Final draft ETSI ES 283 035 V3.2.1 (2017-11)

Network Technologies (NTECH);
Network Attachment;
e2 interface based on the DIAMETER protocol

Reference
RES/NTECH-00036

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

Contents

Intellectual Property Rights

Essential patents

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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This final draft ETSI Standard (ES) has been produced by ETSI Technical Committee Network Technologies (NTECH), and is now submitted for the ETSI standards Membership Approval Procedure.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies a Diameter application for use between a Connectivity session Location and repository Function (CLF) and an Application Function (AF).

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

The following referenced documents are necessary for the application of the present document.

[1] Void.

[2] Void.

[3] Void.

[4] Void.

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

[6] ETSI TS 129 229: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 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+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 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 6733: "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] Void.

[15] IETF RFC 4776: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information".

[16] IETF RFC 3825: "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information".

[17] IETF RFC 4234: "Augmented BNF for Syntax Specifications: ABNF".

[18] Recommendation ITU-T M.1400: "Designations for interconnections among operators' networks".

[19] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".

[20] ETSI TS 129 061: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) (3GPP TS 29.061)".

[21] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

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

[23] IETF RFC 4119: "A Presence-based GEOPRIV Location Object Format".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

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

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

[i.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".

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

3 Definitions and abbreviations

3.1 Definitions

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

access identifier: identifier of an access network termination point

NOTE: Examples of access identifiers include wireline terminations identifiers in fixed access networks and mobile cell identifiers.

access network: collection of network entities and interfaces that provide the underlying IP transport connectivity between end user devices and other networks

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

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 (AVP): Information Element in a Diameter message

NOTE: See IETF RFC 6733 [10].

IP connectivity user: entity requesting IP connectivity from an access network

must: shall

NOTE: The drafting rules of the IETF mandate the modal auxiliary verb "must" where 3GPP/ETSI rules mandate "shall". Similarly, "must not" and "shall not". When the present document cites an IETF document or when it provides text which, for comprehensibility, needs to be congruent with IETF terminology, the terms "must" and "must not" are retained, and need to be interpreted as having the same meaning as "shall" and "shall not" in regular 3GPP/ETSI drafting conventions.

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

3.2 Abbreviations

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

ABNF	Augmented Backus-Naur Form
AF	Application Function
ASCII	American Standard Code for Information Interchange
ASF	Application Server Function
AVP	Attribute-Value Pair
CLF	Connectivity session Location and repository Function
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
FQDN	Fully Qualified Domain Name
GI	Geographical Identifier
IANA	Internet Assigned Numbers Authority
IBCF	Interconnection Border Control Function
ICC	ITU Carrier Code
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LAC	Location-Area-Code
LCI	Location Configuration Information
NASS	Network Attachment Sub-System
NGN	Next Generation Network
NOC	Network-Operator-Code
P-CSCF	Proxy Call Session Control Function
PDBF	Profile Data Base Function
PIDF LO	Presence Information Data Format Location Object
PNA	Presence Network Agent
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
SNA	Subscribe-Notifications-Answer
SNR	Subscribe-Notifications-Request
UAAF	User Authentication and Authorization Function
UDA	User-Data-Answer
UDR	User-Data-Request

UE	User Equipment
URI	Uniform Resource Identifier

4 Overview

The present document specifies a Diameter application for use between a Connectivity session Location and repository Function (CLF) and an Application Function (AF). The interface between the CLF and the AF is known as the e2 interface (figure 1).

A Connectivity session Location and repository Function (CLF) is a data base in an access network that maintains information associated to an IP address and/or an access identifier in the form of dynamic session records or static access records, respectively. How a CLF obtains this information is outside the scope of the present document.

In the context of the present document, an Application Function (AF) represents any network element offering - or providing access to - applications that require information about the characteristics of the IP-connectivity session used to access such applications. Annex A provides background information on the use of a CLF in NGN architectures (ETSI ES 282 001 [i.1]).

