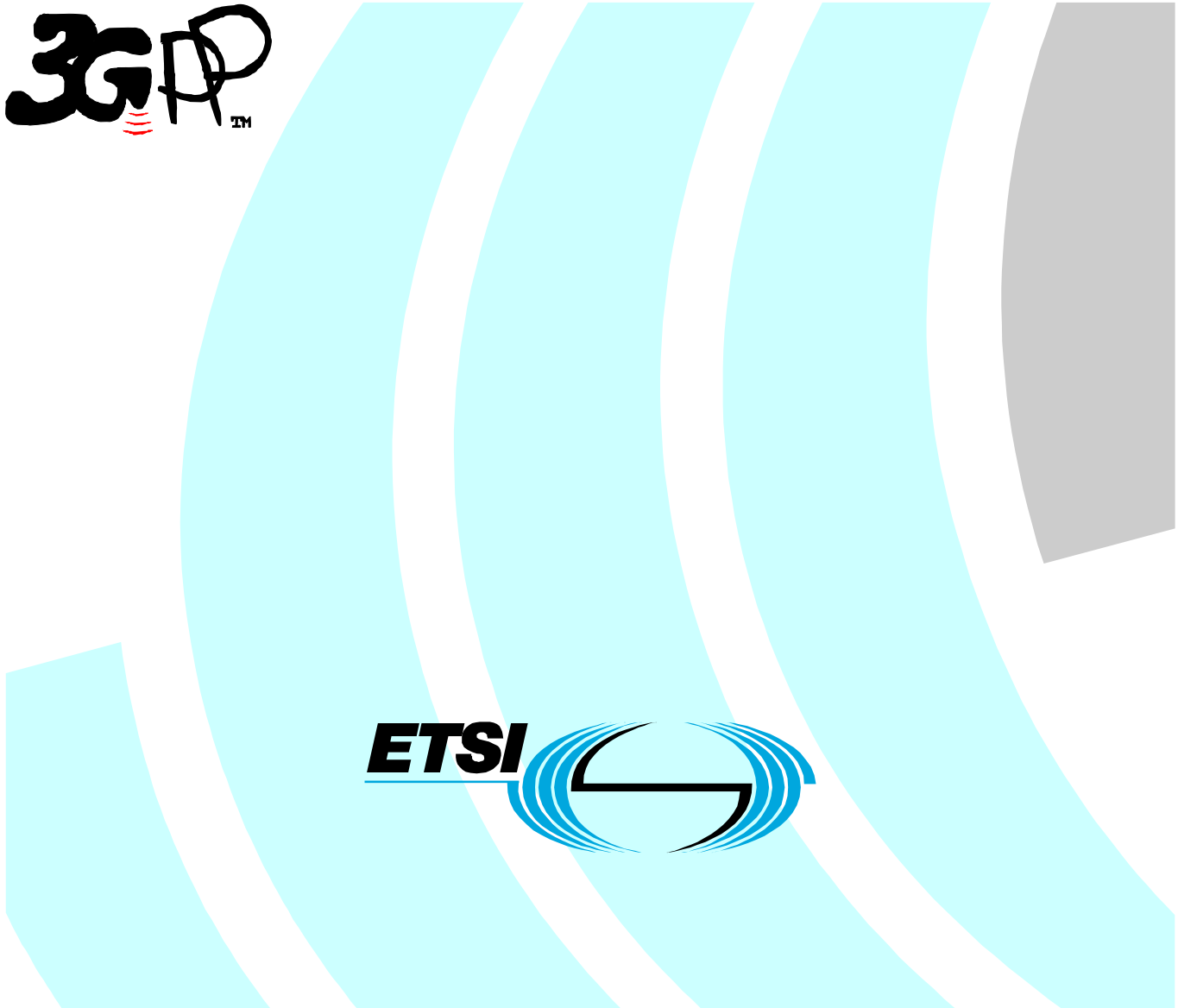
ETSI TS 133 220 V7.3.0 (2006-03)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
Generic Authentication Architecture (GAA);
Generic bootstrapping architecture
(3GPP TS 33.220 version 7.3.0 Release 7)



Reference
RTS/TSGS-0333220v730

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

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

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

Clause 4 of this specification describes a mechanism, called GBA_ME, to bootstrap authentication and key agreement, which does not require any changes to the UICC. Clause 5 of this specification describes a mechanism, called GBA_U, to bootstrap authentication and key agreement, which does require changes to the UICC, but provides enhanced security by storing certain derived keys on the UICC.

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] Void

[4] A. Niemi, et al,: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, 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] Void

[7] Void

[8] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 6)".

[9] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

[10] 3GPP TS 31.103: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[11] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[12] IETF RFC 3548 (2003): "The Base16, Base32, and Base64 Data Encodings".

[13] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[14] IETF RFC 3588 (2003): "Diameter Base Protocol".

[15] 3GPP TS 31.101: "3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[16] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".

[17] IETF RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[18] IETF RFC 2818 (2000): "HTTP over TLS".

[19] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Network Domain Security (NDS); Authentication Framework (AF)".

[20] IETF RFC 2560 (1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[21] FIPS PUB 180-2 (2002): "Secure Hash Standard".

[22] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".

[23] ISO/IEC 10118-3:2004: "Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions".

[24] IETF RFC 3629 (2003): "UTF-8, a transformation format of ISO 10646".

[25] 3GPP TS 33.222: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[26] 3GPP TS 33.246: "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)".

[27] IETF RFC 4279 (2005): "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)"

[28] IETF RFC 2246 (1999): "The TLS Protocol Version 1".

[29] 3GPP TS 24.109: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[30] OMA WAP-219-TLS, 4.11.2001: http://www.openmobilealliance.org/tech/affiliates/wap/wap-219-tls-20010411-a.pdf.

[31] OMA WAP-211-WAPCert, 22.5.2001: http://www.openmobilealliance.org/tech/affiliates/wap/wap-211-wapcert-20010522-a.pdf.

3 Definitions, abbreviations symbols and conventions

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Application: In all places in this document where the term application is used to refer to a service offered by the MNO or a third party to the mobile subscriber, then it always denotes the type of application and not the actual instance of an application installed on an application server.

Bootstrapping Server Function: BSF is hosted in a network element under the control of an MNO. BSF, HSS, and UEs participate in GBA in which a shared secret is established between the network and a UE by running the bootstrapping procedure. The shared secret can be used between NAFs and UEs, for example, for authentication purposes.

Bootstrapping Usage Procedure: A procedure using bootstrapped security association over Ua reference point.

GBA Function: A function on the ME executing the bootstrapping procedure with BSF (i.e. supporting the Ub reference point) and providing Ua applications with security association to run bootstrapping usage procedure. GBA function is called by a Ua application when a Ua application wants to use bootstrapped security association.

ME-based GBA: in GBA_ME, all GBA-specific functions are carried out in the ME. The UICC is GBA-unaware. If the term GBA is used in this document without any further qualification then always GBA_ME is meant, see clause 4 of this specification.

UICC-based GBA: this is a GBA with UICC-based enhancement. In GBA_U, the GBA-specific functions are split between ME and UICC, see clause 5 of this specification.

Network Application Function: NAF is hosted in a network element. GBA may be used between NAFs and UEs for authentication purposes, and for securing the communication path between the UE and the NAF.

Bootstrapping Transaction Identifier: the bootstrapping transaction identifier (B-TID) is used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn.

GBA User Security Settings: GUSS contains the BSF specific information element and the set of all application-specific USSs.

GUSS timestamp: the timestamp of the GUSS is set by the HSS. It changes whenever the HSS has modified the GUSS.

NAF Group: A grouping of NAFs to allow assignment of different USSs to NAFs representing the same application. This grouping is done in each home network separately, i.e. one NAF contacting BSFs in different home networks belongs to different groups in every home network.

NAF_Id: The full DNS name of the NAF, concatenated with the Ua security protocol identifier.

Ua Application: An application on the ME intended to run bootstrapping usage procedure with a NAF.

Ua security protocol identifier: An identifier which is associated with a security protocol over Ua.

User Security Setting: A USS is an application and subscriber specific parameter set that defines two parts, an authentication part, which contains the list of identities of the user needed for the application (e.g. IMPUs, MSISDN, pseudonyms), and an authorisation part, which contains the user permission flags (e.g. access to application allowed, type of certificates which may be issued). In addition, a USS may contain a key selection indication, which is used in the GBA_U case to mandate the usage of either the ME-based key (Ks_(ext)_NAF) or the UICC-based key (Ks_int_NAF) or both. Sometimes also called application-specific user security setting. The USS is delivered to the BSF as a part of GUSS from the HSS, and from the BSF to the NAF if requested by the NAF.

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
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GBA_ME	ME-based GBA
GBA_U	GBA with UICC-based enhancements
GUSS	GBA User Security Settings
HSS	Home Subscriber System
IK	Integrity Key
KDF	Key Derivation Function
Ks_int_NAF	Derived key in GBA_U which remains on UICC
Ks_ext_NAF	Derived key in GBA_U
MNO	Mobile Network Operator
NAF	Network Application Function
PKI	Public Key Infrastructure
SLF	Subscriber Locator Function
USS	User Security Setting

3.3 Symbols

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

||	Concatenation
⊕	Exclusive or

3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

4 Generic Bootstrapping Architecture

The 3GPP authentication infrastructure, including the 3GPP Authentication Centre (AuC), the USIM or the ISIM, 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 establish shared keys. Therefore, 3GPP can provide the "bootstrapping of application security" to authenticate the subscriber by defining a Generic Bootstrapping Architecture (GBA) based on AKA protocol.

4.1 Reference model

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

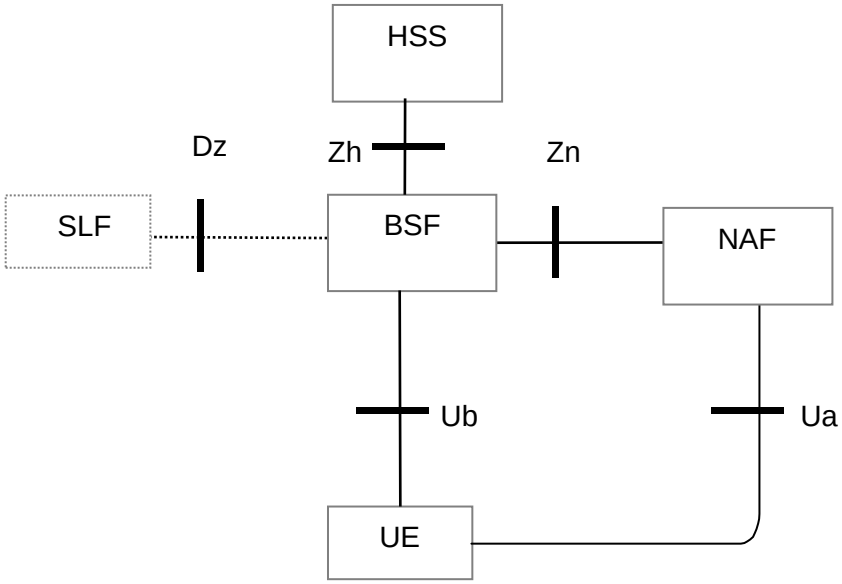
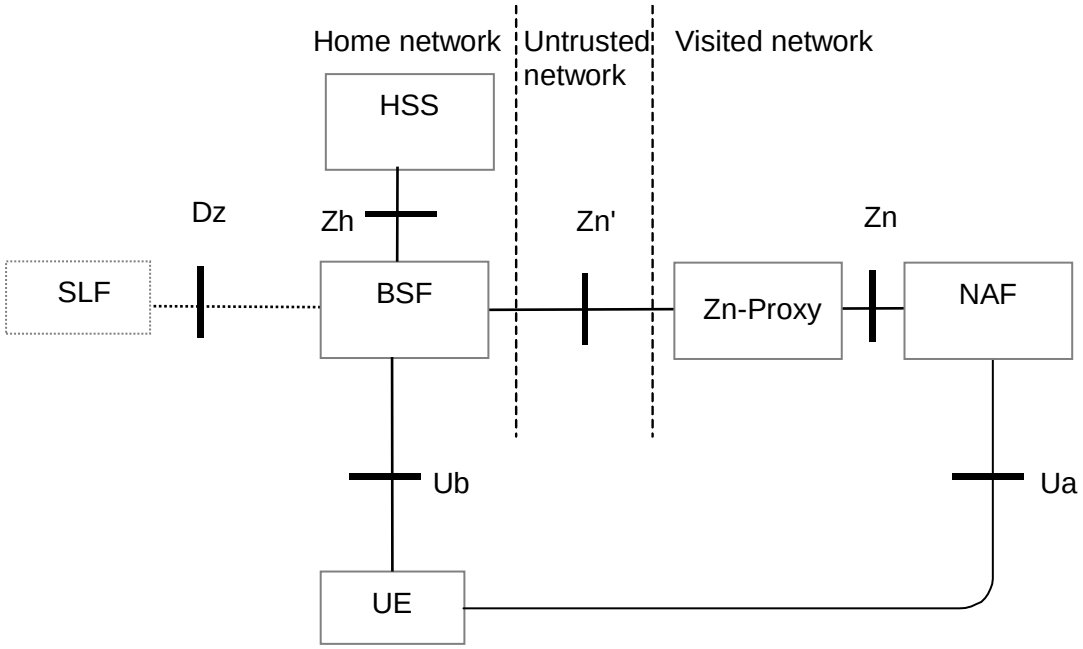


Figure 4.1: Simple network model for bootstrapping

Figure 4.1a shows a simple network model of the entities involved when the network application function is located in the visited network.



NOTE: The Zn' reference point is distinguished from the Zn reference point in that it is used between operators.

Figure 4.1a: Simple network model for bootstrapping in visited network

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 a Network Application Function (NAF). The BSF shall restrict the applicability of the key material to a specific NAF by using the key derivation procedure as specified in Annex B. 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 (GUSS) from the HSS.

The BSF shall be able to keep a list, which assigns NAFs to NAF Groups. This list is used to select if any and which application-specific USS within GUSS is valid for a certain NAF.

NOTE 1: The operator does the assignment of NAFs to NAF Groups. NAF Group definitions in HSS and all connected BSFs belonging to the same operator's network shall be equal (cf., clause 4.2.3). As these network elements belong to the same operator's network, standardisation of the NAF Group definitions themselves is not necessary in 3GPP.

NOTE 2: The NAF grouping may be e.g. "home" and "visited". It allows the BSF to send USSs for the same application with e.g. different authorization flags to different NAFs, e.g., in home network and visited networks. The NAF e.g. in visited network indicates only the requested application, but it is unaware of the grouping in home network of the subscriber.

4.2.2 Network application function (NAF)

After the bootstrapping has been completed, the UE and a 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 a 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 zero or more application-specific USSs from the HSS via the BSF;
- NAF shall be able to set the local validity condition of the shared key material according to the local policy;
- in the case of GBA_U, the NAF shall be able to determine which key (i.e., Ks_ext_NAF or Ks_int_NAF or both) should be used by using a local policy in the NAF or a key selection indication in the application-specific USS. If the NAF has received an application-specific USS, which contains the key selection indication, this shall override the local policy in the NAF;
- NAF shall be able to check lifetime and local validity condition of the shared key material.

NOTE: Without additional measures, GBA does not guarantee the freshness of the key, Ks(_int/ext)_NAF in the sense that it does not guarantee that the key was not used in a previous run of the Ua protocol. The additional measures which may be taken by the UE and the NAF to ensure key freshness in GBA are:
1) enforce a new run of the Ub protocol (thus generating a new Ks) before deriving a new Ks_NAF.
2) store previously used keys Ks(_int/ext)_NAF, or the corresponding key identifiers B-TID, until the end of their lifetime.

A UE and a NAF that support a Ua protocol that does not provide replay protection over unconnected runs of the protocol, will need to take corresponding action to avoid replay attacks if desired.

4.2.2a Zn-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 Zn-Proxy of the NAFs network to communicate with subscriber’s BSF (i.e. home BSF).

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

General requirements for the functionality of Zn-Proxy are:

- Zn-Proxy shall be able to function as a proxy between the visited NAF, and the subscriber’s home BSF;
- Zn-Proxy shall be able to locate subscriber’s home BSF and communicate with it over secure channel;
- Zn-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 Zn-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 Zn-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), i.e. GUSS, is 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 GUSSs that can be mapped to one or more private identities, i.e. IMPIs and IMSIs.

The requirements on the HSS are:

- HSS shall provide the only persistent storage for GUSSs;
- GUSS shall be defined in such a way that interworking of different operators for standardised application profiles is possible;
- GUSS 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.
- GUSS shall be able to contain application-specific USSs that contain parameters that are related to key selection indication in the case of GBA_U (i.e., whether the NAF shall use Ks_ext_NAF or Ks_int_NAF), identification or authorization information of one or more applications hosted by one ore more NAFs. Any other types of parameters are not allowed in the application-specific USS.

NOTE 1: The necessary subscriber profile data may be fetched by the NAF directly from HSS or from its local database using identity information provided by the application-specific USS.

