ETSI TS 183 059-1 V2.1.1 (2009-08)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); a2 interface based on the DIAMETER protocol

Reference

DTS/TISPAN-03117-1-NGN-R2

Keywords

interface, stage 3

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document is applicable to the a2 interface between the Connectivity Session Location and Repository Function (CLF) and the Network Access Configuration Function (NACF).

Whenever it is possible the present document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of Diameter. Where this is not possible, extensions to Diameter are defined within the present document.

2 References

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

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
    - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
    - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI ES 282 004 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

NOTE: The latest version in the V2.y.z series applies.

[2] ETSI ES 282 003 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

NOTE: The latest version in the V2.y.z series applies.

[3] ETSI TS 129 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (3GPP TS 29.229)".

[4] ETSI TS 129 329: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329)".

[5] IETF RFC 2960: "Stream Control Transmission Protocol".

[6] IETF RFC 3588: "Diameter Base Protocol".

[7] IETF RFC 3309: "Stream Control Transmission Protocol (SCTP) Checksum Change".

[8] draft-ietf-geopriv-radius-lo-24 (January 2008): "Carrying Location Objects in RADIUS and Diameter".

[9] ETSI ES 283 034 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol".

NOTE: The latest version in the V2.y.z series applies.

[10] ETSI ES 283 035 (V2.y.z): Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".

NOTE: The latest version in the V2.y.z series applies.

[11] DSL Forum TR-069 (May 2004): "CPE WAN Management Protocol".

[12] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] IETF RFC 3554: "On the use of Stream Control Transmission Protocol (SCTP) with IPSec".

3 Definitions and abbreviations

3.1 Definitions

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

access record: set of information stored in the CLF in relation to an IP address

Application Function (AF): element of the network architecture offering - or providing access to - applications that require information about the characteristics of the IP-connectivity session used to access such applications

attribute-value pair: corresponds to an Information Element in a Diameter message

NOTE: See RFC 3588 [13].

nASS user: See definition in [1].

3.2 Abbreviations

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

ABNF	Augmented Backus-Naur Form
AF	Application Function
A-RACF	Access RACF
AVP	Attribute-Value Pair
CLF	Connectivity session Location and repository Function
CSCF	Call Session Control Function
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IPSec	IP Security

NACF	Network Access Configuration Function
NASS	Network Attachment SubSystem
PNA	Push-Notification-Answer
PNR	Push-Notification-Request
RACF	Resource and Admission Control Function
RACS	Resource and Admission Control Subsystem
RFC	Request For Comments
SCTP	Stream Control Transport Protocol
UCS	Universal Character Set
UDA	User-Data-Answer
UDR	User-Data-Request

4 Overview

The Network Attachment SubSystem (NASS), defined in ES 282 004 [1], maintains information about IP-connectivity associated with NASS User connected to TISPAN networks.

The a2 reference point allows the NACF to register in the CLF the association between the IP address allocated to a NASS User and information identifying the network access to which this equipment is connected.

The following information flows are used on the a2 interface:

- Bind Indication.
- Bind Acknowledgment.
- Unbind Indication.
- Bind information query.
- Bind information query acknowledgement.

The present document specifies the protocol for the a2 Diameter interface.