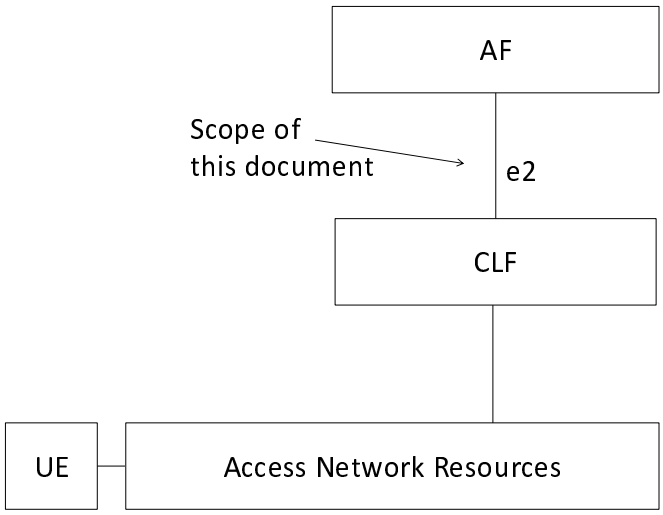

Figure 1: e2 interface

5 Procedure descriptions

5.1 General

The following clauses describe the procedures for supporting interactions between an AF and a CLF.

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 ETSI TS 129 329 [7].

Tables 1 and 2 detail the involved information elements and their mapping to Diameter AVPs.

Table 1: Information query 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 UE for which profile information is being pushed. - The addressing domain in which the IP address is significant.
IP connectivity user ID	User-Name	C	The identity of the IP connectivity user that is attached to the network.
Access Identifier	Global-Access-Id	C	Identifies an access point to IP connectivity services.
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.
Port-Number	Port-Number	O	The originating port number associated to the session for which the AF is attempting to retrieve information.
NOTE: Either the Globally-Unique-IP-Address, the IP connectivity user ID or the Access Identifier 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.
IP connectivity user ID	User-Name	O	The identity of the IP connectivity 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.
Policy Control contact point	Policy-Control-Contact-Point	O	The FQDN or IP address of a policy control entity where resource request shall be sent.
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.
Logical Access ID	Logical-Access-Id	O	The identity of the logical access where the user equipment is connected.
Physical Access ID	Physical-Access-Id	O	The identity of the physical access where the user equipment is connected.
Emergency-Call-Routeing-Info	Emergency-Call-Routeing-Info	O	A URI where to route emergency calls originated from the access and/or session considered.

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, a User-Name AVP or a Global-Access-Id 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 a session record.

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 a session record.

3) If both the Globally-Unique-Address AVP and the User-Name AVP are absent, and a Global-Access-Id AVP is present, use this information to retrieve an access record.

4) If more than one session record include the same IP connectivity user ID 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.

6) If the Globally-Unique-Address AVP, the User-Name AVP and the Global-Access-ID AVP are absent, return an Information Query response with Result-Code set to DIAMETER_MISSING_AVP.

If a unique session record is retrieved, the CLF shall check which session data can be returned to the AF, based on the contents of the Requested-Information AVP, local policy rules and, if applicable, per-IP connectivity user privacy information.

NOTE 1: In case of an NGN architecture the CLF receives privacy information received from the UAAF/PDBF.

If an access record is retrieved, the CLF shall check which data can be returned to the AF, based on the contents of the Requested-Information AVP and local policy rules.

NOTE 2: If the Requested-Information AVP is not received, the list of requested information is inferred from the AF identity.

The CLF shall also 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 Result-Code set to DIAMETER_TOO_BUSY. 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 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 Information Query response.

NOTE 3: Due to the application of operator's policies and IP connectivity user privacy rules, the session data returned in the message may be a subset of the explicitly or implicitly requested session data.

5.2.2 Event Registration/Deregistration

5.2.2.1 Overview

This procedure is used by an AF to subscribe with the CLF to a particular event.

This procedure is mapped to the commands Subscribe-Notifications-Request/Answer defined in the Diameter application specified in ETSI TS 129 329 [7].

Tables 2a and 2b detail the involved information elements and their mapping to Diameter AVPs.

Table 2a: Event Registration/Deregistration Request

Information element name	Mapping to Diameter AVP	Cat.	Description
	Subs-Req-Type	M	Indicates whether the AF is willing to subscribe or unsubscribe to the notification of the event.
IP connectivity user ID	User-Name	C	The identity of the IP connectivity user on behalf of which the event is to be reported.
Globally unique IP Address	Globally Unique Address	C	This information element contains the IP address of the IP connectivity user on behalf of which the event is to be reported, together with the addressing domain in which the IP address is significant.
Subscription Expiration	Expiry-Time	O	Moment of expiration of the subscription to the event.
Event	Event-Type	M	The type of event to be monitored.
AF Identity	AF-Application-Identifier	M	Identifies the AF originating the request.

Table 2b: Event Registration/Deregistration 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.
	Expiry-Time	O	Acknowledges the absolute time at which the subscription expires.

The CLF monitors events related to access sessions. Monitoring of a particular event on a particular session is activated when at least one Application Function has subscribed to be notified of the occurrence of the event.