NOTE 2: The HSS may temporarily remove an application-specific USS from the GUSS if the service is temporarily revoked from the subscriber.

- GUSS shall be able to contain parameters intended for the BSF usage:
  - the type of the UICC the subscriber is issued (i.e. is it GBA_U aware or not, cf. subclause 5);
  - subscriber specific key lifetime:
  - optionally the timestamp indicating the time when the GUSS has been last modified by the HSS.

NOTE 3: These parameters are optional and if they are missing from subscriber's GUSS or subscriber does not have GUSS then the BSF will use the default values in the BSF local policy defined by the particular MNO.

- HSS shall be able to assign application-specific USSs to a NAF Group. This shall be defined in such a way that different USSs for the same application, but for different groups of NAFs, are possible. The restrictions on the number of USSs per GUSS are dependent on the usage of NAF Groups by the operator:
  - if no NAF Groups are defined for this application then at most one USS per application is stored in GUSS;
  - if NAF Groups are defined for this application then at most one USS per application and NAF Group is stored in GUSS.
- NAF Group definitions in the HSS and all connected BSFs belonging to the same operator's network shall be equal.

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 a Ua application on the ME to indicate to the GBA Function on the ME the type or the name of UICC application to use in bootstrapping (see clause 4.4.8);
- 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]).

A GBA-aware ME shall support both GBA_U, as specified in clause 5.2.1 and GBA_ME procedures, as specified in clause 4.5.

4.2.5 SLF

The SLF:

- is queried by the BSF in conjunction with the Zh interface operation to get the name of the HSS containing the required subscriber specific data.
- is accessed via the Dz interface by the BSF.

The SLF is not required in a single HSS environment. Use of SLF is not required when BSF are configured/managed to use pre-defined HSS.

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.

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.

4.3.5 Reference point Dz

The reference point Dz used between the BSF and the SLF allows the BSF to get the name of the HSS containing the required subscriber specific data.

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.
- an attacker shall not be able to exploit a security breach in one security protocol over Ua in order to mount a successful attack against a different security protocol over Ua.

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 requirements on roaming are:

- 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.
- The home network shall be able to control whether its subscriber is authorized to use the service in the visited network.

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 1: 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;
- optionally the BSF may have the capability able to send the timestamp of subscriber's GBA user security settings to the HSS (timestamp option);
- the HSS shall be able to send one 3GPP AKA vector at a time to the BSF;
- the HSS shall be able to send the complete set of subscriber's GBA user security settings needed for security purposes to the BSF.optionally the HSS may have the capability to indicate to the BSF whether the BSF already has the latest copy of the GUSS based on the GUSS timestamp (timestamp option);

NOTE 2: If subscriber's GUSS is updated in HSS, this is not propagated to the BSF. The GUSS in the BSF is updated when the BSF next time fetches the authentication vectors and GUSS from the HSS over Zh reference point as part of the bootstrapping procedure.

- no state information concerning bootstrapping shall be required in the HSS;
- all procedures over reference point Zh shall be initiated by the BSF;
- 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 DIAMETER based Zn reference point shall be secured according to NDS/IP [13];
- If the BSF and the NAF are located in different operators' networks, the DIAMETER based Zn' reference point between the Zn-Proxy and the BSF shall be secured using TLS as specified in RFC 2246 [28];

NOTE 1: Annex E specifies the TLS profile that shall be applied.

- An HTTP based Zn/Zn' reference point shall be secured using TLS as specified in RFC 2246 [28];

NOTE 1b: Annex E specifies the TLS profile that shall be applied.

- The BSF shall verify that the requesting NAF is authorised to obtain the key material or the key material and the requested USS;
- 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 USSs 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 USSs for;

NOTE 2: If some application needs only a subset of an application-specific USS, e.g. only one IMPU, the NAF selects this subset from the complete set of USS sent from BSF.

- The BSF shall be able to be configured on a per NAF or per application basis
  - whether private subscriber identity, i.e. IMPI, may be sent to the NAF;
  - whether a particular USS may be sent to a NAF;

NOTE 3: If the BSF does not send the IMPI or any other user identities in the USS, e.g. IMPU to the NAF, the user remains anonymous towards the NAF; or more precisely, the B-TID functions as a temporary user pseudonym.

- If a NAF requests USSs from the BSF and they are not present in subscriber's GUSS, it shall not cause an error, provided the conditions of the local policy of the BSF are fulfilled. The BSF shall then send only the requested and found USSs to the NAF;
- It shall be possible to configure a local policy as follows: BSF may require one or more application-specific USS to be present in a particular subscriber’s GUSS for a particular requesting NAF, and to reject the request from the NAF in case the conditions are not fulfilled. In order to satisfy this local policy, it is not required that the NAF requests the USSs over the Zn reference point, which the BSF requires to be present in the GUSS, rather it is sufficient that the BSF checks the presence of the USSs locally. It shall also be possible to configure the BSF in such a way that no USS is required for the requesting NAF;

NOTE 4: For more information on the local policy usage, see Annex J.

- The BSF shall be able to indicate to the NAF the bootstrapping time and 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.

NOTE 5: This does not preclude a NAF to refresh the key before the expiry time according to the NAF's local policy.

NOTE 6: If one or more of the USSs that have been delivered to the NAF has been updated in subscriber's GUSS in the HSS, this change is propagated to the NAF the next time it fetches the USS from the BSF over Zn reference point (provided that the BSF has updated subscriber's GUSS from the HSS over Zh reference point).

- NAF shall be able to indicate to BSF the protocol identifier of Ua security protocol it requires the key material by sending NAF-Id to BSF (cf. Annex H).

4.4.7 Requirements on Bootstrapping Transaction Identifier

Bootstrapping transaction identifier (B-TID) shall be used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn.

Requirements for B-TID are:

- B-TID shall be globally unique;

- B-TID shall be usable as a key identifier in protocols used in the reference point Ua;

- NAF shall be able to detect the home network and the BSF of the UE from the B-TID.

NOTE 1: NAF can remove the security association based on deletion conditions after the key has become invalid.

NOTE 2: Care has to be taken that the parallel use of GBA and non-GBA authentication between UE and NAF does not lead to conflicts, e.g. in the name space. This potential conflict cannot be resolved in a generic way as it is dependent on specific protocol and authentication mechanism used between UE and application server. It is therefore out of scope of this specification.
For the example of HTTP Digest authentication used between UE and NAF, parallel use is possible as the following applies: <username,password>-pairs must be unique to one realm only. As the NAF controls the realm names, it has to ensure that only the GBA based realm is named with the reserved 3GPP realm name. In the special case that the NAF wants to allow non GBA based authentication in the GBA realm also, it has to ensure that no usernames in the format of a B-TID are used outside GBA based authentication.

4.4.8 Requirements on selection of UICC application and related keys

When several applications are present on the UICC, which are capable of running AKA, then the ME shall choose one of these UICC applications for performing the GBA procedures specified in this document in the following order of preference:

1. The UE determines which UICC application is to be involved:

   a. the application on the ME that needs Ks_NAF (Ua application) may indicate to the GBA support function (GBA function) the type or the name of the UICC application: no preference, USIM, ISIM, or the "Label" (see definition in TS 31.101 [15]) of the UICC application.

      If the application on the ME indicated a “Label” of the UICC application, step b below shall be executed.

      If the application on the ME indicated that the UICC application type should be:

      - the USIM on the UICC; step b below is skipped and in steps c and d only USIM applications are considered.

      - the ISIM on the UICC; step b below is skipped and in steps c and d only ISIM applications are considered.

if the application on the ME did not indicate a preference, step b below is skipped and the selection process is executed as described below, starting with step c;

b. if a "Label" was indicated in step a, the GBA function shall select (see definition in TS 31.102 [1]) the UICC application with the "Label" indicated; if selection of this UICC application does not succeed the selection procedure fails;

c. if no "Label" was indicated in step a, the GBA function shall choose among the active UICC applications; if there is more than one active UICC applications, the GBA function may show a UICC application choosing dialogue to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user chooses the UICC application to be selected; if no dialogue is shown the GBA function shall select the "last selected" active UICC application; in case the Ua application indicated "no preference" and both a "last selected" USIM and a "last selected" ISIM are active, then the "last selected" USIM is selected.

d. if there are no UICC applications active:

- if there is only one UICC application, the GBA function selects it, if possible;

- if there is more than one UICC application, the GBA function may show a UICC application choosing dialogue to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user chooses the UICC application to be selected; if no dialogue is shown the GBA function shall select the "last selected" UICC application, if possible.

e. if the type indicated in step a and used in step d was ISIM, but there was no ISIM to select, then step d is repeated with type USIM; otherwise the selection process fails.

NOTE 1: Step e is required for the case that an ISIM as defined in TS 33.203 [16] may be realised using a USIM application on the UICC.

2. If there already is a key Ks derived from the chosen UICC application, the UE takes this key to derive Ks_NAF.

3. If there is no such key Ks, the UE first runs the Ub protocol involving the selected UICC application and then goes to step 2.

If a USIM is chosen, the IMPI obtained from the IMSI stored on the USIM as specified in TS 23.003 [11] clause 13.3, is used in the protocol run over Ub.

NOTE 2: Strictly speaking, an IMPI, and the derivation of an IMPI from an IMSI as in TS 23.003 [11], clause 13 are only defined in the context of the IMS. For the purposes of this specification, however, an identifier obtained from an IMSI as specified in TS 23.003 [11], clause 13.3 is also called an IMPI, even if the user has no IMS subscription.

If an ISIM is selected, the IMPI stored on the ISIM is used in the protocol run over Ub.

Whenever a UICC application is successfully selected or terminated, the rules in this clause for choosing the UICC application are re-applied and, consequently, the UICC application chosen for GBA may change.

NOTE 3: At any one time, there is at most one UICC application chosen for performing the GBA procedures.

4.4.9 Requirements on reference point Ua

The generic requirements for reference point Ua are:

- the UE and the NAF shall be able to secure the reference point Ua using the GBA-based shared secret;

NOTE: The exact method of securing the reference point Ua depends on the application protocol used over reference point Ua.

- in the case of GBA_U, the UE and the NAF shall be able to agree which key (i.e, Ks_ext_NAF or Ks_int_NAF or both) is used as the GBA-based shared secret if both keys may be used;

There are two ways to have an agreement between the UE and the NAF which key shall be used Ks_(ext)_NAF or Ks_int_NAF or both:

a) In a generic case, where the protocol used over reference point Ua can be used for different applications (e.g., HTTPS), the protocol should be able to indicate which key should be used.

b) In a specific case, where the protocol is application specific (e.g., MIKEY in MBMS), the agreement can be based on implicit knowledge.

- any security protocol over Ua shall be associated with a Ua security protocol identifier. This identifier shall be specified in Annex H of this specification.

- the NAF shall be able to indicate to the UE that GBA-based shared secret should be used;

- the NAF shall be able to indicate to the UE that the current shared secret has expired and the UE should use newer shared secret with the NAF.

- The default lifetime of the NAF specific key material Ks_(ext/int)_NAF shall be equal to the lifetime of Ks when not specified within the Ua-application specification. The lifetime of the Ks_(ext/int)_NAF shall not exceed the lifetime of corresponding Ks.

- The UE and NAF may adapt the key material Ks_(ext/int)_NAF to the specific needs of the reference point Ua. This adaptation is outside the scope of this specification. The default lifetime of the adapted key material shall be equal to the lifetime of Ks_(ext/int)_NAF when not specified within the Ua-application specification. The lifetime of the adapted key material shall not exceed the lifetime of corresponding Ks_(ext/int)_NAF.

4.4.10 Requirements on reference point Dz

This interface between BSF and SLF is used to retrieve the address of the HSS which holds the subscription for a given user. This interface is not required in a single HSS environment.

4.4.11 Requirements on GBA keys and parameters handling

The ME shall delete all GBA related keys (i.e., Ks, and NAF specific keys) and the corresponding NAF_IDs, B-TID, and key lifetime when at least one of the conditions below is met:

1- the key lifetime of the Ks, which was used to derive the NAF specific keys (Ks_(ext/int)_NAF), expires;

2- the UICC is removed from the ME;

3- the ME is powered up and the ME discovers that another UICC has been inserted to the ME. For this, the ME needs to store in non-volatile memory the last inserted UICC-identity to be able to compare that with the used UICC-identity at UICC insertion and power up; or

4- the ME is powered up and the ME discovers that no UICC has been inserted to the ME.

In the case of GBA_ME, the Key Ks shall be deleted from the ME when the ME is powered down. All other GBA keys (i.e. Ks_(ext)_NAF) may be deleted from the ME when the ME is powered down. If the ME does not delete these GBA keys at power down then the GBA keys (i.e. Ks_(ext)_NAF) together with the NAF_IDs, B-TID and key lifetime shall be stored in non-volatile memory.

Whenever a UICC application is terminated (see section 4.4.8) the shared key Ks established from it in the protocol over the Ub reference point (according to clauses 4.5.2 and 5.3.2) shall be deleted.

NOTE: In case the key Ks has been deleted, but the same UICC is still present (i.e. none of conditions 2, 3 or 4 is met), the Ua applications can continue using the NAF specific keys (Ks_(ext/int)_NAF) until the Ks lifetime expires.

4.5 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 the key material generation procedure.

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 use of shared keys obtained by means of the GBA, the UE shall contact the NAF for further instructions (see figure 4.2).

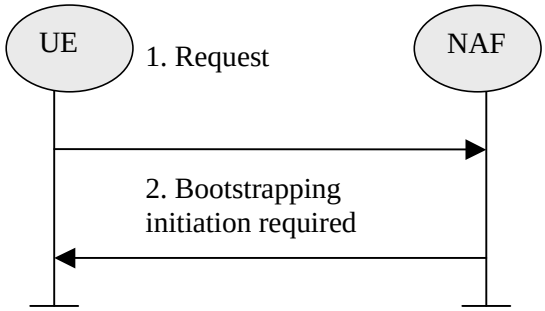


Figure 4.2: Initiation of bootstrapping

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

2. If the NAF requires the use of shared keys obtained by means of the GBA,but the request from UE does not include GBA-related parameters, the NAF replies with a bootstrapping initiation message. The form of this indication may depend on the particular reference point Ua 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 4.3). Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a bootstrapping negotiation indication from the NAF, or when the lifetime of the key in UE has expired (cf. subclause 4.5.3).

NOTE 1: 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.

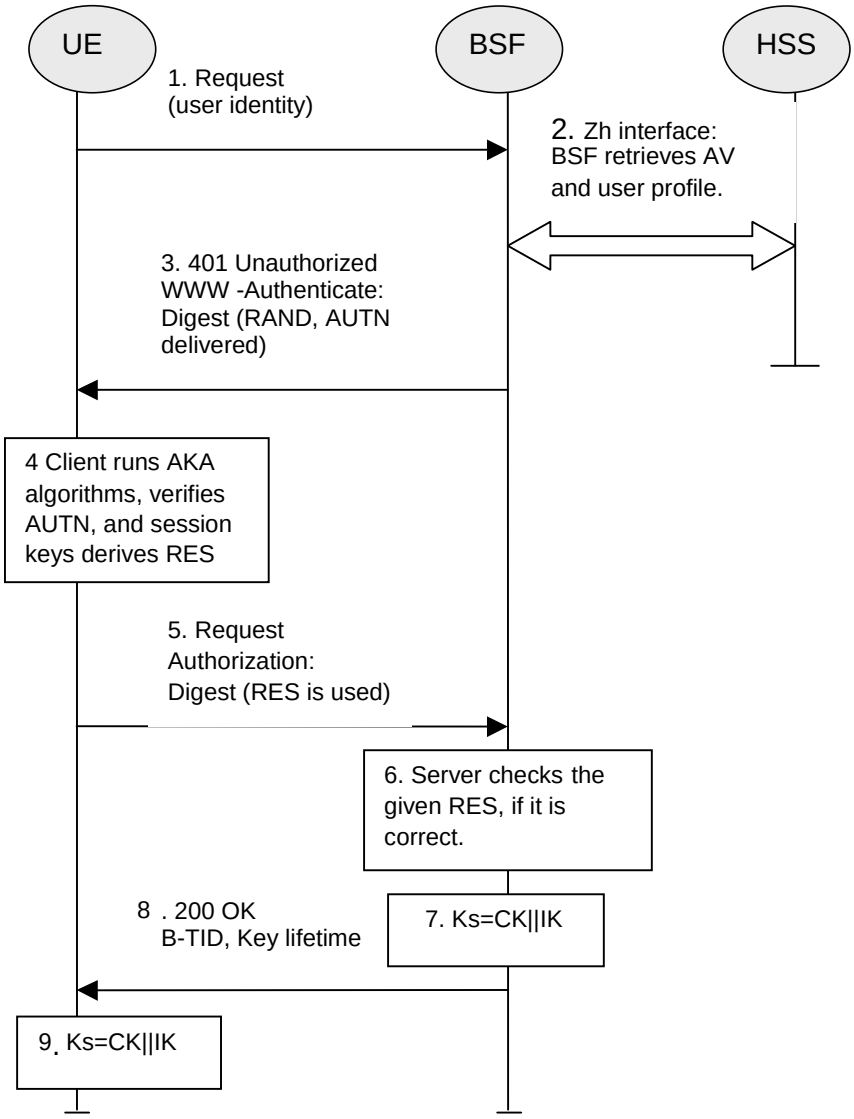


Figure 4.3: The bootstrapping procedure

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

2. BSF retrieves the complete set of GBA user security settings and one Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) over the reference point Zh from the HSS.

