3GPP TSG SA WG3 Security — S3#32 **S3-040060**
09 - 13 February 2004, Edinburgh, Scotland, UK

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.220 CR CRNum** ⌘ **rev** ⌘ Current version: 1.0.0 ⌘

*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
Source:	⌘	Vodafone, Nokia
Work item code:	⌘	GBA and Support for subcriber certificates
Date:	⌘	18/1/2004
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:

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: ⌘ To correct and clarify the specification.

Summary of change: ⌘ Editorial corrections and stylistic changes to clarify the TS, improve consistency of terminology and improve readability.

Cleanup definitions and abbreviations.

Add references.

Add some editor's notes to clarify certain incomplete parts of the TS.

Change order of some sections to improve overall structure of TS.

Consequences if not approved: ⌘

Clauses affected: ⌘ 1, 3, 4.

Other specs affected: ⌘

Y	N		
	X	Other core specifications	⌘
	X	Test specifications	
	X	O&M Specifications	

Other comments: ⌘

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 [5]~~, etc~~. ~~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.

Editor's note: The specification objects are scheduled currently in phases. For the first phase of standardisation, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. In later phases, other configurations may be considered.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application".

[2] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

[3] Franks J., et al,: "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[4] A. Niemi, et al,: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC3310, September 2002.

[5] 3GPP TS 33.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[6] T. Dierks, et al,: "The TLS Protocol Version 1.0", RFC 2246, January 1999.

3 Definitions and a~~A~~bbreviations

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.

3.2 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and Key Agreement
BSF	Bootstrapping ~~s~~Server ~~f~~Function~~ality~~ ~~BSF is hosted in a network element under the control of an MNO.~~
~~BSP~~	~~BootStrapping Procedure~~
CA	Certificate Authority
~~CMP~~	~~Certificate Management Protocols~~
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IK	Integrity Key
MNO	Mobile ~~n~~Network ~~o~~Operator
NAF	~~Operator-controlled n~~Network ~~a~~Application ~~f~~Function ~~functionality.~~ ~~NAF is hosted in a network element under the control of an MNO.~~
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
~~SCP~~	~~Subscriber Certificate Procedure~~
UE	User Equipment

4 Generic Bootstrapping Architecture

The 3GPP authentication infrastructure, including the 3GPP Authentication Centre (AuC), the USIM, and the 3GPP AKA protocol run between them, is a very valuable asset of 3GPP operators. It has been recognised that this infrastructure could be leveraged to enable application functions in the network and on the user side to ~~communicate in situations where they would not be able to do so without the support of the 3GPP authentication infrastructure~~establish shared keys. Therefore, 3GPP can provide the "bootstrapping of application security" to authenticate the subscriber by defining a generic bootstrapping function based on AKA protocol.

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.

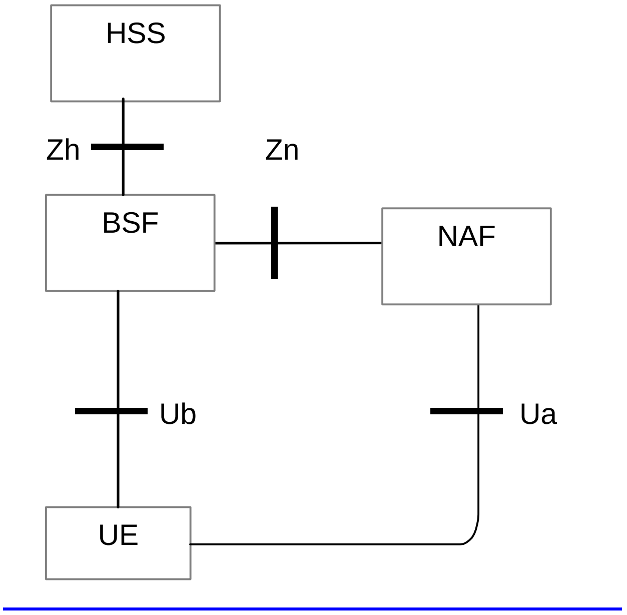


Figure 1: Simple network model for bootstrapping

4.~~1~~2 Network elements

4.~~23.~~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 key material must be generated specifically for each NAF independently, that is, for each key uniquely identified by a transaction identifier and that is shared between a UE and a NAF there is a new run of HTTP Digest AKA [4] over the Ub interface. The BSF can restrict the applicability of the key material to a defined set of NAFs by using a suitable key derivation procedure.

