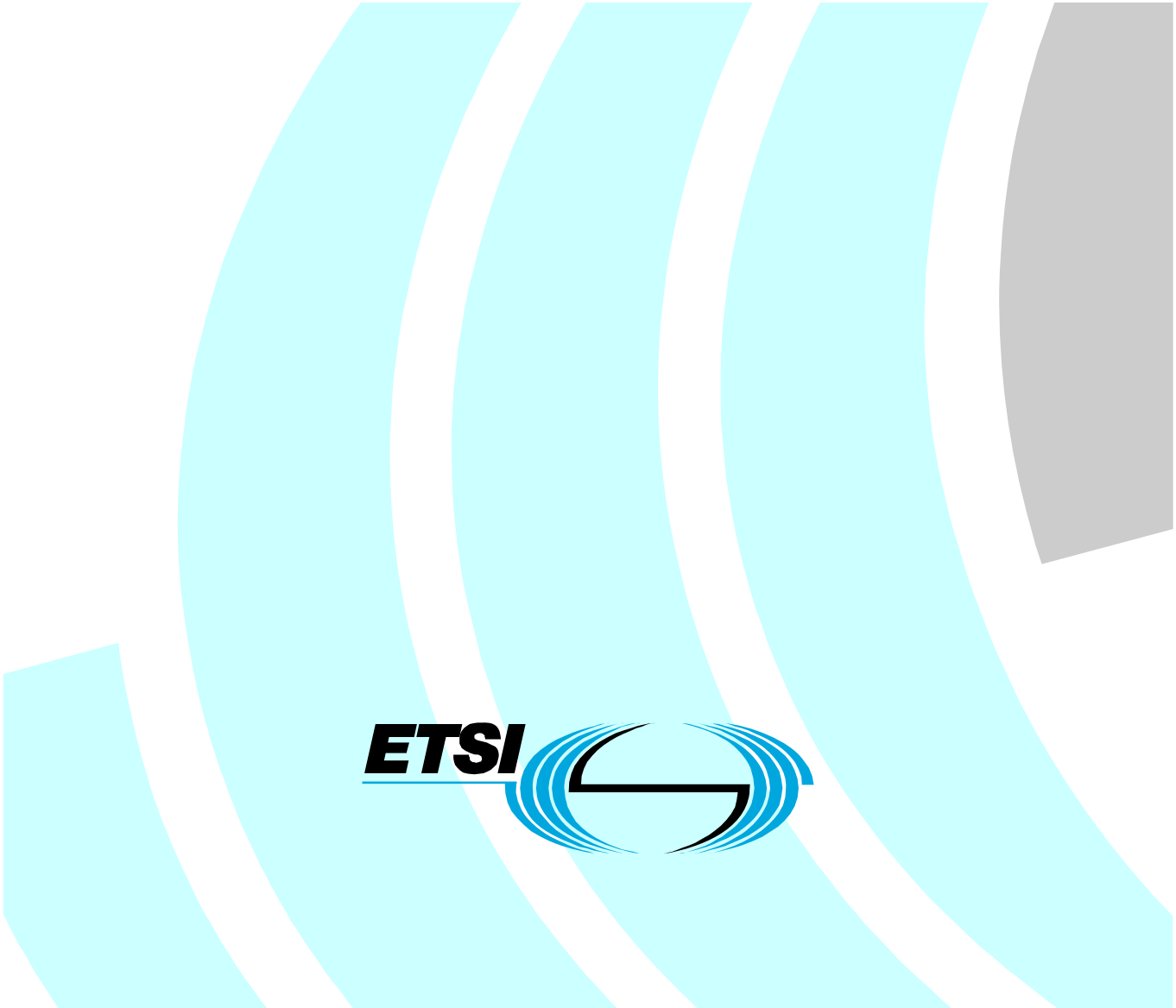
ETSI TS 183 066 V2.1.1 (2009-01)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); a4 interface based on the DIAMETER protocol



Reference
DTS/TISPAN-03189-NGN-R2

Keywords
Stage 3, interface

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

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

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

Foreword

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

1 Scope

The present document defines a protocol applicable to the a4 interface between the User Access Authorization Function (UAAF) and the Connectivity session Location and repository Function (CLF), based on the Diameter protocol.

