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

Intellectual Property Rights .............................................................................................................................................. 5
Foreword .................................................................................................................................................................................. 5
1 Scope .................................................................................................................................................................................. 6
2 References .......................................................................................................................................................................... 6
2.1 Normative references ...................................................................................................................................................... 6
2.2 Informative references .................................................................................................................................................... 7
3 Definitions and abbreviations .............................................................................................................................................. 7
3.1 Definitions .......................................................................................................................................................................... 7
3.2 Abbreviations ..................................................................................................................................................................... 8
4 Overview ............................................................................................................................................................................... 8
5 Procedure descriptions .......................................................................................................................................................... 9
5.1 General ............................................................................................................................................................................... 9
5.2 Procedures on the CLF - AF interface ..................................................................................................................................... 10
5.2.1 Information query .................................................................................................................................................. 10
5.2.1.1 Overview ..................................................................................................................................................... 10
5.2.1.2 Procedure at the AF side ......................................................................................................................... 11
5.2.1.3 Procedure at the CLF side ....................................................................................................................... 11
5.2.2 Event Registration/Deregistration .................................................................................................................................. 12
5.2.2.1 Overview ..................................................................................................................................................... 12
5.2.2.2 Procedure at the AF side .................................................................................................................................. 12
5.2.2.3 Procedure at the CLF side .................................................................................................................................. 13
5.2.3 Notification Events .................................................................................................................................................. 14
5.2.3.1 Overview ..................................................................................................................................................... 14
5.2.3.2 Procedure at the CLF side .................................................................................................................................. 14
5.2.3.3 Procedure at the AF side .................................................................................................................................. 15
6 Use of the Diameter base protocol .................................................................................................................................... 16
6.1 Securing Diameter messages .......................................................................................................................................... 16
6.2 Accounting functionality .................................................................................................................................................. 16
6.3 Use of sessions ............................................................................................................................................................... 16
6.4 Transport protocol ........................................................................................................................................................... 16
6.5 Routing considerations ................................................................................................................................................... 16
6.6 Advertising application support ...................................................................................................................................... 17
7 DIAMETER application ..................................................................................................................................................... 17
7.1 Commands .......................................................................................................................................................................... 17
7.1.1 User-Data-Request command ................................................................................................................................... 18
7.1.2 User-Data-Answer command ................................................................................................................................... 18
7.1.3 Subscribe-Notifications-Request (SNR) Command ..................................................................................................... 19
7.1.4 Subscribe-Notifications-Answer (SNA) Command ..................................................................................................... 19
7.1.5 Push-Notification-Request (PNR) Command ............................................................................................................. 19
7.1.6 Push-Notifications-Answer (PNA) Command ............................................................................................................. 20
7.2 Result-Code AVP values .................................................................................................................................................. 20
7.2.1 Success ......................................................................................................................................................................... 20
7.2.2 Permanent failures ..................................................................................................................................................... 21
7.2.3 Transient failures ....................................................................................................................................................... 21
7.3 AVPs .................................................................................................................................................................................. 21
7.3.1 Location-Information AVP ....................................................................................................................................... 22
7.3.1A Civic-Location AVP ............................................................................................................................................... 22
7.3.1B Geospatial-Location AVP ..................................................................................................................................... 23
7.3.2 RACS-Contact-Point AVP ..................................................................................................................................... 23
7.3.3 Terminal-Type AVP ................................................................................................................................................... 23
7.3.4 Requested-Information AVP ................................................................................................................................... 23
7.3.5 Line-Identifier AVP .................................................................................................................................................. 23
7.3.6  Event-Type AVP .................................................................................................................. 24
7.4   Use of namespaces .............................................................................................................. 24
7.4.1  AVP codes ............................................................................................................................ 24
7.4.2  Experimental-Result-Code AVP values ........................................................................... 25
7.4.3  Command Code values ..................................................................................................... 25
7.4.4  Application-ID value ........................................................................................................ 25

Annex A (informative):  Mapping of e2 operations and terminology to Diameter......................... 26
Annex B (informative):  Change history .......................................................................................... 27
History .............................................................................................................................................. 28
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).
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

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

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

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

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


[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".
ETSI ES 283 035 V2.5.1 (2008-08)

7

3 Definitions and abbreviations

3.1 Definitions

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

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

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

2.2 Informative references

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

Not applicable.
Attribute-Value Pair (AVP): corresponds to an Information Element in a Diameter message

NOTE: See RFC 3588 [10].

