3GPP TSG CN Plenary Meeting #24 NP-040275
2nd – 4th June 2004 Seoul, KOREA.

Source: TSG CN WG4

Title: Liaison statements after CN#23

Agenda item: 6.4.1

Document for: INFORMATION

Tdoc	Tdoc Title	LS to	LS cc	LS Attachment
N4-040473	WLAN charging	SA5, SA1	SA2	
N4-040466	LS on Assignment of the Diameter codes and identifiers	SA5, CN3	CN, SA	N4-040465
N4-040444	Response LS on IMS local services	SA2		
N4-040487	Provisioning an interface for physical storage of GUP components.	SA1, SA2		
N4-040488	Application laver versus transport layer security for GUP	SA3		
N4-040685	LS on MOCN redirect alternatives	SA2, RAN3		
N4-040746	Reply LS on the nature of LCS	SA2	SA1, CN1, GERAN, GERAN2	
N4-040664	Reply LS on Harmonisation of AMR Configurations	SA4	SA2	
N4-040699	LS on Requirement for presence of the GAA-Application-Type AVP	T2, T, SA2	CN	N4-040572
N4-040747	Managing of Metadata: New Procedures vs. Metadata GUP Components	SA2		
N4-040725	LS on Assignment of the Diameter codes and identifiers	CN3		N4-040726
N4-040748	LS on Requirement for presence of the GAA-Application-Type AVP	SA3		N4-040572
N4-040749	LS on change in MBMS Multicast Service Deactivation Procedure;	SA2		
N4-040714	LS on Clarification of TMGI format	RAN2, RAN3	CN1	N4-040713
N4-040751	Reply LS to Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0	Wi-Fi Alliance	SA2	mdr.xls

3GPP TSG CN WG4 Meeting #22bis
Edinburgh, UK, 14th – 20th April 2004

N4-040444

Title:	**LS on IMS local services**
Response to:	**LS S2-041055**
Source:	CN4
To:	SA2
Cc:	

Contact Person:

Name:	Ulrich Wiehe
Tel. Number:	+49 6621 169 139
E-mail Address:	ulrich.wiehe@gksag.de

1. Overall Description:

CN4 thank SA2 for their LS on IMS local services (S2-041055, N4-040428).
CN4 assure SA2 that the VPLMN can be determined from information transferred via the Sh reference point in Release 5. More specifically the Application Server may at any time request a user's location information from the HSS via Sh. This requested information includes the VLR-Number or SGSN-Number, and the identity of the VPLMN can be determined from these numbers.

2. Actions:

None

3. Date of Next CN4 Meeting:

CN4 #23	10th – 14th May 2004	Zagreb, CROATIA
CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE

3GPP TSG CN WG4 Meeting #23 **N4-040749**
Zagreb, CROATIA, 10th – 14th MAY 2004

Title: LS on change in MBMS Multicast Service Deactivation Procedure
Release: Release 6
Work Item: MBMS

Source: CN4
To: SA2
Cc:

Contact Person:
Name: Yuki Takeda
Tel. Number: +81-46-840-3370
E-mail Address: takeda@nttdocomo.co.jp

Attachments: None

---

1. Overall Description:

CN4 found an inconsistency in MBMS Multicast Service Deactivation Procedure between stage 2 design and stage 3 design. It has been found necessary to slightly modify the stage 2 flow in order to be consistent with stage 3.

The signalling flow from TS 23.246 is copied below for information.

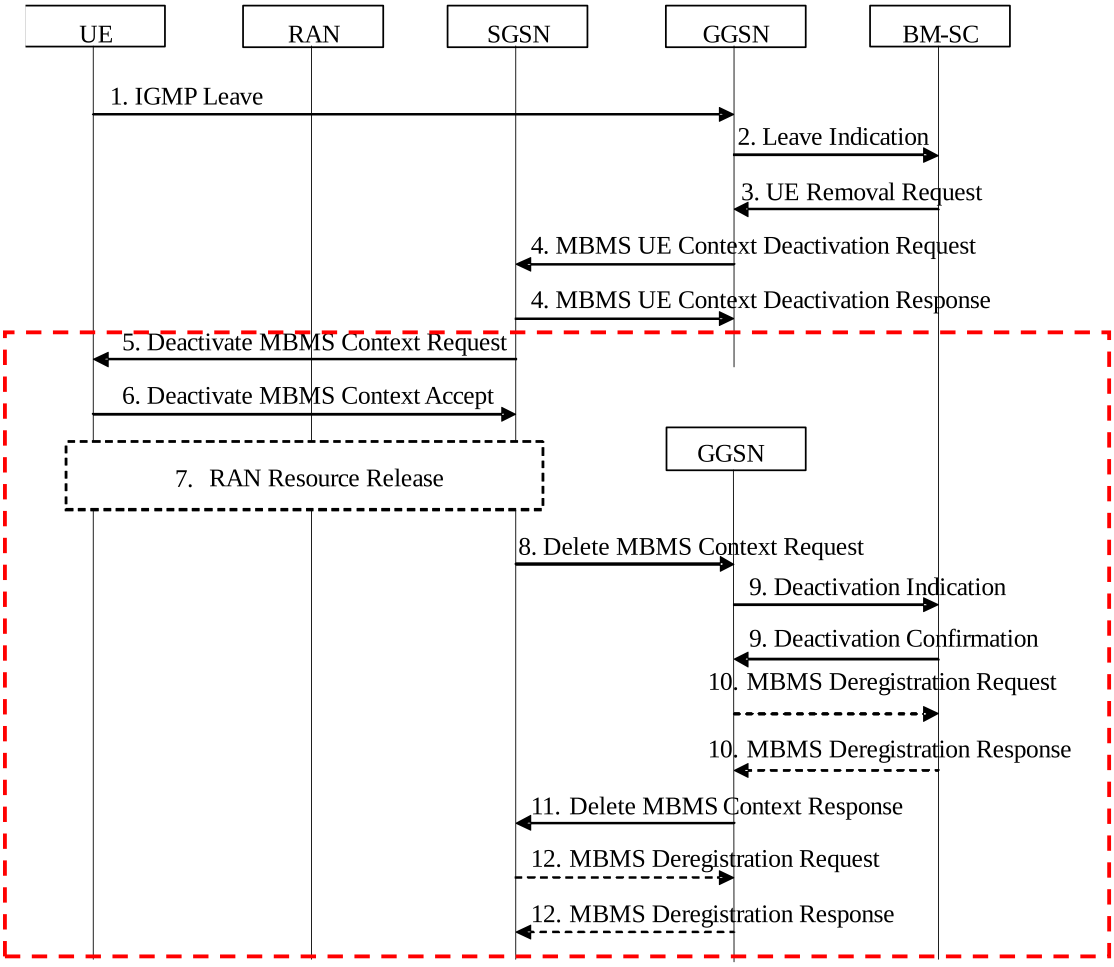
UE
RAN
SGSN
GGSN
BM-SC
1. IGMP Leave
2. Leave Indication
3. UE Removal Request
4. MBMS UE Context Deactivation Request
4. MBMS UE Context Deactivation Response
5. Deactivate MBMS Context Request
6. Deactivate MBMS Context Accept
GGSN
7. RAN Resource Release
8. Delete MBMS Context Request
9. Deactivation Indication
9. Deactivation Confirmation
10. MBMS Deregistration Request
10. MBMS Deregistration Response
11. Delete MBMS Context Response
12. MBMS Deregistration Request
12. MBMS Deregistration Response

Figure 1: MBMS Multicast Service Deactivation

In the stage 3 specification, the GGSN sends a deactivation message to SGSN (step 4 in the Figure 1) after evaluating whether the GGSN to deactivate the MBMS UE context is the SAME or DIFFERENT from the one that received IGMP/MLD leave message. If they are the same, the GGSN initiates to delete its own MBMS UE context by itself and sends a Delete request message to both the SGSN and the BM-SC without waiting for the Delete MBMS Context Request from the SGSN. CN4 believes that this procedure enables to release a network resource quickly and to reduce redundant messages between SGSN and GGSN (ie. step 8 and step 11 in the Figure 1 are removed).

The MBMS Multicast Service Deactivation Flow for when the GGSN is the SAME is shown in Figure 2. The changes are hi-lighted in the dashed-line;

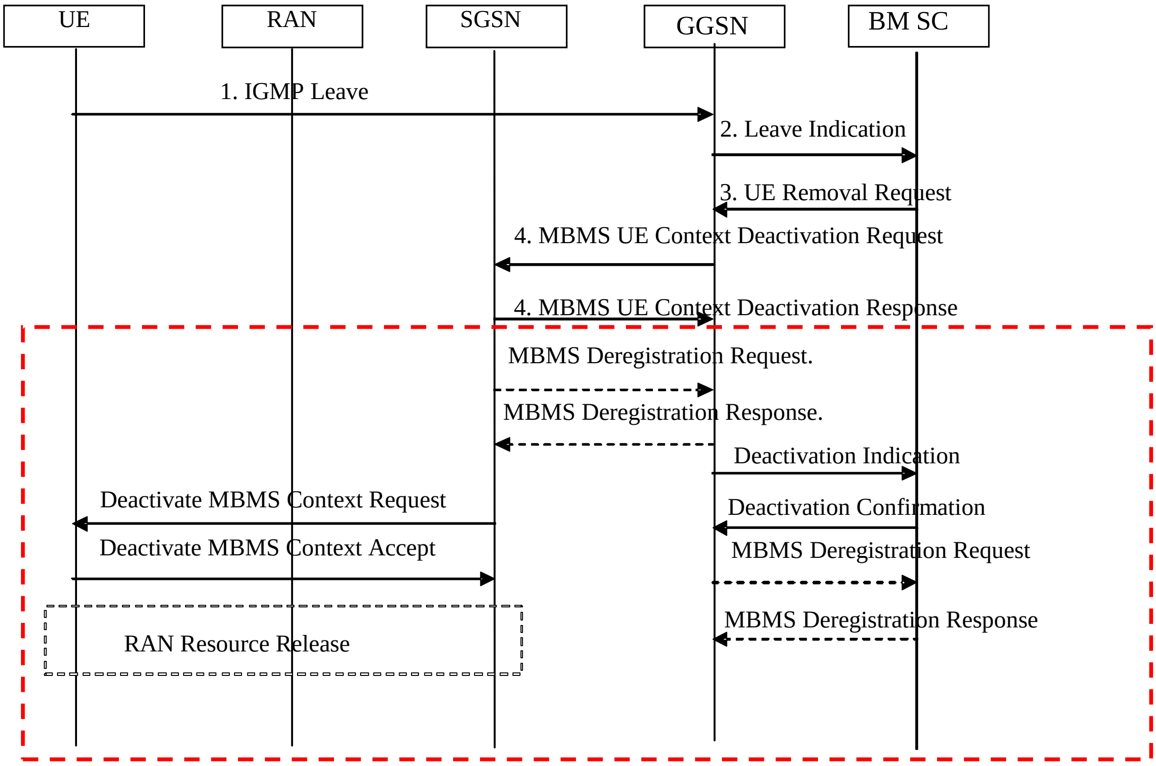
UE
RAN
SGSN
GGSN
BM SC
1. IGMP Leave
2. Leave Indication
3. UE Removal Request
4. MBMS UE Context Deactivation Request
4. MBMS UE Context Deactivation Response
MBMS Deregistration Request.
MBMS Deregistration Response.
Deactivation Indication
Deactivate MBMS Context Request
Deactivation Confirmation
Deactivate MBMS Context Accept
MBMS Deregistration Request
MBMS Deregistration Response
RAN Resource Release

Figure 2: MBMS Multicast Service Deactivation (when the GGSN is the SAME)

2. Actions:

To SA2 group.

