International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3232

(08/2014)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Signalling and control requirements and protocols to support attachment in NGN environments

# Signalling requirements and protocol at the Nc interface between the transport location management physical entity and the transport authentication and authorization physical entity

Recommendation ITU-T Q.3232

ITU-T Q-SERIES RECOMMENDATIONS

**SWITCHING AND SIGNALLING**

| | |
|---|---|
| SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE | Q.1–Q.3 |
| INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING | Q.4–Q.59 |
| FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN | Q.60–Q.99 |
| CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS | Q.100–Q.119 |
| SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2 | Q.120–Q.499 |
| DIGITAL EXCHANGES | Q.500–Q.599 |
| INTERWORKING OF SIGNALLING SYSTEMS | Q.600–Q.699 |
| SPECIFICATIONS OF SIGNALLING SYSTEM No. 7 | Q.700–Q.799 |
| Q3 INTERFACE | Q.800–Q.849 |
| DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1 | Q.850–Q.999 |
| PUBLIC LAND MOBILE NETWORK | Q.1000–Q.1099 |
| INTERWORKING WITH SATELLITE MOBILE SYSTEMS | Q.1100–Q.1199 |
| INTELLIGENT NETWORK | Q.1200–Q.1699 |
| SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000 | Q.1700–Q.1799 |
| SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC) | Q.1900–Q.1999 |
| BROADBAND ISDN | Q.2000–Q.2999 |
| SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN | Q.3000–Q.3999 |
| General | Q.3000–Q.3029 |
| Network signalling and control functional architecture | Q.3030–Q.3099 |
| Network data organization within the NGN | Q.3100–Q.3129 |
| Bearer control signalling | Q.3130–Q.3179 |
| **Signalling and control requirements and protocols to support attachment in NGN environments** | **Q.3200–Q.3249** |
| Resource control protocols | Q.3300–Q.3369 |
| Service and session control protocols | Q.3400–Q.3499 |
| Service and session control protocols – supplementary services | Q.3600–Q.3649 |
| NGN applications | Q.3700–Q.3849 |
| Testing for next generation networks | Q.3900–Q.3999 |

*For further details, please refer to the list of ITU-T Recommendations.*

# Recommendation ITU-T Q.3232

## Signalling requirements and protocol at the Nc interface between the transport location management physical entity and the transport authentication and authorization physical entity


### Summary

Recommendation ITU-T Q.3232 specifies the protocol for the interface between the transport location management physical entity (TLM-PE) and the transport authentication and authorization physical entity (TAA-PE) of the network attachment control entity (NACE). The Nc interface allows the TLM-PE to register the association between a subscriber and the corresponding preferences regarding the privacy of location information provided by the TAA-PE. Reference point Nc is also used to register transport resource subscription information. The TLM-PE may retrieve the transport resource subscription information from the TAA-PE.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T Q.3232 | 2014-08-29 | 11 | 11.1002/1000/12217 |


* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## Table of Contents

# Recommendation ITU-T Q.3232

# Signalling requirements and protocol at the Nc interface between the transport location management physical entity and the transport authentication and authorization physical entity

## 1 Scope

This Recommendation specifies the protocol for the Nc interface between the transport location management physical entity (TLM-PE) and the transport authentication and authorization physical entity (TAA-PE).

## 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.1541] Recommendation ITU-T Y.1541 (2011), *Network performance objectives for IP-based services*.

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2010), *Network attachment control functions in next generation networks*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ETSI ES 283 034] ETSI ES 283 034 V2.2.0 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol*.

[ETSI TS 129 229] ETSI TS 129 229 V11.4.0 (2013), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (3GPP TS 29.229 version 11.4.0 Release 11).*

[ETSI TS 129 329] ETSI TS 129 329 V11.7.0 (2013), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329 version 11.7.0 Release 11)*.

[ETSI TS 183 020] ETSI TS 183 020 V1.1.1 (2006), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment: Roaming in TISPAN NGN Network Accesses; Interface Protocol Definition*.

[ETSI TS 183 066] ETSI TS 183 066 V2.1.1 (2009), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); a4 interface based on the DIAMETER protocol*.

[IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

[IETF RFC 6733] IETF RFC 6733 (2012), *Diameter Base Protocol*.

## 3 Definitions

### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 authentication** [ITU-T Y.2014]: A property by which the correct identifier of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, home environment or serving network.

**3.1.2 location information** [b-ITU-T Q.1001]: The location register should, as a minimum, contain the following information about a mobile station:

– international mobile station identity;

– actual location of the mobile station (e.g., PLMN, MSC area, location area, as required).

### 3.2 Terms defined in this Recommendation

None.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| ABNF | Augmented Backus-Naur Form |
| AM-PE | Access Management Physical Entity |
| ATM | Asynchronous Transfer Mode |
| AVP | Attribute-Value Pair |
| CPE | Customer Premises Equipment |
| DHCP | Dynamic Host Configuration Protocol |
| FQDN | Fully Qualified Domain Name |
| GPRS | General Packet Radio Service |
| GTP | GPRS Tunnelling Protocol |
| HDC-PE | Handover Decision and Control Physical Entity |
| HGW | Home Gateway |
| HGWC-PE | Home Gateway Configuration Physical Entity |
| IANA | Internet Assigned Numbers Authority |
| ID | Identifier |
| IP | Internet Protocol |
| IPsec | IP security |
| MLM-PE | Mobile Location Management Physical Entity |
| MMCE | Mobility Management Control Entity |
| MPLS | Multi-Protocol Label Switching |
| MSC | Mobile Switching Centre |

| | |
|---|---|
| NACE | Network Attachment Control Entity |
| NACF | Network Attachment Control Functions |
| NAC-PE | Network Access Configuration Physical Entity |
| NID-PE | Network Information Distribution Physical Entity |
| NIR-PE | Network Information Repository Physical Entity |
| PD-PE | Policy Decision Physical Entity |
| PLMN | Public Land Mobile Network |
| PPP | Point-to-Point Protocol |
| QoS | Quality of Service |
| RACE | Resource Admission and Control Entity |
| SCE | Service Control Entity |
| SCTP | Stream Control Transmission Protocol |
| TAA-PE | Transport Authentication and Authorization Physical Entity |
| TE | Terminal Equipment |
| TLM-PE | Transport Location Management Physical Entity |
| TRC-PE | Transport Resource Control Physical Entity |
| TUP-PE | Transport User Profile Physical Entity |
| UE | User Equipment |
| VC | Virtual Channel |
| VCI | Virtual Channel Identifier |
| VP | Virtual Path |
| VPI | Virtual Path Identifier |
| VPN | Virtual Private Network |

## 5 Conventions

None.

## 6 Nc interface

### 6.1 Overview

The Nc reference point allows the TLM-PE to register the association between a subscriber and the corresponding preferences regarding the privacy of location information provided by the TAA-PE. Reference point Nc is also used to register transport resource subscription information. The TLM-PE may retrieve the transport resource subscription information from the TAA-PE.