   If the BSF implements the timestamp option and has a local copy of the GUSS for the subscriber that has been fetched from the HSS during a previous bootstrapping procedure, and this GUSS includes a timestamp, the BSF may include the GUSS timestamp in the request message. Upon receiving that timestamp, if the HSS implements the timestamp option, the HSS may compare it with the timestamp of the GUSS stored in the HSS. In this case, if and only if the HSS has done the comparison and the timestamps are equal, then the HSS shall send "GUSS TIMESTAMP EQUAL" indication to the BSF. In any other case, the HSS shall send the GUSS (if available) to the BSF. If the BSF receives "GUSS TIMESTAMP EQUAL" indication, it shall keep the local copy of the GUSS. In any other case, the BSF shall delete the local copy of the GUSS, and store the received GUSS (if sent).

NOTE 2: In a multiple HSS environment, the BSF may have to obtain the address of the HSS where the subscription of the user is stored by querying the SLF, prior to step 2.

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 B-TID value shall be also generated in format of NAI by taking the base64 encoded [12] RAND value from step 3, and the BSF server name, i.e. base64encode(RAND)@BSF_servers_domain_name.

8. The BSF shall send a 200 OK message, including a B-TID, to the UE to indicate the success of the authentication. In addition, in the 200 OK message, the BSF shall supply the lifetime of the key Ks. 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 clause 4.5.3. Ks_NAF shall be used for securing the reference point Ua.

   Ks_NAF is computed as Ks_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_Id), where KDF is the key derivation function as specified in Annex B, and the key derivation parameters consist of the user's IMPI, the NAF_Id and RAND. The NAF_Id consists of the full DNS name of the NAF, concatenated with the Ua security protocol identifier as specified in Annex H. KDF shall be implemented in the ME.

   To allow consistent key derivation based on NAF name in UE and BSF, at least one of the three following prerequisites shall be fulfilled:

   (1) The NAF is known in DNS under one domain name (FQDN) only, i.e. no two different domain names point to the IP address of the NAF. This has to be achieved by administrative means.
   This prerequisite is not specific to 3GPP, as it is necessary also under other circumstances, e.g. for TLS V1.0 without use of wildcard or multiple-name certificates.

   (2) Each DNS entry of the NAF points to a different IP address. The NAF responds to all these IP addresses. Each IP address is tied to the corresponding FQDN by NAF configuration. The NAF can see from the IP address, which FQDN to use for key derivation.

   (3) Ua uses a protocol which transfers the host name (FQDN of NAF as used by UE) to NAF (e.g. HTTP/1.1 with mandatory Host request header field). This requires the NAF to check the validity of the host name, to use this name in all communication with UE where appropriate, and to transfer this name to BSF to allow for correct derivation of Ks_NAF.
   In case of a TLS tunnel this requires either multiple-identities certificates or the deployment of RFC 3546 [9] or other protocol means with similar purpose.

   The UE and the BSF shall store the key Ks with the associated B-TID for further use, until the lifetime of Ks has expired, or until the key Ks is updated or until the deletion conditions are satisfied (see 4.4.11).

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.

1. 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

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 or will expire soon, or the key can not meet the NAF local validity condition, it shall send a suitable bootstrapping renegotiation request to the UE, see figure 4.5. If the key's lifetime has expired the protocol used over reference point Ua shall be terminated. 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.

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

- the key management procedures for GBA related keys in the ME (i.e. Ks and Ks_NAF keys) are described in section 4.4.11.

- 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;

  According to the procedures defined in clauses 4.5.2 and 4.5.3, in the UE there is at most one Ks_NAF key stored per NAF-Id.

2. 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 (This is to allow for consistent key derivation in BSF and UE as described above);

- The NAF may also request one or more application-specific USSs for the applications, which the request received over Ua from UE may access;

- With the key material request, the NAF shall supply NAF-Id (which includes NAF's public hostname that UE has used to access NAF and the Ua security protocol identifier) to BSF, and BSF shall be able verify that NAF is authorized to use that hostname.

3. 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 bootstrapping time and the lifetime of that key, and the requested application-specific and potentially NAF group specific USSs if they are available in subscriber's GUSS and if the NAF is authorized to receive the requested USSs. 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 3: The NAF can further set the local validity condition of the Ks_NAF according to the local policy, for example a limitation of reuse times of a Ks_NAF.

NOTE 4: The NAF will 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.

- The BSF may require that one or more application-specific and potentially NAF group specific USSs shall be present in subscriber's GUSS for the NAF (see clause 4.4.6). If one or more of these required settings are missing from the GUSS, the BSF shall indicate this in the reply to the NAF.

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

4. 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.

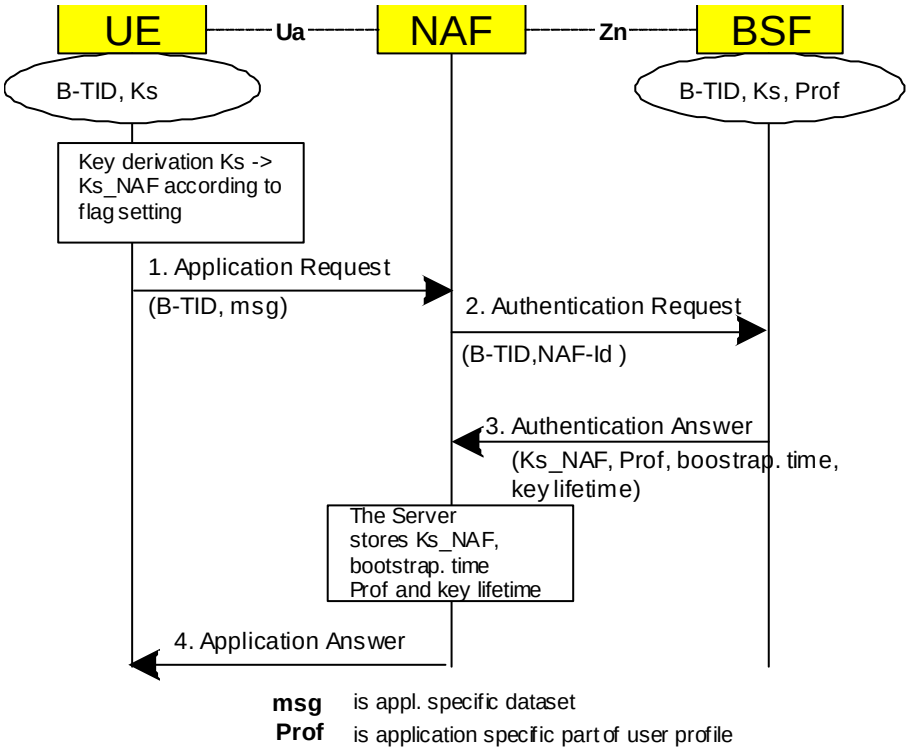


Figure 4.4: The bootstrapping usage procedure

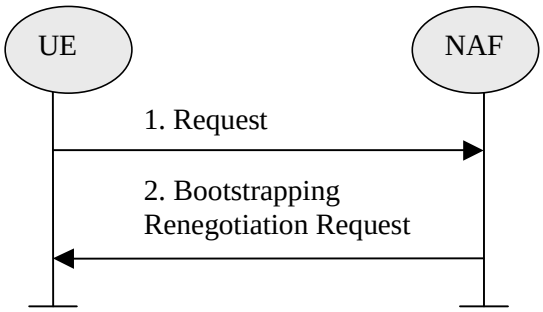


Figure 4.5: Bootstrapping renegotiation request

4.5.4 Procedure related to service discovery

The UE shall discover the address of the BSF the from the identity information related to the UICC application that is used during bootstrapping procedure, i.e., IMSI for USIM, or IMPI for ISIM. The address of the BSF is derived as specified in 3GPP TS 23.003 [11].

5 UICC-based enhancements to Generic Bootstrapping Architecture (GBA_U)

It is assumed that the UICC, BSF, and HSS involved in the procedures specified in this clause are capable of handling the GBA_U specific enhancements. The procedures specified in this clause also apply if NAF is not GBA_U aware.

5.1 Architecture and reference points for bootstrapping with UICC-based enhancements

The text from clause 4.4 of this specification applies also here, with the addition that the interface between the ME and the UICC, as specified in TS 31.102 [1] and TS 31.103 [10], needs to be enhanced with GBA_U specific commands. The requirements on these commands can be found in clause 5.2.1, details on the procedures are in clause 5.3.

5.2 Requirements and principles for bootstrapping with UICC-based enhancements

The requirements and principles from clause 4.3 also apply here with the following addition:

5.2.1 Requirements on UE

The 3G AKA keys CK and IK resulting from a run of the protocol over the Ub reference point shall not leave the UICC.

The UICC shall be able to distinguish between authentication requests for GBA_U, and authentication requests for other 3G authentication domains.

Upon an authentication request from the ME, which the UICC recognises as related to GBA_U, the UICC shall derive the bootstrapping key.

Upon request from the ME, the UICC shall be able to derive further NAF-specific keys from the derived key stored on the UICC.

All GBA-aware MEs shall support procedures for the two previous requests.

5.2.2 Requirements on BSF

BSF shall support both GBA_U and GBA_ME bootstrapping procedures. The decision on running one or the other shall be based on subscription information (i.e. UICC capabilities).

The BSF shall be able to acquire the UICC capabilities related to GBA as part of the GBA user security settings received from the HSS.

5.3 Procedures for bootstrapping with UICC-based enhancements

5.3.1 Initiation of bootstrapping

The text from clause 4.5.1 of this document applies also here.

5.3.2 Bootstrapping procedure

The procedure specified in this clause differs from the procedure specified clause 4.5.2 in the local handling of keys and Authentication Vectors in the UE and the BSF. The messages exchanged over the Ub reference point are identical for both 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 5.1). Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a bootstrapping renegotiation indication from the NAF, or when the lifetime of the key in UE has expired (see clause 5.3.3).

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 5.1 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.

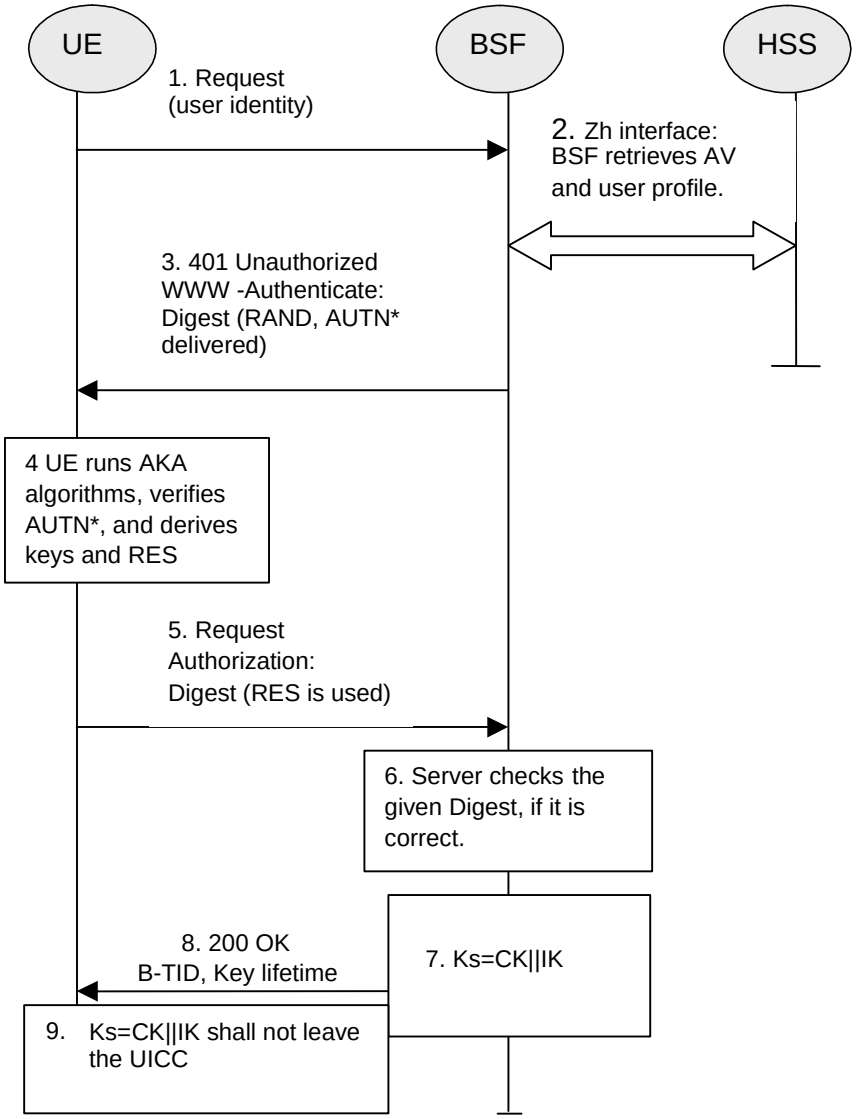


Figure 5.1: The bootstrapping procedure with UICC-based enhancements

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

2. The BSF retrieves the complete set of GBA user security settings and one Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) over the Zh reference point from the HSS.

   If the BSF implements the timestamp option and has a local copy of the GUSS for the subscriber that has been fetched from the HSS during a previous bootstrapping procedure, and this GUSS includes a timestamp, the BSF may include the GUSS timestamp in the request message. Upon receiving that timestamp, if the HSS implements the timestamp option, the HSS may compare it with the timestamp of the GUSS stored in the HSS. In this case, if and only if the HSS has done the comparison and the timestamps are equal, then the HSS shall send "GUSS TIMESTAMP EQUAL" indication to the BSF. In any other case, the HSS shall send the GUSS (if available) to

the BSF. If the BSF receives "GUSS TIMESTAMP EQUAL" indication, it shall keep the local copy of the GUSS. In any other case, the BSF shall delete the local copy of the GUSS, and store the received GUSS (if sent).

The BSF can then decide to perform GBA_U, based on the user security settings (USSs). In this case, the BSF proceeds in the following way:

- BSF computes MAC* = MAC⊕ Trunc(SHA-1(IK))

NOTE 1: Trunc denotes that from the 160 bit output of SHA-1 [21], the 64 bits numbered as [0] to [63] are used within the * operation to MAC.

The BSF stores the XRES after flipping the least significant bit.

NOTE 2: In a multiple HSS environment, the BSF may have to obtain the address of the HSS where the subscription of the user is stored by querying the SLF, prior to step 2.

3. Then BSF forwards the RAND and AUTN* (where AUTN* = SQN ⊕ AK || AMF || MAC*) to the UE in the 401 message (without the CK, IK and XRES). This is to demand the UE to authenticate itself.

4. The ME sends RAND and AUTN* to the UICC. The UICCcalculates IK and MAC (by performing MAC= MAC* ⊕ Trunc(SHA-1(IK))). Then the UICC checks AUTN(i.e. SQN ⊕ AK || AMF || MAC) to verify that the challenge is from an authorised network; the UICC also calculates CK and RES. This will result in session keys CK and IK in both BSF and UICC. The UICC then transfers RES (after flipping the least significant bit) to the ME and stores Ks, which is the concatenation of CK and IK, on the UICC.

5. The ME 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 the key Ks by concatenating CK and IK. The B-TID value shall be also generated in format of NAI by taking the base64 encoded [12] RAND value from step 3, and the BSF server name, i.e. base64encode(RAND)@BSF_servers_domain_name.

8. The BSF shall send a 200 OK message, including the B-TID, to the UE to indicate the success of the authentication. In addition, in the 200 OK message, the BSF shall supply the lifetime of the key Ks.

9. Both the UICC and the BSF shall use the Ks to derive NAF-specific keys Ks_ext_NAF and Ks_int_NAF during the procedures as specified in clause 5.3.3, if applicable. Ks_ext_NAF and Ks_int_NAF are used for securing the Ua reference point.

   Ks_ext_NAF is computed in the UICC as Ks_ext_NAF = KDF(Ks, "gba-me", RAND, IMPI, NAF_Id), and Ks_int_NAF is computed in the UICC as Ks_int_NAF = KDF(Ks, "gba-u, RAND, IMPI, NAF_Id), where KDF is the key derivation function as specified in Annex B, and the key derivation parameters include the user's IMPI, the NAF_Id and RAND. The NAF_Id consists of the full DNS name of the NAF, concatenated with the Ua security protocol identifier as specified in Annex H. The key derivation parameters used for Ks_ext_NAF derivation must be different from those used for Ks_int_NAF derivation. This is done by adding a static string "gba-me" in Ks_ext_NAF and "gba-u" in Ks_int_NAF as an input parameter to the key derivation function.