ACTION: CN4 kindly asks SA2 group to consider the impact of the change, and guide CN4 if an adverse impact is seen from this change.

3. Date of Next CN4 Meeting:

CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE
CN4 #25	15th – 19th November 2004	TBD, South-Korea

3GPP TS 29.109 V0.2.0 (2004-05~~2~~)

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)

The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Select keywords from list provided in specs database.

Keywords

<keyword[, keyword]>

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.

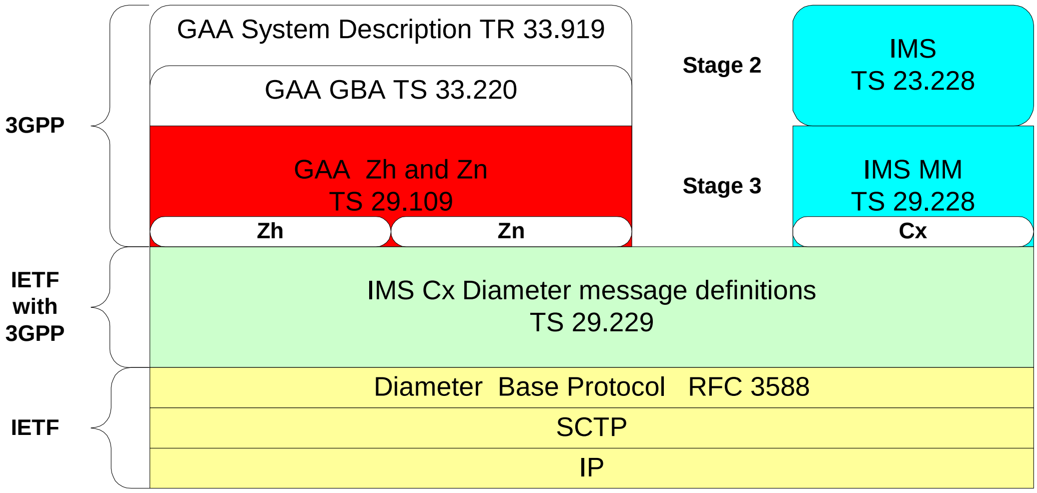

Figure 1.1: Relationships to other specifications

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~~xx.xxx~~: “Bootstrapping interface (Ub) and Network application function interface (Ua);Protocol details”~~; Stage 3”.~~

[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.

~~Editors’ note: The better places for the above definition were some SA3 stage 2 TS.~~

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
~~UserProf(s)~~	~~User's GAA Application Profile(s)~~
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~~xx.xxx~~ [7] and the interface Zh in this specification.

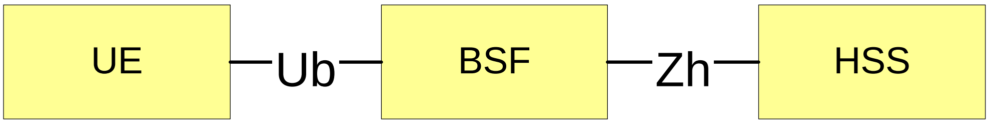

Figure 4.1: Network architecture of bootstrapping procedure

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].

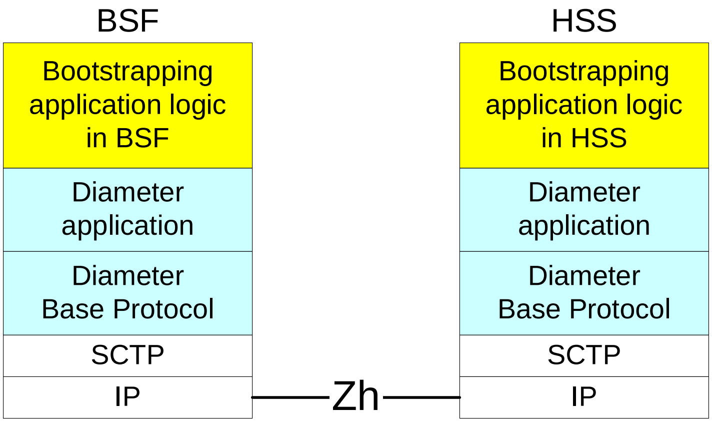

Figure 4.2: Protocol stack of Zh interface

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 ~~application profiles~~ 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 xx.xxx [7]).

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

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

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

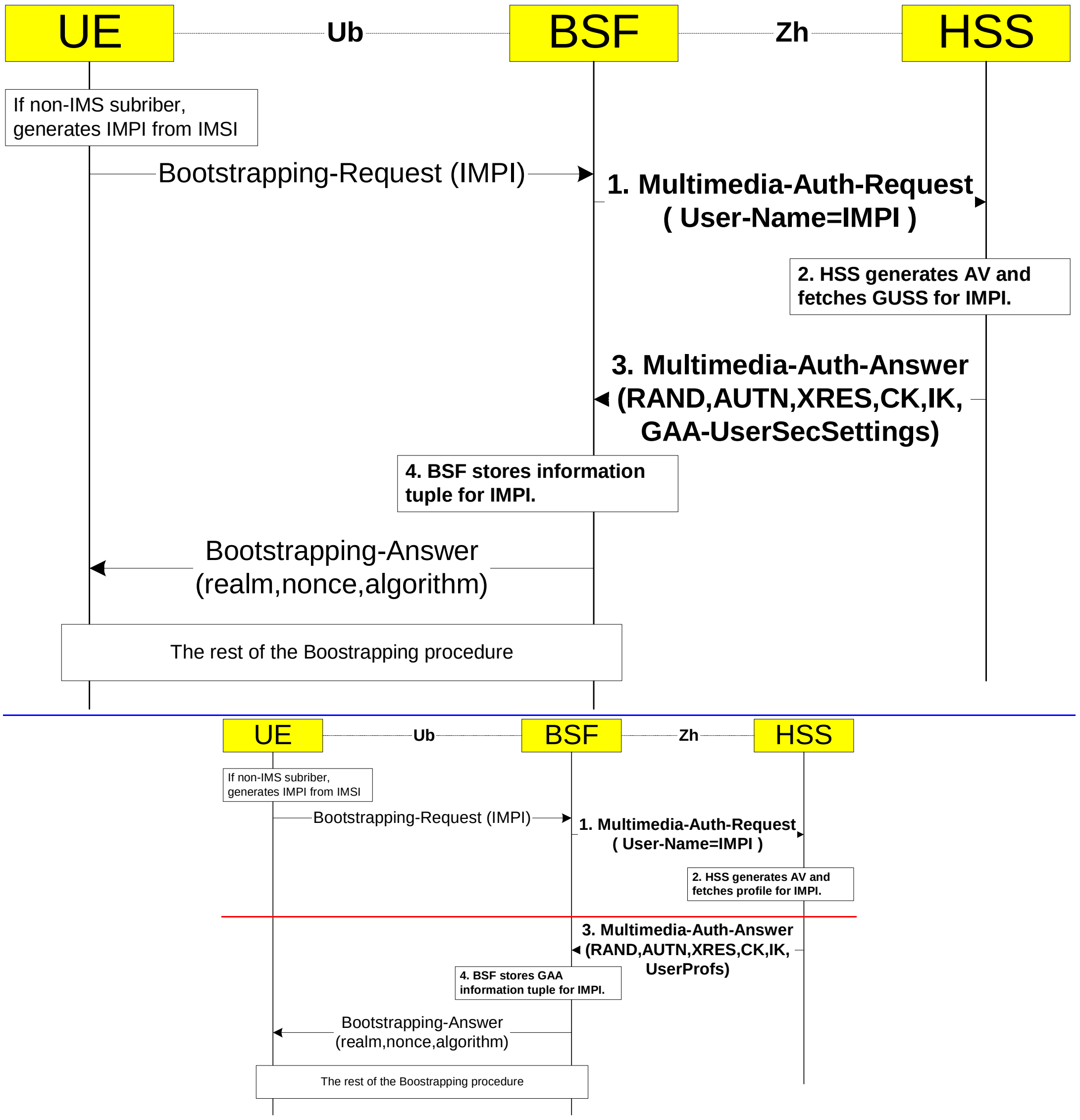
UE
Ub
BSF
Zh
HSS
If non-IMS subriber, generates IMPI from IMSI
Bootstrapping-Request (IMPI)
1. Multimedia-Auth-Request (User-Name=IMPI)
2. HSS generates AV and fetches GUSS for IMPI.
3. Multimedia-Auth-Answer (RAND,AUTN,XRES,CK,IK, GAA-UserSecSettings)
4. BSF stores information tuple for IMPI.
Bootstrapping-Answer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

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
                { Public-Identity~~fier~~ }                  ; Empty value
                [ SIP-Number-Auth-Items]                ; value “1”.
               *[ 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 mandatory Public-Identity may be set to contain non-meaningful "empty" value because the Bootstrapping application logic in the HSS does not check, as IMS MM application does, coherence of the IMPI and the User Public Identity (IMPU). Because the bootstrapping procedure requires only one authentication vector the SIP-Number-Auth-Items AVP may be omitted or set to 1 (default) according 3GPP TS 29.229 [3].

Step 2

When the HSS receives the MAR message, the HSS shall derive the user Authentication Vector (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 ~~Application Profiles~~ into the GAA-UserSecSettings~~Application-Profiles~~.

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 ]         ; value "1"
                     [ SIP-Auth-Data-Item ]            ; one user's AV
                     [ GAA-UserSecSettings~~Application-Profiles~~ ]  ; GUSS~~GAA-Application-Profiles~~
                     ~~(UserProfs)~~
                     *[ 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 only required authentication vector is send in the SIP-Auth-Data-Items AVP and the AVP SIP-Number-Auth-Items AVP may be omitted or set to 1 (default). The ~~user's all GAA application~~ security settings of user's all GAA applications are ~~profiles are~~ send in GAA-UserSecSettings~~Application-Profiles~~ 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~~UserProfs~~> 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.

