3GPP TSG-CN Meeting #24 **NP-040231**
2nd – 4th June 2004. Seoul, Korea

Source: **TSG CN WG 4**

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

Agenda item:

Document for: **INFORMATION,- Draft technical specification 3GPP TS 29.109 v1.0.0**

Presentation of Technical Specification to TSG

Presentation to: **TSG CN Meeting #24**
Document for presentation: **TS 29.109, Version 1.0.0**
Presented for: **Information**

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

Changes since last presentation to TSG Meeting #:
None. The TS is presented first time to the plenary.

Outstanding Issues:

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

- Remaining topics:
  Main remaining work is on transfer and content of user specific permanent control data (alternatively called user profile or user security settings) in the GAA. Also some minor additions to information elements in signalling messages are also likely due to requirements from some new supported GAA applications.

Contentious Issues:

- Handling and usage of user specific control data (i.e. user profile or user security settings) aspects are still open in SA3. The handling and usage of user specific control data affects to GAA data content of HSS and information elements in signalling messages.

3GPP TS 29.109 V1.0.0 (2004-06)

Technical Specification

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

Keywords
3GPP, DIAMETER protocol

3GPP

Postal address

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

Internet
http://www.3gpp.org

Contents

Foreword

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

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

Version x.y.z

where:

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

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

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.

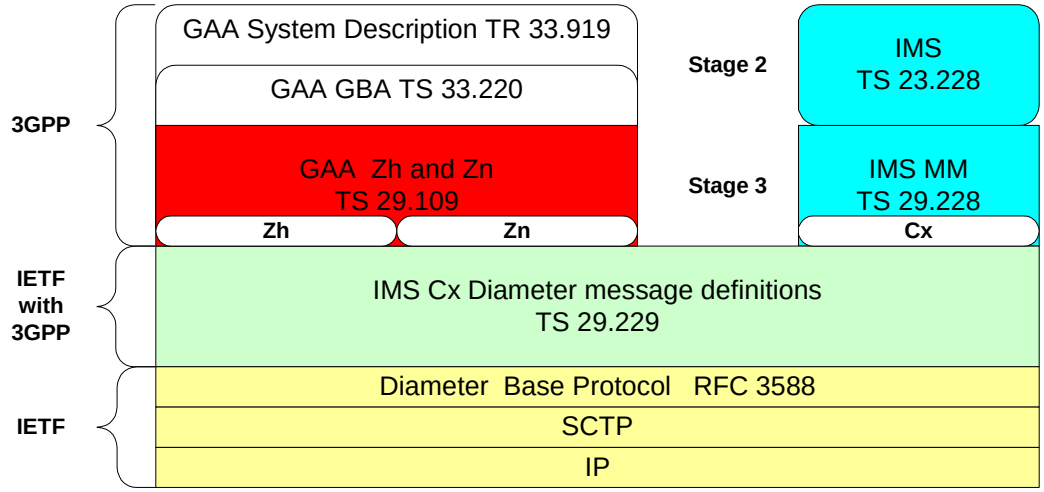

Figure 1.1: Relationships to other specifications

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)" under work in SA3.

[5] 3GPP TS 33.220 "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (rel-6)" under work in SA3.

[6] 3GPP TS 33.221 "Generic Authentication Architecture (GAA); Support for Subscriber Certificates (rel-6)" under work in SA3.

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Bootstrapping information consists of a transaction identifier (TID), a key material (Ks_naf) and an application specific user security settings identified by TID.

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

User Security Settings are GAA application specific security control settings set by home operator to a user. Typically User security Settings consist of allowance flags.

