3GPP TSG CN Plenary Meeting #27 **NP-050041**
9th – 11th March 2005 Tokyo, JAPAN.

Source: TSG CN WG4

Title: Corrections on Subscriber Certificates

Agenda item: 9.3

Document for: APPROVAL

Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Ver_C
N4-050067	29.109	010		Rel-6	GAA Error Codes	C	6.1.1
N4-050094	29.109	011		Rel-6	Only one AV from HSS to BSF	F	6.1.1
N4-050095	29.109	012		Rel-6	Clarification of LifeTime/ExpiryTime terminology	F	6.1.1
N4-050358	29.109	013	1	Rel-6	Application identifiers to Z-interfaces	F	6.1.1
N4-050359	29.109	14	1	Rel-6	Modification of key lifetime material	C	6.1.1

3GPP TSG-CN WG4 Meeting #26 ***N4-050067***

Sydney, Australia, 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.109**	**CR**	**010**	⌘**rev**	**-**	⌘	Current version:	**6.1.1** ⌘

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:	⌘	GAA Error Codes		
Source:	⌘	CN4		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	2004-01-24
Category:	⌘	**C**	***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:	⌘	Incomplete error code definitions.
Summary of change:	⌘	The GAA error codes are redefined according the principle that the effective and simple error code system should only indicate to a NAF the needed actions, not the original reasons of the fault in security domain. This CR updates also a sentence in section 5.2 step 2 in the beging of paragraph about key material derivation.
Consequences if not approved:	⌘	Inconsistency and anomalities in error code definitions.

Clauses affected:	⌘	4.2, 5.2, 6.2.2				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	-
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

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

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 GBA 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 GBA User Security Settings(GUSS) corresponding to the IMPI.
- The HSS supplies to the BSF the requested authentication vector(s) and GUSS (if any).

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

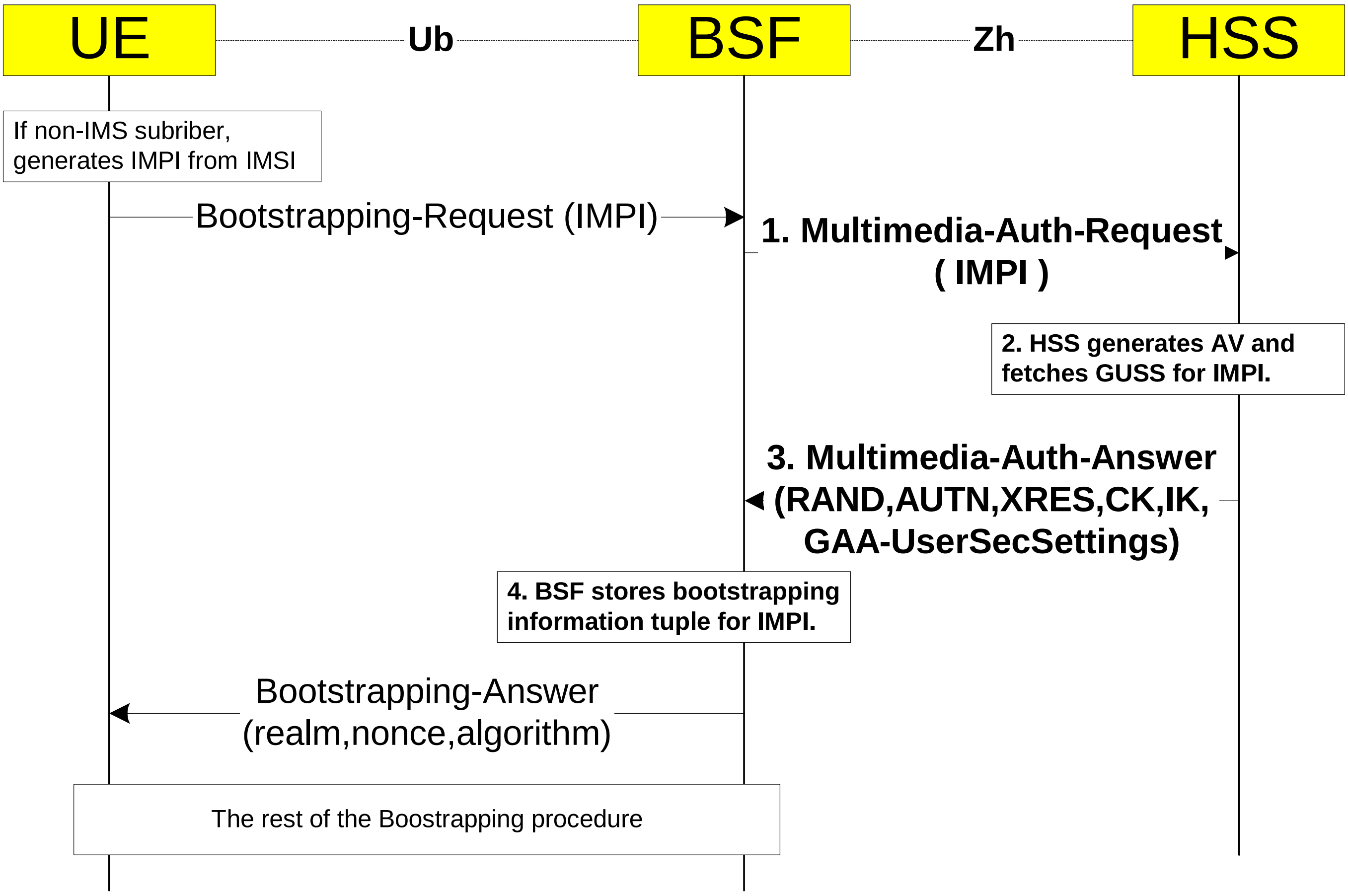

UE
Ub
BSF
Zh
HSS
If non-IMS subriber, generates IMPI from IMSI
Bootstrapping-Request (IMPI)
1. Multimedia-Auth-Request (IMPI)
2. HSS generates AV and fetches GUSS for IMPI.
3. Multimedia-Auth-Answer (RAND,AUTN,XRES,CK,IK, GAA-UserSecSettings)
4. BSF stores bootstrapping information tuple for IMPI.
Bootstrapping-Answer (realm,nonce,algorithm)
The rest of the Boostrapping procedure

Figure 4.3: The GBA 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 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]. If GUSS exists for the IMPI, the HSS shall also fetch the GUSS into the GBA-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 GBA subscription in the HSS (i.e. no GBA-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 ]
                [ GBA-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 GBA-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, ME-Ks,[UICC-Ks],GBA-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).

******* 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 the key material 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 (see 3GPP TS 33.220 [5])

- 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. 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. 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.

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 procedure is presented in Figure 5.3.

