3GPP TSG CN Plenary Meeting #26 **NP-040xxx**
8th – 10th December 2004 Athens, Greece.

Source: TSG CN WG4

Title: Corrections on Subscriber certificates

Agenda item: 9.3

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level N4-040	Phase	Subject	Cat	Ver_C
29.109	001		1316	Rel-6	Authorization Flag Code Annex	B	6.0.0
29.109	002		1317	Rel-6	Finalization of GAA Service Identifier	B	6.0.0
29.109	005		1320	Rel-6	Structure to GAA Service Indentifier	B	6.0.0
23.008	140		1324	Rel-6	Correction to authorization flag definition	F	6.3.0
29.109	009		1500	Rel-6	Introduction of NAF groups	B	6.0.0
29.109	003	1	1609	Rel-6	BSF control information (bsfInfo) tag to GUSS	B	6.0.0
29.109	006	1	1610	Rel-6	Finalisation of terminology	F	6.0.0
23.008	138	1	1612	Rel-6	Domain independent GAA	F	6.3.0
23.003	096	1	1613	Rel-6	BSF address	F	6.4.0
29.109	008	1	1614	Rel-6	Command code 310 Zn messages	B	6.0.0
29.230	007	1	1615	Rel-6	Reservation of command code 310	F	6.1.0
23.008	141		1616	Rel-6	Introduction of NAF Groups	F	6.3.0

3GPP TSG-CN WG4 Meeting #25 ***N4-041316***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **001** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Authorization Flag Code Annex
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-05
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	There is no guarantee that stage 3 specifications of the standardised GAA services contain also lists of used flag codes or even that stage 3 specifications even exist. Therefore the service specific authorization flag codes should be summarized in normative manner in an annex of TS 29.109.
Summary of change:	⌘	The list of all known agreed standardized authorization flag codes is added as a new annex.
Consequences if not approved:	⌘	Missing definition of authorization flag codes for standardized GAA services.

Clauses affected:	⌘	Annex B, Annex C (new)

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

Other comments: ⌘

****** BEGIN CHANGE ******

Annex B (normative): GAA ~~Application~~Service ~~type codes~~

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

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

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

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

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

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

Annex C (normative): GAA Authorization flag codes

For GAA services which have a defined set of special authorization flag codes the following rule holds: The service specified by the GAA authorization flag codes is allowed for a user only if user's user security setting contains that flag.

The following standardised GAA service types that are listed in previous annex B have the following special authorization flag codes:

PKI Portal (1)

2Authentication allowed

3Non-repudiation allowed

Annex DC (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-09	CN#25	NP-040410			Version 2.0.0 approved in CN#25	2.0.0	6.0.0

****** END CHANGE ******

3GPP TSG-CN WG4 Meeting #25 ***N4-041317***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **002** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Finalization of GAA Service Identifier
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-05
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	CN4#24 improved the GAA terminology by introducing the term: GAA Service Identifier. This improvement was introduced in the current version of TS 29.109, but not everywhere. This CR will introduce the term to everywhere.
Summary of change:	⌘	The GAA Application Identifier and corresponding abbreviations are replaced consistently by GAA Service Identifier (GSID).
Consequences if not approved:	⌘	Inconsistency in terminology in TS 29.109.

Clauses affected:	⌘	1, 3.1, 3.3, 5.2, 6.3.1.4

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

Other comments:	⌘	

***** BEGIN CHANGE *****

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.

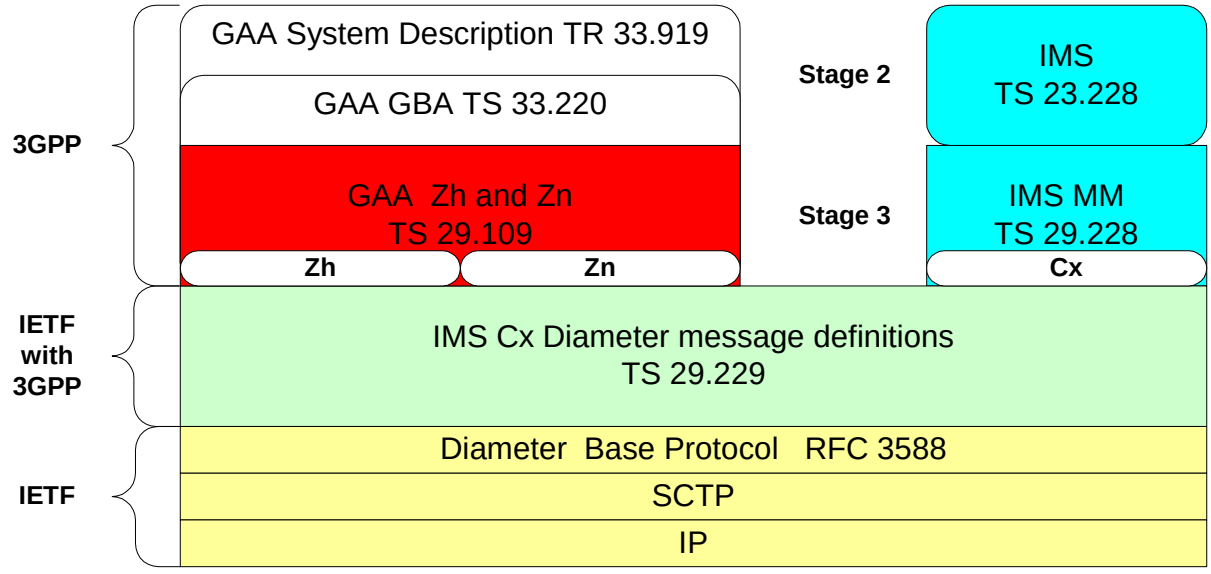
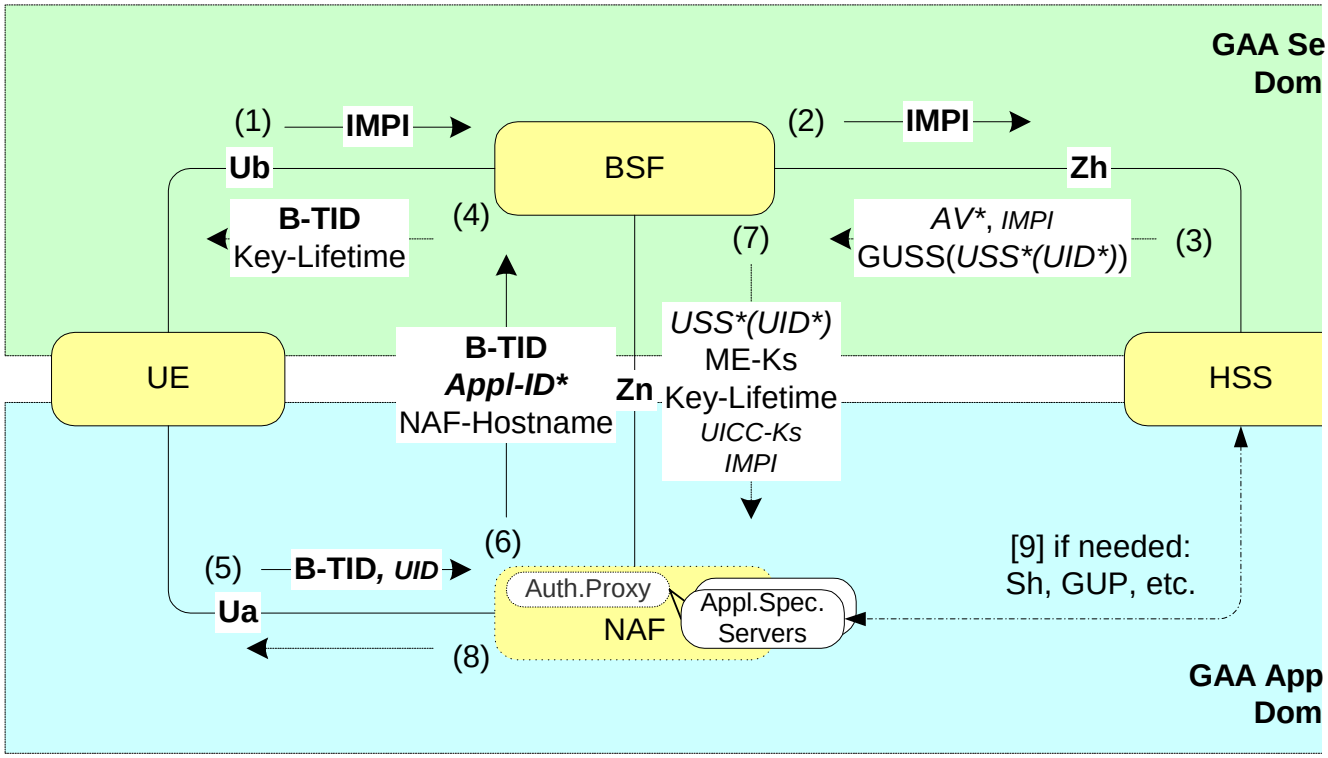
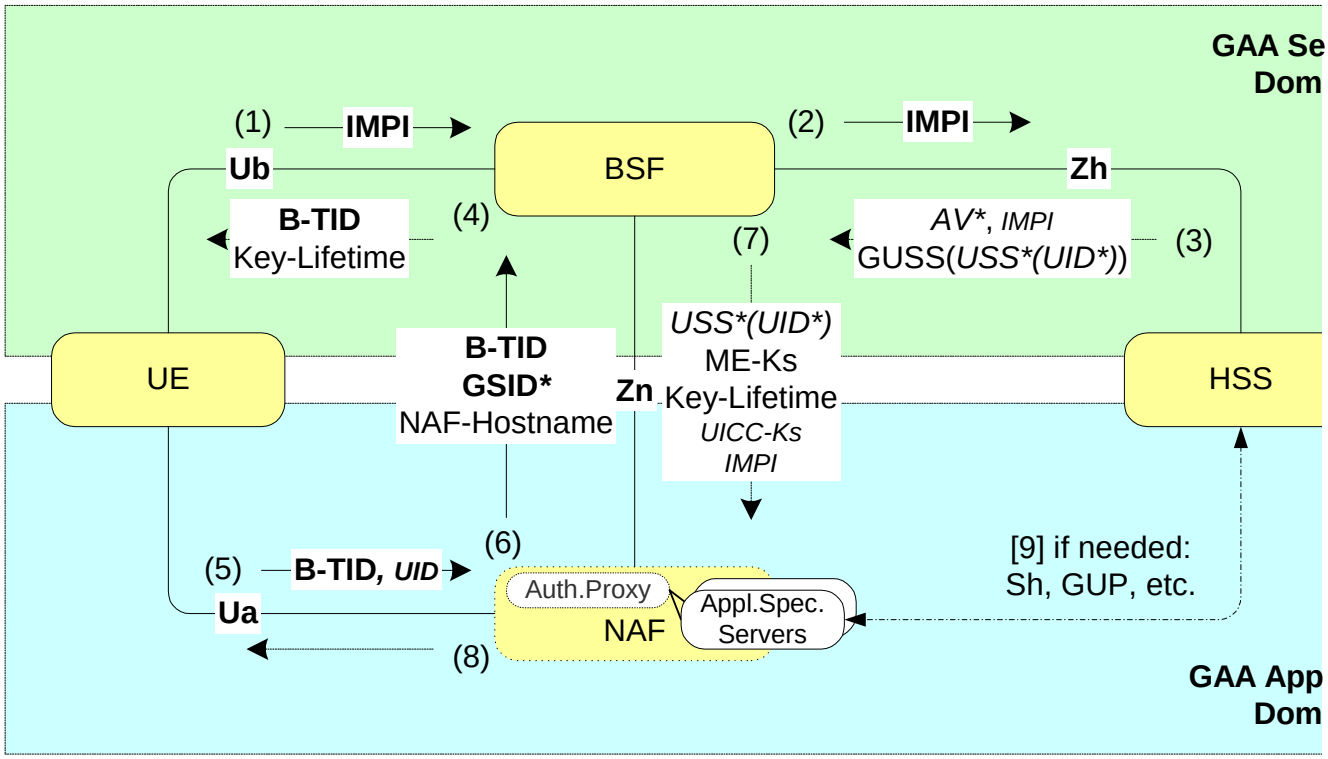


Figure 1.1: Relationships to other specifications

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.