Subscription to an event may be done implicitly (i.e. through management operations) or explicitly using the Event Registration/Deregistration request. Subscription to an event ceases when one of the following conditions is met:

- Expiry of the subscription duration.
- Removal of the session record from the CLF.
- Receipt of an explicit request to unsubscribe.

5.2.2.2 Procedure at the AF side

The AF shall populate the Event Registration/Deregistration Request as follows:

Insert a Subs-Req-Type AVP indicating whether it is willing to subscribe or unsubscribe to the notification of events:

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 IP connectivity users served by the AF is assumed to belong to the same addressing domain) or from the physical or logical interface over which was received a related service request.

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

3) At least one occurrence of the Event-Type AVP shall be present.

4) The Expiry-Time AVP may be present.

5.2.2.3 Procedure at the CLF side

Upon reception of an Event Registration/Deregistration Request, the CLF shall, in the following order:

1) Based on the contents of the AF-Application-Identifier AVP, check whether the AF is allowed to request monitoring of events. If not, return an Event Registration Response with Result-Code set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED.

2) If the Globally-Unique-Address AVP is present, use this information as a key to identify the session for which event monitoring is being requested.

3) If the Globally-Unique-Address AVP is absent but the User-Name AVP is present, use the latter information as a key to the session(s) for which event monitoring is being requested.

4) If both the Globally-Unique-Address AVP and the User-Name AVP are absent, return an Event Registration/Deregistration Response with the Result-Code AVP set to DIAMETER_MISSING_AVP.

5) If no stored session record matches the Globally-Unique-Address AVP or the User-Name AVP and the requested Event differs from USER-LOGON, return an Event Registration Response with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN.

If the Subs-Req-Type AVP indicates that this is a request to subscribe to the notification of events, the CLF shall check whether the requested event can be reported to the AF, based on local policy rules and per-IP connectivity user privacy information received from the UAAF. If the AF is not allowed to request monitoring of the event, return an Event Registration/Deregistration Response with Result-Code set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED. If the AF is allowed to request monitoring of the event, the CLF shall:

1) For all session records matching the request, associate the AF-Application-Identifier with the list of entities that need to be notified when the event identified by the request occurs. The association lasts until the moment indicated by the value of the Expiry-Time AVP as returned to the AF. If no Expiry-Time AVP is supplied, the CLF should treat it as a request for an unlimited subscription.

2) Include in the Event Registration Response an Expiry Time AVP with the absolute time at which the subscription expires in the case of a successful subscription. This time may be earlier than the requested expiry time. If the CLF includes this AVP, then no notification shall be sent to the AF after the expiration time. If the CLF does not include this AVP, that indicates an unlimited subscription.

3) Set the Result-Code to DIAMETER_SUCCESS and return an Event Registration/Deregistration Response.

If the Subs-Req-Type AVP indicates that this is a request to unsubscribe to the notification of events, the CLF shall remove the association of the AF-Identifier with the same list. The Result-Code shall be set to DIAMETER_SUCCESS if the operation is successful or if the AF-Identifier was not present in the list. If the Event-Type AVP is absent, the CLF assumes that the AF is willing to unsubscribe to all events associated with the User-Name or Globally-Unique-Address AVP.

If a subsequent request is received by the CLF where the Expiry Time AVP is present but different from what the CLF has previously stored, the CLF should replace the stored expiration time with what was received in the request.

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.

5.2.3 Notification Events

5.2.3.1 Overview

This procedure is used by a CLF to notify the AF of the occurrence of a particular event.

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

Tables 2c and 2d detail the involved information elements and their mapping to Diameter AVPs.

Table 2c: Notification Event Request

Information element name	Mapping to Diameter AVP	Cat.	Description
IP connectivity user ID	User-Name	C	The identity of the IP connectivity user on behalf of which the event is to be reported.
Globally unique IP Address	Globally Unique Address	C	This information element contains: - The IP address of the IP connectivity user on behalf of which the event is to be reported. - The addressing domain in which the IP address is significant.
AF Identity	AF-Application-Identifier	M	Identifies the AF having registered to the request.
Event	Event-Type	M	The type of event to be monitored.
	[AVP]	O	AVPs carrying CLF information associated to the reported event.

Table 2d: Notification Event 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.

5.2.3.2 Procedure at the CLF side

When a monitored event is detected on a particular access session, the CLF issues a Notification Event Request to each of the application functions having registered to this event.

The Notification Event Request is populated as follows:

1) A least a Globally-Unique-Address or a User-Name AVP shall be included. 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 a related service request.

