3GPP TSG-SA WG3 Meeting S3#36
Shenzhen, China, November 23-26, 2004

Tdoc ⌘S3-040981

CR-Form-v7

CHANGE REQUEST

⌘	**33.220**	**CR**	**021**	⌘ **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:	⌘	Details of USIM/ISIM selection in GAA			
Source:	⌘	Nokia			
Work item code:	⌘	SEC1-SC	***Date:***	⌘	16/11/2004
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:	⌘	At SA3#34 a new section 4.4.8 of TS 33.220 dealing with selection of UICC application for GBA was introduced (approved CR S3-040648). This document points to a necessary correction and, in addition, proposes improvements to the selection process as defined at SA3#34.
Summary of change:	⌘	The correction concerns the fact that a "default USIM" is not defined in 3GPP specifications, and that the term "selection" is used in a way not compatible with other 3G specifications. The two main goals of the improvements are (i) the optional possibility for a Ua application to choose a particular UICC application (not only UICC type) and (ii) more deterministic behaviour and better understandability of the selection process by the user. Requirement regarding to name of the UICC application as an indication is added to subclause 4.2.4.
Consequences if not approved:	⌘	Specification stays inconsistent with regard to the corrections. Sub-optimal behaviour of UICC application selection.

Clauses affected:	⌘	2, 3.1, 4.2.4, 4.4.8				
		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

===== BEGIN CHANGE =====

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application".

[2] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

[3] Franks J., et al,: "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[4] A. Niemi, et al,: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

[5] 3GPP TS 33.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[6] T. Dierks, et al,: "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[7] OMA: "Provisioning Content Version 1.1", Version 13-Aug-2003. Open Mobile Alliance.

[8] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 6)".

[9] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

[10] 3GPP TS 31.103: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[11] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[12] IETF RFC 3548 (2003): "The Base16, Base32, and Base64 Data Encodings".

[13] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[14] IETF RFC 3588 (2003): "Diameter Base Protocol".

[15] 3GPP TS 31.101: "3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics ".

[16] 3GPP TS 33.203: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 6)”

===== BEGIN NEXT 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.

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.

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.

Bootstrapping Usage Procedure: A procedure using bootstrapped security association over Ua reference point.

Ua Application: An application on the ME intended to run bootstrapping usage procedure with a NAF.

GBA Function: An entity on the ME executing the bootstrapping procedure with BSF (i.e. supporting the Ub reference point) and providing Ua applications with security association to run bootstrapping usage procedure. GBA function is called by a Ua application when a Ua application wants to use bootstrapped security association.

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

4.2.4 UE

The required functionalities from the UE are:

- the support of HTTP Digest AKA protocol;
- the capability to use both a USIM and an ISIM in bootstrapping;
- the capability to select either a USIM or an ISIM to be used in bootstrapping, when both of them are present;
- the capability for an Ua application on the ME ~~using the shared secret~~ to indicate to the GBA Function on the ME the type or the name of UICC application to use in bootstrapping (~~i.e., ISIM or USIM~~cf. subclause 4.4.8);
- the capability to derive new key material to be used with the protocol over Ua interface from CK and IK;
- support of NAF-specific application protocol (For an example see TS 33.221 [5]).

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

4.4.8 Requirements on selection of UICC application and related keys

When several applications are present on the UICC, which are capable of running AKA, then the ME shall ~~select~~choose one of these UICC applications for performing the GBA procedures specified in this document in the following order of preference:

1. The UE determines which UICC application is to be involved:

   a. the application on the ME that needs Ks_NAF (Ua application) may indicate to the GBA ~~application~~ support function (GBA function) the type or the name of the UICC application: no preference, USIM, ~~or~~ ISIM, or the “Label” (see definition in TS 31.101 [15]) of the UICC application.

   If the application on the ME indicated a “Label” of the UICC application, step b below shall be executed.

