3GPP TSG-CN Meeting #25 **NP-040410**
8th – 10th September 2004. Palm Springs, USA

Source: **TSG CN WG 4**

Title: **Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Protocol details**

Agenda item:

Document for: **APPROVAL,- Draft technical specification 3GPP TS 29.109 v2.0.0**

2

Presentation of Technical Specification to TSG

Presentation to: **TSG CN Meeting #25**
Document for presentation: **TS 29.109, Version 2.0.0**
Presented for: **Approval**

Abstract of document:
TS 29.109 is the stage 3 specification of network functions and interfaces in Generic Authentication Architecture (GAA) according stage 2 requirements mainly from TS 33.220 of SA3. TS 29.109 defines the Diameter based Zh (BSF-HSS) and Zn (NAF-BSF) interfaces.

Changes since last presentation to TSG Meeting #:
Transfer and content of user specific permanent control data (user security settings) in the GAA has been completed. Also some minor additions and modifications to information elements in signalling messages and some new supported GAA applications have been defined.

Outstanding Issues:

- Completed work:
  This version of the TS contains detailed definition of basic signalling between HSS, Bootstrapping function (BSF) and Network Application Function (NAF) in GAA.

- Remaining topics:
  It was decided to move the XML definitions in Annex A to a separate zip file, and replace them with a table of Information Elements. It has to be decided if GAA is a domain of itself. Currently GAA data structure has been defined as a part of IMS domain. The decision has anyhow no influence on this TS, it will affect 3GPP TS 23.008.

Contentious Issues:

- None

3GPP TS 29.109 V2.0.0 (2004-09)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol, Stage 3; (Release 6)

Keywords
3GPP, Generic Authentication Architecture

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 stage 3 specification defines the Diameter based implementation for bootstrapping Zh interface (BSF-HSS) and GAA Application Zn interface (BSF-NAF) in Generic Authentication Architecture (GAA). The definition contains procedures, message contents and coding. The bootstrapping and subscriber certificates procedures are defined in 3GPP TS 33.220 [5] and 3GPP TS 33.221 [6].

This specification is a part of the Generic Authentication Architecture (GAA) specification series.

The diameter based implementation is based on re-usage of Cx interface Multimedia-Auth-Request/Answer messages originally between CSCF and HSS. These messages are defined in 3GPP TS 29.229 [3]. The 3GPP IMS mobility management uses the same definitions between CSCF and HSS. The present document defines how the defined messages are used with the bootstrapping and GAA application procedures (e.g. subscriber certificates) and the application logic that is needed in GAA network elements (BSF, HSS, and NAF).

Figure 1.1 depicts the relationships of these specifications to the other specifications.

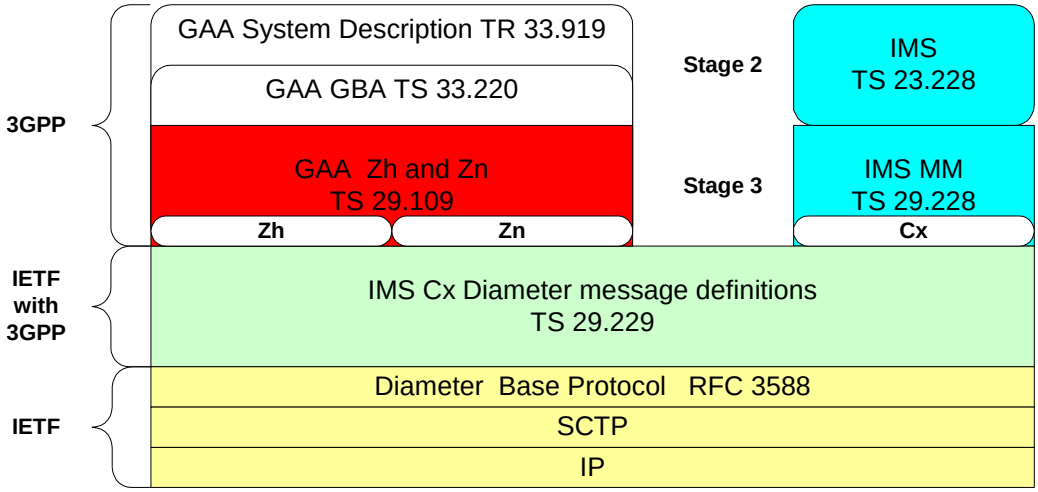
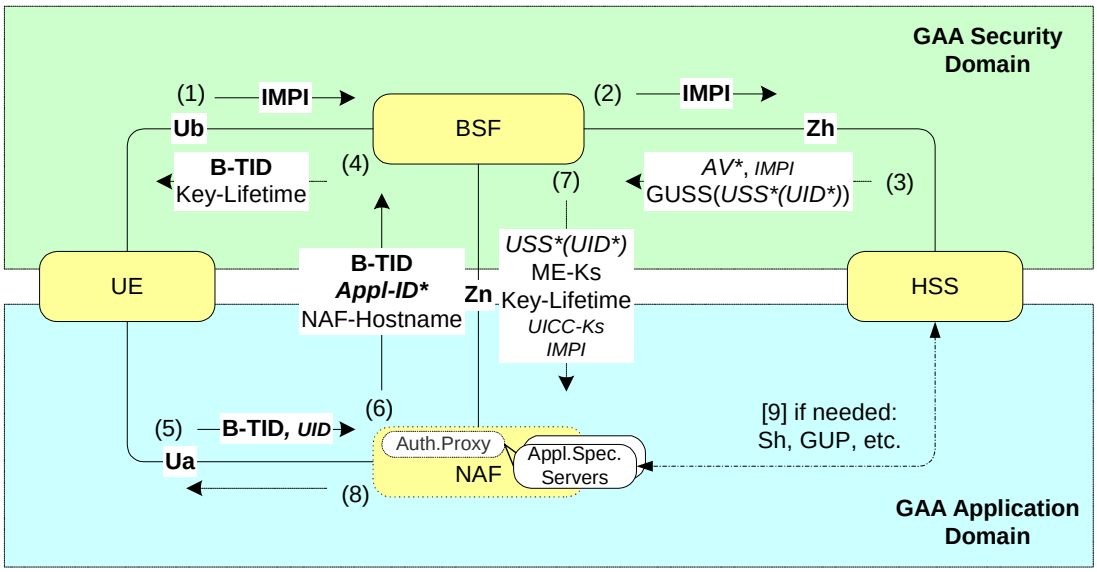


