3GPP TSG SA WG3 Security — S3#34 **S3-040543**

July 6 - 9, 2004

Acapulco, Mexico

Title: **Feasibility of Subscription based key management**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

In SA3#33 a concern was raised if GBA and MIKEY approach can support subscription based key management in MBMS. The contribution discusses the feasibility of subscription based key management. According to [1] the subscription and joining are defined as follows:

***Multicast subscription**: The process by which a user subscribes or is subscribed to a multicast subscription group and thereby is authorised to join certain multicast services. Multicast subscription is performed either upon user selection or due to home environment initiation.*

***Multicast Subscription Group**: A group of users who are subscribed to a certain MBMS in multicast mode and therefore authorised to join and receive multicast services associated with this group.*

***Multicast joining:** The process by which a user joins a multicast group.*

***Multicast group**: A group of users that have an activated MBMS in multicast mode and therefore are ready to or are receiving data transmitted by this service. The multicast group is a subset of the **Multicast subscription group**. Multicast subscription group members may join the corresponding multicast group.*

2 Discussion

2.1 Need for subscription based key management

According to [2] the phases of MBMS service provision are as follows:

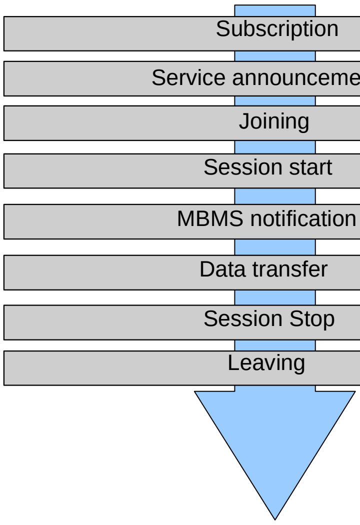

Figure 1. Phases of MBMS Multicast service provision [2].

The MSK key is delivered to the UE from the BM-SC in point-to-point manner. In principle this can be based on subscription or on joining.

According to the comments given in SA3#33 the main argument for subscription based key management is that MSK deliveries can be planned in advance and spread over time. This may avoid key delivery congestion when users start to join the service.

An inevitable consequence of this is that charging will be based on subscription, and not on joining, since the UE will get access (i.e. keys) to the service before joining.

2.2 Requirements for subscription based key management

In order for subscription based key management to be possible in GBA-MIKEY model implies the following requirements to be fulfilled:

- *Req-1: The UE has subscribed to that specific service.*
  This implies that the UE knows the exact MBMS service for which it needs the keys. A general level subscription to MBMS services is not enough.

- *Req-2: The UE needs to know that a specific service uses subscription based key management*.
  This information can be given to the UE in the service announcement. This would imply that all UEs in this service would use subscription based key management. In principle it could be possible that this information is given with the subscription. Subscription could include a parameter whether this UE uses subscription or joining based key management. Then the UE could act accordingly when the service announcement is given out. This way a specific service could include both key management possibilities for different UEs for the same service. (However, it should be noted that subscription mechanisms are out of scope in 3GPP.)

- *Req-3: The UE is able to setup a security association (e.g. MUK) with the BM-SC before joining*[1].
  This is possible since the UE could perform GBA run and establish an SA with the BM-SC, when it has detected from the service announcement that it needs to use subscription based key management. After the MUK has been established, the UE can either request for the keys or the BM-SC can push the keys down to the UE depending on what method is used.

[1] The security association might already be in place if the UE and BM-SC have *some other* active MBMS user service between each other.

2.3 Analysis

The claimed benefit of subscription based key management is avoiding (key delivery) signalling congestion between UE and BM-SC when users start to join the service, for example due to some sudden news. However, it is still FFS if SA4 will define an application layer joining procedure or not. If SA4 will define it, there will be end to end signalling between UE and BM-SC during the joining anyway and the keys could be sent within this procedure. Therefore the benefit of sending keys before the application layer joining could be questionable. If SA4 decides not to define application layer joining procedures, the benefit of subscription based key management seems to be bigger.

3 Conclusions

Based on the analysis above, subscription based key management seems feasible in GBA and MIKEY model if some requirements are met. However, the benefit of it seems to depend on decisions of SA4.

It should also be noted that joining based key management allows both subscription or joining based charging while subscription based key management does not. Thus there seems to be no service reason to use subscription based key management.

4 References

[1] TS 23.246 v 6.3.0, Multimedia Broadcast/ Multicast Service

[2] TS 22.146 v 6.5.0, Multimedia Broadcast/ Multicast Service, Stage 1