3GPP TSG SA WG3 Security — SA3#33 **S3-040219**
10-14 May 2004, Beijing, China

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.246** **CR** ⌘ **rev** **-** ⌘ Current version: **1.1.0** ⌘

*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:	⌘	Using GBA within MBMS
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	08/04/2004
Category:	⌘	
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:

2	*(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)*

Reason for change:	⌘	Introducing the use of GBA within the MBMS specification
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	

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

Other comments:	⌘	-

*************** First change ***************

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246 "MBMS User Services"

[6] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.xxx: "T3-specification describing MBMS application and interface procedures on UICC"

*************** next change ***************

6 Security mechanisms

6.1 Authentication and authorisation of a user

Editor's note: this section will contain the details on authentication and authorization when~~of how~~ a user joins a particular Multicast User Service i.e. how the key MUK in the BM-SC and the UE is generated for use in 'key update procedures' (See sections 6.2) and joining.

Editor's note: The actual protocols used for joining a particular Multicast User Service will be decided by SA4.

When the user wants to join an MBMS user service that allows to use ME based key management then it may run the GBA_ME-procedures as described within [6] section 4 or run the GBA_U-procedures as described within [6] section 5. The BM-SC will act as a NAF according to [6].

When the user wants to join an MBMS user service that requires the use of UICC based key management then it first runs the GBA_U-procedures as described within [6] section 5. The BM-SC will act as a NAF according to [6].

In order for the user to be able to join an MBMS user service requiring ME based key management the support following features is required for the UE:

- The ME needs to support GBA_ME proceducures according to [6].

In order for the user to be able to join an MBMS user service requiring UICC based key management the support following features is required for the UE:

- A UICC needs to be present that implements an MBMS-application (See [7]) and is GBA-aware (See [6]).
- Both the ME and the UICC needs to implement the MBMS-key management interface procedures (see [7]), and the ME needs to support a GBA-aware UICC (See [6]).

As a result of the GBA_ME run, the BM-SC will share a key Ks_NAF with the ME. This key Ks_NAF is used by the BM-SC and the ME to derive the key MUK and the key MRK (MBMS Service Request Key). The key MUK is used to protect MSK deliveries to the ME as described within section 6.2. The key MRK is used to authenticate the UE when joining to the MBMS user service and requesting a MSK key update.

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

As a result of the 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 to protect MSK deliveries to the UICC as described within section 6.2. The key ks_ext_NAF is used as the key MRK to authenticate the UE when joining to the MBMS user service and requesting an MSK key update.

Editor's note: The exact details on how to use MUK and MRK for ffs.