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

3) One or more occurrence of the Event-Type AVP indicating the type of events being notified.

Based on local policy rules and per-IP connectivity user privacy information previously received from the UAAF, the CLF may also include additional information in the Event Registration/Deregistration Request. Table 2e provides an indication of the AVPs that may be returned for each event.

Table 2e: Request-Information to AVP mapping

Event	AVP
USER-LOGON	IP-Connectivity-Status
LOCATION-INFORMATION-CHANGED	Location-Information
POLICY-CONTROL-CONTACT-POINT-CHANGED	Policy-Control-Contact-Point
ACCESS-NETWORK-TYPE -CHANGED	Access-Network-Type
TERMINAL-TYPE -CHANGED	Terminal-Type
LOGICAL-ACCESS-ID-CHANGED	Logical-Access-Id
PHYSICAL-ACCESS-ID-CHANGED	Physical Access-Id
INITIAL-GATE-SETTING-CHANGED	Initial-Gate-Setting
QOS-PROFILE-CHANGED	QoS-Profile
IP-ADDRESS-CHANGED	Globally-Unique-Address
USER-LOGOFF	IP-Connectivity-Status

5.2.3.3 Procedure at the AF side

Upon reception of a Notification Event Request, the AF shall:

1) If neither the globally unique identifier contained in the Globally-Unique-Address AVP nor the IP connectivity user ID contained in the User-Name AVP are known, return a Notification Event Response with a Result-Code AVP value set to DIAMETER_ERROR_USER_UNKNOWN.

2) If the event type contained in the Event-Type AVP is not known, return a Notification Event Response with a Result-Code AVP value set to DIAMETER_INVALID_AVP_VALUE.

3) If the event type contained in the Event-Type AVP is known but was not expected, return a Notification Event Response with a Result-Code AVP value set to DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA.

If the AF cannot process the event for reasons not stated in the above steps return a Notification Event 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. After a provisioned number of unsuccessful retries, the CLF is expected to delete the AF-Identity from the list of application functions registered to the event.

Otherwise, the event shall be processed and the AF shall return the Result-Code AVP set to DIAMETER_SUCCESS in the Notification Event Response.

6 Use of the Diameter base protocol

6.0 General

With the clarifications listed in the following clauses the Diameter Base Protocol defined by IETF RFC 6733 [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 IETF 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 IETF RFC 6733 [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 IETF RFC 2960 [9] and shall utilize the new SCTP checksum method specified in IETF 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 IP connectivity user/session, 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 DIAMETER agent, based on the Diameter routing table in the client. The DIAMETER agent shall act as a DIAMETER relay or proxy as described in IETF RFC 6733 [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 or from the Origin-Host AVP learned from the AF in the Event Registration Request (if any). 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 16777231 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 indicates the manufacturer of the Diameter node as per IETF RFC 6733 [10].

7 DIAMETER application

7.0 General

The Diameter Base Protocol as specified in IETF RFC 6733 [10] is used to support information transfer on the e2 interface.

IETF RFC 6733 [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.

7.1 Commands

7.1.0 General

Only the following commands defined in ETSI 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
Subscribe-Notifications-Request	SNR	308
Subscribe-Notifications-Answer	SNA	308
Push-Notification-Request	PNR	309
Push-Notification-Answer	PNA	309

AVPs defined in ETSI 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 ETSI TS 129 329 [7] and used with additional AVPs defined in the present document.

NOTE: In the context of the present document the user whose data is requested using the UDR command is the IP connectivity user.

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]
                            [Global-Access-Id]
                            [AF-Application-Identifier]
                            *[Requested-Information]
                            [Port-Number]
                            *[ 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 ETSI 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 ETSI 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]
                          [Logical-Access-Id]
                          [Physical-Access-Id]
                          [Access-Network-Type]
                          [Location-Information]
                          [Policy-Control-Contact-Point]
                          [Terminal-Type]
                          [Emergency-Call-Routing-Info]
                          *[ AVP ]
                          *[ Failed-AVP ]
                          *[ Proxy-Info ]
                          *[ Route-Record ]
```

7.1.3 Subscribe-Notifications-Request (SNR) Command

The Subscribe-Notifications-Request (SNR) command, indicated by the Command-Code field set to 308 and the "R" bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request notifications of events. This command is defined in ETSI TS 129 329 [7] and used with additional AVPs defined in the present document.

Message Format:

```
< Subscribe-Notifications-Request > ::= < Diameter Header: 308, REQ, PXY, 16777231 >
                                        < Session-Id >
                                        { Vendor-Specific-Application-Id }
                                        { Auth-Session-State }
                                        { Origin-Host }
                                        { Origin-Realm }
                                        [ Destination-Host ]
                                        { Destination-Realm }
                                        { Subs-Req-Type }
                                        [ Expiry-Time ]
                                        [Globally-Unique-Address]
                                        [User-Name]
                                        [AF-Application-Identifier]
                                        *[Event-Type]
                                        *[ AVP ]
                                        *[ Proxy-Info ]
                                        *[ Route-Record ]
```

7.1.4 Subscribe-Notifications-Answer (SNA) Command

The Subscribe-Notifications-Answer (SNA) command, indicated by the Command-Code field set to 308 and the "R" bit cleared in the Command Flags field, is sent by a server in response to the Subscribe-Notifications-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in clause 6.2 or in ETSI TS 129 229 [6].

Message Format:

```
< Subscribe-Notifications-Answer > ::=  < Diameter Header: 308, PXY, 16777231 >
                                        < Session-Id >
                                        { Vendor-Specific-Application-Id }
                                        { Auth-Session-State }
                                        [ Result-Code ]
                                        [ Experimental-Result ]
                                        { Origin-Host }
                                        { Origin-Realm }
                                        [ Expiry-Time ]
                                        *[ AVP ]
                                        *[ Failed-AVP ]
                                        *[ Proxy-Info ]
                                        *[ Route-Record ]
```

7.1.5 Push-Notification-Request (PNR) 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 ETSI TS 129 329 [7] and used with additional AVPs defined in the present document.

NOTE: In the context of the present document the user whose data are pushed using the PNR command is the IP connectivity user.

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 }
```

```
                                    *[Event-Type]
                                    [Globally-Unique-Address]
                                    [User-Name]
                                    [Access-Network-Type]
                                    [Location-Information]
                                    [Policy-Control-Contact-Point]
                                    [Terminal-Type]
                                    [Logical-Access-Id]
                                    [Physical-Access-Id]
                                    [Access-Network-Type]
                                    [Initial-Gate-Setting]
                                    *[QoS-Profile]
                                    [IP-Connectivity-Status]
                                    *[ AVP ]
                                    *[ Proxy-Info ]
                                    *[ Route-Record ]
```

7.1.6 Push-Notifications-Answer (PNA) 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. The Experimental-Result AVP may contain one of the values defined in clause 6.2 or in ETSI TS 129 229 [6].

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 }
                                    *[ AVP ]
                                    *[ Failed-AVP ]
                                    *[ Proxy-Info ]
                                    *[ Route-Record ]
```

7.2 Result-Code AVP values

7.2.0 General

This clause defines new result code values that shall 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 ETSI TS 129 229 [6] is used in the present document:

- DIAMETER_ERROR_USER_UNKNOWN (5001).

The following error defined in ETSI TS 129 329 [7] is used in the present document:

- DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA (5107).

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 ETSI TS 129 329 [7] is used in the present document:

- DIAMETER_USER_DATA_NOT_AVAILABLE (4100).

7.3 AVPs

7.3.0 General

This clause summarizes the AVP used in the present document, beyond those defined in the Diameter Base Protocol.

Table 4 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
Policy-Control-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
Event-Type	354	7.3.6	Enumerated	V	M			Yes
Line-Identifier	500	7.3.5	OctetString	V			M	Yes
Civic-Location	355	7.3.1A	OctetString	V			M	Yes
Geospatial-Location	356	7.3.1B	OctetString	V			M	Yes
Global-Access-Id	357	7.3.7	Grouped	V			M	Yes
Fixed-Access-ID	358	7.3.8	Grouped	V			M	Yes
Relay-Agent	359	7.3.9	OctetString	V	M			Yes
Operator-Specific-GI	360	7.3.10	OctetString	V			M	Yes
Emergency-Call-Routing-Info	361	7.3.11	UTF8String	V	M			Yes
Port-Number	362	7.3.12	Unsigned32	V	M			Yes
PIDF-Location-Object	363	7.3.13	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. For further details, see ETSI TS 129 229 [6].								

Table 5 describes the Diameter AVPs defined for the Gq interface protocol (ETSI 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 ETSI TS 129 209 [8] but not listed in table 5 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 ETSI TS 129 209 [8]	OctetString	M,V				Yes

Table 6 describes the Diameter AVPs defined for the e4 specification ETSI 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 ETSI ES 283 034 [5] but not listed in table 6 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 ETSI ES 283 034 [5]	Grouped	M,V				Yes
Logical-Access-Id	302	See ETSI ES 283 034 [5]	OctetString	V	M			Yes
Access-Network-Type	306	See ETSI ES 283 034 [5]	Grouped	V	M			Yes
Initial-Gate-Setting	303	See ETSI ES 283 034 [5]	Grouped	V	M			Yes
QoS-Profile	304	See ETSI ES 283 034 [5]	Grouped	V	M			Yes
IP-Connectivity-Status	305	See ETSI ES 283 034 [5]	Enumerated	V	M			Yes
Physical-Access-ID	313	See ETSI ES 283 034 [5]	UTF8String	V	M			Yes

Table 7a describes the Diameter AVPs defined for the Sh interface specification ETSI TS 129 329 [7] 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 ETSI TS 129 329 [7] but not listed in table 7a 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 3GPP (10415).

Table 7a: Diameter AVPs imported from Sh specifications

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
Expiry-Time	709	See ETSI TS 129 329 [7]	Time	V			M	Yes
Subs-Req-Type	705	See ETSI TS 129 329 [7]	Enumerated	M,V				Yes

Table 8 describes the Diameter AVPs defined for the 3GPP Gi/SGi interface specification ETSI TS 129 061 [20] 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 ETSI TS 129 061 [20] but not listed in table 8 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 3GPP (10415).

Table 8: Diameter AVPs imported from Sh specifications

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
3GPP-User-Location-Info	22	See ETSI TS 129 061 [20]	OctetString	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]
      [Civic-Location]
      [Geospatial-Location]
      [Operator-Specific-GI]
      [PIDF-Location-Object]
      *[AVP]
```

