3GPP TSG SA WG3 Security — SA3#35 **S3-040805**

October 5-8, 2004

St Paul's Bay, Malta

Title: **Parallel use of MSKs and MTKs**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

According to the current TS 33.246 chapter 4.2 it is unclear if it is possible to have parallel MSKs within a Key Group and further parallel MTKs within an MSK. It is analyzed in this contribution that, since MSK ID and MTK ID are defined as sequence numbers, this does not seem to be feasible.

2 Background

According to 6.3.3.1 of TS 33.246 every MTK is uniquely identifiable by its Network ID, Key Group ID, MSK ID and MTK ID.

From the following statement in 6.4.4 of TS 33.246 it can be concluded that MSK ID and MTK ID are sequence numbers:

> *For messages that contain an MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. The MSK ID and MTK ID* ***are increased by 1 every*** *time the corresponding key is updated.*

The statement in 4.2 of TS 33.246 says:

> *An MBMS User Service may use* ***one or more*** *MBMS Service Keys (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 to secure the different Transport Services that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS Transport Services, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS Transport Services, as specified within subclauses 6.5 and 6.6.*
>
> *NOTE: According to good security practice the* ***use of the same MTK*** *with two different security protocols shall be avoided.*
>
> *For MBMS User Services it shall be possible to share one or more MSKs with other MBMS User Services, since according to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services.*

NOTE: While sharing MSKs among different MBMS User Services, care shall be taken that the Users are not given access to data that they are not entitled to.

3 Analysis

3.1 Problem

The following issues are unclear from the specification text

1. Is it feasible to have parallel MSKs (with different MSK IDs) *within a Key Group* and further parallel MTKs (with different MTK IDs) within an MSK?

2. Is it feasible to use one MSK for several User Services at the same time?

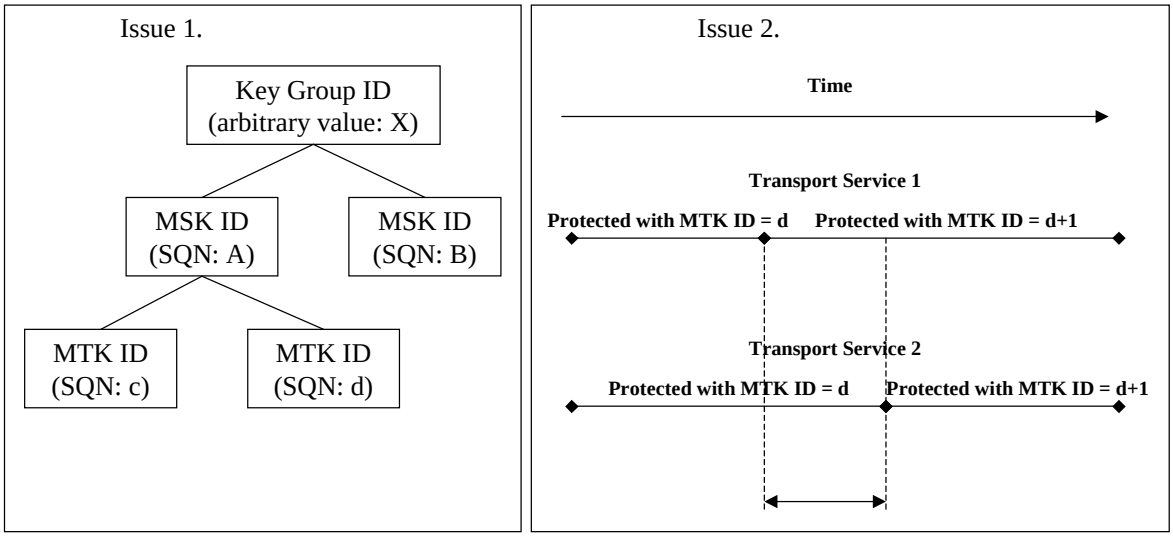

Figure 1. Issues 1 and 2

3.2 Analysis for issue 1

It can be seen that if two MSK IDs *within the same Key Group* are used in parallel with different SQNs, this will not work since the UE will always take the MSK with the larger SQN into use and discard the MSK with the smaller SQN. The same applies for MTKs since the situation is similar. Thus the answer to issue 1 is NO.

It should be noted that the TS specifies the use of several MSKs in section 6.3.2.1.

> *If the UE receives an MSK and already contains two other MSKs under the same Network ID and Key Group ID, then the UE shall delete the older of these two MSKs.*

However, this functionality is assumed to handle synchronisation problems when the MSK is being changed to a new one, and *not* for intentional parallel use of MSKs within one Key Group ID.

The conclusion is that there shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) within a Key Group ID shall not be allowed. This is due to the fact that MSK ID and MTK ID are sequence numbers. I.e. the UE

would discard the MSK/MTK with smaller MSK ID/MTK ID. Of course two parallel MSKs or MTKs are allowed, e.g. in one user service, but only if they have distinct Key Group ID.

3.3 Analysis for issue 2

From analysis of issue 1 it can be seen that using the same MSK for two User Services means also using the same MTK. Note that User Service consists of Transport Services so this problem boils down to question: Is it possible to use one MTK for several Transport Services at the same time? If two Transport Services use the same MTK to protect the traffic, the transport services need to be in synchronisation regarding the use of MTKs with each other. If this is not the case, the UE will drop the traffic with the smaller MTK ID. For example, in Figure 1 the UE would drop the traffic in Transport Service 2 with MTK ID = d, when the UE has started to use Transport Service 1 with MTK ID = d +1. One way to solve this could be that a requirement could be added to the TS that the UE should be able to handle "2 to n consecutive MTKs", but this would still mean at least some synchronisation requirement between the Transport Services or even User Services that are using the same MSK (MTK). This may be very hard to achieve. Thus the answer to issue 2 is NO.

The use of the same MTK with two different transport services (or user services) should be avoided. This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic. I.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

4 Conclusions and proposal

The conclusion is that:

- There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs or MTKs within a Key Group ID shall not be allowed as this will cause synchronization problems in the UE due to the fact that MSK and MTK are identified by sequence numbers

- The use of the same MTK with two different transport services (or user services) should be avoided. This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic. I.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

The accompanying CR implements the change in the TS.

5 References

[1] TS 33.246, Security of MBMS