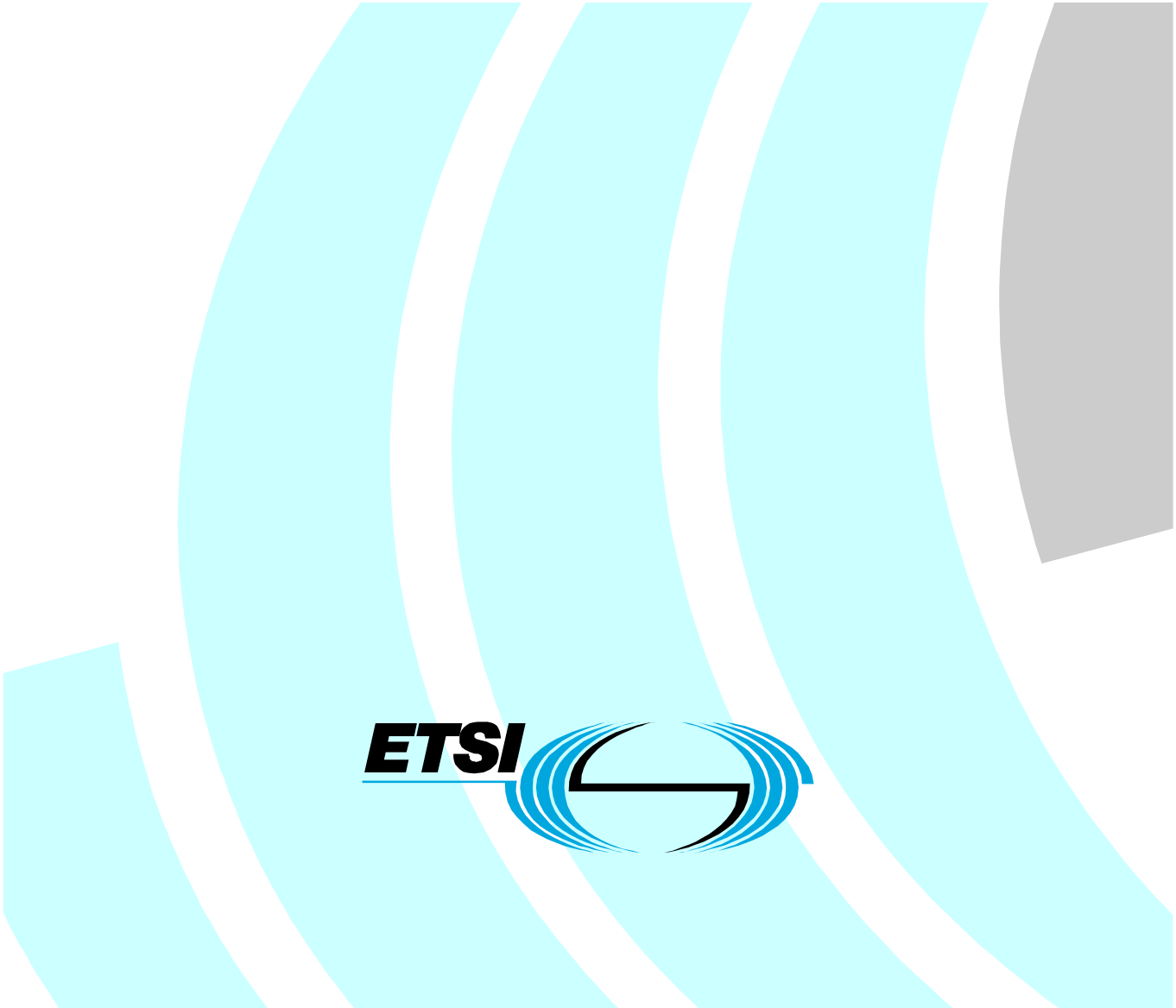
Final draft ETSI ES 283 034 V1.1.1 (2006-04)

ETSI Standard

Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol



Reference
DES/TISPAN-03063-NGN-R1

Keywords
interface, network, system

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 ETSI Standard (ES) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), and is now submitted for the ETSI standards Membership Approval Procedure.

