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: ⌘	Terminology changes		
Source: ⌘	Nokia, Siemens		
Work item code: ⌘	SSC-GBA	***Date:*** ⌘	02/05/2004
Category: ⌘	**D** *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.	***Release:*** ⌘	Rel-6 *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 usage of the term “subscriber profile information” has generated a lot of confusion in different working groups in 3GPP. Since the intended parameters are associated with user’s security settings needed in GAA, the term “subscriber profile information” or terms alike in the current TS, are changed to “user security settings” to clarify that the whole subscriber’s profile is not transferred over Zh and Zn interfaces. The user security settings transfer over Zn interface is missing in the subclause 4.5.3, although this transfer is visible in the Figure 5. This mistake is corrected.
Summary of change: ⌘	The term “subscriber profile information” or terms alike are changed to “user security settings”.
Consequences if not approved: ⌘	The clarification of terms is not done, more misinterpretation may occur.

Clauses affected: ⌘	3.1, 4.2.3, 4.3.5, 4.3.6, 4.4.3, 4.4.4, 4.5.2, 4.5.3			
	Y	**N**		
Other specs affected: ⌘		**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.

Editor's note: Definition to be completed.

Network Application Function: NAF is hosted in a network element under the control of an MNO.

Editor's note: Definition to be completed.

Transaction Identifier:

Editor's note: Definition to be completed.

User security settings: An application-specific parameter set describing the security related usage of bootstrapping function and some NAFs in the context of an application and in relation to a subscriber

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

4.2.3 HSS

~~HSS shall store new parameters~~The set of all user security settings is stored in the subscriber profile in the HSS.~~related to the use of the bootstrapping function~~. Possibly also parameters related to the usage of some NAFs are stored in the HSS. These parameters in general are called “user security settings”. If an application has user security settings there shall be only one set of user security settings per the application stored in the HSS.

Editor's note: Needed new subscriber profile parameters, i.e., user security settings, are FFS.

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

4.3.5 Requirements on Zh interface

The requirements for Zh 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 HSS are located within the same operator’s network.

- the BSF shall be able to send bootstrapping information request concerning a subscriber;
- the HSS shall be able to send 3GPP AKA vectors to the BSF in batches;
- the HSS shall be able to send the complete set of subscriber's GAA ~~profile information~~user security settings needed for security purposes to the BSF;

Editor's note: It's ffs how to proceed in the case where profile is updated in HSS after ~~profile is~~user security settings forwarded. The question is whether ~~this profile~~ change in user security settings 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;

Editor’s note: This requirement may need to be modified depending on what happens in the case where ~~the profile~~user security settings in the HSS is updated.

- the number of different interfaces to HSS should be minimized.

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~~a selected set of application-specific ~~subscriber profile information~~user security settings needed for security purposes from BSF depending on the policy of the BSF and the application indicated in the request from the NAF over Zn;
- 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.

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

4.4.3 Zh interface

Zh interface protocol used between the BSF and the HSS allows the BSF to fetch the required authentication information and ~~subscriber profile information~~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.

4.4.4 Zn interface

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

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

4.5.2 Bootstrapping procedures

When a UE wants to interact with a NAF, and it knows that the bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see figure 3). 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, or when the lifetime of the key in UE has expired (cf. subclause 4.5.3).

NOTE: The main steps from the specifications of the AKA protocol in TS 33.102 [2] and the HTTP digest AKA protocol in RFC 3310 [4] are repeated in figure 3 for the convenience of the reader. In case of any potential conflict, the specifications in TS 33.102 [2] and RFC 3310 [4] take precedence.

