3GPP TSG-SA WG3 Meeting #37 **Tdoc ⌘S3-050078**
Sophia Antipolis, France, 21-25 February 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **042** ⌘ **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:	⌘ Annex D1: correction of the description of the GBA run		
Source:	⌘ Gemplus, Axalto		
Work item code:	⌘ MBMS	***Date:*** ⌘	10/02/2005
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 keys MUK and MRK are derived from the GBA keys. The Ks_int_NAF key is shared by the BM-SC and the UICC and results from a GBA_U NAF Derivation procedure. The Annex D.1 indicates that "*the ME has previously performed a GBA_U bootstrapping procedure as described in TS 33.220. The UICC stores the corresponding Ks_int_NAF together with the NAF_Id associated with this particular bootstrapping procedure*." This description shall be modified to indicate that: • Ks_int_NAF results from a GBA_U Bootstrapping procedure and a subsequent NAF Derivation procedure (and not the GBA_U bootstrapping procedure only) • The UICC stores Ks_int_NAF and associated B-TID together with NAF-ID
Summary of change: ⌘	Correction of the description of the GBA run in Annex D.1 .
Consequences if not approved: ⌘	The current description of the GBA run in the MSK Update procedure is not accurate.

Clauses affected:	⌘	Annex D .1		
Other specs affected:	⌘	Y / N		⌘
		[ ] [X]	Other core specifications	
		[ ] [X]	Test specifications	
		[ ] [X]	O&M Specifications	
Other comments:	⌘			

Annex D (normative): UICC-ME interface

D.1 MSK Update Procedure

This procedure is part of the MSK update procedure as described in clause 6.5 (Validation and key derivation functions in MGV-F).

The ME has previously performed a GBA_U Bootstrapping procedure and a subsequent GBA_U NAF Derivation procedure as described in TS 33.220. The UICC stores the corresponding Ks_int_NAF and associated B-TID together with the NAF_Id associated with this particular bootstrapping procedure.

The ME receives a MIKEY message containing an MSK update procedure. After performing some validity checks, the ME sends the whole message to the UICC. The ME also includes in this request NAF_Id to identify the stored Ks_int_NAF.

The UICC then uses Ks_int_NAF as the MUK value for MUK derivation and MSK validation and derivation (as described in clause 6.5.3).

After successful MSK Update procedure the UICC stores the Network ID, Key Group ID, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).

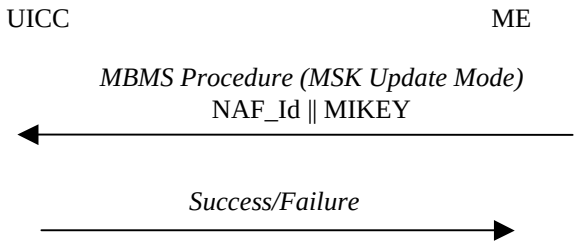

Figure D.1: MSK Update Procedure