   To allow consistent key derivation based on NAF name in UE and BSF, at least one of the prerequisites which are specified in clause 4.5.2 shall be met.

   The UICC and the BSF store the key Ks with the associated B-TID for further use, until the lifetime of Ks has expired, or until the key Ks is updated or until the deletion conditions are satisfied (see 4.4.11)..

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_NAF and Ks_int_NAF 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. A key selection indication, which key (i.e. Ks_int_NAF or Ks_ext_NAF) the NAF shall use in the Ua reference point may be present in the application specific USS as defined in stage 3 specification. If the indication exists, the NAF shall use the indicated key. If the Ks_int_NAF key was indicated in the USS, the UE attempts to use Ks_ext_NAF key, the NAF shall terminate the communication with the UE.

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.

1. UE starts communication over reference point Ua with the NAF using the keys Ks_ext_NAF or Ks_int_NAF, or both, as required:

   - 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 for the selected UICC application is available in the UICC, the ME requests the UICC to derive the key Ks_ext_NAF from Ks, as specified in clause 5.3.2;

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

  If it is not desired by the UE to use the same Ks for the selected UICC application to derive more than one Ks_ext/int_NAF, then the UE should first agree on new key Ks 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 for the selected UICC application is not available in the UE, the UE first agrees on a new key Ks 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. If the key's lifetime has expired the protocol used over reference point Ua shall be terminated. 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 2: 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 3: 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 can reply to the first request sent by a UE by sending a key update request to the UE.

   - 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

     To allow for consistent key derivation in BSF and UE, both have to use the same FQDN for derivation (cf. clause 4.5.2). For each protocol used over Ua it shall be specified if only cases (1) and (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 4 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.

- the key management procedures for GBA related keys in the ME (i.e. Ks_ext_NAF keys) are described in section 4.4.11.

   - all GBA related keys in the UICC do not need to be deleted when the ME is powered down.

NOTE 5: After each run of the protocol over the Ub reference point, a new key Ks, associated with a new B-TID, are derived in the UE according to clause 5.3.2, so that it can never happen, that key Ks with different B-TIDs simultaneously exist in the UE.

- When new key Ks is 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 other keys Ks_ext_NAF or Ks_int_NAF relating to other NAF_Ids, which may be stored on the UE, shall not be affected.

  According to the procedures defined in clauses 5.3.2 and 5.3.3, in the UE there is at most one Ks_int_NAF/Ks_ext_NAF key pair stored per NAF_Id.

NOTE 6: This rule ensures that the keys Ks_ext_NAF and Ks_int_NAF are always in synch at the UE and the NAF.

2. 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 one or more application-specific USSs 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-Id (which includes NAF's public hostname that UE has used to access NAF and the Ua security protocol identifier) to BSF, and BSF shall be able to verify that NAF is authorized to use that hostname.

   3. 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 bootstrapping time and the lifetime time of these keys, and the requested application-specific and potentially NAF group specific USSs if they are available in subscriber's GUSS and if the NAF is authorized to receive the requested USSs. 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 7: The NAF can further set the local validity condition of the Ks_NAF according to the local policy, for example a limitation of reuse times of a Ks_NAF.

   NOTE 8: The NAF will 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 require that one or more application-specific and potentially NAF group specific USSs shall be present in subscriber's GUSS for the NAF (see clause 4.4.6). If one or more of these required settings are missing from the GUSS, the BSF shall indicate this in the reply to the NAF.

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

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

   - If the NAF requested an application-specific USS from the BSF and the USS was returned the NAF, the NAF shall check whether this USS contains an key selection indication. If the key selection indication is present, the NAF shall use only the indicated key. If a different key was used over Ua, then the protocol used over reference point Ua shall be terminated.

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.

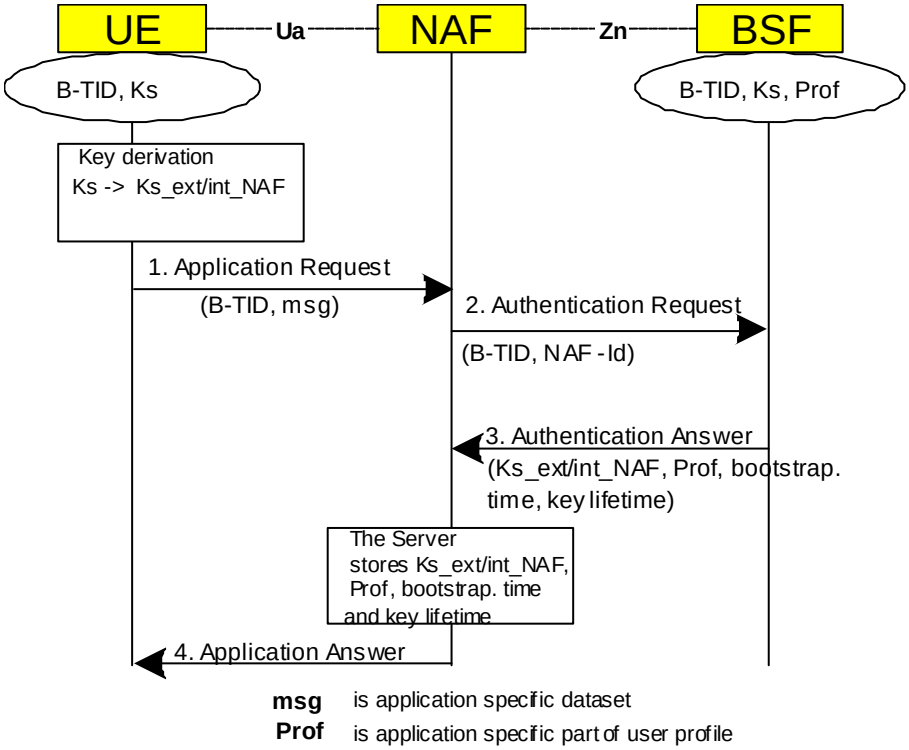


Figure 5.3: The bootstrapping usage procedure with UICC-based enhancements

5.3.4 Procedure related to service discovery

The text from clause 4.5.4 of this document applies also here.

Annex A:
(Void)

Annex B (normative): Specification of the key derivation function KDF

B.1 Introduction

This annex specifies the key derivation function (KDF) that is used in the NAF specific key derivation in both GBA (i.e. GBA_ME) and GBA_U. The key derivation function defined in the annex takes the following assumptions:

1. the input parameters to the key derivation functions are octet strings - not bit strings of arbitrary length:
2. a single input parameter will have lengths no greater than 65535 octets.

B.2 Generic key derivation function

The input parameters and their lengths shall be concatenated into a string S as follows:

1. The length of each input parameter in octets shall be encoded into two-octet string:

   a) express the number of octets in input parameter Pi as a number k in the range [0, 65535].

   b) Li is then a two-octet representation of the number k, with the most significant bit of the first octet of Li equal to the most significant bit of k, and the least significant bit of the second octet of Li equal to the least significant bit of k,

EXAMPLE: If Pi contains 258 octets then Li will be the two-octet string 0x01 0x02.

2. String S shall be constructed from n input parameters as follows:

   S = FC || P0 || L0 || P1 || L1 || P2 || L2 || P3 || L3 ||... || Pn || Ln

   where

   FC is single octet used to distinguish between different instances of the algorithm,

   P0 is a static ASCII-encoded string,

   L0 is the two octet representation of the length of the P0,

   P1 ... Pn are the n input parameters, and

   L1 ... Ln are the two-octet representations of the corresponding input parameters.

3. The final output, i.e. the derived key is equal to HMAC-SHA-256 (as specified in [22] and [23]) computed on the string S using the key Key:

   derived key = HMAC-SHA-256 (Key , S)

B.2.1 Input parameter encoding

A character string shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [24].

B.3 NAF specific key derivation in GBA and GBA_U

In GBA and GBA_U, the input parameters for the key derivation function shall be the following:

- FC = 0x01,
- P1 = RAND,
- L1 = length of RAND is 16 octets (i.e. 0x00 0x10),
- P2 = IMPI encoded to an octet string using UTF-8 encoding (see clause B.2.1),
- L2 = length of IMPI is variable (not greater that 65535),
- P3 = NAF_ID with the FQDN part of the NAF_ID encoded to an octet string using UTF-8 encoding (see clause B.2.1), and
- L3 = length of NAF_ID is variable (not greater that 65535).

In the key derivation of Ks_NAF as specified in clause 4 and Ks_ext_NAF as specified in clause 5,

- P0 = "gba-me" (i.e. 0x67 0x62 0x61 0x2d 0x6d 0x65), and
- L0 = length of P0 is 6 octets (i.e., 0x00 0x06).

In the key derivation of Ks_int_NAF as specified in clause 5,

- P0 = "gba-u" (i.e. 0x67 0x62 0x61 0x2d 0x75), and
- L0 = length of P0 is 5 octets (i.e., 0x00 0x05).

The Key to be used in key derivation shall be:

- Ks (i.e. CK || IK concatenated) as specified in clauses 4 and 5,

NOTE: In the specification this function is denoted as:
Ks_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_Id),
Ks_ext_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_Id), and
Ks_int_NAF = KDF (Ks, "gba-u", RAND, IMPI, NAF_Id).

Annex C:
(Void)

Annex D (informative): Dialog example for user selection of UICC application used in GBA

For certain cases, clause 4.4.8 specifies user involvement in the selection of the UICC application used for GBA procedures. A dialog window example for such an involvement is described below:

- The title of the dialog: "Authentication request".
- Explanation: "A service requires you to authenticate, please select your identity:"
- List of identities: A selectable list of applications on the UICC. The text visible for each application is extracted from the "Label" field of the application list on the UICC.
- Buttons: "Select" and "Cancel".

Annex E (normative): TLS profile for securing Zn/Zn' reference points

This Annex applies for the Zn' reference point when using DIAMETER or HTTP, and applies for the Zn reference point if using HTTP.

The TLS profile is specified in RFC 3588 [14] section 13.2 with following restriction for the CipherSuites:

The BSF and Zn-Proxy shall use the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA or the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA.

In addition, the Zn-Proxy certificate, i.e. the client certificate used in TLS handshake shall contain the subjectAltName extension as specified in RFC 3280 [17]. The subjectAltName extension shall contain one or more dNSName names. The dNSName name may contain the wildcard character '*' and the matching is performed as specified in RFC 2818 [18] section 3.1.

The Zn-Proxy certificate shall contain all the DNS names of NAFs that may send a request for NAF specific shared secret through the Zn-Proxy to the subscriber's home BSF. If a new NAF is added, the new DNS name is either covered in the certificate by using the wildcard character approach (e.g. "*.operator.com"), or a new dNSName name needs to be added to the certificate. In the latter case, new certificate is needed for the Zn-Proxy.

Annex F (informative): Handling of TLS certificates

An authentication framework as available for IPsec [19] is not available for TLS certificates. The purpose of this Annex is to provide guidelines for TLS certificate handling for use on the Zn' reference point in the absence of a framework for TLS certificates.

Within this Annex following abbreviations are used: CA_A is the certification authority in A's network and CA_B is the certification authority in B's network. $Cert_A$ is the certificate of A and $Cert_B$ is the certificate of B. I_A is the set of identifiers that A may use to identify the NAF towards the BSF. T_B is the set of peers trusted by B.

F.1 TLS certificate enrollment

Mutual authentication in TLS is achieved based on public key technology and certificates. Both TLS peers A and B need to contain a certificate store and there shall be at least one certification authority CA that can issue certificates within the security domains in with A and B are part of. $Cert_A$ contains the set I_A of A's identifiers. Each identifier is in the form of fully qualified domain name (FQDN). Similarly, B's certificate is $Cert_B$.

The certificates in the store of B define the group T_B of peers trusted by B. There are several options for creation and enrollment of certificates, three of which are described below.

1. In one option there is a certification authority, CA_B, only in the network of B. CA_B issues a certificate $Cert_B$ to B and a certificate $Cert_A$ to A. The certificates are delivered from CA_B to A and B in a secure way "out of band". Both A and B then add their peer into the group of their trusted peers by inserting that peer's certificate into the certificate store: A inserts $Cert_B$ into A's certificate store and B inserts $Cert_A$ into B's certificate store. This insertion is typically manual and the details depend on the implementation of the management interface to the certificate store.

2. In another option both A's and B's networks contain certification authorities, CA_B and CA_A, respectively. CA_B issues a certificate $Cert_B$ to B and CA_A issues a certificate $Cert_A$ to A. The certificates are delivered from CA_B to A and from CA_A to B in a secure way "out of band". Both A and B then add their peer into the group of their trusted peers by inserting that peer's certificate into the certificate store: A inserts $Cert_B$ into A's certificate store and B inserts $Cert_A$ into B's certificate store.

3. In a third option the CA certificates of both sides are exchanged: the certificate of CA_B is delivered to A and the certificate of CA_A is delivered to B in a secure way "out of band"', inserted to the certificate store, and marked trusted. The validation of $Cert_A$ and $Cert_B$, that are exchanged during TLS handshake, is based on the presence of the corresponding CA certificates in the certificate store.

NOTE: In options 1 and 2 the need for certification authority may be avoided if the peers generate self signed certificates and exchange them in a secure way, "out of band". Also, instead of certificates themselves, certificate fingerprints may be exchanged "out of band" in those options.

F.2 TLS Certificate revocation

In the absence of PKI-revocation interfaces, certificate revocation needs to be performed manually. The revocation operation involves the removal of A from the group T_B of peers trusted by B. In the first two enrollment options described above the revocation happens by B removing the certificate of A, $Cert_A$, from its certificate store. This removal can be done manually. In the third option the certificate of A, $Cert_A$, is not in B's certificate store. For that reason B has to have a way to check the validity of $Cert_A$ with the issuer of the certificate (also in the first two enrollment options the amount of manual maintenance operations will decrease if B can check the validity of $Cert_A$ with the issuer of the certificate). This check may be done by using Online Certificate Status Protocol (OCSP) [20] or by using Certificate Revocation Lists (CRLs) [17] published by the issuer of $Cert_A$.

Annex G (normative): GBA_U UICC-ME interface

This annex describes the UICC-ME interface to be used when a GBA_U aware UICC application is active and the ME is involved in a GBA bootstrapping procedure. When the UICC application is not GBA_U aware, the ME uses AUTHENTICATE command in non-GBA_U security context (i.e. UMTS security context in case of USIM application and IMS security context in case of the ISIM) as defined in TS 31.102 [1] and TS 31.103 [10].

G.1 GBA_U Bootstrapping procedure

This procedure is part of the Bootstrapping procedure as described in clause 5.3.2.

The ME sends RAND and AUTN to the UICC, which performs the Ks derivation as described in clause 5.3.2.

The UICC then stores Ks. The UICC also stores the used RAND to identify the current bootstrapped values. RAND value in the UICC shall be further accessible by the ME.

The ME then finalizes the Bootstrapping procedure and stores in the UICC the Transaction Identifier (B-TID) and Key Life Time associated with the previous bootstrapped keys (i.e. Ks). Transaction Identifier and Key Life Time values in the UICC shall be further accessible by the ME.

At the end of the GBA_U bootstrapping procedure the UICC stores Ks, Transaction Identifier, Key Life Time and the RAND.

The UICC sends RES to the ME.

A new bootstrapping procedure replaces Ks, B-TID, Key LifeTime and RAND values of the previous bootstrapping procedure.

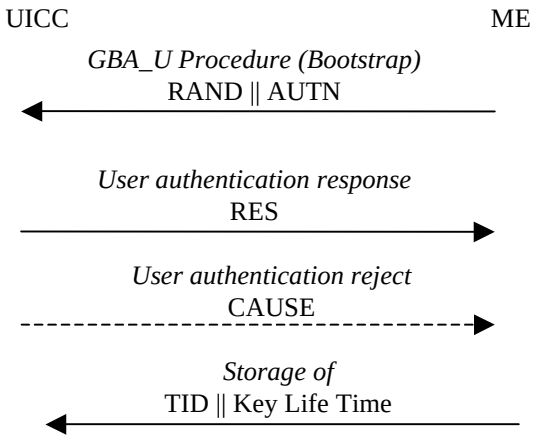


Figure G.1: GBA_U Bootstrap Procedure

G.2 GBA_U NAF Derivation procedure

This procedure is part of the Procedures using bootstrapped Security Association as described in clause 5.3.3

The ME sends NAF_ID and IMPI to the UICC. The UICC then performs Ks_ext_NAF and Ks_int_NAF derivation as described in clause 5.3.2. The UICC uses the RAND and Ks values stored from the previous bootstrapping procedure. The UICC returns Ks_ext_NAF to the ME and stores Ks_int_NAF and associated B-TID together with NAF_Id.

NOTE: A previous GBA_U Bootstrap needs to be undertaken before. If Ks is not available in the UICC, the command will answer with the appropriate error message.

The input parameters IMPI and the FQDN part of NAF_ID shall be encoded to octet strings using UTF-8 encoding rules as specified in IETF RFC 3629 [24].