Editor's note: Key generation for NAF is ffs. Potential solutions may include:
- Separate run of HTTP Digest AKA over Ub interface for each request of key material from a NAF
- Issues with key lifetime are ffs.

4.~~23.~~2.2 Network application function (NAF)

After the bootstrapping has been completed, the UE and an operator-controlled network application function (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 network application function (NAF):

- 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 bootstrapping server function (BSF) during ~~running~~ the run of the application-specific protocol.

4.~~23.~~2.3 HSS

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

Editor's note: Needed new parameters are FFS.

4.~~23.~~2.4 UE

The required ~~new ~~functionalities from the UE are:

- the support of HTTP Digest AKA protocol;
- the capability to derive new key material to be used with the protocol over Ua interface from CK and IK; and
- support of NAF-~~-~~specific application protocol (see [5]).

4.3 Requirements and principles for bootstrapping

Editor's note: The description of AKA bootstrapping shall be added here.

- The bootstrapping function shall not depend on the particular network application function.
- The server implementing the bootstrapping function needs to be trusted by the home operator to handle authentication vectors.
- The server implementing the network application function needs only to be trusted by the home operator to handle derived key material.
- It shall be possible to support network application functions 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.

Editor's note: The specification objects are scheduled currently in phases. For the first phase of standardisation, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. In later phases, other configurations may be considered.

- 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 ~~application server~~network application function using the Generic Bootstrapping Architecture can be used by an attacker to mount successful attacks to the other network application ~~servers ~~functions using the ~~G~~generic b~~B~~ootstrapping ~~A~~architecture.

4.~~12~~3.1 Access Independence

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

4.~~12~~3.2 Authentication methods

~~Authentication method that is used to authenticate the bootstrapping function must be dependent on cellular subscription. In other words, a~~Authentication ~~to ~~between the UE and the bootstrapping server function shall not be possible without a valid cellular subscription. Authentication shall be based on the 3GPP AKA protocol.

4.~~12~~3.3 Roaming

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

Editor's note: For the first phase of standardisation, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. In later phases, other configurations may be considered.

4.~~12~~3.4 Requirements on Ub interface

The requirements for 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.~~12~~3.5 Requirements on Zh interface

The requirements for Zh interface are:

- Mutual authentication, confidentiality and integrity shall be provided.~~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~~ 3GPP AKA vectors to the BSF in batches.
- The HSS shall be able to send the subscriber's GAA profiles to the BSF.

Editor's note: the intention is not to send all the application-specific profile information, but only the information needed for security purposes.

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.

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.

- It is preferred to reuse existing specifications if possible.
- The number of different interfaces to HSS should be minimized.

4.~~12~~3.6 Requirements on Zn interface

The requirements for Zn interface are:

- Mutual authentication, confidentiality and integrity shall be provided.
- The BSF shall verify that the 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 from BSF.

