3GPP TSG SA WG3 Security — S3#32 **S3-040051**
09 - 13 February 2004
Edinburgh, Scotland, UK

Source: **Axalto, Gemplus, Giesecke & Devrient, Oberthur**

Title: **Discussion paper on MBMS key management**

Document for: **Discussion and decision**
Agenda Item: **6.20**

1 Introduction

At the SA3 # 31 meeting a decisions was taken to base the key distribution in a two-tiered approach where MBMS data encryption keys (SK or TEK) are derived from a master key (BAK or TGK) which is stored in a secured way. A questioned compromise concluded in providing the so-called "UICC solution" and the "ME solution" for MBMS key management in Rel-6.

On the other hand, at SA#22 it was reminded that options should be minimised for ease of implementation and interoperability. SA3 was explicitly encouraged to take this remark into account in the final solution.

To help SA3 in their decision, this contribution explores some open issues linked to some of the proposed options.

2 GBA & MIKEY based management procedure

This section summarizes some concerns derived from the usage of a key management procedure based in GBA and MIKEY. These open issues are based in the descriptions contained in the following contributions: [S3-030751], [S3-030723], [S3-030368] [S3z030027] and [S3-030368]

New required Network Entity: Using keys derived from GBA to authenticate and secure the BAK/TGK transfer (or any other needed subscription information) requires that any BMSC interfaces with the Home Network BSF. This dependence precludes access to MBMS services for subscribers of PLMNs which not have this Rel-6 new network functionality, adding an additional network entity to the requirements for supporting MBMS.

Roaming case: Additionally, since the key material derived in GBA providing authentication between the BMSC and the UE is not linked to a specific management action, the visited BMSC gains full control of the key management procedures enabled in MIKEY exchange.

In other words, if the visited BMSC is enabled to provide MBMS services to a subscriber in roaming, he is also enabled to modify any key management data stored in the UE. (e.g. BAK keys of any subscribed MBMS service). This has two major concerns:

-The Home Network is no more aware of the specific MBMS data contained in the subscriber UE. The subscriber may subsequently need to renew all the MBMS related data in the UE when returning to the HPLMN.

-Visited PLMNs may compete for the same storage place in the UE MBMS containers. To be noted that this is especially critic when subscriber in roaming changes between different PLMNs in the same area to obtain access to MBMS services.

Solutions to limit the control of UE MBMS management data by VPLMNs BMSC are hard to achieve, as they need to link the GBA derived keys with a specific MBMS context to enable the VPLMN to manage a subset of MBMS bearer services and not all of them.

Roaming case 2: Contribution S3-030723 on “UICC based MBMS Key management with MIKEY”from Ericsson proposes a mechanism for using MIKEY for the MBMS key management to the UICC. In that scenario, BAK/TGK keys are encrypted with a RK/KEK which is pre-provisioned to the UICC. Again, the way that the Visited BMSC gets knowledge of this KEK is not described and seems not compatible with the control of the UICC by the Home Operator and hard to make compatible with BAK/TGK confidentiality between Home and Visited BMSC.

Mobile centric solution:

GBA requires the usage of HTTP Digest AKA over Ub interface. Additionally, it has been suggested that the BMSC acting as a NAF will encapsulate MIKEY message in GBA protected HTTP Responses. In both cases, the initiative to start the rekeying procedure corresponds to the terminal.

In the general case of advanced/planned key updates, the network should then provide and additional “key availability message” to the terminal. If it is done in Point To Multipoint (PTM) way, the system may become more complex including some kind of “Availability Time” to disable the risk of network congestion following multiple ME asking for the keys at the same time. On the other hand, the alternative of sending a PTP “key availability message” seems to contradict the principles of MBMS on making efficient usage of the radio spectrum. In effect, the alternative of directly providing the key update message by a PUSH mechanism (e.g. by OTA) seems much simple and makes this message not required. Alternatives of carrying MIKEY on other protocols (e.g. SIP) enabling PUSH have been evoked but seem not simple to be put in place for Rel-6.

It is to be noted that the management of BAK/TGK 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).

The decision to ask for a new key should not be terminal originated in the general case. However a mechanism to ask for keys (e.g. when subscriber loses a rekeying procedure) is to be defined.

Support of Subscription Management Operations: There is no mechanism provided by MIKEY to perform other subscription management procedure than BAK/TGK update. In other words, the BMSC does not own a complete control of BAK/TGK stored in the UE. For instance, ways to stop a subscription when a subscriber ends/exit a MBMS subscription requires a key renewal process to all MBMS subscribers of this MBMS service.

MIKEY currently does not support these mechanisms.

Key Management to the UICC:

No detailed description on how to include Key Management commands targeted to the UICC in MIKEY. Though it seems possible to define new parameter in MIKEY IETF draft, it seems a complex way in order to achieve Rel-6 timeframe.