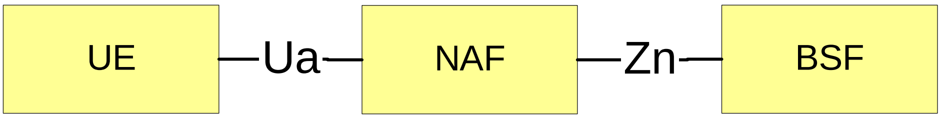

Figure 5.1: Network architecture of GAA application

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].

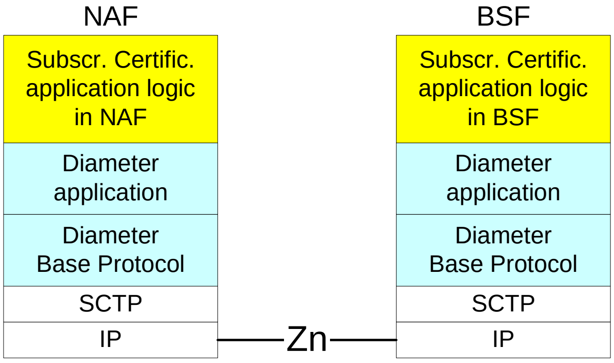

Figure 5.2: Protocol stack of Zn interface

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 ~~profile~~ 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~~user GAA profile (UserProf)~~.
- 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.

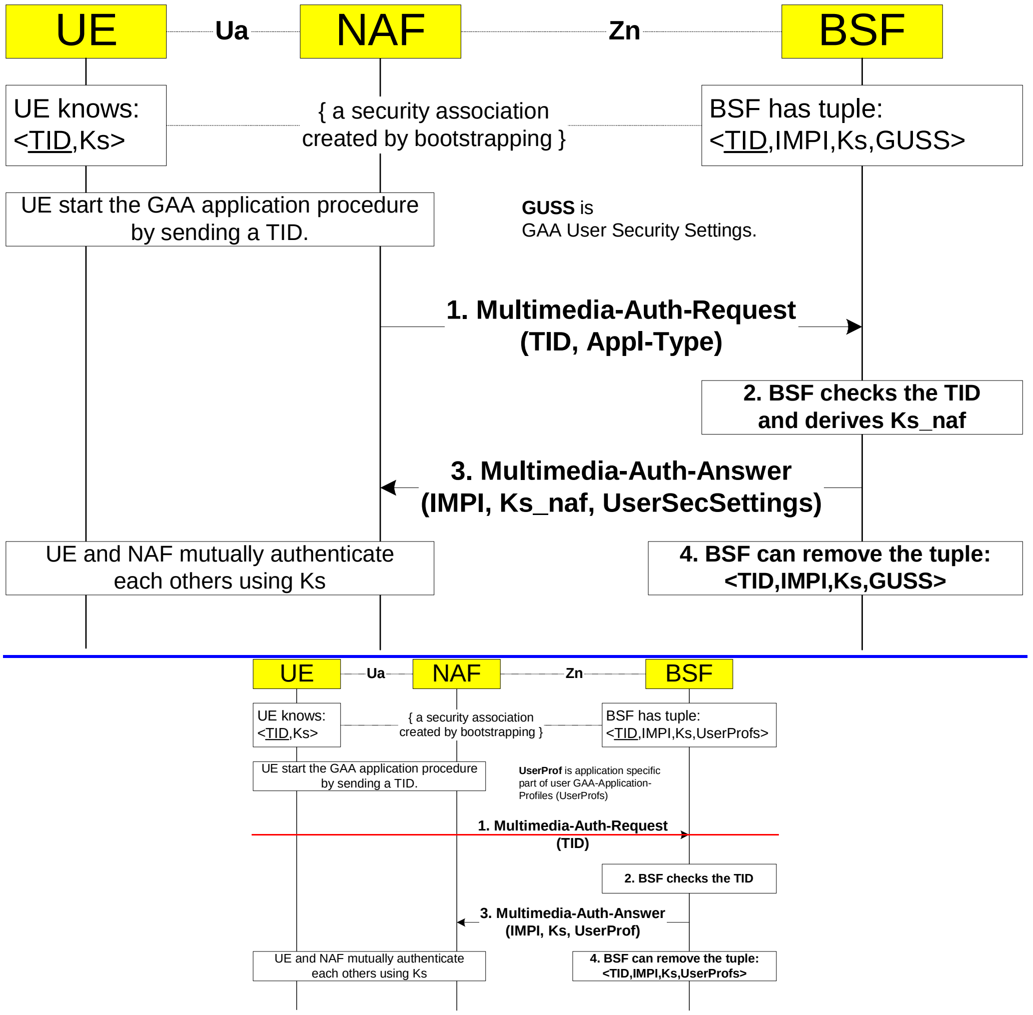
UE
Ua
NAF
Zn
BSF
UE knows: <TID,Ks>
{ a security association created by bootstrapping }
BSF has tuple: <TID,IMPI,Ks,GUSS>
UE start the GAA application procedure by sending a TID.
GUSS is GAA User Security Settings.
1. Multimedia-Auth-Request (TID, Appl-Type)
2. BSF checks the TID and derives Ks_naf
3. Multimedia-Auth-Answer (IMPI, Ks_naf, UserSecSettings)
UE and NAF mutually authenticate each others using Ks
4. BSF can remove the tuple: <TID,IMPI,Ks,GUSS>
UE
Ua
NAF
Zn
BSF
UE knows: <TID,Ks>
{ a security association created by bootstrapping }
BSF has tuple: <TID,IMPI,Ks,UserProfs>
UE start the GAA application procedure by sending a TID.
UserProf is application specific part of user GAA-Application-Profiles (UserProfs)
1. Multimedia-Auth-Request (TID)
2. BSF checks the TID
3. Multimedia-Auth-Answer (IMPI, Ks, UserProf)
UE and NAF mutually authenticate each others using Ks
4. BSF can remove the tuple: <TID,IMPI,Ks,UserProfs>

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
                { User-Name }                             ; Empty value
                { Public-Identity~~fier~~ }                   ; Empty value
                [ GAA-Application-Type~~Id~~ ]                ; Application's type~~identifier~~
                [ 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 3GPP TS 29.229 [3] defines the User-Name and Public-Identity AVPs as mandatory. The mandatory User-name and Public-Identity AVPs may be set to contain non-meaningful "empty" value in this context.

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~~UserProfs~~> 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 ~~profile~~ according the request's GAA-Application-Type~~Id~~ AVP to XXX-UserSecSettings~~profiles~~ 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~~Profile~~ ]    ; XXX application's User Security
                Settings~~profile (UserProf)~~
                *[ 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~~profile~~ to the XXX-UserSecSettings~~Profile~~ from stored GAA-UserSecSettings ~~Application-Profiles (UserProfs)~~ according the GAA-Application-Type~~Id~~ 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~~UserProfs~~> 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~~USER~~_UNKNOWN (5401)

A message was received for an IMPI ~~user~~ 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~~AA_PROFILES~~_UNKNOWN (5403)

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

6.2.2.4 DIAMETER_ERROR_USS~~APPLICATION_PROFILE~~_UNKNOWN (5404)

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

6.2.2.5~~4~~ DIAMETER_ERROR_NOT_SUPPORTED_USS~~USER~~_DATA (5405~~9~~)

The BSF/NAF informs HSS/BSF that the received User Security Settings ~~GAA profile~~ information, which was not recognised or not supported or~~ is~~ 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~~Application-Profiles~~	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~~Id~~	403	6.3.1.4	Enumerated	M,V				No
SSC-UserSecSettings~~Profile~~	410	6.3.2.1	Grouped	M, V				No
SSC-UserSecSettings~~Profile~~-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~~Application-Profiles~~ AVP

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

```
<GAA-UserSecSettings~~Application-Profiles~~>::=<AVP header: 400>
                 [SSC-UserSecSettings~~Profile~~]
                 *[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~~Id~~ AVP

The GAA-Application-Type~~Id AVP~~ 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 ~~GAA~~ application's user security settings~~profile~~ or no GAA user security settings~~profiles~~. The following values are defined with default value 0:

APPLICATION_WITHOUT_GUSS~~AA_PROFILE~~ (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~~Profile~~ AVP

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

6.3.2.2 SSC-UserSecSettings~~Profile~~-Home-Network AVP

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

```
     <SSC-UserSecSettings~~Profiles~~>::=<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~~Profile~~ 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~~profile~~ downloaded over the Zh interface and describe the purpose of the different information classes included in the user's GAA security settings~~profile~~.

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

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

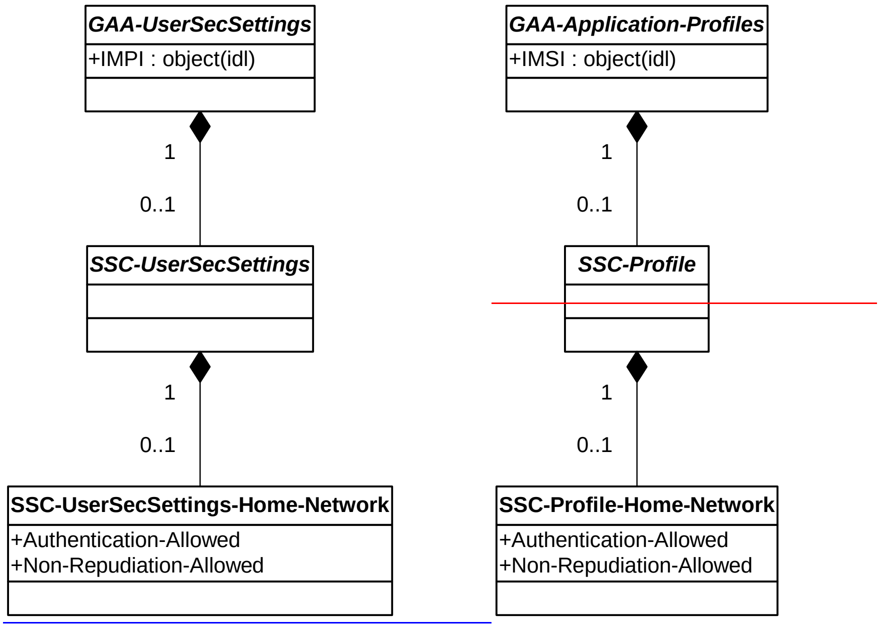

Figure 1: The structure of the GAA User Security Settings~~application profile~~

The SSC-UserSecSettings~~Profile~~ definition for home network is called **SSC-UserSecSettings~~Profile~~-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~~profiles~~ 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~~Profile~~-*-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*

3GPP TSG CN WG4 Meeting #23 ***N4-040572***
Zagreb, Slovenia, 10th – 14st May 2004

Source: Nokia

Title: TS 29.109 – Terminological Changes

Agenda item: 6.7

Document for: Discussion and decision

1. Introduction

The version of TS 29.109 contains following mainly editor changes to revision 0.2.0 refered as current version.