Figure 1.1: Relationships to other specifications

Figure 1.2 provides an informal overall quick introduction to the whole signalling procedures in GAA system. The important identifiers are marked bold and optional data items are italicised. The Ub and Ua interfaces, not defined in this TS , are simplified.



Bold=Important Identity. *Italic*=optional items. Ub and Ua interfaces are simplified.

Figure 1.2: The whole signalling procedure in GAA system

2 References

The following documents contain provisions that, 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] IETF RFC 3588, "Diameter Base Protocol".

[2] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[3] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol".

[4] 3GPP TR 33.919 "Generic Authentication Architecture (GAA); System Description (rel-6)".

[5] 3GPP TS 33.220 "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (rel-6)".

[6] 3GPP TS 33.221 "Generic Authentication Architecture (GAA); Support for Subscriber Certificates (rel-6)".

[7] 3GPP TS 24.109: "Bootstrapping interface (Ub) and Network application function interface (Ua);Protocol details".

[8] 3GPP TS 29.230: "Diameter applications; 3GPP specific codes and identifiers (rel-6)"

[9] IETF RFC 3589: "Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 33.919 [4], 3GPP TS 33.220 [5] and 3GPP TS 33.221 [6] apply with following additions.

Bootstrapping information in a BSF consists of a bootstrapping transaction identifier (B-TID), a key material (Ks) and an application specific user security settings and is identified by B-TID.

GAA application is an application that uses the security association created by GAA Bootstrapping procedure.

User Security Settings are GAA application specific security control settings set by home operator to a user. Typically User security Settings consist of allowed user's public identifications and authorization allowance flags. User Security Settings are identified by GAA Service Identifier.

3.2 Symbols

For the purposes of the present document, the terms and definitions given in 3GPP TR 29.229 [3],

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and Key Agreement
AUTN	Authentication token
AV	Authentication Vector. 3GPP AV=[RAND,AUTN,XRES,CK,IK].
AVP	Attribute-Value-Pair in Diameter messages.
BS	BootStrapping Procedure
BSF	Bootstrapping server functionality BSF is hosted in a network element under the control of an MNO.
B-TID	Bootstrapping Transaction Identifier
CA	Certificate Authority
CK	Confidential Key
FQDN	Full Qualified Domain Name in URI (e.g. http://FQDN:80)
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GUSS	GAA User Security Settings
HSS	Home Subscriber System
IK	Integrity Key
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
Ks	Key Material
MNO	Mobile network operator
NAF	Operator-controlled network application function functionality. NAF is hosted in a network element under the control of an MNO.
RAND	Random challenge in authentication
REQ	In Diameter header indicates that the message is a Request.
SCTP	Stream Control Transmission Protocol
SSC	Subscriber Certificate Procedure
Ua	UE-NAF interface for GAA applications
Ub	UE-BSF interface for bootstrapping
UE	User Equipment
USS	User Security Settings
XRES	Expected response in authentication
Zh	BSF-HSS interface for bootstrapping procedure
Zn	BSF-NAF interface for GAA applications.

4 GAA Bootstrapping Zh interface

4.1 Generic Bootstrapping Network Architecture

The network architecture of the Bootstrapping procedure is presented in Figure 4.1. The interface Ub (bootstrapping) is defined in 3GPP TS 24.109 [7] and the interface Zh in this specification.

Figure 4.1: Network architecture of bootstrapping procedure

The protocol stack of the Zh interface in Bootstrapping procedure is presented in Figure 4.2. The Diameter Base protocol is defined in [1] and the Diameter application in 3GPP TS 29.229 [3]. The requirements for Zh interface are defined in 3GPP TS 33.220 [5].

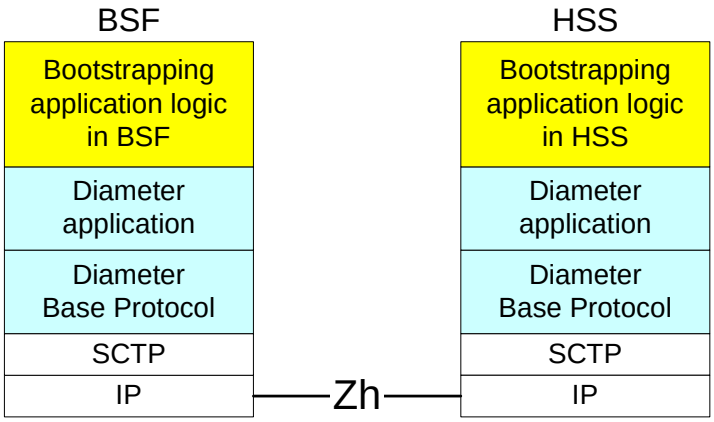


Figure 4.2: Protocol stack of Zh interface

4.2 Protocol Zh between BSF and HSS

The requirements for Zh interface are defined in 3GPP TS 33.220 [5].

