3GPP TSG-SA WG3 SECURITY Meeting #35
St Paul's Bay, Malta, 5-8 October 2004

Tdoc ⌘ S3-040746

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.220** **CR** **022** ⌘ **rev** **-** ⌘ 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 **X**

Title:	⌘	Usage control of the service in visited network
Source:	⌘	Huawei
Work item code:	⌘	SEC1-SC
Date:	⌘	28/09/2004
Category:	⌘	**F**
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	When UE request the service in visited network, a D-proxy will retrieve the shared secrets and corresponding information from BSF located in home network for NAF located in visited network.There is no control of authorization whether the UE can use service in visited network.
Summary of change:	⌘	1 Addition of a requirement to the BSF. 2 Addition of a requirement to the reference point Zn 3 Addition of a sentence to procedure using bootstrapped Security Association: "When a request is from D-proxy in the Visited Network but not a NAF over Zn, the BSF shall check the existence of GBA user security setting, the agreement with operator of visited network and local policies of BSF to decide whether the user is permitted to access the application in the Visited Network or not. If the check is fail, the BSF will not provide any shared secrets to D-proxy and indicate D-proxy with failure cause.
Consequences if not approved:	⌘	The BSF function is incompleted

Clauses affected:	⌘	4.2.1, 4.4.3, 4.4.6, 4.5.3, 5.5.3

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

**********Begin of change**********

4.2 Network elements

4.2.1 Bootstrapping server function (BSF)

A generic Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and an operator-controlled Network Application Function (NAF). The BSF shall restrict the applicability of the key material to a specific NAF by using a suitable key derivation procedure. The key derivation procedure may be used with multiple NAFs during the lifetime of the key material. The lifetime of the key material is set according to the local policy of the BSF. The generation of key material is specified in clause 4.5.2.

The BSF shall be able to acquire the GBA user security settings from the HSS.

The BSF shall be able to provide authorization information to Diameter Proxy that is in a visited network.

NOTE: The authorization information may be only a flag or GBA user security settings according to the request of NAF and the local polices of BSF.

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;
- 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 acquire an (application-specific) user security setting from the HSS via the BSF;
- 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 requirements 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.

4.2.3 HSS

The set of all user security settings (USSs) is stored in the HSS. There shall be at most one USS per application stored in the HSS. In the case where the subscriber has multiple subscriptions, i.e. multiple ISIM or USIM applications on the UICC, the HSS shall contain one or more subscriber profiles that can be mapped to one or more private identities, i.e. IMPIs and IMSIs.

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

The requirement on the HSS are:

- HSS shall provide the only persistent storage for GBA USSs;
- GBA USS shall be defined in such a way that interworking of different operators for standardised application profiles is possible;
- GBA USS 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.

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 application on the ME using the shared secret to indicate the type of UICC application to use in bootstrapping (i.e., ISIM or USIM);
- 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]).

4.3 Bootstrapping architecture and reference points

4.3.1 Reference point Ub

The reference point Ub is between the UE and the BSF. Reference point Ub provides mutual authentication between the UE and the BSF. It allows the UE to bootstrap the session keys based on 3GPP AKA infrastructure.

The HTTP Digest AKA protocol, which is specified in RFC 3310 [4], is used on the reference point Ub. It is based on the 3GPP AKA TS 33.102 [2] protocol. The interface to the USIM is as specified in TS 31.102 [1] and to the ISIM is as specified in TS 31.103 [10].

4.3.2 Reference point Ua

The reference point Ua carries the application protocol, which is secured using the keys material agreed between UE and BSF as a result of the run of HTTP Digest AKA over reference point Ub. For instance, in the case of support for subscriber certificates TS 33.221 [5], it is a protocol, which allows the user to request certificates from the NAF. In this case the NAF would be the PKI portal.

4.3.3 Reference point Zh

The reference point Zh used between the BSF and the HSS allows the BSF to fetch the required authentication information and all GBA 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.

Editor's note: It is ffs, jointly with CN4 and SA2, whether the authorisation part of all USSs is transferred over Zh, or by other means. SA3 expresses a preference for Release 6, however, to transfer the authorisation part of the USSs for, at least, the GBA-specific entities PKI-portal (cf. TS. 33.221) and Authentication Proxy (TS 33.222) over Zh.

