3GPP TSG-SA WG3 Meeting #37
Sophia Antipolis, France, 21-25 February 2005

Tdoc ⌘S3-050086

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.220**	**CR**	**048**	⌘ **rev**	**-**	⌘ Current version:	**6.3.0** ⌘

*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⌘ ☒ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Storage of B-TID in GBA_U NAF Derivation procedure		
Source:	⌘	Gemplus, Axalto		
Work item code:	⌘	SEC1-SC	***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:	⌘	In some cases the NAF-ID is not enough to identify the Ks_int_NAF/Ks_ext_NAF unambigiously. For some example a new NAF key generation, from which the http session was not able to complete towards the corresponding NAF, results in different Ks_ext_NAF/Ks_int_NAF key pairs (on the UE and onother in the NAF) identified with the same NAF_ID. Therefore, text shall be added in TS 33.220 to indicate that the UICC shall store B-TID together with Ks_int_NAF and NAF_ID in order to identify unambiguously the Ks_int_NAF key.
Summary of change:	⌘	Storage of B-TID together with Ks_int_NAF and NAF_ID in GBA_U NAF Derivation procedure.
Consequences if not approved:	⌘	Incomplete description of GBA_U NAF Derivation procedure.

Clauses affected:	⌘	Annex G.2				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

G.2 GBA_U NAF Derivation procedure

This procedure is part of the Procedures using bootstrapped Security Association as described in clause 5.3.3

The ME sends NAF_ID and IMPI to the UICC. The UICC then performs Ks_ext_NAF and Ks_int_NAF derivation as described in clause 5.3.2. The UICC uses the RAND and Ks values stored from the previous bootstrapping procedure. The UICC returns Ks_ext_NAF to the ME and stores Ks_int_NAF and associated B-TID together with NAF_Id.

NOTE: A previous GBA_U Bootstrap needs to be undertaken before. If Ks is not available in the UICC, the command will answer with the appropriate error message.

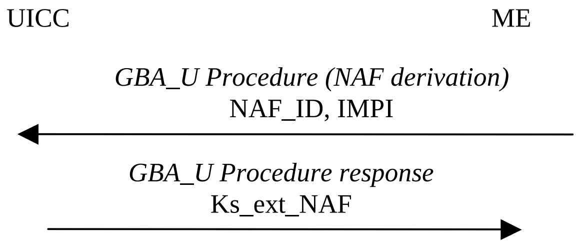

Figure G.2: GBA_U NAF derivation procedure