The Bootstrapping Zh interface performs the retrieval of an authentication vector and GAA User Security Settings from the HSS. The overall Bootstrapping procedure is depicted in Figure 4.3. The basic procedure is:

A) A UE starts the bootstrapping procedure by protocol Ub with a BSF giving the IMPI of the user (see 3GPP TS 24.109 [7]).

B) The BSF starts protocol Zh with user's HSS

- The BSF requests user's authentication vector and GAA User Security Settings corresponding to the IMPI.
- The HSS supplies to the BSF the requested authentication vector and GAA-UserSecSettings.

C) The BSF continues the protocol Ub with the UE (see 3GPP TS 24.109 [7]).

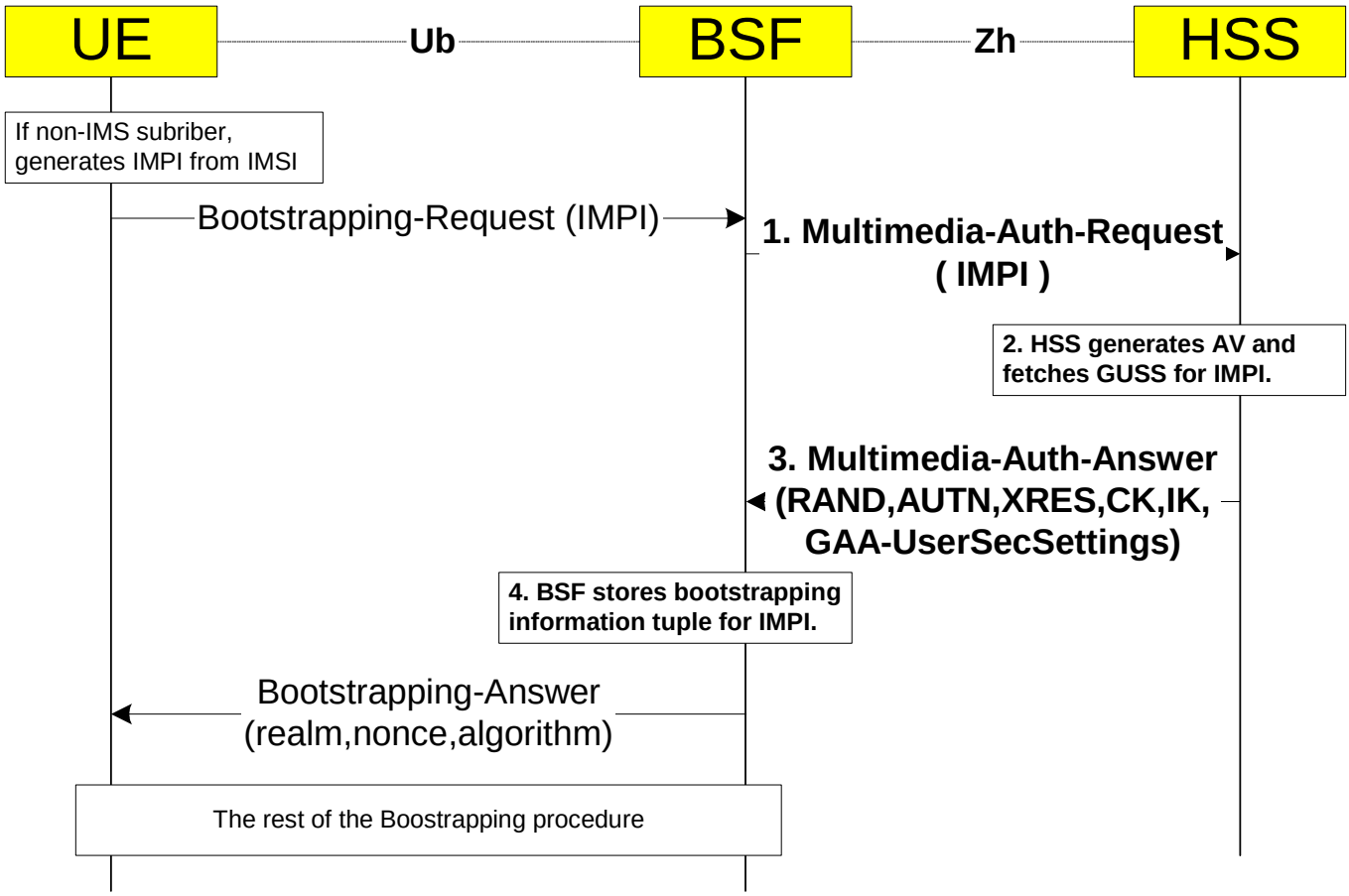


Figure 4.3: The GAA bootstrapping procedure

The steps of the bootstrapping procedure in Figure 4.3 are:

Step 1

The BSF shall send the following Bootstrapping-Request to the HSS in the format of Multimedia-Auth-Request (MAR) message. The content of the message is given below in the same format as in 3GPP TS 29.229 [3]. The curly brackets indicate mandatory AVPs. The square brackets indicate optional AVPs. The "address of" refers to the Fully Qualified Host Name (FQDN).

```
<Multimedia-Auth-Request> ::=<Diameter Header: 303, REQ >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                { Auth-Session-State }                  ; NO_STATE_MAINTAINED
                { Origin-Host }                         ; Address of BSF
                { Origin-Realm }                        ; Realm of BSF
                { Destination-Realm }                   ; Realm of HSS
                [ Destination-Host ]                    ; Address of the HSS
                { User-Name }                           ; IMPI from UE
                [ SIP-Number-Auth-Items]
                *[ AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
```

The content of mandatory Vendor-Specific-Application-ID according [1] is:

```
<Vendor-Specific-Application-Id>::=<AVP header: 260>
                1*  [Vendor-Id]                         ; 3GPP is 10415
                0*1 {Auth-Application-Id}               ; Zh Application id
                0*1 {Acct-Application-Id}               ; Omitted
```

When determining the value of Destination-Host AVP the BSF can use redirector function (SLF) to resolve the address of the HSS if needed (see 3GPP TS 29.229 [3]). The BSF shall set the Auth-Session-State AVP to NO_STATE_MAINTAINED to inform that the HSS does not need to maintain any status information for this session according 3GPP TS 29.229 [3]. The User-name is the IMS Private User Identity (IMPI) as required in 3GPP TS 29.228 [2]. The BSF shall set the number (zero or more) of the ordered authentication vectors to the SIP-Number-Auth-Items according 3GPP TS 29.229 [3].

Step 2

When the HSS receives the MAR message, the HSS shall derive the user Authentication Vectors (AV) information according the IMPI and populates it into SIP-Auth-Data AVP as defined in 3GPP TS 29.229 [3]. The HSS shall also fetch the GAA User Security Settings into the GAA-UserSecSettings.

The MAR/MAA sequence in the Zh interface must not change possible status information of the possible simultaneously ongoing IMS MM application sessions in the HSS.

If the User-Name (IMPI) from the BSF is totally unknown to the HSS, the error situation 5401 is raised. If the IMPI is known, but there is no valid GAA subscription in the HSS (i.e. no GAA-UserSecSettings data available), the error situation 5402 is raised.

Step 3.

The HSS shall send the following Bootstrapping-Answer message in the format of Multimedia-Auth-Answer (MAA) message back to the BSF.

```
< Multimedia-Auth-Answer> ::= < Diameter Header: 303 >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                [ Result-Code ]
                [ Experimental-Result]
                { Auth-Session-State }            ; NO_STATE_MAINTAINED
                { Origin-Host }                   ; Address of HSS
                { Origin-Realm }                  ; Realm of HSS
                [ User-Name ]                     ; IMPI
                [ SIP-Number-Auth-Items ]
                *[ SIP-Auth-Data-Item ]
                [ GAA-UserSecSettings ]           ; GUSS
                *[ AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
```

The HSS shall set the mandatory Auth-Session-State AVP to NO_STATE_MAINTAINED because the HSS does not maintain any state information about this session and the BSF does not need to send any session termination request 3GPP TS 29.229 [3]. The User-name AVP (IMPI) may be sent back for checking. The required authentication vectors are send in the SIP-Auth-Data-Items AVPs and the number of these items shall be set to the AVP SIP-Number-Auth-Items AVP. The security settings of user's all GAA applications are sent in GAA-UserSecSettings AVP.

Step 4.

When the BSF receives the MAA message, the BSF generates the key material (Ks) from confidential key (CK) and integrity key (IK) as described in 3GPP TS 33.220 [5] and stores temporarily the tuple <IMPI,Ks,GAA-UserSecSettings> for further use in GAA applications. The rest of the bootstrapping procedure in Ub interface will later add also the bootstrapping transaction Identifier (B-TID) to that tuple as key.

5 GAA Application Zn interface

5.1 Applications' network architecture

The network architecture of the GAA applications procedure is presented in Figure 5.1. The 3GPP GAA applications are listed in annex B. Different GAA applications may implement the Ua interface in different way. The Ua interface of the Subscriber Certificate application 3GPP TS 33.221 [6] is used here as an example. The Zn interface is defined in this specification.

Figure 5.1: Network architecture of GAA application

The protocol stack of the Zn interface for GAA applications (e.g. Subscriber Certificate) is presented in Figure 5.2. The diameter Base protocol is defined in [1] and the Diameter application in 3GPP TS 29.229 [3].

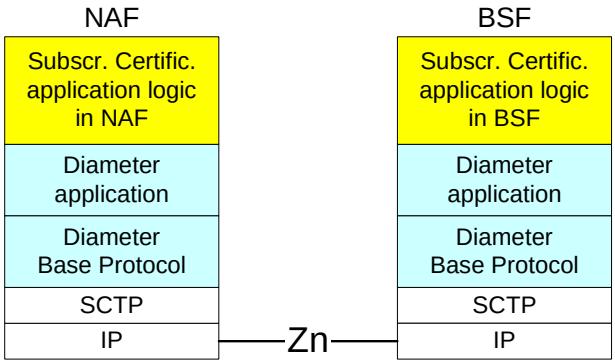


Figure 5.2: Protocol stack of Zn interface

5.2 Protocol Zn between NAF and BSF

The requirements for Zn interface are defined in 3GPP TS 33.220 [5].