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

2 References

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

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

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

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

2.1 Normative references

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

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

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

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

[4] 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".

[5] ETSI TS 183 020: " Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment: Roaming in TISPAN NGN Network Accesses; Interface Protocol Definition".

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

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

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

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

[10] ETSI TS 183 059-1: "Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); a2 interface based on the DIAMETER protocol".

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.

3 Definitions and abbreviations

3.1 Definitions

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

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

NOTE: See definition in RFC 3588 [9].

NASS User: See definition in ES 282 004 [1].

3.2 Abbreviations

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

ABNF	Augmented Backus-Naur Form
AVP	Attribute-Value Pair
CLF	Connectivity session Location and repository Function
CNGCF	Customer Network Gateway Configuration Function
DHCP	Dynamic Host Configuration Protocol
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	IP Security
NAS	Network Access Server
NASS	Network Attachment Sub-System
P-CSCF	Proxy Call Session Control Function
PDBF	Profile Data Base Function
PNA	Push-Notification-Answer
PNR	Push-Notification-Request
PPP	Point-to-Point Protocol
RACS	Resource and Admission Control Subsystem
RFC	Request For Comments
SCTP	Stream Control Transport Protocol
UAAF	User Access Authorization Function
UDA	User-Data-Answer
UDR	User-Data-Request

4 Overview

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

The document specifies the protocol for the NASS a4 interface between the User Access Authorization Function (UAAF) and the Connectivity session Location and repository Function (CLF), based on the Diameter protocol.

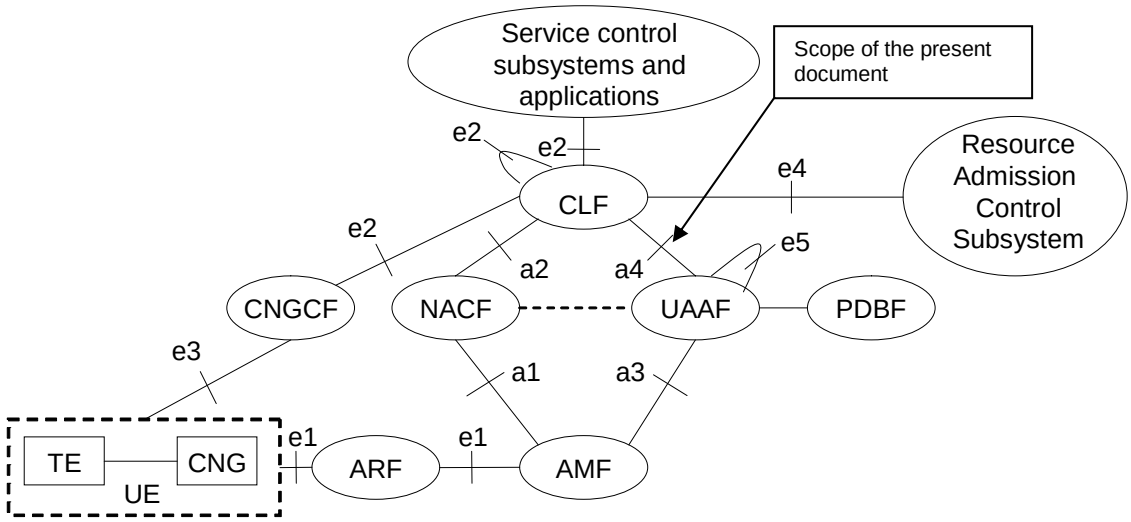


Figure 4.1: a4 interface

The a4 interface allows the CLF to register the association between the NASS User identity and the NASS User preferences regarding the privacy of location information provided by the UAAF. The a4 interface is also used to register NASS User network profile information (QoS profile). The CLF may retrieve the NASS User network profile from the UAAF.

The UAAF - CLF relationship may be operated in pull mode or push mode. The push mode is used when the UAAF is involved in the processing of network access requests in order to authorize or deny access to the network (e.g. when explicit authentication is used). The pull mode is used when implicit authentication is used or in support of CLF recovery procedures.

The following information flows are used on the a4 interface:

- Access Profile Push.
- Access Profile Pull.
- Remove Access Profile.