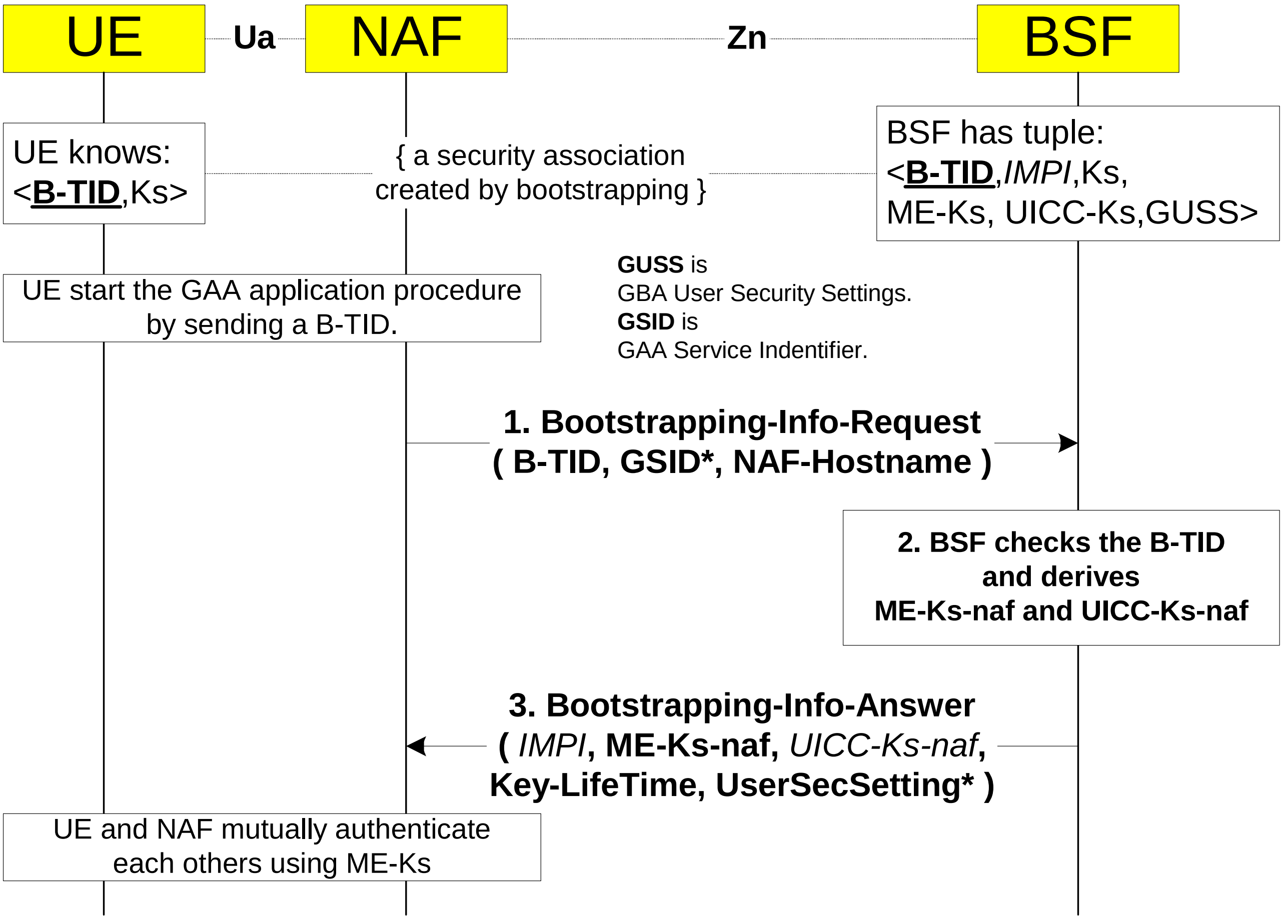

UE
Ua
NAF
Zn
BSF
UE knows:
<B-TID,Ks>
{ a security association
created by bootstrapping }
BSF has tuple:
<B-TID,IMPI,Ks,
ME-Ks, UICC-Ks,GUSS>
UE start the GAA application procedure
by sending a B-TID.
GUSS is
GBA User Security Settings.
GSID is
GAA Service Indentifier.
1. Bootstrapping-Info-Request
(B-TID, GSID*, NAF-Hostname)
2. BSF checks the B-TID
and derives
ME-Ks-naf and UICC-Ks-naf
3. Bootstrapping-Info-Answer
(IMPI, ME-Ks-naf, UICC-Ks-naf,
Key-LifeTime, UserSecSetting*)
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 (BIR) 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-Info-Request> ::=<Diameter Header: 310, TBD, REQ >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                { 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 identifiers
                { 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 indicates the GAA services 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, GBA-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 5403~~4~~ is also 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 key material for the ME (and possibly the key material for the UICC) ~~user authentication vector information~~ according to the B-TID and packs them ~~in~~ into ME-Key-Material AVP (and possible UICC-Key-Material AVP)~~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 GBA-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, and the BSF is locally configured to reject those requests from the NAF, then the error 5402~~5~~ is raised. If the NAF has sent a GAA-Service-Identifierthat have corresponding user's security settings, but the BSF is locally configured to reject those from that NAF, then the error 5402 is raised too.

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 5402~~7~~. 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 also indicated by error code 5402~~6~~.

Step 3

After that the BSF shall send a Bootstrapping-Info-Answer message (BIA) back to the NAF.

```
< Boostrapping-Info-Answer> ::= < Diameter Header: 310, TBD >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                [ Result-Code ]
                [ Experimental-Result]
                { Origin-Host }                 ; Address of BSF
                { Origin-Realm }                ; Realm of BSF
                [ User-Name ]                   ; IMPI
                [ ME-Key-Material ]             ; Required
                [ UICC-Key-Material ]           ; Conditional
                [ Key-LifeTime ]                ; Time of expiry
                [ GBA-UserSecSettings ]         ; Selected USSs
                *[ AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
```

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 "uiccType" tag in bsfInfo from the HSS is set to "GBA_U".

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 selects the appropriate User Security Settings (if any) to the GBA-UserSecSettings AVP from stored GAA-UserSecSettings in Bootstrapping information according the GBA-Service-Identifier AVPs in the request message.

The procedure in the NAF when the BIA is received is described in 3GPP TS 33.220 [5], 3GPP TS 33.222 [11] and optionally in GAA service type specific TSs.

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

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_NOT_AUTHORIZED~~GUSS_UNKNOWN~~ (5402)

A message was received by the BSF which the BSF can not authorize.~~the HSS for an IMPI that does not have GAA subscription i.e. no GBA-UserSecSettings in the HSS~~ In this case the NAF should indicate to the UE that the service is not allowed.

6.2.2.3 DIAMETER_ERROR_TRANSACTION_IDENTIFIER_INVALID~~UNKNOWN~~ (5403)

A message was received by the BSF for an invalid (e.g. unknown or expired) Bootstrapping Transaction Identifier (B-TID). In this case the NAF should request the UE to bootstrap again.

6.2.2.4 Void~~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 Void~~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 Void~~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 Void~~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.~~

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

3GPP TSG-CN WG4 Meeting #26 ***N4-050094***

Sydney, Australia, 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.109 CR 011** ⌘**rev** **-** ⌘ Current version: **6.1.1** ⌘

*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:	⌘	Only one AV from HSS to BSF		
Source:	⌘	CN4		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	2005-01-29
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 has decided that the HSS should send only one AV to the BSF in Multimedia-Auth-Answer (see latest version of TS 33.220; step 2 in both clauses 4.5.2 and 5.3.2).
Summary of change:	⌘	The TS 29.109 is changed so that only one AV is send from a HSS to a BSF.
Consequences if not approved:	⌘	Inconsistency with TS 33.220.

Clauses affected:	⌘	1, 4.2				
		Y	**N**			
Other specs affected:	⌘		**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 procedures for bootstrapping and usage of bootstrapped security association are defined in 3GPP TS 33.220 [5].

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.

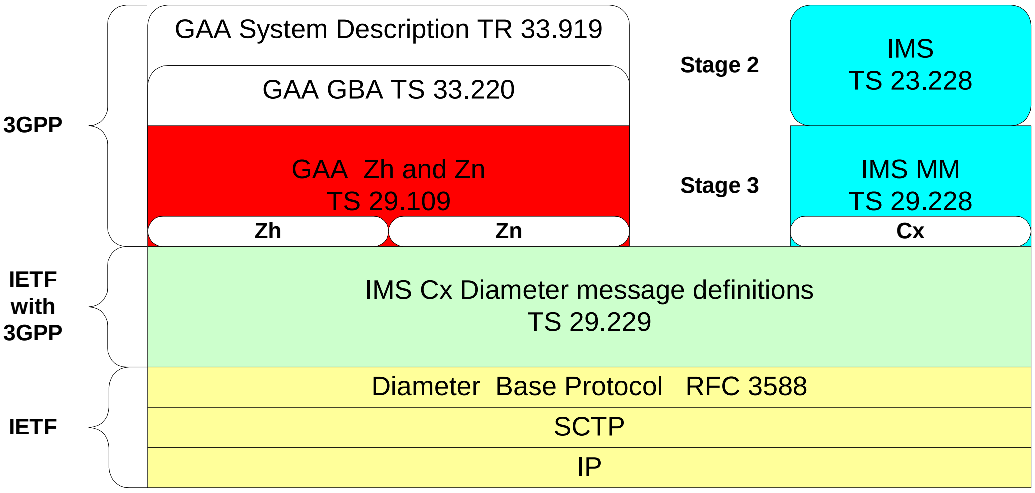
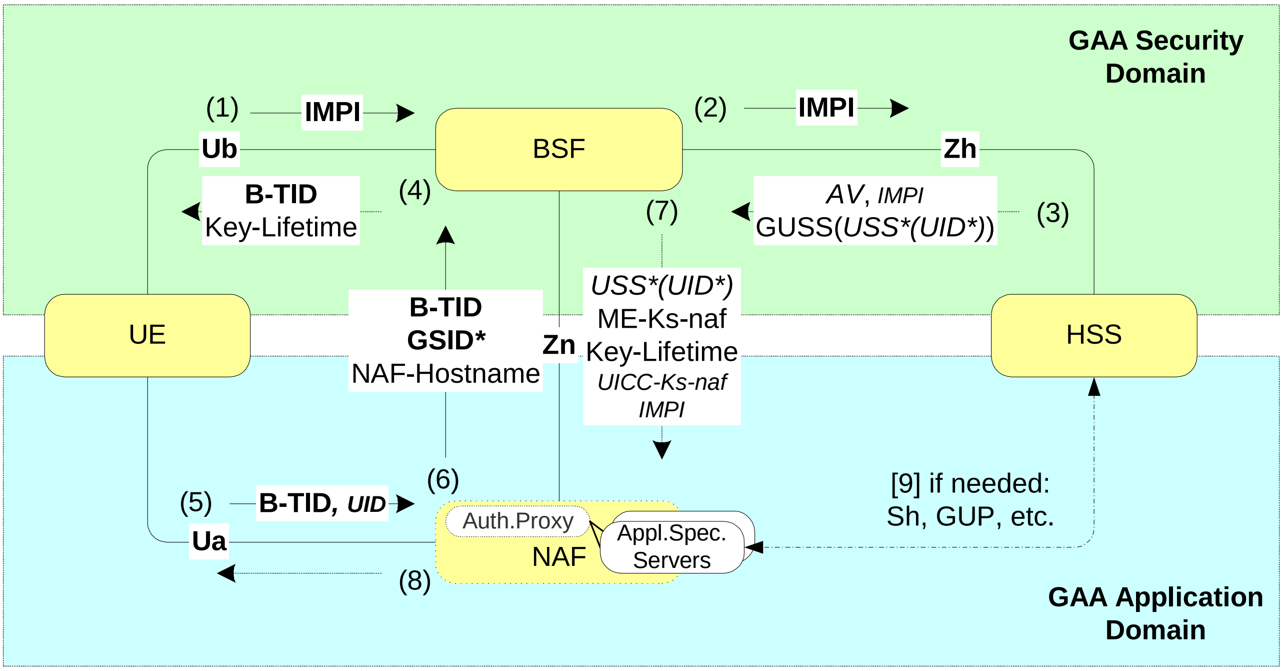
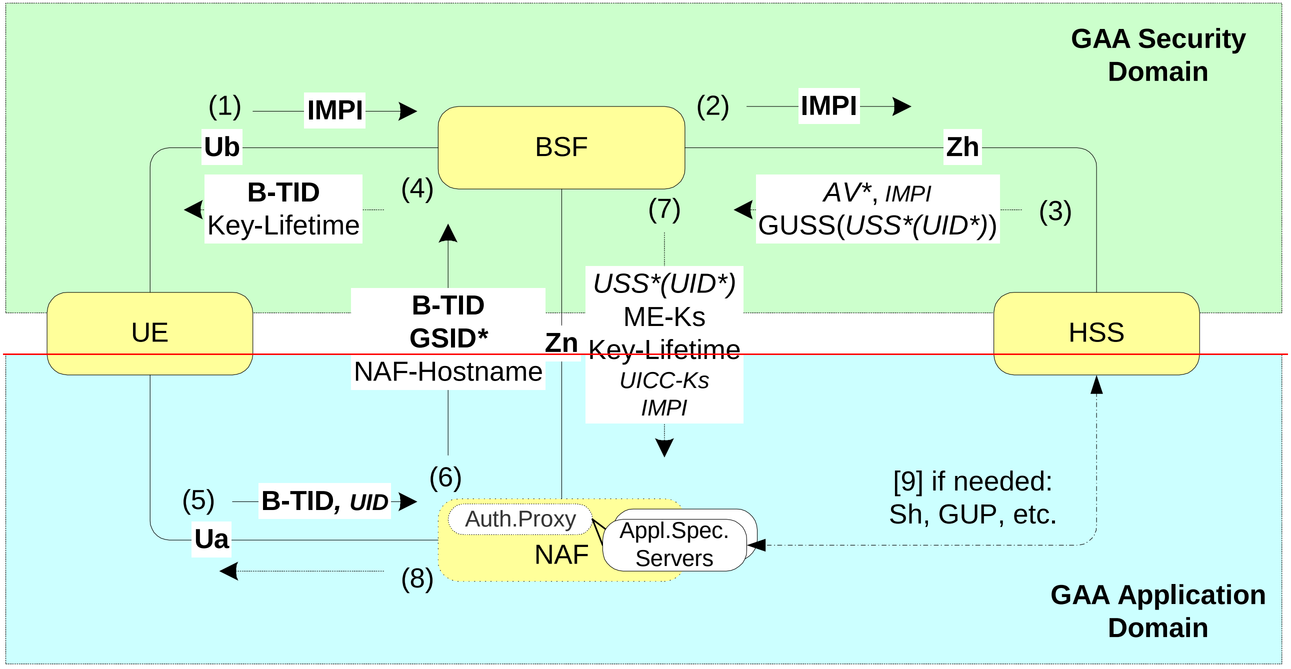