4.3.4 Reference point Zn

The reference point Zn is used by the NAF to fetch the key material agreed during a previous HTTP Digest AKA protocol run over the reference point Ub from the UE to the BSF. It is also used to fetch application-specific user security settings from the BSF, if requested by the NAF.

Editor's note: It is ffs, jointly with CN4 and SA2, whether the authorisation part of the application-specific USSs is transferred over Zn, or by other means. SA3 expresses a preference for Release 6, however, to transfer also the authorisation part of the application-specific USSs for, at least, the GBA-specific entities PKI-portal (cf. TS. 33.221) and Authentication Proxy (TS 33.222) over Zn.

4.4 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 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 is using the GBA, can be used by an attacker to mount successful attacks to the other NAFs using the GBA.

4.4.1 Access Independence

Bootstrapping procedure is access independent. Bootstrapping procedure requires IP connectivity from UE.

4.4.2 Authentication methods

Authentication between the UE and the BSF shall not be possible without a valid cellular subscription. Authentication shall be based on the 3GPP AKA protocol.

4.4.3 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.

BSF in the home network shall be able to decide whether the subscriber is permitted to utilize network application located in a visited network by the existence of GBA user security setting and the local policies of BSF.

4.4.4 Requirements on reference point Ub

The requirements for reference point Ub are:

- the BSF shall be able to identify the UE;
- the BSF and the UE shall be able to authenticate each other based on AKA;
- the BSF shall be able to send a bootstrapping transaction identifier to the UE;
- the UE and the BSF shall establish shared keys;
- the BSF shall be able to indicate to the UE the lifetime of the key material. The key lifetime sent by the BSF over Ub shall indicate the expiry time of the key.

NOTE: This does not preclude a UE to refresh the key before the expiry time according to the UE's local policy.

4.4.5 Requirements on reference point Zh

The requirements for reference point Zh 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 GBA user security settings needed for security purposes to the BSF;

Editor's note: It's ffs how to proceed in the case where GBA user security settings are updated in HSS after GBA user security settings were 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 reference point Zh 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 GBA user security settings in the HSS is updated.

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

4.4.6 Requirements on reference point Zn

The requirements for reference point Zn are:

- mutual authentication, confidentiality and integrity shall be provided;
- If the BSF and the NAF are located within the same operator's network, the Zn reference point shall be secured according to NDS/IP [13];
- If the BSF and the NAF are located in different operators' networks, the Zn' reference point between the D-Proxy and the BSF shall be secured using TLS as specified in RFC 2246 [6];

Editor’s Note: The TLS Certificate profiling needs to be completed and will be added into an Annex.

- The BSF shall verify that the requesting NAF is authorised;
- The NAF shall be able to send a key material request to the BSF, containing NAF's public hostname used by the UE's corresponding request. The BSF shall be able to verify that a NAF is authorized to use this hostname, i.e. the FQDN used by UE when it contacts the NAF;
- The BSF shall be able to send the requested key material to the NAF;
- The NAF shall be able to get a selected set of application-specific user security settings from the BSF, depending on the policy of the BSF and the application indicated in the request from the NAF over Zn;
- The NAF shall be able to indicate to the BSF the single application or several applications it requires user security settings for;

NOTE: If some application needs only a subset of an application-specific user security setting, e.g. only one IMPU, the NAF selects this subset from the complete set of user security settings sent from BSF.

- The BSF shall be able to configure on a per NAF or per application basis if private subscriber identity and which user security settings may be sent to a NAF;
- The BSF shall be able to indicate to the NAF the lifetime of the key material. The key lifetime sent by the BSF over Zn shall indicate the expiry time of the key, and shall be identical to the key lifetime sent by the BSF to the UE over Ub.
- The BSF shall be able to indicate whether the subscriber is permitted to use network application located in visited network over Zn

NOTE: This does not preclude a NAF to refresh the key before the expiry time according to the NAF's local policy.

Editor's note: It is ffs which actions are to be taken over Zn when the BSF receives a user security settings update from the HSS over Zh.

