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

Tdoc ⌘S3-040433

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:	⌘	Editorial changes and clarifications to TS 33.220
Source:	⌘	SA WG3
Work item code:	⌘	SSC-GBA
Date:	⌘	10/05/2004
Category:	⌘	**D**
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:	⌘	Removal of editor's notes, need for clarification of text
Summary of change:	⌘	Replace "interface" by "reference point", switch sections on requirements and reference points, clarify "initiation of bootstrapping" procedure, clarify Procedures using bootstrapped Security Association
Consequences if not approved:	⌘	Unresolved editor's notes, unclear text.

Clauses affected:	⌘	3.1, 3.2, 4.1, 4.3, 4.4, 4.5

		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	none
			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.

Bootstrapping Transaction Identifier:

Editor's note: Definition to be completed.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and Key Agreement
B-TID	Bootstrapping Transaction Identifier
BSF	Bootstrapping Server Function
CA	Certificate Authority
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IK	Integrity Key
KDF	Key Derivation Function
MNO	Mobile Network Operator
NAF	Network Application Function
PKI	Public Key Infrastructure

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

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

4.1 Reference model

Figure 4.1 shows a simple network model of the entities involved in the bootstrapping approach, and the ~~interface~~reference points used between them.

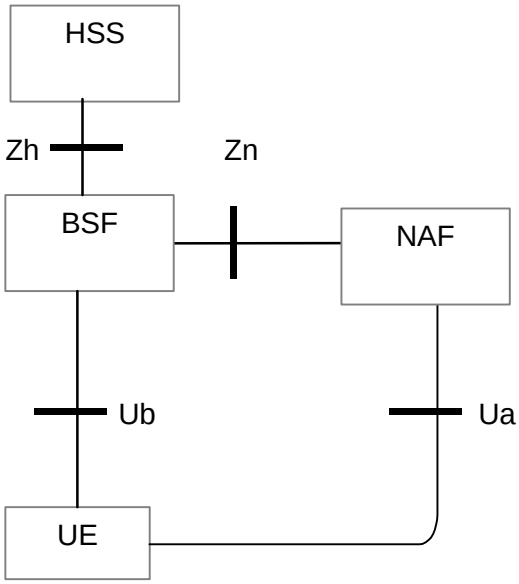


Figure ~~4.~~1: Simple network model for bootstrapping

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

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

4.~~4~~3 Bootstrapping architecture and reference points

4.~~4~~3.1 Reference point Ub ~~interface~~

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 ~~interface~~ 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].

4.~~4~~3.2 Reference point Ua ~~interface~~

The reference point Ua ~~interface~~ 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 ~~interface~~. 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.~~4~~3.3 Reference point Zh ~~interface~~

The reference point Zh ~~interface protocol~~ used between the BSF and the HSS allows 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.

4.43.4 Reference point Zn interface

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

4.34 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;
- 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 is using the GBA, can be used by an attacker to mount successful attacks to the other NAFs using the GBA.

4.34.1 Access Independence

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

4.34.2 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.

4.34.3 Roaming

The roaming subscriber shall be able to utilize the bootstrapping function in the home network.

4.34.4 Requirements on reference point Ub interface

The requirements for reference point Ub interface 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 Transaction Identifier to the UE.

4.34.5 Requirements on reference point Zh interface

The requirements for reference point 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 subscriber's GAA profile information 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 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 ~~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 in the HSS is updated.

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

4.~~3~~4.6 Requirements on reference point Zn ~~interface~~

The requirements for reference point 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 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 reference point 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.

4.~~3~~4.7 Requirements on Transaction Identifier

Transaction identifier shall be used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn ~~interfaces~~.

Requirements for Transaction Identifier are:

- Transaction Identifier shall be globally unique;
- Transaction Identifier shall be usable as a key identifier in protocols used in the reference point Ua ~~interface~~;
- NAF shall be able to detect the home network and the BSF of the UE from the Transaction Identifier.