Figure 1.1: Relationships to other specifications

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 *******

4.2 Protocol Zh between BSF and HSS

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

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

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

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

- The BSF requests user's authentication vector~~s~~ and GBA User Security Settings(GUSS) corresponding to the IMPI.
- The HSS supplies to the BSF the requested authentication vector~~(s)~~ and GUSS (if any).

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

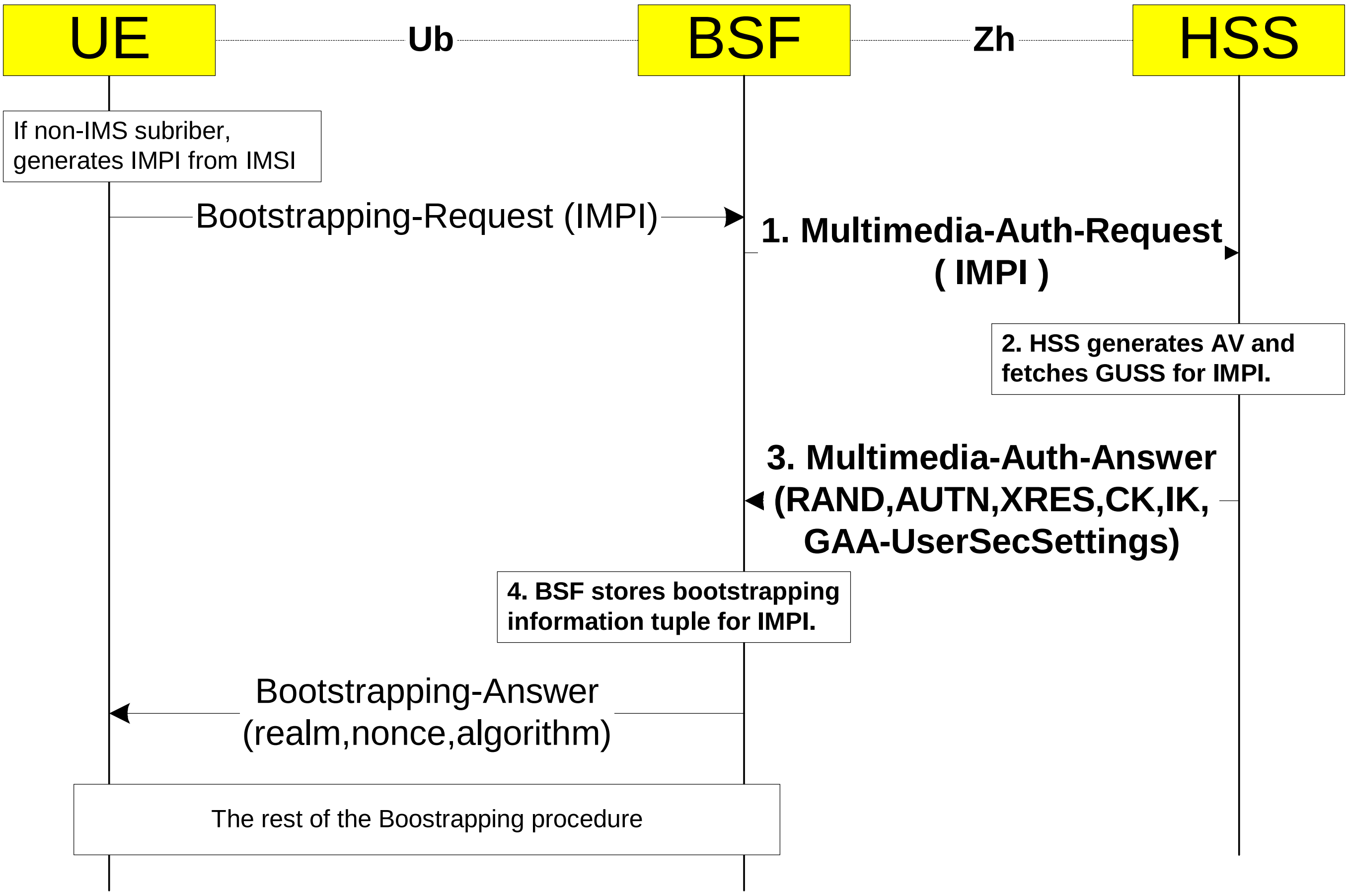

UE
Ub
BSF
Zh
HSS
If non-IMS subriber, generates IMPI from IMSI
Bootstrapping-Request (IMPI)
1. Multimedia-Auth-Request (IMPI)
2. HSS generates AV and fetches GUSS for IMPI.
3. Multimedia-Auth-Answer (RAND,AUTN,XRES,CK,IK, GAA-UserSecSettings)
4. BSF stores bootstrapping information tuple for IMPI.
Bootstrapping-Answer (realm,nonce,algorithm)
The rest of the Boostrapping procedure

Figure 4.3: The GBA 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 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 Vector~~s~~ (AV) information according the IMPI and populates it into SIP-Auth-Data AVP as defined in 3GPP TS 29.229 [3]. If GUSS exists for the IMPI, the HSS shall also fetch the GUSS into the GBA-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 GBA subscription in the HSS (i.e. no GBA-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 ]
                [ GBA-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 vector~~s~~ is~~are~~ send in the SIP-Auth-Data-Items AVP.~~s 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 GBA-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, ME-Ks,[UICC-Ks],GBA-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).

