3GPP TSG-SA WG3 Meeting #36
Shenzhen, China, November 23-26, 2004

Tdoc ⌘S3-041082

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.220** **CR** **036** ⌘ **rev** **1** ⌘ 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:	⌘	Removal of unnecessary editor's notes
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-SC
Date:	⌘	16/11/2004
Category:	⌘	**D**
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:	⌘	Unnecessary editor's notes are deleted.
Summary of change:	⌘	- 3.1: definitions are completed - 4.3.3 and 4.3.4: USS is capable of transferring the authorization part. It is up to application itself whether the authorization part is used or not.
Consequences if not approved:	⌘	

Clauses affected:	⌘	3.1, 4.3.3, 4.3.4

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

Other comments: ⌘

==== ***BEGIN CHANGE*** ====

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Bootstrapping Server Function: BSF is hosted in a network element under the control of an MNO. BSF, HSS, and UEs participate in GBA in which a shared secret is established between the network and a UE by running the bootstrapping procedure. The shared secret can be used between NAFs and UEs, for example, for authentication purposes.

~~Editor's note: Definition to be completed.~~

ME-based GBA: in GBA_ME, all GBA-specific functions are carried out in the ME. The UICC is GBA-unaware. If the term GBA is used in this document without any further qualification then always GBA_ME is meant, see clause 4 of this specification.

UICC-based GBA: this is a GBA with UICC-based enhancement. In GBA_U, the GBA-specific functions are split between ME and UICC, see clause 5 of this specification.

Network Application Function: NAF is hosted in a network element ~~under the control of an MNO~~. GBA may be used between NAFs and UEs for authentication purposes, and for securing the communication path between the UE and the NAF.

~~Editor's note: Definition to be completed.~~

Bootstrapping Transaction Identifier: the bootstrapping transaction identifier (B-TID) is used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn.

GBA User Security Setting: An application-specific parameter set describing the security related usage of bootstrapping function by the BSF and, optionally, some types of NAFs in the context of an application and in relation to a subscriber. A user security setting has two parts, an authentication part, which contains the list of identities of the user needed for the application (e.g. IMPI, IMPUs, MSISDN, pseudonyms), and an authorisation part, which contains the user permission flags (e.g. access to application allowed, type of certificates which may be issued). Sometimes also called application-specific user security setting.

GBA User Security Settings: the set of all application-specific user security settings.

==== ***BEGIN NEXT CHANGE*** ====

4.3.3 Reference point Zh

The reference point Zh used between the BSF and the HSS allows the BSF to fetch the required authentication information and all GBA user security settings from the HSS. The interface to the 3G Authentication Centre is HSS-internal, and it need not be standardised as part of this architecture.

~~Editor's note: It is ffs, jointly with CN4 and SA2, whether the authorisation part of all USSs is transferred over Zh, or by other means. SA3 expresses a preference for Release 6, however, to transfer the authorisation part of the USSs for, at least, the GBA specific entities PKI portal (cf. TS. 33.221) and Authentication Proxy (TS 33.222) over Zh.~~

4.3.4 Reference point Zn

The reference point Zn is used by the NAF to fetch the key material agreed during a previous HTTP Digest AKA protocol run over the reference point Ub from the UE to the BSF. It is also used to fetch application-specific user security settings from the BSF, if requested by the NAF.

~~Editor's note: It is ffs, jointly with CN4 and SA2, whether the authorisation part of the application-specific USSs is transferred over Zn, or by other means. SA3 expresses a preference for Release 6, however, to transfer also the authorisation part of the application specific USSs for, at least, the GBA specific entities PKI portal (cf. TS. 33.221) and Authentication Proxy (TS 33.222) over Zn.~~

==== ***END CHANGE*** ====