3GPP TSG-SA WG3 Security Meeting #35
St Paulís Bay, Malta, 5-8 October 2004

Tdoc ⌘ S3-040863

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **001** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

*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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Deletion of MBMS keys stored in the ME
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	08/10/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	The ME behaviour at UICC change and ME power down for ME based key management is unspecified. This behaviour needs to be specified as it is relevant for security and key request overhead. If the ME deletes the MSK at power down, then the MBMS user will need to request MSK to the BM-SC (http request) and may need to run GBA to reconvene an MBMS session after power on. From a security point of view the deletion of these ME stored MBMS keys at power down is not necessary provided that the same UICC is used at power up. Consequently only at detecting a UICC change all MBMS keys shall be deleted.
Summary of change:	⌘	For ME based key management a) All MBMS keys (MUK, MRK, MSK and MTK) shall be deleted from the ME when a different UICC is inserted. b) All MBMS keys (MUK, 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 then the MBMS keys need to be stored in non-volatile memory.
Consequences if not approved:	⌘	Insecure ME Based key management if MBMS keys are not deleted at UICC change.

Clauses affected:	⌘	6.1

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘

***** Begin of change *****

6 Security mechanisms

6.1 Using GBA for MBMS

GBA[6] is used to agree keys that are needed to run an MBMS Multicast User service. MBMS imposes the following requirements on the MBMS capable UICCs and MEs:

A UICC that contains MBMS key management functions shall implement GBA_U.

An ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC.

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 [6] clause 5. The BM-SC will act as a NAF according to [6].

The MSKs for an MBMS User service shall be stored on either the UICC or the ME. Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions (and that is GBA aware) and requires that the BM-SC is GBA_U aware. As a result of the GBA_U run in these circumstances, 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 to protect MSK deliveries to the UICC as described within subclause 6.3. The key Ks_ext_NAF is used as the key MRK within the protocols as described within subclause 6.2.

NOTE: A run of GBA_U on a GBA aware UICC will not allow the MSKs to be stored on the UICC, if the MBMS management functions are not present on the UICC.

In any other circumstance, a run of GBA results in the BM-SC sharing a key Ks_(ext)_NAF with the ME. This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and the key MRK (MBMS Request Key). The key MUK is used to protect MSK deliveries to the ME as described within subclause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within subclause 6.2.

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 (MUK, 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.

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

***** End of change *****