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

3GPP TSG-CN WG4 Meeting #26 ***N4-050095***

Sydney, Australia, 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.109**	**CR**	**012**	⌘**rev**	**-**	⌘	Current version:	**6.1.1**	⌘

*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:	⌘	Clarification of LifeTime/ExpiryTime terminology			
Source:	⌘	CN4			
Work item code:	⌘	SEC1-SC		***Date:*** ⌘	2005-01-29
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 has developed gradually the LifeTime concept. This has lead to the situation where the term "LifeTime has used in two different meaning: In Zh interface the LifeTime means a interval of time in seconds In Zn interface the LifeTime means a point of time.
Summary of change:	⌘	The solution here proposes usage of different terms for different usage so that the LifeTime meaning a point of time in Zn is changed to the term "ExpiryTime".
Consequences if not approved:	⌘	Unclear synonymical LifeTime terminology in the specification.

Clauses affected:	⌘	1, 5.2, 6.3				
		Y	**N**			
Other specs affected:	⌘		**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 procedures for bootstrapping and usage of bootstrapped security association are defined in 3GPP TS 33.220 [5].

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.

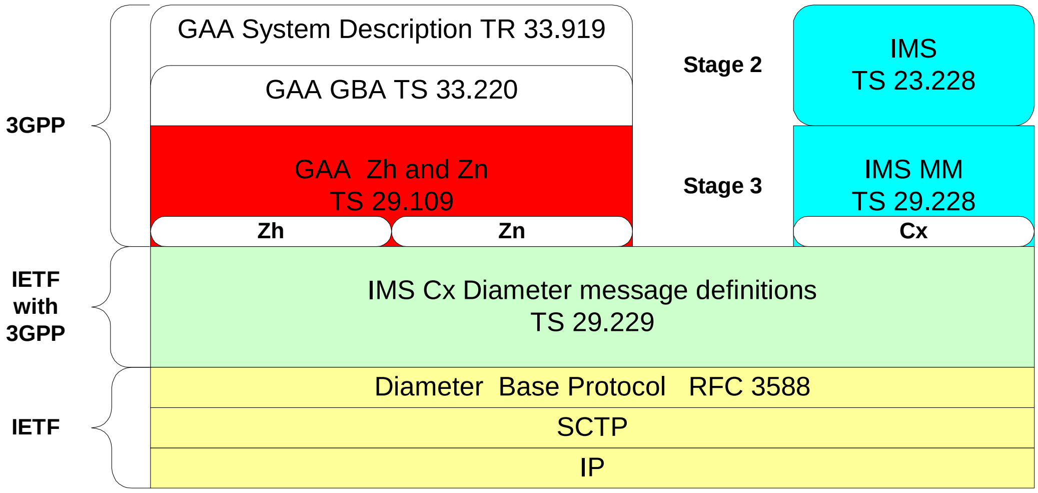
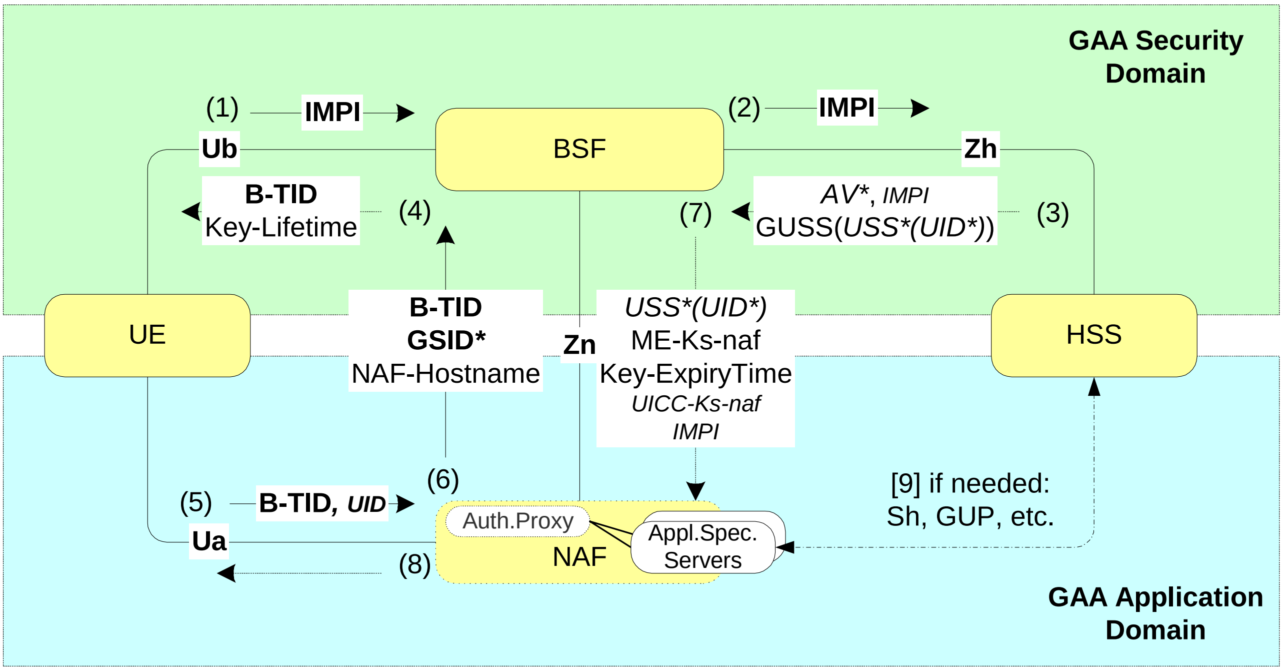
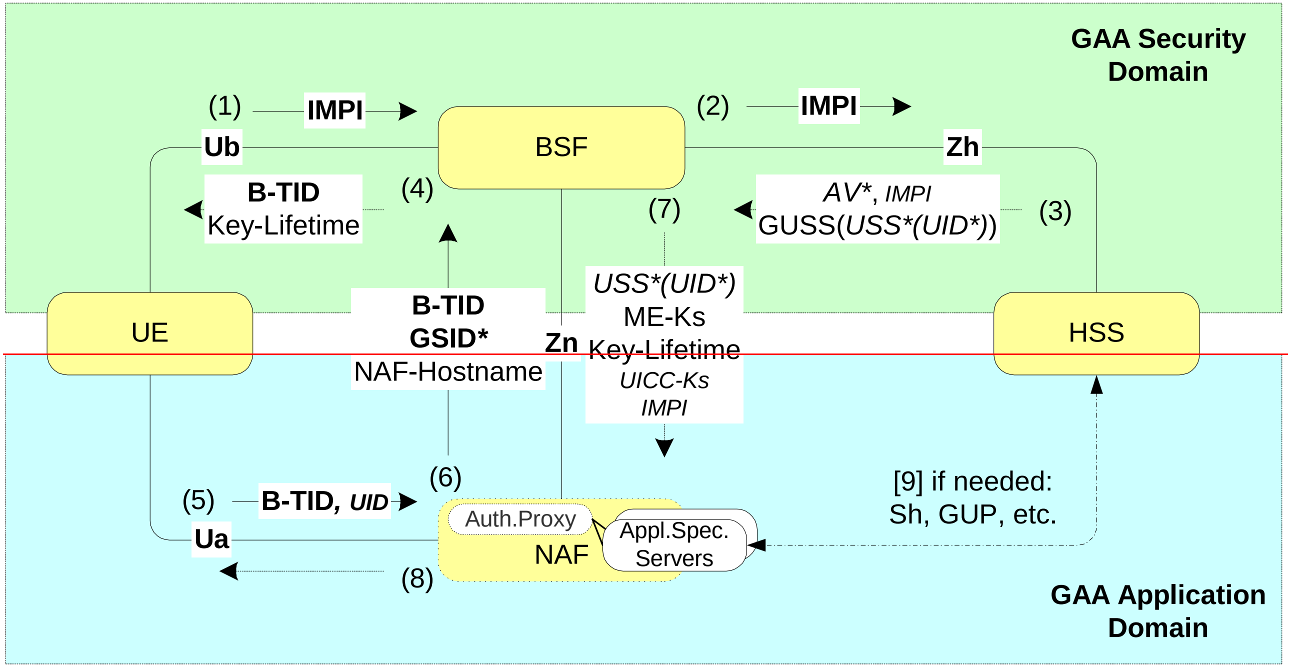


Figure 1.1: Relationships to other specifications

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 *****

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 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 (see 3GPP TS 33.220 [5])

- 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. 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. 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 expiry time~~key lifetime (expiry time)~~ and the appropriate User Security Settings defined for received application identifiers.

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 procedure is presented in Figure 5.3.