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

~~**Figure 1.2: The whole signalling procedure in GAA system**~~

~~*** BEGIN NEXT CHANGE *****~~**

~~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.~~

~~**GAA service** is an operator specific end user service that uses the security association created by GAA Bootstrapping procedure. GAA services are identified by **GAA Service Identifiers**. A GAA service is implemented using some standardised or propriatary GAA application defined by GAA application type.~~

~~**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.~~

~~*** BEGIN NEXT CHANGE *****~~**

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
GSID	GAA Service Identifier
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.

~~*** BEGIN NEXT CHANGE *****~~**

~~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])~~

~~2In 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.~~

~~3It 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.~~

~~4The UE derives the keys required to protect protocol Ua from the key material.~~

~~B) The NAF starts protocol Zn with BSF~~

~~2The 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.~~

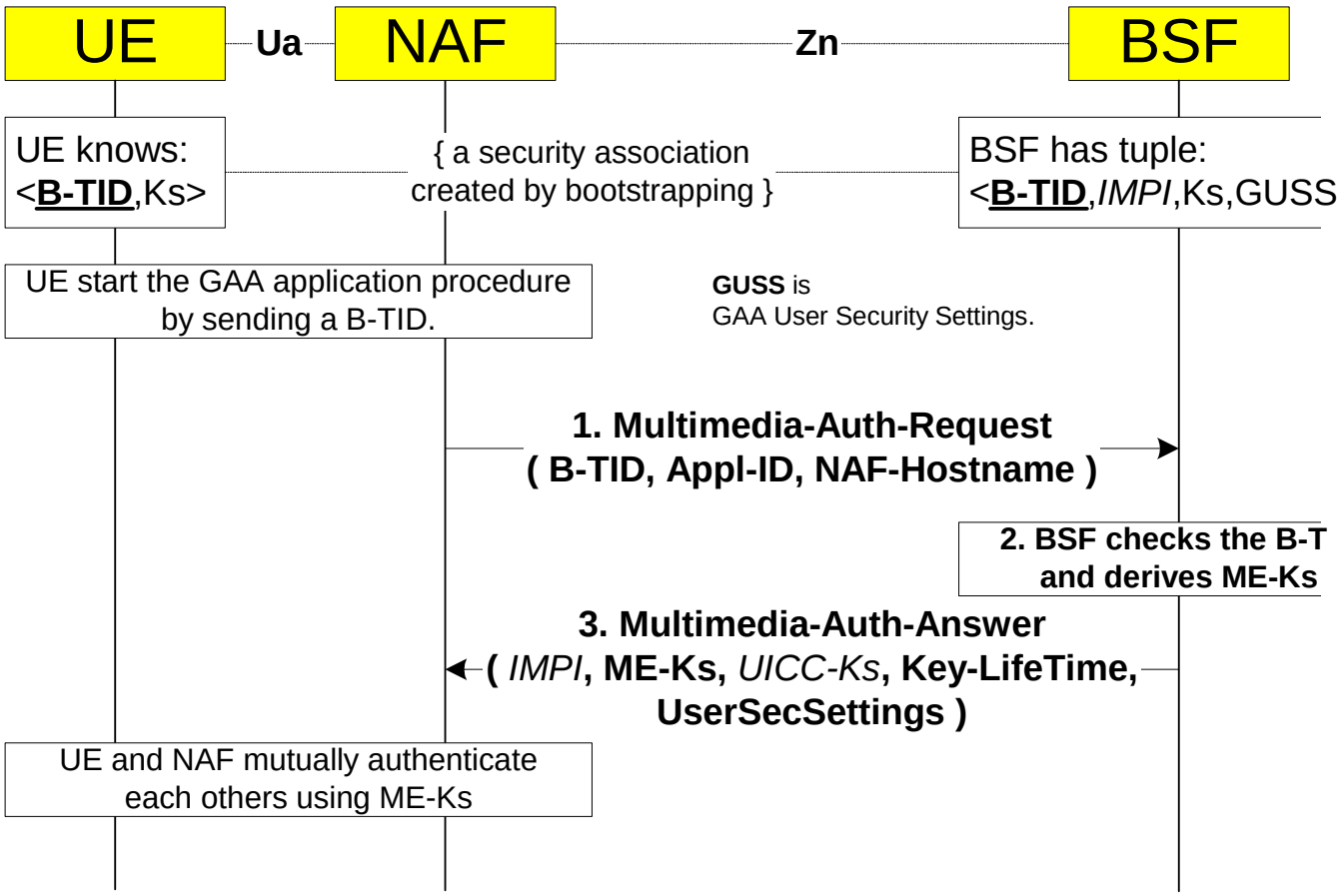
~~3The BSF generates and supplies to the NAF the requested NAF specific key material and the appropriate User Security Settings defined for received application identifiers.~~

~~4The 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.~~


UE
Ua
NAF
Zn
BSF
UE knows:
<B-TID,Ks>
{ a security association
created by bootstrapping }
BSF has tuple:
<B-TID,IMPI,Ks,GUSS
UE start the GAA application procedure
by sending a B-TID.
GUSS is
GAA User Security Settings.
1. Multimedia-Auth-Request
(B-TID, Appl-ID, NAF-Hostname)
2. BSF checks the B-T
and derives ME-Ks
3. Multimedia-Auth-Answer
(IMPI, ME-Ks, UICC-Ks, Key-LifeTime,
UserSecSettings)
UE and NAF mutually authenticate
each others using ME-Ks

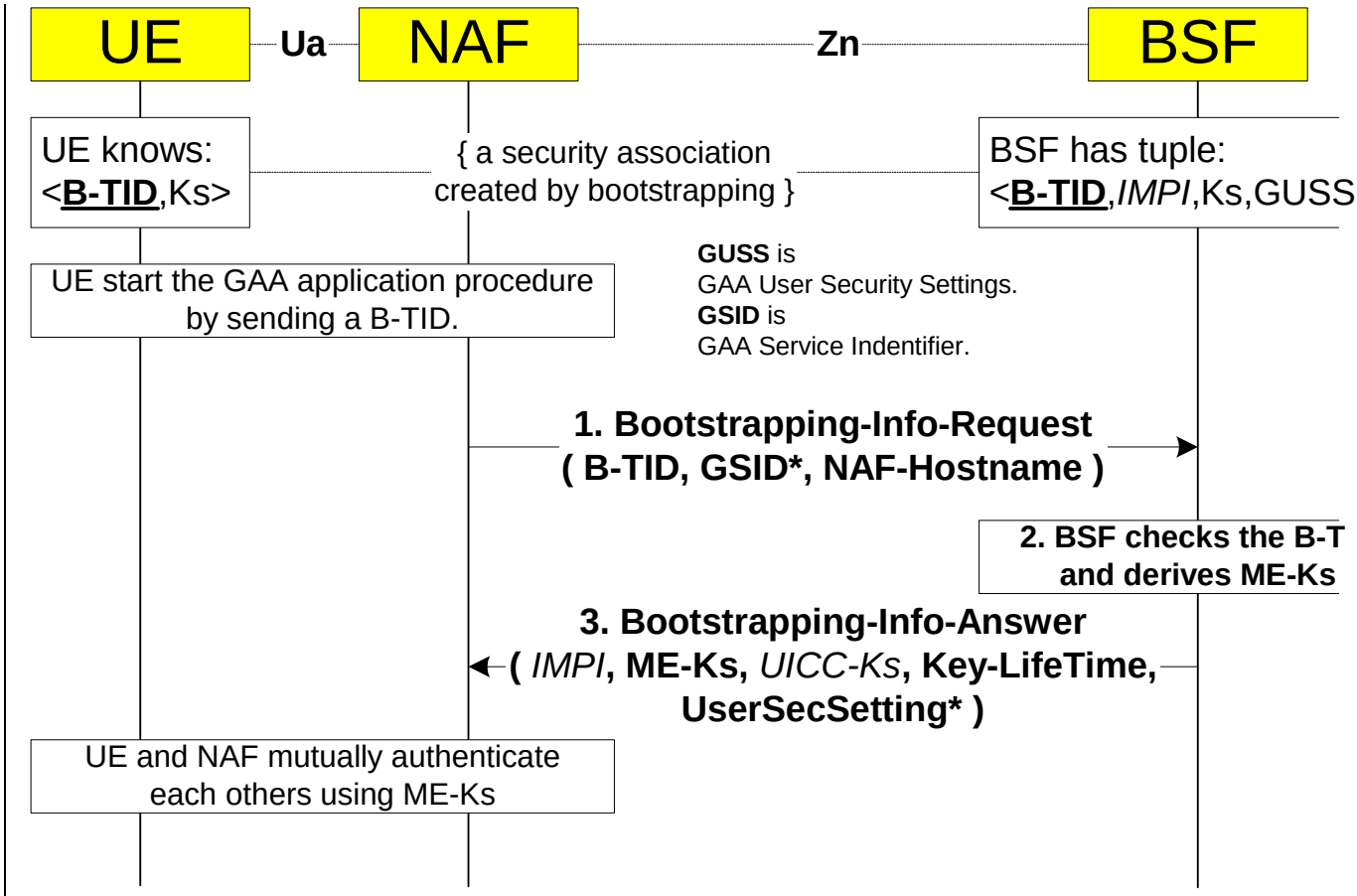


Figure 5.3: The GAA application procedure

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] ; Service
identifiersApplication 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 instanceservices for which the information is retrieved by GAA-Service-Identifier AVPs. 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.

******* BEGIN NEXT CHANGE *******

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 serviceapplication's user security settings.

******* END CHANGE *******

3GPP TSG-CN WG4 Meeting #25 ***N4-041320***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **005** ⌘ **rev** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Structure to GAA Service Indentifier
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-04
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	TS 33.220 (subclause 4.2.3) requires that: "GBA USS shall be defined in such a way that interworking of different operators for standardised application profiles is possible". This CR implements the necessary changes in TS 29.109. The standardisation of internal structure and formation of GAA Service Identifier enables NAFs to predict its GAA service identifier in arbitrary user's home HSS without bookkeeping of service identifiers in every possible home domain. The proposed internal GSID structure informs as a side effect automatically to the HSS the service's GAA application type, which may be needed in the future extension.
Summary of change:	⌘	A standard internal structure for GAA-Service-Identifier is proposed.
Consequences if not approved:	⌘	GAA Service identifiers are arbitrary strings without any utilisable structure. A service operator needs individual agreements, bookkeeping and configuration for service identifiers with each possible home operators.

Clauses affected:	⌘	6.3.1.4, Annex A
Other specs	⌘	Y ☐ N ☒ Other core specifications ⌘ -

affected:		
	X	Test specifications
	X	O&M Specifications
Other comments:	⌘	

****** BEGIN CHANGE ******

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.