1 Scope

The present document defines a protocol for use between the TISPAN NGN Network Attachment Sub-System (NASS) and the Resource and Admission Control Subsystem (RACS), based on Diameter.

The present document is applicable to the e4 interface between the Connectivity Session Location and Repository Function (CLF) and the RACS.

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

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

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

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

[3] ETSI TS 129 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 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); Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329)".

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

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

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

[8] IETF RFC 3309: "SCTP Checksum Change".

[9] IETF RFC 4005 "DIAMETER Network Access Server application".

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

[11] IETF RFC 3046: "DHCP Relay Agent Information Option".

3 Definitions and abbreviations

3.1 Definitions

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

Attribute-Value Pair (AVP): See RFC 3588, corresponds to an Information Element in a Diameter message.

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

3.2 Abbreviations

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

AF	Application Function
A-RACF	Access-Resource and Admission Control Function
ABNF	Augmented Backus-Naur Form
ATM	Asynchroneous Transfer Mode
AVP	Attribute-Value Pair
BGF	Border Gateway Function
CLF	Connectivity session Location and repository Function
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IPSec	IP Security
L2TF	Layer 2 Termination Function
NAS	Network Access Server
NASS	Network Attachment Sub-System
RACF	Resource and Admission Control Function
RACS	Resource and Admission Control Subsystem
RCEF	Resource Control Enforcement Function
RFC	Request For Comments
SCTP	Stream Control Transport Protocol
SPDF	Service-based Policy Decision Function
UAAF	User Authentication and Authorization Function
UCS	Universal Character Set

4 Overview

The Network Attachment Sub-System (NASS), defined in ES 282 004 [1], maintains information about IP-connectivity associated with user equipment connected to TISPAN networks. This information is stored in the Connectivity Session Location and Repository Function (CLF) and made accessible to other subsystems and applications through the following two interfaces (see figure 1):

- The e2 interface enables Application Functions (AF) to retrieve IP-connectivity related session data.
- The e4 interface enables the IP-connectivity related session data to be exchanged between the NASS and the Resource and Admission Control Subsystem (RACS) defined in ES 282 003 [2].

The present document specifies the protocol for the e4 interface.

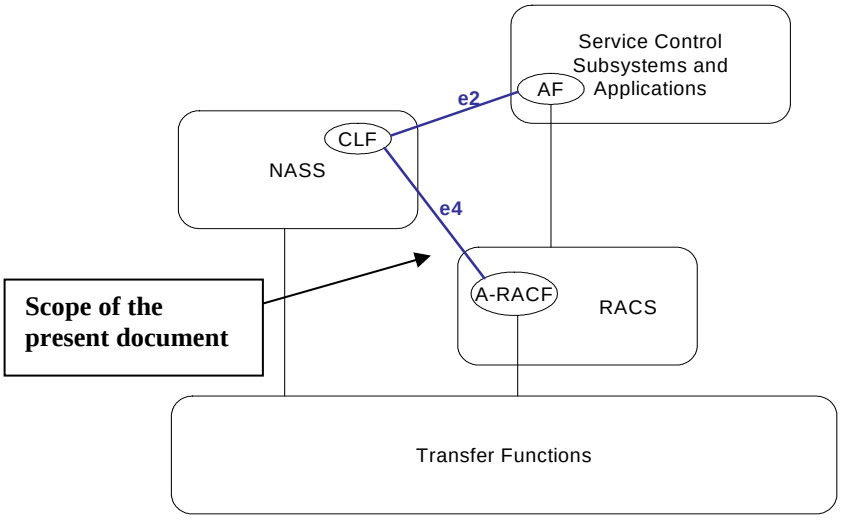


Figure 1: NASS external interfaces

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 (ES 282 004) [1] and RACS specifications (ES 282 003 [2]) using Diameter commands described in clause 7. This involves describing a mapping between the Information Elements defined in the NASS specification (ES 282 004 [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.