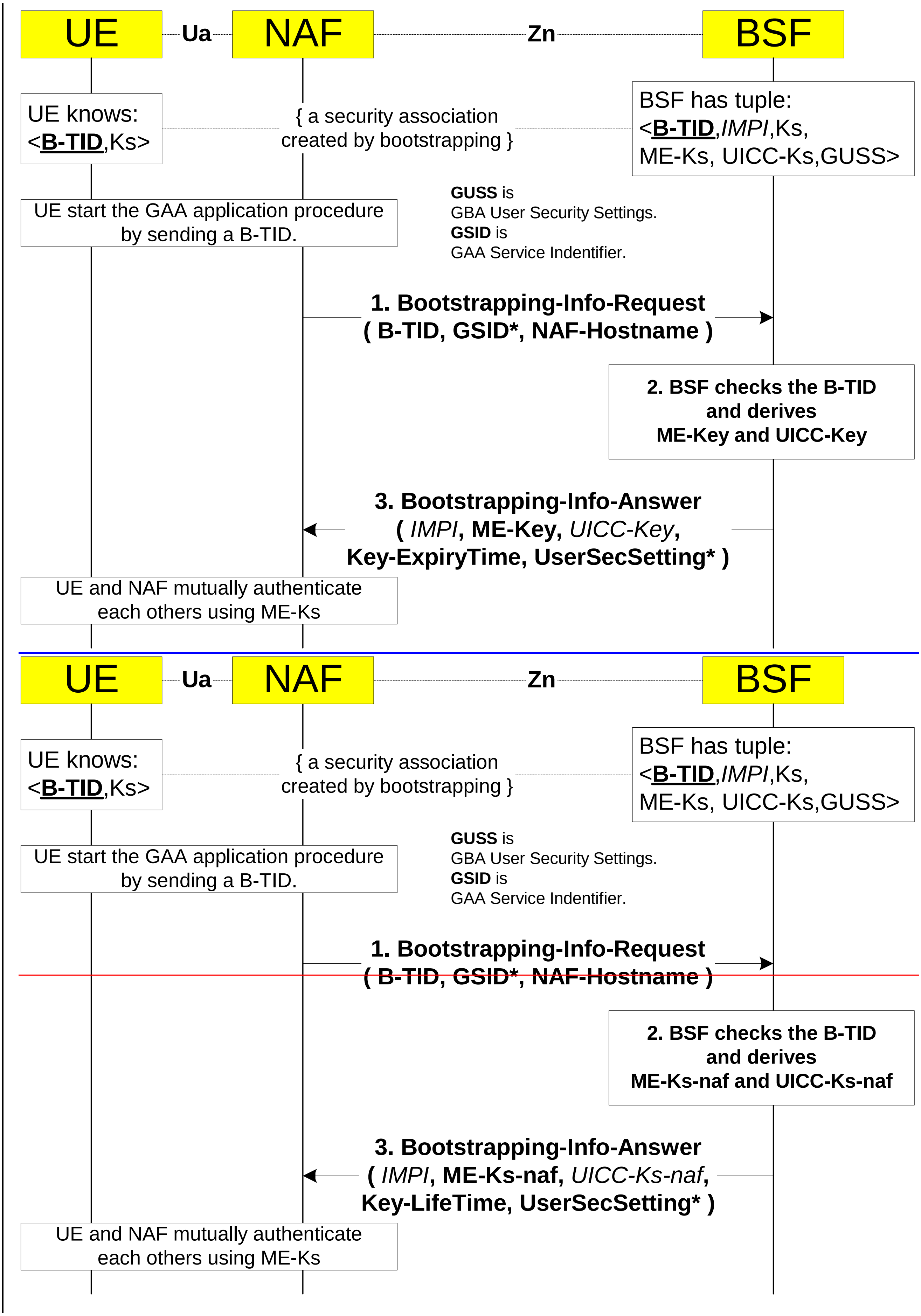

UE
Ua
NAF
Zn
BSF
UE knows: <B-TID,Ks>
{ a security association created by bootstrapping }
BSF has tuple: <B-TID,IMPI,Ks, ME-Ks, UICC-Ks,GUSS>
UE start the GAA application procedure by sending a B-TID.
GUSS is GBA User Security Settings.
GSID is GAA Service Indentifier.
1. Bootstrapping-Info-Request (B-TID, GSID*, NAF-Hostname)
2. BSF checks the B-TID and derives ME-Key and UICC-Key
3. Bootstrapping-Info-Answer (IMPI, ME-Key, UICC-Key, Key-ExpiryTime, UserSecSetting*)
UE and NAF mutually authenticate each others using ME-Ks
UE
Ua
NAF
Zn
BSF
UE knows: <B-TID,Ks>
{ a security association created by bootstrapping }
BSF has tuple: <B-TID,IMPI,Ks, ME-Ks, UICC-Ks,GUSS>
UE start the GAA application procedure by sending a B-TID.
GUSS is GBA User Security Settings.
GSID is GAA Service Indentifier.
1. Bootstrapping-Info-Request ~~(B-TID, GSID*, NAF-Hostname)~~
2. BSF checks the B-TID and derives ME-Ks-naf and UICC-Ks-naf
3. Bootstrapping-Info-Answer (IMPI, ME-Ks-naf, UICC-Ks-naf, Key-LifeTime, UserSecSetting*)
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 (BIR) 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-Info-Request> ::=<Diameter Header: 310, TBD, REQ >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                { 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 identifiers
                { 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 indicates the GAA services 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, GBA-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 GBA-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.