For 3GPP standardized services (e.g., PKI portal), the GAA-Service-Identifier (GSID) shall be in the range 0 to 999999, and the currently standardized values for GSID shall be the GAA-Application-Type-Code of the particular service. The GAA-Application-Type-Codes for 3GPP standardized services are defined in Annex B.

NOTE: In the future, standardized GSID values that are different than the GAA-Application-Type-Code may be standardised (e.g. to differentiate between the services "MBMS streaming" and "MBMS download").

Examples: The GSID is "1" for all PKI-portals, and "4" for all MBMS services.

******* BEGIN NEXT CHANGE *******

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:

1. 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.

2. The value of the attribute “id” in the element “uss” is the same as service identifier (GSID) used in GAA-Service-Identifier AVP.

3. The value of attribute “type” in the element “uss” is GAA application type code defined in annex B.

4. Values of the element “uid” are user’s public authentication identities from the HSS.

5. 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="11234567890" 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 "11234567890" GAA Service Identifier.

****** END CHANGE ******

3GPP TSG-CN WG4 Meeting #25 ***N4-041324***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.008** **CR** **140** ⌘ **rev** **-** ⌘ Current version: **6.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction to authorization flag definition
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-05
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	CN4#24 accepted the application type code as attribute to XML uss flag. The consequence of this is that each application type has properly its own coding space for authorization flag codes. CN4#24 also implemented this in TS 29.109. This CR implements it also to TS 23.008.
Summary of change:	⌘	The structure of authorization flags is simplified.
Consequences if not approved:	⌘	Incompatibility with TS 29.109.

Clauses affected:	⌘	3.9.5

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

Other comments: ⌘

****** BEGIN CHANGE ******

3.9.5 GAA Authorization flag

The GAA Authorization flag is a GAA Service~~Application type specific integer code, which authorizes a defined security operation in the GAA serviceapplication. A list of allowed operations is stored for each GAA Service Subscription.~~

~~The values of the authorization flags for each application type using them are listed in TS 29.109 [59]~~

~~The GAA Authorization flag is concatenated from GAA Application Type code and GAA Application Type specific operation code in range 00-99. The value of a GAA Authorization flag is a sum of 100*(GAA Application Type Code)+(GAA Application Type specific operation code). The values of GAA Authorization flags operation code can be therefore specified separately for each GAA application in their specifications.~~

~~The Authorization Flag is permanent subscriber data and is stored in the HSS, BSF and NAF.~~

~~** END CHANGE ****~~**

3GPP TSG-CN WG4 Meeting #25 ***N4-041500***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **009** ⌘ **rev** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Introduction of NAF groups
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-05
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The MNO may have a need to supply different USSs to NAFs for the same service, dependent on particular NAF, e.g. if located in home or visited network. This distinction is an operator internal decision and may be different from operator to operator for the same NAF. Thus this distinction should not be reflected in GAA service identifier (it is still the same service in the different networks), but by other, operator internal means.
Summary of change:	⌘	NAF grouping for better controllability of GBA usage is introduced.
Consequences if not approved:	⌘	Difficult handling of varying access controls on GBA usage.

Clauses affected:	⌘	5.2, annex A

Other specs affected: ⌘	Y	N			
	X		Other core specifications	⌘	33.220-020
		X	Test specifications		
		X	O&M Specifications		

Other comments: ⌘

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])

1 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.

2 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.

3 The UE derives the keys required to protect protocol Ua from the key material.

B) The NAF starts protocol Zn with BSF

1 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.

2 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.

3 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.

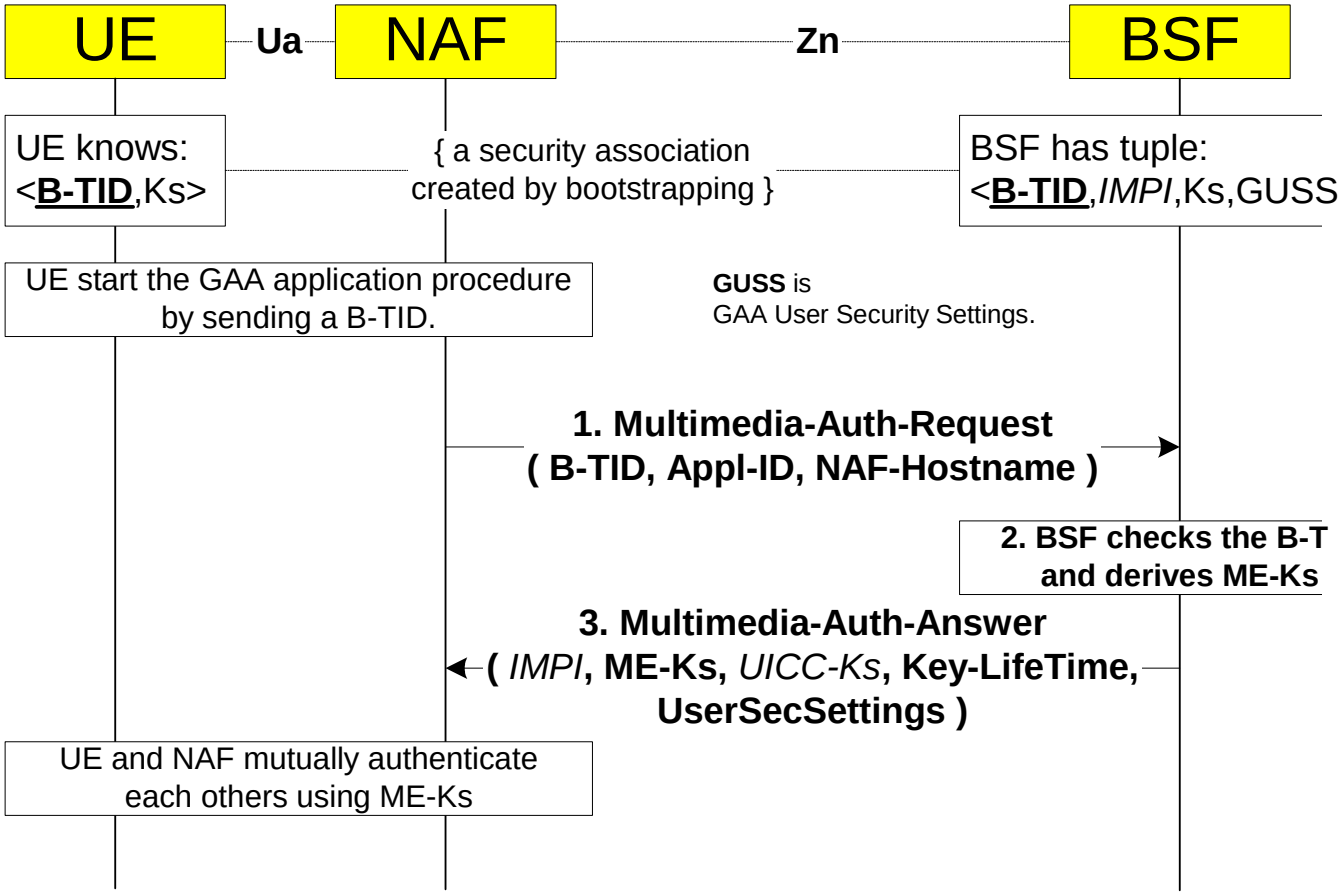


Figure 5.3: The GAA application procedure

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 NAF grouping is used by the operator and there are one or more USSs corresponding to the requested GSID, then also the nafGroup attribute of USS is checked. 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.

********** **begin next change** **********

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:attribute name="nafGroup" use="optional" type="xs:string"/>
  </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:

1 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.

2 The value of the attribute “id” in the element “uss” is the same as service identifier (GSID) used in GAA-Service-Identifier AVP.

3 The value of attribute “type” in the element “uss” is GAA application type code defined in annex B.

4 The value of attribute “nafGroup” in the element “uss” is an operator internal group designator for a NAF group the USS is valid for. If this attribute is missing then only the attribute “id” is used for selection of this element.

5 Values of the element “uid” are user’s public authentication identities from the HSS.

6 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.

3GPP TSG-CN WG4 Meeting #25 ***N4-041609***
Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **003** ⌘**rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	BSF control information (bsfInfo) tag to GUSS
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-17
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The SA3#35 agreed Discussion paper S3-040741 and CR S3-040832 concerning addition of bsfInfo information to the GUSS. This CR implements this addition also to TS 29.109.
Summary of change:	⌘	A new tag (bsfInfo) is added to GUSS XML schema to guide the BSF. The bsfInfo tag is basically a parent tag for several BSF control information sub tags. Currently two sub tags are defined (see S3-040832 ch. 4.2.3 requirement). A uiccType sub tag is needed for control of UICC_Ks generation and a lifeTime tag is needed to set a special key lifetime other than given in BSF configuration.
Consequences if not approved:	⌘	TS 29.109 does not fulfill the requirement of TS 33.220 from SA3.

Clauses affected:	⌘	5.2, Annex A

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

Other comments: ⌘

****** BEGIN CHANGE ******

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])

1 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.

2 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.

3 The UE derives the keys required to protect protocol Ua from the key material.

B) The NAF starts protocol Zn with BSF

1 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.

2 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.

3 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.

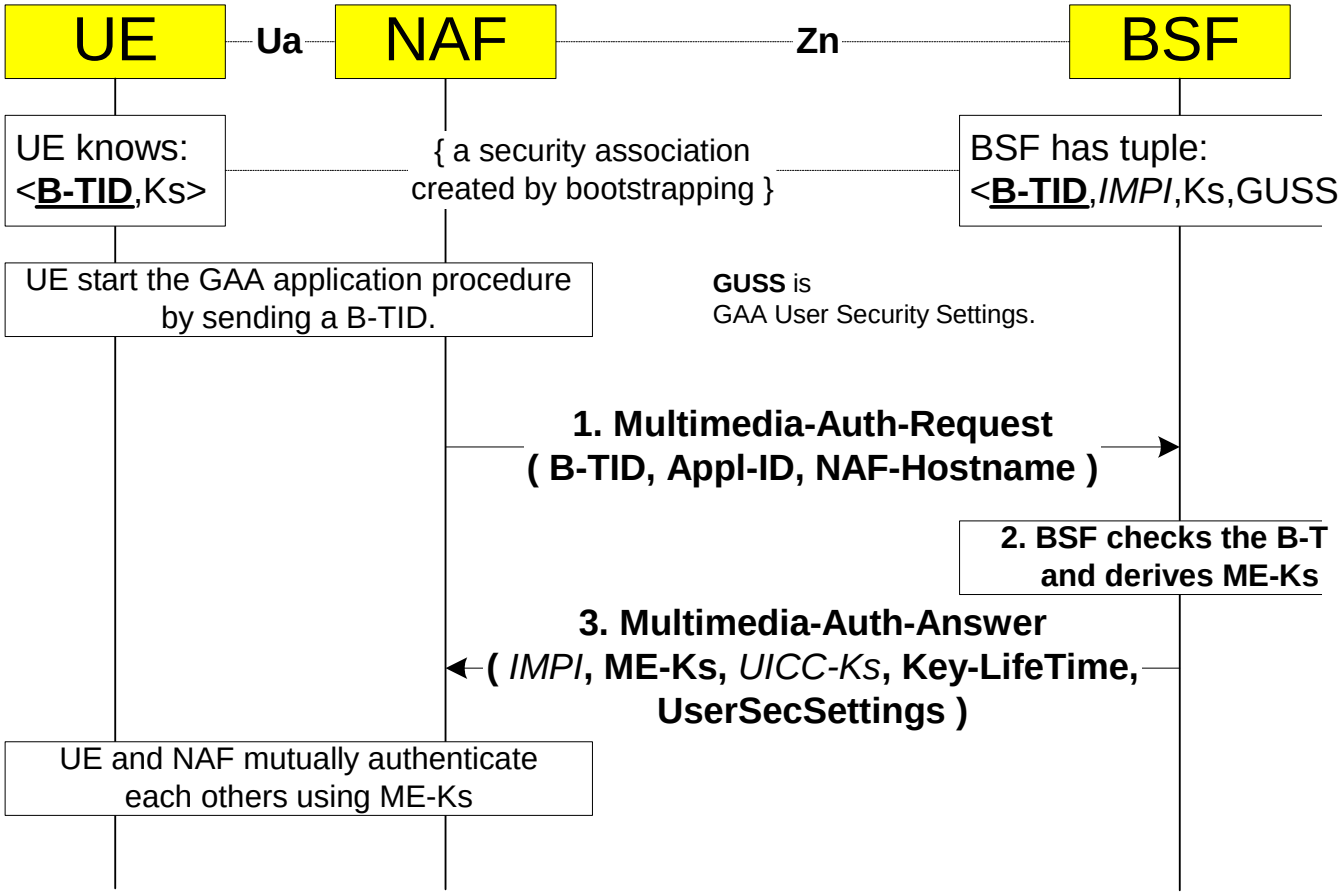


Figure 5.3: The GAA application procedure

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 "uiccType" tag in bsfInfo from the HSS is set to "GBA_U".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 Bootstrapping 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. If a special key lifetime value is given in the "lifeTime" tag inside the bsfInfo from the HSS in bootstraping procedure, it is used instead of the BSF default configuration value.~~