Interactions between the TAA-PE and the TLM-PE may be in the pull mode or the push mode operations. The push mode is used when the TAA-PE is involved in the processing of the 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 TLM-PE recovery procedures.

The following information flows are used on the Nc reference point:

– transport resource information indication;
– transport resource information request;
– transport resource information response;
– transport resource release notification.

## 6.2 Nc reference model

Figure 6-1 shows the reference architecture where the Nc interface is located.

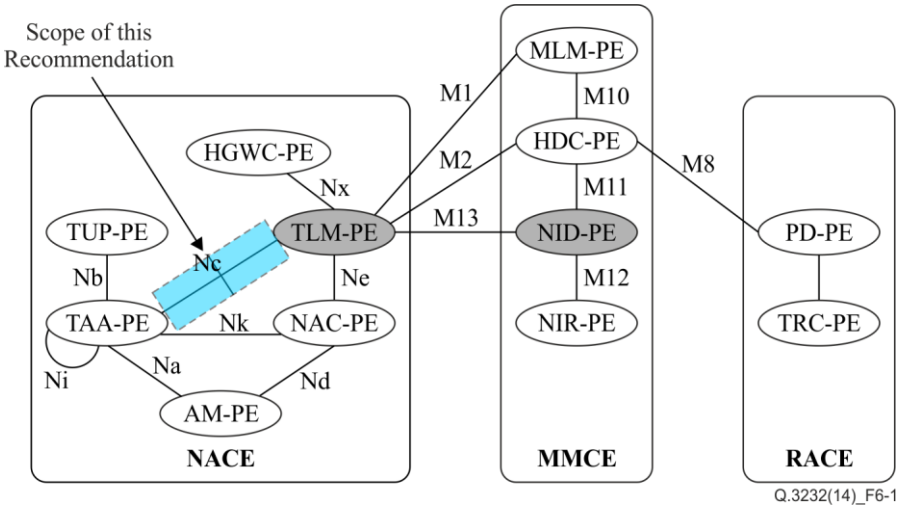


**Figure 6-1 – Nc reference model**

## 6.3 Physical entities and capabilities

### 6.3.1 Transport location management physical entity

The TLM-PE responds to location queries from service control functions and applications. The actual information delivered by TLM-PE may take various forms (e.g., network location, geographical coordinates, postal address) depending on the agreement with the requester and on user preferences regarding the privacy of its location.

The TLM-PE may play several roles, i.e., the home role, the local role, or both. In its home role, the TLM-PE stores a pointer to the TLM-PE instance that is playing the local role for the attachment. The current location information of the user/customer premises equipment (CPE) in the access domain is stored and bound in the local TLM-PE. Thus, when the user/CPE moves in the same access domain, only the location binding information of the local TLM-PE needs to be updated; the location binding information of the home TLM-PE does not need to be updated.

The local TLM-PE is in the access network to which the terminal equipment (TE) is attached. The home TLM-PE is in the network designated by the transport user profile physical entity (TUP-PE). Where these networks differ, communication between the local and the home TLM-PE instances takes place over the Ng reference point. Namely, the home TLM-PE may provide the service control entity (SCE) with user network profile information through the local TLM-PE of visit network to support mobility when the user is nomadic.

Similarly, the home TLM-PE is able to provide the SCE with user network profile information through the local TLM-PE of another service provider for roaming on such access network.

The functionality of the TLM-PE is further detailed in clause 7.2.3 of [ITU-T Y.2014].

### 6.3.2 Transport authentication and authorization physical entity

The TAA-PE performs user authentication, as well as authorization checking, based on the transport subscription profiles for the network access. For each user, the TAA-PE retrieves authentication data and access authorization information from the transport subscription profile information contained in the TUP-PE. The TAA-PE may also perform the collection of accounting data for each user authenticated by the network attachment control entity (NACE).

For the TE, TAA-PE may support the allocation of an IP address or IP prefix. The IP address and IP prefix may be required to be allocated in the authentication process for the host-based mobility architecture and the network-based mobility architecture, respectively. For the host-based mobility, TAA-PE may request the network access configuration physical entity (NAC-PE) for IP allocation. And for both the host-based and the network-based mobility, TAA-PE may just use IP address or IP prefix which is maintained as the user profile information in the TUP-PE. In order to allocate the IP address dynamically, TAA-PE may request NAC-PE to allocate the IP address. In that case, the IP address may be changed whenever the address is requested, even from the same TE. However, in order to allocate the IP address or IP prefix statically, TAA-PE may use the IP address or IP prefix which is maintained in the TUP-PE as user profile information.

The TAA-PE can also act as a proxy. When acting as a proxy, the TAA-PE can locate and communicate with the TAA-PE acting as server which contains the TUP-PE subscription authentication data. The TAA-PE proxy can forward access and authorization requests, as well as accounting messages, received from the access management physical entity (AM-PE), to the TAA-PE acting as server. Responses received back from the TAA-PE, acting as a server, will be returned to the AM-PE via the TAA-PE proxy. Communication between the TAA-PE proxy and the TAA-PE server passes across the Ni reference point.

The functionality of the TAA-PE is further detailed in clause 7.2.4 of [ITU-T Y.2014].

## 7 Signalling requirements

The Nc reference point allows the TLM-PE to register the association between a subscriber and the corresponding preferences regarding the privacy of location information provided by the TAA-PE. Reference point Nc is also used to register transport resource subscription information. The TLM-PE may retrieve the transport resource subscription information from the TAA-PE.

The relationship between the TAA-PE and the TLM-PE may be operated in pull mode or push mode. The push mode is used when the TAA-PE 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 TLM-PE recovery procedures.

The following information flows (see Figure 7-1) are used on the Nc reference point:

– transport resource information indication;
– transport resource information request;
– transport resource information response;
– transport resource release notification.

For further information, refer to clause 8.1.4 of [ITU-T Y.2014].

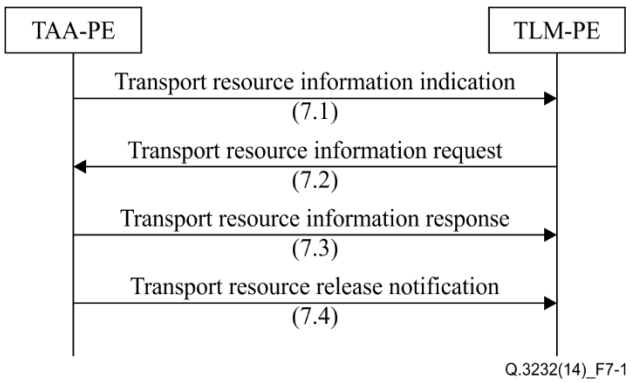


**Figure 7-1 – Transport resource information flows used on the Nc reference point**

## 7.1 Transport resource information indication

The transport resource information indication information flow is used to push transport subscription information from the TAA-PE to the TLM-PE, upon successful authentication of the user. The TAA-PE may decide to send, in the same transport resource information indication information flow, some transport subscription profiles in the form of a profile identifier (because the actual transport subscription profile information is assumed to be available in the TLM-PE) and some other transport subscription profiles in the form of full profile descriptions. This information is retrieved from the TUP-PE by the TAA-PE.