NASS User: See definition in [2].

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
- DHCP: Dynamic Host Configuration Protocol
- 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
- NOC: Network-Operator-Code
- P-CSCF: Proxy Call Session Control Function
- PDBF: Profile Data Base Function
- 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
- SPDF: Service-based Policy Decision Function
- UAAF: User Authentication and Authorization Function
- UDA: User-Data-Answer
- UDR: User-Data-Request

4 Overview

The Network Attachment Sub-System (NASS) defined in ES 282 004 [2] maintains information about IP-connectivity access sessions associated with NASS Users connected to the TISPAN network. This information is stored in the Connectivity session Location and repository Function (CLF) in the form of access records 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 network architecture offering - or providing access to - 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 and the IBCF in the IMS (ES 282 007 [4]), 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.

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 request**

<table>
<thead>
<tr>
<th>Information element name</th>
<th>Mapping to diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Globally unique IP Address</td>
<td>Globally-Unique-Address</td>
<td>C</td>
<td>This information element contains:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-The IP address of the NASS User for which profile information is being pushed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-The addressing domain in which the IP address is significant.</td>
</tr>
<tr>
<td>NASS User ID</td>
<td>User-Name</td>
<td>C</td>
<td>The identity of the NASS User that is attached to the network.</td>
</tr>
<tr>
<td>AF Identity</td>
<td>AF-Application-Identifier</td>
<td>M</td>
<td>Identifies the AF originating the request.</td>
</tr>
<tr>
<td>Requested-items</td>
<td>Requested-Information</td>
<td>O</td>
<td>The list of items requested by the AF.</td>
</tr>
</tbody>
</table>

**NOTE:** Either the Globally-Unique-IP-Address or the NASS User ID shall be included.
Table 2: Information query response

<table>
<thead>
<tr>
<th>Information element name</th>
<th>Mapping to diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>Result-Code / Experimental_Result</td>
<td>M</td>
<td>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.</td>
</tr>
<tr>
<td>NASS User ID</td>
<td>User-Name</td>
<td>O</td>
<td>The identity of the NASS User that is attached to the network.</td>
</tr>
<tr>
<td>Location Information</td>
<td>Location-Information</td>
<td>O</td>
<td>Location information (or a pointer to such information) in a form that is suitable for the requesting application.</td>
</tr>
<tr>
<td>RACS contact point</td>
<td>RACS-Contact-Point</td>
<td>O</td>
<td>The FQDN or IP address of the RACS entity where resource request shall be sent (i.e. SPDF address).</td>
</tr>
<tr>
<td>Access Network Type</td>
<td>Access-Network-Type</td>
<td>O</td>
<td>The type of access network over which IP connectivity is provided to the user equipment.</td>
</tr>
<tr>
<td>Terminal Type</td>
<td>Terminal-Type</td>
<td>O</td>
<td>The type of user equipment to which the IP address was allocated.</td>
</tr>
<tr>
<td>Logical Access ID</td>
<td>Logical-Access-Id</td>
<td>O</td>
<td>The identity of the logical access where the user equipment is connected.</td>
</tr>
<tr>
<td>Physical Access ID</td>
<td>Physical-Access-Id</td>
<td>O</td>
<td>The identity of the physical access where the user equipment is connected.</td>
</tr>
</tbody>
</table>

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 NASS 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.
If a unique NASS user record can be retrieved, the CLF shall:

1) Check which session data can be returned to the AF, based on the contents of the Requested-Information AVP, local policy rules and per-NASS user privacy information previously received from the UAAF/PDBF and stored in the CLF.

   NOTE 1: If the Requested-Information AVP is not received, the list of requested information is inferred from the AF identity.

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 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 2: Due to the application of operator's policies and NASS 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 TS 129 329 [7].