5 Procedure descriptions

5.1 General

5.1.1 Information elements

The following clauses describe the realization of the functional procedures defined in the NASS (ES 282 004 [1]) using Diameter commands described in clause 7. This involves describing a mapping between the Information Elements defined in the NASS specification (ES 282 004 [1]) and Diameter AVPs.

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

- A mandatory Information Element (marked as (M) in the table) shall always be present in the command. If this Information Element is absent, an application error occurs at the receiver and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.

- A conditional Information Element (marked as (C) in the table) shall be present in the command if certain conditions are fulfilled:

  - If the receiver detects that those conditions are fulfilled and the Information Element is absent, an application error occurs and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element. If multiple Information Elements are missing, all corresponding AVP codes shall be included in the Failed-AVP AVP.

  - If those conditions are not fulfilled, the Information Element shall be absent. If however this Information Element appears in the message, it shall not cause an application error and it may be ignored by the receiver if this is not explicitly defined as an error case. Otherwise, an application error occurs at the receiver and an answer message with the Result-Code set to DIAMETER_AVP_NOT_ALLOWED shall be sent back to the originator of the request. A Failed-AVP AVP containing a copy of the corresponding Diameter AVP shall be included in this message.

- An optional Information Element (marked as (O) in the table) may be present or absent in the command, at the discretion of the application at the sending entity. Absence or presence of this Information Element shall not cause an application error and may be ignored by the receiver.

5.1.2 NASS User profile

NASS User profile information sent over the a4 interface comprises QoS profile information and initial gate setting information. Each of these pieces of information may be sent in the form of an identifier using the QoS-Profile-ID and Initial-Gate-Setting-ID AVPs or in the form of an explicit description using the QoS-Profile-Description and Initial-Gate-Setting-Description AVPs.

Tables 5.1 and 5.2 detail the information elements involved in the second case as defined in the NASS specification ES 282 004 [1] and their mapping to DIAMETER AVPs.

Table 5.1: Initial gate setting description

Information element name	Mapping to Diameter AVP	Cat.	Description
List of allowed destinations as well as multicast flows	NAS-Filter-Rule	O	In case of unicast data, the list of default destination IP addresses, ports, prefixes and port ranges to which traffic can be sent. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs which traffic can be received from by the attached NASS User.
List of denied destinations as well as multicast flows	NAS-Filter-Rule	O	In case of unicast, the list of default destination IP addresses, ports, prefixes and port ranges to which traffic is denied. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs for which traffic towards the attached NASS User must be denied.
UL Subscribed Bandwidth	Maximum-Allowed-Bandwidth-UL	O	The maximum amount of bandwidth that can be used without explicit authorization in the uplink direction.
DL Subscribed Bandwidth	Maximum-Allowed-Bandwidth-DL	O	The maximum amount of bandwidth that can be used without explicit authorization in the downlink direction.

Table 5.2: QoS profile description

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

5.2 Procedures on the a4 interface

5.2.1 Access profile push

5.2.1.1 Overview

This procedure is used to push the Access Profile information from the UAAF to the CLF. This information flow occurs when a NASS User has been successful authenticated or in case a modification occurs on a profile that has already been pushed to the CLF.

UAAF may decide to send in the same Access Profile Push some profiles in the form of a profile id (because the actual profile information is assumed to be available in the CLF) and some other profiles in the form of full profile descriptions. This information is retrieved from the PDBF by the UAAF.

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

Table 5.3: Access Profile Push

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally Unique IP Address	Globally-Unique-Address	O	This information element contains: • The IP address of the NASS User for which profile information is being pushed. • The addressing domain in which the IP address is significant.
Logical Access ID	Logical-Access-Id	M	The identity of the logical access to which the user equipment is connected.
NASS User ID	User-Name	O	The NASS User that is attached to the network (see note).
Physical Access ID	Physical-Access-Id	O	The identity of the physical access to which the user equipment is connected.
CNGCF address	CNGCF-Address	O	The address of the CNGCF entity from which configuration data may be retrieved by the user equipment.
P-CSCF Identity (optional)	SIP-Outbound-Proxy	O	The Identity of the P-CSCF for accessing IMS services.
Initial Gate Setting	Initial-Gate-Setting or Initial-Gate-Setting-ID	O	See clause 5.1, table 1.
QoS Profile	QoS-Profile or QoS-Profile-ID	O	See clause 5.1, table 2.
Privacy Indicator	Privacy-Indicator	O	Whether location information can be exported to services and applications.
Data Operation Indication	Data-Operation-Indicator	O	Whether the Access Profile of the NASS User shall be updated or removed. See clause 7.3.1 for the Default value.
NOTE: Ths NASS User ID shall be included if available in the UAAF.			