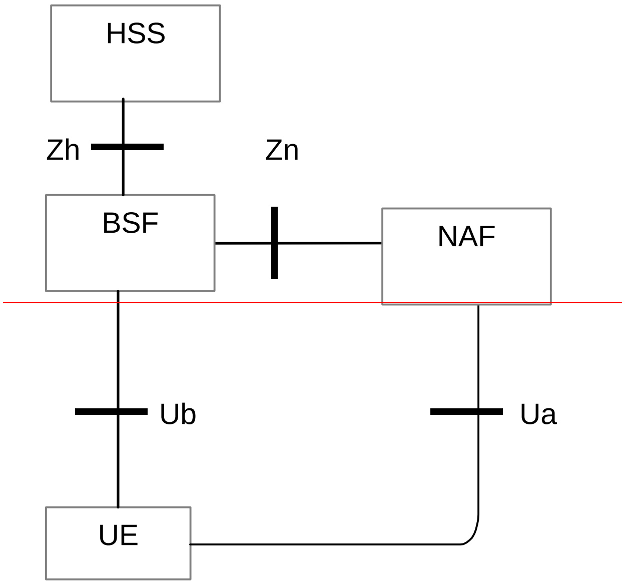
Editor's note: The intention is not to send all the application-specific profile information, but only the information needed for security purposes.

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

4.~~23~~4 Bootstrapping architecture

4.~~23~~4.1 ~~Reference model~~Protocols

~~Figure 1 shows a simple network model of the entities involved in the bootstrapping approach, and the protocols used among them.~~



~~**Figure 1: Simple network model for bootstrapping**~~

Figure 2 illustrates a protocol stacks structure in network elements that are involved in bootstrapping of application security from 3G AKA~~ and support for subscriber certificates~~.

Editor's note: The current protocol stack figure is placed here as a holder. The actual protocols will be defined later.

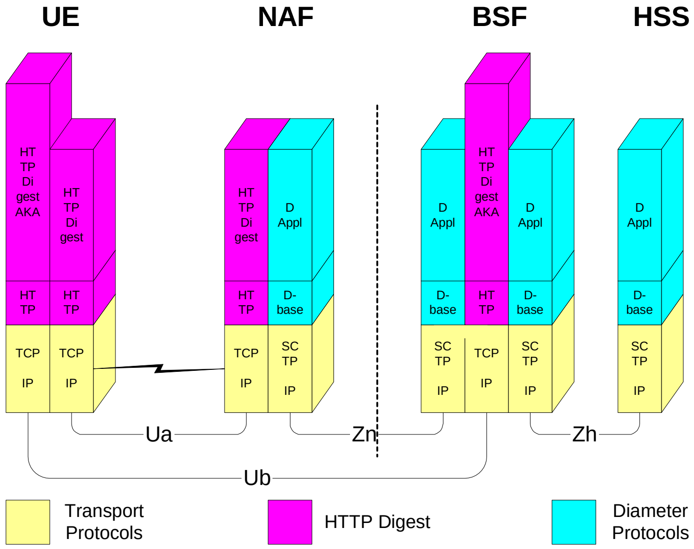


Figure 2: Protocol stack architecture

Editor's note: The protocol on the Ua interface is NAF-specific. An example of the Ua interface protocol when the NAF is HTTP-based is given in Annex A.

~~4.23.2 Network elements~~

~~4.23.2.1 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 key material must be generated specifically for each NAF independently, that is, for each key uniquely identified by a transaction identifier and that is shared between a UE and a NAF there is a new run of HTTP Digest AKA [4] over the Ub interface. The BSF can restrict the applicability of the key material to a defined set of NAFs by using a suitable key derivation procedure.~~

~~Editor's note: Key generation for NAF is ffs. Potential solutions may include:~~

- ~~Separate run of HTTP Digest AKA over Ub interface for each request of key material from a NAF~~
- ~~Issues with key lifetime are ffs.~~

~~4.23.2.2 Network application function (NAF)~~

~~After the bootstrapping has been completed, the UE and an operator-controlled network application function (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 network application function (NAF):~~

- ~~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 bootstrapping server function (BSF) during running the run of the application-specific protocol.~~

~~4.23.2.3 HSS~~

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

~~Editor's note: Needed new parameters are FFS.~~

~~4.23.2.4 UE~~

~~The required new functionalities from the UE are:~~

- ~~the support of HTTP Digest AKA protocol;~~
- ~~the capability to derive new key material to be used with the protocol over Ua interface from CK and IK; and~~
- ~~support of NAF_ specific application protocol (see [5]).~~

4.~~23~~4.~~3~~2 Reference points

4.~~23~~4.~~3~~2.1 Ub interface

The reference point Ub is between the UE and the BSF. The functionality is radio access independent and can be run in both CS and PS domains.