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

<table>
<thead>
<tr>
<th>Information element name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subs-Req-Type</td>
<td></td>
<td>M</td>
<td>Indicates whether the AF is willing to subscribe or unsubscribe to the notification of the event.</td>
</tr>
<tr>
<td>NASS User ID</td>
<td>User-Name</td>
<td>C</td>
<td>The identity of the NASS User on behalf of which the event is to be reported.</td>
</tr>
<tr>
<td>Globally unique IP Address</td>
<td>Globally Unique Address</td>
<td>C</td>
<td>This information element contains the IP address of the NASS User on behalf of which the event is to be reported, together with the addressing domain in which the IP address is significant.</td>
</tr>
<tr>
<td>Expiry-Time</td>
<td></td>
<td>O</td>
<td>Moment of expiration of the subscription to the event.</td>
</tr>
<tr>
<td>Event</td>
<td>Event-Type</td>
<td>M</td>
<td>The type of event to be monitored.</td>
</tr>
<tr>
<td>AF Identity</td>
<td>AF-Application-Identifier</td>
<td>M</td>
<td>Identifies the AF originating the request.</td>
</tr>
</tbody>
</table>
### Table 2b: Event Registration/Deregistration Response

<table>
<thead>
<tr>
<th>Information element name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>Result-Code / Experimental_Result</td>
<td>M</td>
<td>Result of the request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Expiry-Time</td>
<td></td>
<td>O</td>
<td>Acknowledges the absolute time at which the subscription expires.</td>
</tr>
</tbody>
</table>

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:

1) Insert a Subs-Req-Type AVP indicating whether it is willing to subscribe or unsubscribe to the notification of events.
2) 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 NASS 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.
3) The AF-Application-Identifier AVP shall be present.
4) At least one occurrence of the Event-Type AVP shall be present.
5) 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-NASS 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:

6) 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.

7) 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.

8) 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 fulfill 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 TS 129 329 [7].

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

<table>
<thead>
<tr>
<th>Information element name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NASS User ID</td>
<td>User-Name</td>
<td>C</td>
<td>The identity of the NASS User on behalf of which the event is to be reported.</td>
</tr>
<tr>
<td>Globally unique IP Address</td>
<td>Globally Unique Address</td>
<td>C</td>
<td>This information element contains:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- The IP address of the NASS User on behalf of which the event is to be</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>reported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- The addressing domain in which the IP address is significant.</td>
</tr>
<tr>
<td>AF Identity</td>
<td>AF-Application-Identifier</td>
<td>M</td>
<td>Identifies the AF having registered to the request.</td>
</tr>
<tr>
<td>Event</td>
<td>Event-Type</td>
<td>M</td>
<td>The type of event to be monitored.</td>
</tr>
<tr>
<td>[AVP]</td>
<td></td>
<td>O</td>
<td>AVPs carrying CLF information associated to the reported event.</td>
</tr>
</tbody>
</table>
### Table 2d: Notification Event Response

<table>
<thead>
<tr>
<th>Information element name</th>
<th>Mapping to Diameter AVP</th>
<th>Cat.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>Result-Code / Experimental_Result</td>
<td>M</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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-NASS 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

<table>
<thead>
<tr>
<th>Event</th>
<th>AVP</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER-LOGON</td>
<td>IP-Connectivity-Status</td>
</tr>
<tr>
<td>LOCATION-INFORMATION-CHANGED</td>
<td>Location-Information</td>
</tr>
<tr>
<td>RACS-CONTACT-POINT-CHANGED</td>
<td>RACS-Contact-Point</td>
</tr>
<tr>
<td>ACCESS-NETWORK-TYPE-CHANGED</td>
<td>Access-Network-Type</td>
</tr>
<tr>
<td>TERMINAL-TYPE-CHANGED</td>
<td>Terminal-Type</td>
</tr>
<tr>
<td>LOGICAL-ACCESS-ID-CHANGED</td>
<td>Logical-Access-Id</td>
</tr>
<tr>
<td>PHYSICAL-ACCESS-ID-CHANGED</td>
<td>Physical Access-Id</td>
</tr>
<tr>
<td>INITIAL-GATE-SETTING-CHANGED</td>
<td>Initial-Gate-Setting</td>
</tr>
<tr>
<td>QOS-PROFILE-CHANGED</td>
<td>QoS-Profile</td>
</tr>
<tr>
<td>IP-ADDRESS-CHANGED</td>
<td>Globally-Unique-Address</td>
</tr>
<tr>
<td>USER-LOGOFF</td>
<td>IP-Connectivity-Status</td>
</tr>
</tbody>
</table>

