3GPP TSG SA WG3 (Security) –S3 #31 **S3-030742**
18-21 November 2003
Munich, Germany

Agenda Item: **6.9 – GAA and support for subscriber certificates**
Source: **Nortel Networks**
Title: **Application specific user profiles in GBA**
Document for: **Discussion and Decision**

1. User profiles and GBA

The Generic Bootstrapping Architecture (GBA) that is currently being developed in SA3 as part of the Generic Authentication Architecture (GAA) is intended to provide a generic framework for authenticating subscribers by defining a bootstrapping function based on the AKA protocol.

But, in the current GBA specification, requirements are included on the Zh (the interface between BSF and HSS) and Zn (the interface between BSF and NAF) interfaces to provide the application specific user/subscriber profiles to the Network Application Functions. At this point, it seems to us that only the Authentication Vectors (AVs) are required to perform the bootstrapping function. The requirements to acquire the application specific user/subscriber profiles are not part of the GBA. These requirements are to be addressed as part of another Release 6 work item, namely, Generic User Profile (GUP).

We would also like to note that any NAF-specific/Bootstrapping information that may be needed for bootstrapping by the BSF (e.g., key separation between NAFs) is different from the application-specific user profiles. The need for NAF/Bootstrapping specific information from HSS is for further study as no requirement is currently identified or agreed to by SA3.

2. Proposal

Based on the above reasoning, it is proposed that the requirements with respect to transferring application-specific user/subscriber profiles from HSS to BSF (and BSF to NAF) be removed from the GBA. A pseudo-CR implementing the required changes to Rel-6 TS 33.220 v0.1.1 is attached for approval.

3GPP TSG SA WG3 Security — S3#31 **S3-030xxx**
18 - 21 November 2003
Munich, Germany

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.220** **CR** **-** ⌘**rev** **-** ⌘ Current version: 0.1.1 ⌘

*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 application spefic user profile requirements from GBA
Source:	⌘	Nortel Networks
Work item code:	⌘	SSC
Date:	⌘	10/11/2003
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:	⌘	The requirements on application specific user/subscriber profiles are not related to GBA and therefore should be removed
Summary of change:	⌘	Removed requirements on application specific user/subscriber profiles
Consequences if not approved:	⌘	Potential for confusion between GUP and GBA

Clauses affected:	⌘	6.1.3			
Other specs affected:	⌘	**Y**	**N**		
			N	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘	-			

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

********** FIRST CHANGE **********

4.1.5 Requirements on Zh interface

The requirements for Zh interface are:

- The BSF shall be able to communicate securely with the subscriber's HSS.

Editor's note: this requirement is fulfilled automatically if BSF and HSS are in same operator's network.

- The BSF shall be able to send bootstrapping information request concerning a subscriber.
- The HSS shall be able to send authentication vectors to the BSF in batches.
- The HSS shall be abe to send the required authentication information to the BSF. ~~The HSS shall be able to send the subscriber's GAA profiles to the BSF.~~

~~Editor's note: it's ffs how to proceed in the case where profile is updated in HSS after profile is forwarded. The question is whether this profile change should be propagated to BSF.~~

- No state information concerning bootstrapping shall be required in the HSS.
- All procedures over Zh interface shall be initiated by the BSF.
- It is preferred to reuse existing specifications if possible.

- The number of different interfaces to HSS should be minimized

4.1.6 Requirements on Zn interface

The requirements for Zn interface are:

- NAF shall be able to communicate securely with a subscriber's BSF.
- 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 from BSF.~~

Editor's note: in later phases there is an additional requirement that the NAF and the BSF may be in different operators' networks.

********** NEXT CHANGE **********

4.2.2.3 HSS

HSS shall store any new parameters ~~in subscriber profile~~ related to the usage of bootstrapping function. Possibly also parameters related to the usage of some network application function are stored in HSS.

Editor's note: Needed new parameters are FFS.

********** NEXT CHANGE **********

4.2.3.3 Zh interface

Zh interface is used between the BSF and the HSS to allow the BSF to fetch the required authentication information ~~and subscriber profile information from the HSS~~. The interface to the 3G Authentication Centre is HSS-internal, and it need not be standardised as part of this architecture.

4.2.3.4 Zn interface

Zn interface is used by the NAF to fetch the key material agreed during previous HTTP Digest AKA protocol run over Ub interface from the BSF. ~~It may also be used to fetch subscriber profile information from BSF~~.

********** NEXT CHANGE **********

4.3.1 Bootstrapping procedures

When a UE wants to interact with an NAF, and it knows that bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see Figure 1)

Editor's notes: Zh interface related procedure will be added here in future development. It may re-use Cx interface that is specified in TS 29.228.

Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a key update indication from the NAF (cf. subclause 4.3.2).