3.2 Symbols

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

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and Key Agreement
AUTN	Authentication token
AV	Authentication Vector. 3GPP AV=[RAND,AUTN,XRES,CK,IK].
AVP	Attribute-Value-Pair in Diameter messages.
BSF	Bootstrapping server functionality BSF is hosted in a network element under the control of an MNO.
BS	BootStrapping Procedure
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
TID	Transaction Identifier
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
Zn	BSF-NAF interface

4 GAA Bootstrapping Zh interface

4.1 Generic Bootstrapping Network Architecture

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

Figure 4.1: Network architecture of bootstrapping procedure

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

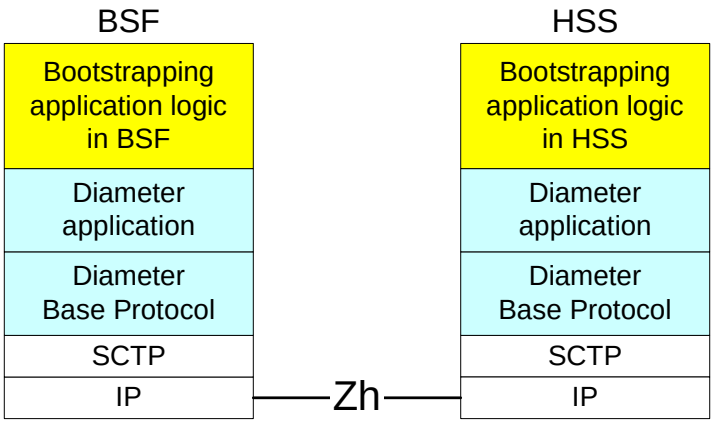

Figure 4.2: Protocol stack of Zh interface

4.2 Protocol Zh between BSF and HSS

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

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

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

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

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

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

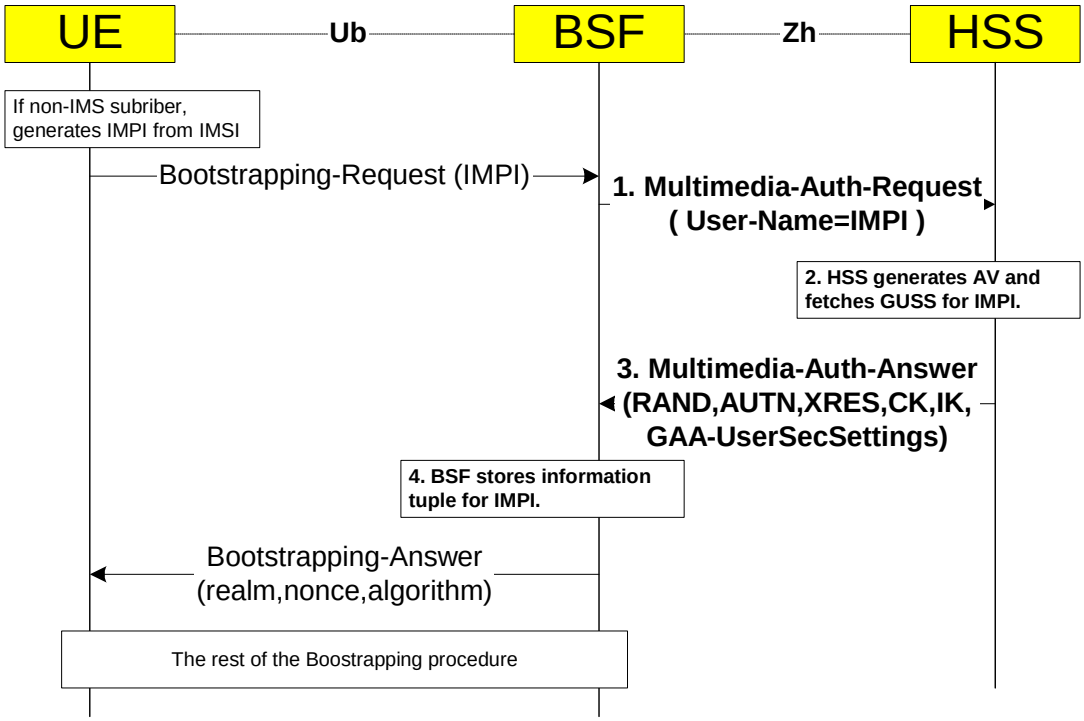

Figure 4.3: The GAA bootstrapping procedure

The steps of the bootstrapping procedure in Figure 4.3 are:

Step 1

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

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

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

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

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

Step 2

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

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

Step 3.

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

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

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

Step 4.

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

5 GAA Application Zn interface

5.1 Applications' network architecture

The network architecture of the GAA applications (e.g. Subscriber Certificates) procedure is presented in Figure 5.1. 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].