Editor's note: Parallel use of GBA and non-GBA infrastructure is ffs. There are use cases when NAF may want to use GBA and non-GBA based infrastructures at the same time. For example, a NAF may want to authenticate subscribers both by using normal HTTP Digest authentication (where the usernames and passwords are distributed using some other mechanism than GBA), and by using GBA based HTTP Digest. However, it seems that in most telecommunication protocols, the server side (i.e. NAF) controls the name space related to key identifiers (cf. Transaction Identifier). For example, in HTTP authentication, the server issues the usernames, and does not allow the re-use of already existing usernames. The parallel use of GBA and non-GBA based infrastructures may cause conflicts on Transaction Identifier namespace. In particular, BSF may assign Transaction Identifier values that NAFs are already using with non-GBA UEs.

Editor's note: GBA shall further specify on how security associations are removed and/or updated in NAF.

~~4.4 Bootstrapping architecture and reference points~~

~~4.4.1 Ub interface~~

~~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 Ub interface. 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].~~

~~4.4.2 Ua interface~~

~~The Ua interface 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 Ub interface. 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.~~

~~4.4.3 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 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 from the BSF.~~

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

********** begin change **********.

4.5.1 Initiation of bootstrapping

Before communication between the UE and the NAF can start, the UE and the NAF first have to agree whether to use the GBA. When a UE wants to interact with a NAF, but it does not know if the NAF requires ~~the bootstrapping procedure is required~~the use of shared keys obtained by means of the GBA, ~~it~~the UE shall contact the NAF for further instructions (see figure4.2).

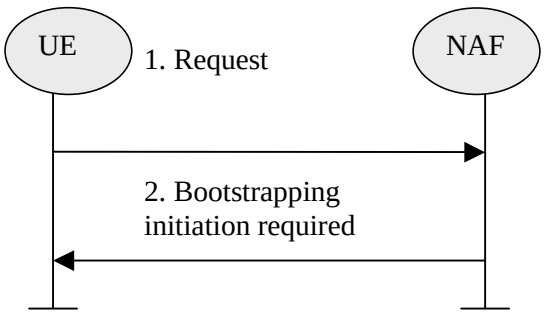


Figure 4.2: Initiation of bootstrapping

1. UE starts communication over reference point Ua ~~interface~~ with the NAF without any ~~bootstrapping~~GBA-related parameters.

2. If the NAF requires ~~bootstrapping~~ the use of shared keys obtained by means of the GBA, but the request from UE does not include ~~bootstrapping~~GBA-related parameters, the NAF replies with a bootstrapping initiation message. The form of this indication may depend on the particular reference point Ua ~~interface~~ and is specified in the relevant stage 3-specifications.

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 ~~4.~~ 4.3). Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a ~~key update~~ bootstrapping renegotiation 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.