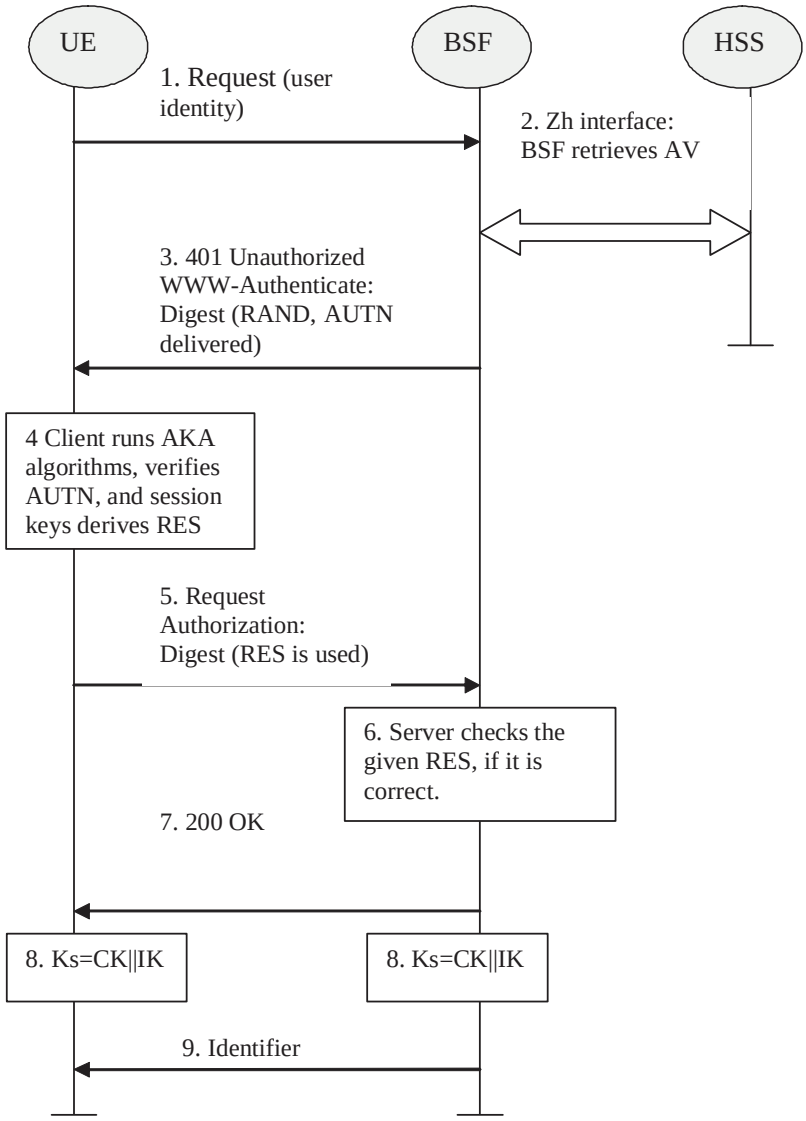

Figure 1: The bootsrapping procedure

1. The UE sends an HTTP request towards the BSF.
2. BSF retrieves the authentication information ~~user profile and a challenge~~, i.e. the Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) over Zh interface from the HSS.
3. Then BSF forwards the RAND and AUTN to the UE in the 401 message (without the CK, IK and XRES). This is to demand the UE to authenticate itself.
4. The UE calculates the message authentication code (MAC) so as to verify the challenge from authenticated network; the UE also calculates CK, IK and RES. This will result in session keys IK and CK in both BSF and UE.
5. The UE sends request again, with the Digest AKA RES as the response to the BSF.
6. If the RES equals to the XRES that is in the AV, the UE is authenticated.
7. The BSF shall send 200 OK message to the UE to indicate the success of the authentication.
8. The key material Ks is generated in both BSF and UE by concatenating CK and IK. The Ks is used for securing the Ua interface.

Editor's note: The key material Ks is 256 bits long. It is up each NAF to make the usage of the key material specifically.

9. BSF may supply a transaction identifier to UE in the cause of Ub interface.

********** NEXT CHANGE **********

4.3.2 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 2

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, there is no need for NAF to retrieve the key(s) over Zn interface.
- If the NAF shares a key with the UE, but an update of that key it sends 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 and is ffs.
- It is assumed that UE supplies sufficient information to NAF, e.g. 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.

NAF starts communication over Zn interface with BSF

- The NAF requests key material corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier) in the start of the protocol used over Ua interface.
- The BSF supplies to NAF the requested 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 NAF derives the keys required to protect the protocol used over Ua interface from the key material in the same way as the UE did.

NAF continues with the protocol used over Ua interface with 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.

Editor's note: Message sequence diagram presentation and its details will be finalized later.

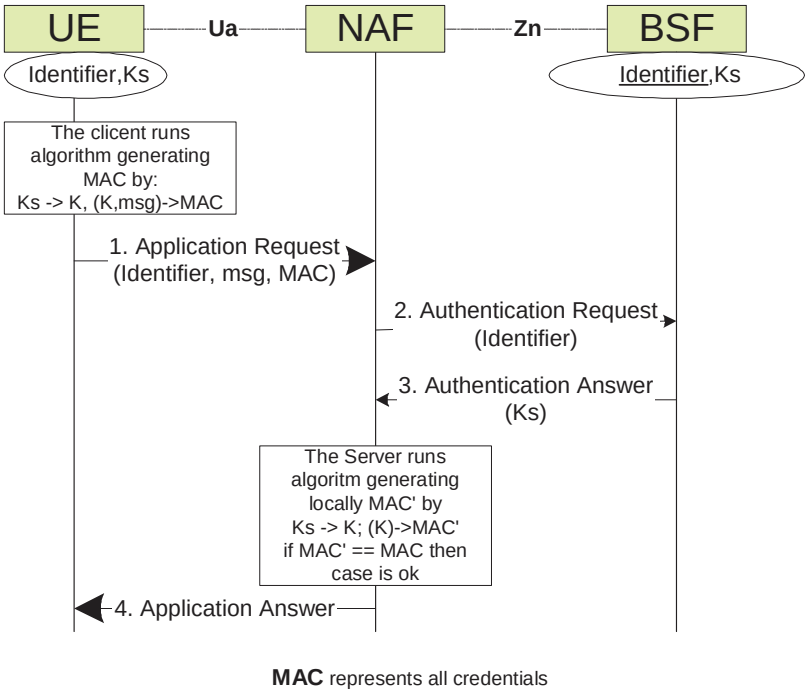

Figure 2: The bootstrapping usage procedure

********** END OF CHANGES **********