Table 7-1 describes the elements contained in the transport resource information indication information flow.

**Table 7-1 – Transport resource information indication (TAA-PE → TLM-PE)**

| | |
|---|---|
| Transport subscriber identifier | A globally unique identifier of the attached CPE. This identifier can be used for locating the transport subscription information for the CPE. |
| Globally unique IP address information (Note 1) | A set of IP address information used for locating the access network in which the CPE is attached. |
| – Unique IP address | The IP address for identifying the attached CPE. |
| – Address realm | The addressing domain of the IP address (e.g., subnet prefix or virtual private network (VPN) ID). |
| Logical connection identifier | A local identifier for logical connection of the access transport network to which the CPE is connected (e.g., asynchronous transfer mode (ATM) virtual path identifier (VPI)/virtual channel identifier (VCI), point-to-point protocol (PPP), multi-protocol label switching (MPLS) label, GPRS tunnelling protocol (GTP) tunnel and logical port). |
| Mobility service parameters (optional) (Note 7) | |
| – Address of MLM-PE(C) (Note 8) | The address of the instance of the mobile location management physical entity (MLM-PE) containing the mobile address binding information. |
| – Address of MLM-PE(P) (Note 8) | The address of the MLM-PE instance which sends the location registration. |
| – Keying material (Note 8) | The material used for the security association between the user equipment (UE) and mobility management control entity (MMCE). |
| – Mobility protocol type | The type of mobility protocol that TE or CPE could support, for example host-based or network-based mobility. |

**Table 7-1 – Transport resource information indication (TAA-PE → TLM-PE)**

| | |
|---|---|
| – Anchor point address (optional) | The upper tunnel end point address, from the point of view of the UE. |
| – Tunnel end point address (optional) (Note 9) | The tunnel end point address for the network node which works as UE's proxy (lower tunnel end point). |
| Home TLM-PE contact point | Fully qualified domain name (FQDN) or IP address of home TLM-PE. |
| Local TLM-PE contact point | FQDN or IP address of local TLM-PE. |
| Privacy indicator | Indicates whether location information can be exported to services and applications. |
| Security association (optional) | The security association negotiated between the home gateway (HGW) and the TAA-PE during the network access authentication and authorization procedure. |
| Transport resource subscription (optional) (Note 2) | |
| – Transport subscription profile identifier (ID) (Note 3) | The identifier of a set of transport subscription profile information. |
| – Transport subscription profile description (Note 3) | |
| – Network class of service | Represents the network service class subscribed by a CPE (e.g., premium, gold, silver, regular). It may include the quality of service (QoS) performance class (e.g., class defined in [ITU-T Y.1541]). |
| – Subscribed upstream bandwidth | The maximum amount of bandwidth subscribed by a CPE for the upstream connections. |
| – Subscribed downstream bandwidth | The maximum amount of bandwidth subscribed by a CPE for the downstream connections. |
| – Level of priority | The maximum level of priority permitted for any reservation request. |
| – Requestor name | Identifies the requestor(s) that are allowed by the transport resource subscription. |
| Default configuration (optional) (Note 4) | |
| – Default configuration identifier (Note 5) | The identifier of a default configuration. |
| – Default configuration description (Note 5) | |
| – Default access control list: allowed destinations as well as multicast flows | The list of default destination IP addresses and/or ports and/or prefixes and/or 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 user equipment. Address ranges are supported within the list. (Note 6) |
| – Default access control list: denied destinations as well as multicast flows | 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 user equipment must be denied. Address ranges are supported within the list. (Note 6) |

**Table 7-1 – Transport resource information indication (TAA-PE → TLM-PE)**

| | |
|---|---|
| – Default upstream bandwidth | The maximum amount of bandwidth that can be used for the upstream connections by default. |
| – Default downstream bandwidth | The maximum amount of bandwidth that can be used for the downstream connections by default. |
| NOTE 1 – In case PPP [b-IETF RFC 1661] is applied, the TAA-PE is required to provide the globally unique IP address information to the TLM-FE. When dynamic host configuration protocol (DHCP) [b-IETF RFC 2131] is applied, this parameter is optional.<br>NOTE 2 – The transport resource subscription may contain multiple transport subscription profiles.<br>NOTE 3 – Either the transport subscription profile ID or the transport subscription profile description may be included, but not both at the same time.<br>NOTE 4 – This information is used by the resource admission and control entity (RACE) to configure the transport functions, before resource reservation requests are received from services/applications.<br>NOTE 5 – Either the default configuration identifier or the default configuration description may be included, but not both at the same time.<br>NOTE 6 – If a destination does not appear in either of the two lists, then gate-setting decisions for those addresses is subject to control by RACE.<br>NOTE 7 – It is available only if the mobility service is applied.<br>NOTE 8 – It is available only if the host-based mobility is applied.<br>NOTE 9 – If the tunnel end point address is statically provisioned or the MLM-PE can obtain it with its own mechanisms, this information is not required. It is available only if the network-based mobility is applied. | |

## 7.2 Transport resource information request

The transport resource information request information flow is used by the TLM-PE to request the transport subscription profile information from the TAA-PE. This information flow is used when relationship between the TLM-PE and the TAA-PE operates in pull mode or in the context of TLM-PE recovery procedures.

Table 7-2 describes the elements contained in the transport resource information request information flow.

**Table 7-2 – Transport resource information request (TLM-PE → TAA-PE)**

| | |
|---|---|
| Globally unique IP address information (Note 1) | A set of IP address information used for locating the access network to which the CPE is attached. |
| – Unique IP address | The IP address for identifying the attached CPE. |
| – Address realm | The addressing domain of the IP address (e.g., subnet prefix or VPN ID). |
| Logical connection identifier | A local identifier for logical connection of access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS label, GTP tunnel and logical port). |
| Transport subscriber identifier (Note 2) | A globally unique identifier for the attached CPE. This identifier can be used for locating the transport subscription information for the CPE. |
| NOTE 1 – If the information flow is used for supporting recovery procedures and the reference point operates in push mode, the globally unique IP address information is required to be included.<br>NOTE 2 – If the reference point operates in the pull mode, the transport subscriber identifier is required to be included. | |

## 7.3 Transport resource information response

The transport resource information response information flow is used to provide transport subscription information from the TAA-PE to the TLM-PE in response to a transport resource information request.

Table 7-3 describes the elements contained in the transport resource information response information flow.