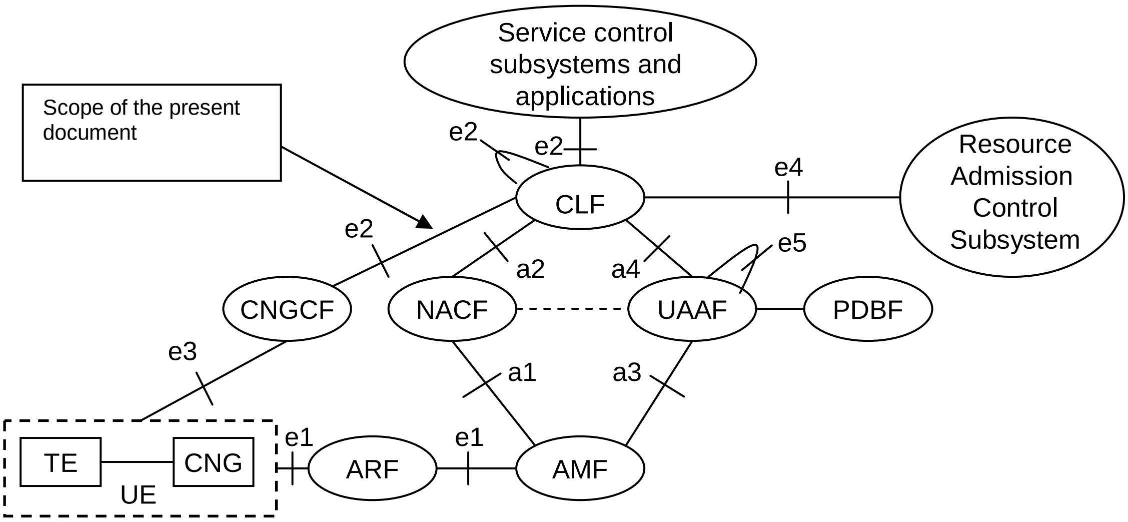
Service control subsystems and applications
Scope of the present document
e2
e2
e4
Resource Admission Control Subsystem
CLF
e2
a2
a4
e5
CNGCF
NACF
UAAF
PDBF
e3
a1
a3
e1
e1
TE
CNG
UE
ARF
AMF

Figure 4.1: a2 interface

5 Procedure Descriptions

5.1 General

5.1.1 Information elements

The following clauses describe the realization of the functional procedures defined in the NASS [1] and RACS specifications [2] using Diameter commands described in clause 7. This involves describing a mapping between the information elements defined in the NASS specification [1] and Diameter AVPs.

In the tables that describe this mapping, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional:

- A mandatory Information Element (marked as (M) in the table) shall always be present in the command. If this Information Element is absent, an application error occurs at the receiver and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.
- A conditional Information Element (marked as (C) in the table) shall be present in the command if certain conditions are fulfilled:
    - If the receiver detects that those conditions are fulfilled and the Information Element is absent, an application error occurs and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element. If multiple Information Elements are missing, all corresponding AVP codes shall be included in the Failed-AVP AVP. If those conditions are not fulfilled, the Information Element shall be absent. If however this Information Element appears in the message, it shall not cause an application error and it may be ignored by the receiver if this is not explicitly defined as an error case. Otherwise, an application error occurs at the receiver and an answer message with the Result-Code set to DIAMETER_AVP_NOT_ALLOWED shall be sent back to the originator of the request. A Failed-AVP AVP containing a copy of the corresponding Diameter AVP shall be included in this message.
- An optional Information Element (marked as (O) in the table) may be present or absent in the command, at the discretion of the application at the sending entity. Absence or presence of this Information Element shall not cause an application error and may be ignored by the receiver.

5.2 Procedures on the CLF - NACF interface

5.2.1 Bind indication/Acknowledgement

5.2.1.1 Overview

This procedure is used to report the binding between the IP address allocated to a user equipment and identity of the access to which this equipment is connected from the NACF to the CLF. This information flow occurs when an IP address has been allocated to a user equipment.

The NACF should trigger this procedure as soon as an IP address has been allocated.

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in clause 7. Tables 5.1 and 5.2 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to Diameter AVPs.

Table 5.1: Bind indication (NACF -> CLF)

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally Unique IP Address	Globally-Unique-Address	M	This information element contains: - The IP address of the NASS User. - The addressing domain in which the IP address is significant.
Logical Access ID	Logical-Access-Id	M	The identity of the logical access to which the user equipment is connected.
Physical Access ID	Physical-Access-Id	O	The identity of the physical access to which the user equipment is connected.
Access Network Type	Access-Network-Type	O	The type of access network providing IP connectivity to the NASS user.
Terminal Type	Terminal-Type	O	The type of user equipment.

Table 5.2: Bind Acknowledgment (CLF -> NACF)

Information element name	Mapping to Diameter AVP	Cat.	Description
CNGCF address	CNGCF-Address	O	The address of the CNGCF entity from which configuration data may be retrieved by the user equipment.
Geographic Location Information	Location-Data	O	Geographic location information.
P-CSCF Identity (optional)	SIP-Outbound-Proxy	O	The Identity of the P-CSCF for accessing IMS services.