5.1.2 Subscriber profile

Subscriber profile information sent over the e4 interface is structured into two groups: the QoS Profile Information and the Initial Gate Setting.

Tables 1 and 2 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to DIAMETER AVPs.

Table 1: Initial gate setting

Information element name	Mapping to Diameter AVP	Cat.	Description
List of allowed destinations	NAS-Filter-Rule	O	The list of default destination IP addresses, ports, prefixes and port ranges to which traffic can be sent.
UL Subscribed Bandwidth	Maximum-Allowed-Bandwidth-UL	O	The maximum amount of bandwidth that can be used without explicit authorization in the uplink direction.
DL Subscribed Bandwidth	Maximum-Allowed-Bandwidth-DL	O	The maximum amount of bandwidth that can be used without explicit authorization in the downlink direction.

Table 2: QoS profile information

Information element name	Mapping to Diameter AVP	Cat.	Description
Transport service class	Transport-Class	O	The transport class applicable to the QoS Profile Information.
Media-Type	Media-Type	O	The media type applicable to the QoS Profile information.
UL Subscribed Bandwidth	Maximum-Allowed-Bandwidth-UL	O	The maximum amount of bandwidth subscribed by the attached user in the uplink direction.
DL Subscribed Bandwidth	Maximum-Allowed-Bandwidth-DL	O	The maximum amount of bandwidth subscribed by the attached user in the downlink direction.
Maximum Priority	Reservation-Priority	O	The maximum priority allowed for any reservation request
Requestor Name	Application Class ID	O	Identifies the application class(es) that are allowed to request resources for the QoS profile.

5.2 Procedures on the CLF - A-RACF interface

5.2.1 Access profile push

5.2.1.1 Overview

This procedure is used to push session-related information from the CLF to the A-RACF. This information flow occurs when an IP address has been allocated to a subscriber or in case a modification occurs on a profile that has already been pushed to the RACS.

The CLF should push session-related-information to the A-RACF as soon as it is available to the CLF. This may require the CLF to pull part of the information from other components of the NASS.

For the same subscriber, the CLF may push several independent session records with different IP addresses, with or without the same logical access identifier.

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in clause 7. Tables 3 and 4 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to Diameter AVPs.

Table 3: Access profile push

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 user equipment used by the subscriber for which profile information is being pushed. - 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.
Access Network Type	Access-Network-Type	O	The type of access network over which IP connectivity is provided to the user equipment.
Subscriber ID	User-Name	C	The user that is attached to the network (see note).
Physical Access ID	Physical-Access-Id	O	The identity of the physical access to which the user equipment is connected.
Initial Gate Setting	Initial-Gate-Setting	O	See clause 5.1, table 1.
QoS Profile	QoS-Profile	O	See clause 5.1, table 2.
NOTE: The Subscriber ID shall be included if available in the CLF.			

Table 4: Access profile push response

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.

5.2.1.2 Procedure at the CLF side

The CLF knows the address of the A-RACF entity where the information should be pushed, either from configuration data or from the user profile (i.e. received from the UAAF/PDPF).

The CLF shall populate the Access Profile Push as follows:

- 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.

The presence of the other AVPs depends on the user profile and local policy rules.

5.2.1.3 Procedure at the A-RACF side

If the Logical Access ID is not included or is invalid, the A-RACF shall return an Access Profile Push response with a Result-Code AVP value set to DIAMETER_INVALID_AVP_VALUE.

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

- Create an internal record to store the received information for future use (i.e. for processing resource reservation requests received from the SPDF).