### 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 NASS 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

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 NASS 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 plays the role of the "CLF Proxy" described in clause 7.1 of ES 282 0004 [2]. The DIAMETER agent shall act as a DIAMETER relay or proxy 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 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 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>
<thead>
<tr>
<th>Command-Name</th>
<th>Abbreviation</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Data-Request</td>
<td>UDR</td>
<td>306</td>
</tr>
<tr>
<td>User-Data-Answer</td>
<td>UDA</td>
<td>306</td>
</tr>
<tr>
<td>Subscribe-Notifications-Request</td>
<td>SNR</td>
<td>308</td>
</tr>
<tr>
<td>Subscribe-Notifications-Answer</td>
<td>SNA</td>
<td>308</td>
</tr>
<tr>
<td>Push-Notification-Request</td>
<td>PNR</td>
<td>309</td>
</tr>
<tr>
<td>Push-Notification-Answer</td>
<td>PNA</td>
<td>309</td>
</tr>
</tbody>
</table>

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.

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

Message Format:

```plaintext
<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:

```plaintext
<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]
  [RACS-Contact-Point]
  [Terminal-Type]
  *[ 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 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 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 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 NASS 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 }
*[EventType]
[Globally-Unique-Address]
[User-Name]
[Access-Network-Type]
[Location-Information]
[RACS-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 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

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).**

The following error defined in 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 TS 129 329 [7] 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.

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>
<thead>
<tr>
<th>Attribute name</th>
<th>AVP Code</th>
<th>Clause defined</th>
<th>Value type</th>
<th>Must</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location-Information</td>
<td>350</td>
<td>7.3.1</td>
<td>Grouped</td>
<td>V</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RACS-Contact-Point</td>
<td>351</td>
<td>7.3.2</td>
<td>DiameterIdentity</td>
<td>V</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminal-Type</td>
<td>352</td>
<td>7.3.3</td>
<td>OctetString</td>
<td>V</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requested-Information</td>
<td>353</td>
<td>7.3.4</td>
<td>Enumerated</td>
<td>V</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event-Type</td>
<td>354</td>
<td>7.3.6</td>
<td>Enumerated</td>
<td>V</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line-Identifier</td>
<td>500</td>
<td>7.3.5</td>
<td>OctetString</td>
<td>V</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Civic-Location</td>
<td>355</td>
<td>7.3.1.A</td>
<td>OctetString</td>
<td>V</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Geospatial-Location</td>
<td>356</td>
<td>7.3.1.B</td>
<td>OctetString</td>
<td>V</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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].

Table 5 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

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>AVP Code</th>
<th>Clause defined</th>
<th>Value type</th>
<th>Must</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF-Application-Identifier</td>
<td>504</td>
<td>See TS 129 209 [8]</td>
<td>OctetString</td>
<td>M,V</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6 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 not 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

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>AVP Code</th>
<th>Clause defined</th>
<th>Value type</th>
<th>Must</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May encrypt</th>
</tr>
</thead>
</table>

Table 7a describes the Diameter AVPs defined for the Sh interface specification 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 TS 129 329 [7] 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 7a: Diameter AVPs imported from Sh specifications

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Clause defined</th>
<th>Value Type</th>
<th>Must</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May Encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subs-Req-Type</td>
<td>705</td>
<td>See TS 129 329 [7]</td>
<td>Enumerated</td>
<td>M,V</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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]]
   *[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 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 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 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:

- NASS-USER-ID (0).
- LOCATION-INFORMATION (1).
- RACS-CONTACT-POINT (2).
- ACCESS-NETWORK-TYPE (3).
- TERMINAL-TYPE (4).
- LOGICAL-ACCESS-ID (5).
- PHYSICAL-ACCESS-ID (6).

The following values 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.

