3GPP TSG SA WG3 Security — S3#35 **S3-040778**
St Paul's Bay, Malta, 5-8 October 2004

CR-Form-v7

CHANGE REQUEST

⌘	**33.220**	**CR**	**027**	⌘ **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⌘ □ ME ☒ Radio Access Network □ Core Network □

Title:	⌘	Requirement on ME capabilities for GBA_U		
Source:	⌘	Gemplus, Axalto, Oberthur		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	27/09//2004
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:

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: ⌘ Procedure for NAF key derivation in the UICC is not mandated in MEs supporting GBA. However, the decision on running GBA_U or GBA_ME bootstrap should not depend either on ME capabilities (1) or on the existence of ME applications requiring GBA_U bootstrap (2). The following reasons are given for both assertions:

(1) No indication of ME's capabilities related to GBA_U or GBA_ME is available to BSF/HSS
(2) Some UE applications (e.g. STK applications, middlets) may need GBA_U derived keys without requiring specific capabilities in any ME application.

So, the scenario where GBA_U is requested by BSF and the NAF derivation is not supported by the ME shall be avoided

Summary of change: ⌘ -Additon of a requirement on UE for mandating procedures for NAF-keys derivation.

Consequences if not approved: ⌘ Complete GBA_U bootstrap will not be possible depending on ME capabilities.

Clauses affected: ⌘ 5.2.1

		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 31.102, TS 31.103
			X	Test specifications		
			X	O&M Specifications		

Other comments: ⌘ -

BEGIN OF CHANGE

5.2.1 Requirements on UE

The 3G AKA keys CK and IK resulting from a run of the protocol over the Ub reference point shall not leave the UICC.

The UICC shall be able to distinguish between authentication requests for GBA_U, and authentication requests for other 3G authentication domains.

Upon an authentication request from the ME, which the UICC recognises as related to GBA_U, the UICC shall derive two keys from CK and IK. ~~All 3G MEs are capable of such a request.~~

Upon request from the ME, the UICC shall be able to derive further NAF-specific keys from the derived key stored on the UICC. ~~Only GBA_U aware 3G MEs are capable of such a request.~~

The ME shall support procedures for the two previous requests.

Editor’s Note: The location (whether in the UICC or in the ME) of the storage of Ks_ext is ffs.