International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3222

(04/2010)

SERIES Q: SWITCHING AND SIGNALLING

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

Requirements and protocol at the interface between transport location management physical entities (Ng interface)

Recommendation ITU-T Q.3222

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 NGN networks	Q.3900–Q.3999

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

Recommendation ITU-T Q.3222

Requirements and protocol at the interface between transport location management physical entities (Ng interface)

Summary

Recommendation ITU-T Q.3222 provides the signalling requirements and protocol for the interface between the local transport location management physical entity and the home transport location management physical entity in the network attachment control function (NACF) block of the next generation network (NGN) release 1. When the local and the home transport location management physical entities (TLM-PEs) are the different access networks, this protocol can be used for communication between both TLM-PE instances. This Recommendation satisfies the requirements for information flows across the Ng reference point as specified in Recommendation ITU-T Y.2014.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3222	2010-04-30	11

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/.

CONTENTS

Recommendation ITU-T Q.3222

Requirements and protocol at the interface between transport location management physical entities (Ng interface)

1 Scope

This Recommendation defines the requirements and protocol for the Ng interface between transport location management physical entities. The Ng reference point enables communication between local and home transport location management physical entities (TLM-PEs).

NOTE – Work for this Recommendation is based on the context of [ITU-T Y.2012] and [ITU-T Y.2014]; this Recommendation satisfies the requirements for information flows across the Ng reference point as specified in [ITU-T Y.2014] and the functional requirement and architecture specified in [ITU-T Y.2012].

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.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[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 (2008), *e4 interface based on the Diameter protocol*.

[ETSI ES 283 035] ETSI ES 283 035 (2008), *e2 interface based on the Diameter protocol*.

[ETSI TS 129 229] ETSI TS 129 229 (2010), *Cx and Dx interfaces based on the Diameter protocol; Protocol details*.

[ETSI TS 129 329] ETSI TS 129 329 (2006), *Sh interface based on the Diameter protocol; Protocol details*.

[IETF RFC 2960] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

[IETF RFC 3046] IETF RFC 3046 (2001), *DHCP Relay Agent Information Option*.

[IETF RFC 3309] IETF RFC 3309 (2002), *Stream Control Transmission Protocol (SCTP) Checksum Change*.

[IETF RFC 3588] IETF RFC 3588 (2003), *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).

3.1.3 location registration (LR) [b-ITU-T Q.1741.3]: The UE registers its presence in a registration area, for instance,k regularly or when entering a new registration area.

3.1.4 nomadism [b-ITU-T Q.1761]: Ability of the user to change his network access point after moving; when changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no handover possible. It is assumed that the normal usage pattern is that users shut down their service session before moving to another access point or changing terminal. This is the mobility alluded to in the case of fixed mobile convergence.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 session data: IP-connectivity related data consisting of globally unique IP address information, transport subscriber identifier, type of access transport, transport resource subscription profile information and physical/logical connection identifier.

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

CEA Capability Exchange Answer

CER Capability Exchange Request

CPE Customer Premises Equipment

FQDN Fully Qualified Domain Name

GTP GPRS Tunnelling Protocol

IMPI IMS Private User Identity

IMPU IMS Public User Identity

MAC Media Access Control

MPLS MultiProtocol Label Switching

MSC Mobile Switching Centre

NACE Network Attachment Control Entity

NACF Network Attachment Control Functions

NAC-PE Network Access Configuration Physical Entity

P-CSC-PE Proxy-Call Session Control Physical Entity

PD-PE Policy Decision Physical Entity

PE-FE Policy Enforcement Functional Entity

PLMN Public Land Mobile Network

PNA Push Notification Answer

PNR Push Notification Request

PPP Point-to-Point Protocol

RACE Resource and Admission Control Entity

RACF Resource and Admission Control Functions

SCE Service Control Entity

SCTP Stream Control Transport Protocol

SDP Session Description Protocol

SIP Session Initiation Protocol

TAA-PE Transport Authentication and Authorization Physical Entity

TLM-PE Transport Location Management Physical Entity

UDA User Data Answer

UDR User Data Request

UE User Equipment

VPN Virtual Private Network

WLAN Wireless Local Area Network

xDSL x Digital Subscriber Line

5 Ng interface

5.1 Overview

The network attachment control entity (NACE) maintains information on IP-connectivity access sessions associated with user equipment connected to the NGN network. This information is stored in the transport location management physical entity (TLM-PE), and can be retrieved by other control functions and applications through the following three interfaces:

– The S-TC1 interface enables service control entity (SCE) to retrieve IP-connectivity related session data.