5.2.1.2 Procedure at the NACF side

After allocating the IP address to a user equipment, or when a Renew is received from a different access line, the NACF shall send a Bind Indication with the following information to CLF:

- The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP.

- The Logical-Access-ID AVP shall be present.

- Physical Access ID and Terminal Type may be present if available.

If the NACF is implemented as a DHCP v4 server, the Logical-Access-Id AVP shall be derived from the value of the DHCP option 82, sub-option 1 and 2 received from the ARF. The Physical-Access-ID may also be derived from the value of these sub-options.

If the NACF is implemented as a DHCP v4 server, the Terminal-Type AVP shall be set from the value of the DHCP option 77 received from the user equipment.

On receipt of a Bind Acknowledgement with a Result-Code AVP indicating DIAMETER_SUCCESS, the NACF shall process the received AVPs as follows:

- If the NACF is implemented as a DHCP v4 server, the CNGCF-Address AVP shall be used to set the value of DHCP Option 43 (DSL Forum Autoconfiguration Server) or DHCP Option 66 (TFTP server).

- If the NACF is implemented as a DHCP v4 server, the Location-Information AVP shall be mapped to the DHCP option 123 or 99.

- If the NACF is implemented as a DHCP v4 server, the SIP-Outbound-Proxy AVP shall be mapped to the DHCP option 120.

The behaviour when the NACF does not receive a Bind Acknowledgement, or when it arrives after the internal timer waiting for it has expires, or when it arrives with an indication that is different to DIAMETER_SUCCESS, is outside the scope of the present document.

5.2.1.3 Procedure at the CLF side

If at least one of the specified AVP(s) is invalid, the CLF shall return a Binding Acknowledgement with a Result-Code AVP value set to DIAMETER_INVALID_AVP_VALUE and a Failed-AVP AVP containing a copy of the invalid AVP(s).

If the globally unique identifier contained in the Globally-Unique-Address AVP is not known, the CLF shall:

- Create an internal record to store the received information for future use.

If the globally unique identifier contained in the Globally-Unique-Address AVP is already known and the received Logical Access ID is different than the one stored in the internal record, the CLF shall:

- interact with RACS entities (i.e. A-RACF) to remove transport policies associated with the existing record and clear associated resources;
- replace the entire content of the internal record with the received information for future use.

If the CLF cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and return a Bind Acknowledgement with a Result-Code AVP value set to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code AVP set to DIAMETER_SYSTEM_UNAVAILABLE.

Otherwise, the requested operation shall take place and the CLF shall return a Bind Acknowledgement with the Result-Code AVP set to DIAMETER_SUCCESS and one or more of the AVPs identified in table 5.2.

5.2.2 Unbind indication

5.2.2.1 Overview

This procedure is used by the NACF to report the case the allocated IP address is released (e.g. DHCP leased timer expiry) or due to a release of the underlying layer 2 resources. This enables the CLF to remove the corresponding record from its internal database.

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in clause 7. Tables 5.3 and 5.4 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to Diameter AVPs.

Table 5.3: Unbind indication (NACF -> CLF)

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally Unique IP Address	Globally-Unique-Address	M	This information element contains: - The IP address of the NASS User. - The addressing domain in which the IP address is significant.

Table 5.4: Unbind indication acknowledgement (CLF -> NACF)

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result Code / Experimental_ Result	M	Result of the request. Result Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental Result AVP shall be used for other errors. This is a grouped AVP which contains a Vendor Id AVP, and the error code in the Experimental Result Code AVP.

5.2.2.2 Procedure at the NACF side

On receipt of release request for the allocated IP address from the user equipment or in case of expiry of the lease period or on receipt of an indication that the underlying layer 2 connection has been lost, the NACF shall clear all information stored against the IP address and issue a Push-Notification-Request representing a Globally-Unique-Address.

The IP-Connectivity-Status AVP shall be set to IP CONNECTIVITY LOST.

