3GPP TSG-SA WG3 Meeting #33
10th – 14th May 2004, Beijing, China

Tdoc ⌘S3-040331

CHANGE REQUEST

⌘	**33.220**	**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:	⌘	Clarification of GBA specific profiles in HSS and over Zh and Zn reference points		
Source:	⌘	Siemens		
Work item code:	⌘	SSC-GBA	***Date:*** ⌘	10/05/2004
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:	⌘	Clarification is needed for requirements on GBA specific profiles stored in HSS to allow for 1) interworking and for 2) flexible extensibility. User and application specific information sent over Zn (and Zh) interface need also clarification.
Summary of change:	⌘	Requirements on GBA specific profiles in HSS are given. NAF shall be able to receive application specific data for one or many applications it supports from BSF together with Ks_NAF. This includes requirements on Zn and Zh.
Consequences if not approved:	⌘	Up to now no requirements are given. Consequently, there is currently no stage work on which to base the pertinent stage 3 work.

Clauses affected:	⌘	4.2.3, 4.3.6, 4.5.3				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	TS 29.109
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*************** begin change *********************

4.2.3 HSS

HSS shall store new parameters in the subscriber profile related to the use of the bootstrapping function. Possibly also parameters related to the usage of some NAFs are stored in the HSS.

The requirement on the HSS are:

- HSS shall provide the only persistent storage for GBA specific subscriber profile information;
- GBA specific subscriber profile information shall be composed of a set of application-specific subscriber profiles;
- GBA specific subscriber profile information shall be defined in such a way that interworking of different operators for standardised application profiles is possible;
- GBA specific subscriber profiles shall be defined in such a way that profiles for operator specific applications and extensions to existing application profiles are supported without need for standardisation of these elements.

~~Editor's note: Needed new subscriber profile parameters are FFS.~~

NOTE: If IMPUs are required for an application they form part of an application-specific subscriber profile.

******************** end change ************************************

******************** begin change **********************************

4.3.6 Requirements on Zn interface

The requirements for Zn interface are:

- mutual authentication, confidentiality and integrity shall be provided;

NOTE: This requirement may be fulfilled by physical or proprietary security measures if BSF and NAF are located within the same operator’s network.

- The BSF shall verify that the requesting NAF is authorised;
- The NAF shall be able to send a key material request to the BSF;
- The BSF shall be able to send the requested key material to the NAF;
- The NAF shall be able to get the subscriber profile information needed for security purposes from BSF;
- The NAF shall be able to indicate to the BSF the single application or several applications it requires subscriber profile information for;

NOTE: If some application needs only a subset of an application-specific subscriber profile, e.g. only one IMPU, the NAF selects this subset from the complete application specific subscriber profile information sent from BSF.

- The BSF shall be able to configure on a per NAF or per application basis if private subscriber identity and which subscriber profile information may be sent to a NAF;
- The BSF shall be able to indicate to the NAF the lifetime of the key material.

~~Editor’s note: Relationship between Transaction Identifier and subscriber identity is ffs. In the case of Presence Ut interface, there are several potential identities that are related to Transaction Identifier, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. Transaction Identifier does not carry enough information on which IMPU the end-user is trying to use.~~

Editor’s note: it is ffs which actions are to be taken over Zn when the BSF receives a profile update from the HSS over Zh.

******************************* end change ************************************

******************************** begin change *****************************

4.5.3 Procedures using bootstrapped Security Association

After UE is authenticated with the BSF, every time the UE wants to interact with an NAF the following steps are executed as depicted in figure 5.

UE starts communication over Ua interface with the NAF:

- in general, UE and NAF will not yet share the key(s) required to protect Ua interface. If they already do (i.e. if a key Ks_NAF for the corresponding key derivation parameter NAF_Id_n is already available),, the UE and the NAF can start to securely communicate right away. If the UE and the NAF do not yet share a key, the UE proceeds as follows:
    - if a key Ks is available in the UE, the UE derives the key Ks_NAF from Ks, as specified in clause 4.5.2;
    - if no key Ks is available in the UE, the UE first agrees on a new key Ks with the BSF over the Ub interface, and then proceeds to derive Ks_NAF;
- if the NAF shares a key with the UE, but an update of that key is needed, e.g. because the key’s lifetime has expired, it shall send a suitable key update request to the UE and terminates the protocol used over Ua interface. The form of this indication may depend on the particular protocol used over Ua interface (cf. 4.5.1);
- the UE supplies Transaction Identifier to the NAF, in the form of a Transaction Identifier, to allow the NAF to retrieve specific key material from BSF;
- the UE derives the keys required to protect the protocol used over Ua interface from the key material, as specified in clause 4.3.2;

NOTE: The UE shall adapt the key material Ks_NAF to the specific needs of the Ua interface. This adaptation is outside the scope of this specification.