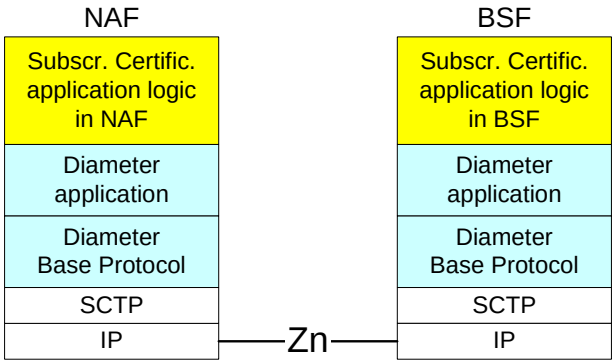

Figure 5.2: Protocol stack of Zn interface

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 transaction identifier (TID), to allow the NAF to retrieve specific key material (Ks) from BSF.
- The UE derives the keys required to protect protocol Ua from the key material (Ks).

B) The NAF starts protocol Zn with BSF

- The NAF requests key material (Ks) corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier) in the start of protocol Ua.
- The BSF supplies to the NAF the requested key material (Ks) and the appropriate User Security Settings.
- The NAF derives the keys required to protect protocol Ua from the key material (Ks) 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.

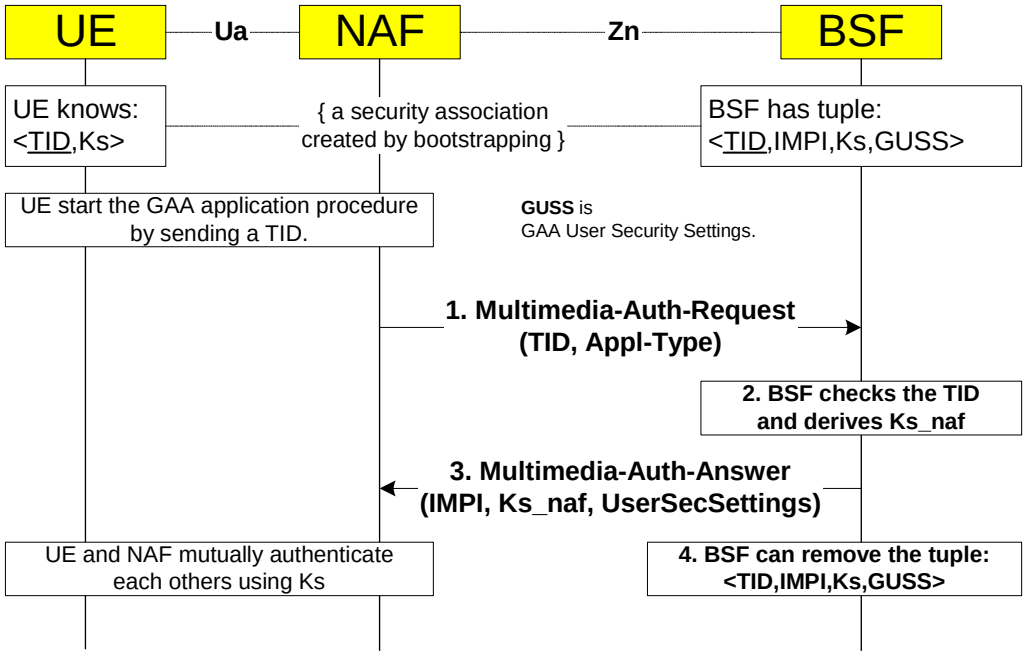

Figure 5.3: The GAA application procedure

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

Step 1

The NAF shall send a GAA-Application-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-Application-Type ]                ; Application's type
                [ Transaction-Identifier ]              ; TID
                *[ 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}               ; value of GAA-application
                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 for which the information is retrieved by GAA-Application-Id. The Transaction-Id defines the earlier bootstrapping procedure execution.

Step 2

In the successful case the BSF has a tuple <TID,IMPI,Ks,GAA-UserSecSettings> identified by Transaction Identifier (TID). When the BSF receives the MAR it checks the existence of the tuple for given TID. If checking fails the BSF sends Multimedia-Auth-Answer (MAA) with Experimental-Result set to indicate the error type. In successful case the Result-Code is set to 2xxx as defined in [1].

