3GPP TSG-SA WG3 Meeting S3#35
St Paul's Bay, Malta, October 5-8, 2004

Tdoc ⌘S3-040862

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **007** ⌘ **rev** **1** ⌘ 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 [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Clarifying ME and BM-SC capabilities
Source:	⌘	**3**, Siemens
Work item code:	⌘	MBMS
Date:	⌘	06/10/2004
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 specification is not entirely clear that the ME shall support key management functions and the BM-SC shall support using GBA_U keys. Furthermore the text stating what shall be supported by an ME and UICC is in a clause about using GBA for MBMS which is not really the best place for this text. The text is moved to an overview clause where it fits better.
Summary of change:	⌘	The text stating what an MBMS capable ME and UICC shall support is moved to a more appropriate clause. Text is added to clarify that an ME shall support ME key management and the BM-SC supports using GBA_U keys.
Consequences if not approved:	⌘	The specification is not clear on the ME supporting MBMS key management and the BM-SC supporting GBA_U keys.

Clauses affected:	⌘	4.1, 6.1
Other specs affected:	⌘	Y N ☐ N Other core specifications ☐ N Test specifications ☐ N O&M Specifications
Other comments:	⌘	

********** First Modification **********

4.1 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a multicast service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a multicast service. The AKA protocol (see TS 33.102 [4]) is used to both authenticate a user and agree on keys to be used between that user and the network. These keys are subsequently used to provide protection of traffic between the network and the UE.

Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS (beyond the normal network bearer security) resides in either the BM-SC or the UE.

The Broadcast Multicast ñ Service Centre (BM-SC) is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission. It is responsible for generating and distributing the keys necessary for multicast security to the UEs and for applying the appropriate protection to data that is transmitted as part of a multicast service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish multicast bearer.

The UE is responsible for receiving or fetching keys for the multicast service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

MBMS imposes the following requirements on the MBMS capable elements:

- a UICC that contains MBMS key management functions shall implement GBA_U;
- a 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 as well as providing key management functions itself;
- a BM-SC that supports MBMS shall support using GBA_U keys to enable UICC key management.

********** Next Modification **********

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. ~~MBMS imposes the following requirements on the MBMS capable UICCs and MEs:~~

- ~~a UICC that contains MBMS key management functions shall implement GBA_U;~~
- ~~a 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 clause 5 of TS 33.220 [6]. The BM-SC will act as a NAF according to TS 33.220 [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 clause 6.3. The key Ks_ext_NAF is used as the key MRK within the protocols as described within clause 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 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.