3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040540

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** **CRNum** ⌘**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:	⌘	GBA_U: generic functions for Ks_int_NAF usage
Source:	⌘	Nokia
Work item code:	⌘	GBA
Date:	⌘	29/06/2004
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:	⌘	In order to be able to execute cryptographic operations on the UICC with Ks_int_NAF from the ME, a requirement is added that generic encrypt and decrypt functions should be availble for the ME. Only MBMS uses GBA_U and Ks_int_NAF in Release 6.
Summary of change:	⌘	A requirement for having generic encrypt and decrypt functions on the UICC related procedures using GBA_U key Ks_int_NAF is added.
Consequences if not approved:	⌘	Requirement for having functions between ME and UICC to use Ks_int_NAF is missing.

Clauses affected:	⌘	5.2.1

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

Other comments: ⌘

===== BEGIN 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 be able to execute generic encrypt and decrypt functions on the UICC that use Ks_int_NAF as the key. Only GBA_U-aware 3G MEs are capable of such a request.

Editor's note: The exact details of generic encrypt and decrypt functions are FFS. Possible additional functionalities that can be performed on the UICC using Ks_int_NAF are FFS.

Editors' Note: The location (whether in the UICC or in the ME) of the storage of Ks_ext is ffs.

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