**********End of change**********

**********Begin of change**********

4.5.3 Procedures using bootstrapped Security Association

Before communication between the UE and the NAF can start, the UE and the NAF first have to agree whether to use shared keys obtained by means of the GBA. If the UE does not know whether to use GBA with this NAF, it uses the Initiation of Bootstrapping procedure described in clause 4.5.1.

Once the UE and the NAF have established that they want to use GBA then every time the UE wants to interact with an NAF the following steps are executed as depicted in figure 4.4.

UE starts communication over reference point Ua with the NAF:

- in general, UE and NAF will not yet share the key(s) required to protect the reference point Ua. If they already do (i.e. if a key Ks_NAF for the corresponding key derivation parameter NAF_Id 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 for the selected UICC application 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 for the selected UICC application is available in the UE, the UE first agrees on a new key Ks with the BSF over the reference point Ub, and then proceeds to derive Ks_NAF;

NOTE 1: If it is not desired by the UE to use the same Ks for the selected UICC application to derive more than one Ks_NAF then the UE should agree on a new key Ks with the BSF over the reference point Ub, and then proceed to derive Ks_NAF;

- if the NAF shares a key with the UE, but the NAF requires an update of that key, e.g. because the key's lifetime has expired, it shall send a suitable bootstrapping renegotiation request to the UE and terminates the protocol used over reference point Ua, see figure 4.5. The form of this indication depends on the particular protocol used over reference point Ua. If the UE receives a bootstrapping renegotiation request, it starts a run of the protocol over reference point Ub, as specified in clause 4.5.2, in order to obtain a new key Ks.

NOTE 2: To allow for consistent key derivation in BSF and UE, both have to use the same FQDN for derivation (see NOTE 2 of clause 4.5.2). For each protocol used over Ua it shall be specified if only cases (1) and (2) of NOTE 2 of clause 4.5.2 are allowed for the NAF or if the protocol used over Ua shall transfer also the FQDN used for key derivation by UE to NAF.

NOTE 3: If the shared key between UE and NAF is invalid , the NAF can set deletion conditions to the corresponding security association for subsequent removal.

- the UE supplies the B-TID to the NAF, in the form as specified in clause 4.3.2, to allow the NAF to retrieve the corresponding keys from the BSF;

NOTE 4: The UE may adapt the key material Ks_NAF to the specific needs of the reference point Ua. 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 reference point Ub 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 reference point Zn with BSF

- The NAF requests key material corresponding to the B-TID supplied by the UE to the NAF over reference point Ua. If the NAF has several FQDNs, which may be used in conjunction with this specification, then the NAF shall transfer in the request over Zn the same FQDN, which was used over Ua (see NOTE 2 on key derivation in this clause);

- The NAF may also request application-specific user security settings for the applications, which the request received over Ua from UE may access;

- With the key material request, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able verify that NAF is authorized to use that hostname;

- The BSF derives the keys required to protect the protocol used over reference point Ua from the key Ks and the key derivation parameters, as specified in clause 4.5.2, and supplies to NAF the requested key Ks_NAF, as well as the lifetime of that key. If the key identified by the B-TID 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 bootstrapping renegotiation request to the UE.

NOTE 5: The NAF shall adapt the key material Ks_NAF to the specific needs of the reference point Ua in the same way as the UE did. This adaptation is outside the scope of this specification.

- When a request is from D-proxy in the Visited Network but not a NAF over Zn, the BSF shall check the existence of GBA user security setting, the agreement with operator of visited network and local policies of BSF to decide whether the user is permitted to access the application in the Visited Network or not. If the check is fail, the BSF will not provide any shared secrets to D-proxy and indicate D-proxy with failure cause.

NOTE : The USS may not exist for every application; in this case, the decision is based on the local policies of BSF.

- The BSF may also send the private user identity (IMPI) and requested user security settings to NAF according to the BSF's policy;

NAF continues with the protocol used over the reference point Ua with the UE.