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 (BIA) back to the NAF.

```
< Boostrapping-Info-Answer> ::= < Diameter Header: 310, TBD >
                               < Session-Id >
                               { Vendor-Specific-Application-Id }
                               [ Result-Code ]
                               [ Experimental-Result]
                               { Origin-Host }                  ; Address of BSF
                               { Origin-Realm }                 ; Realm of BSF
                               [ User-Name ]                    ; IMPI
                               [ ME-Key-Material ]              ; Required
                               [ UICC-Key-Material ]            ; Conditional
                               [ Key-Expiry~~Life~~Time ]           ; Time of expiry
                               [ GBA-UserSecSettings ]          ; Selected USSs
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

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 “uiccType” tag in bsfInfo from the HSS is set to "GBA_U".

The Key-Expiry~~Life~~Time AVP contains the expiry time of the Bootstrapping information in the BSF according its configuration. The expiry time is represented according the Diameter Time data format in seconds that have passed since 0h on January 1, 1900 UTC ~~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 when the expiry time is calculated.

The BSF selects the appropriate User Security Settings (if any) to the GBA-UserSecSettings AVP from stored GAA-UserSecSettings in Bootstrapping information according the GBA-Service-Identifier AVPs in the request message.

The procedure in the NAF when the BIA is received is described in 3GPP TS 33.220 [5], 3GPP TS 33.222 [11] and optionally in GAA service type specific TSs.

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

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.**
GBA-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-Expiry~~Life~~Time	404	6.3.1.5	Time	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 GBA-UserSecSettings AVP

The GAA-UserSecSettings AVP (AVP code 400) is of type OctetString. If transmitted on the Zh interface it contains GBA user security settings (GUSS). If transmitted on the the Zh interface it contains the relevant USSs only. The content of GBA-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. According this AVP the BSF can select the right service’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 Service Type Codes for 3GPP standardized services are defined in Annex B.

NOTE: In the future, standardized GSID values that are different than the GAA Service 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.

6.3.1.5 Key-Expiry~~Life~~Time AVP

The Key-Expiry~~Life~~Time AVP (AVP code 404) is of type Time. This AVP informs the NAF about the expiry time of the key.

6.3.1.6 ME-Key-Material AVP

The required ME-Key-Material AVP (AVP code 405) is of type OctetString. The NAF 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 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.

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

3GPP TSG-CN WG4 Meeting #26 ***N4-050358***

Sydney, Australia, 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.109**	**CR**	**013**	⌘**rev**	**1**	⌘	Current version:	**6.1.1**	⌘

*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:	⌘	Application identifiers to Z-interfaces			
Source:	⌘	CN4			
Work item code:	⌘	SEC1-SC		***Date:*** ⌘	17.02.2005
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:	⌘	Application identifiers have been allocated to Zh and Zn interfaces in TS 29.230 v6.2.0.
Summary of change:	⌘	The missing application identifiers have been included to the TS according the TS 29.230 v6.2.0. Proxy bit is added to the messages.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.2, 5.2				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	-
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN CHANGE ***

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 GBA 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 GBA User Security Settings(GUSS) corresponding to the IMPI.
- The HSS supplies to the BSF the requested authentication vector(s) and GUSS (if any).

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

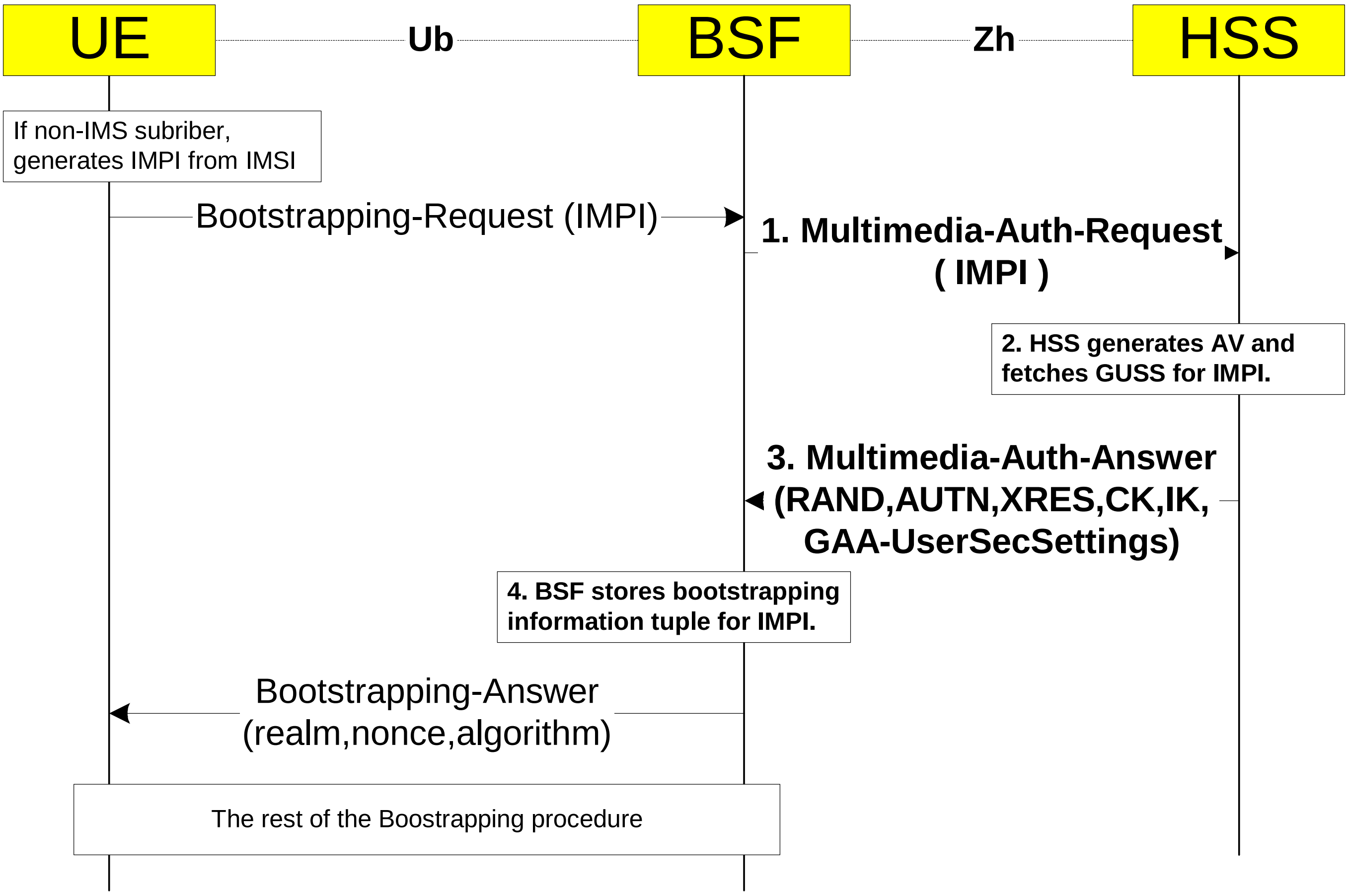

UE
Ub
BSF
Zh
HSS
If non-IMS subriber, generates IMPI from IMSI
Bootstrapping-Request (IMPI)
1. Multimedia-Auth-Request (IMPI)
2. HSS generates AV and fetches GUSS for IMPI.
3. Multimedia-Auth-Answer (RAND,AUTN,XRES,CK,IK, GAA-UserSecSettings)
4. BSF stores bootstrapping information tuple for IMPI.
Bootstrapping-Answer (realm,nonce,algorithm)
The rest of the Boostrapping procedure

Figure 4.3: The GBA 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, PXY, 16777221 >
                         < 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}        ; 16777221~~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 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]. If GUSS exists for the IMPI, the HSS shall also fetch the GUSS into the GBA-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 GBA subscription in the HSS (i.e. no GBA-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~~, PXY, 16777221 >
                               < 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 ]
                               [ GBA-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 GBA-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, ME-Ks,[UICC-Ks],GBA-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).

******* 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 the key material 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 (see 3GPP TS 33.220 [5])

- 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. 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. 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.

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 procedure is presented in Figure 5.3.

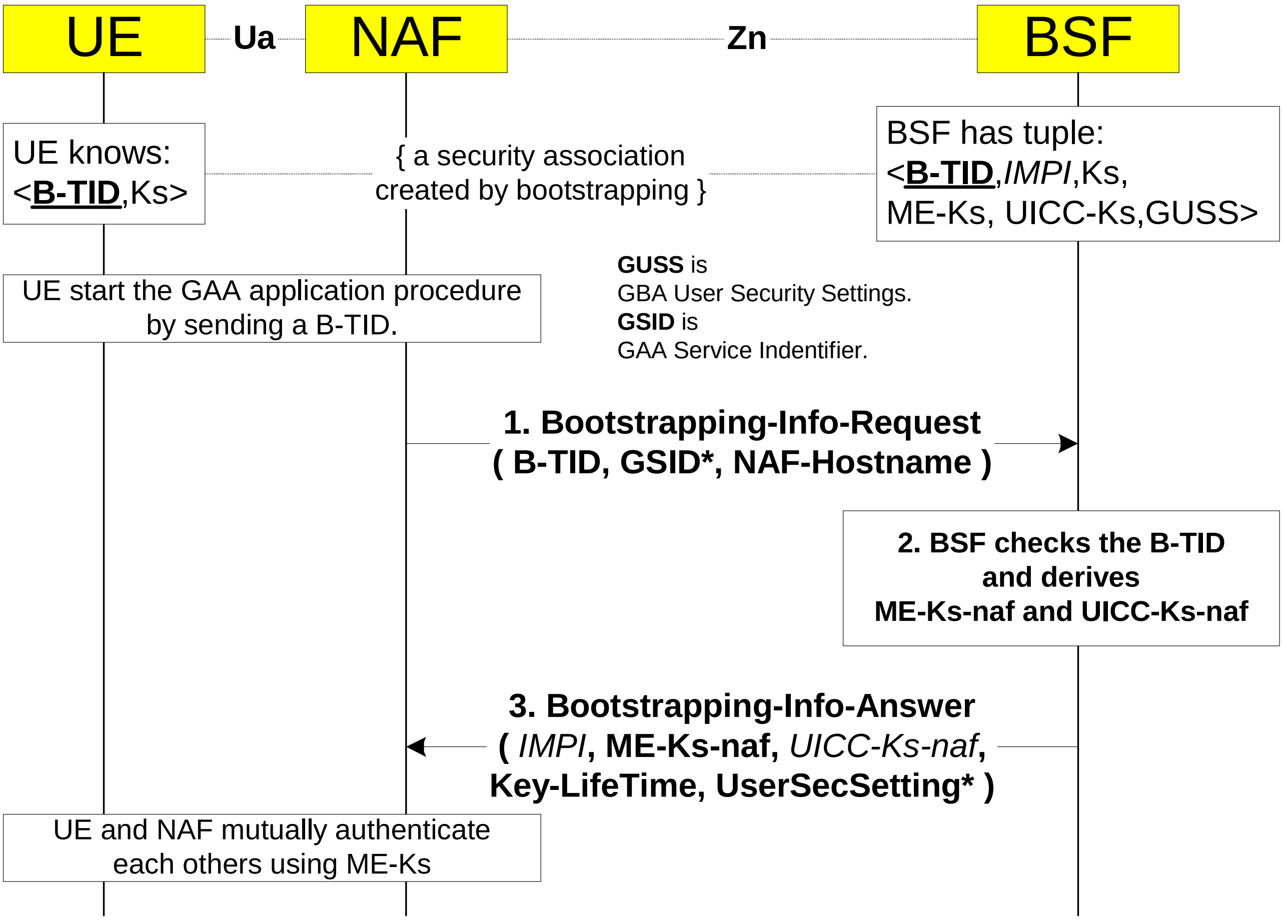

UE
Ua
NAF
Zn
BSF
UE knows: <B-TID,Ks>
{ a security association created by bootstrapping }
BSF has tuple: <B-TID,IMPI,Ks, ME-Ks, UICC-Ks,GUSS>
GUSS is GBA User Security Settings.
GSID is GAA Service Indentifier.
UE start the GAA application procedure by sending a B-TID.
1. Bootstrapping-Info-Request (B-TID, GSID*, NAF-Hostname)
2. BSF checks the B-TID and derives ME-Ks-naf and UICC-Ks-naf
3. Bootstrapping-Info-Answer (IMPI, ME-Ks-naf, UICC-Ks-naf, Key-LifeTime, UserSecSetting*)
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 (BIR) 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-Info-Request> ::=<Diameter Header: 310~~, TBD~~, REQ, PXY, 16777220 >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                { 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 identifiers
                { 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}                 ; 16777220~~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 indicates the GAA services 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, GBA-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 GBA-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.

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 (BIA) back to the NAF.