Table 5.4: Access Profile Push response

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

5.2.1.2 Procedure at the UAAF side

The UAAF knows the address of the CLF entity where the information should be pushed, either from configuration data or from the NASS User profile (i.e. received from the PDBF).

The UAAF shall populate the Access Profile Push as follows:

- The Logical-Access-ID AVP shall be present.
- In case PPP is applied, the Globally-Unique-Address AVP shall be present. In case DHCP is applied, this AVP is optional. The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP.
- If available in the UAAF, the User-Name AVP shall be present.
- In case PPP is applied, the Physical-Access-Id AVP may be present.

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

5.2.1.3 Procedure at the CLF side

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

If the Logical Access ID contained in the Logical-Access-ID AVP is not known, the CLF shall:

- Create an internal record to store the received information for future use (e.g. push the Access Profile to the RACS).

If the Logical Access ID contained in the Logical-Access-ID AVP is already known, the CLF shall:

- Replace the entire content of the internal record with the received information for future use (e.g. push the Access Profile to the RACS).
- Push the updated Access Profile to RACS if appropriate.

If the contents of the request are invalid the CLF shall return an Access Profile Push response with a Result-Code AVP value set to the appropriate value.

If the CLF cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and return an Access Profile Push response with a Result-Code AVP value set to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code AVP set to DIAMETER_SYSTEM_UNAVAILABLE. In the later case, the UAAF is expected to retry after a provisioned time period.

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

5.2.2 Access profile pull

5.2.2.1 Overview

The Access Profile Pull information flow is used by the CLF to request the Access Profile information from the UAAF. This information flow is used when the CLF - UAAF operates in pull mode or in the context of CLF recovery procedures.

This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in clause 7. Tables 5 and 6 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to Diameter AVPs.

Table 5.5: Access Profile Pull request

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally unique IP Address	Globally-Unique-Address	C	This information element contains: • The IP address of the NASS User for which profile information is being pushed. • The addressing domain in which the IP address is significant.
NASS User ID	User-Name	C	The NASS User that is attached to the network.
Logical Access ID	Logical-Access-Id	C	The identity of the logical access to which the user equipment is connected.
NOTE: At least one of the above elements should be included.			

Table 5.6: Access Profile Pull response

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally Unique IP Address	Globally-Unique-Address	O	This information element contains: • The IP address of the NASS User for which profile information is being pushed. • The addressing domain in which the IP address is significant.
Logical Access ID	Logical-Access-Id	M	The identity of the logical access to which the user equipment is connected.
NASS User ID	User-Name	O	The NASS User that is attached to the network (see note).
Physical Access ID	Physical-Access-Id	O	The identity of the physical access to which the user equipment is connected.
CNGCF address	CNGCF-Address	O	The address of the CNGCF entity from which configuration data may be retrieved by the user equipment.
P-CSCF Identity (optional)	SIP-Outbound-Proxy	O	The Identity of the P-CSCF for accessing IMS services.
Initial Gate Setting	Initial-Gate-Setting or Initial-Gate-Setting-ID	O	See clause 5.1, table 1.
QoS Profile	QoS-Profile or QoS-Profile-ID	O	See clause 5.1, table 2.
Privacy Indicator	Privacy-Indicator	O	Whether location information can be exported to services and applications.
NOTE: The NASS User ID shall be included if available in the UAAF.			

5.2.2.2 Procedure at the CLF side

The CLF shall populate the Access Profile Pull Request as follows:

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

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

5.2.2.3 Procedure at the UAAF side

Upon reception of the Access Profile Pull Request, the UAAF shall, in the following order:

1) If the Logical-Access-ID AVP is present, use this information as a key to retrieve the requested Access Profile.

2) If the Logical-Access-ID AVP is absent but the Globally-Unique-Address AVP is present, use the latter information as a key to retrieve the requested Access Profile.