**Table 7-3 – Transport resource information response (TAA-PE → TLM-PE)**

| | |
|---|---|
| Transport subscriber identifier | A globally unique identifier of the attached CPE. This identifier can be used for locating the transport subscription information for the CPE. |
| Globally unique IP address information (Note 1) | A set of IP address information used for locating the access network in which the CPE is attached. |
| – Unique IP address | The IP address for identifying the attached CPE. |
| – Address realm | The addressing domain of the IP address (e.g., Subnet prefix or VPN ID). |
| Logical connection identifier | A local identifier for logical connection of access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS label, GTP tunnel and logical port). |
| Mobility service parameters (optional) (Note 7) | |
| – Address of MLM-PE(C) (Note 8) | The address of the instance of the MLM-PE containing the mobile address binding information. |
| – Address of MLM-PE(P) (Note 8) | The address of the MLM-PE instance which sends the location registration. |
| – Keying material (Note 8) | The material used for the security association between the UE and MMCE. |
| – Mobility protocol type | The type of mobility protocol that TE or CPE could support, for example host-based or network-based mobility. |
| – Anchor point address (optional) | The upper tunnel end point address, from the point of view of the UE. |
| – Tunnel end point address (optional) (Note 9) | The tunnel end point address for the network node which works as UE's proxy (lower tunnel end point). |
| Privacy indicator | Indicates whether location information can be exported to services and applications. |
| Security association (optional) | The security association negotiated between the HGW and the TAA-PE during the network access authentication and authorization procedure. |
| Transport resource subscription (optional) (Note 2) | |
| – Transport subscription profile ID (Note 3) | The identifier of a set of transport subscription profile information. |
| – Transport subscription profile description (Note 3) | |
| – Network class of service | Represents the network service class subscribed by a CPE (e.g., premium, gold, silver, regular). It may include the QoS performance class (e.g., class defined in [ITU-T Y.1541]). |
| – Subscribed upstream bandwidth | The maximum amount of bandwidth subscribed by a CPE for the upstream connections. |

**Table 7-3 – Transport resource information response (TAA-PE → TLM-PE)**

| | |
|---|---|
| – Subscribed downstream bandwidth | The maximum amount of bandwidth subscribed by a CPE for the downstream connections. |
| – Level of priority | The maximum level of priority permitted for any reservation request. |
| – Requestor name | Identifies the requestor(s) that are allowed by the transport resource subscription. |
| Default configuration (optional) (Note 4) | |
| – Default configuration identifier (Note 5) | The identifier of a default configuration. |
| – Default configuration description (Note 5) | |
| – Default access control list: allowed destinations as well as multicast flows | The list of default destination IP addresses and/or ports and/or prefixes and/or 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 user equipment. Address ranges are supported within the list. (Note 6) |
| – Default access control list: denied destinations as well as multicast flows | 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 user equipment must be denied. Address ranges are supported within the list. (Note 6) |
| – Default upstream bandwidth | The maximum amount of bandwidth that can be used for the upstream connections by default. |
| – Default downstream bandwidth | The maximum amount of bandwidth that can be used for the downstream connections by default. |

NOTE 1 – In case PPP [b-IETF RFC 1661] is applied, the TAA-PE is required to provide the globally unique IP address information to the TLM-PE. When DHCP [b-IETF RFC 2131] is applied, this parameter is optional.

NOTE 2 – The transport resource subscription may contain multiple transport subscription profiles.

NOTE 3 – Either the transport subscription profile ID or the transport subscription profile description may be included, but not both at the same time.

NOTE 4 – This information is used by the RACE to configure the transport functions, before resource reservation requests are received from services/applications.

NOTE 5 – Either the default configuration identifier or the default configuration description may be included, but not both at the same time.

NOTE 6 – If a destination does not appear in either of the two lists, gate setting decisions for those addresses is subject to control by RACE.

NOTE 7 – It is available only if the mobility service is applied.

NOTE 8 – It is available only if the host-based mobility is applied.

NOTE 9 – If the tunnel end point address is statically provisioned or the MLM-PE can obtain it with its own mechanisms, this information is not required. It is available only if the network-based mobility is applied.

### 7.4 Transport resource release notification

The transport resource release notification information flow is used by the TAA-PE to request the TLM-PE to delete the information it held about a CPE. This event occurs as a result of network management actions.

Table 7-4 describes the elements contained in the transport resource release notification information flow.

**Table 7-4 – Transport resource release notification (TAA-PE → TLM-PE)**

| | |
|---|---|
| Globally unique IP address information (Note) | A set of IP address information used for locating the access network to which the CPE is attached. |
| – Unique IP address | The IP address for identifying the attached CPE. |
| – Address realm | The addressing domain of the IP address (e.g., Subnet prefix or VPN ID). |
| Logical connection identifier (optional) | A local identifier for logical connection of access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS label, GTP tunnel and logical port). |
| Transport subscriber identifier (Note) | A globally unique identifier for the attached CPE. This identifier can be used for locating the transport subscription information for the CPE. |
| NOTE – Either the globally unique IP address information or the transport subscriber identifier is included. | |

## 8 Description of procedures

### 8.1 General

The following clauses describe the realization of the functional procedures defined in the NACE specifications using Diameter commands described in clause 10. This involves describing a mapping between the information elements defined in the NACE specification and Diameter attribute-value pairs (AVPs).

In the tables that describe this mapping, each information element is marked as mandatory (M), conditional (C) or optional (O) [ETSI ES 283 034].

### 8.2 Procedure at the Nc interface

#### 8.2.1 Transport resource information indication

##### 8.2.1.1 Overview

This procedure is used to push the transport resource information from the TAA-PE to the TLM-PE. This information flow occurs when a NACE user has been successfully authenticated or in case a modification occurs on a profile that has already been pushed to the TLM-PE.

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in Sh interface [ETSI TS 129 329]. Tables 8-1 and 8-2 detail the involved information elements as defined in the NACE and their mapping to Diameter AVPs.

**Table 8-1 – Transport resource information indication**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| Unique IP address | Globally-Unique-Address | O |
| Address realm | | |