From S3-030723: “Ericsson is in the process to further enhance MIKEY based on received feedback from IESG review. This gives us we believe a small window of opportunity to further enhance MIKEY to consider also MBMS requirements. However Ericsson is not in the position right now to signal how easy this is from an IETF point of view but Ericsson will report the progress and the general enhancement work on MIKEY.”

Additionally, this approach requires the definition of a new command in the ME-UICC interface which has been considered unnecessary in the last T3 MBMS ad-hoc [T3z040010] as existing mechanisms for delivering keys to the UICC are available from Rel-99 providing all the required functionalities.

Note: the only change required by UICC-based solution consists in modifying slightly an existing command for key derivation in the UICC (to retrieve SK/TEK).

IETF Draft Status: The decision on using an IETF draft instead of existing 3GPP standards to perform MBMS key management has not been sufficiently justified in terms of additional functionalities that it provides.

A justification in using this new procedure instead of reusing existing 3GPP mechanisms should in any case be justified, taken into account what are the new functionalities it provide, the new network entities that are involved, and the new protocols to be defined.

3 BAK/TGK Key storage in the ME

The following section summarizes some concerns derived from the storage of a BAK/TGK keys in the ME.

ME revealing the BAK: The ME is considered not trusted in keeping the secrecy of BAK/TGK while the two-tiered approach is based in the guarantee of this secrecy.

Secure portability of MBMS keys: If BAK/TGK are stored in the ME, the link between the MBMS data and the subscription is not assured:

- The ME should erase MBMS subscription related information when the subscription changes (e.g. the user changes its USIM from one terminal to another). Again, the ME is not trusted to do that. One consequence is that a fraudulent user could use the same account to ask for BAK keys in different terminals.

- Additionally, a subscriber who changes his terminal should renew all BAK/TGK keys linked to this subscribed MBMS services.

MBMS Parameters Storage In the ME solution, key storage is not performed in a standardized way which may difficult the maintenance operations when different proprietary mechanisms are involved. Solutions as Device Management seem to be difficult to achieve for Rel-6 timeframe.

4 Co-existence of Solutions

Capabilities detection: If both solutions are present, the BMSC shall be informed of the UE capabilities i.e. ME or UICC MBMS capable. However, no mechanisms are yet defined for that. The optional solutions in a streaming one-way environment result in problems to manage them securely. If the keys are provided to the ME as well as to an UICC based solution the provider does not know where the key is really stored at the end. Moreover, the roaming case seems more difficult to be taken into account since some operators may mandate UICC-based solution.

Standardization options: 3GPP SA has implicitly encouraged SA3 to avoid options. From 3GPP SA# 22 draft meeting report:

> **[...] It was clarified that the use of the UICC-based solution had been discussed in SA WG3 and a UICC-based solution could offer a higher security and low impact on network resources, some companies thought that there was some risk in meeting the Rel-6 timescale if it was restricted to a UICC-only based solution. This position may be reviewed if the assumption of completing the MBMS specification work for March 2004 was found to be unnecessary and a later completion date was agreed upon in 3GPP. Several operators expressed a preference for the UICC-based only solution. The TSG SA Chairman asked whether any operators would reject the UICC-only proposal on the grounds that a next-generation UICC is required and there was no objection indicated. It was commented that the Options for implementation should be kept to a minimum for ease of implementation and interoperability. Members were asked to contribute to SA WG3 on this and TSG SA requested that SA WG3 also consider their request that the final solution should not include any options [...]**

-SA1 #23 has also rejected the need to address the backward compatibility problem of pre-Rel6 UICC considering that the problem will be minimised using USAT. From SA1# 22 S1-40263 draft meeting report:

> **[..] A CR to 22.146 (S1-040050) proposed a requirement that " MBMS shall be accessible independently of the smart card being used in UE i.e. pre-release 6 UICC."**
> **The CR was rejected, based on the understanding that it would be possible to access MBMS with pre-release USIMs using USAT. The requirement would contradict the task given to SA3 to design a "zero option solution" for MBMS security [...]**

5 Conclusion

Taken into account the previous analysis, it is considered that too many drawbacks are present in using GBA&MIKEY solution. The alternative which is considered reuses existing OTA key management procedures, already standardized from Rel99, fulfilling the requirements for MBMS key management and using existing and already deployed infrastructure and procedures (see 3GPP T3 MBMS ad-hoc meeting report T3z040010). The work in T3 is nearly finished and ready for approval in Rel-6 timeframe.

On the other hand, it seems no more justified the need of a combined solution according to SA#22 and SA1 #23 meeting discussion:
Taken all this into considerations, this contributions proposes that:

- Only UICC solution is addressed in Rel-6 timeframe.

- Existing OTA mechanisms are used for MBMS key management.