3GPP TSG SA WG3 Security – S3#34
Acapulco, Mexico, 6 –9 July 2004

S3-040663

CR-Form-v7

CHANGE REQUEST

⌘ **33.222** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Precision on the NAF-specific key to use to secure Ua interface in case of GBA_U
Source:	⌘	Gemplus
Work item code:	⌘	SSC-GBA
Date:	⌘	08/07/04
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:
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 the description of GBA_U (TS 33.220) the definition of a default type of NAF-specific key to use for procedures using bootstrapping Security Association was removed. So, it is necessary to indicate in HTTPS TS 33.222 that the NAF-specific key used to secure Ua interface in case of GBA_U is Ks_ext_NAF.
Summary of change:	Indicate that Ks_ext_NAF is the type of NAF-specific key to use to secure Ua interface in case of GBA_U.
Consequences if not approved:	GBA_U provides two types of NAF-specific keys (Ks_ext_NAF and Ks_int_NAF). In case of GBA_U used for HTTPS, the current document does not indicate which NAF-specific key to use to secure Ua interface.

Clauses affected:	5.2

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

Other comments:

5 Authentication schemes

5.1 Reference model

Figure 1 shows a network model of the entities that utilize the bootstrapped secrets, and the reference points used between them.

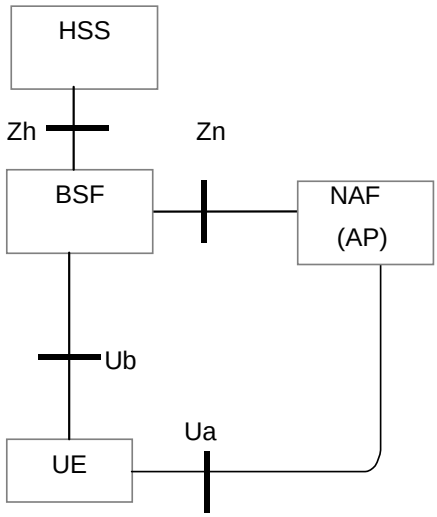

Figure 1: High level reference model for NAF using a bootstrapping service

5.2 General requirements and principles

This document is based on the architecture specified in TS 33.220 [3]. All notions not explained here can be found in TS 33.220 [3].

In the scope of GBA_U, the key that is used to secure the Ua reference point shall be Ks_ext_NAF.

5.2.1 Requirements on the UE

To utilise GBA as described in this document the UE shall be equipped with a HTTPS capable client (e.g. browser) implementing the particular features of GBA as specified in TS 33.220 [3].

5.2.2 Requirements on the NAF and BSF

To utilise GBA as described in this document the NAF and BSF shall support the features of GBA as specified in TS 33.220 [3].

Additionally in the scope of this specification, HTTP and TLS shall be supported by the NAF for the UE-NAF reference point (Ua).