- Derive the following information from the Logical Access ID:
  - The identification and bandwidth capacity of the layer 2 resources over which the subscriber traffic is carried.
  - The address of the physical node(s) implementing the BGF, L2TF and RCEF.
- If the received information contains an Initial Gate Settings AVP, perform any appropriate actions to enforce the policy information. This may involve interacting with the RCEF through the Re interface.

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

- Replace the entire content of the internal record with the received information for future use.
- If the received information contains an Initial Gate Settings, perform any appropriate actions to enforce the new policy information. This may involve interacting with the RCEF through the Re interface.

Such an update shall not have any impact on ongoing application sessions for which an authorization has already been provided by the A-RACF.

If the contents of the request is invalid the A-RACF shall return an Access Profile Push response with a Result-Code AVP value set to the appropriate value as described in clause 5.1.

If the creation or modification of the session record is successful but a failure occurs during the processing of the Initial Gate Settings (e.g. due to a failure in the interaction with the RCEF), the A-RACF shall return an Access Profile Push response with a Result-Code AVP value set to DIAMETER_LIMITED_SUCCESS.

If the A-RACF 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 an Access Profile Push response with a Result-Code AVP value set to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code AVP set to DIAMETER_SYSTEM_UNAVAILABLE. In the later case, the CLF is expected to retry after a provisioned time period.

Otherwise, the requested operation shall take place and the A-RACF shall return the Result-Code AVP set to DIAMETER_SUCCESS and the stored session data in the Access Profile Push response.

5.2.2 Access profile pull

5.2.2.1 Overview

This procedure is used by the RACS to request the Access Profile information from the CLF, 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 and 6 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to Diameter AVPs.

Table 5: Access profile pull request

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally unique IP Address	Globally-Unique-Address	C	This information element contains: - The IP address of the user equipment used by the subscriber for which profile information is being pushed. - The addressing domain in which the IP address is significant.
Subscriber ID	User-Name	C	The user that is attached to the network.
RACS-Id	AF-Application-Identifier	M	Identifies the A-RACF function requesting profile information.

Table 6: Access profile pull response

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally unique IP Address	Globally-Unique-Address	C	This information element contains: - The IP address of the user equipment used by the subscriber for which profile information is being pushed. - 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.
Access Network Type	Access-Network-Type	O	The type of access network over which IP connectivity is provided to the user equipment.
Subscriber ID	User-Name	C	The user that is attached to the network.
Physical Access ID	Physical-Access-Id	O	The identity of the physical access to which the user equipment is connected.
Initial Gate Settings	Initial-Gate-Settings	O	See clause 5.1, table 1.
QoS Profile	QoS-Profile	O	See clause 5.1, table 2.

5.2.2.2 Procedure at the A-RACF side

The A-RACF may use this procedure after a restart, upon reception of the resource reservation request associated with an IP-Address for which no record is stored.

The A-RACF shall populate the Access Profile Pull request as follows:

1) The User-Name AVP or the Globally-Unique-Address AVP shall be included. The Globally-Unique-Address AVP shall be included in configurations where more than one IP address may be assigned per subscriber identifier.

2) If present, the Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP. The Address-Realm AVP shall be included and set either using configuration data (in which case all terminal equipment served by the A-RACF belong to the same addressing domain) or from the physical or logical interface over which was received the resource request that triggered the pull procedure.

3) The AF-Application-Identifier AVP shall be present and set to the A-RACF Identity.

5.2.2.3 Procedure at the CLF side

Upon reception of the Access Profile Pull request, the CLF 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 the Globally-Unique-Address AVP is absent but the User-Name AVP is present, use the latter information as a key to retrieve the requested session information.

3) If both the Globally-Unique-Address AVP and the User-Name AVP are absent, return an Access Pull Profile response with Result-Code set to DIAMETER_MISSING_AVP.

4) If more than one record include the same subscriber identity matching the value of the User-Name AVP and no Globally-Unique-Address AVP is included, return an Access Pull Profile response with Result-Code set to DIAMETER_UNABLE_TO_COMPLY.