3) If both the Logical-Access-ID AVP and the Globally-Unique-Address AVP are absent but the User-Name AVP is present, use the latter information as a key to retrieve the requested Access Profile.

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

5) If more than one record include the same NASS User ID matching the value of the User-Name AVP and neither Globally-Unique-Address AVP nor Logical-Access-ID AVP is included, return an Access Pull Profile response with Result-Code set to DIAMETER_UNABLE_TO_COMPLY.

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

If a unique NASS User record can be retrieved, the UAAF shall:

7) 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 UAAF may delay the response message until the update has been completed and shall include in the response message the updated data requested. The UAAF shall ensure that the data returned is not corrupted by this conflict.

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

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

5.2.3 Remove Access Profile

5.2.3.1 Overview

The Remove Access Profile information flow is used by the UAAF to request the CLF to delete the information it held about a NASS User. This event occurs as a result of network management actions.

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in clause 7. Tables 7 and 8 detail the involved information elements as defined in the NASS specification ES 282 004 [1] and their mapping to Diameter AVPs.

Table 5.7: Remove Access Profile Indication

Information element name	Mapping to Diameter AVP	Cat.	Description
Globally unique IP Address	Globally-Unique-Address	O	This information element contains: • The IP address of the NASS User for which profile information is being pushed. • The addressing domain in which the IP address is significant.
NASS User ID	User-Name	O	The identity of the NASS User that is attached to the network.
Logical Access ID	Logical-Access-Id	M	The identity of the logical access to which the user equipment is connected.
Data Operation Indication	Data-Operation-Indicator	M	Whether the Access Profile of the NASS User shall be updated or removed.

Table 5.8: Remove Access Profile Response

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

5.2.3.2 Procedure at the UAAF side

The UAAF shall populate the Remove Access Profile Indication as follows:

- The Logical-Access-ID AVP shall be present.
- In case PPP is applied, the Globally-Unique-Address AVP shall be present. In case DHCP is applied, this AVP is optional. The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP.
- If available in the UAAF, the User-Name AVP shall be present.

- The Data-Operation-Indicator AVP shall be present, and the value of this AVP shall be set to REMOVE.

5.2.3.3 Procedure at the CLF side

If the Logical Access ID contained in the Logical-Access-ID AVP is not known, the CLF shall stop processing the request and set the Experimental-Result-Code to DIAMETER_ERROR_USER_UNKNOWN in the Remove Access Profile Response.

If the Logical Access ID contained in the Logical-Access-ID AVP is already known, the CLF shall:

- remove the existing session record;
- notify the RACS.

If the CLF cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code set to DIAMETER_SYSTEM_UNAVAILABLE. In the later case, the UAAF is expected to retry after a provisioned time period.

Otherwise, the requested operation shall take place and the CLF shall return a Remove Access Profile Response message with the Result-Code AVP set to DIAMETER_SUCCESS.

6 Use of the Diameter base protocol

With the clarifications listed in the following clauses the Diameter Base Protocol defined by RFC 3588 [9] 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 [8].

6.2 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used on the a4 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 [9]. 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 a4 interface shall make use of SCTP RFC 2960 [6] and shall utilize the new SCTP checksum method specified in RFC 3309 [7].

6.5 Routing considerations

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

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

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

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

6.6 Advertising Application Support

The CLF and UAAF shall advertise support of the a4 specific application by including the value 16777257 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 [9].

7 DIAMETER application

This clause specifies a Diameter application that allows a Diameter server and Diameter client exchange information related to NASS User network profile information.

The Diameter application identifier assigned to this application is 16777257 (allocated by IANA).

The Diameter Base Protocol as specified in RFC 3588 [9] is used to support information transfer on both interfaces.

RFC 3588 [9] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and event codes specified in clause 5. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) are unmodified.

7.1 Commands

The present document re-uses and modifies commands defined in the TS 129 329 [3] for the Sh interface. Only the following commands defined in TS 129 329 [3] are used. Any other command defined in TS 129 329 [3] shall be ignored.

Table 7.1: Command-code values

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

AVPs defined in TS 129 329 [3] and not used in the present document are not shown in the below clauses. If received, these AVPs shall be ignored by the CLF and the A-RACF.