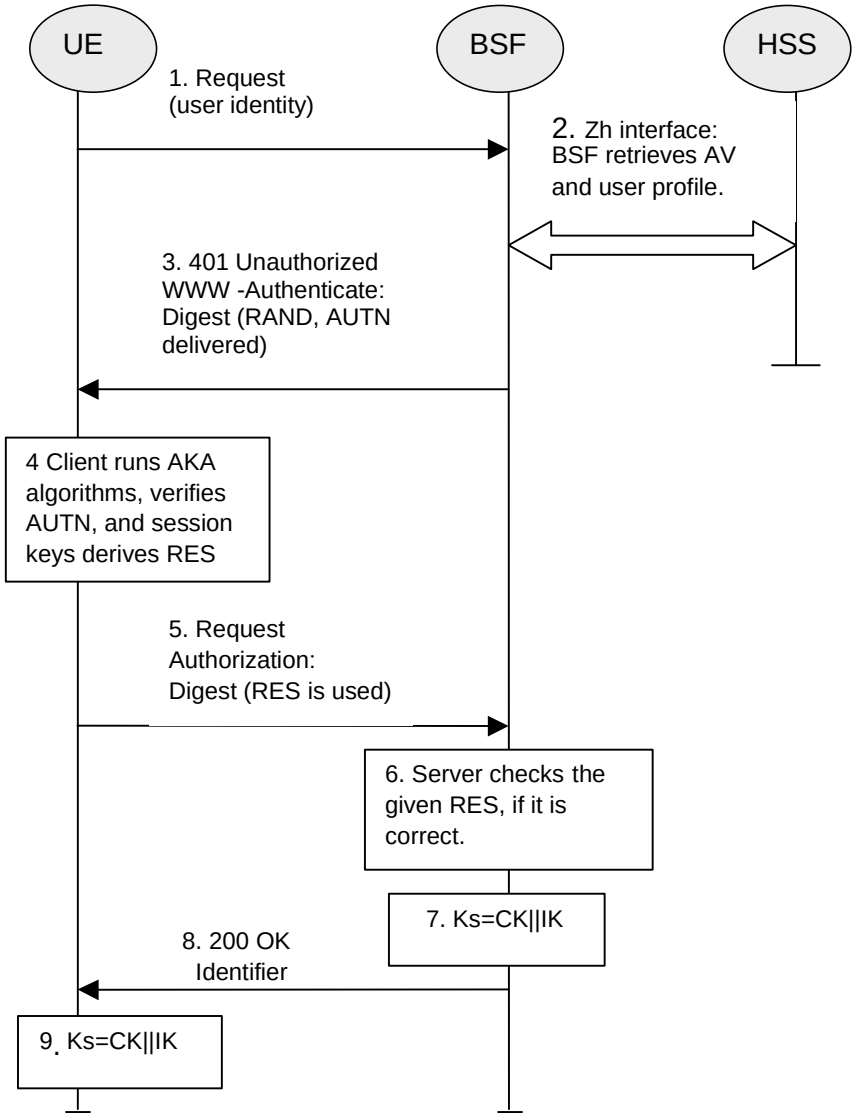


Figure 4.3: The bootstrapping procedure

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

2. BSF retrieves the user profile and one or a whole batch of Authentication Vectors (AV, AV = RAND||AUTN||XRES||CK||IK) over the reference point 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 during the procedures as specified in section 4.5.3~~, if applicable~~. Ks_NAF is used for securing the reference point 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

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 section 4.5.1.

Once the UE and the NAF have established that they want to use GBA ~~After UE is authenticated with the BSF, every~~ then every time the UE wants to interact with an NAF the following steps are executed as depicted in figure ~~5~~4.4.

UE starts communication over reference point Ua ~~interface~~ with the NAF:

- in general, UE and NAF will not yet share the key(s) required to protect the reference point 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 reference point Ub ~~interface~~, and then proceeds to derive Ks_NAF;
- if the NAF shares a key with the UE, but the NAF requires an update of that key ~~is needed~~, e.g. because the key's lifetime has expired, it shall send a suitable bootstrapping renegotiation~~key update~~ request to the UE and terminate~~s~~ the protocol used over reference point Ua ~~interface~~, cf. Figure 4.5. The form of this indication ~~may~~ depends on the particular protocol used over reference point Ua ~~interface (cf. 4.5.1)~~; If the UE receives a

bootstrapping renegotiation request, it starts a run of the protocol over Ub, as specified in section 4.5.2, in order to obtain a new key Ks.

- the UE supplies the Transaction Identifier to the NAF, in the form ~~of a Transaction Identifier~~as specified in subsection 4.3.2, to allow the NAF to retrieve the corresponding keys from the ~~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 may ~~shall~~ adapt the key material Ks_NAF to the specific needs of the reference point 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 reference point 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 reference point Zn ~~interface~~ with BSF

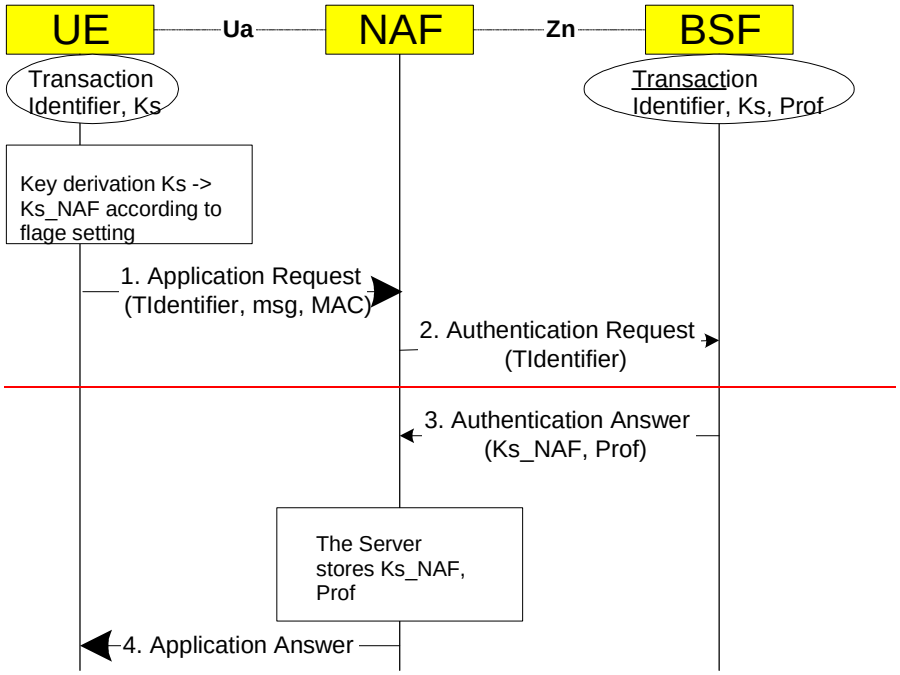
- The NAF requests key material corresponding to Transaction Identifier supplied by the UE to the NAF ~~used~~ over the reference point Ua ~~interface~~;