5) If no session record is stored for the Globally-Unique-Address AVP or the User-Name AVP, return an Access Pull Profile with the Experimental-Result-Code AVP shall be set to DIAMETER_ERROR_USER_UNKNOWN.

If a unique subscriber record car be retrieved, the CLF shall:

1) Check which session data can be returned to the A-RACF, based on local policy rules and per-subscriber privacy information stored in the CLF.

2) Check whether the session data to be retrieved is currently being updated by another entity. If there is an update of the data in progress, the CLF may delay the response message until the update has been completed and shall include in the response message the updated data requested. The CLF shall ensure that the data returned is not corrupted by this conflict.

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 AVP set to DIAMETER_USER_DATA_NOT_AVAILABLE.

Otherwise, the requested operation shall take place and the CLF shall return the Result-Code AVP set to DIAMETER_SUCCESS and the session data in the Access Profile Pull response.

5.2.3 IP connectivity release indication

5.2.3.1 Overview

This procedure is used by the CLF to report loss of IP connectivity. This enables the RACS to remove the access profile from its internal data base. This event occurs in 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 procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in clause 7. Tables 7 and 8 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to Diameter AVPs.

Table 7: IP connectivity release indication

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 user equipment used by the subscriber for which profile information is being pushed. - The addressing domain in which the IP address is significant.
Subscriber ID	User-Name	O	The user that is attached to the network.
IP-Connectivity Status	IP-Connectivity-Status	M	Whether IP connectivity to/from the user equipment is currently available.

Table 8: IP connectivity release indication response

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.

5.2.3.2 Procedure at the CLF side

On receipt of an external event indicating that the allocated IP address has been released or the underlying layer 2 connection has been lost, the CLF shall clear all information stored against the IP address and issue a Push-Notification-Request representing an IP-Connectivity-Release-Indication with the IP-Connectivity-Status AVP set to the value IP-CONNECTIVITY-LOST.

NOTE: Receipt of an indication that a layer 2 connection has been lost may lead the CLF to issue several notifications, in case multiple access sessions where associated with this connection.

5.2.3.3 Procedure at the A-RACF side

If the globally unique identifier contained in the Globally-Unique-Address AVP is not known, the A-RACF shall stop processing the request and set the Experimental-Result-Code to DIAMETER_ERROR_USER_UNKNOWN in the IP Connectivity Release Indication Response.

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

- remove the existing session record;
- interact with transfer layer entities (i.e. RCEF) to remove transport policies associated with the session and clear associated resources;
- notify the SPDF.

If the A-RACF 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. In the later case, the CLF is expected to retry after a provisioned time period.

Otherwise, the requested operation shall take place and the A-RACF shall return an IP-Connectivity-Release-Indication response with the Result-Code AVP set to DIAMETER_SUCCESS.

6 Use of the Diameter base protocol

With the clarifications listed in the following clauses the Diameter Base Protocol defined by RFC 3588 [7] 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 [10].

6.2 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used on the e4 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 [7]. 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 e4 interface shall make use of SCTP RFC 2960 [6] and shall utilize the new SCTP checksum method specified in RFC 3309 [8].

6.5 Routing considerations

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

Requests initiated by the CLF towards the RACS shall include both Destination-Host and Destination-Realm AVPs. The CLF obtains the Destination-Host AVP to use in requests towards an A-RACF, from configuration data and/or the subscriber profile. Consequently, the Destination-Host AVP is declared as mandatory in the ABNF for all requests initiated by the CLF.

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

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

6.6 Advertising application support

The CLF and A-RACF shall advertize support of the used 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 advertized 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 shall indicate the manufacturer of the Diameter node as per RFC 3588 [7].

7 DIAMETER application

This clause specifies 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 **xxxxx** (allocated by IANA).

The Diameter Base Protocol as specified in RFC 3588 [7] is used to support information transfer on both interfaces.

RFC 3588 [7] 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 unrecognized information handling) are unmodified.