The BSF derives the user authentication vector information according the 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-Application-Type AVP to XXX-UserSecSettings AVP.

Step 3

After that the BSF shall send a GAA-Application-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
                [ GAA-Key-Material ]            ; Contains Ks_naf
                [ XXX-UserSecSettings ]         ; XXX application's User Security
                Settings
                *[ 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 User-name AVP (IMPI) may be sent back for checking. The key material (Ks) is sent in the GAA-Key-Material AVP. The BSF select the appropriate user's applications Security Settings to the XXX-UserSecSettings from stored GAA-UserSecSettings according the GAA-Application-Type AVP in the request message.

The procedure in the NAF when the MAA is received is described in 3GPP TS 33.221 [6].

Step 4

When the MAA message is send the BSF can remove the tuple <TID,IMPI,Ks,GAA-UserSecSettings> stored by bootstrapping procedure.

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 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.

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.

6.2.2.1 DIAMETER_ERROR_IMPI_UNKNOWN (5401)

A message was received for an IMPI that is unknown.

6.2.2.2 DIAMETER_ERROR_TRANSACTION_IDENTIFIER_UNKNOWN (5402)

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

6.2.2.3 DIAMETER_ERROR_GUSS_UNKNOWN (5403)

A message was received for a user that does not have GAA-UserSecSettings at all in the HSS.

6.2.2.4 DIAMETER_ERROR_USS_UNKNOWN (5404)

A message was received for a user that does not have the security settings for the GAA application that requires its settings, in the GAA-UserSecSettings.

6.2.2.5 DIAMETER_ERROR_NOT_SUPPORTED_USS_DATA (5405)

The BSF/NAF informs HSS/BSF that the received User Security Settings information, which was not recognised or not supported or information is insufficient.

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	Grouped	M, V				No
Transaction-Identifier	401	6.3.1.2	OctetString	M.V				No
GAA-Key-Material	402	6.3.1.3	OctedString	M,V				No
GAA-Application-Type	403	6.3.1.4	Enumerated	M,V				No
SSC-UserSecSettings	410	6.3.2.1	Grouped	M, V				No
SSC-UserSecSettings-Home-Network	412	6.3.2.2	Grouped	M, V				No
Authentication-Allowed	414	6.3.2.4	Enumerated	M,V				No
Non-Repudiation-Allowed	415	6.3.2.5	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.								

The AVP codes 400-409 are reserved for common GAA AVPs. The AVP codes 410-429 are reserved for Subscriber Certificate application. The codes 430-449, 450-469, 470-489 are respectively reserved for future GAA application.

6.3.1 Common AVPs

6.3.1.1 GAA-UserSecSettings AVP

The GAA-UserSecSettings AVP (AVP code 400) is of type Grouped. This AVP contains all the subscriber's GAA application specific security settings. The structure of this AVP is outlined in annex A.

```
<GAA-UserSecSettings>::=<AVP header: 400>
                [SSC-UserSecSettings]
                *[AVP]
```

6.3.1.2 Transaction-Identifier AVP

The Transaction-Identifier AVP (AVP code 401) is of type OctetString.

6.3.1.3 GAA-Key-Material AVP

The GAA-Key-Material AVP (AVP code 402) is of type OctetString.

6.3.1.4 GAA-Application-Type AVP

The GAA-Application-Type AVP (AVP code 403) is of type Enumerated. This AVP informs a BSF which GAA application sends the request message. According this AVP the BSF can select the right application's user security settings or no GAA user security settings. The following values are defined with default value 0:

APPLICATION_WITHOUT_GUSS (0)
SSC (1)

6.3.2 Subscriber Certificate (SSC)

AVP codes 410-429 are reserved for Subscriber Certificate application

6.3.2.1 SSC-UserSecSettings AVP

The SSC-UserSecSettings AVP (AVP code 410) is of type Grouped. This AVP contains information from home operator to the serving about what type of actions is allowed using the certificate.

```
<SSC-UserSecSettings>::=<AVP header: 410>
                {SSC-UserSecSettings-Home-Network}
```