5.2.2.3 Procedure at the CLF side

If the globally unique identifier contained in the Globally-Unique-Address AVP is not known, the CLF shall stop processing the request and set the Experimental-Result-Code to DIAMETER_ERROR_USER_UNKNOWN in the Unbind Indication acknowledgement.

If the globally unique identifier contained in the Globally-Unique-Address AVP is already known, the CLF shall:

- remove the existing session record;
- interact with RACS entities (i.e. A-RACF) to remove transport policies associated with the session and clear associated resources.

If the CLF cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code set to DIAMETER_SYSTEM_UNAVAILABLE.

Otherwise, the requested operation shall take place and the CLF shall return an Unbind Indication response with the Result-Code AVP set to DIAMETER_SUCCESS.

5.2.3 Bind information query/acknowledgment

5.2.3.1 Overview

This procedure is used by the CLF to request binding information from the NACF, in the context of recovery procedures.

This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in clause 7. Tables 5.5 and 5.6 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to Diameter AVPs.

Table 5.5: Bind information query (CLF -> NACF)

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally Unique IP Address	Globally-Unique-Address	M	This information element contains: - The IP address of the NASS User. - The addressing domain in which the IP address is significant.

Table 5.6: Bind information query acknowledgement (NACF -> CLF)

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result Code / Experimental_ Result	M	Result of the request. Result Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental Result AVP shall be used for other errors. This is a grouped AVP which contains a Vendor Id AVP, and the error code in the Experimental Result Code AVP.
Globally Unique IP Address	Globally-Unique-Address	O	This information element contains: - The IP address of the NASS User. - The addressing domain in which the IP address is significant.
Logical Access ID	Logical-Access-Id	O	The identity of the logical access to which the user equipment is connected.
Physical Access ID	Physical-Access-Id	O	The identity of the physical access to which the user equipment is connected.
Access Network Type	Access-Network-Type	O	The type of access network providing IP connectivity to the NASS user.
Terminal Type	Terminal-Type	O	The type of user equipment.

5.2.3.2 Procedure at the CLF side

The CLF may use this procedure after a restart, upon reception of the query request from AF associated with an IP-Address for which no record is stored.

The CLF determines the NACF responsible for this IP address from the IP realm, and possibly the address range within this realm, it belongs to. In order to cope with network configurations where multiple NACF are associated with the same IP realm and are using overlapping address ranges, the CLF may apply one of the following procedures:

- The CLF queries each of the NACF until it gets a Bind Information Query acknowledgement with the Result-Code AVP set to DIAMETER_SUCCESS.

- The CLF sends the query to a Diameter Agent that has sufficient routing information to enable this query to be delivered to the appropriate NACF instance.

If no successful answer is received, the CLF shall delete all information that may have been stored regarding this IP address and provides an appropriate response to the requesting AF.

The CLF shall populate the Binding Information Query as follows:

1) The Globally-Unique-Address AVP shall be included.

2) The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP.

5.2.3.3 Procedure at the NACF side

Upon reception of the Bind Information Query, the NACF shall, in the following order:

1) If the Globally-Unique-Address AVP is present, use this information as a key to retrieve the requested session information.

2) If no session record is stored for the Globally-Unique-Address AVP, return a Bind Information Query Acknowledgment with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN.

If the NACF cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code AVP set to DIAMETER_USER_DATA_NOT_AVAILABLE.

Otherwise, the requested operation shall take place and the NACF shall return a Bind Information Query acknowledgement with the Result-Code AVP set to DIAMETER_SUCCESS and the session data described in table 5.6.

6 Use of the Diameter base protocol

With the clarifications listed in the following sub clauses the Diameter Base Protocol defined by RFC 3588 [6] shall apply.

6.1 Securing Diameter Messages

For secure transport of Diameter messages, IPSec may be used. Guidelines on the use of SCTP with IPSec can be found in RFC 3554 [i.1].

6.2 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used on the a2 interface.

6.3 Use of sessions

Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in RFC 3588 [6]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

6.4 Transport protocol

Diameter messages over the a2 interface shall make use of SCTP as defined in RFC 2960 [5] and shall utilize the new SCTP checksum method specified in RFC 3309 [7].