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

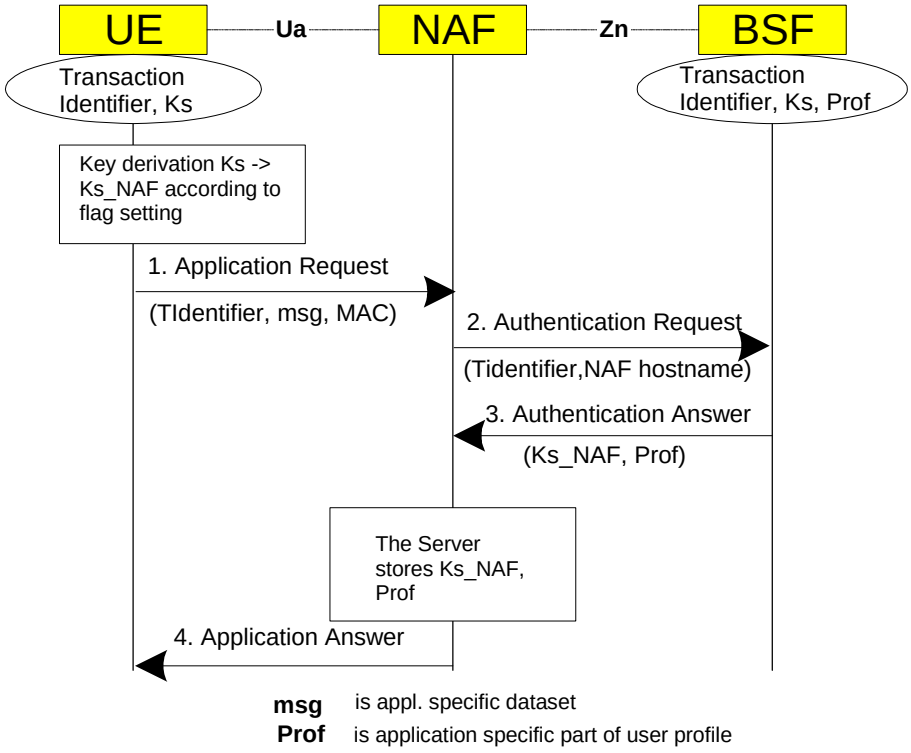

Figure 4.4: The bootstrapping usage procedure

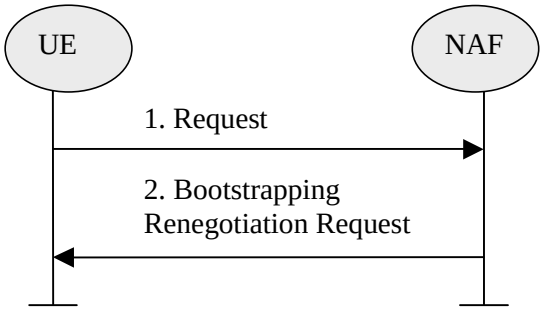

Figure 4.5: Bootstrapping renegotiation request

**********End of change**********

**********Begin of change**********

5.3.3 Procedures using bootstrapped Security Association

Before communication between the UE and the NAF can start, the UE and the NAF first have to agree whether to use shared keys obtained by means of the GBA. If the UE does not know whether to use GBA with this NAF, it uses the Initiation of Bootstrapping procedure described in clause 5.3.1.

Once the UE and the NAF have established that they want to use GBA then every time the UE wants to interact with a NAF the following steps are executed as depicted in figure 5.3.

Next, the UE and the NAF have to agree, which type of keys to use, Ks_ext_NAF or Ks_int_NAF, or both. The default is the use of Ks_ext_NAF only. This use is also supported by MEs and NAFs, which are GBA_U unaware. If Ks_int_NAF, or both Ks_ext and Ks_int are to be used, this use has to be agreed between UE and NAF prior to the execution of the procedure described in the remainder of this clause 5.3.3. Any such agreement overrules the default use of the keys. How this agreement is reached is application-specific and is not within the scope of this document.

NOTE 1: This agreement may be mandated by the specification, which defines the Ua reference point between UE and NAF, e.g. TS 33.246 for the use of GBA in MBMS, or negotiated by the NAF and the UE over the Ua reference point, or reached by configuration.

Editors' Note: The support of unaware GBA_U MEs, which are GBA_ME aware only is FFS.