The protocol Zn retrieves an authentication vector and user security settings data by NAF from BSF. After UE is authenticated with the BSF, every time the UE wants to interact with an NAF the following steps are executed as depicted in Figure 5.3. The basic procedure is:

A) The UE starts protocol Ua with the earlier bootstrapped NAF (see 3GPP TS 33.221 [6])

- In general, the UE and the NAF will not yet share the key(s) required to protect protocol Ua. If they already do, there is no need for the NAF to invoke protocol Zn.
- It is assumed that UE supplies sufficient information to NAF, e.g. a Bootstrapping Transaction Identifier (B-TID), to allow the NAF to retrieve specific key material (e.g. ME-Ks) from BSF.
- The UE derives the keys required to protect protocol Ua from the key material.

B) The NAF starts protocol Zn with BSF

- The NAF requests NAF specific key material corresponding to the information supplied by the UE to the NAF (e.g. a bootstrapping transaction identifier) in the start of protocol Ua.
- The BSF generates and supplies to the NAF the requested NAF specific key material and the appropriate User Security Settings defined for received application identifiers.
- The NAF derives the keys required to protect protocol Ua from the its key material in the same way as the UE did.

C) The NAF continues protocol Ua with the UE (see 3GPP TS 33.221 [6])

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

The common GAA application (e.g. Subscriber Certificate) procedure is presented in Figure 5.3.

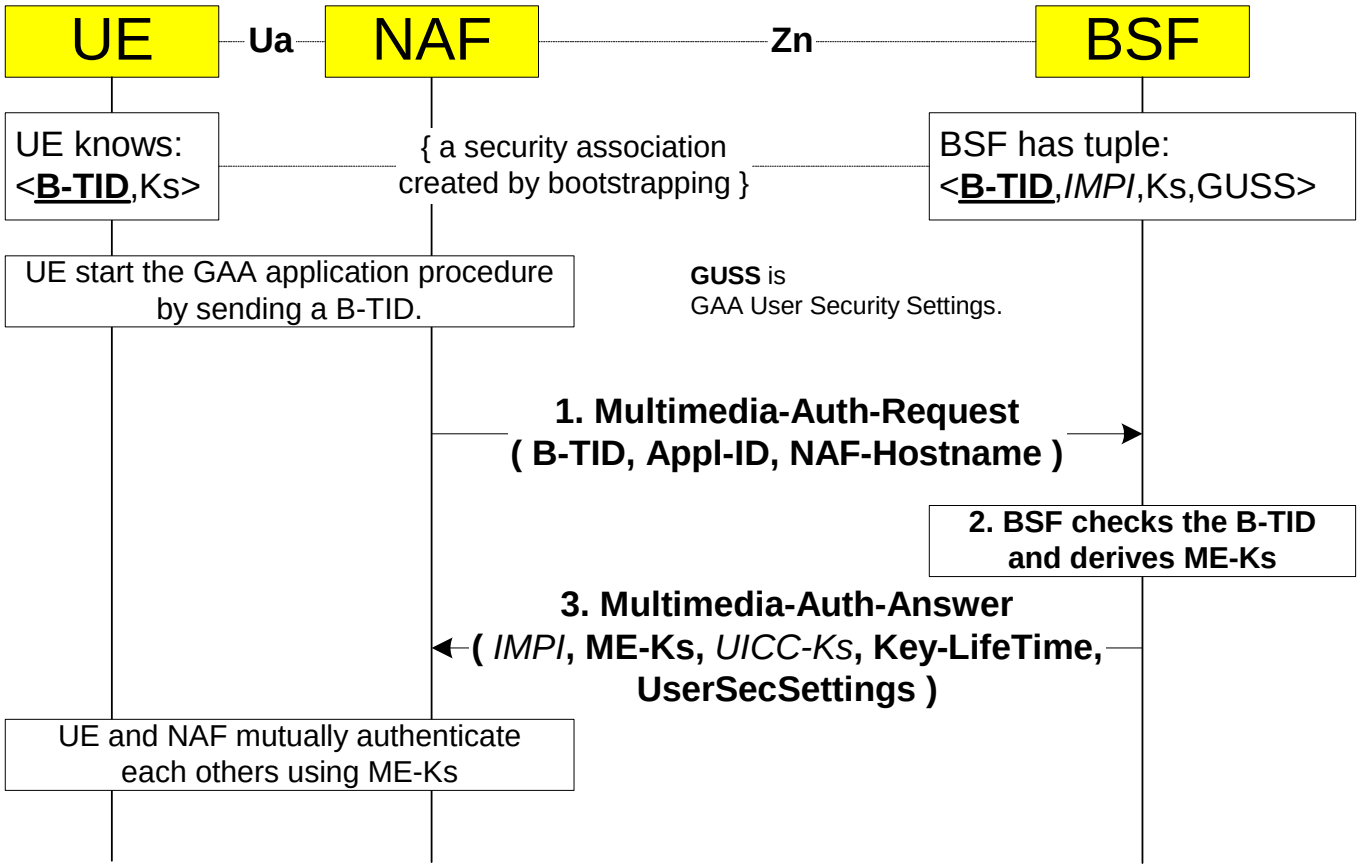


Figure 5.3: The GAA application procedure

The steps of the GAA application procedure in Figure 5.3 are:

Step 1

The NAF shall send a Bootstrapping-Info-Request message in the format of Multimedia-Auth-Request (MAR) message to the BSF. The content of the message is given here in the same format as in 3GPP TS 29.229 [3]. The curly brackets indicate mandatory AVPs. The square brackets indicate optional AVP. The address refers to the Fully Qualified Host Name (FQDN).

```
< Multimedia-Auth-Request> ::=<Diameter Header: 303, REQ >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                { Auth-Session-State }                    ; NO_STATE_MAINTAINED
                { Origin-Host }                           ; Address of NAF
                { Origin-Realm }                          ; Realm of NAF
                { Destination-Realm }                     ; Realm of BSF
                [ Destination-Host ]                      ; Address of the BSF

                * [ GAA-Service-Identifier ]              ; Application instance code
                { Transaction-Identifier }                ; B-TID
                { NAF-Hostname }                          ; FQDN of NAF as seen by UE
                *[ AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
```

The content of Vendor-Specific-Application-ID according [1] is:

```
<Vendor-Specific-Application-Id>::=<AVP header: 260>
                1*  [Vendor-Id]                           ; 3GPP is 10415
                0*1 {Auth-Application-Id}                 ; Zn Application id
                0*1 {Acct-Application-Id}                 ; Omitted
```

The Destination-Realm AVP is set to the NAF's default BSF. When determining the value of Destination-Host AVP in home network the NAF can use redirector function (SLF) to resolve the address of the BSF if needed (see 3GPP TS 29.229 [3]). The derivation of the Destination-Host in the visited network case is FSS in the later phases.

The NAF may set the Auth-Session-State AVP to NO_STATE_MAINTAINED to inform that the BSF does not need to maintain any status information for this session according 3GPP TS 29.229 [3].

The NAF indicates the GAA application instance for which the information is retrieved by GAA-Service-Identifier AVP. The Bootstrapping Transaction Identifier defines the earlier bootstrapping procedure execution.

Step 2

In the successful case the BSF has a tuple <B-TID,IMPI,Ks,GAA-UserSecSettings> identified by Bootstrapping Transaction Identifier (B-TID). When the BSF receives the request it checks the existence of the tuple for given B-TID. If checking fails the BSF sends an Answer message with Experimental-Result set to indicate the error type 5403. If the tuple for B-TID exists, but is expired, error type 5404 is send to indicate needs for renewal of the boostrapping procedure. In successful case the Result-Code is set to 2xxx as defined in [1].

The BSF derives the user authentication vector information according the B-TID and packs in into SIP-Auth-Data AVP defined in 3GPP TS 29.229 [3]. The BSF select correct user's Security Settings according the request's GAA-Service-Identifier AVP to GAA-UserSecSettings AVP. If the NAF has sent a GAA-Service-Identifier that does not have corresponding user's security settings, the error 5405 is raised.

If the NAF identified by its Origin-Host AVP is configured in the BSF not to be authorized to use the given NAF-Hostname, the BSF may raise the error situation 5407. The BSF may also be configured so that a certain NAF is not authorized to use a certain GAA-Service-Identifier. This situation may be indicated by error code 5406.

Step 3

After that the BSF shall send a Bootstrapping-Info-Answer message in the format of the following Multimedia-Auth-Answer (MAA) message back to the NAF.

```
< Multimedia-Auth-Answer> ::= < Diameter Header: 303 >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                [ Result-Code ]
                [ Experimental-Result]
                { Auth-Session-State }            ; NO_STATE_MAINTAINED
                { Origin-Host }                   ; Address of BSF
                { Origin-Realm }                  ; Realm of BSF
                [ User-Name ]                     ; IMPI
                [ ME-Key-Material ]               ; Required
                [ UICC-Key-Material ]             ; Application Type conditional
                [ Key-LifeTime ]                  ; In seconds
                [ GAA-UserSecSettings ]           ; Selected  USSs
                *[ AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
```

The BSF should set the mandatory Auth-Session-State AVP to NO_STATE_MAINTAINED to inform that the BSF does not require the NAF to maintain any status information. The BSF may or may not send the User-name AVP (IMPI) according its configuration. The mandatory common key material with the ME (ME-Ks) is sent in the ME-Key-Material AVP. The common key material with the UICC (UICC-Ks) is optionally sent in the UICC-Key-Material AVP only if the GAA application type specific information received from Ub during the bootstrapping procedure enables its generation. The Key-LifeTime AVP contains the expiry time of the Bootsrapping information in the BSF according its configuration. The expiry time is represented in seconds that have passed since January 1, 1970 00:00:00.000 GMT. The BSF select the appropriate User Security Settings to the GAA-UserSecSettings AVP from stored GAA-UserSecSettings in Bootstrapping information according the GAA-Service-Identifier AVPs in the request message.

The procedure in the NAF when the MAA is received is described in GAA application type specific TSs.

6 Diameter application for Zh and Zn interfaces

6.1 Command-Code values

The Zh and Zn interfaces do not assign new Command-Codes.

The messages in Zh and Zn interfaces use the same Command-Code value 303 as Multimedia-Auth-Request/Answer messages defined in 3GPP TS 29.229 [3] for Cx interface.

6.2 Result-Code AVP values

This section defines new result code values that must be supported by all Diameter implementations that conform to this specification. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and Result-Code AVP shall be absent.

6.2.1 Success

Errors that fall within the Success category are used to inform a peer that a request has been successfully completed.

The success category result codes defined in 3GPP TS 29.229 [3] for Cx interface are useless and therefore not required in Zh and Zn interfaces.