6.5 Routing considerations

This clause specifies the use of the Diameter routing AVPs Destination-Realm and Destination-Host.

Requests initiated by the NACF towards the CLF shall include both Destination-Host and Destination-Realm AVPs. The NACF obtains the Destination-Host AVP to use in requests towards a CLF, from configuration data. Consequently, the Destination-Host AVP is declared as mandatory in the ABNF for all requests initiated by the NACF.

Requests initiated by the CLF towards the NACF shall include both Destination-Host and Destination-Realm AVPs. The CLF obtains the Destination-Host AVP to use in requests towards a NACF, from the Origin-Host and Origin-Realm AVPs received in previous commands from the NACF related to the same IP realm. Consequently, the Destination-Host AVP is declared as mandatory in the ABNF for all requests initiated by the CLF.

Destination-Realm AVP is declared as mandatory in the ABNF for all requests.

6.6 Advertising application support

The NACF and CLF shall advertise support of the e4 specific application by including the value of the application identifier in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The vendor identifier value of ETSI (13019) shall be included in the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and in the Vendor-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. Additionally, support of 3GPP AVPs shall be advertised by adding the vendor identifier value of 3GPP (10415) to the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands,

NOTE: The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that is not included in the Vendor-Specific-Application-Id AVPs as described above indicate the manufacturer of the Diameter node as per RFC 3588 [6].

7 DIAMETER application

This clause specifies the use of the e4 a Diameter application that allows a Diameter server and a Diameter client exchange information related to IP-connectivity sessions.

The Diameter application identifier assigned to this application is 16777231 (allocated by IANA for e4).

The Diameter Base Protocol as specified in RFC 3588 [6] is used to support information transfer on both interfaces.

RFC 3588 [6] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and event codes specified in clause 5. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) are unmodified.

7.1 Commands

The present document re-uses and modifies commands defined in ETSI e4 interface ES 283 034 [9] which itself re-uses and modifies commands defined in the 3GPP Sh specifications [4]. Only the following commands defined in TS 129 329 [4] are used. Any other command defined in TS 129 329 [4] shall be ignored.

Table 7.1a: Command-code values

Command-Name	Abbreviation	Code
User-Data-Request	UDR	306
User-Data-Answer	UDA	306
Push-Notification-Request	PNR	309
Push-Notification-Answer	PNA	309

AVPs defined in TS 129 329 [4] and not used in the present document are not shown in the below clauses. If received, these AVPs shall be ignored by the NACF and the CLF.

New AVPs are represented in bold.

7.1.1 Push-Notification-Request command

The Push-Notification-Request (PNR) command, indicated by the Command-Code field set to 309 and the "R" bit set in the Command Flags field, is sent by a Diameter server to a Diameter client in order to notify changes in the NASS User data in the server. This command is defined in TS 129 329 [4] and used with additional AVPs defined in the present document.

Message Format:

```
< Push-Notification-Request > ::=  < Diameter Header: 309, REQ, PXY, 16777231 >
                                      < Session-Id >
                                      { Vendor-Specific-Application-Id }
                                      { Auth-Session-State }
                                      { Origin-Host }
                                      { Origin-Realm }
                                      { Destination-Host }
                                      { Destination-Realm }
                                      [Globally-Unique-Address]
                                      [Logical-Access-Id]
                                      [Physical-Access-Id]
                                      [Terminal-Type]
                                      [Access-Network-Type]
                                      [IP-Connectivity-Status]
                                      *[ AVP ]
                                      *[ Proxy-Info ]
                                      *[ Route-Record ]
```

7.1.2 Push-Notification-Answer command

The Push-Notifications-Answer (PNA) command, indicated by the Command-Code field set to 309 and the "R" bit cleared in the Command Flags field, is sent by a client in response to the Push-Notification-Request command. This command is defined in TS 129 329 [4]. The Experimental-Result AVP may contain one of the values defined in clause 7.2 or in TS 129 229 [3] or in the present document.