In general, UE and NAF will not yet share the key(s) required to protect the Ua reference point. If they do not, the UE proceeds as follows:

- if Ks_ext_NAF is required and a key Ks_ext for the selected UICC application is available in the UE, the UE derives the key Ks_ext_NAF from Ks_ext, as specified in clause 5.3.2;

- if Ks_int_NAF is required and a key Ks_int for the selected UICC application is available in the UICC, the ME requests the UICC to derive the key Ks_int_NAF from Ks_int, as specified in clause 5.3.2;

NOTE 2: If it is not desired by the UE to use the same Ks_ext/int for the selected UICC application to derive more than one Ks_ext/int_NAF then the UE should first agree on new keys Ks_ext and Ks_int with the BSF over the Ub reference point, as specified in clause 5.3.2, and then proceeds to derive Ks_ext_NAF or Ks_int_NAF, or both, as required.

- if Ks_ext and Ks_int for the selected UICC application are not available in the UE, the UE first agrees on new keys Ks_ext and Ks_int with the BSF over the Ub reference point, as specified in clause 5.3.2, and then proceeds to derive Ks_ext_NAF or Ks_int_NAF, or both, as required;

- if the NAF shares a key with the UE, but the NAF requires an update of that key, it shall send a suitable bootstrapping renegotiation request to the UE and terminate the protocol used over Ua reference point. The form of this indication depends on the particular protocol used over Ua reference point. If the UE receives a bootstrapping renegotiation request, it starts a run of the protocol over Ub, as specified in clause 5.3.2, in order to obtain new keys.

NOTE 3: If the shared keys between UE and NAF become invalid, the NAF can set deletion conditions to the corresponding security association for subsequent removal.

NOTE 4: If it is not desired by the NAF to use the same Ks to derive more than one Ks_int/ext_NAF then the NAF should always reply to the first request sent by a UE by sending a key update request to the UE.

UE and NAF can now start the communication over Ua reference point using the keys Ks_ext_NAF or Ks_int_NAF, or both, as required. They proceed as follows:

- The UE supplies the B-TID to the NAF, as specified in clause 5.3.2, to allow the NAF to retrieve the corresponding keys from the BSF

NOTE 5: To allow for consistent key derivation in BSF and UE, both have to use the same FQDN for derivation (cf. NOTE 2 of clause 4.5.2). For each protocol used over Ua it shall be specified if only cases (1) and (2) of NOTE 2 of clause 4.5.2 are allowed for the NAF or if the protocol used over Ua shall transfer also the FQDN used for key derivation by UE to NAF.

NOTE 6: The UE may adapt the keys Ks_ext_NAF or Ks_int_NAF to the specific needs of the Ua reference point. This adaptation is outside the scope of this specification.

- when the UE is powered down, or when the UICC is removed, any GBA_U keys shall be deleted from storage in the ME. There is no need to delete keys Ks_int and Ks_int_NAF from storage in the UICC;

NOTE 7: After each run of the protocol over the Ub reference point, new keys Ks_ext and Ks_int, associated with a new B-TID, are derived in the UE according to clause 5.3.2, so that it can never happen, that keys Ks_ext and Ks_int with different B-TIDs simultaneously exist in the UE.

- When new keys Ks_ext and Ks_int are agreed over the Ub reference point and new NAF-specific keys need to be derived for one NAF_Id, then both, Ks_ext_NAF and Ks_int_NAF (if present), shall be updated for this NAF_Id, but further keys Ks_ext_NAF or Ks_int_NAF relating to other NAF_Ids, which may be stored on the UE, shall not be affected;

NOTE 8: This rule ensures that the keys Ks_ext_NAF and Ks_int_NAF are always in synch at the UE and the NAF.

NAF now starts communication over the Zn reference point with the BSF.

- The NAF requests from the BSF the keys corresponding to the B-TID, which was supplied by the UE to the NAF over the Ua reference point. If the NAF is GBA_U aware it indicates this by including a corresponding flag in the request. If the NAF has several FQDNs, which may be used in conjunction with this specification, then the NAF shall transfer in the request over Zn the same FQDN, which was used over Ua (see note above on key derivation in this clause).

- The NAF may also request application-specific user security settings for the applications, which the request received over Ua from UE may access;

- With the keys request over the Zn reference point, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able to verify that NAF is authorized to use that hostname.