**Table 8-1 – Transport resource information indication**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| Transport subscriber identifier (Note 1) | User-Name | O |
| Logical connection identifier | Logical-Access-Id | M |
| Mobility service parameters (optional) | Mobility-Service-Parameters | O |
| – Address of MLM-PE(C) | Central-MLM-PE-Contact-Point | O |
| – Address of MLM-PE(P) | Proxy-MLM-PE-Contact-Point | O |
| – Keying material | Keying-Material | O |
| – Mobility protocol type | Mobility-Protocol-Type | O |
| – Anchor point address | Anchor-Point-Address | O |
| – Tunnel end point address (optional) | Tunnel-End-Point-Address | O |
| Home TLM-PE contact point | Home-TLM-PE-Contact-Point | O |
| Local TLM-PE contact point | Local-TLM-PE-Contact-Point | O |
| Privacy indicator | Privacy-Indicator | O |
| Security association | Security-Association | O |
| Transport resource subscription (optional) | QoS-Profile-ID or Qos-Profile-Description | O |
| – Transport subscription profile ID (Note 2) | QoS-Profile-ID | O |
| – Transport subscription profile description (Note 2) | Qos-Profile-Description | O |
| – Network class of service | Transport-Class | O |
| – Subscribed upstream bandwidth | Maximum-Allowed-Bandwidth-UL | O |
| – Subscribed downstream bandwidth | Maximum-Allowed-Bandwidth-DL | O |
| – Level of priority | Reservation-Priority | O |
| – Requestor name | Application Class ID | O |
| Default configuration (optional) | Initial-Gate-Setting-ID or Initial-Gate-Setting-Description | O |
| – Default configuration identifier (Note 3) | Initial-Gate-Setting-ID | O |
| – Default configuration description (Note 3) | Initial-Gate-Setting-Description | O |
| – Default access control list: allowed destinations as well as multicast flows | NAS-Filter-Rule | O |
| – Default access control list: denied destinations as well as multicast flows | NAS-Filter-Rule | O |

**Table 8-1 – Transport resource information indication**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| – Default upstream bandwidth | Maximum-Allowed-Bandwidth-UL | O |
| – Default downstream bandwidth | Maximum-Allowed-Bandwidth-DL | O |
| Data operation indication (Note 4) | Data-Operation-Indicator | O |
| NOTE 1 – The transport subscriber identifier shall be included if available in the TLM-PE.<br>NOTE 2 – For the transport resource subscription, either the transport subscription profile ID or the transport subscription profile description may be included, but not both at the same time.<br>NOTE 3 – For the default configuration, either the default configuration identifier or the default configuration may be included, but not both at the same time.<br>NOTE 4 – Whether the profile of NACE user shall be updated or removed. When Data-Operation-Indicator AVP is omitted, the receiver shall perform the update operation by default. | | |

**Table 8-2 – Transport resource information indication response**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| Result | Result-Code/Experimental_Result | M |

#### 8.2.1.2 Procedure at the TAA-PE side

The TAA-PE knows the address of the TLM-PE entity where the information should be pushed, either from the configuration data or from the transport resource information (i.e., received from the TUP-PE).

The TAA-PE shall populate the Transport resource information 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 TAA-PE, 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 transport resource information and the local policy rules.

#### 8.2.1.3 Procedure at the TLM-PE side

If the Logical-Access-ID AVP is not present or is invalid, the TLM-PE shall return a Transport resource information indication response with a Result-Code AVP value set to DIAMETER_INVALID_AVP_VALUE.

If the "logical connection identifier" contained in the Logical-Access-ID AVP is not known, the TLM-PE shall:

- Create an internal record to store the received information for future use (e.g., push the transport resource information to the RACE).

If the "logical connection identifier" contained in the Logical-Access-ID AVP is already known, the TLM-PE shall:

- Replace the entire content of the internal record with the received information for future use (e.g., push the transport resource information to the RACE).
- Push the updated transport resource information to the RACE if appropriate.

If the contents of the request are invalid the TLM-PE shall return a Transport resource information indication response with a Result-Code AVP value set to the appropriate value.

If the TLM-PE 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 a Transport resource information indication 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 latter case, the TAA-PE is expected to retry after a provisioned time period.

Otherwise, the requested operation shall take place and the TLM-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS in the Transport resource information indication response.

### 8.2.2 Transport resource information request

#### 8.2.2.1 Overview

The transport resource information request is used by the TLM-PE to request the transport resource information from the TAA-PE. This information flow is used when the TLM-PE – TAA-PE operates in the pull mode or in the context of TLM-PE recovery procedures.

This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in Sh interface [ETSI TS 129 329]. Tables 8-3 and 8-4 detail the involved information elements as defined in the NACE and their mapping to Diameter AVPs.

**Table 8-3 – Transport resource information request**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| Unique IP address | Globally-Unique-Address | C |
| Address realm | | |
| Transport subscriber identifier | User-Name | C |
| Logical connection identifier | Logical-Access-Id | C |
| NOTE – At least one of the above elements should be included. | | |

**Table 8-4 – Transport resource information response**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| Result | Result-Code/Experimental_Result | M |
| Unique IP address | Globally-Unique-Address | O |
| Address realm | | |
| Transport subscriber identifier (Note 1) | User-Name | O |
| Logical connection identifier | Logical-Access-Id | M |
| Mobility service parameters (optional) | Mobility-Service-Parameters | O |
| – Address of MLM-PE(C) | Central-MLM-PE-Contact-Point | O |
| – Address of MLM-PE(P) | Proxy-MLM-PE-Contact-Point | O |

**Table 8-4 – Transport resource information response**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| – Keying material | Keying-Material | O |
| – Mobility protocol type | Mobility-Protocol-Type | O |
| – Anchor point address | Anchor-Point-Address | O |
| – Tunnel end point address (optional) | Tunnel-End-Point-Address | O |
| Home TLM-PE contact point | Home-TLM-PE-Contact-Point | O |
| Local TLM-PE contact point | Local-TLM-PE-Contact-Point | O |
| Privacy indicator | Privacy-Indicator | O |
| Security association | Security-Association | O |
| Transport resource subscription (optional) | QoS-Profile-ID or Qos-Profile-Description | O |
| – Transport subscription profile ID (Note 2) | QoS-Profile-ID | O |
| – Transport subscription profile description (Note 2) | Qos-Profile-Description | O |
| – Network class of service | Transport-Class | O |
| – Subscribed upstream bandwidth | Maximum-Allowed-Bandwidth-UL | O |
| – Subscribed downstream bandwidth | Maximum-Allowed-Bandwidth-DL | O |
| – Level of priority | Reservation-Priority | O |
| – Requestor name | Application class ID | O |
| Default configuration (optional) | Initial-Gate-Setting-ID or Initial-Gate-Setting-Description | O |
| – Default configuration identifier (Note 3) | Initial-Gate-Setting-ID | O |
| – Default configuration description (Note 3) | Initial-Gate-Setting-Description | O |
| – Default access control list: allowed destinations as well as multicast flows | NAS-Filter-Rule | O |
| – Default access control list: denied destinations as well as multicast flows | NAS-Filter-Rule | O |
| – Default upstream bandwidth | Maximum-Allowed-Bandwidth-UL | O |
| – Default downstream bandwidth | Maximum-Allowed-Bandwidth-DL | O |
| NOTE 1 – The transport subscriber identifier shall be included if available in the TLM-PE.<br>NOTE 2 – For the transport resource subscription, either the transport subscription profile ID or the transport subscription profile description may be included, but not both at the same time.<br>NOTE 3 – For the default configuration, either the default configuration identifier or the default configuration may be included, but not both at the same time. | | |

**Table 8-4 – Transport resource information response**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| NOTE 4 – Whether the profile of NACE user shall be updated or removed. When Data-Operation-Indicator AVP is omitted, the receiver shall perform the update operation by default. | | |

#### 8.2.2.2 Procedure at the TLM-PE side

The TLM-PE shall populate the Transport resource information 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 transport subscriber identifier.