Editor's note: The solution for CS domain is ffs.

4.~~23~~4.~~3~~2.1.1 Functionality

Reference point Ub provides mutual authentication between the UE and the BSF entities. It allows the UE to bootstrap the session keys based on ~~the~~ 3GPP AKA infrastructure. The session key as result of key agreement functionality, is used to support further applications e.g. certificate issuer.

4.~~23~~4.~~3~~2.1.2 Protocol

~~Ub interface is in format of~~ The HTTP Digest AKA protocol, which is specified in [4], is used on the Ub interface. It is based on the 3GPP AKA [2] protocol that requires ~~information~~ functions from USIM and/or ISIM. The interface to the USIM is as specified in~~for 3G~~ [1].

4.~~23~~4.~~3~~2.2 Ua interface

The Ua interface carries~~is~~ 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 [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.~~23~~4.~~3~~2.3 Zh interface

Zh interface ~~is~~ protocol used between the BSF and the HSS ~~to~~ 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.~~23~~4.~~3~~2.4 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.

4.~~34~~5 Procedures

This chapter specifies in detail the format of the bootstrapping procedure that is further utilized by various applications. It contains the AKA authentication procedure with BSF, and ~~latter~~ the key material generation procedure.

4.~~34~~5.1 Initiation of bootstrapping

When a UE wants to interact with an NAF, but it does not know if bootstrapping procedure is required, it shall contact NAF for further instructions (see figure 3).

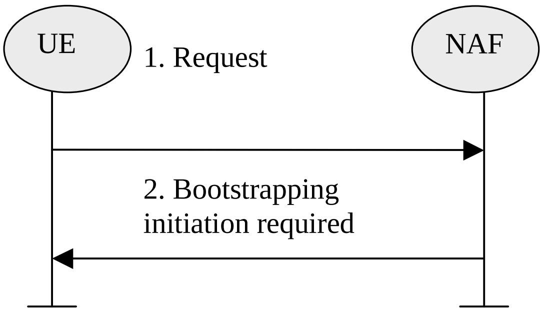


Figure 3: Initiation of bootstrapping

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

2. If the NAF require bootstrapping but the request from UE does not include bootstrapping~~-~~related parameters, NAF replies with a bootstrapping initiation message. The form of this indication may depend on the particular Ua interface and is ffs.

Editor's note: If the protocol over Ua interface is based on HTTP, then NAF can initiate the bootstrapping procedure by using HTTP status codes (e.g. 401 Unauthorized).

4.~~34~~5.2 Bootstrapping procedures

When a UE wants to interact with an NAF, and it knows that the bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see figure 4)

Editor's note: 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 4.3.3).