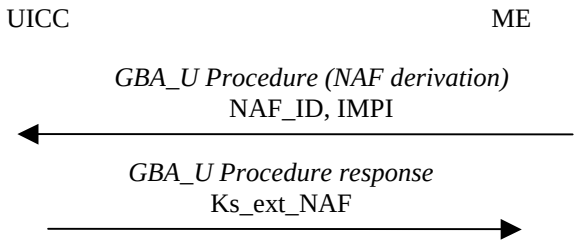


Figure G.2: GBA_U NAF derivation procedure

Annex H (normative): Ua security protocol identifier

H.1 Definition

The Ua security protocol identifier is a string of five octets. The first octet denotes the organization which specifies the Ua security protocol. The four remaining octets denote a specific security protocol within the responsibility of the organization.

For all Ua protocols specified by 3GPP this Annex shall contain a complete list of these protocols. For Ua protocols specified by other organizations this Annex shall only specify the organization octet of the Ua security protocol identifier. Two organization octets are reserved for special use.

H.2 Organization Octet

The organization octet denotes the organization specifying the particular protocol. Each organization intending to specify a Ua security protocol identifier shall apply to 3GPP to receive an organization octet value, which shall be registered within this Annex. Following is a list of registered organization octets:

"0x00" as first octet is the default value for protocols not specified otherwise. When octet "0x00" is used as first octet, only Ua security protocol identifier (0x00,0x00,0x00,0x00,0x00) shall be used.

NOTE: All protocols having this Ua security protocol identifier cannot be separated from each other.

"0x01" .. "0xFE" as the first octet denote organizations specifying Ua security protocol identifiers.

"0xFF" as the first octet denotes the private range of Ua security protocol identifiers.

NOTE: identifiers with "0xFF" as first octet may be used for defining local/experimental protocols without need for registration. When using such an identifier, however, it may happen that a security breach in one security protocol over Ua can be exploited by an attacker to mount successful attacks on a different security protocol over Ua.

The following values for organizations are assigned:

"0x01" 3GPP

NOTE: All protocols having the organization octet "0x01" are specified in annex H.3.

"0x02" 3GPP2

"0x03" Open Mobile Alliance

"0x04" GSMA

H.3 Ua security protocol identifiers for 3GPP specified protocols

The following Ua security protocol identifiers are specified by 3GPP:

(0x01,0x00,0x00,0x00,0x00) Ua security protocol according to TS 33.221 [5].

(0x01,0x00,0x00, 0x00,0x01) Ua security protocols according to TS 33.246 [26].NOTE: TS 33.246[26] provides key separation between the keys that are used within HTTP digest and MIKEY protocols.

(0x01,0x00,0x00, 0x00,0x02) Ua security protocol HTTP digest authentication according to TS 24.109 [29], unless HTTP digest authentication is used in the context of another Ua security protocol, which is already covered elsewhere in this Annex.

(0x01,0x00,0x01,yy,zz) Ua security protocol for "Shared key-based UE authentication with certificate-based NAF authentication", according to TS 33.222 [25], or "Shared key-based mutual authentication between UE and NAF", according to TS 33.222 [25]. Here, "yy,zz" is the protection mechanism CipherSuite code according to the defined values for TLS CipherSuites in TLS V1.0 [28] and PSK Ciphersuites for TLS [27].

NOTE: As an example: RFC2246 [28] CipherSuite TLS_RSA_WITH_3DES_EDE_CBC_SHA has code = { 0x00,0x0A }, thus the according protocol identifier shall be (0x01,0x00,0x01,0x00,0x0A).

Annex I (normative): 2G GBA

This annex specifies the implementation option to allow the use of SIM cards or SIMs on UICC for GBA. The procedure specified in this annex is called 2G GBA. 2G GBA allows access to applications in a more secure way than would be possible with the use of passwords or with GSM without enhancements. It may be useful for operators who have not yet fully deployed USIMs.

I.1 Reference model

The reference model is the same as described in section 4.1.

I.2 Network elements

I.2.1 Bootstrapping server function (BSF)

A generic Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the 2G AKA protocol and the TLS protocol, and agree on session keys that are afterwards applied between UE and a Network Application Function (NAF). The BSF shall restrict the applicability of the key material to a specific NAF by using the key derivation procedure as specified in Annex B. 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 I.5.2.

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

The BSF shall be able to discover from the type of authentication vectors sent by the HSS whether the subscriber is a 2G or a 3G subscriber.

The BSF shall be able to keep a list, which assigns NAFs to NAF Groups. This list is used to select if any and which application-specific USS within GUSS is valid for a certain NAF.

NOTE 1: The operator does the assignment of NAFs to NAF Groups. NAF Group definitions in HSS and all connected BSFs belonging to the same operator's network shall be equal (cf., clause I.2.3). As these network elements belong to the same operator's network, standardisation of the NAF Group definitions themselves is not necessary in 3GPP.

NOTE 2: The NAF grouping may be e.g. "home" and "visited". It allows the BSF to send USSs for the same application with e.g. different authorization flags to different NAFs, e.g., in home network and visited networks. The NAF e.g. in visited network indicates only the requested application, but it is unaware of the grouping in home network of the subscriber.

I.2.2 Network application function (NAF)

After the bootstrapping has been completed, the UE and a 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 a NAF are:

- there need not be a 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 zero or more application-specific USSs from the HSS via the BSF;
- NAF shall be able to set the local validity condition of the shared key material according to the local policy;
- NAF shall be able to check lifetime and local validity condition of the shared key material;
- NAF shall have a policy whether to accept 2G subscribers. However, whether the SIM card is allowed to be used with a specific Ua application or not, is dependent on the relevant Ua application. If there is a specific TS for the particular Ua protocol, e.g. TS 33.141 for Presence, and unless this specification explicitly prohibits the use of SIM, the operator is allowed to configure a BSF policy whether to accept 2G subscribers or not for this Ua application.

NOTE: Without additional measures, GBA does not guarantee the freshness of the key, Ks(_int/ext)_NAF in the sense that it does not guarantee that the key was not used in a previous run of the Ua protocol. The additional measures which may be taken by the UE and the NAF to ensure key freshness in GBA are:
1) enforce a new run of the Ub protocol (thus generating a new Ks) before deriving a new Ks_NAF.
2) store previously used keys Ks(_int/ext)_NAF, or the corresponding key identifiers B-TID, until the end of their lifetime.

A UE and a NAF that support a Ua protocol that does not provide replay protection over unconnected runs of the protocol, will need to take corresponding action to avoid replay attacks if desired.

I.2.2a Zn-Proxy

The text from section 4.2.2a applies also here.

I.2.3 HSS

The set of all user security settings (USSs), i.e. GUSS, is stored in the HSS.

The requirements on the HSS are:

- HSS shall provide the only persistent storage for GUSSs;
- GUSS shall be defined in such a way that interworking of different operators for standardised application profiles is possible;
- GUSS 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.
- GUSS shall be able to contain application-specific USSs that contain parameters that are related to identification or authorization information of one or more applications hosted by one ore more NAFs. Any other types of parameters are not allowed in the application-specific USS.

NOTE 1: The necessary subscriber profile data may be fetched by the NAF directly from HSS or from its local database using identity information provided by the application-specific USS.

NOTE 2: The HSS may temporarily remove an application-specific USS from the GUSS if the service is temporarily revoked from the subscriber.

- GUSS shall be able to contain parameters intended for the BSF usage:
  - subscriber specific key lifetime;
  - optionally the timestamp indicating the time when the GUSS has been last modified by the HSS.

NOTE 3: These parameters are optional and if they are missing from subscriber's GUSS or subscriber does not have GUSS then the BSF will use the default values in the BSF local policy defined by the particular MNO.

- HSS shall be able to assign application-specific USSs to a NAF Group. This shall be defined in such a way that different USSs for the same application, but for different groups of NAFs, are possible. The restrictions on the number of USSs per GUSS are dependent on the usage of NAF Groups by the operator:
  - if no NAF Groups are defined for this application then at most one USS per application is stored in GUSS;
  - if NAF Groups are defined for this application then at most one USS per application and NAF Group is stored in GUSS.
- NAF Group definitions in the HSS and all connected BSFs belonging to the same operator's network shall be equal.
  - Information on UICC type and on key choice are not required for 2G subscribers. 2G GBA is regarded as ME-based.

I.2.4 UE

The required functionalities from the UE are:

- the support of HTTP Digest AKA protocol;
- the support of TLS;
- the capability to use a SIM in bootstrapping;
- the capability for a Ua application on the ME to indicate to the GBA Function on the ME whether a SIM is allowed for use in bootstrapping (see clause I.4.8);
- the capability to derive new key material to be used with the protocol over Ua interface from Kc, RAND, SRES and Ks-input;
- support of NAF-specific application protocol (For an example see TS 33.221 [5]).

A 2G GBA-aware ME shall support both 3G GBA_U, as specified in clause 5.2 and 3G GBA_ME procedures, as specified in clause 4.5.

I.2.5 SLF

The text from section 4.2.5 applies also here.

I.3 Bootstrapping architecture and reference points

I.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 2G AKA infrastructure.

I.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 the protocol over reference point Ub.

I.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 2G Authentication Centre is HSS-internal, and it need not be standardised as part of this architecture.

I.3.4 Reference point Zn

The reference point Zn is used by the NAF to fetch the key material agreed during a previous 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.

I.3.5 Reference point Dz

The text from section 4.3.5 applies also here.

I.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.
- an attacker shall not be able to exploit a security breach in one security protocol over Ua in order to mount a successful attack against a different security protocol over Ua.
- Existing SIM cards or SIMs on UICCs and their specifications shall not be impacted.
- If USIM or ISIM are available they shall be used as specified in sections 4 and 5, and 2G GBA shall not be used.
- 2G GBA shall not impact the USIM / ISIM based GBA as specified in sections 4 and 5.
- 2G GBA shall not reduce security for USIM / ISIM users.
- 2G GBA shall minimise the changes to the USIM / ISIM based GBA specified in section 4.
- 2G GBA shall provide measures to mitigate known vulnerabilities of GSM.

I.4.1 Access Independence

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

I.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 GSM authentication (also called 2G AKA) protocol. BSF authentication shall in addition be based on TLS with server certificates.

I.4.3 Roaming

The text from section 4.4.3 applies also here.

I.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 the methods in I.4.2;
- 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.

I.4.5 Requirements on reference point Zh

The requirements for reference point Zh are:

- mutual authentication, confidentiality and integrity shall be provided;

NOTE 1: 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;
- optionally the BSF may have the capability able to send the timestamp of subscriber's GBA user security settings to the HSS (timestamp option);
- the HSS shall be able to send one 2G AKA vector at a time to the BSF;
- the HSS shall be able to send the complete set of subscriber's GBA user security settings needed for security purposes to the BSF. Optionally the HSS may have the capability to indicate to the BSF whether the BSF already has the latest copy of the GUSS based on the GUSS timestamp (timestamp option);

NOTE 2: If subscriber's GUSS is updated in HSS, this is not propagated to the BSF. The GUSS in the BSF is updated when the BSF next time fetches the authentication vectors and GUSS from the HSS over Zh reference point as part of the bootstrapping procedure.

- no state information concerning bootstrapping shall be required in the HSS;
- all procedures over reference point Zh shall be initiated by the BSF;
- the number of different interfaces to HSS should be minimized.

I.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 DIAMETER based Zn reference point shall be secured according to NDS/IP [13];
- If the BSF and the NAF are located in different operators' networks, the DIAMETER based Zn' reference point between the Zn-Proxy and the BSF shall be secured using TLS as specified in RFC 2246 [6];

NOTE 1: Annex E specifies the TLS profile that shall be applied.

- An HTTP based Zn/Zn' reference point shall be secured using TLS as specified in RFC 2246 [6];

NOTE 1b: Annex E specifies the TLS profile that shall be applied.

- The BSF shall verify that the requesting NAF is authorised to obtain the key material or the key material and the requested USS;
- 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 USSs 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 USSs for;

NOTE 2: If some application needs only a subset of an application-specific USS the NAF selects this subset from the complete set of USS sent from BSF.

- The BSF shall be able to be configured on a per NAF or per application basis if private subscriber identity and which application-specific USSs may be sent to a NAF;
- If a NAF requests USSs from the BSF and they are not present in subscriber's GUSS, it shall not cause an error, provided the conditions of the local policy of the BSF are fulfilled. The BSF shall then send only the requested and found USSs to the NAF;
- It shall be possible to configure a local policy as follows: BSF may require one or more application-specific USS to be present in a particular subscriber’s GUSS for a particular requesting NAF, and to reject the request from the NAF in case the conditions are not fulfilled. In order to satisfy this local policy, it is not required that the NAF requests the USSs over the Zn reference point, which the BSF requires to be present in the GUSS, rather it is sufficient that the BSF checks the presence of the USSs locally. It shall also be possible configure the BSF in such a way that no USS is required for the requesting NAF;
- The BSF shall be able to indicate to the NAF the bootstrapping time and 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.

NOTE 3: This does not preclude a NAF to refresh the key before the expiry time according to the NAF's local policy.

NOTE 4: If one or more of the USSs that have been delivered to the NAF has been updated in subscriber's GUSS in the HSS, this change is propagated to the NAF the next time it fetches the USS from the BSF over Zn reference point (provided that the BSF has updated subscriber's GUSS from the HSS over Zh reference point).

- The BSF shall send information to the NAF that the subscriber is a 2G subscriber. If no such information is sent the NAF shall assume that the subscriber is a 3G subscriber.

NOTE 5: This requirement enables a NAF to accept 2G subscribers according to its local policy. The second sentence ensures backward compatibility with the procedures specified in section 4 and 5 of this specification. Note also that inclusion of information on the type of subscription in the GUSS would not suffice to satisfy this requirement as a GUSS need not be present for every subscriber.

- The BSF may determine according to its local policy that the NAF shall not serve 2G subscribers. If this is the case, the BSF does not send keys to the NAF.

NOTE 6: This requirement allows an operator controlling the BSF to determine which applications shall use 3G security only. This requirement is also necessary for NAFs, which are not capable to evaluate the information about the subscription type sent by the BSF, e.g. pre-release 7 NAFs.

- NAF shall be able to indicate to BSF the protocol identifier of Ua security protocol it requires the key material by sending NAF-Id to BSF (cf. Annex H).

I.4.7 Requirements on Bootstrapping Transaction Identifier

Bootstrapping transaction identifier (B-TID) shall be used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn.

Requirements for B-TID are:

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

NOTE 1: NAF can remove the security association based on deletion conditions after the key has become invalid.

NOTE 2: Care has to be taken that the parallel use of GBA and non-GBA authentication between UE and NAF does not lead to conflicts, e.g. in the name space. This potential conflict cannot be resolved in a generic way as it is dependent on specific protocol and authentication mechanism used between UE and application server. It is therefore out of scope of this specification.
For the example of HTTP Digest authentication used between UE and NAF, parallel use is possible as the following applies: <username,password>-pairs must be unique to one realm only. As the NAF controls the realm names, it has to ensure that only the GBA based realm is named with the reserved 3GPP realm name. In the special case that the NAF wants to allow non GBA based authentication in the GBA realm also, it has to ensure that no usernames in the format of a B-TID are used outside GBA based authentication.

I.4.8 Requirements on selection of UICC application and SIM card

If a UICC is present in the UE, containing a USIM or an ISIM, then a USIM or ISIM shall be used as specified in section 4.4.8. Otherwise a SIM shall be used.

If no UICC, but a SIM card is present in the UE, the SIM card shall be used. The IMPI is obtained from the IMSI as specified in section 4.4.8.

I.4.9 Requirements on reference point Ua

The text from section 4.4.9 applies also here.

I.4.10 Requirements on reference point Dz

The text from section 4.4.10 applies also here.

I.5 Procedures

This chapter specifies in detail the format of the 2G GBA bootstrapping procedure that is further utilized by various applications. It contains the authentication procedure with BSF, and the key material generation procedure.

I.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 use of shared keys obtained by means of the GBA, the UE shall contact the NAF for further instructions (see figure I.2).

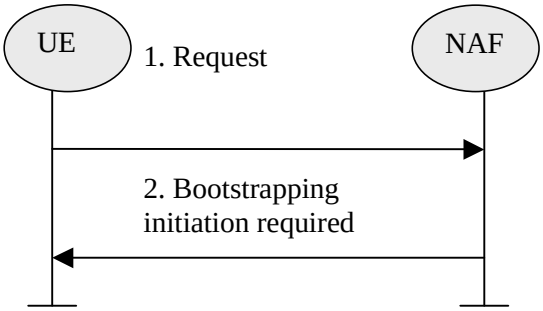


Figure I.2: Initiation of bootstrapping

1. UE starts communication over reference point Ua with the NAF without any GBA-related parameters.
2. If the NAF requires the use of shared keys obtained by means of the GBA, but the request from UE does not include GBA-related parameters, the NAF replies with a bootstrapping initiation message. The form of this indication may depend on the particular reference point Ua and is specified in the relevant stage 3-specifications.

