3GPP TSG SA WG3 Security — S3#32 **S3-040111**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: **6.20 (MBMS)**

Source: **Ericsson, Nokia, Siemens**

Title: **Comments on S3-040050/51: 'UICC based MBMS key management'.**

Document for: **Discussion and decision**

1 Introduction

Contributing companies agree with the SA#22 statement that 'options should be minimized for ease of implementation and interoperability'. This can certainly be done in several ways. One possibility is to drop the ME-based solution as is favoured by the analysed paper [S3-040051]. Another one is to drop the UICC-based solution. But there seem to be usecases justifying both solutions. Therefore a third possibility at hand is to try to harmonize the protocols and handling towards the terminal and UICC i.e. go for a single network view. This contribution provides comments on the 'concerns' listed within [S3-040051] against the 'GBA-based key management approach' for MBMS.

2 Analysis of S3-040051/50 claims

The claims have been structured in categories to allow a structured discussion during the meeting. The *italic* text has been copied from the commented contributions.

1) <u>General claims</u>

1.a) Requiring new network entities [S3-040051]

"*<u>New required Network Entity:</u> 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.* "

The introduction of MBMS requires that the operator has to upgrade his Radio, as well as Core Network elements. Whereas the use of GBA-servers by the operator is introduced as part of other Rel-6 features, the availability of OTA-servers also cannot be assumed. Operators, that currently do not have OTA-servers, will be required to invest too. The claimed dependence on HN functionality also applies in case of OTA: a roaming subscriber will not be able to use MBMS services in a VN if the HN does not support OTA. But in that case it would be very probable that the HN operator would not allow the user to use MBMS services in the VN.

Within [S3-040050], a **new** network entity seems to be proposed: '*A **Trusted Third Party:** This entity is present to address the case of MBMS roaming agreement where the Visited Network wants to keep secret its BAK values'*. Neither SA3, nor SA2 have discussed the introduction of such a network element within the MBMS-architecture. A problem statement related security solution analysis is missing to be able endorse the need for a TTP now by SA2 and SA3. The flows of [S3-040051] already indicate that it requires a lot of new key management messages. Also similar as with 1.b) these interfaces need to be standardized!

1.b) Standardizing interfaces [S3-040050]

'The interface between the Home BM-SC and the OTA server is proprietary and operator dependent'
Contributing companies do not agree with this proposed way forward as both BM-SC and OTA-servers may be delivered by different vendors. The required security for the interface between the OTA-server

and the BM-SC would be equivalent as for the BSF to BM-SC. SA3 needs to specify the security requirements for this interface.

"Interface *between the BM-SCs shall be standardized independently of the chosen solution, since it is necessary for MBMS roaming. This interface is used to transfer data such as the "MBMS Admin data" present in the MBMS administrative procedures described further."*

No requirement for an interface between the BM-SCs should exist as both home BM-SC and visited BM-SC provide services independently of each other".

2) Security related claims

2.a) UICC Access control [S3-040051]

"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."

Siemens contribution [S3-040098] to this meeting has made similar observations to the OTA framework. This should therefore be translated into a requirement that keeps the keys and access for MBMS related updates to the UICC card completely separate from the other UICC-data access. SA3 needs to define the requirements for access control and then evaluate how this translates to the SA3-proposals.

2.b) Support of subscription management operations [S3-040050]

'MIKEY currently does not support these mechanisms.'

This is true for the current draft-RFC (draft-ietf-msec-mikey-08.txt). Mobile specific optimizations need to be added to this and including key management operation could be accomplished too. But first let us clarify and agree on the exact requirements for such operations within SA3 and include them (when acceptable) within TS 33.246. The Subscription Management operations have been introduced by some companies within T3 but the requirements for it have never been introduced within SA3-specification.

The use of a registration key:

An equivalent issue is the use of the key RK (Registration Key). The requirement within TS 33.246 that necessitates such a key is unknown and its apparent advantage is not clear. This seems to be a misalignment between T3 and S3. The use of a registration key introduces an additional layer of keys. The OTA message itself would be secured by OTA specific keys, and the 'BAK' be encrypted by the RK.

2.c) Key management to the UICC [S3-040051]

'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.'

It seems to be true that any modifications to MIKEY might be difficult to achieve in IETF in Rel-6 timeframe. This has been acknowledged in both Ericsson contribution [S3-040059] and in Nokia contribution [S3-040081]. Therefore both of these contributions propose that it may be necessary to specify the modifications to MIKEY in 3GPP.

Extract from [S3-040059] from Ericsson:

"However, the timeframe of release 6 might not allow for new standards track RFC to be written. Therefore Ericsson proposes that the needed extensions to MIKEY should be specified in 3GPP."

Extract from [S3-040081] from Nokia:

"MIKEY MBMS extensions are published as an Informational RFC. If it impossible to publish RFC in time then required enhancements are incorporated into relevant 3GPP specifications."

2.d) IETF Draft Status [S3-040051]

'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.'

Overlapping work between standardization organizations should be avoided. Instead alignment with and re-use of other standardization organizations' work can be regarded beneficial from business point of view and it also saves resources. Using MIKEY in MBMS intends to align multicast work done in IETF and in 3GPP. The alignment of MBMS security and IETF MSEC work has been discussed earlier in [S3-030368]. It should be noted that as a part of multicast alignment SA2 has re-used IETF multicast functionality by implementing the IGMP/MLD messages.

It should be noted also that MIKEY draft has been approved to be an IETF RFC, see [S3-040057].

3 Conclusion

This contribution has shown that the concept that has been developed by T3-adhoc [S3-040050] is not in sync with the SA3-requirements. Furthermore it has been shown that the listed claims made against the concept using GBA are unfounded. The claim within the conclusion of [S3-040051] that the work is nearly finished is therefore misleading. In order to avoid that T3-work further deviates for the SA3-requirements/working assumptions a list of misalignments should be sent to T3.

4 References

[S3-030368] Ericsson: Introducing SRTP and MIKEY in TS 33.246

[S3-040050] Axalto, Gemplus, Giesecke & Devrient, Oberthur", MBMS UICC based solution.

[S3-040051] Axalto, Gemplus, Giesecke & Devrient, Oberthur", Discussion paper on MBMS Key management.

[S3-040057] Ericsson: Status of SRTP and MIKEY in IETF

[S3-040059] Ericsson: Enhanced MIKEY in MBMS key management

[S3-040081] Nokia: Use of MIKEY in the combined method.

[S3-040098] Siemens: OTA security considerations