3GPP TSG-SA WG3 Meeting S3#33
Beijing, China, May 10-14, 2004

Tdoc ⌘S3-040328

CR-Form-v7

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:	⌘	NAF in visited network
Source:	⌘	Siemens, Nokia
Work item code:	⌘	SSC-GBA
Date:	⌘	03/05/2004
Category:	⌘	**B**
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 possibility that NAF is in the visited network is added to the specification.
Summary of change:	⌘	UE is able to authenticate using GBA towards a NAF which is in a visited network. UE always bootstraps with BSF in subscriber's home network. When UE contact a NAF in a visited network, NAF needs to be able to communicate with subscriber's home BSF. This is accomplished using a Diameter Proxy (D-Proxy) that functions as a proxy between the NAF in the visited network, and the BSF in home network. D-Proxy is placed in the visited network.
Consequences if not approved:	⌘	GBA does not support NAF which are not in the home network.

Clauses affected:	⌘	1, 4.1, 4.2.2, 4.2.2a (new), 4.3, 4.3.3, 4.3.6

Other specs affected:	Y	N			
⌘	X		Other core specifications	⌘	TS 29.109
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	

===== BEGIN CHANGE ====

1 Scope

The present document describes the security features and a mechanism to bootstrap authentication and key agreement for application security from the 3GPP AKA mechanism. Candidate applications to use this bootstrapping mechanism include but are not restricted to subscriber certificate distribution TS 33.221 [5]. Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides.

The scope of this specification includes a generic AKA bootstrapping function, an architecture overview and the detailed procedure how to bootstrap the credential.

~~NOTE: The specification objects are scheduled currently in phases. For this specification release, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. In further specification release, other configurations may be considered.~~

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

4.1 Reference model

Figure 1 shows a simple network model of the entities involved in the bootstrapping approach, and the interfaces used between them.

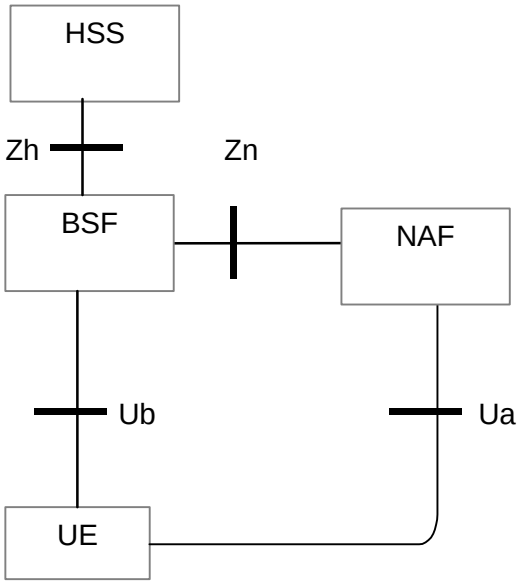

Figure 1: Simple network model for bootstrapping

Figure 1a shows a simple network model of the entities involved when the network application function is located in the visited network.

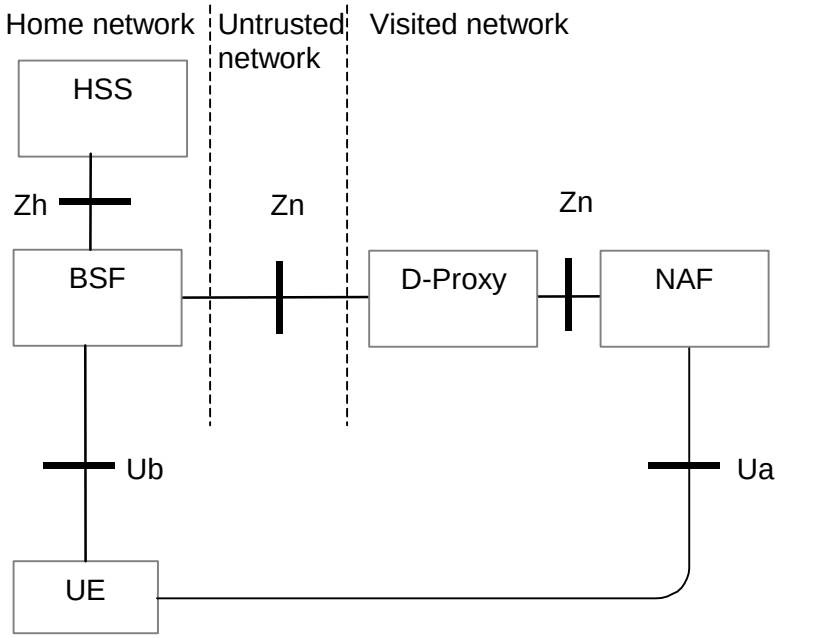

Figure 1a: Simple network model for bootstrapping in visited network

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

4.2.2 Network application function (NAF)

After the bootstrapping has been completed, the UE and an operator-controlled NAF can run some application specific protocol where the authentication of messages will be based on those session keys generated during the mutual authentication between UE and BSF.

General assumptions for the functionality of an operator-controlled NAF are:

- there is no previous security association between the UE and the NAF;
- NAF shall be able to locate and communicate securely with the ~~subscriber's~~ BSF of its own network;
- NAF shall be able to acquire a shared key material established between UE and the BSF during the run of the application-specific protocol;
- NAF shall be able to check lifetime of the shared key material.

4.2.2a Diameter proxy (D-Proxy)

In the case where UE has contacted a NAF that is operated in another network than home network, this visited NAF shall use a diameter proxy (D-Proxy) of the NAFs network to communicate with subscriber's BSF (i.e., home BSF).

NOTE: D-Proxy functionality may be implemented as a separate network element, or be part of any NE in the visited network that implements Diameter proxy functionality (examples of such NE's are the BSF of the network that the visited NAF belongs to, or an AAA-server).

General assumptions for the functionality of D-Proxy are:

- D-Proxy shall be able to function as a proxy between the visited NAF, and the subscriber's home BSF;
- D-Proxy shall be able to locate subscriber's home BSF and communicate with it over secure channel;
- D-Proxy shall be able to validate that the visited NAF is authorized to participate in GBA and shall be able to assert to subscriber's home BSF the visited NAFs DNS name. The D-Proxy shall also be able to assert to the BSF that the visited NAF is authorized to request the GBA specific user profiles contained in the NAF request.

- The physical security level of the D-proxy shall not be lower than the highest level of the NAFs which it interfaces with.

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

4.3 Requirements and principles for bootstrapping

The following requirements and principles are applicable to bootstrapping procedure:

- the bootstrapping function shall not depend on the particular NAF;
- the server implementing the bootstrapping function needs to be trusted by the home operator to handle authentication vectors;
- the server implementing the NAF needs only to be trusted by the home operator to handle derived key material;
- it shall be possible to support NAF in the operator's home network and in the visited network;
- the architecture shall not preclude the support of network application function in ~~the visited network, or possibly even in~~ a third network;
- to the extent possible, existing protocols and infrastructure should be reused;
- in order to ensure wide applicability, all involved protocols are preferred to run over IP;
- it shall be prevented that a security breach in one NAF who using the GBA, can be used by an attacker to mount successful attacks to the other NAFs using the GBA.

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

4.3.3 Roaming

The roaming subscriber shall be able to utilize the bootstrapping function in the home network. The subscriber shall be able to utilize network application function that is in a visited network.

===== BEGIN NEXT 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.

Editor's note: In the visited NAF scenario, it should be decided how the communication between a D-Proxy and a BSF is secured. The possible solutions for securing this link include TLS and IPsec.

- 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 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.

===== END CHANGE ====