2. Corrections and technical updates

2.1 IMSI fixed to IMPI in figure

Currently figure 1 in Annex A contains incorrectly (typing error) IMSI, which should be IMPI.

2.2 Added definition to chapter 3.1 definition

Bootstrapping information consists of a Transaction Identifier (TID), a Key material (Ks_naf) and an application specific user security settings identified by TID.

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.

2.3 Failure name changed

Name of Permanent failure cause “DIAMETER_ERROR_USER_UKNOWN” changed to “DIAMETER_ERROR_IMPI_UKNOWN “ in chapter 6.2.2.

2.4 Reference [7] fixed

TS number is missing in current reference [7] in references chapter 2.
Now TS 29.xxx is determined to be TS 24.109:

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

3. Terminolgical changes

3.1 User Profile changed to User Security Settings

Operator may set GAA application depending security specific control information (e.g. flags) to control the usage of application to the HSS. Current version uses term “Profile” about these security specific control information. This information can be terminologcally mixed with non-security specify user profiles. That is way the following terminolgical changes from “profile” to “User Security Settings” is proposed. The following tbale summaries the detailled implemntation of this changes. If some abbreviation is used e.g. in figures it is marked by parenthsis.

Old terms in 0.2.0	**Corresponding new terms**
GAA-Application-Profiles (UserProfs)	GAA-UserSecSettings (GUSS)
XXX-Profile (UserProf)	XXX-UserSecSettings (USS)
SSC-Profile	SSC-UserSecSettings
SSC-Profile-Home-Network	SSC-UserSecSettings-Home-Network

The abbreviation GUSS and USS are also added to abbreviation list.

3.2 GAA-Application-Id to -Type

Currently TS 29.109 v0.2.0 calls the AVP that is used in Zn request message to indicate to BSF the application of the NAF (Subscriber Certificate, Presence, MBMS,….) is called to “GAA-Application-Id”. This may be sometimes misleading because somebody may think occurrences of the application (Presence service in NAF1 and in NAF2) rather than the application type itself.

The “**GAA-Application-Id**” is changes to more unambiguous name for this AVP is “**GAA-Application-Type**”.

3GPP TSG CN WG4 Meeting #23 ***N4-040748***
Zagreb, CROATIA, 10th – 14th MAY 2004

Title:	**[DRAFT]** LS on Requirement for presence of the GAA-Application-Type AVP
Release:	Release 6
Work Item:	GAA
Source:	CN4
To:	SA3

Contact Person:

Name: Dan Warren, Vodafone
Tel. Number: +44 7795 300783
E-mail Address: dan.warren@vodafone.com

Attachments: N4-040572.

1. Overall Description:

At CN4 #23, document N4-040572 was discussed. This document proposes updates to TS29.109, the Generic Authentication Architecture Stage 3 document. Within this document, the GAA-Application-Id AVP is redefined as the GAA-Application-Type AVP.

During the meeting there was discussion of the intent of Generic Authentication Architecture and whether there should be content included that is application specific (and therefore not generic). Two possible interpretations were put forward. Either;-

- Generic Authentication Architecture is a generic architecture to be used for authentication, and so the authentication data could be application specific.

Or

- Generic Authentication Architecture is an architecture that allows for generic authentication, and so the authentication data defined would be applied the same way regardless of application.

It is not clear from the stage 2 documentation which of these two understandings is the real intent of GAA work. The fact that the HSS is providing the same parameters for authentication regardless of application suggests the latter understanding, but the requirement for the inclusion of an identification of application type suggests the former.

If the latter of the two possible interpretations is correct, there would seem to be no requirement for an indication of application type to be transported, in which case the AVP highlighted above in N4-040572 would be redundant information and would not fit with the generic nature of GAA.

2. Actions:

To SA3 group.

ACTION: CN4 asks SA3 to provide guidance to CN4 on which of the two understandings of the intent of GAA is correct.

3. Date of Next CN4 Meeting:

CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE
CN4 #25	15th – 19th November 2004	TBD, South-Korea

3GPP TSG CN WG4 Meeting #23
Zagreb, Croatia, 10th – 14th May 2004

N4-040747

Title:	Managing of Metadata: New Procedures vs. Metadata GUP Components.
Release:	Rel-6
Work Item:	GUP
Source:	CN4
To:	SA2
Cc:	

Contact persons:

Name:	Ari Laine
Tel. Number:	+358 50 3878646
E-mail Address:	ari.p.laine@nokia.com
Name:	Zdravko Jukic
Tel. Number:	+46 70 3595439
E-mail Address:	zdravko.jukic@ericsson.com

Attachments: none

1. Overall Description:

The metadata, as it is used in this discussion paper, is information about GUP Components. A collection of metadata for a certain purpose could be viewed as a metadata type, e.g. information about physical storage location of the GUP Components.

There is a need to manage that metadata information.

Approach 1:

Existing GUP procedures and dedicated metadata GUP Components together fulfil the need to manage the metadata information. In this approach GUP interface remains unchanged when new metadata type needs to be introduced. For new metadata type the new GUP Component needs to be specified. This is done in a same fashion as for any other GUP Component. This approach is in line with the stage 2 document which and reuses the current set of operations.

Approach 2:

Alternative idea is to extend the basic set of GUP procedures with additional dedicated procedures for metadata management. For each type of metadata a new set of dedicated procedures (addXXX, listXXX and deleteXXX) needs to be specified. Whenever there is a need to change any existing or to add a new metadata type, stage 2 document may need to be updated.

2. Actions:

CN4 kindly asks SA2 to provide some guidance on the issue of managing of metadata. More specifically, CN4 would like to receive from SA2 some recommendation in terms of which solution is more appropriate.

3. Date of Next CN4 Meeting:

CN4#24	16-20 August 2004	Sophia, France.

3GPP TSG CN WG4 Meeting #23 Zagreb, CROATIA, 10th – 14th MAY 2004

N4-040746

Title:	**[DRAFT]** Reply LS on the nature of LCS
Response to:	LS (S2-041015) on the nature of LCS from SA2.
Source:	CN4
To:	SA2
Cc:	SA1, CN1, GERAN, GERAN2

Contact Person:

Name:	Dan Warren, Vodafone
Tel. Number:	+44 7795 300783
E-mail Address:	dan.warren@vodafone.com

1. Overall Description:

CN4 thank SA2 for their LS on the Nature of LCS (S2-041015) and also thank CN1 and GERAN for their responses (N1-040658 and GP-041244) to the original SA2 LS.

Similar to the GERAN response, CN4 have taken the view that LCS is not a supplementary service as such (rather more a network capability), but uses tools defined for identification of supplementary services to indicate support (or not) of LCS within the core network and to communicate the features that are to be employed by the network in providing location information for a subscriber. In particular, MAP protocol (TS 29.002) defines a supplementary service code set for the identification of the specific variants and options of the LCS service that are required to be employed within sections 7.6.3.62, 7.6.3.62A, 7.6.4.1, 7.6.4.44 and 7.6.4.45, but the understanding of CN4 is that LCS is not a Supplementary Service itself.

CN4 does not propose any changes to any of the specs under CN4 control. Given the existing understanding in CN4, which is reinforced by the detailed analysis provided by GERAN, CN4 believes that the nature of LCS will be clearly identified following any improvements to stage 1 and/or 2 specifications that are deemed necessary after this LS exchange. CN4 does not feel that any clarification of the nature of LCS is appropriate for inclusion in CN4 controlled specifications.

2. Actions:

None

3. Date of Next CN4 Meeting:

CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE
CN4 #25	15th – 19th November 2004	TBD, South-Korea

3GPP TS 29.230 V0.4.0 (2004-05)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network
Diameter applications;
3GPP specific codes and identifiers
(Release 6)

Keywords

<keyword[, keyword]>

3GPP

Postal address

3GPP support office address

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

Internet

http://www.3gpp.org

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document lists the 3GPP specific Diameter protocol codes, including the AVP codes and Experimental result codes.

This document lists also the application identifiers assigned to 3GPP specific Diameter applications by IANA and the Diameter command code range which is assigned to 3GPP by IANA.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 29.228: " IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents"

[2] 3GPP TS 29.229: " Cx and Dx interfaces based on the Diameter protocol; Protocol details"

[3] 3GPP TS 29.328: " IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents"

[4] 3GPP TS 29.329: " Sh Interface based on the Diameter protocol; Protocol details"

[5] 3GPP TS 32.225: " Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)"

[6] 3GPP TS 29.234: "3GPP System to WLAN Interworking; Stage 3 Description"

[7] 3GPP TS 29.109: " Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Protocol details "

[8] 3GPP TS 29.209: " Technical Specification Group Core Network; Policy control over Gq interface"

[9] IETF RFC 3588: "Diameter Base Protocol"

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

[11] IANA's Enterprise-Numbers: http://www.iana.org/assignments/enterprise-numbers

[12] IANA's AAA parameters register: ftp://ftp.iana.org/assignments/aaa-parameters/

3 Definitions and abbreviations

3.1 Definitions

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

3GPP specific: A definition which is used in conjunction with the 3GPP's vendor identifier.

3.2 Abbreviations

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

AVP	Attribute-Value-Pair
IANA	Internet Assigned Numbers Authority

4 Application identifiers

The Diameter applications are identified with the application identifiers as specified in the RFC 3588 [9]. There are two kind of applications: IETF standards track applications and vendor specific applications. All application identifiers are assigned by IANA [12]. This chapter lists the application identifiers asigned by IANA to all 3GPP Diameter applications.

The application identifiers are transferred in Diameter command's header in the Application-ID field.

4.1 3GPP specific application identifiers

The 3GPP specific application identifiers allocated by IANA are listed in the following table.

Table 4.1: 3GPP specific application identifiers

Application identifier	Application	3GPP TS
167772151	3GPP Cx/Px	29.228 [1] and 29.229 [2]
167772152	3GPP Sh/Ph	29.328 [3] and 29.329 [4]
167772153	3GPP Rf/Ro	32.225 [5]

Editors note: The following applications are under development and they don't have the application id yet.

	3GPP Wx	29.234 [6]
	3GPP Zn	29.109 [7]
	3GPP Zh	29.109 [7]
	3GPP Gq	29.209 [8]

5 Command codes

The command codes are used for communicating the command associated with the Diameter message. The command code is carried in the Diameter header's Command-Code field. The command codes can be divided into standard command codes allocated by IANA and experimental command codes for testing purposes only.

5.1 Command codes allocated for 3GPP

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

Table 5.1: Command codes allocated for 3GPP

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

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

310			
311			
312			
313			

6 Vendor identifier

The vendor identifier (a.k.a Enterprise number) indicates the vendor specific attributes, result codes and application identifiers in Diameter commands. The vendor identifier is used in the Vendor-ID field of the AVP header and in the Vendor-Id AVP. The Vendor-Id AVP is used to identify the vendor in the Vendor-Specific-Application-Id and Experimental-Result-Code grouped AVPs.