- when the UE is powered down, or when the UICC is removed, any keys Ks and Ks_NAF shall be deleted from storage;
- when a new Ks is agreed over the Ub interface and a key Ks_NAF, derived from one NAF_Id, is updated, the other keys Ks_NAF, derived from different values NAF_Id, stored on the UE shall not be affected;

NAF starts communication over Zn interface with BSF

- The NAF requests key material corresponding to Transaction Identifier supplied by the UE to the NAF used over Ua interface;
- The NAF may also request application specific subscriber profile information for the applications, which the request received over Ua from UE may access;
- The BSF derives the keys required to protect the protocol used over Ua interface from the key material Ks and the key derivation parameters, as specified in clause 4.5.2, and supplies to NAF the requested key material Ks_NAF, as well as the lifetime time of that key material. If the key identified by the Transaction Identifier supplied by the NAF is not available at the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a key update request to the UE.
- The BSF also sends private user identity (IMPI) and requested application specific subscriber profile information to NAF according to the BSF’s policy;

NOTE: The NAF shall adapt the key material Ks_NAF to the specific needs of the Ua interface in the same way as the UE did. This adaptation is outside the scope of this specification.

NAF continues with the protocol used over the Ua interface with the UE.

Once the run of the protocol used over Ua interface is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to use Ua interface in a secure way.

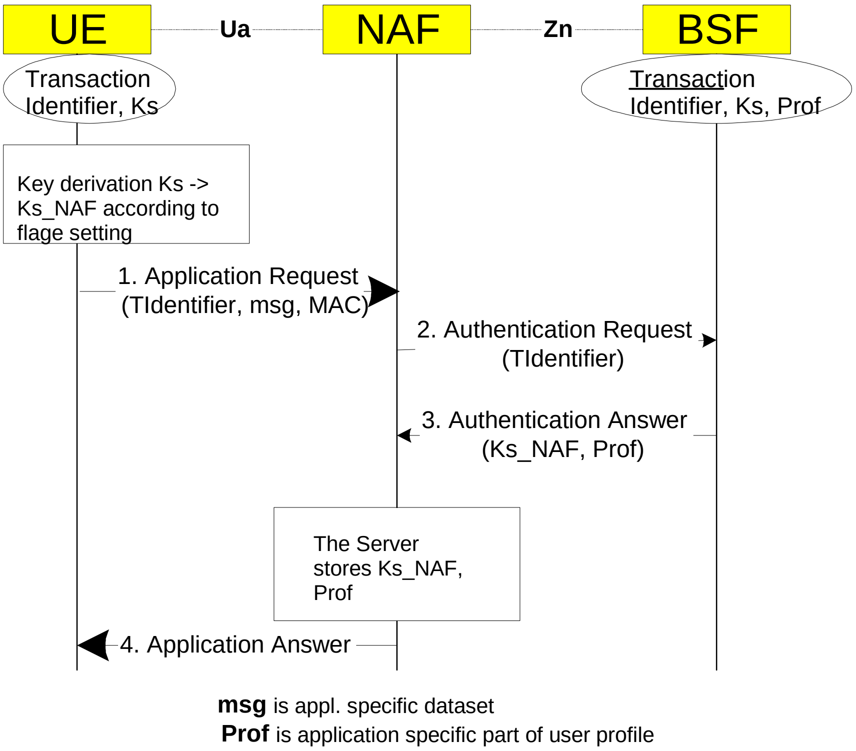
UE
Ua
NAF
Zn
BSF
Transaction Identifier, Ks
Transaction Identifier, Ks, Prof
Key derivation Ks -> Ks_NAF according to flage setting
1. Application Request (TIdentifier, msg, MAC)
2. Authentication Request (TIdentifier)
3. Authentication Answer (Ks_NAF, Prof)
The Server stores Ks_NAF, Prof
4. Application Answer
msg is appl. specific dataset
Prof is application specific part of user profile

Figure 5: The bootstrapping usage procedure

**************************** end change ***************************************