7.3.1A Civic-Location AVP

The Civic-Location AVP (AVP code 355 13019) provides location information in a form based on the encoding format defined in section 3.1 of IETF RFC 4776 [15] excluding the first 3 octets (i.e. the code for this DHCP option, the length of the DHCP option, and the "what" element).

7.3.1B Geospatial-Location AVP

The Geospatial-Location AVP (AVP code 356 13019) provides location information using the Location Configuration Information (LCI) format defined in IETF RFC 3825 [16], starting with the third octet (i.e. the code for the DHCP option and the length field is not included).

7.3.2 Policy-Control-Contact-Point AVP

The RACS-Contact-Point AVP (AVP code 351 13019) is of type DiameterIdentity and identifies a policy control 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:

- NASS-USER-ID (0).
- LOCATION-INFORMATION (1).
- POLICY-CONTROL-CONTACT-POINT (2).
- ACCESS-NETWORK-TYPE (3).
- TERMINAL-TYPE (4).
- LOGICAL-ACCESS-ID (5).
- PHYSICAL-ACCESS-ID (6).
- EMERGENCY-CALL-ROUTING-INFO (11).

The following values are reserved for future use. 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:

- 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 (AVP code 500 13019) is of type OctetString and identifies the line to which the user equipment is connected.

The contents of the OctetString value shall be a text string that conform to the following ABNF specification using the notation defined in IETF RFC 4234 [17]:

value = network-operator-code SEMI location-area-code [SEMI line-code]

network-operator-code = "noc" EQUAL 3ALPHA 1*6ALPHANUM

location-area-code = "lac" EQUAL 4HEXDIG

line-code = "line-code" EQUAL 4*HEXDIG

EQUAL = "="

SEMI = ";"

ALPHANUM = ALPHA / DIGIT

The Network-Operator-Code (NOC) consists of a country code followed by the International Telecommunication Union (ITU) Carrier Code (ICC) identifying a unique network operator within a country (see Recommendation ITU-T M.1400 [18]). The value of the "noc" parameter shall be set to an three uppercase ASCII characters containing a three-letter alphabetic country code as defined in ISO 3166-1 [19], followed by an ICC value of one to six uppercase alphanumeric ASCII characters containing the carrier code.

The Location-Area-Code (LAC) uniquely identifies a geographical location area within a network. The value of the "lac" parameter shall be a 2 octets binary value and its hexadecimal representation shall be encoded as a text string.

The Line-Code (line-code) uniquely identifies a logical (or physical) access within a network or within a location area (depending on the network operator implementation). The value of the "line-code" parameter shall be at least a 2 octets binary value and its hexadecimal representation shall be encoded as a text string.

