3GPP TSG SA WG3 Security — S3#33 **S3-040380**
10 - 14 May 2004 *(commented by AXALTO)Comments by Ericsson*
Beijing, China

Agenda Item: MBMS
Source: Ericsson

Title: Joining based key management

Document for: Discussion /Decision

1. Introduction

In SA3#32 the following statement was made [1] on the OTA based key management:

It is to be noted that the management of BAK/TGK[1] is a subscription data management not necessarily linked to the MBMS joining procedure. In other words, the operator may perform MBMS key management operation even if the MBMS subscriber has not implicitly wished to join to a particular MBMS service at this time. In that case, the PTP BAK/TGK management should enable a smart planning in time by the Operator previously to the effective new BAK/TGK is used. Is to be noted that this planning may be based in parameters that are only known by the Operator (e.g. network congestion). "

This contribution discusses issues that arise if key management is based on subscription and not on user's explicit joining.

2. Discussion

First, the above statement that key management is subscription data management and not joining based data is against the following requirement in TS 33.246 [2]:

R5d: Only authorized users that have joined an MBMS multicast service shall be able to receive MBMS keys delivered from the MBMS key generator.

This requirement was introduced when decision on two-tiered model was not yet taken. Anyway, it should be clarified further. If "MBMS keys" means MTKs (or any key material needed to perform MTK derivation) then requirement is fulfilled even if MSKs are delivered before/during/after the joining. Else, if MBMS keys mean MSK, joining procedure and MSK delivery are then linked.

<Ericsson> SA3 may need to clarify the requirement. Anyway, the MSK is the main input to MTK derivation. If the user does not have the MSK, he is not able to derive the MTK either. Also, unauthorized users are able to receive "any key material needed to perform MTK derivation" since it is sent in multicast, except for the MSK. Therefore it seems logical that the requirement refers to MSK.

Secondly, if the MSK of a specific MBMS service has been delivered to the UICC before the user has joined the MBMS service, how does the UICC know when it is allowed to derive MTK from the MSK and provide the MTK to the ME? Let's reformulate the question:

What if an operator wants to deliver an MSK today and he does not want his subscriber to use it until next month? What does the Operator do?

<Ericsson> Please don't change the question. Your question assumes that the operator knows when the user will join the service. Isn't the user then allowed to join the service whenever he wants to? The original problem still exists: If the MSK has been delivered to the UE and then the user makes an ad-hoc joining to the service, how does the UICC know when it is allowed to derive MTK from the MSK and provide the MTK to the ME?

There are two easy solutions:

[1] It should be noted that the BAK/TGK is called MSK according to new key terminology specified in TS 33.246.

1- The Easiest one: Operator does not use MSK until next month.
2- Putting and MTK_SEQ (Sequence number) in the UICC corresponding to the first SEQ used in the next month traffic (to be noted that this enables interesting charging mechanisms based in “partial” key delivery)

Why this complicated "explicit point-to-point indication" is then proposed?

<Ericsson> Refer to the answer above.

One alternative could be that a key lifetime is associated with the MSK when the MSK is delivered to the UICC before joining. This lifetime would indicate to the UICC when it is allowed to derive MTK from the MSK. However, this kind of lifetime is useless since the UICC does not know if the user will ever join the service.

This means that the UICC requires an explicit point-to-point indication from the network to know when the user has joined the service. **It can be seen that MSK key management procedure before joining the MBMS user service is pure overhead since point to point signaling is needed anyway when the user joins the MBMS user service, therefore the latter signaling could be used for actual MSK delivery as well**.

If the UICC does not require an explicit authenticated indication of user’s joining from the network, there are two possible actions for the UICC:

- either the UICC will never derive MTK from the MSK and provide the MTK to the ME
- the UICC might derive MTK from the MSK and provide the MTK to the ME even though the user has not joined the specific MBMS user service. In this case the ME could reside in a cell where the MBMS user service is transmitted and request the UICC for the appropriate key derivation based on MSK. The user would get service for free which is against the requirement above

??? Two-tiered approach is based in frequent renewals of MTK to avoid the attack that is being described.

<Ericsson> The bullet points above describe the alternatives for UICC if the UICC does not get any explicit authenticated indication of user’s ad hoc joining to the service.

As can be seen neither of these actions are acceptable so an explicit point-to-point authenticated joining indication from the network is required for OTA model to work.

As seen in previous comments no complicated "explicit point-to-point indication" is needed.

<Ericsson> Refer to the previous comments: Without the indication the UICC has no knowledge of user’s ad hoc joining.

