3GPP TSG SA WG3 Security — S3#31 **S3-030699**
18 - 21 November 2003
Munich, Germany

Agenda Item: 6.20 (MBMS)

Source: Siemens

Title: MBMS UICC open issues

Document for: Discussion/Decision

1. Introduction

At the SA3 meeting in Povoa no decisions where taken on a key distribution protocol. Especially many open issues were listed towards a UICC based solution. This contribution provides in section 2 a list with open issues (some can be seen as disadvantages on particular solutions) that are available from previous discussions with the aim to be useful to SA3 to check the maturity and feasibility of the different solutions at the moment that a decision is taken. It should be recognized that this list may need to be updated if contributions with suitable solutions or additional issues are provided to this meeting.

2. Solutions for updating keys to the UICC

This section discusses the alternative protocols to transport a Key Encryption Key (KEK) or BAK to the UICC. The alternatives proposals as known from the last SA3 meeting are: OTA, MIKEY and GBA-based protocols. As OTA has been designed for use with UICC it is not a candidate for transferring keys to the UE in terminal based MBMS-solutions. The addressed issues below are typical for a UICC based solution.

2.1 OTA

1-1. The requirement for acceptable on-time deliveries of UICC-keys to late MBMS-entrants are unknown. Stringent time settings could be a problem for OTA.

S3-030583 to SA3#30: "*The use of OTA may cause delays in initial keying or re-keying.*
Secure OTA uses secured SMS messages. The transport of SMS has no real-time constraints but uses a push and forward mechanism in the network. If an MBMS user wants to join an already ongoing service then it is unacceptable to receive the BAK/TEK many minutes later. If the delivery latency is low and kept within know acceptable time boundaries then this would pose no problem."

1-2. No solutions (i.e. selected protocols) are yet available for connection OTA-servers to MBMS-server that reside in the VN.

S3-030583 to SA3#30: '*The OTA encryption method may be operator specific which limits the use of updating UICC information to HN-services.*
The used encryption algorithm within OTA is either proprietary, DES or 3DES. In case only an operator specific algorithm has been pre-configured on the card this poses a problem while within the MBMS model the user shall be able to obtain services from the VN. This will require that HN OTA-servers shall be involved even for MBMS services provided by a visited network".

1-3. The use of OTA needs to be supplemented by a terminal mechanism that requests key updates.

S3-030583 to SA3#30: *"Such a mechanism is necessary to allow the terminal to re-synchronise keys after detecting that it has missed a key update. This functionality need to be implemented in the terminal as the UICC is a passive actor. This is not a disadvantage of OTA but due to the UICC characteristics. "*

1-4. No estimations of the moderate free memory amount of existing pre Rel-6 UICC in the field is available.

S3-030534 to SA3#30: "*Additionally, the free memory required for this pre-R6 MBMS application is estimated being less than 1 Kbytes, **probably** fitting in most of the existing UICCs, but again considered as an operator's deployment matter*."

2.2 MIKEY

This open issues section assumes that the MIKEY protocol would be implemented at the UICC.

2-1. No solution for key deletion to the UICC is provided.
S3-030511 (LS from T3) to SA3#30: lists a BAK-deletion function. It is yet unclear what protocol shall be used for this and if such a function is needed as *NO requirement* for it has been listed in TS 33.246 (S3-030517).

2-2. No solution to bootstrap the MIKEY-run (the KEK-generation) is provided.
S3-030583 to SA3#30 *"But in order to bootstrap this E2E transport, the sending entity and the UE need a shared secret which may be supplied by a GBA-run."* This is the so-called generate-KEK step.

2-3. No detailed estimation of the complexity of terminating MIKEY at the UICC is available.

Solutions may be possible that MIKEY is implemented on the Terminal for the ptp key delivery but the 'generate-KEK step' is provided by either OTA or GBA or other mechanisms. In such a case an interface between MIKEY and the UICC has to be developed which details are yet unspecified.

2.3 GBA

3-1. No detailed solution for terminating GBA securely on the UICC has been provided.

3. Conclusion

Without significant progress on the issues highlighted in section 2 of this contribution, a decision in this meeting in favour of a UICC-based solution within Rel-6 should not be made. Also the requirements on UICC-based solutions shall be verified on completeness and stability before going further in that direction.