3GPP TSG SA WG3 Security — S3#32 **S3-040099**
9-13 February 2004
Edinburgh, UK

Source: **Siemens**

Title: **Proposed terminology for MBMS keys**

Document for: **Discussion and decision**

Agenda Item: **6.20 (MBMS)**

1 Introduction

This contribution proposes to agree on the naming of the keys that are used for protecting the MBMS streaming data. In the past the same name (e.g. KEK used within ptp or ptm-delivery) was used for keys in another context, as well as the case where a key with a certain function had many different names (TEK and SK; BAK and TGK) throughout the various company contributions. This led sometimes to misunderstandings in the technical discussion.

2 Overview of used terminology

SA3#31 did agree on following working assumption (extracted from the Report):

"*It will be possible to run the whole MBMS security with ME only, but will also be possible to run key management using the UICC. A migratory path between the two solutions is needed and the solutions will be developed to allow this. Deviations between the two solutions would only be made for the benefit of the whole system (this implies the use of a 2-tiered system). The difference between the two solutions for delivering the low-level keys would be visible only inside the UE and secondly, the BMSC would know which solution is implemented in the UE side. A Rel-6 compliant UE will support both UICC based and ME based solutions and the Operator will have control over the choice of method used for MBMS services.*"

This has introduced a 2-tiered key system and again new names for the MBMS keys. A definition of these keys is missing (e.g. what is the high and what is the low level key ?). Furthermore, the latest version of TS 33.246 (SP-030586) does contain many names for keys used within MBMS.

- The requirements part of the specification uses 'MBMS keys'. See mainly Clause 4.1.4 on 'Requirements on MBMS Key Management'.
- Stage 2 part of the specification (Ex. Clause 6.1 and 6.3) use High Level key and Low level Key.
- The threat section (Annex B) uses 'encryption keys'.

Within Company contributions to the last meeting various naming have been used when proposing stage 3 solutions (some examples: BAK, TEK, KEK, SK, TGK). Without any agreement on exact key names and definitions, the TS will end up with a mixture of names. It is therefore proposed to define suitable MBMS key names within SA3#32 meeting.

There seem to be three options:

A) Define own 3GPP key terminology

This could be the compromise if the proponents of IETF or 3GPP2 based Stage-3 naming cannot agree to go for option B respectively option C. The use of 'high level' and 'low level' key provides already an abstraction of the used keying names as for option B and C.

B) Strive for harmonization of terminology with IETF

Contributions proposing SRTP and IETF protocols did use IETF based naming (TGK, KEK, TEK).

C) Strive for harmonization of terminology with 3GPP2

Contributions proposing UICC based key management did mostly use BAK and SK as the initial concept was based on 3GPP2 model.

It is proposed to define own 3GPP terminology to get an abstraction on the used stage 3 protocols (different for download and streaming) for the different MBMS User Services. It also allows avoiding implicit characteristics assignment as is the case for BAK. The key BAK has always been used as a key that is stored on the UICC, but now SA3 have agreed to adopt the same two-tiered model for ME and UICC based Key management.

Option A is preferred by Siemens as it allows making abstraction of the Stage 3 realization. The proposal made in section 3 does implement this.

3 Pseudo-CR text for new terminology

This terminology should at the same time apply to all MBMS user services that are possible over MBMS ptm links. Three Service types have been defined within TS 22.246 User Services: Download, Streaming and Caroussel.

It is proposed to change the title of clause 3 to 'Definitions and abbreviations' and to include a section 3.1 on 'Definitions'.

3.1 Definitions

MMK= MBMS Master Key: The MBMS service specific key that is securely transferred from the BM-SC towards the UE. This key may be stored within the ME or the UICC depending on the MBMS service. For MBMS Streaming the MKK is not used directly to protect the MBMS data (See MSK).

Editors Note: How the MKK is used for download is still under study.

MSK = MBMS Session Key: A Key that is obtained by the UE by calling a function fx (MKK, Key-deriv parameters) that may be realized on the ME or the UICC depending on the MBMS-service. The Key MSK is used to decrypt the received MBMS data.

Editors Note on MKK and MSK: These definitions are subject to further modification as two alternative two-tiered keying systems are still under consideration a) the SK_RAND model b) the key encryption model. For Case a) fx may be a PRF (hash function) while for case b) an encryption algorithm is needed. Key-deriv will be RAND for case a). For case b Key-deriv will be a MSK encrypted with MMK.

Further corrections throughout TS 33.246 have to be made and are left to the Editor to complete.

4 Conclusion

Siemens proposes to adopt the above proposed terminology and to inform T3 of the adopted naming.