New AVPs are represented in bold.

7.1.1 User-Data-Request command

The User-Data-Request (UDR) command, indicated by the Command-Code field set to 306 and the "R" bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request user data. This command is defined in TS 129 329 [3] and used with additional AVPs defined in the present document.

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

Message Format:

```
< User-Data -Request > ::= < Diameter Header: 306, REQ, PXY, 16777257 >
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                [Globally-Unique-Address]
                                [Logical-Access-Id]
                                [User-Name]
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

7.1.2 User-Data-Answer command

The User-Data-Answer (UDA) command, indicated by the Command-Code field set to 306 and the "R" bit cleared in the Command Flags field, is sent by a server in response to the User-Data-Request command. This command is defined in TS 129 329 [3] and used with additional AVPs defined in the present document. The Experimental-Result AVP may contain one of the values defined in clause 7.2 or in TS 129 229 [2].

Message Format:

```
< User-Data-Answer > ::=   < Diameter Header: 306, PXY, 16777257 >
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                 [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [Globally-Unique-Address]
                                [User-Name]
                                [Logical-Access-Id]
                                [Physical-Access-Id]
                                [CNGCF-Address]
                                [SIP-Outbound-Proxy]
                                [Initial-Gate-Setting-Description]
                                *[QoS-Profile-Description]
                                [QoS-Profile-ID]
                                [Initial-Gate-Setting-ID]
                                *[Privacy-Indicator]
                                *[ AVP ]
                                *[ Failed-AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

7.1.3 Push-Notification-Request command

The Push-Notification-Request (PNR) command, indicated by the Command-Code field set to 309 and the "R" bit set in the Command Flags field, is sent by a Diameter server to a Diameter client in order to notify changes in the user data in the server. This command is defined in TS 129 329 [3] and used with additional AVPs defined in the present document.

Message Format:

```
< Push-Notification-Request > ::=  < Diameter Header: 309, REQ, PXY, 16777257 >
                                   < Session-Id >
                                   { Vendor-Specific-Application-Id }
                                   { Auth-Session-State }
                                   { Origin-Host }
                                   { Origin-Realm }
                                   { Destination-Host }
                                   { Destination-Realm }
                                   [Globally-Unique-Address]
                                   [User-Name]
                                   [Logical-Access-Id]
                                   [Physical-Access-Id]
                                   [CNGCF-Address]
                                   [SIP-Outbound-Proxy]
                                   [Initial-Gate-Setting-Description]
                                   *[QoS-Profile-Description]
                                   [QoS-Profile-ID]
                                   [Initial-Gate-Setting-ID]
                                   *[Privacy-Indicator]
                                   [Data-Operation-Indicator]
                                   *[ AVP ]
                                   *[ Proxy-Info ]
                                   *[ Route-Record ]
```

7.1.4 Push-Notification-Answer command

The Push-Notifications-Answer (PNA) command, indicated by the Command-Code field set to 309 and the "R" bit cleared in the Command Flags field, is sent by a client in response to the Push-Notification-Request command. This command is defined in TS 129 329 [3]. The Experimental-Result AVP may contain one of the values defined in clause 7.2 or in TS 129 229 [2].

Message Format:

```
< Push-Notification-Answer > ::= < Diameter Header: 309, PXY, 16777257 >
                                 < Session-Id >
                                 { Vendor-Specific-Application-Id }
                                 [ Result-Code ]
                                 [ Experimental-Result ]
                                 { Auth-Session-State }
                                 { Origin-Host }
                                 { Origin-Realm }
                                 *[ AVP ]
                                 *[ Failed-AVP ]
                                 *[ Proxy-Info ]
                                 *[ Route-Record ]
```

7.2 Result-Code AVP values

This clause defines new result code values that must be supported by all Diameter implementations that conform to the present document. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and Result-Code AVP shall be absent.

7.2.1 Success

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

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

7.2.2 Permanent failures

Errors that fall within the Permanent Failures category are used to inform the peer that the request failed, and should not be attempted again.

No errors within this category have been defined so far. However the following error defined in TS 129 229 [2] is used in the present document:

- DIAMETER_ERROR_USER_UNKNOWN (5001).