Message Format:

```
< Push-Notification-Answer > ::=  < Diameter Header: 309, PXY, 16777231 >
                                     < Session-Id >
                                     { Vendor-Specific-Application-Id }
                                     [ Result-Code ]
                                     [ Experimental-Result ]
                                     { Auth-Session-State }
                                     { Origin-Host }
                                     { Origin-Realm }
                                     [CNGCF-Address]
                                     [Location-Data]
                                     [SIP-Outbound-Proxy]
                                     *[ AVP ]
                                     *[ Failed-AVP ]
                                     *[ Proxy-Info ]
                                     *[ Route-Record ]
```

7.1.3 User-Data-Request command

The User-Data-Request (UDR) command, indicated by the Command-Code field set to 306 and the "R" bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request NASS User data. This command is defined in TS 129 329 [4] and used with additional AVPs defined in the present document.

Message Format:

```
< User-Data -Request > ::= < Diameter Header: 306, REQ, PXY, 16777231 >
                                     < Session-Id >
                                     { Vendor-Specific-Application-Id }
                                     { Auth-Session-State }
                                     { Origin-Host }
                                     { Origin-Realm }
                                     [ Destination-Host ]
```

{ Destination-Realm }
[Globally-Unique-Address]
[Logical-Access-Id]
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.1.4 User-Data-Answer command

The User-Data-Answer (UDA) command, indicated by the Command-Code field set to 306 and the "R" bit cleared in the Command Flags field, is sent by a server in response to the User-Data-Request command. This command is defined in TS 129 329 [4] and used with additional AVPs defined in the present document. The Experimental-Result AVP may contain one of the values defined in clause 7.2 or in TS 129 229 [3] or in the present document.

Message Format:

< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777231 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Globally-Unique-Address]
[Logical-Access-Id]
[Physical-Access-Id]
[Terminal-Type]
[Access-Network-Type]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

7.2 Result-Code AVP values

This clause defines new result code values that must be supported by all Diameter implementations that conform to the present document. 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.

7.2.1 Success

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

No result codes within this category have been defined so far.

7.2.2 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.

No errors within this category have been defined so far. However the following error defined in TS 129 229 [3] is used in the present document:

DIAMETER_ERROR_USER_UNKNOWN (5001)

When this result code is used, the 3GPP Vendor ID shall be included in the Vendor-Id AVP of the Experimental-Result AVP.

7.2.3 Transient Failures

Errors that fall within the transient failures category are those used to inform a peer that the request could not be satisfied at the time that it was received. The request may be able to be satisfied in the future.

The following error defined in ES 283 034 [9] is used in the present document:
DIAMETER_SYSTEM_UNAVAILABLE (4001)

This error is returned when a request could not be satisfied at the time that it was received due to a temporary internal failure or congestion. When this result code is used, the ETSI Vendor ID shall be included in the Vendor-Id AVP of the Experimental-Result AVP.

The following error defined in TS 129 229 [3] is also used in the present document:

DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

When this result code is used, the 3GPP Vendor ID shall be included in the Vendor-Id AVP of the Experimental-Result AVP.

7.3 AVPs

The following tables summarize the AVP used in the present document, beyond those defined in the Diameter Base Protocol.

Table 7.1 describes the Diameter AVPs defined in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. The Vendor-Id header of all AVPs defined in the present document shall be set to ETSI (13019).

Table 7.1: Diameter AVPs defined in the present document

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
SIP-Outbound-Proxy	601 13019	7.3	OctetString	V	M			No
CNGCF-Address	600 13019	7.3	Grouped	V	M			No
TFTP-Server	602 13019	7.3	UTF8String	V	M			No
ACS-Server	603 13019	7.3	UTF8String	V	M			No
NOTE: 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.								

Table 7.2 describes the Diameter AVPs defined for the e2 interface protocol (ES 283 035 [10]) and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. Vendor-Id header for these AVPs shall be set to ETSI (13019).

Table 7.2: Diameter AVPs imported from the e2 specification

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
Terminal-Type	352	See ES 283 035 [10]	OctetString	V	M			No
NOTE: 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.								

