3GPP TSG SA WG3 Security — S3#37
Sophia-Antipolis, France, 21–25 February 2005

Tdoc ⌘S3-050049

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **036** ⌘ **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 [ ]

Title:	⌘	On the derivation of the GBA keys for MBMS
Source:	⌘	Oberthur Card Systems
Work item code:	⌘	MBMS
Date:	⌘	09/02/2005
Category:	⌘	**B**
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:	⌘	33.246 says : "The exact details on how to derive the keys MRK and MUK from the GBA keys are for ffs". .
Summary of change:	⌘	Specifies the derivation methods for GBA keys
Consequences if not approved:	⌘	
Clauses affected:	⌘	6.1, new clause in 6.2

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

Other comments: ⌘

*** BEGIN OF CHANGES ***

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] 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~~ derived by the BM-SC and the UICC ~~as~~ to obtain the key MUK to protect MSK deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is ~~used as~~ derived to obtain 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~~ obtain 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.

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.

6.2.1 Derivation of the GBA keys

In this section we will define the derivation mechanism of GBA keys to obtain the MUK and MRK keys :

- In the GBA_U case, Ks_int_NAF (256 bits) will be used to obtain the MUK key and Ks_ext_NAF (256 bits) will be used to derive the MRK key. We will have MUK = f1(Ks_int_NAF, parameters of derivation) and MRK = f2(Ks_ext_NAF, parameters of derivation) where f1, f2 and parameters must be defined.

- In the GBA_ME case, Ks_(ext)_NAF (256 bits) will be derivated to obtain both MUK key and the MRK key. We will have MUK = f1(Ks_ext_NAF, parameters of derivation) and MRK = f2(Ks_ext_NAF, parameters of derivation) where f1, f2 and parameters of derivation must be defined.

6.2.1~~1~~2 Authentication and authorisation in application level joining

When the user wants to join (or leave) an MBMS user service, it shall use HTTP digest authentication [8] 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 [6] 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. The final decision on application level join and leave procedures relies of work in SA4.

6.2.2~~3~~3 Authentication and authorisation in MBMS bearer establishment

The authentication of the UE during MBMS bearer establishment relies on the authenticated point-to-point connection with the network, which was set up using network security described in TS 33.102 [4]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.

6.2.3~~4~~4 Authentication and authorisation in MSK request

When the UE requests MSK(s), the UE shall be authenticated with HTTP digest as in subclause 6.2.1.

6.2.4~~5~~5 Authentication and authorisation in post delivery procedures

When the UE requests post delivery procedures, the UE shall be authenticated with HTTP digest as in chapter 6.2.1.

*** END OF CHANGES ***