3. Considerations on OTA model

Double signalling
Based on the analysis above it can be stated that subscription based MSK key management requires *double signalling* to the UICC, since (in addition to key delivery before joining the MBMS user service) explicit authenticated point to point signalling is needed to indicate to the UICC that user has joined the MBMS user service and that the UICC is allowed to derive MTK from the MSK and provide the MTK to the ME.

As seen in previous comments no complicated "explicit point-to-point indication" is needed, neither is double signaling.

<Ericsson> Please refer to previous comments.

Joining without subscription
In SA3#32 a service scenario was raised where users could join a specific MBMS service without prior subscription. Since OTA model seems to be based on user’s subscription, it is unclear whether OTA model can support this kind of service scenario, where key management is based solely on joining the MBMS user service and not on subscription. This has not to be confused with any MBMS subscription information that is available within the HSS for the purpose

of indicating to the BM-SC that the user is authorized to join any MBMS user service. This kind of MBMS subscription in the HSS is one thought to be on a very general level. The BM-SC would handle the more fine-granular adhoc subscription which is actually joining the MBMS user service. Admitting that this scenario is defined in SA1, it is completely possible that the joining to that MBMS service may trigger MSK update using OTA.

<Ericsson> OTA model has not defined any methods for user's joining to the service (with or without subscription).

Surviving unplanned joining signalling
OTA servers typically have been designed to handle subscription data management that is not bursty in nature and usually can be planned in advance. Therefore it should be studied whether OTA servers can meet the performance requirements of dynamic and bursty traffic loads that may result when sudden news arise and large amounts of users try to join the MBMS user service simultaneously. This unplanned joining signalling may result from either key delivery signalling or joining indications that seem to be required for subscription based key management. OTA Servers are already dimensioned for application downloads, browsing or backup STK applications (for instance) that handle much more data than the needed for MSK management. Anyway, one of the advantages of the two-tiered approach is that it enables planning in advance of MSK updates.

<Ericsson> OTA has not solved the problem how to indicate to the UICC that the user has made an ad hoc joining to the service. Please refer to the main issue in this contribution.

To be noted that the unplanned joining scenario described is much more critical in the GBA/MIKEY approach because the data overhead is much bigger (~20 times) (S3-040249)

<Ericsson> Please refer to the comment contribution of S3-040249, which indicates that 249 was not comparing the same functionality.

Home environment based key management
The OTA model may also introduce a bottleneck in the HN OTA server as is described in more detail in [3].

Are not this "bottleneck" also applicable for BSF in the Home Network for GBA/MIKEY proposal?

<Ericsson> The MBMS key management in combined model is in VN. The GBA is not part of MBMS key management.

4. Proposal

It is proposed that SA3 endorses a solution where MSK key management is joining based activity such as GBA with MIKEY, and not based on a static subscription data management such as OTA model.

It can be an operator policy to deliver the MSKs of certain services once the user has first join them (i.e. MSK update triggered by joining). **Both proposal on key delivery (GBA and OTA) can certainly do that**. However, mandating this mechanism will certainly reduce the advantages of the two-tiered approach:

-planning in advance: Operators can decide to update keys when the network is less charged (e.g. at night)

-Reducing overload in simultaneous joining: If joining is the triggering event for MSK updates, simultaneous joining of many users will certainly be hard to achieve due to excessive network resource consumption in key delivery.

<Ericsson> It still needs to be addressed how the how does the UICC know when it is allowed to derive MTK from the MSK and provide the MTK to the ME?

-provisioning: You can have MSKs securely stored in the UICC for a long period of time before usage (even at personalization stage), reducing the cost on network resources and reducing the time needed for introduction of a new MSK. Moreover it is possible to have a set of MSKs for the same service that will be used as an effective counter attack measure to dissuade frauds.

However, if OTA model is considered, the following concerns should be addressed:

- subscription based MSK key management requires *double signalling*
- it is unclear whether OTA model can support this kind of service scenario, where key management is based solely on joining and not on subscription.
- it should be studied whether OTA servers can handle dynamic and bursty traffic loads that may result when sudden news arise and large amounts of users try to join the service simultaneously.
- OTA model may introduce a bottleneck in the home environment since the key management of each *local* MBMS service from *every* visited network *uses the resources of the home environment* OTA server

5. References

[1] TD S3-040051, Discussion paper on MBMS key management, SA2#32, Axalto et al

[2] TS 33.246 v 1.1.0, Security of Multimedia Broadcast/Multicast Service,

[3] TD S3-040222, MBMS: Key distribution architectures analysis, SA2#33