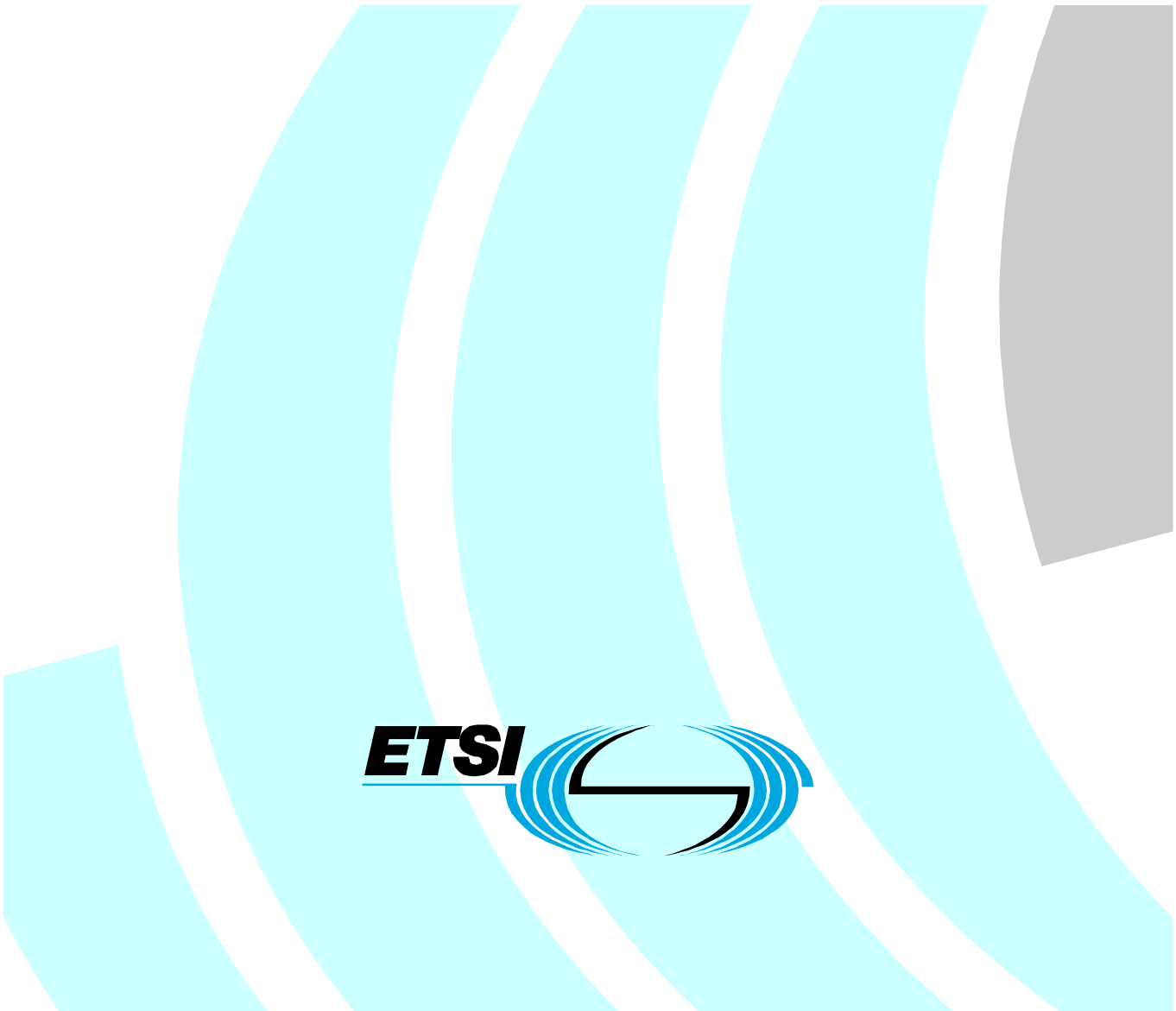
Final draft ETSI ES 283 035 V1.2.1 (2007-04)

ETSI Standard

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol



Reference
RES/TISPAN-03097-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 service control subsystems or applications of the TISPAN NGN architecture, based on Diameter.

The present document is applicable to the e2 interface between the Connectivity Session Location and Repository Function (CLF) and an Application Function (AF).

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.

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

[1] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

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

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

[4] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[5] ETSI ES 283 034: "Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol".

[6] 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)".

[7] 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)".