7.3.6 Event-Type AVP

The Event-Type AVP (AVP code 354 13019) is of type Enumerated. The following values are defined:

- USER-LOGON (0).
- LOCATION-INFORMATION-CHANGED (1).
- POLICY-CONTROL-CONTACT-POINT-CHANGED (2).
- ACCESS-NETWORK-TYPE -CHANGED (3).
- TERMINAL-TYPE-CHANGED (4).
- LOGICAL-ACCESS-ID-CHANGED (5).
- PHYSICAL-ACCESS-ID-CHANGED (6).
- IP-ADDRESS-CHANGED (7).
- INITIAL-GATE-SETTING-CHANGED (8).
- QOS-PROFILE-CHANGED (9).
- USER-LOGOFF (10).

The USER-LOGON event is reported when the CLF successfully creates a session record.

The USER-LOGOFF event is reported when the CLF suppresses a session record.

All other events are reported when the related part of the session record is modified.

7.3.7 Global-Access-Id AVP

The Global-Access-Id AVP (AVP code 357 13019) is of type Grouped.

AVP Format:

```
Global-Access-Id ::= < AVP Header: 357 13019 >
          [Fixed-Access-ID]
          [3GPP-User-Location-Info]
          *[AVP]
```

7.3.8 Fixed-Access-ID AVP

The Fixed-Access-ID AVP (AVP code 358 13019) is of type Grouped. Either a Logical-Access-ID or a Physical-Access-ID AVP shall be present.

AVP Format:

```
    Fixed-Access-ID ::= < AVP Header: 358 13019 >
          {Relay-Agent}
          [Logical-Access-ID]
          [Physical-Access-ID]
          *[AVP]
```

7.3.9 Relay-Agent AVP

The Relay-Agent AVP (AVP code 359 13019) is of type OctetString and identifies the entity that has assigned an identifier to a logical or physical access.

7.3.10 Operator-Specific-GI AVP

The Operator-Specific-GI AVP (AVP code 360 13019) is of type OctetString and identifies the location where the user equipment is camping, using an operator-specific format, as specified in ETSI TS 124 229 [21].

7.3.11 Emergency-Call-Routing-Info

The Emergency-Call-Routing-Info AVP (AVP code 361 13019) is of type UTF8String and provides a URI where to route emergency calls, encoded as a text string according to IETF RFC 3986 [22].

7.3.12 Port-Number

The Port-Number (AVP code 362 13019) is of type Unsigned32 and contains a port number.

7.3.13 PIDF-Location-Object

The PIDF-Location-Object AVP (AVP code 363 13019) is of type UTF8String and contains a PIDF LO element according to IETF RFC 4119 [23].

7.4 Use of namespaces

7.4.0 General

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 ETSI TS 129 329 [7] and modified by ETSI ES 283 034 [5].

7.4.4 Application-ID value

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

Annex A (informative): Application to NGN Architectures

A.1 Overview

In an NGN architecture (ETSI ES 282 001 [i.1]), a CLF is a functional entity of the Network Attachment Sub-System (NASS) defined in ETSI ES 282 004 [i.2]. The information it stores is made accessible to other subsystems and applications through the following two interfaces (see figure A.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 ETSI ES 282 003 [i.3].

The present document specifies the protocol for the e2 interface.

Examples of Application Functions in NGN architectures are the P-CSCF and the IBCF in the IMS (ETSI ES 282 007 [i.4]), certain categories of Application Server Functions (ASF) (ETSI ES 282 001 [i.1]) or a Presence Network Agent (PNA) as defined in ETSI TS 182 008 [13]. In the later case, the Pn reference point of the presence architecture is mapped to the e2 interface.