6.1 3GPP's vendor identifier

The IANA has allocated a vendor identifier value 10415 for 3GPP [11].

7 Attribute-Value-Pair codes

The AVP codes are used together with the vendor identifier to identify each attribute uniquely. There are multiple AVP namespaces. The IETF IANA namespace, that is, the AVPs with vendor identifier zero or without vendor identifier, is controlled by IANA. Each vendor controls the AVP codes within their AVP namespaces.

7.1 3GPP specific AVP codes

The 3GPP specific AVPs have the Vendor-Specific bit ('V' bit) set in the AVP header and they carry the 3GPP's vendor identifier in the Vendor-ID field of the AVP header. The 3GPP specific AVP codes are presented in the following table.

Table 7.1: 3GPP specific AVP codes

AVP Code	Attribute Name	Data Type	Specified in the TS
1	Visited-Network-Identifier	OctetString	29.229 [2]
2	Public-Identity	UTF8String	
3	Server-Name	UTF8String	
4	Server-Capabilities	Grouped	
5	Mandatory-Capability	Unsigned32	
6	Optional-Capability	Unsigned32	
7	User-Data	OctetString	
8	SIP-Number-Auth-Items	Unsigned32	
9	SIP-Authentication-Scheme	UTF8String	
10	SIP-Authenticate	OctetString	
11	SIP-Authorization	OctetString	
12	SIP-Authentication-Context	OctetString	
13	SIP-Auth-Data-Item	Grouped	
14	SIP-Item-Number	Unsigned32	
15	Server-Assignment-Type	Enumerated	
16	Deregistration-Reason	Grouped	
17	Reason-Code	Enumerated	
18	Reason-Info	UTF8String	
19	Charging-Information	Grouped	
20	Primary-Event-Charging-Function-Name	DiameterURI	
21	Secondary-Event-Charging-Function-Name	DiameterURI	
22	Primary-Charging-Collection-Function-Name	DiameterURI	
23	Secondary-Charging-Collection-Function-Name	DiameterURI	
24	User-Authorization-Type	Enumerated	
25	User-Data-Request-Type	Enumerated	
26	User-Data-Already-Available	Enumerated	
27	Confidentiality-Key	OctetString	
28	Integrity-Key	OctetString	
Note: The AVP codes from 29 to 99 are reserved for TS 29.229.			
100	User-Identity	Grouped	29.329 [4]
101	MSISDN	OctetString	
102	User-Data	OctetString	
103	Data-Reference	Enumerated	
104	Service-Indication	OctetString	
105	Subs-Req-Type	Enumerated	
106	Requested-Domain	Enumerated	
107	Current-Location	Enumerated	
108	Identity-Set	Enumerated	
Note: The AVP codes from 109 to199 are reserved for TS 29.329.			
			32.225 [5]
Note: The AVP codes from 200 to 299 are reserved for TS 32.225			
			29.234 [6]
Note: The AVP codes from 300 to 399 are reserved for TS 29.234			
			29.109 [7]
Note: The AVP codes from 400 to 499 are reserved for TS 29.109			
			29.209 [8]
Note: The AVP codes from 500 to 599 are reserved for TS 29.209			

8 Experimental result codes

The Diameter answer messages must carry either Result-Code AVP or Experimental-Result AVP. The values of Result-Code AVP are controlled by IANA. The Experimental-Result AVP is a grouped AVP containing the Vendor-Id AVP and Experimental-Result-Code AVP, thus the experimental result codes are controlled in a vendor-specific manner.

8.1 3GPP specific result codes

The 3GPP specific result codes are always transferred in the Experimental-Result AVP, which has the Vendor-Id with value of 3GPP's vendor identifier. The 3GPP specific result codes shall follow the same classification as defined for the values of Result-Code AVP in IETF RFC 3588 [9]. That means, the result codes are grouped to following ranges:

- 1xxx (Informational)
- 2xxx (Success)
- 4xxx (Transient Failures)
- 5xxx (Permanent Failures)

8.1.1 Informational

The Informational result codes shall use the values from 1001 to 1999 in the Experimental-Result-Code AVP.

Editor's note: No informational result codes have been yet defined in 3GPP.

8.1.2 Success

The Success result codes shall use the values from 2001 to 2999 in the Experimental-Result-Code AVP. The reserved 3GPP specific Success result codes are presented in the following table.

Table 8.1.2: 3GPP specific Success result codes

Experimental Result Code	Result text	Specified in the TS
2001	DIAMETER_FIRST_REGISTRATION	29.229 [2]
2002	DIAMETER_SUBSEQUENT_REGISTRATION	
2003	DIAMETER_UNREGISTERED_SERVICE	
2004	DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED	
2005	DIAMETER_SERVER_SELECTION	
Note: The Experimental Result Codes from 2006 to 2020 are reserved for the TS 29.229.		
		29.109 [7]
Note: The Experimental Result Codes from 2401 to 2420 are reserved for the TS 29.109.		

8.1.3 Transient Failures

The Transient Failure result codes shall use the values from 4001 to 4999 in the Experimental-Result-Code AVP. The reserved 3GPP specific Transient Failure result codes are presented in the following table.

Table 8.1.3: 3GPP specific Transient Failure result codes

Experimental Result Code	Result text	Specified in the TS
4100	DIAMETER_USER_DATA_NOT_AVAILABLE	29.329 [4]
4101	DIAMETER_PRIOR_UPDATE_IN_PROGRESS	
Note: The Experimental Result Codes from 4102 to 4120 are reserved for the TS 29.329.		
		32.225 [5]
Note: The Experimental Result Codes from 41xx to 41yy are reserved for the TS 32.225.		

8.1.4 Permanent Failures

The Permanent Failure result codes shall use the values from 5001 to 5999 in the Experimental-Result-Code AVP. The reserved 3GPP specific Permanent Failure result codes are presented in the following table.

Table 8.1.4: 3GPP specific Permanent Failure result codes

Experimental Result Code	Result text	Specified in the TS
5001	DIAMETER_ERROR_USER_UNKNOWN	29.229 [2]
5002	DIAMETER_ERROR_IDENTITIES_DONT_MATCH	
5003	DIAMETER_ERROR_IDENTITY_NOT_REGISTERED	
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	
5005	DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED	
5006	DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED	
5007	DIAMETER_ERROR_IN_ASSIGNMENT_TYPE	
5008	DIAMETER_ERROR_TOO_MUCH_DATA	
5009	DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA	
5010	DIAMETER_MISSING_USER_ID	
Note: The Experimental Result Codes from 5011 to 5020 are reserved for the TS 29.229.		
		32.225 [5]
Note: The Experimental Result Codes from 5021 to 5040 are reserved for the TS 32.225.		
		29.234 [6]
Note: The Experimental Result Codes from 5041 to 5060 are reserved for the TS 29.234.		
		29.209 [8]
Note: The Experimental Result Codes from 5061 to 5080 are reserved for the TS 29.209.		
5100	DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED	29.329 [4]
5101	DIAMETER_ERROR_OPERATION_NOT_ALLOWED	
5102	DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ	
5103	DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED	
5104	DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED	
5105	DIAMETER_ERROR_TRANSPARENT_DATA OUT_OF_SYNC	
Note: The Experimental Result Codes from 5106 to 5119 are reserved for the TS 29.329.		
		29.109 [7]
Note: The Experimental Result Codes from 5400 to 5419 are reserved for the TS 29.109.		

Annex A (informative): Assignment of the Diameter codes and identifiers in 3GPP

This annex defines the recommended assignment procedure of Diameter codes and identifiers within the 3GPP.

A.1 Application identifiers

If a working group detects it will require a new application identifier, it should contact the 3GPP TSG-CN WG 4 via a Liaison Statement. The LS shall contain the name of the Diameter application and a reference to the corresponding 3GPP TS. The 3GPP TSG-CN WG 4 will then request the application identifier from IANA. When the application identifier will be received, the corresponding working group will be informed by 3GPP TSG-CN WG 4 and the table 4.1 in this specification will be updated.

According to RFC 3588 the creation of a new application should be avoided if at all possible and therefore it is recommended to use the existing application identifiers whenever possible.

A.2 Command codes

If a working group detects there is a need for a new command code(s) from the 3GPP's range, it should contact the 3GPP TSG-CN WG 4 via an LS. The LS shall contain the reference to the 3GPP TS, which specifies the command(s). The 3GPP TSG-CN WG 4 will inform the assigned command code(s) to the corresponding working group and the table 5.1 in this specification will be updated.

It should be noted that the standard command codes allocated for 3GPP are scarce resource and getting new ones would require IETF specification work to be done. Therefore it is recommended to use the existing command codes whenever possible.

A.3 AVP codes

If a working group detects a Diameter application needs new 3GPP specific AVP codes, it should contact the 3GPP TSG-CN WG 4 via an LS. The LS shall contain the name of the Diameter application and a reference to the corresponding 3GPP TS. The 3GPP TSG-CN WG 4 will allocate a range of 100 AVP codes for the application. The range will be informed to the corresponding working group and the table 7.1 will be updated in this specification to show the reserved range. The working group can use the allocated range as a working assumption when defining the actual AVPs.

When the corresponding working group has specified the AVPs, and the specification has been approved and is under CR control, it should inform the AVPs to the 3GPP TSG-CN WG 4 via an LS. The LS should list the used AVP codes in the form of the table 7.1.

If there will be defined new AVPs for a Diameter application through the CR procedure, the assigned AVP range can be used, but the 3GPP TSG-CN WG 4 should be also informed about the new AVP codes via an LS.

Re-using of the existing AVPs is recommended, but special attention should be paid on the use of enumerated AVPs. Defining new values for an enumerated AVP should be agreed case by case with the working group responsible of the particular enumerated AVP. 3GPP TSG-CN WG 4 shall be informed via an LS about the new values assigned to the enumerated AVP.

A.4 Result codes

If a working group detects a Diameter application needs new 3GPP specific result codes, it should contact the 3GPP TSG-CN WG 4 via an LS. The LS shall contain the name of the Diameter application and a reference to the corresponding 3GPP TS. The 3GPP TSG-CN WG 4 will allocate a range of 20 result codes from each required result code group for the application. The ranges will be informed to the corresponding working group and the tables in the chapter 8 of this specification will be updated to show the reserved ranges. The working group can use the allocated ranges as a working assumption when defining the actual result codes.

When the corresponding working group has specified the result codes, and the specification has been approved and is under CR control, it should inform the codes to the 3GPP TSG-CN WG 4 via an LS. The LS should list the used result codes in the form of the tables in chapter 8.

If there will be defined new result codes for a Diameter application through the CR procedure, the assigned result code ranges can be used, but the 3GPP TSG-CN WG 4 should be also informed about the new result codes via an LS.