6.2.2 Permanent Failures

Errors that fall within the Permanent Failures category are used to inform the peer that the request failed, and should not be attempted again.

The Permanent failure category result codes defined in 3GPP TS 29.229 [3] for Cx interface are useless and therefore not required in Zh and Zn interfaces.

6.2.2.1 DIAMETER_ERROR_IMPI_UNKNOWN (5401)

A message was received by the HSS for an IMPI that is unknown.

6.2.2.2 DIAMETER_ERROR_GUSS_UNKNOWN (5402)

A message was received by the HSS for an IMPI that does not have GAA subscription i.e. no GAA-UserSecSettings in the HSS.

6.2.2.3 DIAMETER_ERROR_TRANSACTION_IDENTIFIER_UNKNOWN (5403)

A message was received by the BSF for an unknown Bootstrapping Transaction Identifier (B-TID).

6.2.2.4 DIAMETER_ERROR_TRANSACTION_IDENTIFIER_EXPIRED (5404)

A message was received by the BSF for a Bootstrapping Transaction Identifier (B-TID) that is already expired.

6.2.2.5 DIAMETER_ERROR_APPLICATION_ID_UNKNOWN (5405)

A message was received by the BSF for Application Identifier that is unknown i.e. it does not have any binding to an USS belonging to the received B-TID.

6.2.2.6 DIAMETER_ERROR_SERVICE_ID_NOT_AUTHORIZED (5406)

A message was received by the BSF with an Service Identifier identifying an USS that the NAF is not authorized to receive.

6.2.2.7 DIAMETER_ERROR_HOSTNAME_NOT_AUTHORIZED (5407)

A message was received by the BSF from a NAF with NAF-Hostname that is not authorized to be used by the NAF.

6.3 AVPs

The AVPs defined in 3GPP TS 29.229 [3] for 3GPP IMS Cx interface Multimedia-Auth-Request/Answer messages are used as they are.

The following table describes the additional new Diameter AVPs defined for the Zh and Zn interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

Table 6.1: New Diameter Multimedia Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
GAA-UserSecSettings	400	6.3.1.1	OctedString	M, V				No
Transaction-Identifier	401	6.3.1.2	OctetString	M, V				No
NAF-Hostname	402	6.3.1.3	OctetString	M, V				No
GAA-Service-Identifier	403	6.3.1.4	OctedString	M, V				No
Key-LifeTime	404	6.3.1.5	Unsigned 32	M, V				No
ME-Key-Material	405	6.3.1.6	OctedString	M, V				No
UICC-Key-Material	406	6.3.1.7	OctedString	M, V				No
NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header.								

6.3.1 Common AVPs

6.3.1.1 GAA-UserSecSettings AVP

The GAA-UserSecSettings AVP (AVP code 400) is of type OctetString. This AVP contains a set of user security settings. The content of GAA-UserSecSettings AVP is a XML document which is defined in annex A.

6.3.1.2 Transaction-Identifier AVP

The Transaction-Identifier AVP (AVP code 401) is of type OctetString. This AVP contains the Bootstrapping Transcation Identifier (B-TID).

6.3.1.3 NAF-Hostname

The NAF-Hostname AVP (AVP code 402) is of type OctetString. This AVP contains the full qualified domain name (FQDN) of the NAF that the UE uses. This may be a different domain name that with which the BSF knows the NAF.

6.3.1.4 GAA-Service-Identifier AVP

The GAA-Service-identifier AVP (AVP code 403) is of type OctedString. This AVP informs a BSF which NAF operator specific instance of the GAA application sends the request message. According this AVP the BSF can select the right application's user security settings.

6.3.1.5 Key-LifeTime AVP

The Key-LifeTime AVP (AVP code 404) is of type Unsigned32. This AVP informs the NAF about the expiry time of the key. The expiry time is represented in seconds that have passed since January 1, 1970 00:00:00.000 GMT.

6.3.1.6 ME-Key-Material AVP

The required ME-Key-Material AVP (AVP code 405) is of type OctetString. The BSF is sharing this key material with the Mobile Equipment (ME).

6.3.1.7 UICC-Key-Material AVP

The condition UICC-Key-Material AVP (AVP code 406) is of type OctetString. The BSF may share this key material with a security element (e.g. USIM, ISIM, etc..) in the UICC. Only some GAA applications use this conditional AVP.

7 Use of namespaces

This clause contains the namespaces that have either been created in this 3GPP specification, or in 3GPP specification 3GPP TS 29.229 [3] or the values assigned to existing namespaces managed by IANA.

7.1 AVP codes

This specification reserves the 3GPP vendor specific values 10415:400-499 and actually assign values 10415:400-406 for the GAA from the 3GPP AVP Code namespace for 3GPP Diameter applications ([8]). The 3GPP vendor specific AVP code space is managed by 3GPP CN4. See section 6 for the assignment of the namespace in this specification.

Besides the Diameter Base Protocol AVPs [1] this specification reuses the following AVPs from 3GPP TS 29.229 [3]: `Authentication-Session-State, User-Name`, `SIP-Auth-Data-Item` and `SIP-Number-Auth-Items`.

7.2 Experimental-Result-Code AVP values

This specification reserves Experimental-Result-Code AVP values 10415:2401-2409 and 10415:5401-5409. See section 6.2.

7.3 Command Code values

Only Command-Code 303 from 3GPP TS 29.229 [3] is used in this specification. The same Commnad-Code value 303 is used in both Zh and Zn messages.