7.1 Commands

The present document 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 9: 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 CLF and the A-RACF.

New AVPs are represented in bold.

7.1.1 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 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, **xxxxxxx** >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
[Globally-Unique-Address]
[AF-Application-Identifier]
[User-Name]
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.1.2 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, **xxxxx**>
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Logical-Access-Id]
[Physical-Access-Id]
[Access-Network-Type]
[Initial-Gate-Setting]
***[Qos-Profile]**
[IP-Connectivity-Status]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

7.1.3 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 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, **xxxxxxx** >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
[Globally-Unique-IPAddress]
[User-Name]
[Logical-Access-Id]
[Physical-Access-Id]
[Access-Network-Type]
[Initial-Gate-Setting]
***[QoS-Profile]**
[IP-Connectivity-Status]
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.1.4 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, xxxxx >
                                  < Session-Id >
                                  { Vendor-Specific-Application-Id }
                                  [ Result-Code ]
                                  [ Experimental-Result ]
                                  { Auth-Session-State }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  *[ 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 present document defines the following error with this category:

- 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.

The following table 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 10: 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**
Globally-Unique-Address	300	7.3	Grouped	M,V				Yes
Address-Realm	301	7.3	OctetString	M,V				Yes
Logical-Access-Id	302	7.3	OctetString	V	M			Yes
Initial-Gate-Setting	303	7.3	Grouped	V	M			Yes
QoS-Profile	304	7.3	Grouped	V	M			Yes
IP-Connectivity-Status	305	7.3	Enumerated	V	M			Yes
Access-Network-Type	306	7.3	Grouped	V	M			Yes
Aggregation-Network-Type	307	7.3	Enumerated	V	M			Yes
Maximum-Allowed-Bandwidth-UL	308	7.3	Unsigned32	V	M			Yes
Maximum-Allowed-Bandwidth-DL	309	7.3	Unsigned32	V	M			Yes
Maximum-Priority	310	7.3	Unsigned32	V	M			Yes
Transport-Class	311	7.3	Unsigned32	V	M			Yes
Application-Class-ID	312	7.3	UTF8String	V	M			Yes
Physical-Access-ID	313	7.3	UTF8String	V	M			Yes
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 11 describes the Diameter AVPs defined for the Gq interface protocol (TS 129 209 [5]) 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. AVPs defined in TS 129 209 [5] but no listed in the following table should not be sent by Diameter conforming to the present document and shall be ignored by receiving entities. The Vendor-Id header for these AVPs shall be set to 3GPP (10415).

Table 11: Diameter AVPs imported from the Gq specification

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
Media-Type	700	See TS 129 209 [5]	Grouped	V	M			Yes
AF-Application-Identifier	703	See TS 129 209 [5]	OctetString	M,V				Yes

The following table describes the Diameter AVPs defined for the NAS application (RFC 4005[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. AVPs defined in RFC 4005 [9] but no listed in the following table should not be sent by Diameter conforming to the present document and shall be ignored by receiving entities. No Vendor-Id shall be included in the AVP header.

Table 12: Diameter AVPs imported from the NAS application

Attribute Name	AVP Code	Clause defined	Value Type	AVP Flag rules				
				Must	May	Should not	Must not	May Encrypt
NAS-Port-Type	61	See RFC 4005 [9]	Enumerated		M		V	Yes
NAS-Filter-Rule	400	See RFC 4005 [9]	IPFilterRule		M		V	Yes
Framed-IP-Address	8	See RFC 4005 [9]	OctetString		M		V	Yes
Framed-IPv6-Prefix	97	See RFC 4005 [9]	OctetString		M		V	Yes

7.3.1 Globally-Unique-Address AVP

The Globally-Unique-Address AVP (AVP code 300 13019) is of type Grouped.