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

7.2.3 Transient failures

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

No errors within this category have been defined so far. However the following error defined in TS 129 329 [3] is used in the present document:

- DIAMETER_USER_DATA_NOT_AVAILABLE (4100).

7.3 AVPs

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

Table 7.2 describes the Diameter AVPs defined in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. The Vendor-Id header of all AVPs defined in the present document shall be set to ETSI (13019).

Table 7.2: 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**
Data-Operation-Indicator	420	7.3.1	Enumerated	V	M			Yes
NOTE: The AVP header bit denoted as "M", indicates whether support of the AVP is required. The AVP header bit denoted as "V", indicates whether the optional Vendor-ID field is present in the AVP header.								

Table 7.3 describes the Diameter AVPs defined for the e4 application (ES 283 034 [4]) 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 [4] 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 for these AVPs shall be set to ETSI (13019).

Table 7.3: Diameter AVPs imported from the ES 283 034 [4] (e4 specification)

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
Globally-Unique-Address	300	See ES 283 034 [4]	Grouped	M,V				Yes
Logical-Access-Id	302	See ES 283 034 [4]	OctetString	V	M			Yes
Initial-Gate-Setting-Description	303	See ES 283 034 [4]	Grouped	V	M			Yes
QoS-Profile-Description	304	See ES 283 034 [4]	Grouped	V	M			Yes
Physical-Access-ID	313	See ES 283 034 [4]	UTF8String	V	M			Yes
Initial-Gate-Setting-ID	314	See ES 283 034 [4]	Unsigned32	V	M			Yes
QoS-Profile-ID	315	See ES 283 034 [4]	Unsigned32	V	M			Yes
NOTE: The AVP header bit denoted as "M", indicates whether support of the AVP is required. The AVP header bit denoted as "V", indicates whether the optional Vendor-ID field is present in the AVP header.								

Table 7.4 describes the Diameter AVPs defined in TS 183 020 [5] and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. AVPs defined in TS 183 020 [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 for these AVPs shall be set to ETSI (13019).

Table 7.4: Diameter AVPs imported from the TS 183 020 [5]

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
Privacy-Indicator	440	See TS 183 020 [5]	Grouped	V	M			Yes
NOTE: The AVP header bit denoted as "M", indicates whether support of the AVP is required. The AVP header bit denoted as "V", indicates whether the optional Vendor-ID field is present in the AVP header.								

Table 7.5 describes the Diameter AVPs defined in TS 183 059-1 [10] and used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted. Flags values are described in the context of the present document rather than in the context of the application where they are defined. AVPs defined in TS 183 059-1 [10] 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 for these AVPs shall be set to ETSI (13019).

Table 7.5: Diameter AVPs imported from the TS 183 059-1 [10]

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
SIP-Outbound-Proxy	601	See TS 183 059-1 [10]	OctetString	V	M			Yes
CNGCF-Address	600	See TS 183 059-1 [10]	Grouped	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.								

7.3.1 Data-Operation-Indicator

The Data-Operation-Indicator AVP (AVP code 420 13019) is of type Enumerated and represents the type of data operation the receiver shall perform after receiving this AVP. When the Data-Operation-Indicator AVP is omitted, the receiver shall perform the update operation by default.

The following values are defined:

- UPDATE (0).
- REMOVE (1).

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 420 to 439 range from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 7.3 for the assigned values.

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 codes assigned to 3GPP.

7.4.4 Application-ID value

The present document uses value 16777257, allocated by IANA, as application identifier.

Annex A (informative): Mapping of a4 operations and terminology to Diameter

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

Table A.1: a4 message to Diameter command mapping

a4 message	Source	Destination	Command-Name	Abbreviation
Access Profile Pull	CLF	UAAF	User-Data-Request	UDR
Access Profile Pull Response	UAAF	CLF	User-Data-Answer	UDA
Access Profile Push	UAAF	CLF	Push-Notification-Request	PNR
Access Profile Push Response	CLF	UAAF	Push-Notification-Answer	PNA
Remove Access Profile Indication	UAAF	CLF	Push-Notification-Request	PNR
Remove Access Profile Response	CLF	UAAF	Push-Notification-Answer	PNA

History

Document history		
V2.1.1	January 2009	Publication