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

#### 8.2.2.3 Procedure at the TAA-PE side

Upon reception of the Transport resource information request, the TAA-PE 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 NACE 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 NACE profile.

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

5) If more than one record include the same transport subscriber identifier matching the value of the User-Name AVP and neither Globally-Unique-Address AVP nor Logical-Access-ID AVP is included, return a transport resource information response with Result-Code set to DIAMETER_UNABLE_TO_COMPLY.

6) If no transport resource information record is stored for the Globally-Unique-Address AVP or the Logical-Access-ID AVP or the User-Name AVP, return a Transport resource information response with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN.

If a unique transport resource information record can be retrieved, the TAA-PE 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 TAA-PE may delay the response message until the update has been completed and shall include in the response message the updated data requested. The TAA-PE shall ensure that the data returned is not corrupted by this conflict.

If the TAA-PE 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 user authorization answer (UAA) 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 TAA-PE shall return the UAA Result-Code AVP set to DIAMETER_SUCCESS and the session data in the Transport resource information response.

### 8.2.3 Transport resource release notification

#### 8.2.3.1 Overview

The transport resource release notification is used by the TAA-PE to request the TLM-PE to delete the information it held about a NACE 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 Sh interface [ETSI TS 129 329]. Tables 8-5 and 8-6 detail the involved information elements as defined in the NACE and their mapping to Diameter AVPs.

**Table 8-5 – Transport resource release notification**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| Unique IP address | Globally-Unique-Address | O |
| Address realm | | |
| Transport subscriber identifier | User-Name | O |
| Logical connection identifier | Logical-Access-Id | M |
| Data operation indication | Data-Operation-Indicator | M |

**Table 8-6 – Transport resource release notification response**

| Information element name | Mapping to Diameter AVP | Category |
|---|---|---|
| Result | Result-Code/Experimental_Result | M |

#### 8.2.3.2 Procedure at the TAA-PE side

The TAA-PE shall populate the Transport resource release notification 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 TAA-PE, the User-Name AVP shall be present.
- Data-Operation-Indicator AVP shall be present, and the value of this AVP shall be set to REMOVE.

#### 8.2.3.3 Procedure at the TLM-PE side

If the logical access ID contained in the Logical-Access-ID AVP is not known, the TLM-PE shall stop processing the request and set the Experimental-Result-Code to DIAMETER_ERROR_USER_UNKNOWN in the Transport resource release notification response.

If the logical access ID contained in the Logical-Access-ID AVP is already known, the TLM-PE shall:

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

If the TLM-PE 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 latter case, the TAA-PE is expected to retry after a provisioned time period.

Otherwise, the requested operation shall take place and the TLM-PE shall return a Transport resource release notification response with the Result-Code AVP set to DIAMETER_SUCCESS.

## 9 Use of Diameter base protocol

With the clarifications listed in the following clauses, the Diameter base protocol defined by [IETF RFC 6733] shall apply.

### 9.1 Securing Diameter messages

For secure transport of Diameter messages, IP security (IPsec) may be used. Guidelines on the use of stream control transmission protocol (SCTP) with IPsec can be found in [b-IETF RFC 3554].

### 9.2 Accounting functionality

Accounting functionality (accounting session state machine, related command codes and AVPs) is not used at the Nc interface.

### 9.3 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 [IETF RFC 6733].

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in [IETF RFC 6733]. 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.

### 9.4 Transport protocol

Diameter messages over the Nc interface shall make use of SCTP [IETF RFC 4960] and shall utilize the new SCTP checksum method specified in [IETF RFC 4960].

### 9.5 Routing considerations

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

With regard to the Diameter protocol used at the Nc interface, the TLM-PE acts as a Diameter server and the TAA-PE acts as the Diameter client.

Requests initiated by the TAA-PE towards the TLM-PE shall include both Destination-Host and Destination-Realm AVPs. The TAA-PE obtains the Destination-Host AVP to use in requests towards a TLM-PE, from configuration data in TAA-PE or the user profile from the TUP-PE. Consequently, the Destination-Host AVP is declared as mandatory in the augmented Backus-Naur form (ABNF) for all requests initiated by the TAA-PE.

Requests initiated by the TLM-PE towards the TAA-PE shall include both Destination-Host and Destination-Realm AVPs. The TLM-PE obtains the Destination-Host AVP to use in requests towards

a TAA-PE, from the Origin-Host and Origin-Realm AVPs received in previous commands from the TAA-PE related to the same IP realm. Consequently, the Destination-Host AVP is declared as mandatory in the ABNF for all requests initiated by the TLM-PE.

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

### 9.6 Advertising application support

The Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer (CEA) commands are specified in [IETF RFC 6733]. The Diameter base application identifier (0) shall be used in the Diameter message header of these messages.

If TLM-PE and TAA-PE indicate support of the Nc application, then the Nc application identifier (16777325) shall be used in the Diameter message header of all subsequent messages exchanged within this association.

Support of the Nc application within the CER/CEA is indicated by supplying an instance of the Vendor-Specific-Application-Id containing a Vendor-Id AVP set to ITU-T (11502) and an Auth-Application-Id AVP set to Nc (16777325).

The TLM-PE and TAA-PE are required to advertise the support of AVPs specified in 3GPP, ETSI, and ITU-T documents by including the values 10415 (3GPP), 13019 (ETSI), and 11502 (ITU-T) in three different instances of the Supported-Vendor-Id AVP in the CER and CEA commands respectively (see Table 9-1).

**Table 9-1 – Vendor identifiers for Nc**

| Vendor | Vendor identifier |
|---|---|
| 3GPP | 10415 |
| ETSI | 13019 |
| ITU-T | 11502 |

NOTE – The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that are not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per [IETF RFC 6733].

## 10 Message specification

### 10.1 Commands

This Recommendation reuses the Diameter command defined in [ETSI TS 129 329]. Other commands shall be ignored by the TLM-PE and TAA-PE (see Table 10-1).

**Table 10-1 – Command code**

| Command | Abbreviation | Defining reference | Command code | See clause |
|---|---|---|---|---|
| Push-Notification-Request | PNR | [ETSI TS 129 329] | 309 | 10.1.1 |
| Push-Notification-Answer | PNA | [ETSI TS 129 329] | 309 | 10.1.2 |
| User-Data-Request | UDR | [ETSI TS 129 329] | 306 | 10.1.3 |
| User-Data-Response | UDA | [ETSI TS 129 329] | 306 | 10.1.4 |

#### 10.1.1 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 [ETSI TS 129 329] and used with additional AVPs defined in this Recommendation.