– The Ru interface enables the IP-connectivity related session data to be exchanged between the NACE and the resource and admission control entity (RACE) defined in [ITU-T Y.2012].

– The Ng interface enables the home TLM-PE to retrieve session data related to IP-connectivity from the local TLM-PE.

This Recommendation specifies the protocol for the Ng interface.

The Ng interface enables the home TLM-PE to retrieve session data related to IP-connectivity from the local TLM-PE.

When the user/customer premises equipment (CPE) moves in a different access domain, the location binding information of the local TLM-PE needs to be registered. On the other hand, when the user/CPE moves within 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 service control entities (SCEs) can retrieve information about the characteristics of the IP-connectivity session used to access (e.g., network location information) from the TLM-PE. The form of location information that is provided by the TLM-PE depends on the requestor. When the user/CPE moves in a different access domain, the service control functions of the home network access the TLM-PE in the visited network for location information via a proxy-TLM-PE in the home network.

Therefore, two operations may occur at the Ng interface as following:

– location registration, in the direction from the local TLM-PE to the home TLM-PE;

– information query, in the direction from the home TLM-PE to the local TLM-PE.

5.2 Ng reference model

This clause describes the reference architecture. As the initial architecture, the illustration below can be used:

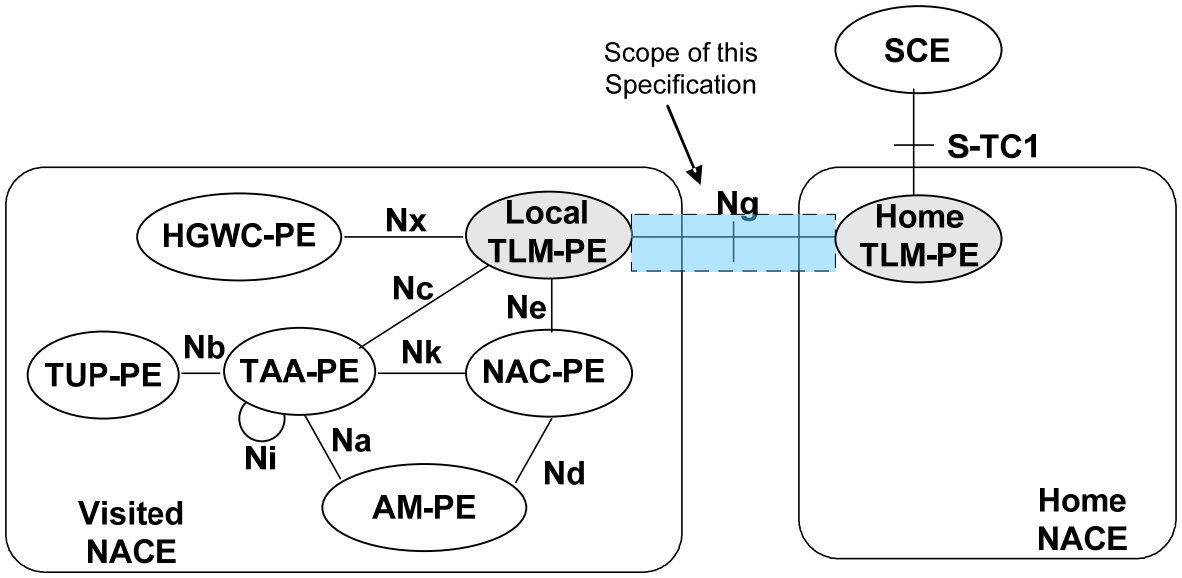

Figure 5-1 – Ng reference model

5.3 Physical entities and capabilities

5.3.1 Transport location management physical entity (TLM-PE)

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, etc.) depending on the agreement with the requester and on the user's 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/CPE in the access domain is stored and bound in the local TLM-PE. So 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 is attached. The home TLM-PE is in the network designated by the TUP-TE. 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 SCE with user network profile information through the local TLM-PE of the visited 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 Signalling requirements

The Ng reference point enables the home TLM-PE to retrieve network location information from the local TLM-PE. The primary parameter for retrieving the location information shall be the assigned IP address allocated to the terminal.

The form of location information provided by the local TLM-PE depends on the home TLM-PE.

The following information flows are used on this interface:

– Location Registration Request/Response;

– Information Query Request/Response.