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

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

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

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

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

[13] ETSI TS 182 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Presence Service; Architecture and functional description (Endorsement of 3GPP TS 23.141 and OMA-AD-Presence-SIMPLE-V1-0)".

[14] ETSI TS 183 033: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia; Diameter based protocol for the interfaces between the Call Session Control Function and the User Profile Server Function/Subscription Locator Function; Signalling flows and protocol details [3GPP TS 29.228 V6.8.0 and 3GPP TS 29.229 V6.6.0, modified]".

3 Definitions and abbreviations

3.1 Definitions

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

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

Attribute-Value Pair (AVP): corresponds to an Information Element in a Diameter message

NOTE: See RFC 3588 [10].

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-Resource and Admission Control Function
ASF	Application Server Function
AVP	Attribute-Value Pair
CLF	Connectivity session Location and repository Function
CSCF	Call Session Control Function
IANA	Internet Assigned Numbers Authority
IBCF	Interconnection Border Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
NASS	Network Attachment Sub-System
P-CSCF	Proxy Call Session Control Function
PDBF	Profile Data Base Function
PNA	Presence Network Agent
RACF	Resource and Admission Control Function
RACS	Resource and Admission Control Subsystem
RFC	Request For Comments
SCTP	Stream Control Transport Protocol
SPDF	Service-based Policy Decision Function
UAAF	User Authentication and Authorization Function
UDA	User-Data-Answer
UCS	Universal Character Set

4 Overview

The Network Attachment Sub-System (NASS) defined in ES 282 004 [2] maintains information about IP-connectivity access sessions associated with user equipment connected to the TISPAN network. 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 [3].

The present document specifies the protocol for the e2 interface.

In the context of the present document, an Application Function (AF) is a generic term representing any element of the service layer architecture offering applications that require information about the characteristics of the IP-connectivity session used to access such applications. Examples of such Application Functions are the P-CSCF in the IMS (ES 282 007 [4]), the IBCF, certain categories of Application Server Functions (ASF) (ES 282 001 [1]) or a Presence Network Agent (PNA) as defined in TS 182 008 [13]. In the later case, the Pn reference point of the presence architecture is mapped to the e2 interface.

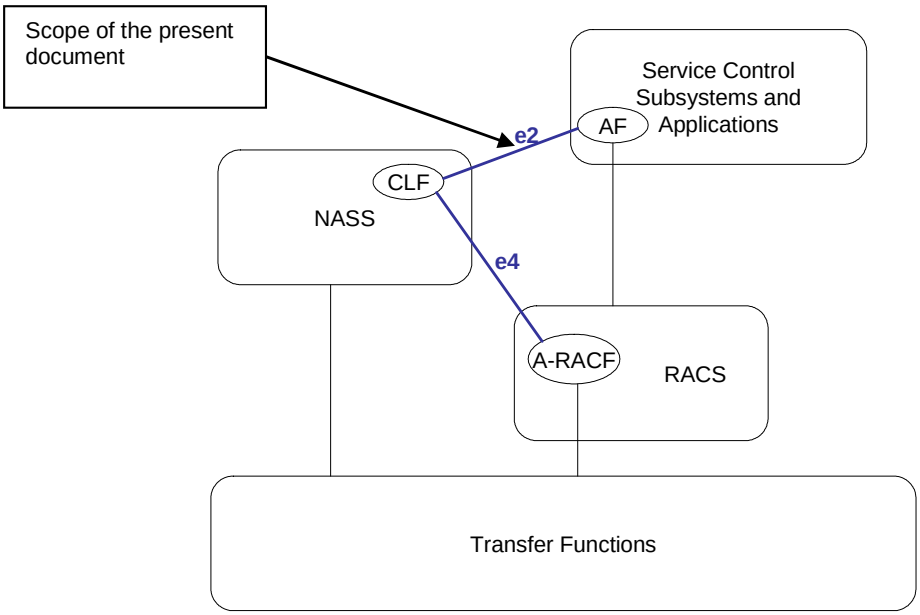


Figure 1: NASS external interfaces

5 Procedure descriptions

5.1 General

The following clauses describe the realization of the functional procedures defined in the NASS (ES 282 004 [2]) and RACS specifications (ES 282 003 [3]) using Diameter commands described in clause 7. This involves describing a mapping between the Information Elements defined in the NASS specification (ES 282 004 [2]) 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 tables 1 and 2) 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 tables 1 and 2) 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 - AF interface

5.2.1 Information query

5.2.1.1 Overview

This procedure is used by an AF to retrieve from the CLF location information and other data related to an access session.