AVP Format:

```
Globally-Unique-Address ::= < AVP Header: 300 13019 >
    [Frame-IP-Address]
    [Frame-IPv6-Prefix]
    [Address-Realm]
```

7.3.2 Address-Realm AVP

The Address-Realm AVP (AVP code 301 13019) is of type OctetString and contains an address realm in the form of a FQDN.

7.3.3 Logical-Access-ID AVP

The Logical-Access-ID AVP (AVP code 302 13019) is of type OctetString. This AVP contains either a Circuit-ID (as defined in RFC 3046 [11]) or a technology independent identifier.

NOTE: In the xDSL/ATM case, the Logical Access ID may explicitly contain the identity of the VP and VC carrying the traffic.

7.3.4 Initial-Gate-Setting AVP

The Initial-Gate-Setting AVP (AVP code 303 13019) is of type Grouped.

AVP Format:

```
Initial-Gate-Setting ::= < AVP Header: 303 13019 >
      {NAS-Filter-Rule}
      [Maximum-Allowed-Bandwidth-UL]
      [Maximum-Allowed-Bandwidth-DL]
```

Absence of the Maximum-Allowed-Bandwidth-UL AVP indicates that no limitation is placed by the subscription on the amount of bandwidth that can be used on the uplink direction.

Absence of the Maximum-Allowed-Bandwidth-DL AVP indicates that no limitation is placed by the subscription on the amount of bandwidth that can be used on the downlink direction.

7.3.5 QoS-Profile AVP

The QoS-Profile AVP (AVP code 304 13019) represent of QoS-Profile element and is of type Grouped.

AVP Format:

```
QoSProfile ::= < AVP Header: 304 13019 >
      *[Application-Class-ID]
      *[Media-Type]
      [Reservation-Priority]
      [Maximum-Allowed-Bandwidth-UL]
      [Maximum-Allowed-Bandwidth-DL]
      [Transport-Class]
```

Absence of the Application-Class-ID AVP indicates that the QoS Profile instance applies to any requestor.

Absence of the Media-Type AVP indicates that the QoS Profile element applies to any media type.

Absence of the Reservation-Priority AVP indicates that reservation requests that conform to the bandwidth limitations can be accepted regardless of their priority.

Absence of the Maximum-Allowed-Bandwidth-UL AVP indicates that no limitation is placed by the subscription on the amount of bandwidth that can be used on the uplink direction, for the QoS profile.

Absence of the Maximum-Allowed-Bandwidth-DL AVP indicates that no limitation is placed by the subscription on the amount of bandwidth that can be used on the downlink direction for the QoS profile.

Absence of the Transport-Class AVP indicates that the QoS Profile instance does not mandate a specific transport class behaviour.

7.3.6 IP-Connectivity-Status AVP

The IP-Connectivity-Status AVP (AVP code 305 13019) is of type Enumerated.

The following values are defined:

- IP-CONNECTIVITY-ON (0).
- IP-CONNECTIVITY-LOST (1).

7.3.7 Access-Network-Type AVP

The Access-Network-Type AVP (AVP code 306 13019) is of type Grouped, and it indicates the type of port on which the user equipment is connected and the type of aggregation network.

AVP Format:

```
Access-Network-Type ::= < AVP Header: 306 13019 >
      {NAS-Port-Type}
       [Aggregation-Network-Type]
```

7.3.8 Aggregation-Network-Type AVP

The Aggregation-Network-Type AVP (AVP code 307 13019) is of type Enumerated.

The following values are defined:

- UNKNOWN (0).
- ATM (1).
- ETHERNET (2).

7.3.9 Maximum-Allowed-Bandwidth-UL AVP

The Maximum-Allowed-Bandwitdth-UL AVP (AVP code 308 13019) is of type Unsigned32 and indicated the maximum uplink bandwidth that can be authorized for a particular traffic class. The AVP value is expressed in kbits/s.