```
< Boostrapping-Info-Answer> ::= < Diameter Header: 310~~, TBD~~, PXY, 16777220 >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                [ Result-Code ]
                [ Experimental-Result]
                { Origin-Host }                  ; Address of BSF
                { Origin-Realm }                 ; Realm of BSF
                [ User-Name ]                    ; IMPI
                [ ME-Key-Material ]              ; Required
                [ UICC-Key-Material ]            ; Conditional
                [ Key-LifeTime ]                 ; Time of expiry
                [ GBA-UserSecSettings ]          ; Selected USSs
               *[ AVP ]
               *[ Proxy-Info ]
               *[ Route-Record ]
```

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 "uiccType" tag in bsfInfo from the HSS is set to "GBA_U".

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 selects the appropriate User Security Settings (if any) to the GBA-UserSecSettings AVP from stored GAA-UserSecSettings in Bootstrapping information according the GBA-Service-Identifier AVPs in the request message.

The procedure in the NAF when the BIA is received is described in 3GPP TS 33.220 [5], 3GPP TS 33.222 [11] and optionally in GAA service type specific TSs.

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

3GPP TSG-CN WG4 Meeting #26 ***N4-050359***

Sydney, Australia, 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.109**	**CR**	**14**	⌘**rev**	**1**	⌘	Current version:	**6.1.1**	⌘

*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: ⌘	Modification of key lifetime material			
Source: ⌘	CN4			
Work item code: ⌘	SEC1-SC		***Date:*** ⌘	2005-02-15
Category: ⌘	**C** *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.		***Release:*** ⌘	Rel-6 *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: ⌘	Currently, the NAF can only implictly discover the actual bootstrapping time. The NAF may need the actual bootstrapping time to discover the freshness of the original GBA session key Ks. Upon discovering the bootstrapping time the NAF can determine whether the original bootstrapping procedure is too old according to its policies and whether it requires the UE re-run the bootstrapping procedure. Also, the operator may have subscriber specific bootstrapping lifetimes (e.g., for prepaid subscribers). This can be set in subscriber's GBA User Security Settings (cf. clause 4.2.3 of TS 33.220). In this case the implicit discovery of the actual bootstrapping time is not possible as the bootstrapping lifetime time may vary per subscriber. **NOTE:** SA3 will discuss this issue in their next meeting (February 21-25), and decide whether the bootstrapping time is needed. Therefore we ask that this CR is **conditionally approved** by CN4 pending on the decision made by SA3.
Summary of change: ⌘	The solution here proposes the necessary change to include the life span of the key material into the 29.109
Consequences if not approved: ⌘	Time of bootstrapping cannot be determined directly by the NAF.

Clauses affected: ⌘	1, 3.1, 5.2, 6.3, 6.3.1.9 (new)				
	Y	**N**			
Other specs affected: ⌘	**X**		Other core specifications	⌘	TS 33.220
		X	Test specifications		

	□ ☒ 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 procedures for bootstrapping and usage of bootstrapped security association are defined in 3GPP TS 33.220 [5].

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.

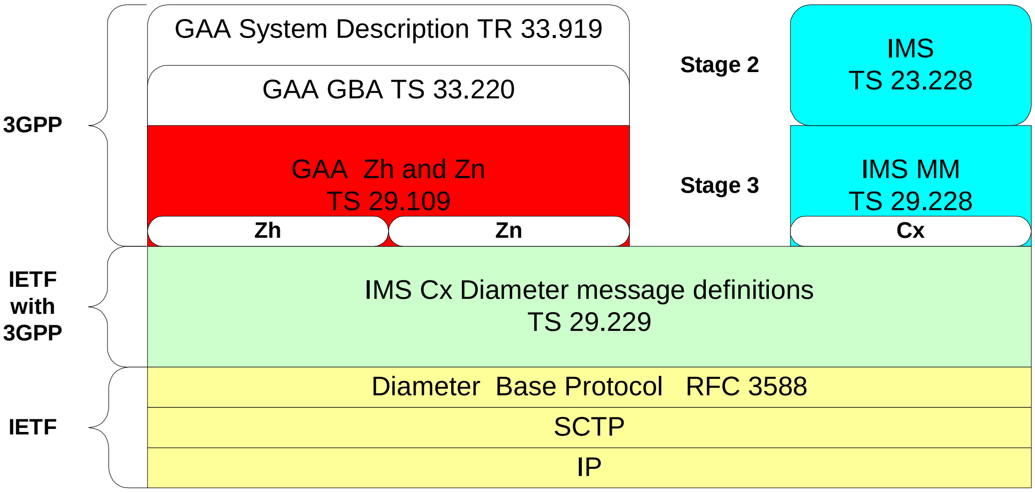
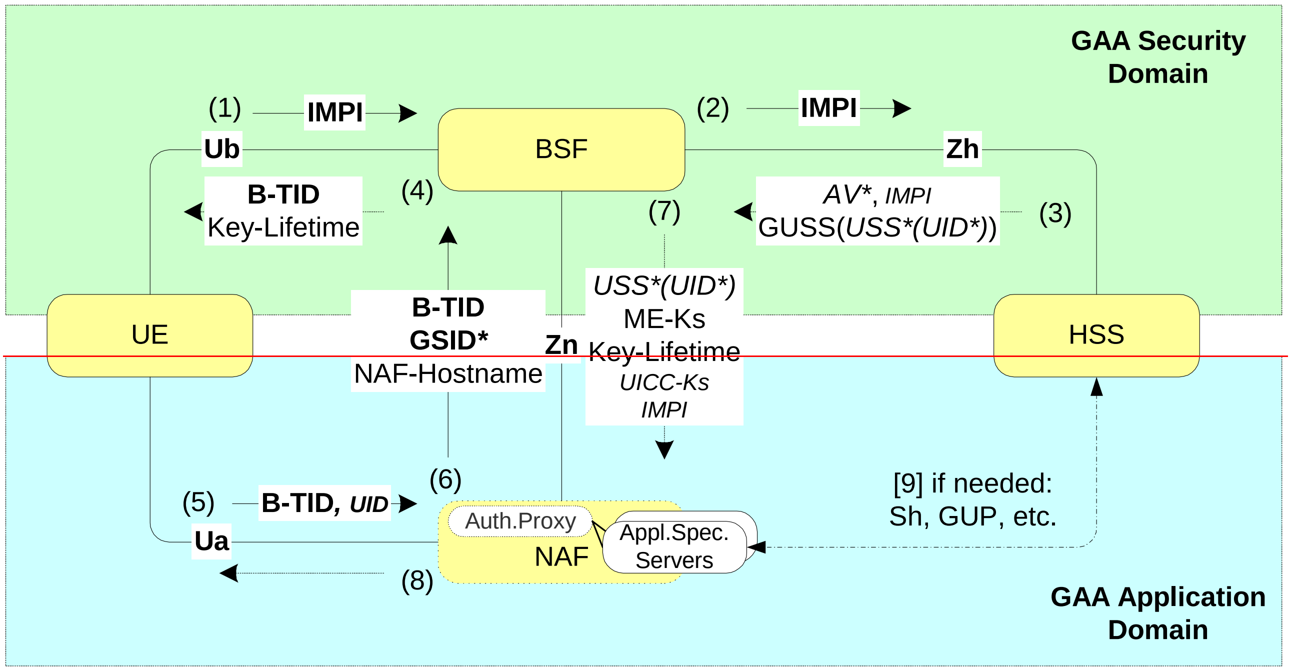
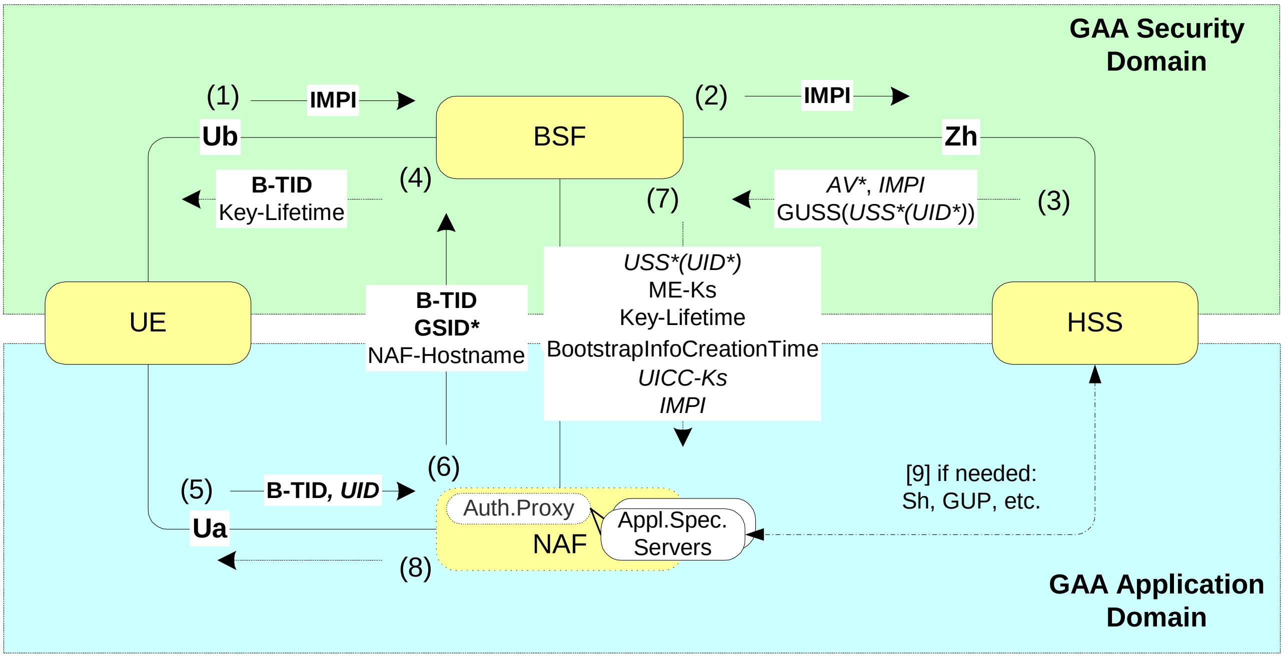


Figure 1.1: Relationships to other specifications

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 TS 23.008 [10], 3GPP TR 33.919 [4], 3GPP TS 33.220 [5] apply with following additions.

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

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

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.

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.

******* 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 the key material 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 (see 3GPP TS 33.220 [5])

- 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. 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. 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), the bootstrapinfo creation time, and the appropriate User Security Settings defined for received application identifiers.

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 procedure is presented in Figure 5.3.

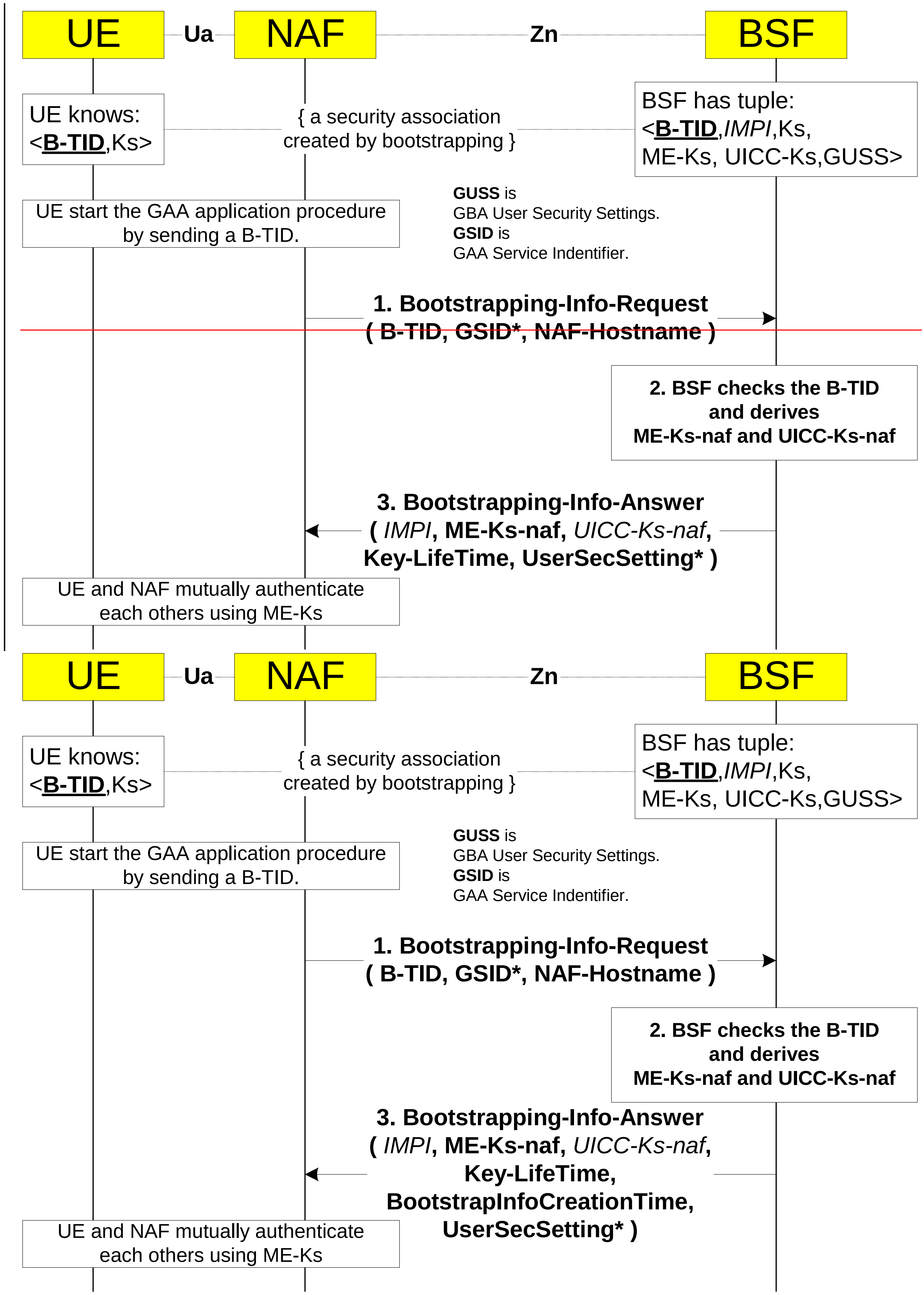

UE
Ua
NAF
Zn
BSF
UE knows:
<B-TID,Ks>
{ a security association
created by bootstrapping }
BSF has tuple:
<B-TID,IMPI,Ks,
ME-Ks, UICC-Ks,GUSS>
UE start the GAA application procedure
by sending a B-TID.
GUSS is
GBA User Security Settings.
GSID is
GAA Service Indentifier.
1. Bootstrapping-Info-Request
(B-TID, GSID*, NAF-Hostname)
2. BSF checks the B-TID
and derives
ME-Ks-naf and UICC-Ks-naf
3. Bootstrapping-Info-Answer
(IMPI, ME-Ks-naf, UICC-Ks-naf,
Key-LifeTime, UserSecSetting*)
UE and NAF mutually authenticate
each others using ME-Ks
UE
Ua
NAF
Zn
BSF
UE knows:
<B-TID,Ks>
{ a security association
created by bootstrapping }
BSF has tuple:
<B-TID,IMPI,Ks,
ME-Ks, UICC-Ks,GUSS>
UE start the GAA application procedure
by sending a B-TID.
GUSS is
GBA User Security Settings.
GSID is
GAA Service Indentifier.
1. Bootstrapping-Info-Request
(B-TID, GSID*, NAF-Hostname)
2. BSF checks the B-TID
and derives
ME-Ks-naf and UICC-Ks-naf
3. Bootstrapping-Info-Answer
(IMPI, ME-Ks-naf, UICC-Ks-naf,
Key-LifeTime,
BootstrapInfoCreationTime,
UserSecSetting*)
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 (BIR) 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-Info-Request> ::=<Diameter Header: 310, TBD, REQ >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                { 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 identifiers
                { 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 indicates the GAA services 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, Bootstrapinfo creation time, GBA-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 GBA-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.

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 (BIA) back to the NAF.