This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in TS 129 329 [7].

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

Table 1: Information query

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.
AF Identity	AF-Application-Identifier	M	Identifies the AF originating the request.
Requested-Items	Requested-Information	O	The list of items requested by the AF.
NOTE: Either the Globally-Unique-IP-Address or the Subscriber-Id shall be included.			

Table 2: Information query 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 the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Subscriber ID	User-Name	O	The user that is attached to the network.
Location Information	Location-Information	O	Location information (or a pointer to such information) in a form that is suitable for the requesting application.
RACS contact point	RACS-Contact-Point	O	The FQDN or IP address of the RACS entity where resource request shall be sent (i.e. SPDF address).
Access Network Type	Access-Network-Type	O	The type of access network over which IP connectivity is provided to the user equipment.
Terminal Type	Terminal-Type	O	The type of user equipment to which the IP address was allocated.

5.2.1.2 Procedure at the AF side

The AF shall populate the Information Query as follows:

1) Insert either a Globally-Unique-Address or a User-Name AVP. 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 AF 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.

2) The AF-Application-Identifier AVP shall be present.

3) The Requested-Information AVP shall be present if specific information is requested and shall be absent if all available information is requested.

5.2.1.3 Procedure at the CLF side

Upon reception of the Information Query, 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 Information Query 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 Information Query 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 Information Query with the Experimental-Result-Code AVP shall be set to DIAMETER_ERROR_USER_UNKNOWN.

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

1) Check which session data can be returned to the AF, 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.

Under temporary overload conditions, the CLF shall stop processing the request and return an Information Query response with the Experimental-Result-Code set to DIAMETER_USER_DATA_NOT_AVAILABLE. The AF may retry retrieving the required information at a later stage.

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 the Result-Code to DIAMETER_UNABLE_TO_COMPLY.

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 Information Query response.

NOTE: Due to the application of operator's policies and subscriber privacy rules, the session data returned in the message may be a subset of the explicitly or implicitly requested session data.

6 Use of the Diameter base protocol

With the clarifications listed in the following clauses the Diameter Base Protocol defined by RFC 3588 [10] 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 [12].

6.2 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used on the e2 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 [10]. 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 e2 interface shall make use of SCTP RFC 2960 [9] and shall utilize the new SCTP checksum method specified in RFC 3309 [11].

6.5 Routing considerations

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

If an AF knows the address/name of the CLF for a certain user, both the Destination-Realm and Destination-Host AVPs shall be present in the request. Otherwise, only the Destination-Realm AVP shall be present and the command shall be routed to a Proxy CLF, based on the Diameter routing table in the client. The proxy CLF shall act as a DIAMETER relay as described in RFC 3588 [10].

Requests initiated by the CLF towards an AF shall include both Destination-Host and Destination-Realm AVPs. The CLF obtains the Destination-Host AVP to use in requests towards an AF from configuration data or information received from the UAAF/PDBF. 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 CLF and AF shall advertise support of the e2 specific application by including the value 16777231of 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 shall indicate the manufacturer of the Diameter node as per RFC 3588 [10].

7 DIAMETER application

The Diameter Base Protocol as specified in RFC 3588 [10] is used to support information transfer on the e2 interface.

RFC 3588 [10] 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.

The present document re-uses the Diameter application defined for the e4 interface in ES 283 034 [5].

7.1 Commands

Only the following commands defined in ES 283 034 [5] are used. Other commands shall be ignored by the AF and CLF.

Table 3: Command-Code values

Command-Name	Abbreviation	Code
User-Data-Request	UDR	306
User-Data-Answer	UDA	306

AVPs defined in ES 283 034 [5] and not used in the present document are not represented in the below clauses. If received, these AVPs shall be ignored by the CLF and the AF.

New AVPs defined in the present document 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 [7] 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]
[User-Name]
[AF-Application-Identifier]
[Requested-Information]
*[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 [7] and used with additional AVPs defined in the present document. The Experimental-Result AVP may contain one of the values defined in clause 6.2 or in TS 129 229 [6].

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 }
                                    [User-Name]
                                    [Access-Network-Type]
                                    [Location-Information]
                                    [RACS-Contact-Point]
                                    [Terminal-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 Code within this category has 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 [6] is used in the present document:

- DIAMETER_ERROR_USER_UNKNOWN (5001).

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.