- The BSF derives the keys required to protect the protocol used over reference point 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 bootstrapping renegotiation ~~key update~~ request to the UE.

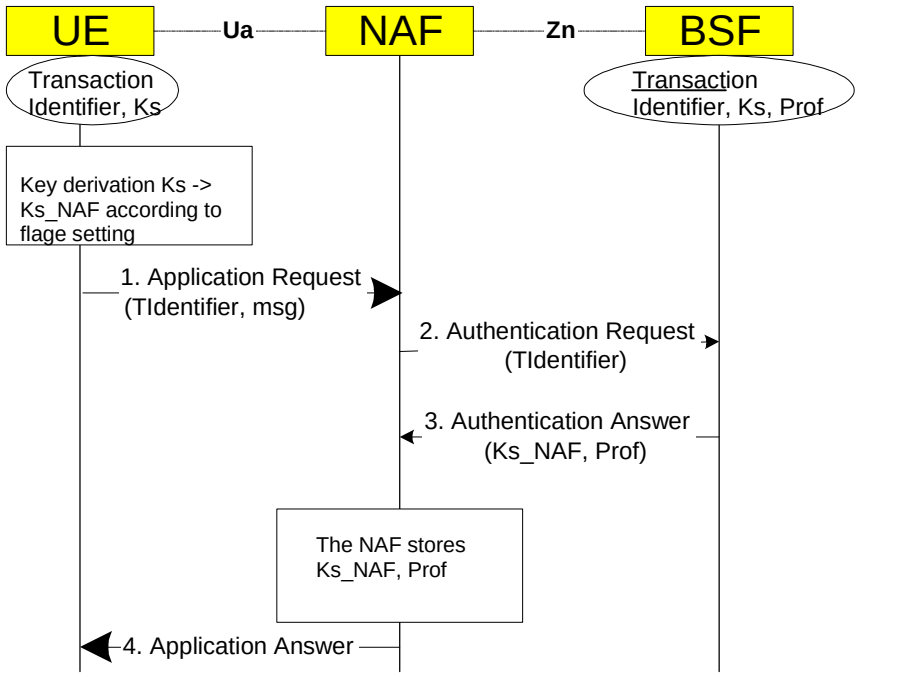
NOTE: The NAF ~~shall~~ may adapt the key material Ks_NAF to the specific needs of the reference point Ua ~~interface~~ in the same way as the UE did. This adaptation is outside the scope of this specification.

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

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



msg is appl. specific dataset
Prof is application specific part of user profile



msg is appl. specific dataset
Prof is application specific part of user profile

Figure 4.4~~5~~: The bootstrapping usage procedure

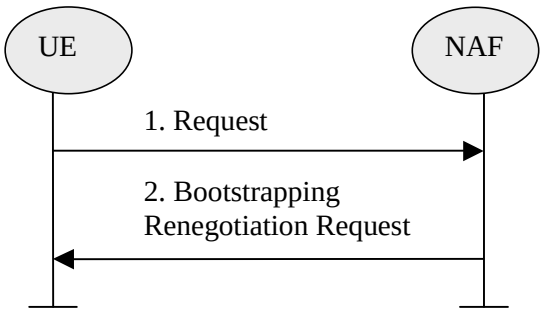


Figure 4.5: Bootstrapping renegotiation request

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