I.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 I.3). Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a bootstrapping negotiation indication from the NAF, or when the lifetime of the key in UE has expired (cf. subclause I.5.3).

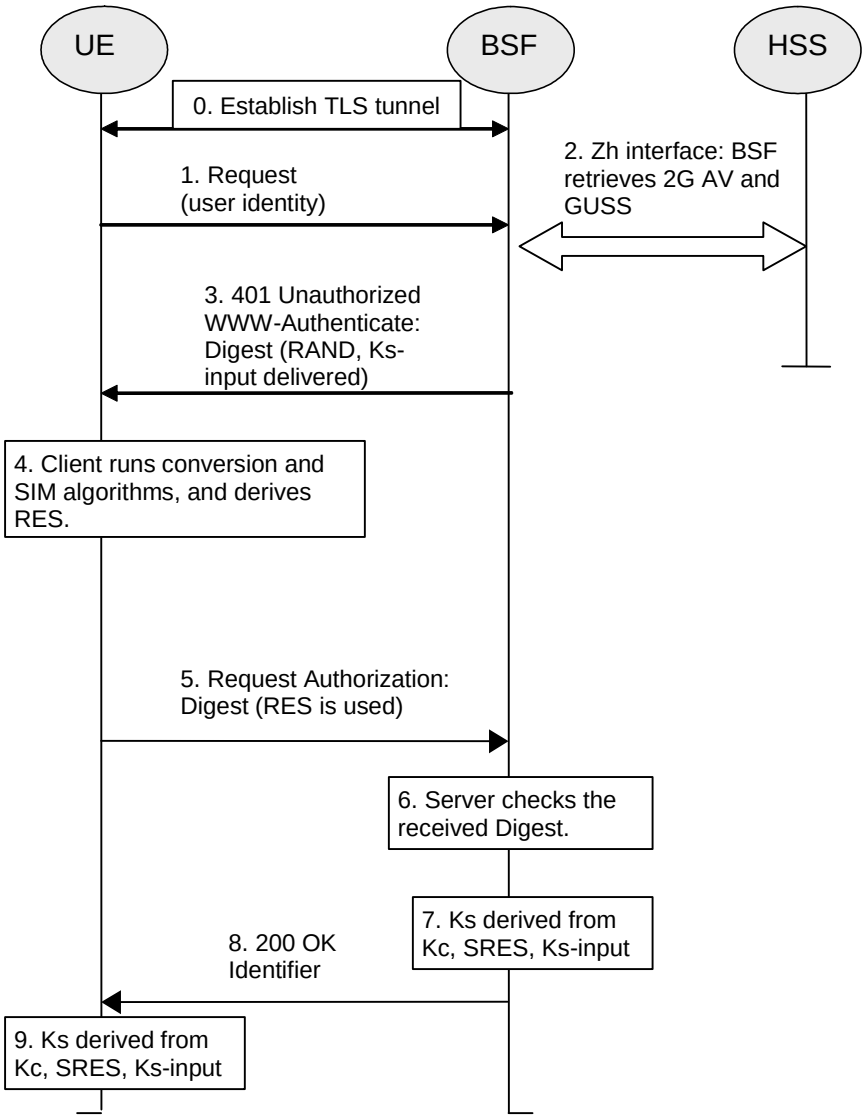


Figure I.3: The bootstrapping procedure

1. The UE sets up a confidentiality-protected TLS tunnel with the BSF. In the set up of the TLS tunnel, the UE shall authenticate the BSF by means of a certificate provided by the BSF. The UE shall check that the "realm" attribute contains the same FQDN of the BSF that was present in the certificate offered by the BSF. All further communication between ME and BSF is sent through this TLS tunnel. The UE now sends an initial HTTPS request.

2. The BSF requests authentication vectors and GUSS from the HSS over Zh. The HSS returns the complete set of GBA user security settings (GUSS) and one 2G authentication vectors (AV = RAND, SRES, Kc) over the Zh reference point. The BSF discovers that the UE is equipped with 2G SIM by looking at the type of authentication vectors.

   If the BSF implements the timestamp option and has a local copy of the GUSS for the subscriber that has been fetched from the HSS during a previous bootstrapping procedure, and this GUSS includes a timestamp, the BSF may include the GUSS timestamp in the request message. Upon receiving that timestamp, if the HSS implements the timestamp option, the HSS may compare it with the timestamp of the GUSS stored in the HSS. In this case, if and only if the HSS has done the comparison and the timestamps are equal, then the HSS shall send "GUSS TIMESTAMP EQUAL" indication to the BSF. In any other case, the HSS shall send the GUSS (if available) to the BSF. If the BSF receives "GUSS TIMESTAMP EQUAL" indication, it shall keep the local copy of the GUSS. In any other case, the BSF shall delete the local copy of the GUSS, and store the received GUSS (if sent).

   The BSF converts one 2G authentication vector (RAND, Kc, SRES) to the parameter RES.

   - RES = KDF (key, "3gpp-gba-res", SRES), truncated to 128 bits

where key = Kc || Kc || RAND and KDF is the key derivation function specified in Annex B of TS 33.220.

The BSF shall also select a 128-bit random number “Ks-input” and set
server specific data = Ks-input
in the aka-nonce of HTTP Digest AKA, cf. [4].

NOTE 1: "Truncated to 128 bits" means that from the 256 bits output of KDF, the 128 bits numbered as [0] to [127] are used.

NOTE 2: In a multiple HSS environment, the BSF may have to obtain the address of the HSS where the subscription of the user is stored by querying the SLF, prior to step 2.

3. The BSF shall forward RAND and server specific data in the 401 message to the UE (without RES). This is to demand the UE to authenticate itself.

4. The UE extracts RAND from the message and calculates the corresponding Kc and SRES values. It then calculates the parameter RES from these values as specified in step 2.

5. The UE sends another HTTP request, containing the Digest AKA response (calculated using RES as the password) and a cnonce (cf. [3]), to the BSF.

6. The BSF authenticates the UE by verifying the Digest AKA response. If the authentication fails the BSF shall not re-use the authentication vector in any further communication.

7. The BSF shall generate key material Ks by computing Ks = KDF (key, Ks-input, "3gpp-gba-ks", SRES).
The B-TID value shall be also generated in format of NAI by taking the base64 encoded [12] RAND value from step 3, and the BSF server name, i.e. base64encoded(RAND)@BSF_servers_domain_name.

8. The BSF shall send a 200 OK message, including a B-TID and an authentication-info header (cf. [3]), to the UE to indicate the success of the authentication. In addition, in the 200 OK message, the BSF shall supply the lifetime of the key Ks.

9. The UE shall abort the procedure if the server authentication according to [3] fails. If it is successful the UE shall generate the key material Ks in the same way as the BSF.

10. Both the UE and the BSF shall use the Ks to derive the key material Ks_NAF for use with the procedures specified in clause I.5.3. Ks_NAF shall be used for securing the reference point Ua.

    Ks_NAF is computed as Ks_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_Id), where KDF is the key derivation function as specified in Annex B, and the key derivation parameters consist of the user's IMPI, the NAF_Id and RAND. The NAF_Id consists of the full DNS name of the NAF, concatenated with the Ua security protocol identifier as specified in Annex H. KDF shall be implemented in the ME.

    To allow consistent key derivation based on NAF name in UE and BSF, at least one of the three following prerequisites shall be fulfilled:

    (1)The NAF is known in DNS under one domain name (FQDN) only, i.e. no two different domain names point to the IP address of the NAF. This has to be achieved by administrative means.

    (2) Each DNS entry of the NAF points to a different IP address. The NAF responds to all these IP addresses. Each IP address is tied to the corresponding FQDN by NAF configuration. The NAF can see from the IP address, which FQDN to use for key derivation.

    (3) Ua uses a protocol which transfers the host name (FQDN of NAF as used by UE) to NAF (e.g. HTTP/1.1 with mandatory Host request header field). This requires the NAF to check the validity of the host name, to use this name in all communication with UE where appropriate, and to transfer this name to BSF to allow for correct derivation of Ks_NAF.
    In case of a TLS tunnel over Ua this requires either multiple-identities certificates for the NAF or the deployment of RFC 3546 [9] over Ua or other protocol means with similar purpose over Ua.

    The UE and the BSF shall store the key Ks with the associated B-TID for further use, until the lifetime of Ks has expired, or until the key Ks is updated or until the deletion conditions are satisfied (see 4.4.11).

I.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 I.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 I.4.

1. 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 I.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;

     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 or will expire soon, or the key can not meet the NAF local validity condition, it shall send a suitable bootstrapping renegotiation request to the UE, see figure I.5. If the key's lifetime has expired the protocol used over reference point Ua shall be terminated. 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 I.5.2, in order to obtain a new key Ks.

     To allow for consistent key derivation in BSF and UE, both have to use the same FQDN for derivation (see clause I.5.2). For each protocol used over Ua it shall be specified if only cases (1) and (2) of clause I.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 1: 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 I.3.2, to allow the NAF to retrieve the corresponding keys from the BSF;

   NOTE 2: 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.

   - the key management procedures for GBA related keys in the ME (i.e. Ks and Ks_NAF keys) are described in section 4.4.11.

   - 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;

     According to the procedures defined in clauses I.5.2 and I.5.3, in the UE there is at most one Ks_NAF key stored per NAF-Id.

2. 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 one or more application-specific USSs for the applications, which the request received over Ua from UE may access;

- With the key material request, the NAF shall supply NAF-Id (which includes NAF's public hostname that UE has used to access NAF and the Ua security protocol identifier) to BSF, and BSF shall be able verify that NAF is authorized to use that hostname;

3. 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 I.5.2, and supplies to NAF the requested key Ks_NAF, as well as the bootstrapping time and the lifetime of that key, and the requested application-specific and potentially NAF group specific USSs if they are available in subscriber's GUSS and if the NAF is authorized to receive the requested USSs. In addition, the BSF shall indicate to the NAF that the subscriber is a 2G subscriber. 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 3: The NAF can further set the local validity condition of the Ks_NAF according to the local policy, for example a limitation of reuse times of a Ks_NAF.

NOTE 4: The NAF will 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.

- The BSF may require that one or more application-specific and potentially NAF group specific USSs shall be present in subscriber's GUSS for the NAF (see clause I.4.6). If one or more of these required settings are missing from the GUSS, the BSF shall indicate this in the reply to the NAF.

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

- If the BSF or the NAF determined, according to their local policies, that the NAF shall not serve 2G subscribers, the NAF shall terminate the protocol over the reference point Ua.

4. 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.

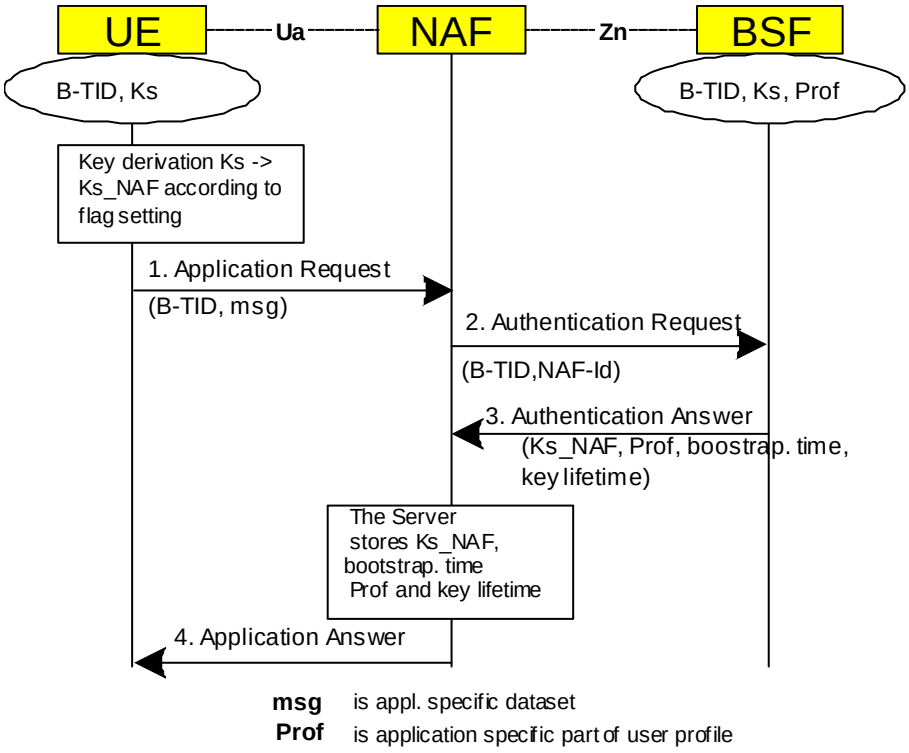


Figure I.4: The bootstrapping usage procedure

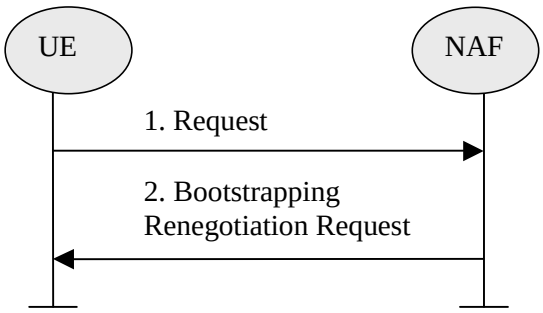


Figure I.5: Bootstrapping renegotiation request

I.5.4 Procedure related to service discovery

The UE shall discover the address of the BSF from the IMSI on the SIM. The same discovery procedure as specified in Section 4.5.4. shall be used.

I.6 TLS Profile

The UE and the BSF shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [30] or higher. Earlier versions are not allowed.

NOTE 1: The management of Root Certificates is out of scope of this Technical Specification.

NOTE 2: Revocation of certificates is out of scope of this Technical Specification. It is noted, however, that choosing short lifetimes for BSF certificates may considerably reduce the risk, in case BSF certificates may ever be compromised.

I.6.1 Protection mechanisms

The UE shall use the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA or the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA.

The BSF shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA.

I.6.2 Authentication of the BSF

The BSF is authenticated by the Client as specified in WAP-219-TLS [30], which in turn is based on RFC 2246 [6].

The BSF certificate profile shall be based on WAP Certificate and CRL Profile as defined in WAP 211 WAPCert [31].

I.6.3 Authentication of the UE

The BSF shall not request a certificate in a Server Hello Message from the UE. The BSF shall authenticate the UE as specified in clause I.5.2 of this specification.

I.6.4 Set-up of Security parameters

The TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the BSF shall allow for resuming a session. The lifetime of a Session ID is subject to local policies of the UE and the BSF. A recommended lifetime is five minutes. The maximum lifetime specified in [6] is 24 hours.

NOTE: If the BSF adheres to the recommended lifetime the UE can be certain to be able to resume the TLS session in case of bootstrapping re-negotiation.

Annex J (informative): Usage of USS with local policy enforcement in BSF

This Annex describes how the local policy enforcement in the BSF is used between the NAF and the BSF to control the key delivery to the NAF.

J.1 General

A BSF may have a local policy for zero or more NAFs where the policy for a NAF may state that subscriber's GUSS shall include one or more USSs identified by a GSID. In other words, for a particular NAF the BSF may require that one more USSs shall be present in subscriber's GUSS.

In general, there are two network elements where access control based on some local policy is enforced, i.e. NAF and BSF. Thus two phases with access control based on USSs have to be covered:

1) Access control within NAF for Ua requests: Whether the subscriber is allowed to access the service is decided in the NAF and possibly with the help of USSs. Upon receiving the B-TID from the UE, the NAF fetches the NAF specific shared key (Ks_(ext/int)_NAF) from the BSF, and optionally fetches the USSs, which typically contain NAF specific persistent user identities, and authorization flags. Based on a local policy in the NAF, which may include evaluating the contents of the USS, the NAF decides whether the subscriber is allowed to access the service.

2) Access control within BSF for Zn requests: In certain cases, the operator may wish to implement access control in the BSF. This functionality can be used with any NAF, but the main reason for having this is to implement home operator control in the cases where the NAF is in a visited network.

This Annex describes the access control case within the BSF for Zn requests in more detail.

The following facts should be noted on use of this Annex:

- This access control is completely local to the network of the BSF operator (i.e. home operator of subscriber). This implies that no inter-operator agreement is necessary for implementation of this access control.

- The local policies of the BSF may be based on NAF names and on NAF groups. For the sake of brevity only NAFs are mentioned in the following descriptions.

J.2 Usage scenarios

Four different scenarios can be identified how the local policy enforcement in the BSF will work:

1) A NAF does not use USSs (i.e. it does not request a USS from the BSF), and the BSF does not have a local policy for this NAF.

2) A NAF does not use USSs (i.e. it does not request a USS from the BSF), and the BSF does have a local policy for this NAF.

3) A NAF does use USSs (i.e., it requests one or more USSs from the BSF), and the BSF does not have a local policy for this NAF.

4) A NAF does use USSs (i.e., it request one or more USSs from the BSF), and the BSF does have a local policy for this NAF.

The steps executed in each of these scenarios are described in more detail in the following subclauses.