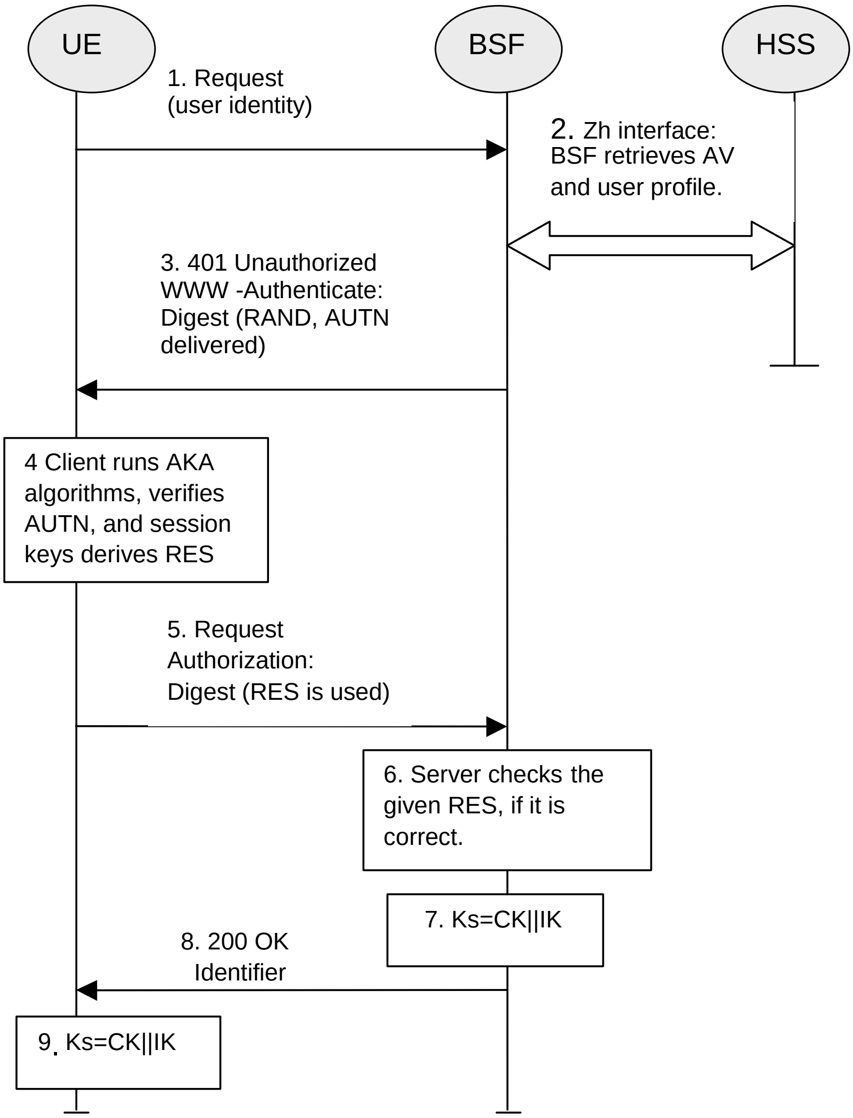

Figure 3: The bootstrapping procedure

1. The UE sends an HTTP request towards the BSF.

2. BSF retrieves the complete set of user ~~profile~~security settings and one or a whole batch of Authentication Vectors (AV, AV = RAND||AUTN||XRES||CK||IK) over the 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 checks AUTN to verify that the challenge is from an authorised 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 another HTTP request, containing the Digest AKA response (calculated using RES), to the BSF.

6. The BSF authenticates the UE by verifying the Digest AKA response.

7. The BSF generates key material Ks by concatenating CK and IK. The Transaction Identifier value shall be also generated in format of NAI by taking the RAND value from step 3, and the BSF server name, i.e. RAND@BSF_servers_domain_name.

8. The BSF shall send a 200 OK message, including a Transaction Identifier, to the UE to indicate the success of the authentication. The BSF also supplies a flag DER_FLAG to the UE, which indicates whether key derivation shall be applied to Ks or not. If key derivation is performed it is to be applied uniformly to all keys shared

between any UE and any NAF. In addition, in the 200 OK message, the BSF shall supply the lifetime of the key Ks, and an indication whether multiple key derivation shall be used. The key material Ks is generated in UE by concatenating CK and IK.

9. Both the UE and the BSF shall use the Ks to derive the key material Ks_NAF, if applicable. Ks_NAF is used for securing the Ua interface.

   Ks_NAF is computed as Ks_NAF = KDF (Ks, key derivation parameters), where KDF is a suitable key derivation function, and the key derivation parameters include the user's IMSI, the NAF_Id and RAND. The NAF_Id consists of the full DNS name of the NAF. KDF shall be implemented in the ME.

Editor's note: The definition of the KDF and the possible inclusion of further key derivation parameters are left to ETSI SAGE and to be included in the Annex B of the present specification.

If multiple key derivation is used then the UE and the BSF store the key Ks with the associated Transaction Identifier for further use, until the lifetime of Ks has expired, or until the key Ks is updated. Otherwise, the key Ks and the Transaction Identifier may be deleted in the UE and in the BSF after the key Ks_NAF has been derived.

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 and a set of NAF specific user security settings corresponding to Transaction Identifier supplied by the UE to the NAF used over Ua interface;
- 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, NAF specific user security settings if available and compatible with the BSF's policy, 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.

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.

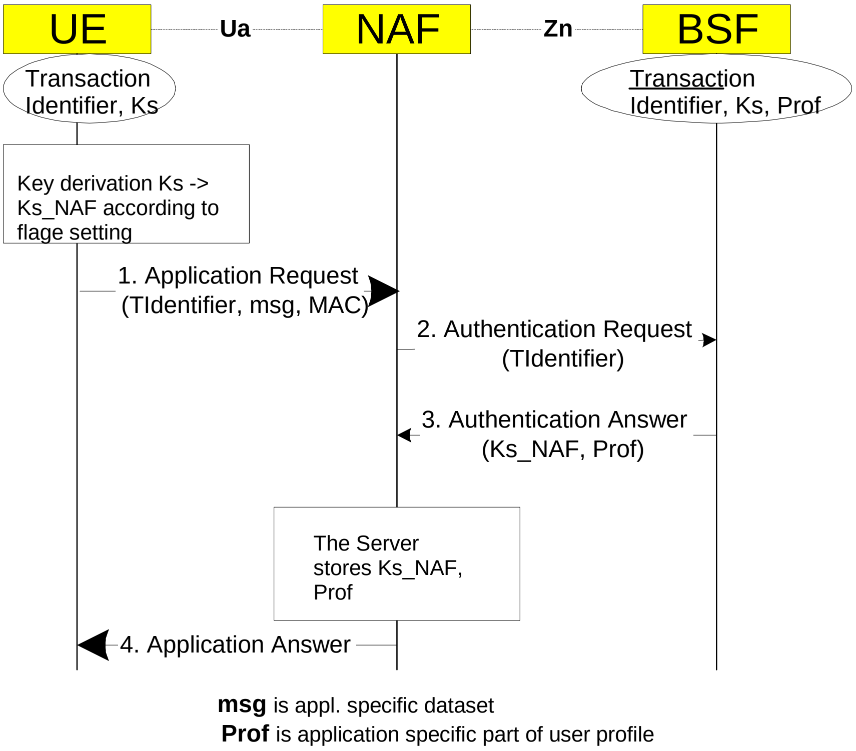
UE
Ua
NAF
Zn
BSF
Transaction Identifier, Ks
Transaction Identifier, Ks, Prof
Key derivation Ks -> Ks_NAF according to flage setting
1. Application Request (TIdentifier, msg, MAC)
2. Authentication Request (TIdentifier)
3. Authentication Answer (Ks_NAF, Prof)
The Server stores Ks_NAF, Prof
4. Application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

Figure 5: The bootstrapping usage procedure

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