~~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.~~

~~** BEGIN NEXT CHANGE ****~~**

~~Annex A (normative): GBAA-UserSecSettings XML definition~~

~~This annex contains the XML schema definition for an XML document carrying the GBAA User Security Settings inside GBAA_UserSecSettings AVP in Zh and Zn 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 GBAA specific data set  -->
  <xs:complexType name=""guss"">
    <xs:sequence>
      <xs:element ref="bsfInfo" minOccurs="0"/>
      <xs:element ref=""ussList""/>
    </xs:sequence>
    <xs:attribute name=""id"" type=""xs:string""/>
  </xs:complexType>

  <!-- BSF specific information element -->
  <xs:complexType name="bsfInfo">
    <xs:sequence>
      <xs:element name="uiccType"  type="xs:string"  minOccurs="0" />
      <xs:element name="lifeTime"  type="xs:integer" minOccurs="0" />
    </xs:sequence>
  </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:

2The 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.

3The value of the attribute “id” in the element “uss” is the same as service identifier (GSID) used in GAA Service Identifier AVP.

4The value of the element “uiccType” in the element "bsfInfo" is:
GBA to indicate the basic case, or
GBA_U to indicate that generation of UICC_Ks is also required in the BSF.
The default value is GBA.

5The value of the element “lifeTime” in the element "bsfInfo" indicates a user specific key lifetime (duration in seconds) and it is defined as Key-LifeTime AVP. If the lifeTime element is missing the default value in the BSF is used.

6The value of attribute “type” in the element “uss” is GAA application type code defined in annex B.

7Values of the element “uid” are user’s public authentication identities from the HSS.

8Values 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”>
    <bsfInfo>
        <lifeTime>864003313548123</lifeTime>
    </bsfInfo>
    <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. The BSF shall not generate UICC_Ks, because uiccType is missing. A special key lifetime defines that athe duration after which the key expires is 86400 secondsspecial expiry time 3 313 548 123 seconds after 0h UTC on 1 January 1900 is used instead of value in conficuration in the BSF.

~~** END CHANGE ****~~**

3GPP TSG-CN WG4 Meeting #25 ***N4-041610***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **006** ⌘**rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Finalisation of terminology
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-0185
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change: ⌘ The last SA3#35 meeting accepted new requirements for the content of the GAA. Text is agigned accordingly.

Summary of change: ⌘ Three terminological changes area proposed:

D1) GAA Security Settings => GBA Security Settings

This change aligns the usage of the term to current SA3 practise.

The last SA3#35 meeting accepted new requirements for the content of the GAA Security Settings. Earlier the GAA Security Settings contains entirely GAA specific control information that was transparently transferred in bootstrapping procedure. Now the GAA User Security setting in HSS and Zh interface contains also data for the BSF, that is internal control information for the bootstrapping procedure (GBA).

D2) GAA Application Type => GAA Service Type

For compability with terms GAA Service and GAA Service Identifier (GSID)

D3) The singular/plural s:s are fixed in some places to current definitions.

D4) Reference to definitions in TS 23.008 is added.

		Definitions that are currently moved to TS 23.008 are removed here. Boostrapping information definitions are clarified, etc.. **D5) Several textual improvements** **F1) Data content of bootstrapping information tuple updated** **B1) GBA_U-awareness indicator is added** This implements the requirement in S3-040832 section 5.3.3 "If the NAF is GBA_U aware it indicates this by including a corresponding flag in the request.".
Consequences if not approved:	⌘	Inconsistency with stage 2

Clauses affected:	⌘	3,4,5,6,7,A,B				
Other specs affected:	⌘	**Y**	**N**		⌘	-
			X	Other core specifications		
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	Small replacements almost everywhere.				

***** BEGIN CHANGE *****

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 for bootstrapping and usage of bootstrapped security association 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.

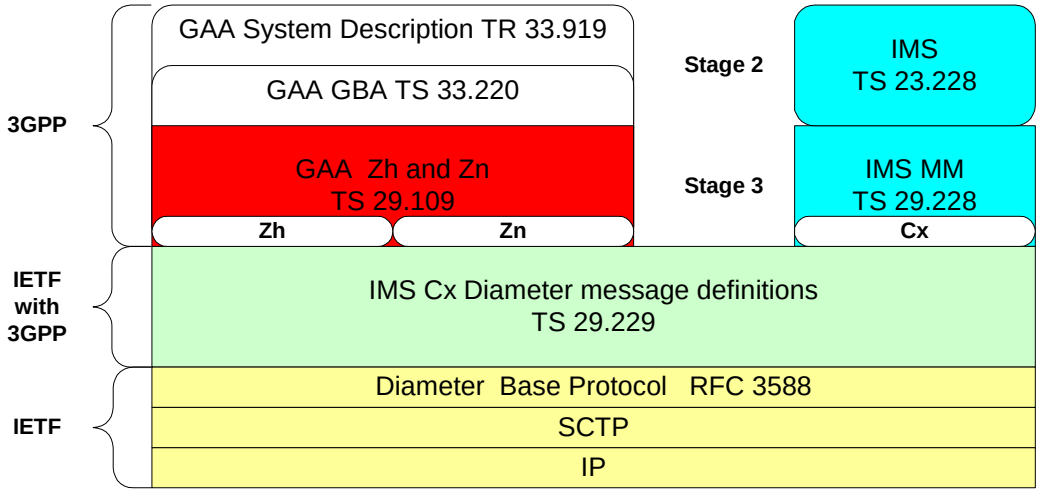
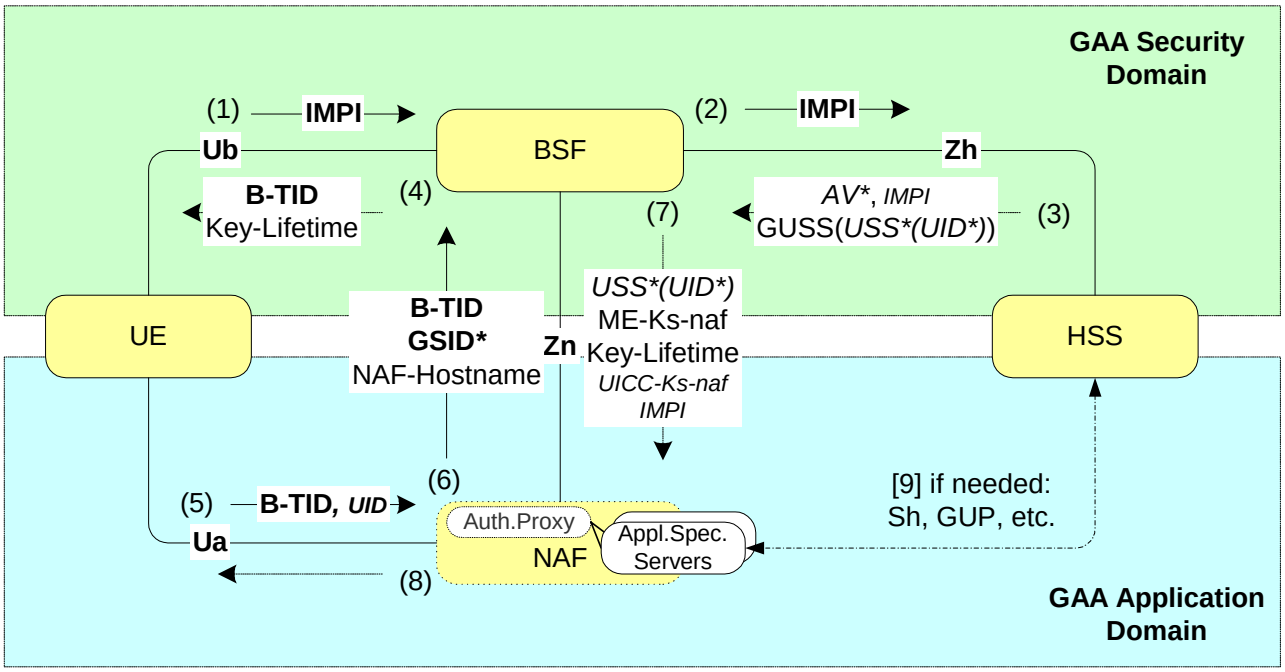
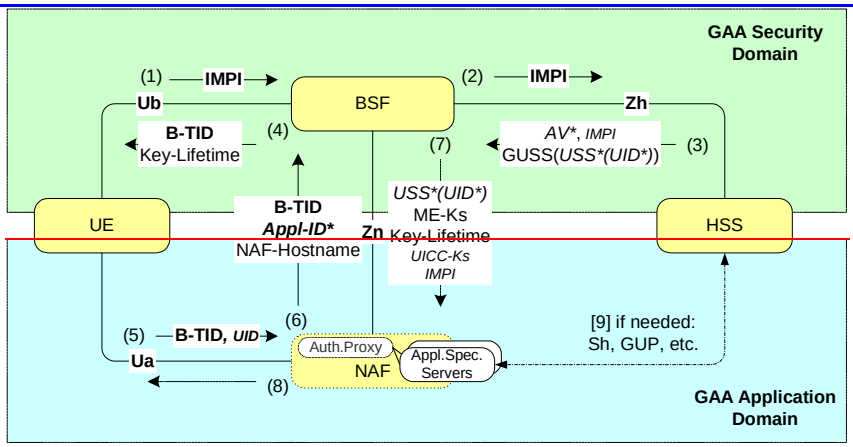


Figure 1.1: Relationships to other specifications

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.



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”.

[10] 3GPP TS 23.008: “Organisation of subscriber data”

[11] 3GPP TS 33.222: " Generic Authentication Architecture (GAA); Access to network application functions using secure hypertext transfer protocol (HTTPS) (rel-6)”.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 23.008 [10], 3GPP TR 33.919 [4] and ~~,~~ 3GPP TS 33.220 [5] ~~and 3GPP TS 33.221 [6]~~ apply with following additions.