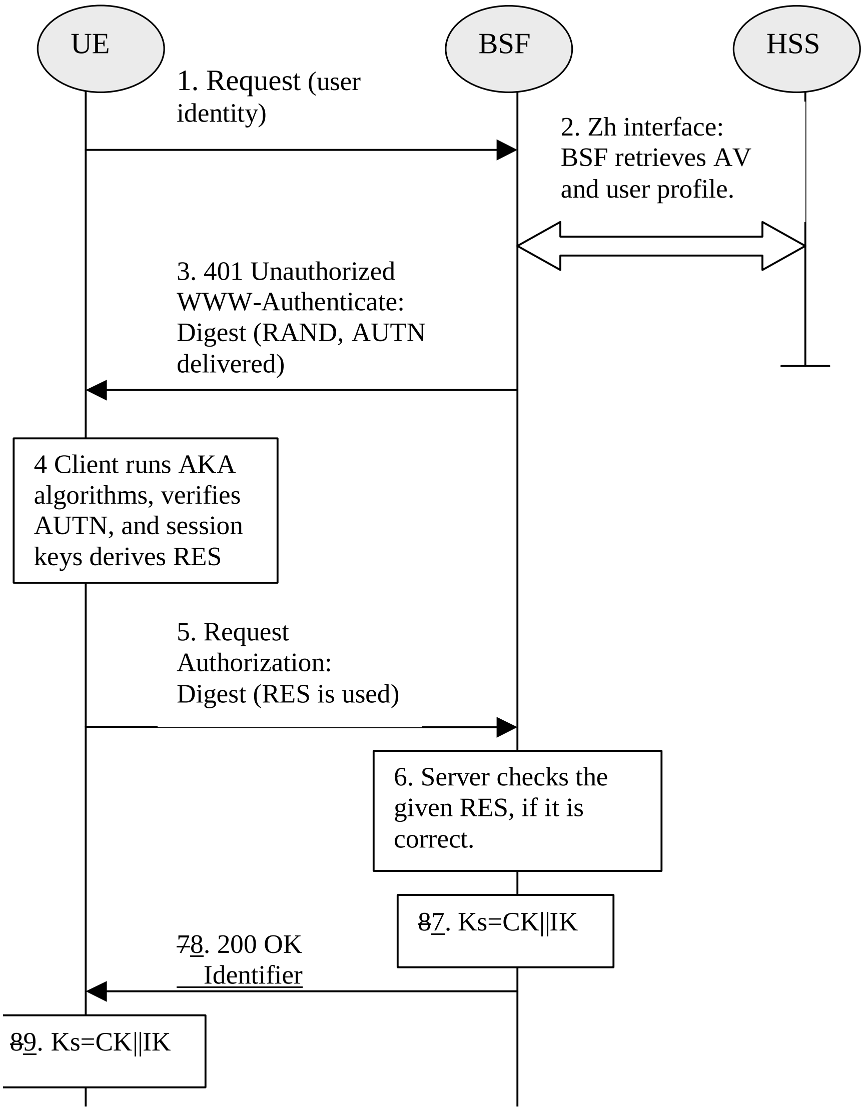

UE
BSF
HSS
1. Request (user identity)
2. Zh interface: BSF retrieves AV and user profile.
3. 401 Unauthorized WWW-Authenticate: Digest (RAND, AUTN delivered)
4 Client runs AKA algorithms, verifies AUTN, and session keys derives RES
5. Request Authorization: Digest (RES is used)
6. Server checks the given RES, if it is correct.
~~8~~7. Ks=CK||IK
~~7~~8. 200 OK Identifier
~~8~~9. Ks=CK||IK

Figure 4: The bootstrapping procedure

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

2. BSF retrieves the 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~~ checks AUTN to verify that the challenge is from an authorised~~enticated~~ 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, ~~again, with~~containing the Digest AKA response (calculated using RES), ~~as the response~~ to the BSF.

6. The BSF authenticates the UE by verifying the Digest AKA response.~~If the RES equals to the XRES that is in the AV, the UE is authenticated.~~

7. The BSF generates key material Ks by concatenating CK and IK. Ks is used to derive the key material Ks_NAF. Ks_NAF is used for securing the Ua interface.

8. The BSF shall send a 200 OK message, ~~and shall supply~~including a transaction identifier, to the UE to indicate the success of the authentication. The BSF may also supply the parameter *n* used to determine the NAF_Id_n (cf. ~~previous~~ next bullet) to the UE over the Ub interface. ~~If the parameter *n* is not supplied then no key derivation is performed, i.e. Ks = Ks_NAF.~~

9. The key material Ks is generated in UE by concatenating CK and IK. The Ks is used to derive the key material Ks_NAF. 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_n and RAND. The NAF_Id_n consists of the n rightmost domain labels in the DNS name of the NAF, separated by dots (n= 1, ..., 7). For n = 0, NAF_Id_n equals the full DNS name of the NAF. The next bullet specifies how the UE obtains n.

