**3GPP TSG-SA WG3 Meeting #37**
**Sophia Antipolis, France, February 21-25, 2005**

***Tdoc ⌘S3-050047***

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **33.246** | **CR** | **035** | ⌘ | **rev** | **-** | ⌘ | Current version: | **6.1.0** | ⌘ |

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Proposed change affects:*** | UICC apps⌘ | X | ME | X | Radio Access Network | | Core Network X |

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | ME based MBMS key derivation for ME based MBMS key management | | |
| ***Source:*** | ⌘ | Nokia, Siemens | | |
| ***Work item code:*** | ⌘ | MBMS | ***Date:*** ⌘ | 14/02/2005 |
| ***Category:*** | ⌘ | **C** | ***Release:*** ⌘ | Rel-6 |
| | | *Use <u>one</u> of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | *Use <u>one</u> of the following releases:*<br>*Ph2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)*<br>*Rel-7 (Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | The details how MRK and MUK are derived for ME based MBMS key management are missing |
| ***Summary of change:*** | ⌘ | The MRK is derived from Ks_NAF by using the GBA's key derivation function defined in TS 33.220. The MUK is equal to Ks_NAF. |
| ***Consequences if not approved:*** | ⌘ | It is not specified how MRK and MUK are derived for ME based MBMS key management. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.1, 6.2, Annex F (new) | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

**===== BEGIN CHANGE =====**

## 6.1 Using GBA for MBMS

TS 33.220 [6] (Generic Bootstrapping Architecture) is used to agree keys that are needed to run an MBMS Multicast User service.

Before a user can access an MBMS User service, the UE needs to share GBA-keys with the BM-SC. If no valid GBA-keys are available at the UE, the UE shall perform a GBA run with the BSF of the home network as described within ~~clause 5 of~~ TS 33.220 [6]. The BM-SC will act as a NAF (Network Application Function) according to TS 33.220 [6].

The MSKs for an MBMS User service shall be stored on either the UICC if the UICC is capable of MBMS key management or the ME if the UICC is not capable of MBMS key management.

Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions.

As a result of a GBA_U run, the BM-SC will share a key Ks_ext_NAF with the ME and share a key Ks_int_NAF with the UICC. This key Ks_int_NAF is used by the BM-SC and the UICC as the key MUK (MBMS User Key) to protect MSK (MBMS Service Key) deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK (MBMS Request Key) within the protocols as described within clause 6.2.

A run of GBA_ME results in the BM-SC sharing a key Ks_~~(ext)_~~NAF with the ME. Both the BM-SC and the ME use the key Ks_NAF as MUK. ~~This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and t~~The key MRK is derived from the key Ks_NAF by the BM-SC and the ME as specified in Annex F of this specification. The key MUK is used to protect MSK deliveries to the ME as described within clause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within clause 6.2.

The MUK is identified by the combination of B-TID and NAF-ID and the MRK is defined by B-TID, where B-TID and NAF-ID are defined as specified in TS 33.220 [6].

For ME based key management:

- All MBMS keys (MUK, MRK, MSK and MTK) shall be deleted from the ME when a different UICC is inserted. Therefore the ME needs to store in non-volatile memory the last inserted UICC-identity to be able to compare that with the used UICC-identity at UICC insertion and power on.
- All MBMS keys (MRK, MSK and MTK) may be deleted from the ME when the ME is powered down. If the ME does not delete the MBMS keys at power down then the MBMS keys need to be stored in non-volatile memory. The ME should store the MUKs in non-volatile memory in order to be able to authenticate the first MIKEY message of a push solicited pull procedure (see clause 6.3.2.2.4).

NOTE: If the ME deletes the MSK at power down, then the MBMS client would need to request MSK to the BM-SC and may need to run GBA to reconvene an MBMS session.

## 6.2 Authentication and authorisation of a user

~~Editor's Note: The exact details on how to derive the keys MRK and MUK from the GBA keys are for ffs.~~

Editor's Note: According to S3-040212, SA4 has a working assumption to use HTTP as the transport protocol but this is only agreed for the download repair service.

**===== BEGIN NEXT CHANGE =====**

# Annex F (Normative):
# MRK key derivation for ME based MBMS key management

The MRK shall be derived from the key Ks_NAF using the GBA key derivation function (see TS 33.220 [6], Annex B) as follows (see notation style is explained in TS 33.220, Annex B):

- FC = 0x01,
- P0 = "mbms-mrk" (i.e. 0x6d 0x62 0x6d 0x73 0x2d 0x6d 0x72 0x6b), and
- L0 = length of P0 is 8 octets (i.e., 0x00 0x08).

The Key to be used in key derivation shall be:

- Ks_NAF (i.e. NAF specific key) as specified in TS 33.220 [6].

In summary, the MRK shall be derived from the Ks_NAF, and static string "mbms-mrk" as follows:

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

**===== END CHANGE =====**