3GPP TSG SA WG3 Security — S3#34 **S3-040489**

July 6 - 9, 2004

Acapulco, Mexico

Source: **Siemens**

Title: **N to N relationship between User Services and Transport Services**[1]

Document for: **Discussion and Decision**

Agenda Item: **MBMS**

1 Introduction

This contribution analyses the relationship between different types of User Services and the Transport Services, and looks at the consequences for MBMS MSK Key management. The conclusion is that the key management shall be done at MBMS User Service level, not at Transport Service level. For MBMS User Services containing non-shared Transport Services it shall be possible to use one or more MSK's on different Transport Services while an MSK that is used with a shared Transport Service shall not be used within another Transport Service. Section 4 contains a proposed pseudo-CR.

2 Analysis of User Services according to TS 22.246

There are two requirements within TS 22.246 (Section 5 High Level Requirements) which have impacts on the way the MSK handling is done.

> (1) "*A MBMS user service is composed of one ore more MBMS transport services. By using the same MBMS transport services for more than one MBMS user service an operator is able to extend the range of offered MBMS user services without sacrificing additional resources over the air*."
>
> (2) *" It shall be possible for an MBMS user service to make use of different application independent MBMS transport services at different times or in parallel. The MBMS transport services used may vary for instance in QoS parameters or target broadcast or multicast area*."

Figure 1 provides one example whereby one MBMS Transport Service is shared among two different User Services (as described by (1)).

[1] For a definition see TS 22.246

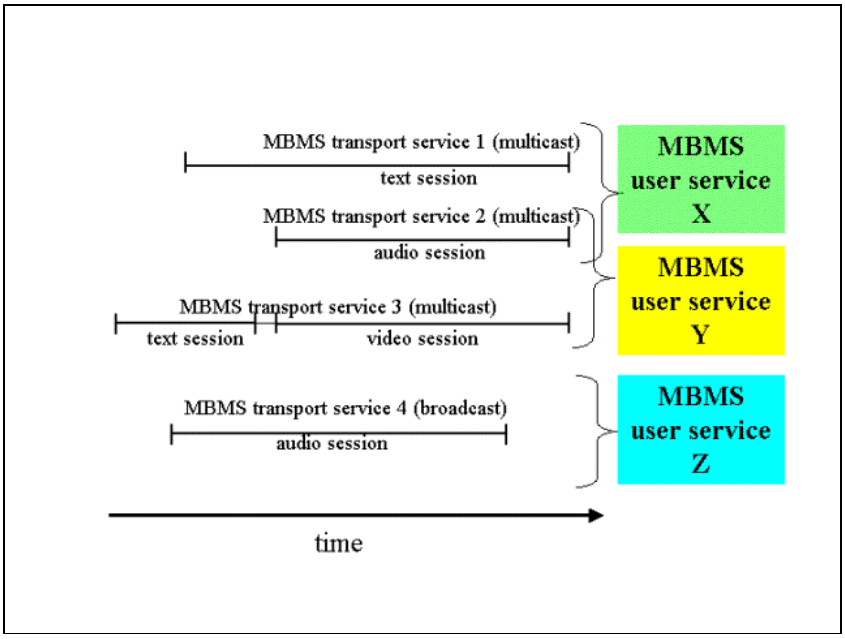

MBMS transport service 1 (multicast)
text session
MBMS transport service 2 (multicast)
audio session
MBMS transport service 3 (multicast)
text session
video session
MBMS transport service 4 (broadcast)
audio session
time
MBMS user service X
MBMS user service Y
MBMS user service Z

Figure 1: two MBMS user services sharing one transport Service

"In this figure User Service X could e.g. be a low-tariff traffic service, consisting of 2 multicast services: Transport Service 1 - text - and Transport Service 2 - voice. But Transport Service 2, the voice component, could be re-used at the same time in a different (high-tariff) User Service Y, which also gives the same traffic information, but provides a video component (Transport Service 3) instead of the text. There is a gain in resources while Transport Service 2 has to be multicasted only once to be used in two User services."

Consequentially, for these kinds of User Services, it is impossible to have only one MSK per User Service, as it would allow low-tariff users to access data of the High-tariff users. Therefore for these types of User Services **the MSK that is used within a shared Transport Service cannot be used within another Transport Service**.

Now requirement (2) also states that an MBMS User Service shall be able to make use of different MBMS Transport Services at different times or in parallel. This means that the BM-SC shall be able to use two Transport Services in parallel. If these parallel Transport Services are non-shared then there is no reason to use different MSKs for these Transport Services. Indeed, it may be advantageous for the operator to able to decide on Transport Service (re)-allocation without causing additional MSK Key Management messages. This seems to be especially relevant for these cases where resource management decisions can cause setup of additional Transports Services at a certain time which was not anticipated at the set-up of the User Service. **For MBMS User Services with non-shared Transport Services it shall be possible to use one or more MSK's on different Transport Services.** For this type of User Services the UE has to combine the incoming data (then data segments of both of these transport service may based on the same MSK and therefore may use the same MTK's) anyhow.

3 Conclusions

The conclusions that can be derived from section 2 are:

1) A MBMS User Service may contain one or more MSKs which may be in use at the same time.

2) The key management shall be done at MBMS User Service level, not at Transport Service level.