6.3.2.2 SSC-UserSecSettings-Home-Network AVP

The SSC-UserSecSettings-Home-Network AVP (AVP code 412) is of type Grouped. This AVP contains the user's SSC security settings for home operator.

```
<SSC-UserSecSettings>::=<AVP header: 412>
                {Authentication-Allowed}
                {Non-Repudiation-Allowed}
```

6.3.2.3

```
void
```

6.3.2.4 Authentication-Allowed AVP

The Authentication-allowed AVP (AVP code 414) is of type Enumerated. This AVP informs whether the issuing of subscriber certificate with keyUsage "Authentication" is allowed or not. The absence of this AVP raises error situation. The following values are defined:

AUTHENTICATION_NOT_ALLOWED (0)
AUTHENTICATION_ALLOWED (1)

6.3.2.5 Non-Repudiation-Allowed AVP

The Non-Repudiation-Allowed AVP (AVP code 415) is of type Enumerated. This AVP informs whether the issuing of subscriber certificate with keyUsage "Non-Repudiation" is allowed or not. The absence of this AVP raises error situation. The following values are defined:

NON_REPUDIATION_NOT_ALLOWED (0)
NON_REPUDIATION_ALLOWED (1)

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 10415:400-403 and 10415:410-415 for the GAA from the 3GPP AVP Code namespace for 3GPP Diameter applications. 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`, `SIP-Number-Auth-Items`. The `Public-Identifier` AVP is also used from 3GPP TS 29.229 [3] although is not needed, but it is defined to be mandatory in the reused message in 3GPP TS 29.229 [3].

7.2 Experimental-Result-Code AVP values

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

7.3 Command Code values

This specification reuses only Command-Code 303 from 3GPP TS 29.229 [3].
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 [8] the coding may be different for version 6.

Annex A (informative): GAA-UserSecSettings UML model

The purpose of this UML model is to define in an abstract level the structure of the user's GAA user security settings downloaded over the Zh interface and describe the purpose of the different information classes included in the user's GAA security settings.

User's GAA security settings element is called **GAA-UserSecSettings**. Inside the GAA-UserSecSettings is an information element for each GAA application that is defined for the user. All GAA applications may not need special security settings. The security settings for the Subscriber Certificate (SSC) application is called **SSC-UserSecSettings**.

The following picture gives an outline of the UML model of the user's GAA security settings, which are downloaded from HSS to BSF:

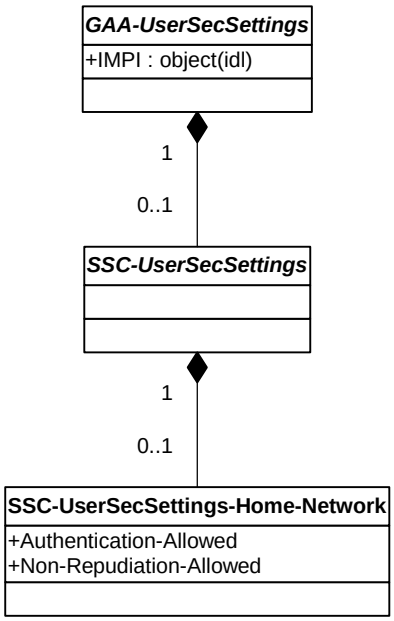

Figure A.1: The structure of the GAA User Security Settings

The SSC-UserSecSettings definition for home network is called **SSC-UserSecSettings-Home-Network**. Since it may be possible in later releases, that the PKI Portal (NAF) is located in non-home network, it is reasonable to define own user security settings for both home and foreign network cases. However, only support for home network PKI Portal (NAF) is required in release 6.

In the Zn interface the BSF downloads to the NAF only the requested SSC-UserSecSettings-*-Network leaf for current application and network type.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2003-10					*First Draft TS created*		*0.0.0*
2003-10					*Version after CN4#21*	*0.0.0*	*0.1.0*
2004-02					*Version after CN4#22*	*0.1.0*	*0.2.0*
2004-05					*Version after CN4#23*	*0.2.0*	*0.3.0*
2004-06	CN#24	NP-040231			Version 1.0.0 for information	0.3.0	1.0.0