NOTE: This note gives an example how to obtain the NAF_Id_n: if the DNS name of the NAF is "server1.presence.bootstrap.operator.com", and n = 3, then NAF_Id_n = " bootstrap.operator.com".

If the parameter *n* is not supplied then no key derivation is performed, i.e. Ks = Ks_NAF.

Editor's note: The definition of the KDF and the possible inclusion of further key derivation parameters is left to ETSI SAGE.

4.~~34~~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, 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 is necessary, 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, in the form of~~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, as specified in clause 4.3.2.

NOTE 1: The UE may adapt the key material Ks_NAF to the specific needs of the Ua interface. This adaptation is outside the scope of this specification.

NAF starts communication over Zn interface with BSF

- The NAF requests key material corresponding to the information supplied by the UE to the NAF (in the form of~~e.g.~~ a transaction identifier) in the start of the protocol used over Ua interface.

- The BSF derives the keys required to protect the protocol used over Ua interface from the key material and the key derivation parameters, as specified in clause 4.3.2, and 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.

NOTE 2: The NAF may 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.

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

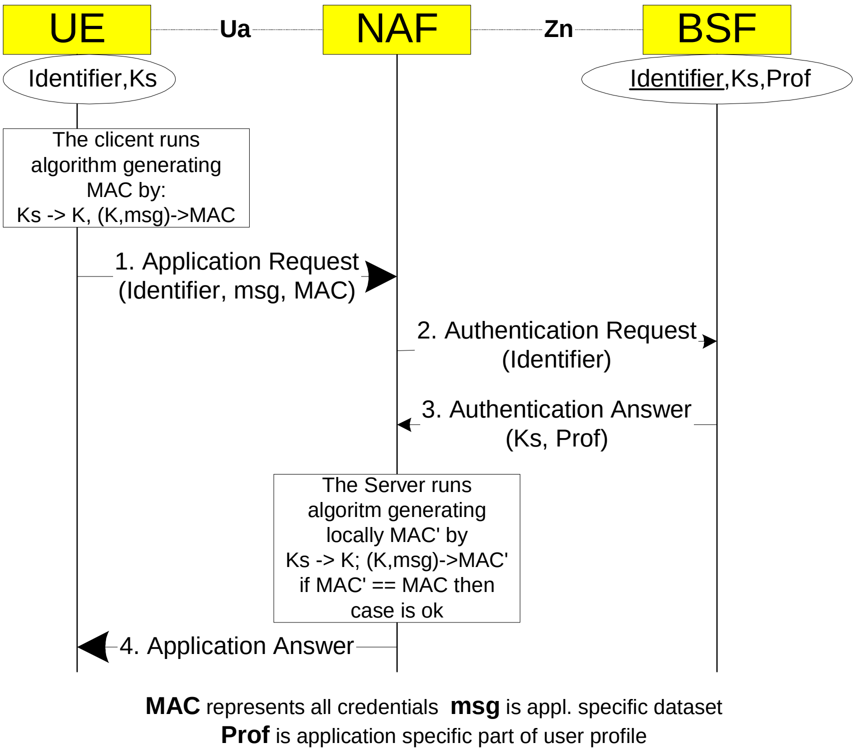

UE
Ua
NAF
Zn
BSF
Identifier,Ks
Identifier,Ks,Prof
The clicent runs algorithm generating MAC by: Ks -> K, (K,msg)->MAC
1. Application Request (Identifier, msg, MAC)
2. Authentication Request (Identifier)
3. Authentication Answer (Ks, Prof)
The Server runs algoritm generating locally MAC' by Ks -> K; (K,msg)->MAC' if MAC' == MAC then case is ok
4. Application Answer
MAC represents all credentials msg is appl. specific dataset
Prof is application specific part of user profile

Figure 5: The bootstrapping usage procedure