Re-using of the existing result codes is recommended.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-04					First draft to be presented in CN4#22bis	0.0.0	0.1.0
2004-04					Informative annex added to describe the assignment procedure	0.1.0	0.2.0
2004-04					Annex A improved	0.2.0	0.3.0
2004-05					Ranges of AVP codes and result codes pre-allocated	0.3.0	0.4.0

3GPP TSG CN WG4 Meeting #23 ***N4-040725***
Zagreb, CROATIA, 10th – 14th MAY 2004

Title:	LS on Assignment of the Diameter codes and identifiers
Response to:	LS N3-040346 on Assignment of the Diameter codes and identifiers from CN3.
Release:	Rel-6

Source:	CN4
To:	CN3
Cc:	-

Contact Person:

Name:	Minna Myllymäki
Tel. Number:	+358505216209
E-mail Address:	**minna.myllymaki@nokia.com**

Attachments: N4-040726

1. Overall Description:

CN4 thank CN3 for their quick an clear response to the LS on Assignment of the Diameter codes and identifiers.

CN4 is happy to inform CN3, that the following Diameter code ranges have been allocated for Gq interface (i.e. TS 29.209):

- AVP codes from 500 to 599
- Experimental-Result-Codes from 5061 to 5080 for permanent failures.

(CN4 will also update the TS 29.230 accordingly.)

CN4 would like also to inform CN3, that CN4 will request the Diameter application identifier for Rel-6 Gq interface from IANA. The CN4 will inform the CN3 when the IANA has assigned the application identifier.

2. Action to CN3

When CN3 has specified the AVPs and result codes, and the specification has been approved and is under CR control, it should inform the AVPs and codes to the 3GPP TSG-CN WG 4 via an LS. The LS should list the used result codes in the form of the tables in chapter 8.

3. Date of Next CN4 Meetings:

CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE
CN4 #25	15th – 19th November 2004	TBD, South-Korea

3GPP TSG CN WG4 Meeting #23
Zagreb, CROATIA, 10th – 14th MAY 2004

N4-040713
Revised of N4-040549

CR-Form-v7

CHANGE REQUEST

⌘	**23.003**	**CR**	**088**	⌘**rev**	**1**	⌘	Current version:	**6.2.0** ⌘

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

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

Title:	⌘	Addition of TMGI		
Source:	⌘	Fujitsu		
Work item code:	⌘	MBMS	***Date:*** ⌘	30/4/2004
Category:	⌘	**B**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (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)*

Reason for change:	⌘	In the TS 23.246, TMGI (Temporary Mobile Group Identity) is defined for MBMS notification purpose. However this idetity is missing in TS 23.003.
Summary of change:	⌘	1. The reference to TS 23.246 was added. 2. The definition of TMGI was added.
Consequences if not approved:	⌘	The inconsistency between stage2 and stage3 remains.

Clauses affected:	⌘	1.1.1, 15(new)				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

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

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

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

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

1.1 References

1.1.1 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.905: "3G Vocabulary".

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

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

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

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

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

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

[8] void

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

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

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

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

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

[14] RFC 791: "Internet Protocol".

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

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

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

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

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

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

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

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

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

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

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

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

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

[28] void

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

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

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

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

[33] void

[34] void

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**** Next Change ****

14 Numbering, addressing and identification for 3GPP System to WLAN Interworking

14.1 Introduction

This clause describes the format of the parameters needed to access the 3GPP system supporting the WLAN interworking. For further information on the use of the parameters see 3GPP TS 24.234 [48].

14.2 Home network realm

The home network realm shall be in the form of an Internet domain name, e.g. operator.com, as specified in RFC 1035 [19].

When attempting to authenticate within WLAN access, the WLAN UE shall derive the home network domain name from the IMSI as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>. 3gppnetwork.org" domain name;
3. add the label "wlan." to the beginning of the domain name.

An example of a WLAN NAI realm is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999

Which gives the home network domain name: wlan.mnc015.mcc234.3gppnetwork.org.

14.3 Root NAI

The Root NAI shall take the form of a NAI, and shall have the form username@realm as specified in clause 3 of RFC 2486 [25].

The username part format of the Root NAI shall comply with draft-arkko-pppext-eap-aka [50] when EAP AKA authentication is used and with draft-haverinen-pppext-eap-sim [51], when EAP SIM authentication is used.

When the username part includes the IMSI, the Root NAI shall be built according to the following steps:

1. Generate an identity conforming to NAI format from IMSI as defined in EAP SIM [51] and EAP AKA [50] as appropiate;
2. Convert the leading digits of the IMSI, i.e. MNC and MCC, into a domain name, as described in subclause 14.2.

The result will be a root NAI of the form:

"0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP AKA authentication and
"1<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP SIM authentication

For example, for EAP AKA authentication: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the root NAI then takes the form 0234150999999999@wlan.mnc015.mcc234.3gppnetwork.org.

14.4 Decorated NAI

Editor's note: it is FFS whether selected VPLMN(s) will be indicated in a prefix (i.e. vplmn1.com/vplmn2.com/username@home realm) or in a suffix format (i.e. username@vplmn1.vplmn2.home realm). See draft-adrangi-eap-network-discovery-and-selection [49].

xx Identification of Multimedia Broadcast/Multicast Service

xx.1 Introduction

This clause describes the format of the parameters needed to access the Multimedia Broadcast/Multicast service. For further information on the use of the parameters see 3GPP TS 23.246 [xx].

xx.2 Structure of TMGI

Temporary Mobile Group Identity (TMGI) is used for MBMS notification purpose. The BM-SC allocates a globally unique TMGI per MBMS bearer service.

TMGI is composed of three parts:

1) MBMS Service ID consisting of three octets. MBMS Service ID identifies an MBMS bearer service within the PLMN.

2) Mobile Country Code (MCC) consisting of three digits. The MCC identifies uniquely the country of domicile of the BM-SC;

3) Mobile Network Code (MNC) consisting of two or three digits. The MNC identifies the PLMN which the BM-SC belongs to. The length of the MNC (two or three digits) depends on the value of the MCC.

3GPP TSG-CN WG4 Meeting #23 **N4-040714**
Zagreb, Croatia, 10th – 14th May 2004.

Title:	LS on Clarification of TMGI format
Response to:	
Release:	Rel-6
Work Item:	MBMS
Source:	CN4
To:	RAN2, RAN3
Cc:	CN1

Contact Person:

Name:	Shinichiro Aikawa
Tel. Number:	+81 44 754 8511
E-mail Address:	saikawa@jp.fujitsu.com

Attachments: N4-040713 [CR to TS 23.003]

1. Overall Description:

CN4 would like to inform RAN2 and RAN3 that CN4 approved the attached CR, which proposed the definition of TMGI (Temporary Mobile Group Identity) in TS 23.003. In the TS 23.246, TMGI is defined for MBMS notification purpose. The definition on the structure of the TMGI in the approved CR was based on TR 29.846 which CN1 is working on. CN4 would like to confirm that this structure is in line with relevant specifications in RAN2 and RAN3.

2. Actions:

To RAN2, RAN3 groups.

ACTION:

CN4 asks RAN2 and RAN3 groups to review the attached CR in this LS and send feedback if necessary.

3. Date of Next TSG-CN WG4 Meetings:

CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE
CN4 #25	15th – 19th November 2004	TBD, KOREA

3GPP TSG-CN4 Meeting #23 **Tdoc N4-040699**
Zagreb, Croatia, 10th – 14th May 2004

Title:	Reply to LS on Transfer of T2 GUP TS's
Response to:	LS N4-040653 (T2-040231)
Release:	Rel-6
Work Item:	GUP
Source:	CN4
To:	T2, T, SA2
Cc:	CN

Contact Person:

Name:	**Zdravko Jukic**
Tel. Number:	+46 70 359 5439
E-mail Address:	zdravko.jukic@ericsson.com

Attachments: None.

---

1. Overall Description:

CN4 received the LS N4-040653 (T2-040231) from T2. T2 informed CN4 about the on-going restructuring of T2 and the need of transferring the two T2's GUP TS's to another WG.
TS 23.241, Generic User Profiles Stage 2, Data Description Method, (current version 6.0.0) and TS 24.241, Generic User Profiles Common Objects Stage 3 (current version 0.5.1) need to be transferred to another WG, and this transfer process should be started immediately.

Both documents are closely related to the GUP Stage 3 specification owned by CN4. Therefore the CN4 WG strongly recommends that CN4 WG takes over the responsibility for both specifications.

2. Actions:

To T, T2, SA2 group.

ACTION: CN4 asks SA2, T and T2 groups to initiate the process of transferring the responsibility for both TS 23.241 and TS 24.241 from T2 to CN4.

3. Date of Next TSG-CN4 Meetings:

CN4_24	16th – 20th August 2004	Sophia Antipolis, France (ETSI)
CN4_25	15th – 19th November 2004	Korea

3GPP TSG-CN1 Meeting #34 Tdoc N1-041014, N4-040685
Zagreb, Croatia 10 – 14 May 2004

Title:	LS on MOCN redirect alternatives
Response to:	LS (S2-041676) on Evaluation of MOCN redirect alternatives from SA2
Release:	Release 6
Work Item:	Network Sharing
Source:	CN1 and CN4
To:	SA2, RAN3
Cc:	

Contact Person:

Name: Rouzbeh Farhoumand
Tel. Number: +1 469 682 9924
E-mail Address: rouzbeh.farhoumand@ericsson.com

Attachments:

---

1. Overall Description:

In a joint session between CN1 and CN4 WGs in Zagreb, the Working Groups reviewed the incoming LS in S2-041676 and several related input company contributions. SA2 had the following request to both CN1 and CN4:

ACTION: *SA2 kindly asks CN4 and CN1 to study the two alternatives ("a RAN centric approach" and "a CN centric approach") and possible improvements, and provide guidance on what alternative would be best from CN specifics and protocol point of view (simplest, least impact, best inter-operator interface, etc). This does not preclude CN4 to suggest further solutions.*

After treating the input company contributions evaluating both CN and RAN centric approaches, majority of the companies expressing views were in agreement in recommending the **RAN centric approach** to be selected as the routing mechanism in the MOCN configuration. Given the low frequency of multiple redirects, the RAN centric approach was considered as the preferred method as it is expected to have the least impact on the CN standards, architecture and affected nodes.

In addition, CN1 and CN4 discussed in brief the connection-less interrogation as an optimization and extension to the RAN centric approach, and concluded that SA2 and RAN3 may wish to consider that closer.

2. Actions:

To SA2 group.

ACTION: SA2 is kindly asked to take the recommendation by CN1 and CN4 into account when finalizing the architecture work.

To RAN3 group.

ACTION: RAN3 is kindly asked to take the recommendation by CN1 and CN4 into account during their evaluation process.

3. Date of Next TSG-CN1 Meetings:

CN1_35	16th – 20th August 2004	Sophia Antipolis, France (ETSI)
CN1_36	15th – 19th November 2004	Korea

3GPP TSG CN WG4 Meeting #23 **N4-040664**
Location, Country, Date.