7.3.10 Maximum-Allowed-Bandwidth-DL AVP

The Maximum-Allowed-Bandwidth-DL AVP (AVP code 309 13019) is of type Unsigned32 and indicated the maximum downlink bandwidth that can be authorized for a particular traffic class. The AVP value is expressed in kbits/s.

7.3.11 Reservation-Priority

The Reservation-Priority AVP (AVP code 310 13019) is of type Enumerated and represent a priority level to serve resource reservation requests.

The following values are defined:

- PRIORITY 0 (0).
- PRIORITY 1 (1).
- PRIORITY 2 (2).
- PRIORITY 3 (3).
- PRIORITY 4 (4).
- PRIORITY 5 (5).
- PRIORITY 6 (6).
- PRIORITY 7 (7).

NOTE: PRIORITY 0 is the lowest priority.

7.3.12 Transport-Class

The Transport-Class AVP (AVP code 311 13019) is of type Unsigned32 and contains an integer used as an index pointing to a class of transport services to be applied (e.g. forwarding behaviour).

7.3.13 Application-Class-ID

The Application-Class-ID AVP (AVP code 312 13019) is of type UTF8String and represents a class of applications that share the same QoS profile.

7.3.14 Physical-Access-ID

The Physical-Access-ID AVP (AVP code 313 13019) is of type UTF8String and identifies the physical access to which the user equipment is connected. It includes a port identifier and the identity of the access node where the port resides.

7.3.15 NAS-Port-Type AVP

The NAS-Port-Type AVP is defined in the NAS application, specified in RFC 4005 [9].

7.3.16 NAS-Filter-Rule AVP

The NAS-Filter-Rule AVP is defined in the NAS application, specified in RFC 4005 [9].

7.3.17 Framed-IP-Address AVP

The Framed-IP-Address AVP is defined in the NAS application, specified in RFC 4005 [9].

7.3.18 Framed-IP-Prefix AVP

The Framed-IPv6-Prefix AVP is defined in the NAS application, specified in RFC 4005 [9].

7.3.19 Origin-Host AVP

The Origin-Host AVP is defined in the DIAMETER base protocol, RFC 3588 [7].

7.3.20 AF-Application-Identifier AVP

The AF-Application-identifier AVP (AVP code 504 10415) is of type OctetString and is defined in the Gq specification, TS 129 209 [5].

7.3.21 Media-Type AVP

The Media-Type AVP is defined in the Gq specification (TS 129 209 [5]) and shall be used with the Vendor-Id header set to 3GPP (10415).

7.4 Use of namespaces

This clause contains the namespaces that have either been created in the present document, or the values assigned to existing namespaces managed by IANA.

7.4.1 AVP codes

The present document assigns the AVP values in the 300 to 349 range from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 7.3 for the assignment of the namespace in the present document.

7.4.2 Experimental-Result-Code AVP values

The present document assigns the Experimental-Result-Code AVP value 4001 to the following experimental result code:

- DIAMETER_SYSTEM_UNAVAILABLE.

7.4.3 Command Code values

The present document does not assign command code values but uses existing command codes assigned to 3GPP.

7.4.4 Application-ID value

The present document uses value **xxxx**, allocated by IANA, as application identifier.

Annex A (informative): Mapping of e4 operations and terminology to Diameter

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

Table A.1: e4 message to Diameter command mapping

e4 message	Source	Destination	Command-Name	Abbreviation
Access Profile Pull	RACS	CLF	User-Data-Request	UDR
Access Profile Pull Response	CLF	RACS	User-Data-Answer	UDA
Access Profile Push	CLF	RACS	Push-Notification-Request	PNR
Access Profile Push Response	RACS	CLF	Push-Notification-Answer	PNA
IP Connectivity Release Ind	CLF	RACS	Push-Notification-Request	PNR
IP Connectivity Release resp	RACS	CLF	Push-Notification-Answer	PNA

History

Document history			
V1.1.1	April 2006	Membership Approval Procedure	MV 20060602: 2006-04-04 to 2006-06-02