```
< Boostrapping-Info-Answer> ::= < Diameter Header: 310, TBD >
                < Session-Id >
                { Vendor-Specific-Application-Id }
                [ Result-Code ]
                [ Experimental-Result]
                { Origin-Host }                   ; Address of BSF
                { Origin-Realm }                  ; Realm of BSF
                [ User-Name ]                     ; IMPI
                [ ME-Key-Material ]               ; Required
                [ UICC-Key-Material ]             ; Conditional
                [ Key-LifeTime ]                  ; Time of expiry
                [ BootstrapInfoCreationTime ]     ; Bootstrapinfo creation time
                [ GBA-UserSecSettings ]           ; Selected USSs
               *[ AVP ]
               *[ Proxy-Info ]
               *[ Route-Record ]
```

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 "uiccType" tag in bsfInfo from the HSS is set to "GBA_U".

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 BootstrapInfoCreationTime AVP contains the bootstrapinfo creation time, i.e., creation time of the Bootstrapping information in the BSF. The bootstrapinfo creation time is represented in seconds that have passed since January 1, 1900 00:00:00.000 UTC.

The BSF selects the appropriate User Security Settings (if any) to the GBA-UserSecSettings AVP from stored GAA-UserSecSettings in Bootstrapping information according the GBA-Service-Identifier AVPs in the request message.

The procedure in the NAF when the BIA is received is described in 3GPP TS 33.220 [5], 3GPP TS 33.222 [11] and optionally in GAA service type specific TSs.

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

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.**
GBA-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	Time	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
BootstrapInfoCreationTime	408	6.3.1.9	Time	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 GBA-UserSecSettings AVP

The GAA-UserSecSettings AVP (AVP code 400) is of type OctetString. If transmitted on the Zh interface it contains GBA user security settings (GUSS). If transmitted on the the Zh interface it contains the relevant USSs only. The content of GBA-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. According this AVP the BSF can select the right service’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 Service Type Codes for 3GPP standardized services are defined in Annex B.

NOTE: In the future, standardized GSID values that are different than the GAA Service 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.

6.3.1.5 Key-LifeTime AVP

The Key-LifeTime AVP (AVP code 404) is of type Time. This AVP informs the NAF about the expiry time of the key.

6.3.1.6 ME-Key-Material AVP

The required ME-Key-Material AVP (AVP code 405) is of type OctetString. The NAF 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 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.

6.3.1.9 BootstrapInfoCreationTime AVP

The BootstrapInfoCreationTime AVP (AVP code 408) is of type Time. This AVP informs the NAF about the bootstrapinfo cration time of the key.

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

7.1 AVP codes

This specification reserves the 3GPP vendor specific values 10415:400-499 and actually assign values 10415:400-40~~6~~8 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.

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