Title:	Reply LS on Harmonisation of AMR Configurations
Response to:	LS S4-040154 on Harmonisation of AMR Configurations
Release:	
Work Item:	
Source:	CN4
To:	SA4
Cc:	SA2

Contact Person:

Name:	Phil Hodges
Tel. Number:	+61404069546
E-mail Address:	Philip.hodges@ericsson.com

Attachments:

---

1. Overall Description:

CN4 thank SA4 for their LS response on harmonisation of AMR configurations. CN4 specification 23.153 already reference the 28.062 specification in section 5.6 “CN Node handling of Codec Types & Codec Modes” when proposing codec configurations and when selecting codec configurations, but this is more of a recommendation than an explicit reference. Thus if changes are made to specify restrictions on AMR configurations in SA4 specifications we would probably need to make this reference clearer and obligatory but the intention would be to continue to reference to SA4 specifications for this as it is seen as stage 3, (application specific) and not stage 2 (procedural). Thus CN4 expect SA4 to specify this in their stage 3 specification, CN4 assumes that TS 26.103 would be the best place for this but ofcourse leaves this decision to SA4.

CN4 also discussed a CR that provides some further clarifications to the handling of the codec mode negotiations to indicate that if an originating node cannot support all subsets of the proposed configurations then it shall indicate the individual subsets that it supports via separate single codec IEs in the Supported Codec List. This clarification was agreed to be incorporated in Rel4 version onwards and so this should ensure backward compatibility with any restrictions to the codec mode selection at a Rel6 (onwards) terminating node; in other words CN4 does not believe these changes will cause any backward incompatibilities.

2. Actions:

To SA4 group.

ACTION: CN4 asks SA4 group to inform us when they have completed this work and provide CN4 with the details so that CN4 can then ensure our specifications are updated to point to these changes.

3. Date of Next TSG-CN WG4 Meetings:

TSG-CN4 Meeting #24	16th – 20th August 2004	Sophia Antipolis, France
TSG-CN4 Meeting #25	15th – 19thNovember 2004	Korea

3GPP TSG-CN WG4 Meeting #CN4-22bis **N4-040488**
Edinburg, UK, 19 April 2004.

Title:	**Application Layer vs Transport Layer security for GUP**
Response to:	S3-040199 (N4-040242) LS on GUP security directions
Release:	Rel-6
Work Item:	GUP
Source:	CN4
To:	SA3
Cc:	

Contact Person:

Name: Arnaud SAHUGUET
Tel. Number: +1 908 582 6491
E-mail Address: sahuguet@lucent.com

Attachments: **none**

---

1. Overall Description:

For TS 29.240, CN4 needs to define some security mechanisms to permit the secure and authenticated exchange of information between client applications, GUP servers and GUP data sources.
There seems to be 3 options:

- transport level security using SSL/TLS; in this scenario, client and server authenticates over a secure HTTP connection and exchange over the wire plain text (i.e. not encrypted) SOAP messages.
- Application level security using WS-Security; in this scenario, client and server exchange over the wire some encrypted SOAP messages.
- A combination of both.

2. Actions:

To SA3 group.

ACTION:

CN4 asks SA3 for the status within SA3 regarding the security requirements concerning GUP.
More specifically, CN4 would like to know what kind of security mechanism(s) will be recommended by SA3 for GUP security.

3. Date of Next CN4 Meetings:

CN4 #23	10th – 14th May 2004	Zagreb, CROATIA
CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE

3GPP TSG-CN WG4 Meeting #CN4-22bis **N4-040487**
Edinburgh, UK, 19 April 2004.

Title:	**Provisioning Function for Physical Storage of GUP components**
Response to:	-
Release:	Rel-6
Work Item:	GUP
Source:	CN4
To:	SA1, SA2
Cc:	

Contact Person:
Name: Arnaud SAHUGUET
Tel. Number: +1 908 582 6491
E-mail Address: sahuguet@lucent.com

Name: Nick Russell
Tel. Number: +44 7748938929
E-mail Address: nick.russell@vodafone.com

Attachments: **none**

1. Overall Description:

For TS 29.240, CN4 would like to define the mechanism(s) by which the GUP server knows about where the various GUP components are physically stored. Based on these mappings, the GUP server will be able to route requests from applications to the corresponding data sources.
In the SA1 and SA2 documents (TS22.240, TS 23.240), there is no explicit requirement for a method/function to inform the GUP server about the physical location of the GUP components.

CN4 thinks that the existence and standardisation of such a method/function is critical for GUP interworking and can be implemented with minimal work (reusing already existing interfaces) and without further delay (Release 6 time frame).

2. Actions:

To SA1, SA2 groups.

ACTION:

1. CN4 asks SA1 and/or SA2 to consider adding a requirement to provision this.
2. CN4 also asks SA1 and SA2 to confirm our intended reuse of the Rg interface for this purpose.

3. Date of Next CN4 Meetings:

CN4 #23	10th – 14th May 2004	Zagreb, CROATIA
CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE

3GPP TSG CN WG4 Meeting #22bis **_N4-040473_**
Edinburgh, UK, 14th – 20th April 2004

Title:	LS on WLAN Charging Identifiers
Release:	Rel-6
Source:	CN4
To:	SA5, SA1
Cc:	SA2

Contact Person:
Name: Jouni korhonen
Tel. Number: +358 40 5344455
E-mail Address: Jouni.korhonen@teliasonera.com

Attachments:

1. Overall Description:

CN4 understands that some charging should take place in the VPLMN related to a subscribers WLAN-IW usage. It is unclear; however, to CN4 which identities should be used in this charging process. For example, should the MSISDN or IMSI be used for this purpose?

2. Actions:

To the SA5, SA1 group.

ACTION: CN4 kindly asks the SA5 and SA1 working group to give guidance as to which identity/identities should be used at the VPLMN (WAG/AAA-proxy) in order to perform charging. Further, CN4 would appreciate if SA5 could indicate whether the VPLMN charging solution in WLAN-IW corresponds with other inter-operator roaming based solutions?

3. Date of Next CN4 Meeting:

CN4 #23	10th – 14th May 2004	Zagreb, CROATIA
CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE

3GPP TS 29.230 V0.3.0 (2004-04)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network
Diameter applications;
3GPP specific codes and identifiers
(Release 6)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

<keyword[, keyword]>

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

Copyright Notification

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document lists the 3GPP specific Diameter protocol codes, including the AVP codes and Experimental result codes.

This document lists also the application identifiers assigned to 3GPP specific Diameter applications by IANA and the Diameter command code range which is assigned to 3GPP by IANA.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 29.228: " IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents"

[2] 3GPP TS 29.229: " Cx and Dx interfaces based on the Diameter protocol; Protocol details"

[3] 3GPP TS 29.328: " IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents"

[4] 3GPP TS 29.329: " Sh Interface based on the Diameter protocol; Protocol details"

[5] 3GPP TS 32.225: " Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)"

[6] 3GPP TS 29.234: "3GPP System to WLAN Interworking; Stage 3 Description"

[7] 3GPP TS 29.109: " Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Protocol details "

[8] 3GPP TS 29.209: " Technical Specification Group Core Network; Policy control over Gq interface"

[9] IETF RFC 3588: "Diameter Base Protocol"

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

[11] IANA's Enterprise-Numbers: http://www.iana.org/assignments/enterprise-numbers

[12] IANA's AAA parameters register: ftp://ftp.iana.org/assignments/aaa-parameters/

3 Definitions and abbreviations

3.1 Definitions

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

3GPP specific: A definition which is used in conjunction with the 3GPP's vendor identifier.

3.2 Abbreviations

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

AVP	Attribute-Value-Pair
IANA	Internet Assigned Numbers Authority

4 Application identifiers

The Diameter applications are identified with the application identifiers as specified in the RFC 3588 [9]. There are two kind of applications: IETF standards track applications and vendor specific applications. All application identifiers are assigned by IANA [12]. This chapter lists the application identifiers asigned by IANA to all 3GPP Diameter applications.

The application identifiers are transferred in Diameter command's header in the Application-ID field.

4.1 3GPP specific application identifiers

The 3GPP specific application identifiers allocated by IANA are listed in the following table.

Table 4.1: 3GPP specific application identifiers

Application identifier	Application	3GPP TS
167772151	3GPP Cx/Px	29.228 [1] and 29.229 [2]
167772152	3GPP Sh/Ph	29.328 [3] and 29.329 [4]
167772153	3GPP Rf/Ro	32.225 [5]

Editors note: The following applications are under development and they don't have the application id yet.

	3GPP Wx	29.234 [6]
	3GPP Zn	29.109 [7]
	3GPP Zh	29.109 [7]
	3GPP Gq	29.209 [8]

5 Command codes

The command codes are used for communicating the command associated with the Diameter message. The command code is carried in the Diameter header's Command-Code field. The command codes can be divided into standard command codes allocated by IANA and experimental command codes for testing purposes only.

5.1 Command codes allocated for 3GPP

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

Table 5.1: Command codes allocated for 3GPP

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

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

310			
311			
312			
313			

6 Vendor identifier

The vendor identifier (a.k.a Enterprise number) indicates the vendor specific attributes, result codes and application identifiers in Diameter commands. The vendor identifier is used in the Vendor-ID field of the AVP header and in the Vendor-Id AVP. The Vendor-Id AVP is used to identify the vendor in the Vendor-Specific-Application-Id and Experimental-Result-Code grouped AVPs.

6.1 3GPP's vendor identifier

The IANA has allocated a vendor identifier value 10415 for 3GPP [11].

7 Attribute-Value-Pair codes

The AVP codes are used together with the vendor identifier to identify each attribute uniquely. There are multiple AVP namespaces. The IETF IANA namespace, that is, the AVPs with vendor identifier zero or without vendor identifier, is controlled by IANA. Each vendor controls the AVP codes within their AVP namespaces.

7.1 3GPP specific AVP codes

The 3GPP specific AVPs have the Vendor-Specific bit ('V' bit) set in the AVP header and they carry the 3GPP's vendor identifier in the Vendor-ID field of the AVP header. The 3GPP specific AVP codes are presented in the following table.