In all scenarios the NAF has received B-TID from the UE over the Ua reference point before the following steps are executed. The steps describe only the procedures that are related to the local policy enforcement in the BSF with respect to USS existence. Also transfer of other information elements not related to this access control is not mentioned (e.g. key lifetime, private subscriber identity).

J.2.1 Scenario 1: NAF does not use USSs, BSF does not have local policy for NAF

In this scenario, the NAF does not use USSs and the BSF does not have a local policy for this NAF.

1. The NAF requests the NAF specific shared key(s) from the BSF. It does not include any GSIDs in the request.
2. The BSF locates the subscriber information in its local memory using the B-TID.
3. The BSF checks whether a local policy exists for the NAF - in this scenario there is no local policy, i.e. for this particular NAF, the BSF does not require any USSs (identified by GSIDs) to be present in subscriber's GUSS.
4. The BSF derives the NAF specific shared key(s), and sends them to the NAF in the response.
5. The NAF receives the response with the NAF specific shared key(s).

After receiving the NAF specific shared key(s), the NAFmay perform access control to the service according to its own policies and continues to communicate with the UE.

J.2.2 Scenario 2: NAF does not use USSs, BSF does have local policy for NAF

In this scenario, the NAF does not use USSs and the BSF does have a local policy for this NAF.

1. The NAF requests the NAF specific shared key(s) from the BSF. It does not include any GSIDs in the request.
2. The BSF locates the subscriber information in its local memory using the B-TID.
3. The BSF checks whether a local policy exists for the NAF - in this scenario there is a local policy for this NAF, i.e. for this particular NAF, the BSF does not require any USSs (identified by GSIDs) to be present in subscriber's GUSS.

   The BSF checks whether all the required USSs identified by GSIDs are present in subscriber's GUSS: If yes, the BSF continues from step 4. If not, the BSF the BSF sends an error message to the NAF.

NOTE: As specified in clause 4.4.8, it is not required that the NAF requests the USSs over the Zn reference point, which the BSF requires to be present in the GUSS for particular NAF, rather it is sufficient that the BSF checks the presence of the USSs locally.

4. The BSF derives the NAF specific shared key(s), and sends them to the NAF in the response.
5. The NAF receives the response with the NAF specific shared key(s).

After receiving the NAF specific shared key(s), the NAF may perform access control to the service according to its own policies and continues to communicate with the UE.

If the NAF received the "not authorized" error message, it may indicate this to the UE over Ua reference point. In any case, the GAA based security setup will fail between the UE and the NAF since the NAF did not get the NAF specific shared key(s).

J.2.3 Scenario 3: NAF does use USSs, BSF does not have local policy for NAF

In this scenario, the NAF does use USSs and the BSF does not have a local policy for this NAF.

1. The NAF requests the NAF specific shared key(s) from the BSF. It includes the GSIDs it needs in the request.
2. The BSF locates the subscriber information in its local memory using the B-TID.
3. The BSF checks whether a local policy exists for the NAF - in this scenario there is no local policy, i.e. BSF does not require USSs identified by GSIDs to be present in subscriber's GUSS.

4. The BSF derives the NAF specific shared key(s), and sends them and the USSs identified by the GSIDs to the NAF in the response. If a particular USS is not found in subscriber's GUSS, or the NAF is not authorized to receive a particular USS, these USSs are omitted from the response.

5. The NAF receives the response with the NAF specific shared key(s), and those requested USSs that were available (i.e., found in subscriber's GUSS and allowed by the BSF to be received by the NAF).

After receiving the NAF specific shared key(s) and the available USSs, the NAF may perform access control to the service according to its own policies (e.g. USS required or not, authorization flags required) and continue to communicate with the UE.

J.2.4 Scenario 4: NAF does use USSs, BSF does have local policy for NAF

In this scenario, the NAF does use USSs and the BSF does have a local policy for this NAF.

1. The NAF requests the NAF specific shared key(s) from the BSF. It includes the GSIDs it needs in the request.

2. The BSF locates the subscriber information in its local memory using the B-TID.

3. The BSF checks whether a local policy exists for the NAF - in this scenario there is a local policy for this NAF, i.e., one or more USSs identified by GSIDs shall be present in subscriber's GUSS.

   The BSF checks whether all the required USSs identified by GSIDs are present in subscriber's GUSS: If yes, the BSF continues from step 4. If not, the BSF the BSF sends an error message to the NAF.

4. The BSF derives the NAF specific shared key(s), and sends them and the USSs identified by the GSIDs to the NAF in the response. If a particular USS is not found in subscriber's GUSS, or the NAF is not authorized to receive a particular USS, these USSs are omitted from the response.

5. The NAF receives the response with the NAF specific shared key(s), and those requested USSs that were available (i.e., found in subscriber's GUSS and allowed by the BSF to be received by the NAF).

After receiving the NAF specific shared key(s) and the available USSs, the NAF may perform access control to the service according to its own policies (e.g. USS required or not, authorization flags required) and continue to communicate with the UE.

If the NAF received the "not authorized" error message, it may indicate this to the UE over Ua reference point. In any case, the GAA based security setup will fail between the UE and the NAF since the NAF did not get the NAF specific shared key(s).

Annex K (informative): Interoperator GBA-usage examples

This Annex gives examples how interoperator GBA is set up and operated.

K.1 Example on interoperator GBA setup

Interoperator GBA is set up the following way:

- Each home network operator sets up a BSF, which will enable bootstrapping sessions for its own subscribers.

- Each operator acting as a Serving Network for foreign subscribers in interoperator GBA needs to set up a Zn-Proxy which will forward the authentication requests from its own NAFs to the subscriber's home BSF outside of the VPLMN. The GBA secret is provisioned from the home operator's BSF through the Zn-Proxy to the NAF.

NOTE 1: The security requirements on the Zn' reference point between the Zn-Proxy and the BSF can be found in clause 4.2.2a.

- Each home operator that wants to provide the GBA secrets to foreign NAFs has to authorize these NAFs to request bootstrapping secrets. This is done by using TLS client certificates issued to Zn-Proxies in the serving network by the home network operator.

NOTE 2: The TLS client certificate profile is specified in the normative Annex E, and TLS client certificate issuing is discussed in the informative Annex F.

- An operator that wishes to co-operate in interoperator GBA with another operator shall issue a TLS client certificate to the other operator's Zn-Proxy. Two operators may both act as home operators or as serving operators (i.e., both possess a BSF and a Zn-Proxy), but this Annex also applies to configurations where one operator is always acting as home operator (i.e., hosts the BSF) and the other operator only as serving operator (i.e., the operator hosts only the Zn-Proxy). In the second case, where the serving foreign operator has the Zn-Proxy only, the TLS client certificate is to be handed down in one direction only (see also Annex E on usage of client certificates).

NOTE 3: The enrollment of the TLS client certificate is outside the scope of the GBA specification (see Annex F.1). When two operators sign a roaming agreement, they may also enroll TLS client certificate for each others Zn-Proxies. Similarily, the revocation of the TLS client certificate is outside the scope of the GBA specification (see Annex F.2)

NOTE 4: Interoperator GBA is based on bilateral agreements between the two operators. For example, if operator1 has a "GBA agreement" with operator2 and operator1 signs another "GBA agreement" with operator3, this does not mean that operator3 and operator2 have implicitly a "GBA agreement". Operator2 and operator3 shall separately sign a "GBA agreement".

NOTE 5: The home operator may use NAF groups to support local policy checks within its BSF (cf. clause 4.2.1). These may be e.g. one group for NAFs in home network and one group for NAFs in serving networks, or separate groups for each serving network the home operator has "GBA agreements" with. This NAF grouping is under sole responsibility of the home operator and only visible to him. The Zn-Proxies and NAFs in serving networks are not aware of any NAF grouping done in home network.

As described in clause 4.2.2a, a Zn-Proxy may be co-located with a BSF (see Figure K-2). This has the benefit that the NAF has only one logical channel to BSF/Zn-Proxy. Therefore the NAF does not need to make a decision based on the B-TID whether to send the authentication request to the Zn-Proxy or to the BSF. However, this decision can be based on the B-TID as it contains the address of the BSF.

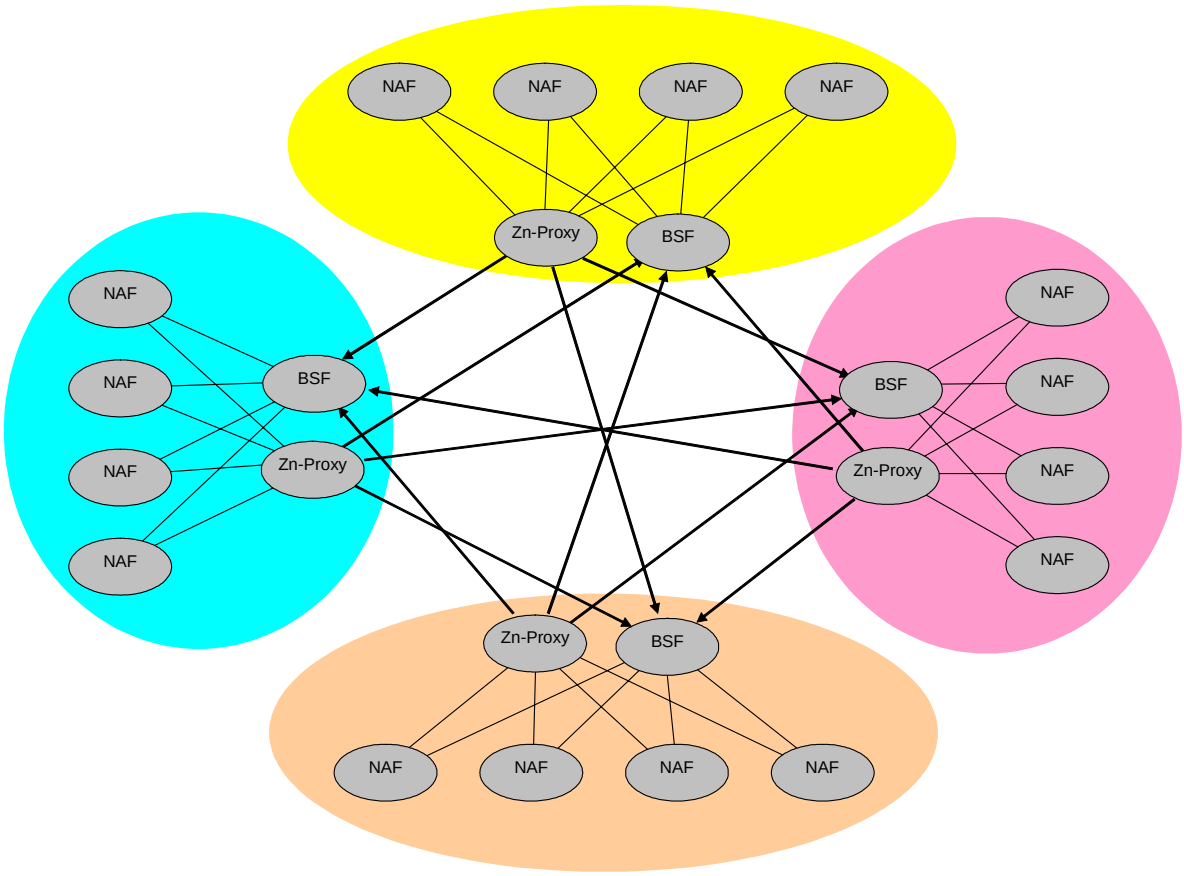


Figure K-1. Interoperator GBA with separate BSF and Zn-Proxy.

NOTE 6: The figure K-1 does not show the most general case, where there could be one Zn-proxy per home network in each serving network. It is expected that networks will be optimized and that the existence of one dedicated Zn-proxy for each foreign subscriber home network will be a rare occurance. The co-location of all Zn-Proxies of one serving network in one location as shown in Figure K-1 is a special case.

NOTE 7: The TLS connections between Zn-Proxy and BSF are "directed", this is indicated in Figure K-1 by the arrowed lines where the arrows point to the server TLS role. The role of the client certificates in these TLS connections is explicitly outlined. Each direction requires a TLS server certificate used at BSF and a TLS client certificate used at Zn-Proxy.

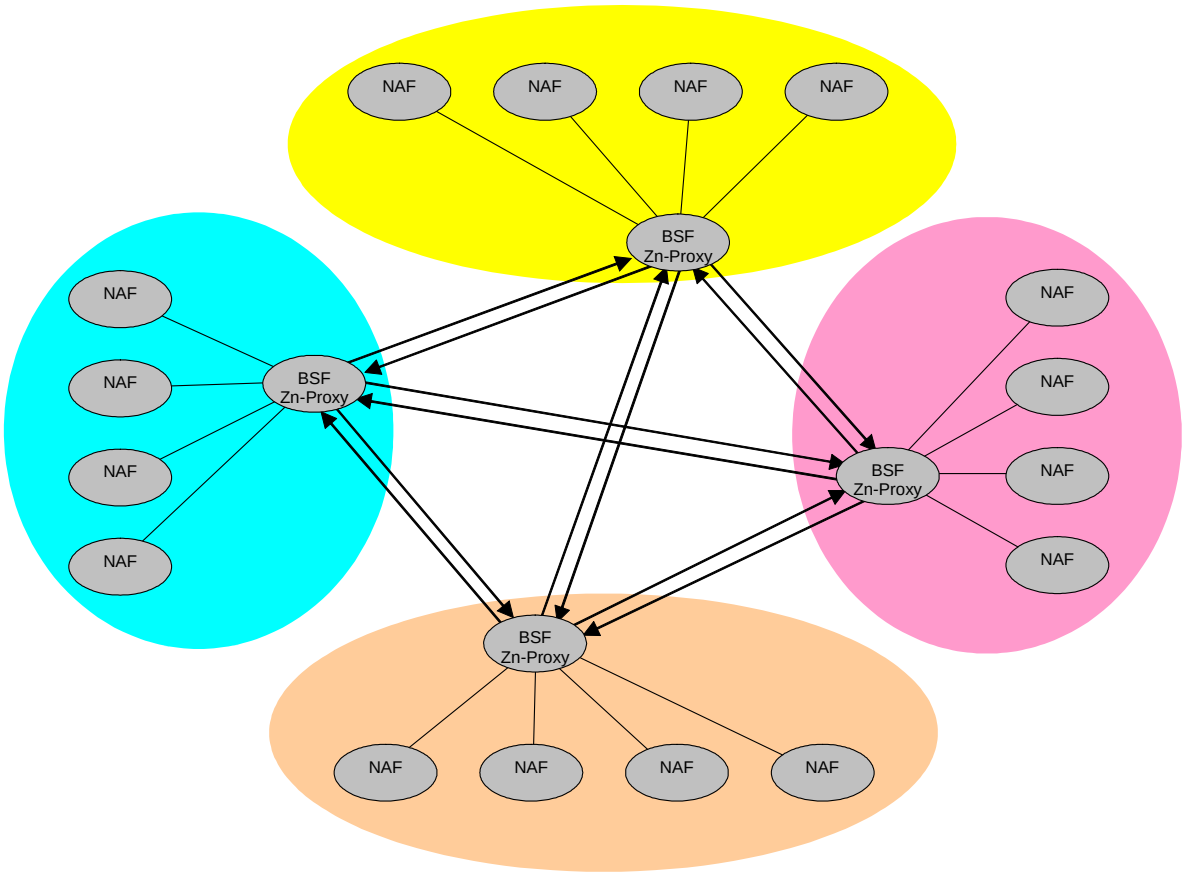


Figure K-2. Interoperator GBA with co-located BSF and Zn-Proxy.

NOTE 8: The two distinct TLS connections between Zn-Proxy and BSF are "directed", this is indicated in Figure K-2 by the two lines. Thus the two TLS connection directions may not be intermixed, as the role of the client certificates in these TLS connections is explicitly outlined. Each direction requires a server TLS certificate used at BSF and a client TLS certificate used at Zn-Proxy.

K.2 Example on interoperator GBA operation

Interoperator GBA usage goes as follows:

NOTE 1: This description is based on GBA_ME bootstrapping to simplify the examples, but GBA_U bootstrapping can also be used in interoperator GBA operation.

1. A UE contacts a NAF that does not belong to subscriber's home network. The foreign NAF notifies the UE that 3GPP bootstrapping is required to secure the connection between the UE and the NAF.

2. The UE bootstraps with the home network via the subscriber's BSF. The address of subscriber's home BSF is generated from user's IMSI or IMPI as specified in TS 33.220, clause 4.5.4. The key Ks, and the B-TID are established between the BSF and the UE.

3. The UE derives the NAF specific key Ks_NAF, and uses Ks_NAF and the B-TID on the Ua reference point between the UE and the foreign NAF. At some point during this setup the UE transfers the B-TID to the NAF in the serving network.

