3GPP TSG SA WG3 Security — SA3#33 **S3-040391**
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 (combination of S3-040219/238)
Source:	⌘	SA3
Work item code:	⌘	MBMS
Date:	⌘	13/05/2004
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 31.102: "T3-specification describing MBMS application and interface procedures on UICC"

[8] IETF RFC 2617 "HTTP Digest Authentication"

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

6 Security mechanisms

6.0 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] section 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 by requirement is GBA aware) and requires that all of the network elements, i.e. HSS, BSF and BM-SC, to be 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 6.2. The key ks_ext_NAF is used as the key MRK within the protocols as described within clause 6.1

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 6.2. The key MRK is used to authenticate the UE towards the MBMS within the protocols as described within clause 6.1

6.1 Authentication and authorisation of a user

Editor's note: this section will contain the details on authentication and authorization of an MBMS user~~f how a user joins a particular Multicast Service~~

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

When the user wants to join an MBMS user service, it shall use HTTP digest authentication [6] for authentication. HTTP digest is run between BM-SC and ME. The MBMS authentication procedure is based on the general user authentication procedure over Ua interface that is specified in chapter "Procedures using the bootstrapped Security Association" in [6]. The BM-SC will act as a NAF according to [6].

The following adaptations apply to HTTP digest:

- The transaction identifier as specified in [8] is used as username
- MRK (MBMS Request Key) is used as password.
- The joined MBMS user service is specified in client payload of HTTP Digest message.

Editor's Note: The contents of the client payload are FFS and may require input from TSG SA WG4.

Editor's Note: The use of bootstrapped keys for leaving an MBMS user service, for an MSK key request and request to a download repair server is 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.