Bootstrapping information (Bootstrapped data) in a BSF consists of a bootstrapping transaction identifier (B-TID), a key material (Ks, Ks_ME, Ks_UICC), the key lifetime (expiry time), the IMPI and the GUSS (if received from HSS) with BSF control information. ~~and is identified by B-TID~~. Each bootstrapping procedure creates a bootstrapped data entity with B-TID as retrieval key.

NAF specific Bootstrapping information transferred from a BSF to a NAF contains NAF and its service specific parts from bootstrapped data and needed key information derived from the bootstrapped data.

GAA application ~~is an~~**is** an application that uses the security association created by GB~~A~~A 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.~~

Service/Application. The term service is used here in its common meaning. A service is something that a MNO offers to subscribers. GAA Services are identified by GAA Service Identifier. In stage 2 documents ([4], [5], [6] and [11]) the term application is used in the same meaning i.e. MNOs offer applications to subscribers. There is a reason to avoid the usage of the term application here. The application is an already reserved term in Diameter. In Diameter applications are identified by Application Identifiers.

3.2 Symbols

For the purposes of the present document, the terms and definitions given in 3GPP TS 23.008 [10].~~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	GB~~A~~A User Security Settings
GSID	GAA Service Identifier
HSS	Home Subscriber System
IK	Integrity Key
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
Ks	Key Material
ME-Ks	Mobile Equipment Key Material
ME-Ks-naf	ME-Ks for a specific NAF
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
UICC-Ks	UICC Key Material
UICC-Ks-naf	UICC-Ks for a specific NAF
USS	User Security Settings (a part of GUSS)
XRES	Expected response in authentication
Zh	BSF-HSS interface for bootstrapping procedure
Zn	BSF-NAF interface for GAA applications.

4 GBAA 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].

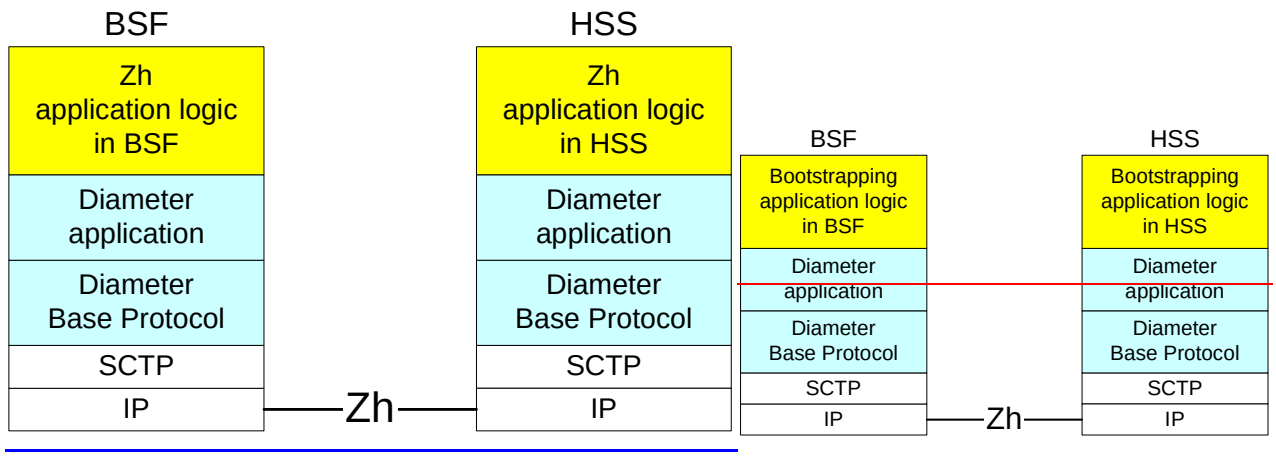


Figure 4.2: Protocol stack of Zh interface

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 vectors and possibly GBAA 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 vectors and GBAA User Security Settings(GUSS) corresponding to the IMPI.
- The HSS supplies to the BSF the requested authentication vector(s) and GUSS ~~GAA UserSecSettings~~ (if any).

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

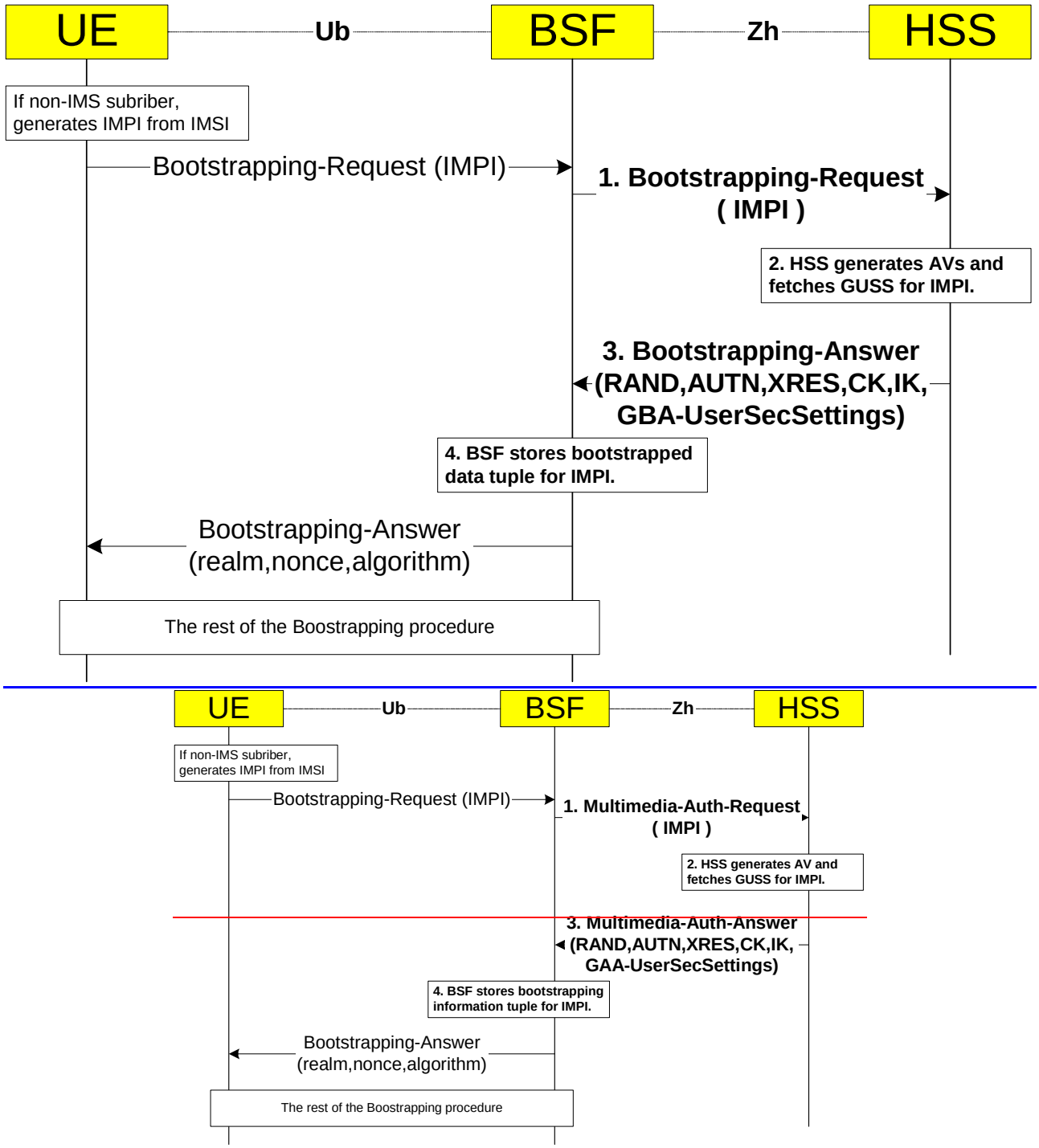


Figure 4.3: The GBAA bootstrapping procedure

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, TBD, 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 (one~~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~~ If GUSS exists for the IMPI, the HSS shall also fetch the GUSS~~GAA User Security Settings~~ into the GAB~~A~~-UserSecSettings AVP.

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 GB~~A~~A subscription in the HSS (i.e. no GB~~A~~A-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, TBD >
                < 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 ]
                [ GBAA-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 GB~~A~~A-UserSecSettings AVP.

Step 4.

When the BSF receives the MAA message, the BSF generates the needed key material (Ks, ME-Ks and optionally UICC-Ks) from confidential key (CK) and integrity key (IK) as described in 3GPP TS 33.220 [5] and stores temporarily the tuple <IMPI,Ks,Ks-ME,[Ks-UICC],GB~~A~~A-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 and the key lifetime (expiry time).

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

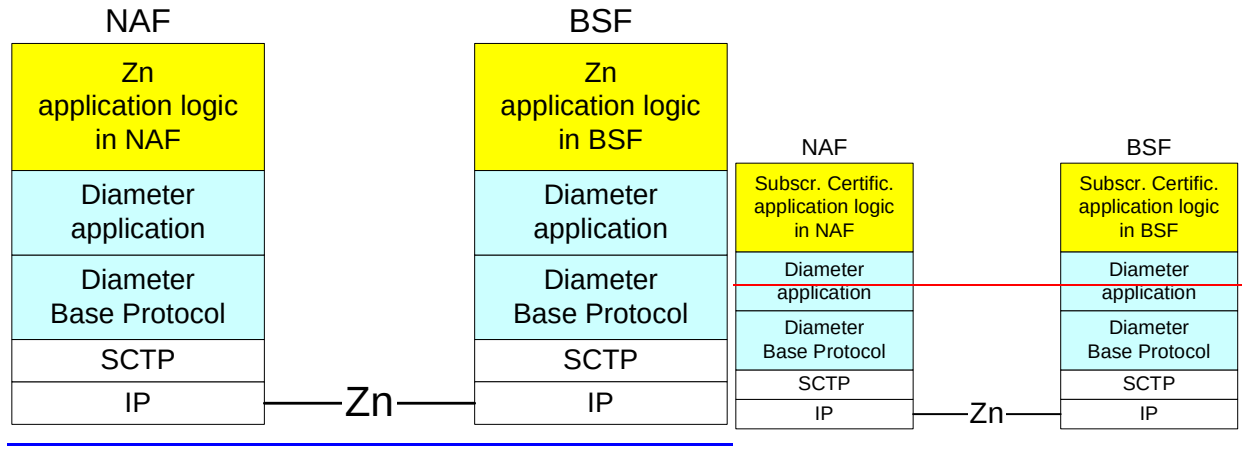


Figure 5.2: Protocol stack of Zn interface

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 the key material ~~an authentication vector~~ and possibly 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 33.220~~1~~ [5~~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, i.e. ~~e.g. a~~ the Bootstrapping Transaction Identifier (B-TID), to allow the NAF to retrieve specific key material (e.g. ME-Ks and UICC-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 (i.e. ~~e.g. a~~ the bootstrapping transaction identifier) in the start of protocol Ua.

- The BSF generates and supplies to the NAF the requested NAF specific key material, the key lifetime (expiry time)~~-~~ 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.