*Message Format:*

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777325>
                              < 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}
                              [ Mobility-Service-Parameters]
                              [ Home-TLM-PE-Contact-Point]
                              [ Local-TLM-PE-Contact-Point]
                              *[ Privacy-Indicator]
                              [ Security-Association]
                              [ QoS-Profile-ID]
                              *[ QoS-Profile-Description]
                              [ Initial-Gate-Setting-ID]
                              [ Initial-Gate-Setting-Description]
                              [ Data-Operation-Indicator]
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

### 10.1.2 Push-Notification-Answer command

The Push-Notification-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-Code AVP may contain one of the values defined in clause 10.2.

*Message Format:*

```
< Push-Notification-Answer > ::= < Diameter Header: 309, PXY, 16777325>
                             < Session-Id >
                             { Vendor-Specific-Application-Id }
                             [ Result-Code ]
                             [ Experimental-Result ]
                             { Auth-Session-State }
                             { Origin-Host }
                             { Origin-Realm }
                             *[ AVP ]
                             *[ Failed-AVP ]
                             *[ Proxy-Info ]
                             *[ Route-Record ]
```

### 10.1.3 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 server to a Diameter client in order to notify changes in the user data in the server. This command is defined in [ETSI TS 129 329] and used with additional AVPs defined in this Recommendation.

*Message Format:*

```
< User-Data-Request > ::= < Diameter Header: 306, REQ, PXY, 16777325>
                          < 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]
                          *[ AVP ]
                          *[ Proxy-Info ]
                          *[ Route-Record ]
```

### 10.1.4 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 client in response to the User-Data-Request command. The Experimental-Result-Code AVP may contain one of the values defined in clause 10.2.

*Message Format:*

```
< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777325>
                          < 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]
                          [ Mobility-Service-Parameters]
                          [ Home-TLM-PE-Contact-Point]
                          [ Local-TLM-PE-Contact-Point]
                          *[ Privacy-Indicator]
                          [ Security-Association]
                          [ QoS-Profile-ID]
                          *[ QoS-Profile-Description]
                          [ Initial-Gate-Setting-ID]
                          [ Initial-Gate-Setting-Description]
                          *[ AVP ]
                          *[ Failed-AVP ]
                          *[ Proxy-Info ]
                          *[ Route-Record ]
```

## 10.2 Experimental-Result-Code AVP values

This clause defines specific values of the Experimental-Result-Code AVP used in this Recommendation. Most of these are imported from 3GPP and ETSI specifications, as indicated in the clauses below.

### 10.2.1 Experimental-Result-Code AVP values imported from ETSI TS 129 229 and ETSI TS 129 329

This clause defines the specific values of the Experimental-Result-Code AVP imported from [ETSI TS 129 229] and [ETSI TS 129 329] (vendor-id is ETSI):

DIAMETER_ERROR_USER_UNKNOWN (5001)

The request failed because the IP address or Globally-Unique Address is not found.

DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

The requested data is not available at this time to satisfy the requested operation

## 10.3 Attribute-value pairs

The following tables summarize the AVPs used in this Recommendation. These are, in addition to the AVPs, defined in [IETF RFC 6733].

Table 10-2 describes the Diameter AVPs defined by [ETSI ES 283 034] and used within this Recommendation. These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI ES 283 034]. The Vendor-Id header of all AVPs defined in Table 10-2 shall be set to ETSI (13019).

**Table 10-2 – Diameter AVPs imported from ETSI ES 283 034**

| Attribute name | AVP code | Clause defined | Value type | AVP flag rules | | | | May encrypt |
|---|---|---|---|---|---|---|---|---|
| | | | | Must | May | Should not | Must not | |
| Globally-Unique-Address | 300 | 10.3.1 | Grouped | M,V | | | | Y |
| Logical-Access-Id | 302 | 10.3.2 | OctetString | V | M | | | Y |
| Initial-Gate-Setting-Description | 303 | 10.3.3 | Grouped | V | M | | | Y |
| QoS-Profile-Description | 304 | 10.3.4 | Grouped | V | M | | | Y |
| Physical-Access-ID | 313 | 10.3.5 | UTF8String | V | M | | | Y |
| Initial-Gate-Setting-ID | 314 | 10.3.6 | Unsigned32 | V | M | | | Y |
| QoS-Profile-ID | 315 | 10.3.7 | Unsigned32 | V | M | | | Y |
| NOTE – The AVP flag bit denoted as "M" indicates support of the AVP is required. The AVP flag bit denoted as "V" indicates the optional Vendor-ID field is present in the AVP header. | | | | | | | | |

Table 10-3 describes the Diameter AVPs defined by [ETSI TS 183 020] and used within this Recommendation. These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI TS 183 020]. The Vendor-Id header of all AVPs defined in Table 10-3 shall be set to ETSI (13019).

**Table 10-3 – Diameter AVPs imported from ETSI TS 183 020**

| Attribute name | AVP code | Clause defined | Value type | AVP flag rules | | | | May encrypt |
|---|---|---|---|---|---|---|---|---|
| | | | | Must | May | Should not | Must not | |
| Privacy-Indicator | 440 | 10.3.8 | Grouped | V | M | | | Y |
| NOTE – The AVP flag bit denoted as "M" indicates support of the AVP is required. The AVP flag bit denoted as "V" indicates the optional Vendor-ID field is present in the AVP header. | | | | | | | | |

Table 10-4 describes the Diameter AVPs defined by [ETSI TS 183 066] and used within this Recommendation. These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI TS 183 066]. The Vendor-Id header of all AVPs defined in Table 10-4 shall be set to ETSI (13019).

**Table 10-4 – Diameter AVPs imported from ETSI TS 183 066**

| Attribute name | AVP code | Clause defined | Value type | AVP flag rules | | | | May encrypt |
|---|---|---|---|---|---|---|---|---|
| | | | | Must | May | Should not | Must not | |
| Data-Operation-Indicator | 420 | 10.3.9 | Enumerated | V | M | | | Y |
| NOTE – The AVP flag bit denoted as "M" indicates support of the AVP is required. The AVP flag bit denoted as "V" indicates the optional Vendor-ID field is present in the AVP header. | | | | | | | | |

Table 10-5 describes the AVPs defined solely within this Recommendation. The ITU-T Vendor-Id (11502) shall be used in the Vendor-Id field of the AVP header.