   If the application on the ME indicated that the UICC application type should be:

   - the USIM on the UICC; step b below is skipped and in steps c and d only USIM applications are considered.

   - the ISIM on the UICC; step ~~c~~ b below is skipped and in steps c and d only ISIM applications are considered.

   If the application on the ME did not indicate a preference, step b below is skipped and the selection process is executed as described below starting with step c,

   b. if a “Label” was indicated in step a, the GBA function shall select (see definition in TS 31.102 [1]) the UICC application with the “Label” indicated; if selection of this UICC application does not succeed the selection procedure fails;

   c. if no “Label” was indicated in step a, the ~~ME~~ GBA function shall ~~select~~ choose among the active ~~ISIMs~~UICC applications; if there is more than one active ~~ISIM~~UICC application, the ~~UE~~ GBA function may show a~~n~~ ~~ISIM~~ UICC application ~~selection~~ choosing dialogue to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user chooses~~selects~~ the UICC application to be selected~~ISIM~~; if no dialogue is shown the ~~ME~~ GBA function shall select ~~any one of the active ISIMs~~the “last selected” active UICC application; in case the Ua application indicated “no preference” and both a “last selected” USIM and a “last selected” ISIM are active, then the “last selected” USIM is selected.

   ~~c. the ME shall select among the active USIMs; if there is more than one active USIM, the UE may show a USIM selection dialog to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user selects the USIM; if no dialogue is shown the ME shall select any one of the active USIMs.~~

   d. if there are no UICC applications active:

   - if there is only one UICC application, the ~~UE~~GBA function ~~activates~~ selects it, if possible~~, and selects it~~;

   - if there is more than one UICC application, the ~~UE~~ GBA function may show a UICC application ~~selection~~ choosing dialogue to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user ~~selects~~ chooses the UICC application to be ~~activated~~selected; if no dialogue is shown the ~~ME~~ GBA function shall ~~activate~~ select the ~~default USIM~~”last selected” UICC application, if possible~~, and select it~~.

   e. if the type indicated in step a and used in step d was ISIM, but there was no ISIM to select, then step d is repeated with type USIM; otherwise the selection process fails.

NOTE 1: Step e is required for the case that an ISIM as defined in TS 33.203 [16] may be realised using a USIM application on the UICC.

2. If there already is a key Ks derived from the chosen~~selected~~ UICC application, the UE takes this key to derive Ks_NAF.

3. If there is no such key Ks, the UE first runs the Ub protocol involving the selected UICC application and then goes to step 2.

If a USIM is chosen~~selected~~, the IMPI obtained from the IMSI stored on the USIM as specified in 3GPP TS 23.003 section 13.3 [11], is used in the protocol run over Ub.

NOTE ~~1~~2: Strictly speaking, an IMPI, and the derivation of an IMPI from an IMSI as in 3GPP TS 23.003 section 13 [11] are only defined in the context of the IMS. For the purposes of this specification, however, an identifier obtained from an IMSI as specified in 3GPP TS 23.003 section 13.3 [11] is also called an IMPI, even if the user has no IMS subscription.

If an ISIM is selected, the IMPI stored on the ISIM is used in the protocol run over Ub.

Whenever a~~n~~ UICC application is successfully selected or terminated~~ISIM or a USIM is activated or deactivated~~, the rules in this subsection for ~~selecting~~ choosing the UICC application are re-applied and, consequently, the ~~selected~~ UICC application chosen for GBA may change.

Whenever a UICC application is terminated ~~de-selected~~ the shared key Ks established from it in the protocol over the Ub reference point (according to sections 4.5.2 and 5.3.2) shall be deleted.

NOTE ~~2~~3: At any one time, there is at most one UICC application chosen~~selected~~ for performing the GBA procedures.

NOTE ~~3~~4: The Ua applications ~~on the ME~~ can continue using the NAF specific keys derived also after the shared key Ks itself has been deleted until the key lifetime expires.

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