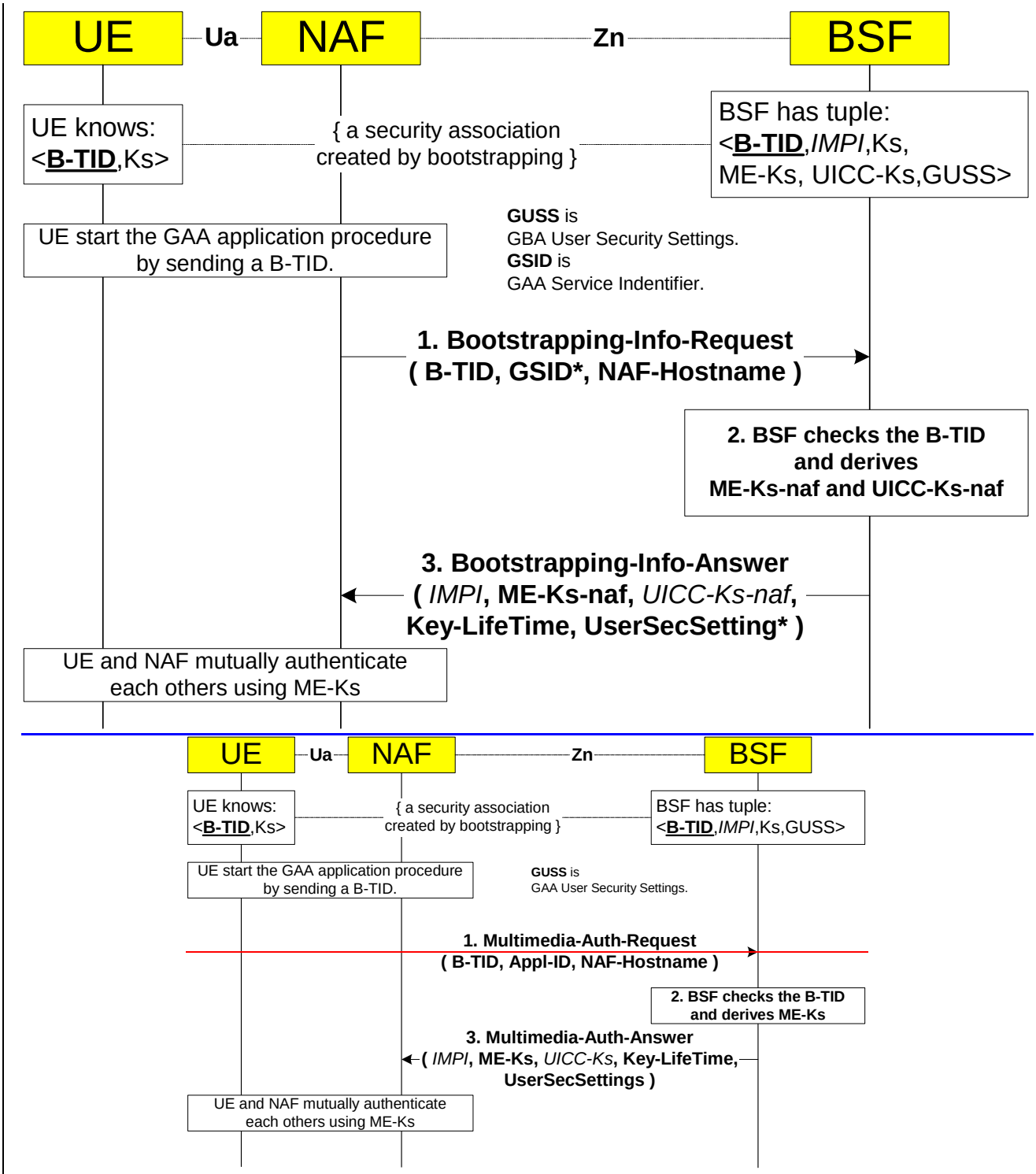


Figure 5.3: The GAA application procedure

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, TBD, 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
                  [ GBA_U-Awareness-Indicator ]             ; GBA_U awareness of the NAF
                  *[ 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 services~~application instance~~ for which the information is retrieved by GAA-Service-Identifier AVPs. 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,ME-Ks,UICC-Ks,Key lifetime, GB~~A~~A-UserSecSettings> identified by Bootstrapping Transaction Identifier (B-TID). When the BSF receives the request it checks the existence and validity 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 GB~~A~~A-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.

The NAF may be addressed from the UE with different FQDNs. The BSF shall check if this NAF-Hostname is allowed to be used for the NAF. 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, TBD >
                  < 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 cConditional
                  [ Key-LifeTime ]                  ; Time of expiryIn seconds
                  [ GBAA-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-naf) is sent in the ME-Key-Material AVP. The common key material with the UICC (UICC-Ks-naf) 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 selects the appropriate User Security Settings (if any) to the GBAA-UserSecSettings AVP from stored GBAA-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 3GPP TS 33.220 [5], 3GPP TS 33.222 [11] and optionally in GAA serviceapplication 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 GBA-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.**
GBAA-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	TimeUnsigned 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
GBA_U-Awareness-Indicator	407	6.3.1.8	Enumerated	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 GBAA-UserSecSettings AVP

The GBAA-UserSecSettings AVP (AVP code 400) is of type OctetString. If transmitted on the Zh interface it This AVP contains a set of GBA user security settings (GUSS). If transmitted on the the Zh interface it contains the relevant USSs only. The content of GBAA-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 about the support of a GAA-service by the NAF~~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 Time~~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 NAF~~BSF~~ is sharing this key material (ME-Ks-naf) 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 NAF~~BSF~~ may share this key material (UICC-Ks-naf) with a security element (e.g. USIM, ISIM, etc.~~.~~) in the UICC. Only some GAA applications use this conditional AVP.

6.3.1.8 GBA_U-Awareness-Indicator

The conditional GBA_U-Awareness-Indicator AVP (AVP code 407) is of type Enumerated. The following values are defined.

NO (0) The sending node is not GBA_U aware

YES(1) The sending node is GBA_U aware

The default value is 0 i.e. absence of this AVP indicates that the sending node is not GBA_U aware.

******* BEGIN NEXT CHANGE *******

Annex A (normative): GBAA-UserSecSettings XML definition

This annex contains the XML schema definition for an XML document carrying the GBAA User Security Settings inside GBAA-UserSecSettings AVP in Zh and Zn 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 GBAA specific 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 service ~~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 service~~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 service~~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. The BSF shall not generate UICC_Ks, because uiccType is missing. A special key lifetime defines that a special expiry time 3 313 548 123 seconds after 0h UTC on 1 January 1900 is used instead of value in conficuration in the BSF.

Annex B (normative): GAA ServiceApplication type codes

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

For examples Each GAA serviceapplication 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 serviceapplication types with their own definitions in the future.

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

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

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

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

******* END CHANGE *******

3GPP TSG-CN WG4 Meeting #25 ***N4-041612***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.008** **CR** **138** ⌘ **rev** **1** ⌘ Current version: **6.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Domain independent GAA
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-18
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	SA3 and SA2 have sent LSs to CN4 (S3-040827 and S2-043406) where it required that "*would like to point out that the GAA parameters are best stored in the HSS independently from the data stored for CS & PS domains and the IM CN subsystem, as the capability for a service to utilize GAA is not tied to any of these particular domains. However, a user utilizing GAA for service authentication must have a subscription (CS and/or PS) with the mobile operator providing GAA.*" This CR implements these LS requirements to TS 23.008. In section 9.3.9 there is anyhow a confusion with terms GAA subscription and user security setting. Besides SA3#34 decided to add also BSF control information to GAA subscription.
Summary of change:	⌘	The description of GAA only data is moved away from the IM domain chapter 3 and a new main chapter 4 in proposed for GAA only related data. Also three figures that clarify the internal/external conceptual structures of GAA data are proposed. The terminological confusion is fixed by clearly separating the GAA Service Parameters and user security setting from each other. The added "UICC Security Type" to GAA subscription data content from SA3#35 is also updated (see S3-040832 ch. 4.2.3).
Consequences if not approved:	⌘	Incompatibility with LS requirements of SA3 and SA2. Incompatibility with TS 29.109.

Clauses affected:	⌘	3.9, 3B (new), 5.3, 5.4 (new)

		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	-
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	The correctional CRs against the moved GAA material are contributed as separated CRs. The new proposed table 5.4 in this CR is already edited according these correctional CRs.				

****** BEGIN CHANGE ******

3.9 VoidData related to Generic Authentication Architecture

The Generic Authentication Architecture (GAA) is defined in 3GPP TS 33.220 [58] and 3GPP TS 29.109 [59]. For data related to GAA, see also the definition of Private User Identity in chapter 3.1.1.

3.9.1 GAA Application Type

The GAA Application Type is an enumerated integer, which is defined in 3GPP TS 29.109 [58].

The GAA Application Type is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.9.2 GAA Service Identifier

The GAA Service Identifier (GSID) is an integer, which uniquely identifies a GAA Service. For example a set of NAFs belonging to a certain GAA Service Type and owned or managed by a certain operator may provide the same operator specific service and they may use the same GAA Service Identifier to identify their services to BSF. The owner of the user's home HSS may define different GAA Authorization flags and allowed Private User Identities for each GAA Service Identifiers separately.

The GAA Service Identifier is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.9.3 GAA Service Subscription

The GAA Service Subscription (GSS) is uniquely identified by a combination of Private User Identities and GAA Service Identifier. GAA Service Subscription combines the user and the GAA Service together. No duplicates are allowed.

The User Security Setting is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.9.4 User Public Identity

The User Public Identity (UID) is a freely defined string that can be used as user's public identity in a GAA application. A list of allowed User Public Identities is stored for each GAA Service Subscription. A User Public Identity may be connected to several GAA Service Subscription.

The User Public Identity is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.9.5 GAA Authorization flag

The GAA Authorization flag is a GAA Application specific integer code, which authorizes a defined security operation in the GAA application. A list of allowed operations is stored for each GAA Service Subscription.

The GAA Authorization flag is concatenated from GAA Application Type code and GAA Application Type specific operation code in range 00-99. The value of a GAA Authorization flag is a sum of 100*(GAA Application Type

Code)+(GAA Application Type specific operation code). The values of GAA Authorization flags operation code can be therefore specified separately for each GAA application in their specifications.

The Authorization Flag is permanent subscriber data and is stored in the HSS, BSF and NAF.

3.9.6 Bootstrapping Transaction Identifier

The Bootstrapping Transaction Identifier (B-TID) identifies the security association between a BSF and a UE after a bootstrapping procedure in GAA. According [57] the B-TID value shall be also generated in format of NAI by taking the base64 encoded RAND value [60] and the BSF server name, i.e. base64 encoded (RAND)@BSF_servers_domain_name.

The Bootstrapping Transaction Identifier is temporary subscriber data and is stored in the BSF and NAF.

3.9.7 Key Lifetime

Key Lifetime is an integer which defines the expiry time of bootstrapping information in BSF in seconds passed since January 1, 1970 00:00:00.000 GMT.

The Key Lifetime is temporary subscriber data and is stored in the BSF and NAF.

****** BEGIN NEXT CHANGE ******

3B Data related to Generic Authentication Architecture

The Generic Authentication Architecture (GAA) is independent from CS/PS and IM domains, but it requires a subscription in the HSS for every its users at least in one of the domains for generation of authentication vectors. The need for a GAA specific subscriptiondata in the HSS for GAA specific user identities and/or authorization controls is GAA application dependingent. At the same time, GAA shall not be considered as a separate domain in the same sense as the notion of a "domain" is considered for CS and PS.

The Generic Authentication Architecture is defined in 3GPP TS 33.220 [58] and 3GPP TS 29.109 [59]. For data related to GAA, see also the definition of Private User Identity in chapter 3.1.1.

3B.1 GAA Service Type

The GAA Service Type is an enumerated integer, which is defined in 3GPP TS 29.109 [58].

The GAA Service Type is permanent subscriber data and is stored in the HSS, BSF and NAF.