**Table 10-5 – Diameter AVPs defined in this Recommendation**

| Attribute name | AVP code | Clause defined | Value type | AVP flag rules | | | | May encrypt |
|---|---|---|---|---|---|---|---|---|
| | | | | Must | May | Should not | Must not | |
| Mobility-Service-Parameters | 1050 | 10.3.10 | Grouped | V | M | | | Y |
| Home-TLM-PE-Contact-Point | 1051 | 10.3.11 | DiameterIdentity | V | M | | | Y |
| Local-TLM-PE-Contact-Point | 1052 | 10.3.12 | DiameterIdentity | V | M | | | Y |
| Security-Association | 1053 | 10.3.13 | OctetString | V | M | | | Y |
| Central-MLM-PE-Contact-Point | 1054 | 10.3.14 | DiameterIdentity | V | M | | | Y |
| Proxy-MLM-PE-Contact-Point | 1055 | 10.3.15 | DiameterIdentity | V | M | | | Y |
| Mobility-Protocol-Type | 1056 | 10.3.16 | Enumerated | V | M | | | Y |
| Anchor-Point-Address | 1057 | 10.3.17 | DiameterIdentity | V | M | | | Y |
| Tunnel-End-Point-Address | 1058 | 10.3.18 | DiameterIdentity | V | M | | | Y |
| NOTE – The AVP flag bit denoted as "M" indicates support of the AVP is required. The AVP flag bit denoted as "V" indicates the optional Vendor-ID field is present in the AVP header. | | | | | | | | |

### 10.3.1 Globally-Unique-Address AVP

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

*AVP format:*

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

### 10.3.2 Logical-Access-ID AVP

The Logical-Access-ID AVP (AVP code 302 13019) is of type OctetString. This AVP contains either a circuit identifier or a technology independent identifier.

NOTE – In the ATM case, the logical access ID may explicitly contain the identity of the virtual path (VP) and virtual channel (VC) carrying the traffic.

### 10.3.3 Initial-Gate-Setting-Description AVP

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

*AVP Format:*

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

### 10.3.4 QoS-Profile-Description AVP

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

*AVP Format:*

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

### 10.3.5 Physical-Access-ID AVP

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

### 10.3.6 Initial-Gate-Setting-ID AVP

The Initial-Gate-Setting-ID AVP (AVP code 314 13019) is of type Unsigned32 and contains a pointer to a pre-defined set of initial gate setting information. This AVP and the Initial-Gate-Setting-Description AVP shall not be used in the same command.

### 10.3.7 QoS-Profile-ID AVP

The QoS-Profile-ID AVP (AVP code 315 13019) is of type Unsigned32 and contains a pointer to a pre-defined set of QoS profile information.

### 10.3.8 Privacy-Indicator AVP

The Privacy-Indicator AVP (AVP code 440 13019) is of type Grouped and provides policy rules for disclosure of subscriber profile elements to applications.

*AVP Format:*

```
Privacy-Indicator ::= < AVP Header: 440 13019 >
       * {Requested-Information}
       * [AF-Application-Identifier]
```

### 10.3.9 Data-Operation-Indicator AVP

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).

### 10.3.10 Mobility-Service-Parameters AVP

The Mobility-Service-Parameters AVP (AVP code 1050 11502) is of type Grouped and provides mobility service parameters.

*AVP Format:*

```
Mobility-Service-Parameters ::= < AVP Header: 1050 11502 >
       [Central-MLM-PE-Contact-Point]
       [Proxy-MLM-PE-Contact-Point]
       [Keying-Material]
       [Mobility-Protocol-Type]
       [Anchor-Point-Address]
       [Tunnel-End-Point-Address]
```

### 10.3.11 Home-TLM-PE-Contact-Point AVP

The Home-TLM-PE-Contact-Point AVP (AVP code 1051 11502) is of type DiameterIdentity and identifies the FQDN or IP address of the home TLM-PE.

### 10.3.12 Local-TLM-PE-Contact-Point AVP

The Local-TLM-PE-Contact-Point AVP (AVP code 1052 11502) is of type DiameterIdentity and identifies the FQDN or IP address of the local TLM-PE.

### 10.3.13 Security-Association AVP

The Security-Association AVP (AVP code 1053 11502) is of type OctetString and identifies the security association negotiated between the HGW and the TAA-PE during the network access authentication and authorization procedure.

### 10.3.14 Central-MLM-PE-Contact-Point AVP

The Central-MLM-PE-Contact-Point AVP (AVP code 1054 11502) is of type DiameterIdentity and identifies the address of the instance of the MLM-PE containing the mobile address binding information.

### 10.3.15 Proxy-MLM-PE-Contact-Point AVP

The Proxy-MLM-PE-Contact-Point AVP (AVP code 1055 11502) is of type DiameterIdentity and identifies the address of the MLM-PE instance which sends the location registration.

### 10.3.16 Mobility-Protocol-Type AVP

The Mobility-Protocol-Type AVP (AVP code 1056 11502) is of type Enumerated and identifies the type of mobility protocol that TE or CPE could support, for example host-based or network-based mobility.

The following values are defined:

- HOST-BASED-MOBILITY (0).

- NETWORK-BASED-MOBILITY (1).

### 10.3.17 Anchor-Point-Address AVP

The Anchor-Point-Address AVP (AVP code 1057 11502) is of type DiameterIdentity and identifies the upper tunnel end point address, from the UE point of view.

### 10.3.18 Tunnel-End-Point-Address AVP

The Tunnel-End-Point-Address AVP (AVP code 1058 11502) is of type DiameterIdentity and identifies the tunnel end point address for the network node which works as UE's proxy (lower tunnel end point).

## 10.4 Use of namespaces

This clause contains the namespaces that have either been created in this Recommendation or the values assigned to existing namespaces managed by the Internet Assigned Numbers Authority (IANA).

### 10.4.1 AVP codes

This Recommendation uses AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. In addition, this Recommendation assigns AVP code values within the Diameter AVP Code namespace managed by ITU-T. See clause 10.3.

### 10.4.2 Experimental-Result-Code AVP values

This Recommendation assigns the Experimental-Result-Code AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 10.2.

### 10.4.3 Command code values

This Recommendation does not assign command code values but uses existing commands defined by the Internet Engineering Task Force (IETF), including those requested by 3GPP.

### 10.4.4 Application-ID value

This Recommendation defines the Nc Diameter application with application ID 16777325.
The vendor identifier assigned by IANA to ITU-T is 11502
(http:/www.iana.org/assignments/enterprise-numbers).

# 11 Security considerations

The security requirements within the functional requirements and architecture of the network attachment control functions (NACF) are addressed by [ITU-T Y.2701]. The Nc interface shall follow the security requirements of [ITU-T Y.2014].

Clause 9.1 recommends the use of IPsec to ensure secure transport of Diameter messages. Guidelines on the use of SCTP with IPsec can be found in [b-IETF RFC 3554].

Further considerations are provided in the security considerations section of [IETF RFC 6733].

# Bibliography


[b-ITU-T Q.1001] Recommendation ITU-T Q.1001 (1988), *General aspects of public land mobile networks.*

[b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP).*

[b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

[b-IETF RFC 3554] IETF RFC 3554 (2003), *On the Use of Stream Control Transmission Protocol (SCTP) with IPsec*.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Terminals and subjective and objective assessment methods |
| **Series Q** | **Switching and signalling** |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| Series X | Data networks, open system communications and security |
| Series Y | Global information infrastructure, Internet protocol aspects and next-generation networks |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2015