This specification reuses only the Command-Code value, not the content of the original specification. The AVPs, that are defined required in TS 29.229 [3], but are not needed in Zh or Zn interfaces, are removed and are therefore not required in Zh or Zn interface messages. All new AVPs for GAA are defined optional although they may be mandatory in GAA viewpoint.

This specification does not assign new command codes to the 3GPP TS 29.229 [3].

Editor's note:
Currently IANA has accepted the Command-Code 303 for Multimedia-Auth-Request/Answer for version 5. According [9] the coding may be different for version 6.

Annex A (normative): GAA-UserSecSettings XML definition

This annex contains the XML schema definition for an XML document carrying the GAA User Security Settings inside GAA-UserSecSettings AVP in Zh interface.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="guss-schema-of-3gpp-gaa"
    xmlns:tns="guss-schema-of-3gpp-gaa"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <!-- This import brings in the XML language attribute xml:lang-->
  <xs:import namespace="http://www.w3.org/XML/1998/namespace"
      schemaLocation="http://www.w3.org/2001/xml.xsd"/>

  <!—- The whole user’s GAA spcific data set  -->
  <xs:complexType name=“guss”>
    <xs:sequence>
       <xs:element ref=“ussList”/>
    </xs:sequence>
    <xs:attribute name=“id” type=“xs:string”/>
  </xs:complexType>

  <!—-List of all users individual User Security Settings -->
  <xs:complexType name=“ussList”>
    <xs:sequence minOccurs=“0” maxOccurs=“unbounded”>
       <xs:element ref=“uss”/>
    </xs:sequence>
  </xs:complexType>

  <!—- User Security Setting data -->
  <xs:complexType name=“uss”>
    <xs:sequence>
      <xs:element ref=“uids”/>
      <xs:element name=“flags”/>
    </xs:sequence>
    <xs:attribute name=“id”   use=“required” type=“xs:string”/>
    <xs:attribute name=“type” use=“required” type=“xs:int”/>
  </xs:complexType>

  <!—- User Public Identities for authentication -->
  <xs:complexType name=“uids”>
    <xs:sequence minOccurs=“1” maxOccurs=“unbounded”>
      <xs:element name=“uid”  type=“xs:string”/>
    </xs:sequence>
  </xs:complexType>

  <!—- GAA Application type specific Authorization flag codes -->
  <xs:complexType name=“flags”>
    <xs:sequence minOccurs=“0” maxOccurs=“unbounded”>
      <xs:element name=“flag”  type=“xs:int”/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
```

The values are:

- The value of the attribute "id" in the element "guss" is the the same as user's IM Private Identity (IMPI) used in User-Name AVP.
- The value of the attribute "id" in the element "uss" is the same as service identifier (GSID) used in GAA-Service-Identifier AVP.
- The value of attribute "type" in the element "uss" is GAA application type code defined in annex B.
- Values of the element "uid" are user's public authentication identities from the HSS.
- Values of element "flag" are user's authorization flag codes from the HSS for GAA application type indicated in the type attribute in the parent uss element. If an authorization flag exist the NAF have permission to give the corresponding service, otherwise not

In the following illustrative example the values are italised and underlined. The content of one User Security Setting tag is boxed.

```
<guss id="358500004836551@ims.mnc050.mcc358.3gppnetwork.org">
     <ussList>
          <uss id="1234567890" type="1">
               <uids>
                    <uid>tel:358504836551</uid>
                    <uid>lauri.laitinen@nokia.com</uid>
                    …
               <uids>
               <flags>
                    <flag>1</flag>
                    …
               <flags>
          </uss>
          …
     </ussList>
</guss>
```

The above GAA User Security Settings example for user "358500004836551@ ims.mnc050.mcc358.3gppnetwork.org" defines that for PKI-Portal (GAA application type code is 1) services are allowed for user identities "tel:358504836551" and "lauri.laitinen@nokia.com" and authentication is allowed (flag 1 exists) but non-repudiation is not allowed (flag 2 is missing) to NAFs that provide the GAA service identified by "1234567890" GAA Service Identifier.

Annex B (normative): GAA Application type codes

The GAA Application Type code values are used in GAA to indicate interpretation, coding and usage of GAA application type specific data.

For examples each GAA application type may have their own set of authorization flags which meaning and coding is defined in their application type specific specification. There may also be proprietary GAA application types with their own definitions in the future.

Code values 0 – 999999 are reserved for standardized GAA application types.

The following values are defined for standardized GAA application types with 3GPP specification:

0 Unspecific application
1 PKI-Portal
2 Authentication Proxy
3 Presence
4 MBMS

Default value is 0. An unspecific application may or may not have user security settings containing or not a list of public identities. An unspecific application cannot have specified authorization flags or other application type specific data.

Annex C (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2003-10					*First Draft TS created*		*0.0.0*
2003-10					*Version after CN4#21*	*0.0.0*	*0.1.0*
2004-02					*Version after CN4#22*	*0.1.0*	*0.2.0*
2004-05					*Version after CN4#23*	*0.2.0*	*0.3.0*
2004-06	CN#24	NP-040231			Version 1.0.0 for information	0.3.0	1.0.0
2004-08					Version at CN4#24	1.0.0	1.1.0
2004-08	CN#25	NP-040410			Approved in CN4#24 and sent to CN#25 for approval	1.1.0	2.0.0