- 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 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 = "="
```
SEMIX = ";"
ALPHANUM = ALPHA / DIGIT

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

7.4 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

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

<table>
<thead>
<tr>
<th>e2 message</th>
<th>Source</th>
<th>Destination</th>
<th>Command-Name</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Query Request</td>
<td>AF</td>
<td>CLF</td>
<td>User-Data-Request</td>
<td>UDR</td>
</tr>
<tr>
<td>Information Query Response</td>
<td>CLF</td>
<td>AF</td>
<td>User-Data-Answer</td>
<td>UDA</td>
</tr>
<tr>
<td>Event Registration Request</td>
<td>AF</td>
<td>CLF</td>
<td>Subscribe-Notifications-Request</td>
<td>SNR</td>
</tr>
<tr>
<td>Event Registration Response</td>
<td>CLF</td>
<td>AF</td>
<td>Subscribe-Notifications-Answer</td>
<td>SNA</td>
</tr>
<tr>
<td>Notification Event Request</td>
<td>CLF</td>
<td>AF</td>
<td>Push-Notification-Request</td>
<td>PNR</td>
</tr>
<tr>
<td>Notification Event Response</td>
<td>AF</td>
<td>CLF</td>
<td>Push-Notification-Answer</td>
<td>PNA</td>
</tr>
</tbody>
</table>
Annex B (informative):
Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>WG Doc.</th>
<th>CR</th>
<th>Rev</th>
<th>CAT</th>
<th>Title / Comment</th>
<th>Current Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>03-09-07</td>
<td>13b164r1</td>
<td>001</td>
<td>B</td>
<td></td>
<td>Event Management Capabilities</td>
<td>1.2.1</td>
<td>2.0.0</td>
</tr>
<tr>
<td>03-09-07</td>
<td>14bTD091r1</td>
<td>002</td>
<td>F</td>
<td></td>
<td>Alignment with Stage 2</td>
<td>2.0.1</td>
<td>2.0.3</td>
</tr>
<tr>
<td>13-09-07</td>
<td>14ID030r2</td>
<td>003</td>
<td>F</td>
<td></td>
<td>Destination-Host AVP in Routing Considerations</td>
<td>2.0.3</td>
<td>2.1.1</td>
</tr>
<tr>
<td>13-09-07</td>
<td>14ID030r3</td>
<td>004</td>
<td>F</td>
<td></td>
<td>Expiry-Time AVP</td>
<td>2.0.3</td>
<td>2.1.1</td>
</tr>
<tr>
<td>13-09-07</td>
<td>14ID030r4</td>
<td>005</td>
<td>F</td>
<td></td>
<td>Proxy in Routing Considerations</td>
<td>2.0.3</td>
<td>2.1.1</td>
</tr>
<tr>
<td>13-09-07</td>
<td>14ID039r2</td>
<td>006</td>
<td>D</td>
<td></td>
<td>Terminology Alignment for Notification Events with NASS R2</td>
<td>2.0.3</td>
<td>2.1.1</td>
</tr>
<tr>
<td>02-11-07</td>
<td>15bTD120r3</td>
<td>007</td>
<td>F</td>
<td></td>
<td>Correction to transient failure error response</td>
<td>2.1.1</td>
<td>2.2.0</td>
</tr>
<tr>
<td>02-11-07</td>
<td>15bTD260r1</td>
<td>008</td>
<td>D</td>
<td></td>
<td>WI03116 Clarification on CLF Proxy in Routing Considerations</td>
<td>2.1.1</td>
<td>2.2.0</td>
</tr>
<tr>
<td>02-11-07</td>
<td>15bTD262r2</td>
<td>009</td>
<td>D</td>
<td></td>
<td>WI03116 NASS User</td>
<td>2.1.1</td>
<td>2.2.0</td>
</tr>
<tr>
<td>30-11-07</td>
<td>15G3TD084r1</td>
<td>010</td>
<td>F</td>
<td></td>
<td>Location information formats</td>
<td>2.2.0</td>
<td>2.3.0</td>
</tr>
<tr>
<td>30-11-07</td>
<td>15G3TD056r1</td>
<td>011</td>
<td>D</td>
<td></td>
<td>Moving the definition of the Location Identifier AVP from TS 183 003 to ES 283 035</td>
<td>2.2.0</td>
<td>2.3.0</td>
</tr>
<tr>
<td>07-03-08</td>
<td>16bTD104r1</td>
<td>012</td>
<td>F</td>
<td></td>
<td>Structure of location data</td>
<td>2.3.0</td>
<td>2.5.0</td>
</tr>
<tr>
<td>07-03-08</td>
<td>16bTD106r1</td>
<td>013</td>
<td>F</td>
<td></td>
<td>Miscellaneous Improvements</td>
<td>2.3.0</td>
<td>2.5.0</td>
</tr>
<tr>
<td>07-03-08</td>
<td>16bTD113</td>
<td>014</td>
<td>F</td>
<td></td>
<td>Line identifier</td>
<td>2.3.0</td>
<td>2.5.0</td>
</tr>
</tbody>
</table>
## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>V2.5.0</strong></td>
</tr>
<tr>
<td><strong>V2.5.1</strong></td>
</tr>
</tbody>
</table>