No errors within this category have been defined so far. However the following error defined in TS 129 229 [6] is used in the present document:

- DIAMETER_USER_DATA_NOT_AVAILABLE (4100).

7.3 AVPs

This clause summarizes 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 4: 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**
Location-Information	350	7.3.1	Grouped	V	M			Yes
RACS-Contact-Point	351	7.3.2	DiameterIdentity	V	M			Yes
Terminal-Type	352	7.3.3	OctetString	V	M			Yes
Requested-Information	353	7.3.4	Enumerated	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. For further details, see TS 129 229 [6].								

The following table describes the Diameter AVPs defined for the Gq interface protocol (TS 129 209 [8]) 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 [8] 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 5: 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**
AF-Application-Identifier	504	See TS 129 209 [8]	OctetString	M,V				Yes

The following table describes the Diameter AVPs defined for the e4 specification ES 283 034 [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 ES 283 034 [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 of all these AVPs shall be set to ETSI (13019).

Table 6: Diameter AVPs imported from e4 specifications

				AVP flag rules				
Attribute name	**AVP Code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Globally-Unique-Address	300	See ES 283 034 [5]	Grouped	M,V				Yes
Logical-Access-Id	302	See ES 283 034 [5]	OctetString	V	M			Yes
Access-Network-Type	306	See ES 283 034 [5]	Grouped	V	M			Yes

The following table describes the Diameter AVPs defined for the Cx/Dx interface specification TS 183 033 [14] 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 183 033 [14] 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 of all these AVPs shall be set to ETSI (13019).

Table 7: Diameter AVPs imported from Cx/Dx specifications

				AVP flag rules				
Attribute name	**AVP Code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Line-Identifier	500	See TS 183 033 [14]	Line-Identifier	V	M			Yes

7.3.1 Location-Information AVP

The Location-Information AVP (AVP code 350 13019) is of type Grouped.

AVP Format:

```
Location-Information ::= < AVP Header: 350 13019 >
      [Line-Identifier]
      *[AVP]
```

7.3.2 RACS-Contact-Point AVP

The RACS-Contact-Point AVP (AVP code 351 13019) is of type DiameterIdentity and identifies the RACS element to which resource reservation requests shall be sent.

7.3.3 Terminal-Type AVP

The Terminal-Type AVP (AVP code 352 13019) is of type OctetString and contains a value of the User Class DHCP Option (77).

7.3.4 Requested-Information AVP

The Requested-Information AVP (AVP code 353 13019) is of type Enumerated. The following values are defined:

- SUBSCRIBER-ID (0).
- LOCATION-INFORMATION (1).
- RACS-CONTACT-POINT (2).
- ACCESS-NETWORK-TYPE (3).
- TERMINAL-TYPE (4).

The following values (5 to 10) are reserved for future use. They are out of scope of this Release. Should a CLF receive a UDR (as defined in clause 7.1.1) containing any of these reserved values within the Requested-Information AVP, it should handle it the same way as if any other non-specified value had been received.

- LOGICAL-ACCESS-ID (5).
- PHYSICAL-ACCESS-ID (6).
- ACCESS-NETWORK-TYPE (7).
- INITIAL-GATE-SETTING (8).
- QOS-PROFILE (9).
- IP-CONNECTIVITY-STATUS (10).

7.3.5 Line-Identifier AVP

The Line-Identifier AVP is of type OctetString and is defined in TS 183 033 [14].

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 350 to 399 range from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 7.3 for the list of AVP values assigned in the present document.

7.4.2 Experimental-Result-Code AVP values

The present document does not assign any Experimental-Result-Code AVP value.

7.4.3 Command Code values

The present document does not assign command code values but uses existing command defined by TS 129 329 [7] and modified by ES 283 034 [5].

7.4.4 Application-ID value

The present document uses value 16777231, allocated by IANA for the e4 interface in ES 283 034 [5], as application identifier.

Annex A (informative): Mapping of e2 operations and terminology to Diameter

The following table defines the mapping between information elements defined in ES 282 004 [2] and Diameter commands.

Table A.1: e2 message to Diameter command mapping

e2 message	Source	Destination	Command-Name	Abbreviation
Location Information Query	AF	CLF	User-Data-Request	UDR
Location Information Response	CLF	AF	User-Data-Answer	UDA

History

Document history		
V1.1.1	July 2006	Publication
V1.2.1	April 2007	Membership Approval Procedure MV 20070601: 2007-04-03 to 2007-06-01