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

Tdoc ⌘S3-040784

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.220** **CR** **029** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	Description of UICC-ME interface
Source:	⌘	Nokia, Samsung Electronics
Work item code:	⌘	SEC1-SC
Date:	⌘	27/09/2004
Category:	⌘	**C**
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:	⌘	Description of UICC-ME interface to be used when a GBA_U aware UICC application is active and the ME is involved in a GBA bootstrapping procedure.
Summary of change:	⌘	1. Addition of description of GBA_U bootstrapping procedure. 2. Addition of description of GBA_U initialization procedure 3. Addition of description of GBA_U key derivation procdure.
Consequences if not approved:	⌘	The description of the UICC-ME interface to be used in the above mentioned case is not specified.

Clauses affected:	⌘	Annex D (new)

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 31.102, TS 33.103
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

===== BEGIN CHANGE =====

Annex D (normative): UICC-ME interface for GBA_U

This section describes the UICC-ME interface to be used when a GBA_U aware UICC application is active and the ME is involved in a GBA bootstrapping procedure. When the UICC application is not GBA_U aware, the ME uses the AUTHENTICATE command in non-GBA_U security context (i.e. UMTS security context in case of USIM application and IMS security context in case of the ISIM) as defined in 3GPP TS 31.102 [tba] and 3GPP TS 31.103 [tba].

D.1 GBA_U bootstrapping procedure

This procedure is part of the Bootstrapping procedure as described in section 5.3.2

The ME sends RAND and AUTN to the UICC and the UICC validates the AUTN. The UICC then performs the Ks_int derivation as described in 5.3.2. The UICC stores Ks_int. The UICC also stores the used RAND to identify the current bootstrapped values. RAND value in the UICC shall be further accessible by the ME.

The UICC sends RES', CK' and IK' to the ME.

NOTE: if the ME is GBA_U unaware the procedure described in section is sufficient for the GBA_ME based bootstrapping procedure. In order to complete the GBA_U based bootstrapping procedure on the UICC, the initialization step described in subclause D.2 must be executed.

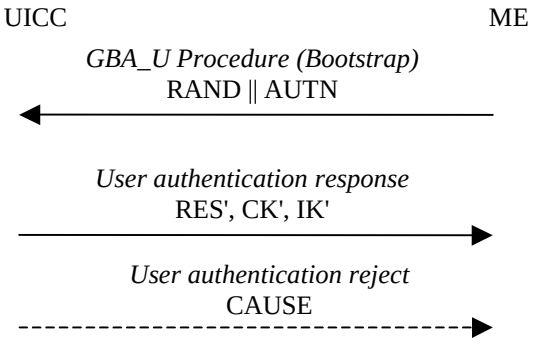

Figure D.1: GBA_U/GBA_ME bootstrapping procedure

D.2 GBA_U initialization procedure

This procedure is part of the procedures using bootstrapped security association as described in section 5.3.3

The ME stores the bootstrapping transaction identifier (B-TID) and key lifetime associated with the bootstrapped key Ks_int in the UICC. The bootstrapping transaction identifier and key lifetime values in the UICC shall be further accessible by the ME.

At the end of the GBA_U initialization procedure the UICC stores Ks_int, B-TID, key lifetime and the RAND. A new bootstrapping procedure replaces Ks_int, B-TID, key lifetime and RAND values of the previous bootstrapping procedure.

NOTE: The storing of B-TID and key lifetime to the UICC needs to be performed only once per bootstrapping procedure.

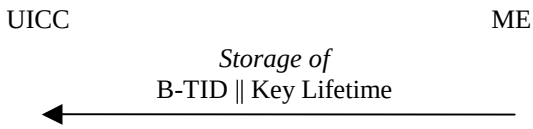

Figure D.2: GBA_U initialization with B-TID and key lifetime on the UICC

D.3 GBA_U key derivation procedure

This procedure is part of the procedures using bootstrapped security association as described in section 5.3.3

The ME sends NAF_ID and IMPI to the UICC. The UICC then performs Ks_int_NAF derivation as described in 5.3.2. The UICC uses the RAND and Ks_int values stored from the previous bootstrapping procedure. The UICC stores Ks_int_NAF together with NAF_Id.

NOTE: A GBA_U bootstrapping procedure needs to be performed before the GBA_U key derivation procedure. If a Ks_int is not available in the UICC, the command will answer with the appropriate error message.

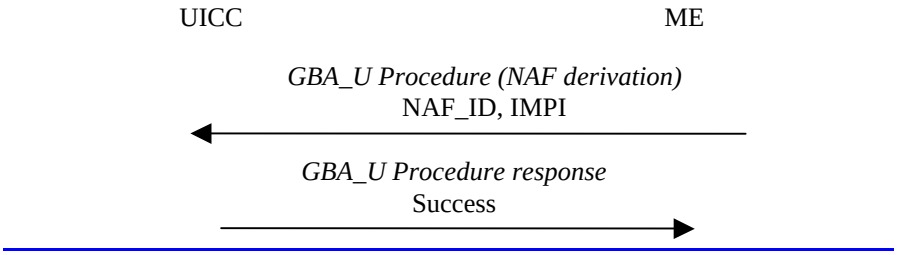

Figure D.3: GBA_U key derivation procedure on the UICC

===== END CHANGE =====