3B.2 GAA Service Identifier

The GAA Service Identifier (GSID) is an integer, which uniquely identifies a GAA Service. For example a set of NAFs belonging to a certain GAA Service Type and owned or managed by a certain operator may provide the same operator specific service and they may use the same GAA Service Identifier to identify their services to BSF. The owner of the user's home HSS may define different GAA Authorization flags and allowed Private User Identities for each GAA Service Identifiers separately.

The GAA Service Identifier is permanent subscriber data and is stored in the HSS, BSF and NAF.

3B.3 GBA User Security Settings

The GBA User Security Settings (GUSS) is identified by a Private User Identity. The GBA User Security Settings contains optional BSF control information (i.e., UICC Security Type and optional Key Lifetime) and a set of User Security Setting (USS).

The GBA User Security Settings is permanent subscriber data and is stored in the HSS, and the BSF.

3B.4 User Security Setting

The User Security Setting (USS) is unique identified by a combination of Private User Identifiers (IMPI) and GAA Service Identifiers (GSID). The User Security Setting contains a list of allowed public indentities for the service and possible authorization flags. No duplicates are allowed.

The User Security Setting is permanent subscriber data and is stored in the HSS, BSF and NAF.

3B.5 User Public Identity

The User Public Identity (UID) is a freely defined string that can be used as user's public identity in a GAA application. A list of allowed User Public Identities is stored for each GAA Service Subscription. A User Public Identity may be connected to several GAA Service Subscription.

The User Public Identity is permanent subscriber data and is stored in the HSS, BSF and NAF.

3B.6 GAA Authorization flag

The GAA Authorization flag is a GAA Application specific integer code, which authorizes a defined security operation in the GAA application. A list of allowed operations is stored for each GAA Service Subscription.

The GAA Authorization flag is concatenated from GAA Application Type code and GAA Application Type specific operation code in range 00-99. The value of a GAA Authorization flag is a sum of 100*(GAA-Application-Type Code)+(GAA-Application-Type specific operation code). The values of GAA Authorization flags operation code can be therefore specified separately for each GAA application in their specifications.

The Authorization Flag is permanent subscriber data and is stored in the HSS, BSF and NAF.

3B.7 Bootstrapping Transaction Identifier

The Bootstrapping Transaction Identifier (B-TID) identifies the security association between a BSF and a UE after a bootstrapping procedure in GAA. According [57] the B-TID value shall be also generated in format of NAI by taking the base64 encoded RAND value [60] and the BSF server name, i.e. base64 encoded (RAND)@BSF_servers_domain_name.

The Bootstrapping Transaction Identifier is temporary subscriber data and is stored in the BSF and NAF.

3B.8 Key Lifetime

Key Lifetime is an integer which defines the expiry time of bootstrapping information in BSF in seconds passed since January 1, 1970 00:00:00.000 GMT.

The Key Lifetime is temporary subscriber data and is stored in the BSF and NAF.

3B.9 UICC Security Type

The UICC Security Type indicates the allocation of security procedure inside a User Equipment i.e. are security applications executed entirely inside mobile equipment or also in UICC .

The values of UICC Security Type are defined in TS 29.109 [59]

The UICC Security Type is permanent subscriber data and is stored in the HSS and BSF.

****** BEGIN NEXT CHANGE ******

5.3 IP Multimedia Service Data Storage

Table 5.3: Overview of data used for IP Multimedia services

	PARAMETER	Subclause	HSS	S-CSCF	IM-SSF	AS	~~BSF~~	~~NAF~~	TYPE	
	rivate User Identity	3.1.1	M	M		-	~~M~~		P	
	ublic Identity	3.1.2	M	M		-			P	
	arring Indication	3.1.3	M	M		-			P	
	ist of authorized visited network identifiers	3.1.4	M	-		-			P	
	egistration Status	3.2.1	M	-		-			T	
	-CSCF Name	3.2.2	M	-		-			T	
	iameter Client Address of S-CSCF	3.2.3	M	-		-			T	
	iameter Server Address of HSS	3.2.4	-	M	-	C			T	
	AND, XRES, CK, IK and AUTN	3.3.1	M	C		-			T	
	erver Capabilities	3.4.1	C	C		-			P	
	ubscribed Media Profile Identifier	3.5.1	C	C		-			P	
	nitial Filter Criteria	3.5.2	C	C		-			P	
	pplication Server Information	3.5.3	C	C	-	-			P	
	ervice Indication	3.5.4	M	-		M			P	
	rimary Event Charging Function Name	3.7.1	C	C	-	-			P	
	econdary Event Charging Function Name	3.7.2	C	C	-	-			P	
	rimary Charging Collection Function Name	3.7.3	M	M	-	-			P	
	econdary Charging Collection Function Name	3.7.4	C	C	-	-			P	
	smSCF address for IM CSI	3.8.4	C	-		-			P	
	M-SSF address for IM CSI	3.8.5	C	-		-			T	
	-IM-CSI	3.8.1	C	-	C	-			P	
	T-IM-CSI	3.8.2	C	-	C	-			P	
	-IM-CSI	3.8.3	C	-	C	-			P	
	smSCF address for IM CSI	3.8.4	C	-	-	-			P	
	M-SSF address for IM CSI	3.8.5	C	-	-	-			T	
~~-~~	~~AA Application Type~~	~~3.9.1~~	~~M~~				~~M~~	~~M~~		~~P~~
~~-~~	~~AA Service Identifier~~	~~3.9.2~~	~~M~~				~~M~~	~~M~~		~~P~~
~~-~~	~~AA Service Subscription~~	~~3.9.3~~	~~M~~				~~M~~	~~M~~		~~P~~
~~-~~	~~ser Public Identity~~	~~3.9.4~~	~~M~~				~~M~~	~~M~~		~~P~~
~~-~~	~~AA Authorization flag~~	~~3.9.5~~	~~M~~				~~M~~	~~M~~		~~P~~
~~-~~	~~ootstrapping Transaction Identifier~~	~~3.9.6~~	~~M~~				~~M~~	~~M~~		~~T~~
~~-~~	~~ey Lifetime~~	~~3.9.7~~	~~M~~				~~M~~	~~M~~		~~T~~

****** BEGIN CHANGE ******

5.4 Generic Authentication Architecture Service Data Storage

Table 5.4: Overview of data used for GAA services

PARAMETER	Subclause	HSS	BSF	NAF	TYPE
Private User Identity	3.1.1	M	M	C	P
GAA Service Type	3B.1	M	M	M	P
GAA Service Identifier	3B.2	M	M	M	P
GBA User Security Settings	3B.3	M	M		P
User Security Setting	3B.4	M	M	M	P
User Public Identity	3B.5	M	M	M	P
GAA Authorization flag	3B.6	C	C	C	P
Bootstrapping Transaction Identifier	3B.7		M	M	T
Key Lifetime	3B.8	C	M	M	P
UICC Security Setting	3B.9	C	C		P

The possible user's GBA User Security Settings (GUSS) are stored in HSS with User Private Identifier (IMPI) as retrieval key.

The bootstrapping procedure creates a bootstrapping information entity to the BSF with B-TID as retrieval key.

****** END CHANGE ******

3GPP TSG-CN WG4 Meeting #25 ***N4-041613***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.003** **CR** **096** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	BSF address
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	04/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	SA3 removed the BSF discovery addfress mechanism and replaced the text by the format of the BSF address. This CR includes the text agreed in S3-040831 by which the BSF address is derived from either IMSI or IMPI depending on the UICC application that was used in the bootstrapping.
Summary of change:	⌘	Include a new section for GAA to indicate the BSF address format.
Consequences if not approved:	⌘	Misalignment between Stage 2 and 3 for the Online charging failure

Clauses affected:	⌘	1.1.1,added a new section X

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

⌘

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

****** First modified section ******

1.1.1 Normative 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 21.905: "3G Vocabulary".

[2] 3GPP TS 23.008: "Organization of subscriber data".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2"

[4] 3GPP TS 23.070: "Routeing of calls to/from Public Data Networks (PDN)".

[5] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[6] 3GPP TS 29.060: "GPRS Tunnelling protocol (GPT) across the Gn and Gp interface".

[7] 3GPP TS 43.020: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[8] void

[9] 3GPP TS 51.011: " Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[11] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

[12] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land Mobile Stations in public land mobile networks (PLMN)".

[13] ITU-T Recommendation X.121: "International numbering plan for public data networks".

[14] IETF RFC 791: "Internet Protocol".

[15] IETF RFC 2373: "IP Version 6 Addressing Architecture".

[16] 3GPP TS 25.401: "UTRAN Overall Description".

[17] 3GPP TS 25.413: "UTRAN Iu Interface RANAP Signalling".

[18] IETF RFC 2181: "Clarifications to the DNS Specification".

[19] IETF RFC 1035: "Domain Names - Implementation and Specification".

[20] IETF RFC 1123: "Requirements for Internet Hosts -- Application and Support".

[21] IETF RFC 2462: "IPv6 Stateless Address Autoconfiguration".

[22] IETF RFC 3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[23] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes".

[24] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2"

[25] IETF RFC 2486: "The Network Access Identifier"

[26] IETF RFC 3261: "SIP: Session Initiation Protocol"

[27] 3GPP TS 31.102: "Characteristics of the USIM Application."

[28] void

[29] 3GPP TS 44.118: "Radio Resource Control (RRC) Protocol, Iu Mode".

[30] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2"

[31] 3GPP TS 29.002: "Mobile Application Part (MAP) specification"

[32] 3GPP TS 22.016: "International Mobile Equipment Identities (IMEI)"

[33] void

[34] void

[35] 3GPP TS 45.056: "CTS-FP Radio Sub-system"

[36] 3GPP TS 42.009: "Security aspects" [currently not being raised to rel-5 – Pete H. looking into it]

[37] 3GPP TS 25.423: "UTRAN Iur interface RNSAP signalling"

[38] 3GPP TS 25.419: "UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)"

[39] 3GPP TS 25.410: "UTRAN Iu Interface: General Aspects and Principles"

[40] ISO/IEC 7812: "Identification cards - Numbering system and registration procedure for issuer identifiers"

[41] 3GPP TS 31.102 "Characteristics of the USIM Application"

[42] 3GPP TS 33.102 "3G security; Security architecture"

[43] 3GPP TS 43.130: "Iur-g interface; Stage 2"

[45] IETF RFC 2806: "URLs for Telephone Calls"

[46] 3GPP TS 44.068: "Group Call Control (GCC) protocol".

[47] 3GPP TS 44.069: "Broadcast Call Control (BCC) Protocol ".

[48] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3".

[49] IETF Internet-Draft: "Network Discovery and Selection within the EAP Framework". draft-adrangi-eap-network-discovery-and-selection-00, work in progress.

[50] IETF Internet-Draft: "EAP AKA Authentication". draft-arkko-pppext-eap-aka-11, work in progress.

[51] IETF Internet-Draft: "EAP SIM Authentication". draft-haverinen-pppext-eap-sim-12, work in progress.

[52] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architechture and functional description"

[53] IETF Internet-Draft: 'The Network Access Identifier'.draft-arkko-roamops-rfc2486bis-00, work in progress.

[54] IETF RFC 2279: "UTF-8, a transformation format of ISO 10646".

[55] 3GPP TS 33.234: "Wireless Local Area Network (WLAN) interworking security".

[56] IETF Internet-Draft: 'The Network Access Identifier'.draft-arkko-roamops-rfc2486bis-00, work in progress.