Table 7.3 describes the Diameter AVPs defined for the e4 interface protocol (ES 283 034 [9]) and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. Vendor-Id header for these AVPs shall be set to ETSI (13019).

Table 7.3: Diameter AVPs imported from the e4 specification

Attribute Name	AVP Code	Clause defined	Value Type	AVP Flag rules				May Encrypt
				Must	May	Should not	Must not	
Logical-Access-Id	302	See ES 283 034 [9]	OctetString	V	M			No
Physical-Access-Id	313	See ES 283 034 [9]	UTF8String	V	M			No
Access-Network-Type	306	See ES 283 034 [9]	Grouped	V	M			No
IP-Connectivity-Status	305	See ES 283 034 [9]	Enumerated	V	M			No
NOTE: 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.								

Table 7.4 describes the Diameter AVPs defined in IETF specifications other than RFC 3588 [6] and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined.

Table 7.4: Diameter AVPs defined in IETF specifications

Attribute Name	AVP Code	Clause defined	Value Type	AVP Flag rules				May Encrypt
				Must	May	Should not	Must not	
Location-Data	128	[8]	OctetString		M		V	No
NOTE: 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.								

7.3.1 Logical-Access-ID AVP

See the definition in e4 ES 283 034 [9].

7.3.2 Physical-Access-ID

See the definition in e4 ES 283 034 [9].

7.3.3 Terminal-Type AVP

See the definition in e2 ES 283 035 [10].

7.3.4 IP-Connectivity-Status

The IP Connectivity Status AVP (AVP code 305 13019) is defined in the e4 specification ES 283 034 [9].

7.3.5 CNGCF-Address

The CNGCF-Address AVP (AVP code 600 13019) is of type Grouped and contains one or more CNGCF addresses, each of which identifying different types of CNGCF implementation.

AVP Format:

```
CNGCF-Address ::= < AVP Header: 600 13019 >
    [TFTP-Server]
    [ACS-Server]
```

7.3.6 SIP-Outbound-Proxy

The SIP-Outbound-Proxy AVP (AVP code 601 13019) is of type OctetString and identifies a SIP outbound proxy (e.g. a P-CSCF when accessing to the IMS) in the form of an FQDN.

7.3.7 Access-Network-Type AVP

The Access-Network-Type AVP (AVP code 306 13019) is defined in the e4 specification ES 283 034 [9].

7.3.8 Location-Data AVP

The Location-Data AVP is defined in draft-ietf-geopriv-radius-lo-19 [8]. It contains location data in the form of either Civic Location or Geospatial Location.

7.3.9 TFTP-Server

The TFTP-Server AVP (AVP code 602 13019) is of type UTF8String and identifies a TFTP server.

7.3.10 ACS-Server

The ACS-Server AVP (AVP code 603 13019) is of type UTF8String and identifies an Autoconfiguration Server conforming to the DSL Forum specifications (TR-69 [11]) in the form of a URI (RFC 3986 [12]).

Annex A (informative): Mapping of a2 operations and terminology to Diameter

TableA.1 defines the mapping between the information flows defined in ES 282 004 [1] and Diameter commands:

Table A.1: a2 message to Diameter command mapping

a2 message	Source	Destination	Command-Name	Abbreviation
Bind Indication	NACF	CLF	Push-Notification-Request	PNR
Bind Indication Acknowledgement	CLF	NACF	Push-Notification-Answer	PNA
Unbind Indication	NACF	CLF	Push-Notification-Request	PNR
Unbind Indication Acknowledgement	CLF	NACF	Push-Notification-Answer	PNA
Bind Information Query	CLF	NACF	User-Data-Request	UDR
Bind Information Query Acknowledgement	NACF	CLF	User-Data-Answer	UNA

Annex B (informative): Bibliography

ETSI TS 129 209: "Universal Mobile Telecommunications System (UMTS); Policy control over Gq interface (3GPP TS 29.209) "

IETF RFC 2234: "Augmented BNF for syntax specifications: ABNF".

IETF RFC 4005: "Diameter Network Access Server application".

History

Document history		
V2.1.1	August 2009	Publication