3) For MBMS User Services containing non-shared Transport Services it shall be possible to use one or more MSK's on different Transport Services.

4) An MSK that is used with a shared Transport Service shall not be used within another Transport Service.

It is proposed to adopt the above understanding by accepting the pCR text in section 4 of this contribution.

4 Proposed pCR-text for TS 33.246

***** first proposed change ****

6.0 Key Management Model

A MBMS User Service may contain one or more MSKs which may be in use at the same time and are managed at the MBMS User Service Level. The BM-SC controls the use of the MSKs towards the different Transport Services. The MSKs are not directly used towards the MBMS Transport Services but as a second level key MTK as specified within clauses 6.4 and 6.5.

According to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services. For MBMS User Services containing non-shared Transport Services it shall be possible to use one or more MSK's with different Transport Services. An MSK that is used with a shared Transport Service shall not be used within another Transport Service.

6.1 Using GBA for MBMS

GBA[6] is used to agree keys that are needed to run an MBMS Multicast User service. MBMS imposes the following requirements on the MBMS capable UICCs and MEs:

A UICC that contains MBMS key management functions shall implement GBA_U.

An ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC.

Before a user can access an MBMS User service, the UE needs to share GBA-keys with the BM-SC. If no valid GBA-keys are available at the UE, the UE shall perform a GBA run with the BSF of the home network as described within [6] section 5. The BM-SC will act as a NAF according to [6].

The MSKs for an MBMS User service shall be stored on either the UICC or the ME. Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions (and by requirement is GBA aware) and requires that all of the network elements, i.e. HSS, BSF and BM-SC, to be GBA_U aware. As a result of the GBA_U run in these circumstances, the BM-SC will share a key Ks_ext_NAF with the ME and share a key Ks_int_NAF with the UICC. This key Ks_int_NAF is used by the BM-SC and the UICC as the key MUK to protect MSK deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK within the protocols as described within clause 6.2.

NOTE: A run of GBA_U on a GBA aware UICC will not allow the MSKs to be stored on the UICC, if the MBMS management functions are not present on the UICC.

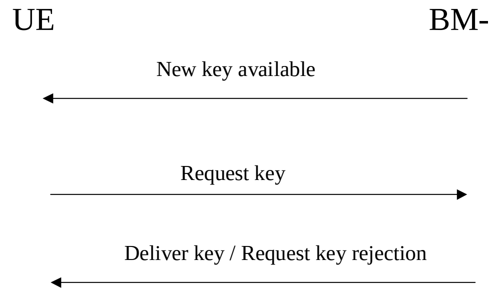
In any other circumstance, a run of GBA results in the BM-SC sharing a key Ks_(ext)_NAF with the ME. This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and the key MRK (MBMS Request Key). The key MUK is used to protect MSK deliveries to the ME as described within clause 6.3. The key MRK is used to authenticate the UE towards the MBMS within the protocols as described within clause 6.2.

****** next proposed change ****

6.3 Key update procedure

Once a UE has joined a multicast service, the UE should try to get the MSKs that will be used to 'protect' the data transmitted as part of this multicast service. If the UE fails to get hold of the MSKs or receives confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still-valid, older MSK, the UE shall leave the MBMS user service. The UE tries to get the MSK using the second message in the below flow.

The BM-SC controls when the MSKs used in a multicast service are to be changed. The below flow describes how MSK changes are performed.



The first message is sent out by the BM-SC to indicate that new MSKs are available. It is an optional message in the flow. If it is sent to all UEs, then the BM-SC should provide the rules to the UE for subsequent request for the new MSKs when a UE joins a multicast service, to avoid simultaneous requesting from all the UEs.

Editor's note: A possible method for achieving the above is for the BM-SC to allocates different "request delay time" to different UEs; such that when the UEs receive the new key available message, they shall send the request key message after the delay requested by the BM-SC. Alternatively it is possible to use the key lifetime methods suggested in S3-040059.

The second message is used to request ~~an~~ MSKs. This is sent by the UE when it either receives the first message in the flow and does not have the new MSKs, or has just joined a multicasts service and does not have the~~an~~ MSKs for that service or has received some protected content and does not have the MSK that was used to protect the content. If the UE fails to get hold of the updated MSKs or receive confirmation that no updated MSKs are~~is~~ necessary or available at this time, then, unless the UE has a still valid older MSK, the UE shall leave the MBMS service.

- After receiving the second message the BM-SC should send out the appropriate MSK to the UE protected by the relevant means, or reject the UE's key request with an indication of the cause. Upon successfully receiving the new MSK, the UE should store this key for later use.

Editor's note: MIKEY was chosen as the method for carrying keys. The use of MIKEY will be based on the proposal in S3-040258.

******* next proposed change ******

C.6 Requirements on confidentiality protection of MBMS User Service data

R7a: It shall be possible to protect the confidentiality of MBMS User Service data on the radio interface.

R7b: The MBMS User Service data may be encrypted with ~~a~~ common encryption keys, which shall be available to all users that have joined the MBMS User Service.

R7c: It may be required to encrypt the MBMS User Service data on the “BM-SC - GGSN” interface, i.e. the reference points Gi.

R7d: It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on protect the MBMS User Service from the BM-SC to the UE.

R7e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS User Service when it is applied.