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

****** Second modified section ******

x Numbering, addressing and identification within the GAA subsystem

x.1 Introduction

This clause describes the format of the parameters needed to access the GAA system. For further information on the use of the parameters see 3GPP TS 33.221 [xx]. For more information on the ".3gppnetwork.org" domain name and its applicability, see Annex D of the present document.

x.2 BSF address

The UE shall discover the address of the BSF (BootStrapping Function) 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 following way:

- In the case where the USIM is used in bootstrapping, the address information shall be derived as follows:

    1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [1]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;

    2. use the MCC and MNC derived in step 1 to create the "bsf.mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name;

    3. add the label "bsf." to the beginning of the domain.

  Example 1: If IMSI in use is "234150999999999", where MCC=234, MNC=15, and MSIN=0999999999, the BSF address would be "bsf.mnc015.mcc234.3gppnetwork.org".

- In the case where ISIM is used in bootstrapping, the address information shall be derived as follows:

    1. extract the domain name from the IMPI;

    2. add the label "bsf." to the beginning of the domain.

  Example 2: If the IMPI in use is "user@operator.com", the BSF address would be "bsf.operator.com ".

3GPP TSG-CN WG4 Meeting #25 ***N4-041614***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109** **CR** **008** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Command code 310 Zn messages
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-18
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	See discussion paper N4-041417
Summary of change:	⌘	Command code 310 is introduced and the messages names in interfaces are separated to Bootstrapping-Info-Request/Answer.
Consequences if not approved:	⌘	Incorrect specification

Clauses affected:	⌘	3, 5,6,7

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

Other comments: ⌘

** BEGIN CHANGE **

**** BEGIN CHANGE ***

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.
BIA	BootstrappingInfo-Answer message
BIR	BootstrappingInfo-Request message
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.

Begin next change

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].

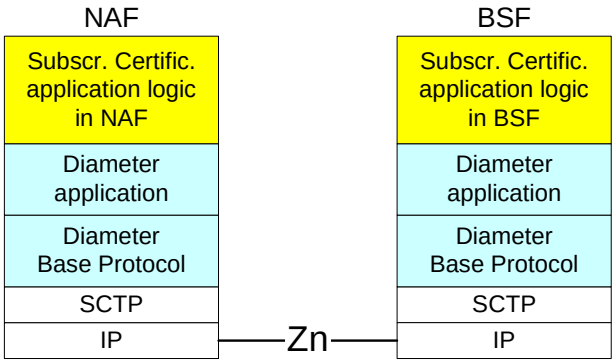


Figure 5.2: Protocol stack of Zn interface

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.

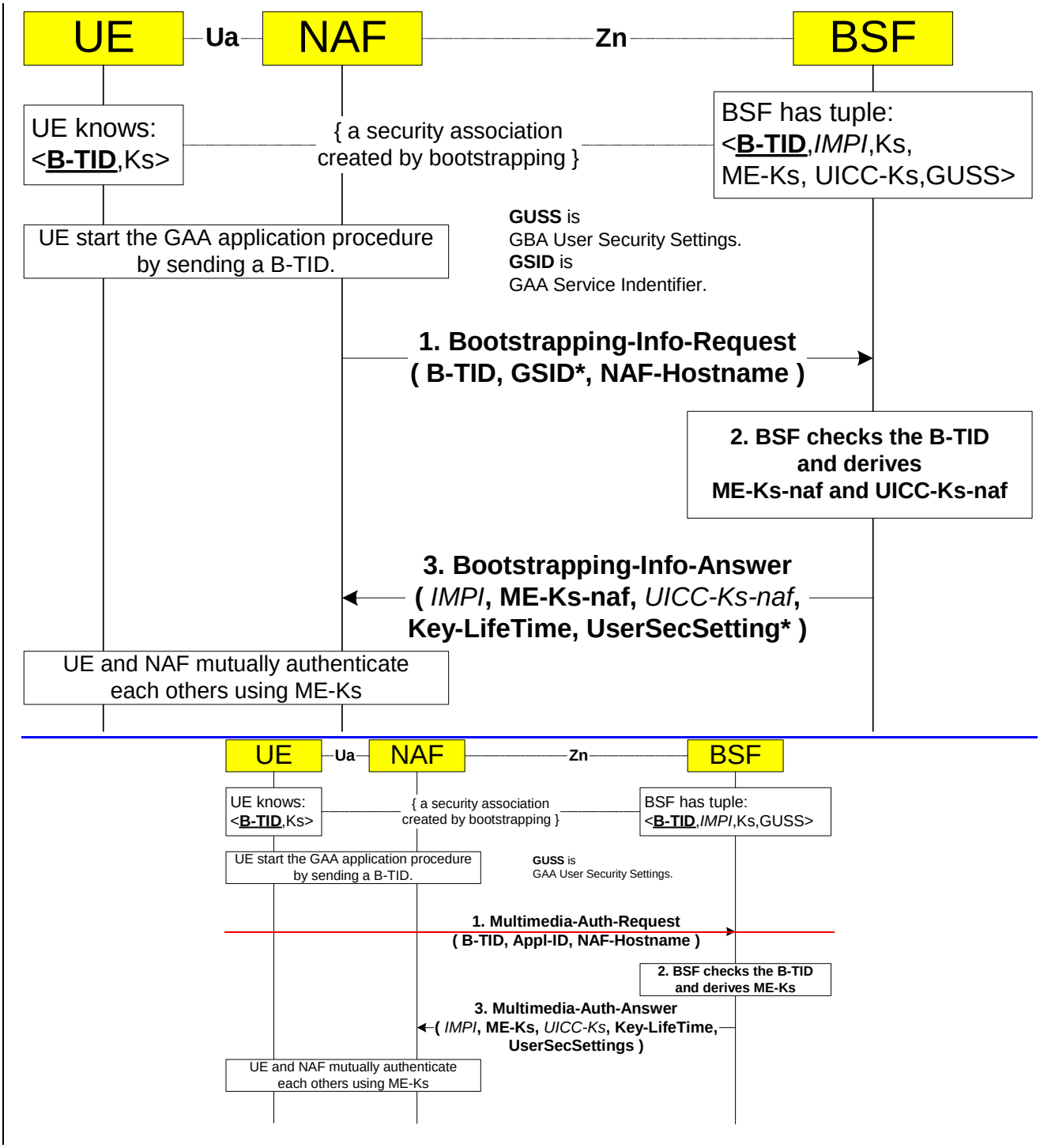


Figure 5.3: The GAA application procedure

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

Step 1

The NAF shall send a Bootstrapping-Info-Request message (BIR) ~~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).

```
< Bootstrapping-InfoMultimedia-Auth-Request> ::=<Diameter Header: 31103, 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 (BIA) ~~in the format of the following Multimedia-Auth-Answer (MAA) message~~ back to the NAF.

```
< Boostrapping-Info-Multimedia-Auth-Answer> ::= < Diameter Header: 31103 >
                    < 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 ]
```

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 BIMAA 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 assigns new Command-Codes 310 and 311.

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-Codes 310 and 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.~~

END CHANGE

3GPP TSG-CN WG4 Meeting #25 ***N4-041615***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.230** **CR** **007** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Reservation of command code 310
Source:	⌘	Nokia
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-18
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Reservation of command code value 310 for GAA Zn interface messages also in command code allocation table. See N4-041417.
Summary of change:	⌘	New command code is introduced
Consequences if not approved:	⌘	The command code may be accidentally be used for other purposes.

Clauses affected:	⌘	5.2

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

Other comments: ⌘

***** BEGIN CHANGE *****

5.1 Command codes allocated for 3GPP

Based on the IETF RFC 3589 [10] the IANA has allocated a standard command code range 300 - 313 for 3GPP. The command codes are presented in the following table.

Table 5.1: Command codes allocated for 3GPP

Command code	Command name	Abbreviation	Specified in 3GPP TS
300	User-Authorization-Request/-Answer	UAR/UAA	29.229 [2]
301	Server-Assignment-Request/-Answer	SAR/SAA	
302	Location-Info-Request/-Answer	LIR/LIA	
303	Multimedia-Auth-Request/-Answer	MAR/MAA	
304	Registration-Termination-Request/-Answer	RTR/RTA	
305	Push-Profile-Request/-Answer	PPR/PPA	
306	User-Data-Request/-Answer	UDR/UDA	29.329 [4]
307	Profile-Update-Request/-Answer	PUR/PUA	
308	Subscribe-Notifications-Request/-Answer	SNR/SNA	
309	Push-Notification-Request/-Answer	PNR/PNA	
310	Boostrapping-Info-Request/Answer	BIR/BIA	29.109 [7]

Editors note: The following command codes have been allocated to 3GPP, but they have not been used yet..

~~310~~			
311			
312			
313			

******* END CHANGE *******

3GPP TSG-CN WG4 Meeting #25 ***N4-041616***

Seoul, Korea, 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.008** **CR** **141** ⌘ **rev** **-** ⌘ Current version: **6.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Introduction of NAF Groups
Source:	⌘	CN4
Work item code:	⌘	SEC1-SC
Date:	⌘	2004-11-18
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	CN4 decided to add NAF Group and NAF Address items to TS 29.109 (see N4-041500, N4-410320).
Summary of change:	⌘	This CR adds NAF Group and NAF Address items
Consequences if not approved:	⌘	Incompatibility with TS 29.109.

Clauses affected:	⌘	3.9.10 3.9.11, 3.9.12, 5.4 (all new),

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

Other comments:	⌘	This CR contains two alternative proposals for section 5.3 for cases where CN4 accepts or do not accept the LSs from SA3 and SA2 concerning GAA data independence from CS/PS/IM domains.

****** BEGIN CHANGE ******

3.B.10 NAF Group

The NAF Group contains one or more NAF Address elements (cf. subclause 3.9.12) defining the NAFs that belong to the NAF Group. The NAF Group is identified by NAF Group Identity (cf. subclause 3.9.11).

NOTE: The grouping of NAFs 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.

The NAF Group Setting is permanent subscriber data and is stored in the BSF.

3.B.11 NAF Group Identity

The NAF Group Identity is a freely defined string that the home operator can uses as a name of a group of NAFs.

The NAF Group Identity is permanent subscriber data and is stored in the HSS and BSF.

3.B.12 NAF Address

The NAF Address is a freely defined string that can be used identify one or more NAFs. The NAF Address may contain a fully qualified domain identitying a single NAF. The NAF Address may also contain a domain name with wildcards "*" and it can be used to identity multiple NAFs.

The NAF Address is permanent subscriber data and is stored in the BSF.

****** BEGIN NEXT CHANGE ******

5.4 Generic Authentication Architecture Service Data Storage

Table 5.4: Overview of data used for GAA services

PARAMETER	Subclause	HSS	BSF	NAF	TYPE
Private User Identity	3.1.1	M	M	C	P
GAA Service Type	3B.1	M	M	M	P
GAA Service Identifier	3B.2	M	M	M	P
GBA User Security Settings	3B.3	M	M		P
User Security Setting	3B.4	M	M	M	P
User Public Identity	3B.5	M	M	M	P
GAA Authorization flag	3B.6	C	C	C	P
Bootstrapping Transaction Identifier	3B.7		M	M	T
Key Lifetime	3B.8	C	M	M	P
UICC Security Setting	3B.9	C	C		P
NAF Group	3B.10		M		P
NAF Group Identity	3B.11	C	M		P
NAF Address	3B.12		M		P

The possible user's GBA User Security Settings (GUSS) are stored in HSS with User Private Identifier (IMPI) as retrieval key.

The bootstrapping procedure creates a bootstrapping information entity to the BSF with B-TID as retrieval key.

****** END CHANGE ******