3GPP TSG SA WG3 Security — SA3#37 **S3-050046**
February 21-25, 2005
Sophia Antipolis, France

Source:	Nokia, Siemens
Title:	ME based MBMS key derivation for ME based MBMS key management
Agenda item:	6.20
Document for:	Discussion/Decision

1 Introduction

The current MBMS specification [1] lacks the key derivation details when the UE is equipped with a UICC that does not support MBMS key management functions (i.e. a GBA_U-unaware UICC has been inserted). In this case, both the MRK and the MUK must be derived from the single NAF specific key Ks_NAF as specified in TS 33.246 [1]. This paper discusses the possible methods to derive the needed MBMS keys and proposes a way forward.

NOTE: To remind the reader, in the GBA_U-aware UICC case, the MRK and the MUK have been defined to be as follows (see TS 33.246 [1], clause 6.1):

MUK = Ks_int_NAF

MRK = Ks_ext_NAF

2 Discussion

Two alternatives can be identified that can be used to derive the MRK and the MUK from the Ks_NAF:

1. Ks_NAF which is 256 bits long can splitted in a way that the first 128 bits form the MRK, and the latter 128 bits form the MUK.

2. A key derivation function with Ks_NAF and some other input parameters can be used to form the MRK and the MUK.

The option 1 results in keys that are only 128 bits (with GBA_U, key lengths will be 256 bits; Ks_ext_NAF and Ks_int_NAF both have a bit-length of 256). As a consequence the MBMS implementations in both the UE and in the BM-SC would have to take into account that the input key lengths for ME and UICC based MBMS key management differ. An additional key derivation step would be needed to enlarge the key again to 256 bits. Splitting the key into two halves before enlarging a part of it also reduces the resulting key entropy. Therefore, it is preferred to use a key derivation method that works on the full Ks_NAF. Also giving MIKEY a MUK of length 128 bits violates with the HMAC SHA-1 (RFC 2104 [3] (see section 2)) rules which recommends that the minimal key length should be the length of hash function output, i.e. in the SHA-1 case this is 160 bits.

As a consequence only option 2 remains possible. Several variants for key derivation are possible which need to be designed according to following requirements (ensure key separation):

- A compromise of the key MRK should not lead to a compromise of the key MUK and vice versa.

- Needless key derivations should be avoided.

MIKEY [4] performs a key derivation on the key MUK to obtain an integrity and an encryption key (see section 4.1.4 of [4]).

Amongst others, following key derivation variants seem to comply with the above mentioned requirements:

Variant-1:
ME based key management:
MUK = Ks_NAF

MRK = KDF(Ks_NAF,"mbms-mrk")   (derived in ME and BM-SC)

UICC based key management:
MUK = Ks_int_NAF
MRK = Ks_ext_NAF

Variant-1 has the following advantages: For UICC based key management no extra derivations are needed, for ME based key management a simple MRK key derivation function is used.

Variant-2:
ME based key management:
MUK = Ks_NAF
MRK = KDF(Ks_NAF,"mbms-mrk")   (derived in ME and BM-SC)

UICC based key management:
MUK = Ks_int_NAF
MRK = KDF(Ks_ext_NAF,"mbms-mrk")   (derived in ME and BM-SC)

Variant-2 has the following advantages: the MBMS client and server handling is kept similar concerning key derivation for UICC and ME based key management.

As an alternative to Variant-1 and -2, further input parameters could be added to the generic KDF input (e.g. B-TID, NAF-ID). However, it is proposed to use the KDF only with the label parameter as the parameters mentioned above were already used as input to derive Ks_(ext/int)_NAF.

3 Conclusion & Proposal

SA3 needs to make decision how the MRK and the MUK are derived from GBA's Ks_NAF in the case of ME based Key management.

We propose that for ME based key management a simple MRK key derivation function is used: The Variant-1 using GBA's key derivation function (see TS 33.220 [2], Annex B):

MRK = KDF (Ks_NAF, "mbms-mrk")

MUK = Ks_NAF

This approach has been implemented in the accompanying CR to TS 33.246.

References

[1] 3GPP TS 33.246: " Security; Security of Multimedia Broadcast/Multicast Service".

[2] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[3] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[4] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".