Table 7.1: 3GPP specific AVP codes

AVP Code	Attribute Name	Data Type	Specified in the TS
1	Visited-Network-Identifier	OctetString	29.229 [2]
2	Public-Identity	UTF8String	
3	Server-Name	UTF8String	
4	Server-Capabilities	Grouped	
5	Mandatory-Capability	Unsigned32	
6	Optional-Capability	Unsigned32	
7	User-Data	OctetString	
8	SIP-Number-Auth-Items	Unsigned32	
9	SIP-Authentication-Scheme	UTF8String	
10	SIP-Authenticate	OctetString	
11	SIP-Authorization	OctetString	
12	SIP-Authentication-Context	OctetString	
13	SIP-Auth-Data-Item	Grouped	
14	SIP-Item-Number	Unsigned32	
15	Server-Assignment-Type	Enumerated	
16	Deregistration-Reason	Grouped	
17	Reason-Code	Enumerated	
18	Reason-Info	UTF8String	
19	Charging-Information	Grouped	
20	Primary-Event-Charging-Function-Name	DiameterURI	
21	Secondary-Event-Charging-Function-Name	DiameterURI	
22	Primary-Charging-Collection-Function-Name	DiameterURI	
23	Secondary-Charging-Collection-Function-Name	DiameterURI	
24	User-Authorization-Type	Enumerated	
25	User-Data-Request-Type	Enumerated	
26	User-Data-Already-Available	Enumerated	
27	Confidentiality-Key	OctetString	
28	Integrity-Key	OctetString	
Note: The AVP codes from 29 to 99 are reserved for TS 29.229.			
100	User-Identity	Grouped	29.329 [4]
101	MSISDN	OctetString	
102	User-Data	OctetString	
103	Data-Reference	Enumerated	
104	Service-Indication	OctetString	
105	Subs-Req-Type	Enumerated	
106	Requested-Domain	Enumerated	
107	Current-Location	Enumerated	
108	Identity-Set	Enumerated	
Note: The AVP codes from 109 to199 are reserved for TS 29.329.			

8 Experimental result codes

The Diameter answer messages must carry either Result-Code AVP or Experimental-Result AVP. The values of Result-Code AVP are controlled by IANA. The Experimental-Result AVP is a grouped AVP containing the Vendor-Id AVP and Experimental-Result-Code AVP, thus the experimental result codes are controlled in a vendor-specific manner.

8.1 3GPP specific result codes

The 3GPP specific result codes are always transferred in the Experimental-Result AVP, which has the Vendor-Id with value of 3GPP's vendor identifier. The 3GPP specific result codes shall follow the same classification as defined for the values of Result-Code AVP in IETF RFC 3588 [9]. That means, the result codes are grouped to following ranges:

- 1xxx (Informational)
- 2xxx (Success)
- 4xxx (Transient Failures)

- 5xxx (Permanent Failures)

8.1.1 Informational

The Informational result codes shall use the values from 1001 to 1999 in the Experimental-Result-Code AVP.

Editor's note: No informational result codes have been yet defined in 3GPP.

8.1.2 Success

The Success result codes shall use the values from 2001 to 2999 in the Experimental-Result-Code AVP. The reserved 3GPP specific Success result codes are presented in the following table.

Table 8.1.2: 3GPP specific Success result codes

Experimental Result Code	Result text	Specified in the TS
2001	DIAMETER_FIRST_REGISTRATION	29.229 [2]
2002	DIAMETER_SUBSEQUENT_REGISTRATION	
2003	DIAMETER_UNREGISTERED_SERVICE	
2004	DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED	
2005	DIAMETER_SERVER_SELECTION	
Note: The Experimental Result Codes from 2006 to 2020 are reserved for the TS 29.229.		

8.1.3 Transient Failures

The Transient Failure result codes shall use the values from 4001 to 4999 in the Experimental-Result-Code AVP. The reserved 3GPP specific Transient Failure result codes are presented in the following table.

Table 8.1.3: 3GPP specific Transient Failure result codes

Experimental Result Code	Result text	Specified in the TS
4100	DIAMETER_USER_DATA_NOT_AVAILABLE	29.329 [4]
4101	DIAMETER_PRIOR_UPDATE_IN_PROGRESS	
Note: The Experimental Result Codes from 4102 to 4120 are reserved for the TS 29.329.		

8.1.4 Permanent Failures

The Permanent Failure result codes shall use the values from 5001 to 5999 in the Experimental-Result-Code AVP. The reserved 3GPP specific Permanent Failure result codes are presented in the following table.

Table 8.1.4: 3GPP specific Permanent Failure result codes

Experimental Result Code	Result text	Specified in the TS
5001	DIAMETER_ERROR_USER_UNKNOWN	29.229 [2]
5002	DIAMETER_ERROR_IDENTITIES_DONT_MATCH	
5003	DIAMETER_ERROR_IDENTITY_NOT_REGISTERED	
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	
5005	DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED	
5006	DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED	
5007	DIAMETER_ERROR_IN_ASSIGNMENT_TYPE	
5008	DIAMETER_ERROR_TOO_MUCH_DATA	
5009	DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA	
5010	DIAMETER_MISSING_USER_ID	
Note: The Experimental Result Codes from 5011 to 5020 are reserved for the TS 29.229.		
5100	DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED	29.329 [4]
5101	DIAMETER_ERROR_OPERATION_NOT_ALLOWED	
5102	DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ	
5103	DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED	
5104	DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED	
5105	DIAMETER_ERROR_TRANSPARENT_DATA OUT_OF_SYNC	
Note: The Experimental Result Codes from 5106 to 5120 are reserved for the TS 29.329.		

Annex A (informative): Assignment of the Diameter codes and identifiers in 3GPP

This annex defines the recommended assignment procedure of Diameter codes and identifiers within the 3GPP.

A.1 Application identifiers

If a working group detects it will require a new application identifier, it should contact the 3GPP TSG-CN WG 4 via a Liaison Statement. The LS shall contain the name of the Diameter application and a reference to the corresponding 3GPP TS. The 3GPP TSG-CN WG 4 will then request the application identifier from IANA. When the application identifier will be received, the corresponding working group will be informed by 3GPP TSG-CN WG 4 and the table 4.1 in this specification will be updated.

According to RFC 3588 the creation of a new application should be avoided if at all possible and therefore it is recommended to use the existing application identifiers whenever possible.

A.2 Command codes

If a working group detects there is a need for a new command code(s) from the 3GPP's range, it should contact the 3GPP TSG-CN WG 4 via an LS. The LS shall contain the reference to the 3GPP TS, which specifies the command(s). The 3GPP TSG-CN WG 4 will inform the assigned command code(s) to the corresponding working group and the table 5.1 in this specification will be updated.

It should be noted that the standard command codes allocated for 3GPP are scarce resource and getting new ones would require IETF specification work to be done. Therefore it is recommended to use the existing command codes whenever possible.

A.3 AVP codes

If a working group detects a Diameter application needs new 3GPP specific AVP codes, it should contact the 3GPP TSG-CN WG 4 via an LS. The LS shall contain the name of the Diameter application and a reference to the corresponding 3GPP TS. The 3GPP TSG-CN WG 4 will allocate a range of 100 AVP codes for the application. The range will be informed to the corresponding working group and the table 7.1 will be updated in this specification to show the reserved range. The working group can use the allocated range as a working assumption when defining the actual AVPs.

When the corresponding working group has specified the AVPs, it should inform them to the 3GPP TSG-CN WG 4 via an LS. The LS should list the used AVP codes in the form of the table 7.1.

If there will be defined new AVPs for a Diameter application through the CR procedure, the assigned AVP range can be used, but the 3GPP TSG-CN WG 4 should be also informed about the new AVP codes via an LS.

Re-using of the existing AVPs is recommended, but special attention should be paid on the use of enumerated AVPs. Defining new values for an enumerated AVP should be agreed case by case with the working group responsible of the particular enumerated AVP. 3GPP TSG-CN WG 4 shall be informed via an LS about the new values assigned to the enumerated AVP.

A.4 Result codes

If a working group detects a Diameter application needs new 3GPP specific result codes, it should contact the 3GPP TSG-CN WG 4 via an LS. The LS shall contain the name of the Diameter application and a reference to the corresponding 3GPP TS. The 3GPP TSG-CN WG 4 will allocate a range of 20 result codes from each required result code group for the application. The ranges will be informed to the corresponding working group and the tables in the chapter 8 of this specification will be updated to show the reserved ranges. The working group can use the allocated ranges as a working assumption when defining the actual result codes.

When the corresponding working group has specified the result codes, it should inform them to the 3GPP TSG-CN WG 4 via an LS. The LS should list the used result codes in the form of the tables in chapter 8.

If there will be defined new result codes for a Diameter application through the CR procedure, the assigned result code ranges can be used, but the 3GPP TSG-CN WG 4 should be also informed about the new result codes via an LS.

Re-using of the existing result codes is recommended.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-04					First draft to be presented in CN4#22bis	0.0.0	0.1.0
2004-04					Informative annex added to describe the assignment procedure	0.1.0	0.2.0
2004-04					Annex A improved	0.2.0	0.3.0

3GPP TSG CN WG4 Meeting #22bis **N4-040466**
Edinburgh, UK, 14th – 20th April 2004

Title:	LS on Assignment of the Diameter codes and identifiers
Release:	Rel-6
Source:	CN4
To:	CN3, SA5
Cc:	CN, SA

Contact Person:
Name: Kalle Tammi
Tel. Number: +358 40 5058670
E-mail Address: kalle.tammi@nokia.com

Attachments: N4-040465 [Draft TS 29.230 v0.3.0]

1. Overall Description:

As agreed by the CN#23, the CN4 has the responsibility to coordinate the 3GPP specific Diameter codes and identifiers. The CN4 has created a draft of the TS 29.230, which documents those codes and identifiers, to be the basis of the coordination. The annex A of the TS contains the recommended rules for the assignment procedure of different Diameter codes and identifiers.

2. Actions:

To CN3 and SA5 groups.

ACTION: CN4 kindly asks the other working groups to review the attached draft TS 29.230 and provide input to CN4 on any existing deficiencies. Special attention should be paid on the annex A, which describes the recommended assignment procedure of any new Diameter codes and identifiers within the 3GPP.

3. Date of Next CN4 Meeting:

CN4 #23	10th – 14th May 2004	Zagreb, CROATIA
CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE

3GPP TSG CN4 – CN4#23 **N4-040751**
10 - 14 May 2004
Zagreb, Croatia

Title: **Reply LS to Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0**
Work Item: **WLAN-3G Interworking**
Source: **CN4**
To: **Wi-Fi Alliance**
Cc: SA2

Contact Person:
Name: Paul Sitch
Tel. Number: +358 40 761 8849
E-mail Address: paul.sitch@nokia.com

Attachments: 1: CN4 Comments form.

1. Overview

CN4 would like to thank Wi-Fi Alliance for their Liaison Statement and Request for Comment on the Marketing Requirement Document Draft Version 1.0.

CN4 would like to suggest some improvements to the above document in order to make sure that the mobile market requirements are fully taken into account in Wi-Fi Alliance certifications. CN4 suggestions can be found in the attached MRD Comment Form, according to your request.

2. Action

CN4 kindly asks Wi-Fi Alliance to take into account the attached comments.

3. Date of the Next CN4 meetings

CN4 #24	16th-20th August 2004	Sophia Antipolis, FRANCE
CN4 #25	15th – 19th November 2004	TBD, SOUTH KOREA