- The BSF derives the keys Ks_ext_NAF, and Ks_int_NAF (if additionally required), as specified in clause 5.3.2. If the NAF indicated in its request that it is GBA_U aware, the BSF supplies to NAF both keys, Ks_ext_NAF, and Ks_int_NAF, otherwise the BSF supplies only Ks_ext_NAF. In addition, the BSF supplies the lifetime time of these keys. If the key identified by the B-TID 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 bootstrapping renegotiation request (See figure 4.5) to the UE;

NOTE: The NAF may adapt the keys Ks_ext_NAF and Ks_int_NAF to the specific needs of the Ua reference point in the same way as the UE did. This adaptation is outside the scope of this specification.

- The BSF may also send the private user identity (IMPI) and requested user security settings to NAF according to the BSF's policy.

- When a request is from D-proxy in the Visited Network but not a NAF over Zn, the BSF shall check the existence of GBA user security setting, the agreement with operator of visited network and local policies of BSF to decide whether the user is permitted to access the application in the Visited Network. If the check is fail, the BSF will not provide any shared secrets to D-proxy and indicate D-proxy with failure cause.

NOTE: The USS may not exist for every application, in this case, the decision is based on the local policies of BSF.

The NAF now continues with the protocol used over the Ua reference point with the UE.

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

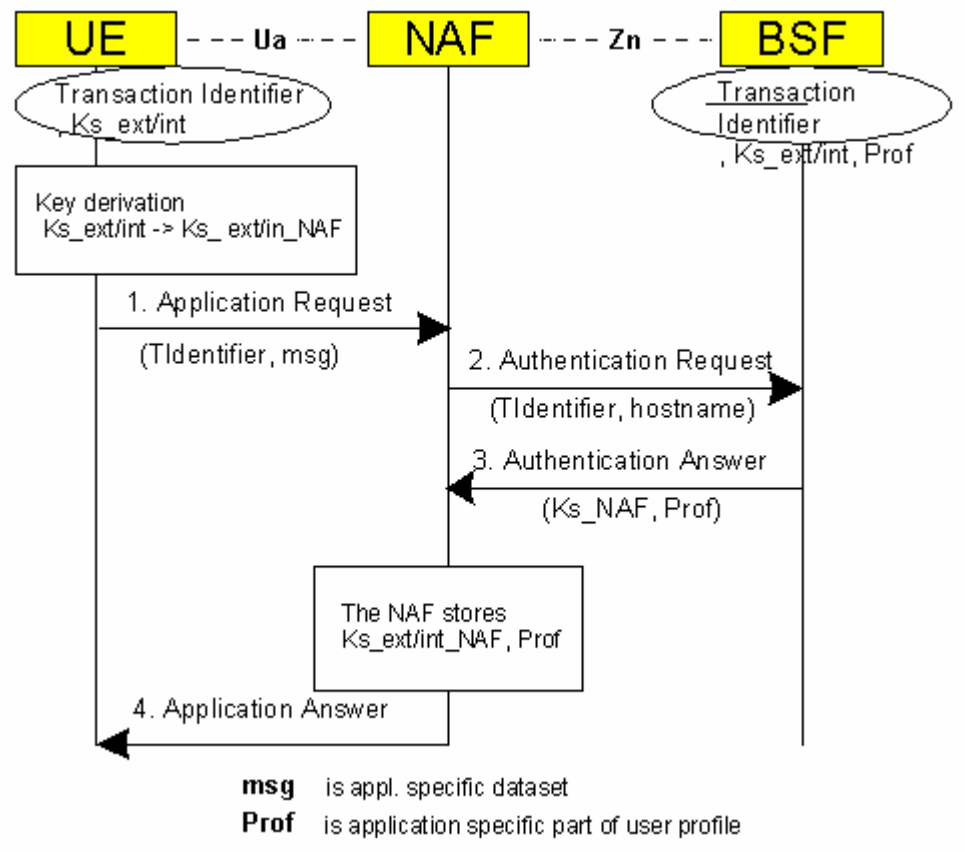

Figure 5.3: The bootstrapping usage procedure with UICC-based enhancements

**********End of change**********