4. Upon receiving the B-TID, the foreign NAF has two modes of operations depending on the actual setup of the Zn-Proxy and the BSF in the serving network:

   NOTE 2: Any BSF in a network different from the home network of a subscriber and any Zn-Proxy are not visible to the subscriber. To avoid any confusion with the subscribers BSF in the home network, the BSF in a visited network is called foreign BSF in this clause.

a) If the Zn-Proxy and the foreign BSF are separate entities, the foreign NAF shall inspect the B-TID to discover whether the subscriber belongs to its own network, or whether it is a visiting subscriber. In the former case, the request for the Ks_NAF is sent to the BSF, in the latter case, the request is sent to the Zn-Proxy.

b) If the Zn-Proxy and the foreign BSF are a co-located entity, the NAF sends the request for the Ks_NAF to this co-located entity. The NAF does not need to inspect the B-TID.

NOTE 3: Since the B-TID contains the address of subscriber's home BSF, it can be used to discover the home network of the subscriber. A NAF supporting this approach can work with both separated and co-located configurations.

5. Upon receiving the request from the NAF, the Zn-Proxy shall inspect the following:

   b) Validate that the NAF is authorized to request the Ks_NAF (i.e., the DNS part of NAF_Id in the message is correct).

   b) Discover the BSF of the subscriber by inspecting the B-TID.

6. The Zn-Proxy will establish or use the existing DIAMETER or HTTP session to subscriber's home BSF. This DIAMETER or HTTP session is secured by TLS, and the Zn-Proxy shall use a client certificate that the BSF trusts.

7. The Zn-Proxy will forward the request to subscriber's home BSF.

8. Subscriber's home BSF shall validate that the DNS part of the NAF_Id in the request also exists in the client certificate of the Zn-Proxy.

9. Subscriber's home BSF locates the bootstrapping information using the B-TID, processes the request (including possible requests for USSs, local policy check, etc.), derive the NAF specific key, and send the response to the Zn-Proxy.

10. The Zn-Proxy will forward the response to the NAF.

11. The NAF continues with the Ua connection establishment with the UE.

Figure K-3 depicts the entities involved in the above procedure.

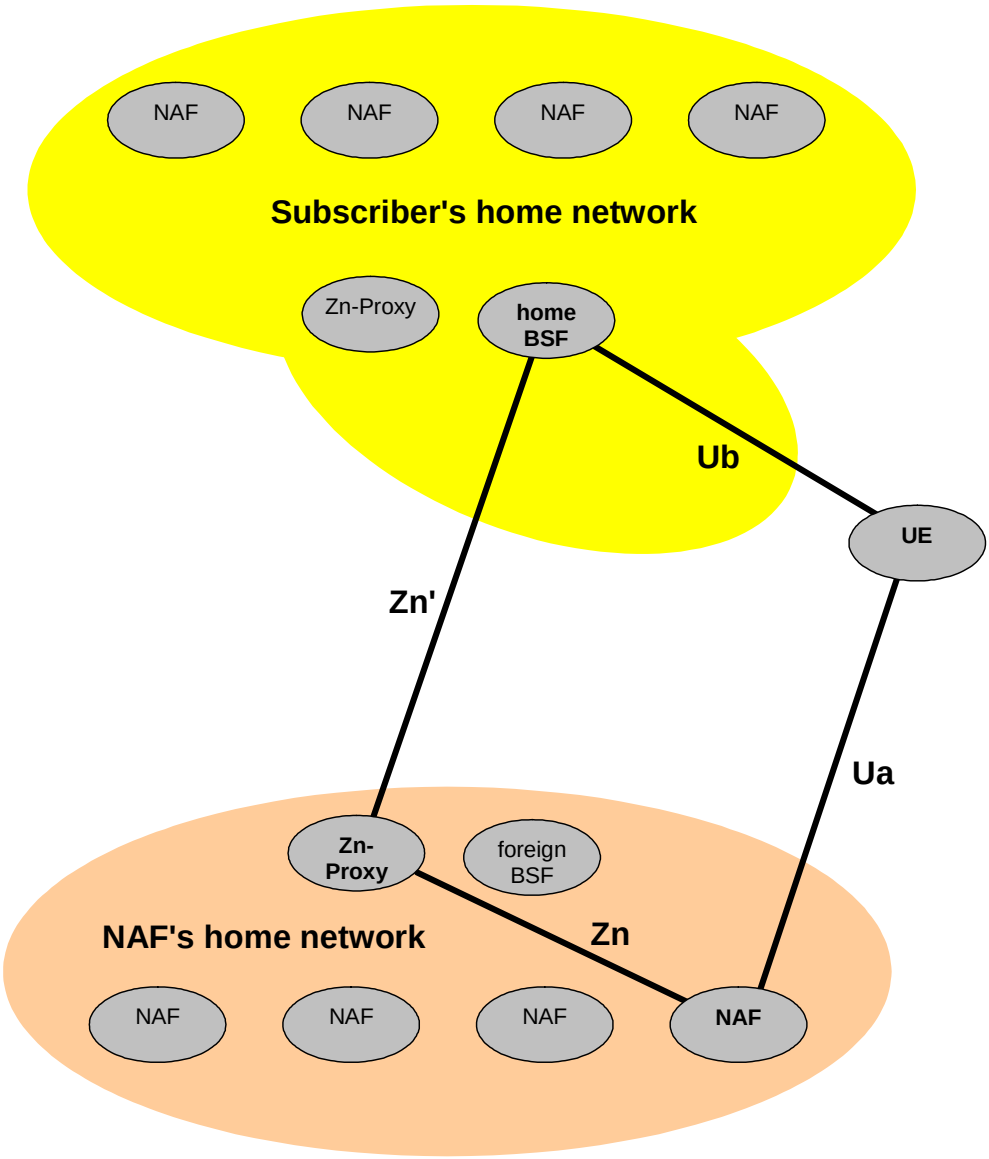


Figure K-3: Interoperator GBA usage.

Annex L (informative): Information on how security threats related to known GSM vulnerabilities are addressed by the 2G GBA solution

The 2G GBA solution aims to provide mutual authentication between UE and BSF. This annex examines how the 2G GBA solution mitigates the impersonation of UE or the BSF i.e. security threats related to the known GSM vulnerabilities.

The threats that are originated from the weakness in the usage of the COMP128 algorithm exist independently of the usage of 2G GBA.

L.1 Impersonation of the UE to the BSF during the run of the Ub protocol

This is the main threat to the 2G GBA solution.

1) An attacker (being in the possession of 2G GBA equipment) could try to perform a Man-in-the-middle-attack, impersonating a genuine GSM user to the BSF. In this scenario the attacker would be at the client end of the TLS tunnel to the BSF and send the challenge RAND to the target GSM user, in order to obtain SRES and Kc. However, for the attack to be successful, he would have to find also Kc within the runtime allowed for steps 3 to 5 of the protocol over Ub, as specified in Annex I.5.2. This may be feasible when the terminal of the target GSM user still runs A5/2, but is infeasible for the foreseeable future when one of the other GSM encryption algorithms is used. A5/2 will be removed from networks by the end of 2006, and will not be present in any 2G GBA enabled terminals. A vulnerability caused by A5/2 would only exist in the case where a GSM user has subscribed to 2G GBA feature, but uses his SIM in an old terminal with A5/2 enabled while being targeted by the attacker. But the practical implications of this remaining vulnerability are expected to be limited as a user subscribed to 2G GBA will own a Release 7 terminal (2G GBA will be a Release 7 feature), and the likelihood of him inserting his SIM in an old terminal, and an attacker obtaining this information and exploiting it for a man-in-the-middle attack, may be low in practice. Furthermore, old terminals will gradually disappear.

2) SIM cloning: an attacker being able to find the long-term key Ki of a genuine GSM user is able to fully impersonate him in all contexts, including the 2G-GBA one (if this has been subscribed by the genuine user).. The attacker could do this by exploiting weaknesses of A3/A8 as they were found for COMP128, while in possession of the SIM i.e. the attacker tries to find the long term key K. Even if 2G GBA does not increase the risk of possible A3/A8 breakages, it has to be noted that the COMP128-related issue disappears when more secure A3/A8 algorithms are used. These are available today, cf. “GSM MILENAGE”, as specified in TS 55.205 v610. Operators are advised in general to discontinue the use of COMP128

3). Unauthorized access to SIM needs to be countered by platform security methods. The impacts of a compromised SIM/ME or UICC/ME interface on GAA security are similar in 2G GBA and 3G GBA.

L.2 Impersonation of the BSF to the UE during the run of the Ub protocol

To prevent an impersonation attack of the BSF to the UE during the run of the Ub protocol the authentication of the BSF to the UE is improved by protecting the communication with TLS. An attacker succeeds only if he can break both, the certificate-based TLS authentication to the UE and mutual authentication provided by HTTP Digest using a password derived from GSM procedures. One way to break TLS is to compromise the certificate.

L.3 Finding the GBA key Ks during or after the Ub protocol run

For BSF-to-UE authentication and for establishment of the key Ks, the solution relies on both, GSM security and TLS security. The attacker needs to know all the parameters of the GSM triplet, in particular Kc, and additionally break the TLS security, as the attacker also needs to know the Ks-input parameter confidentially transmitted by the BSF over TLS. Breaking GSM security after the Ub protocol run alone does not provide sufficient information to break 2G GBA.

L.4 Bidding down attack

To avoid a bidding down attack (also called downplay attack), the 2G GBA solution requires that a GBA-enabled terminal that supports SIM based 2G GBA must support also USIM/ISIM based 3G GBA as specified in I.2.4. If a USIM/ISIM is available, then the terminal must use the USIM/ISIM based 3G GBA as specified in I.4.8.

Annex M (informative): Change history

Change history									
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New	WI
2004-03	SP-23	SP-040175	-	-	D	Presented for approval at TSG SA #23	1.2.1	2.0.0	
2004-03	SP-23	-	-	-	F	Approved and placed under Change Control (Rel-6)	2.0.0	6.0.0	
2004-06	SP-24	SP-040375	001	-	F	Removal of Annex A	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040376	002	-	B	NAF remove the security associations	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040377	003	1	D	Removal of editors notes on Transaction Identifiers	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040378	004	1	B	Introduction of a UICC-based Generic Bootstrapping Architecture	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040379	005	-	D	Editorial corrections to TS 33.220	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040380	006	-	C	Support for NAF in visited network	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040381	007	-	C	Editorial changes and clarifications to TS 33.220	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040382	008	-	F	Multiple key derivation mandatory	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040383	009	-	C	NAF's public hostname verification	6.0.0	6.1.0	SEC1--SC
2004-09	SP-25	SP-040619	010	-	C	Detailing of key lifetime	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	011	-	C	Details of USIM/ISIM usage in GAA	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	012	-	C	Generic Ua interface requirements	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	013	-	F	B-TID generation	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	014	-	B	Securing Zn reference point	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	015	-	D	GBA User Security Settings	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	016	-	C	Creation of GBA_U AV in the BSF	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	017	-	F	Clarification of the definition of a default type of NAF-specific key	6.1.0	6.2.0	SEC1-SC
2004-12	SP-26	SP-040855	018	1	C	BSF discovery using default domain method	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	019	1	C	Local validity condition set by NAF	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	020	3	C	GBA User Security Settings (GUSS) usage in GAA and Introduction of NAF groups	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	021	2	C	Details of USIM/ISIM selection in GAA	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	023	-	B	TLS profile for securing Zn' reference point	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	025	2	F	Optimization of the GBA_U key derivation procedure	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	027	2	F	Requirement on ME capabilities for GBA_U	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	034	1	D	Adding a note about replay protection	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	035	1	C	Complete the MAC modification for GBA_U	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	036	1	F	Removal of unnecessary editor's notes	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	038	1	C	Fetching of one AV only on each Zh run between BSF and HSS	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	039	1	B	Clean up of TS 33.220	6.2.0	6.3.0	SEC1-SC

2004-12	SP-26	SP-040855	040	1	F	New key management for ME based GBA keys	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	041	1	C	Key derivation function	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	042	1	D	Re-negotation of keys	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	043	1	C	No GUSS/USS update procedures in Release-6	6.2.0	6.3.0	GBA-SSC
2004-12	SP-26	SP-040855	044	1	C	Clarify the number of NAF-specific keys stored in the UE per NAF-Id	6.2.0	6.3.0	SEC1-SC
2005-03	SP-27	SP-040139	045	1	F	Key derivation function: character encoding	6.3.0	6.4.0	SEC1-SC
2005-03	SP-27	SP-040139	047	1	D	Bootstrapping timestamp	6.3.0	6.4.0	SEC1-SC
2005-03	SP-27	SP-040139	048	-	F	Storage of B-TID in GBA_U NAF Derivation procedure	6.3.0	6.4.0	SEC1-SC
2005-06	SP-28	SP-050262	050	1	F	Usage of USS for local policy enforcement in BSF	6.4.0	6.5.0	SEC1-SC
2005-06	SP-28	SP-050262	051	1	F	Correcting figure 4.4	6.4.0	6.5.0	SEC1-SC
2005-06	SP-28	SP-050263	052	-	B	GBA User Security Settings (GUSS) transfer optimisation	6.4.0	7.0.0	SEC1-SC
2005-09	SP-29	SP-050553	0054	-	A	Clarification of anonymous access to NAF in GBA	7.0.0	7.1.0	SEC1-SC
2005-09	SP-29	SP-050554	0056	-	A	Removing IMPI from USS	7.0.0	7.1.0	SEC1-SC
2005-09	SP-29	SP-050572	0057	-	C	Informative annex on usage of USS for local policy enforcement in BSF	7.0.0	7.2.0	SEC1-SC
2005-09	SP-29	SP-050557	0059	-	A	Removing duplication of text relating to BSF addressing	7.0.0	7.1.0	SEC-SC1
2005-09	SP-29	SP-050555	0061	-	A	Clarification of lifetime of derived keys	7.0.0	7.1.0	SEC1-SC
2005-09	SP-29	SP-050575	0062	-	B	Introduction of key selection mechanism	7.0.0	7.2.0	SEC1-SC
2005-09	SP-29	SP-050556	0064	-	A	Addition of the Dz interface for multiple HSS deployments	7.0.0	7.1.0	SEC1-SC
2005-09	SP-29	SP-050565	0066	-	A	Removing requirement to send authentication vectors in batches	7.0.0	7.1.0	GBA
2005-09	SP-29	SP-050551	0068	-	A	Clarification concerning input parameter encoding for GBA_U NAF derivation procedure	7.0.0	7.1.0	SEC1-SC
2005-09	SP-29	SP-050577	0069	1	B	Normative annex on 2G GBA	7.0.0	7.1.0	2G GBA
2005-09	SP-29	SP-050552	0071	-	A	Providing Ua-security protocol based key separation	7.0.0	7.1.0	SEC1-SC
2005-10	post SP-29	-	-	-	-	Editorial change to align annexes between Release 6 and Release 7 based on CRs at SP-29	7.1.0	7.1.1	
2005-12	SP-30	SP-050768	0073	-	A	NAF_Id encoding	7.1.1	7.2.0	SEC1-SC
2005-12	SP-30	SP-050775	0074	-	B	Informative annex with examples on interoperator GBA usage	7.1.1	7.2.0	GAA2
2005-12	SP-30	SP-050775	0075	-	F	Clarification of local policy enforcement	7.1.1	7.2.0	GAA2
2005-12	SP-30	SP-050777	0076	-	F	Alignment of 2G GBA with recent CRs	7.1.1	7.2.0	2GGBA
2005-12	SP-30	SP-050777	0077	-	F	Addition of information requested by SA plenary on 2G GBA	7.1.1	7.2.0	2GGBA
2005-12	SP-30	SP-050777	0078	-	F	IMPI obtained from IMSI in 2G GBA	7.1.1	7.2.0	2GGBA
2005-12	SP-30	SP-050775	0079	-	F	Removal of possible interoperability problems	7.1.1	7.2.0	GAA2
2006-03	SP-31	SP-060061	0080	-	B	D-proxy renaming to Zn-Proxy	7.2.0	7.3.0	SEC7-GAA2 (GAAExt)
2006-03	SP-31	SP-060061	0082	-	B	Protection of Zn/Zn' reference point for http based protocols	7.2.0	7.3.0	SEC7-GAA2 (GAAExt)
2006-03	SP-31	SP-060051	0084	-	A	Restricting the TLS CipherSuites in Annex E and cleanup of references	7.2.0	7.3.0	SEC1-SC
2006-03	SP-31	SP-060061	0085	-	F	Clarifications of requirement	7.2.0	7.3.0	SEC7-2GGBA
2006-03	SP-31	SP-060056	0087	-	A	GBA keys handling and UICC presence detection	7.2.0	7.3.0	TEI
2006-03	SP-31	SP-060049	0089	-	A	Clarify the confusion of the useof NAF-ID and FQDN	7.2.0	7.3.0	(SEC1) (GAAext)
2006-03	SP-31	SP-060061	0090	-	F	key derivation clarifications	7.2.0	7.3.0	SEC7-GAA2 (GAAExt)
2006-03	SP-31	SP-060061	0091	-	F	Use of SIM for a Ua application	7.2.0	7.3.0	SEC7-GAA2 (GAAExt)

History

Document history		
V7.2.0	December 2005	Publication
V7.3.0	March 2006	Publication