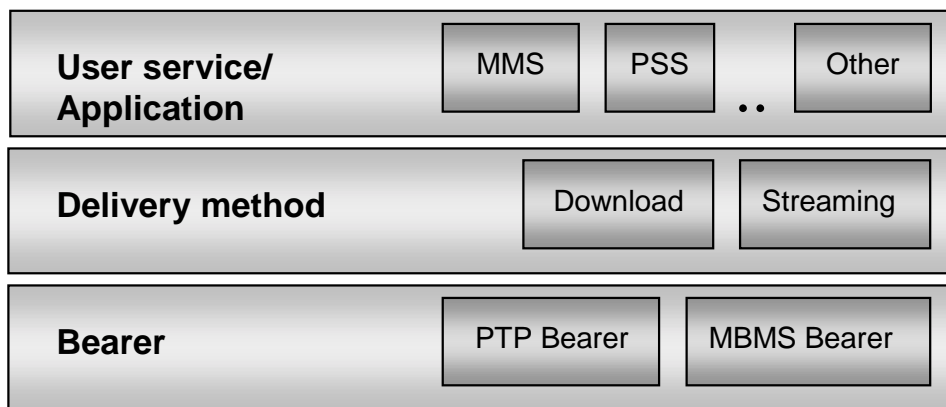
Figure 2: Functional Layers for MBMS User Service

-   **Bearers**. **Bearers provide the mechanism by which IP data is transported.** MBMS bearers as defined in [4] (TS 23.246) and [3] (TS 22.146) are used to transport multicast and broadcast traffic in an efficient one-to-many manner and are the foundation of MBMS-based services. **MBMS bearers may be used jointly with unicast PDP contexts in offering complete service capabilities**.

-   **Delivery Method**. When delivering MBMS content to a receiving application one or more delivery methods are used. **The delivery layer provides functionality such as security and key distribution,** reliability control by means of forward-error-correction techniques and unicast post delivery supplementation, reception verification and support for inter-operator service profiles. Two delivery methods are defined, namely download and streaming. MBMS delivery may utilize both MBMS bearers and PTP bearers.

-   **User service**. The MBMS User service enables applications. Different application impose different requirements when delivering content to MBMS subscribers and may use different MBMS delivery methods. **As an example a messaging application such as MMS would use the download delivery method while a streaming application such as PSS would use the streaming delivery method.**

4.2 MBMS User Service Entities

The figure below shows the MBMS user service entities and their inter-relations. Relation cardinality is depicted as well.
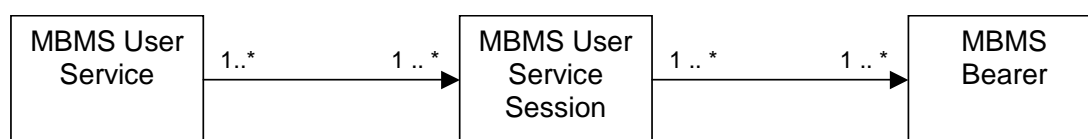
Figure 3: Entities and Relations

An MBMS user service is an entity that is used in presenting a complete service offering to the end-user and allowing him to activate or deactivate the service. It is typically associated with short descriptive material presented to the end-user, which would potentially be used by the user to decide whether and when to activate the offered service.

A single service entity can contain multiple distinct multimedia objects or streams, which may need to be provided over various MBMS download or MBMS streaming sessions. A download session or a streaming session is associated with its MBMS bearers and a set of delivery method parameters specifying how content is to be received on the mobile side.

A set of one or more MBMS bearers can be used for delivering data as part of an MBMS download or streaming session. As an example, the audio and visual part of video stream can be carried on separate MBMS bearers.

An MBMS bearer (identified by IP group address and APN) might be used in providing data to more than one MBMS download or streaming session (TS 22.246 [3] section 5).