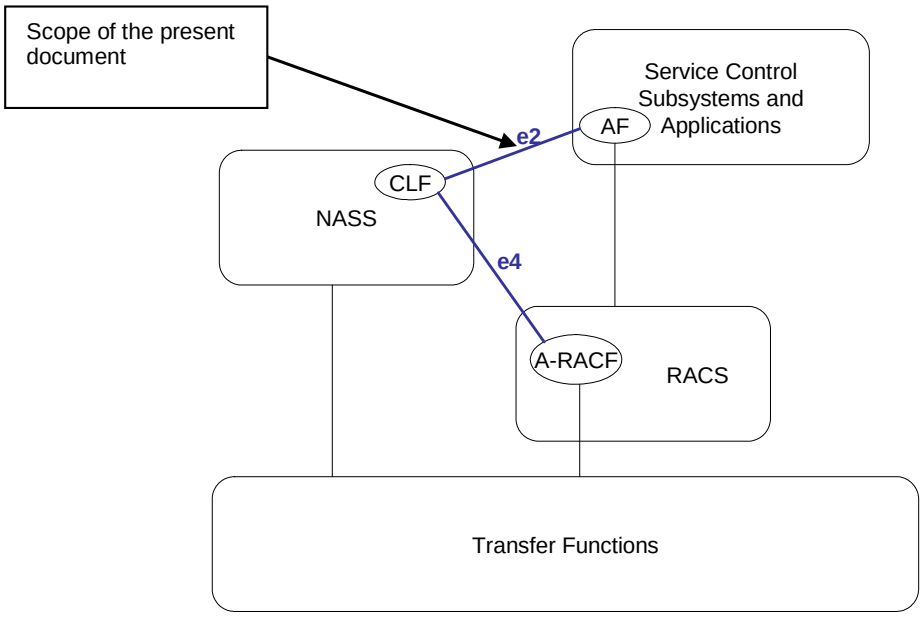

Figure A.1: NASS external interfaces

A.2 Mapping of e2 operations and terminology to Diameter

A DIAMETER Agent plays the role of the "CLF Proxy" described in clause 7.1 of ETSI ES 282 004 [i.2].

Table A.1 defines the mapping between information flows defined in ETSI ES 282 004 [i.2] and Diameter commands.

Table A.1: e2 message to Diameter command mapping

e2 Information flow	Source	Destination	Command-Name	Abbreviation
Information Query Request	AF	CLF	User-Data-Request	UDR
Information Query Response	CLF	AF	User-Data-Answer	UDA
Event Registration Request	AF	CLF	Subscribe-Notifications-Request	SNR
Event Registration Response	CLF	AF	Subscribe-Notifications-Answer	SNA
Notification Event Request	CLF	AF	Push-Notification-Request	PNR
Notification Event Response	AF	CLF	Push-Notification-Answer	PNA

Annex B (informative): Change history

Change history							
Date	**WG Doc.**	**CR**	**Rev**	**CAT**	**Title/Comment**	**Current Version**	**New Version**
03-09-07	13b164r1	001		B	Event Management Capabilities	1.2.1	2.0.0
03-09-07	14bTD051r1	002		F	Alignment with Stage 2	2.0.1	2.0.3
13-09-07	14tTD302r1	003		F	Destination-Host AVP in Routing Considerations	2.0.3	2.1.1
13-09-07	14tTD303r1	004		F	Expiry-Time AVP	2.0.3	2.1.1
13-09-07	14tTD304r1	005		F	Proxy in Routing Considerations	2.0.3	2.1.1
13-09-07	14tTD392r1	006		D	Terminology Alignment for Notification Events with NASS R2	2.0.3	2.1.1
02-11-07	15bTD120r3	007		F	Correction to transient failure error response	2.1.1	2.2.0
02-11-07	15bTD260r1	008		D	WI03116 Clarification on CLF Proxy in Routing Considerations	2.1.1	2.2.0
02-11-07	15bTD262r2	009		D	WI03116 IP connectivity user	2.1.1	2.2.0
30-11-07	WG3TD054r1	010		F	Location Information formats	2.2.0	2.3.0
30-11-07	WG3TD056r1	011		D	Moving the definition of the Location Identifier AVP from ETSI TS 183 003 to ETSI ES 283 035	2.2.0	2.3.0
07-03-08	16bTD104r1	012		F	Structure of location data	2.3.0	2.5.0
07-03-08	16bTD106r1	013		F	Miscellaneous Improvements	2.3.0	2.5.0
07-03-08	16bTD113	014		F	Line identifier	2.3.0	2.5.0
19-03-13	NTECH(13)02_005	015		F	Line Identifier Coding	2.5.1	2.5.2
27-03-14	NTECH(14)06_023	018		F	NASS User Id	2.6.1	3.0.0
26-06-14	NTECH(14)07_005r2	019		B	Extensions of the CLF querying capabilities	3.0.0	3.1.0
26-06-14	NTECH(14)07_009	020		F	Wrong Vendor Id		
04-09-14 16-12-14	NTECH(14)08_006r1 NTECH(14)09_005	021 022		B F	M.493 extensions and final corrections	3.1.0	3.1.1
10-06-16	NTECH(15)12_002	023		F	Inconsistencies between tabular description and ABNF	3.1.1	3.2.1

History

Document history		
V1.1.1	July 2006	Publication
V1.2.1	June 2007	Publication
V2.5.1	August 2008	Publication
V2.6.1	January 2014	Publication
V2.7.1	July 2014	Publication
V3.1.1	April 2015	Publication
V3.2.1	November 2017	Membership Approval Procedure MV 20180123: 2017-11-24 to 2018-01-23