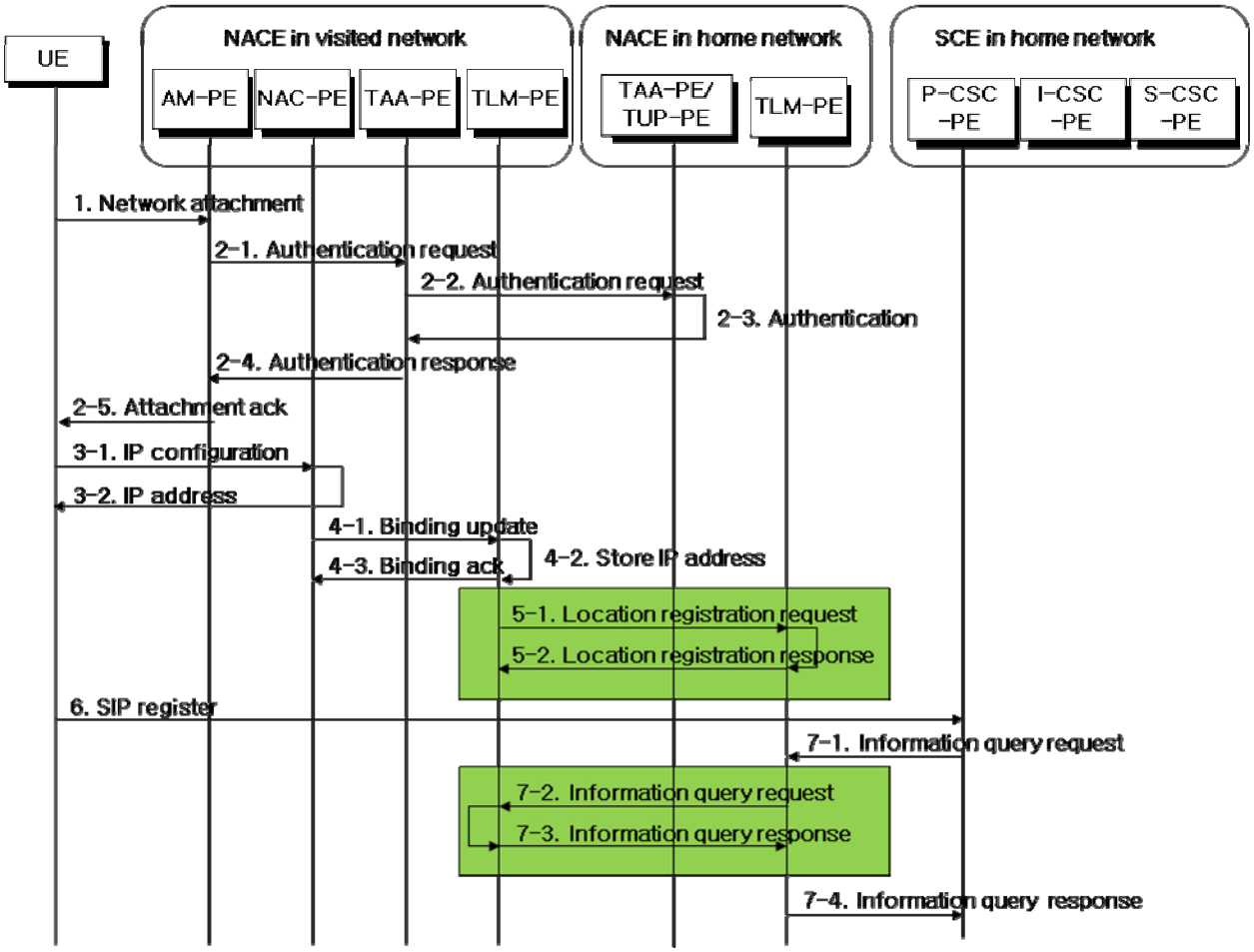

Figure 6-1 – High-level information flows

This generic case describes a scenario in which the service control entity (SCE) is located in its home network, not in the visited network. In x digital subscriber line (xDSL) access network or WLAN hotspot environment, a service control entity (SCE) requires the UE's line identifier or access point location to provide location-based services. Because the service control entity (SCE) knows only the TLM-PE in its home network, it should request its own home TLM-PE to acquire location information. But, the real association information of IP address and location is stored in and accessible to the TLM-PE of the visited network.

However, the service control entity has no idea about the TLM-PE in the visited network. The TLM-PE in the home network should proxy the request to the TLM-PE in the visited network and gets the response back.

1) The UE gets a network attachment after the authentication at the NACE level in the visited network.

2-1) The AM-PE sends an authentication and authorization request to the TAA-PE in the visited network.

2-2) The TAA-PE forwards a NACE authentication and authorization request to the TAA-PE in the home network by proxy, because it does not have the user's network level database in its TUP-PE. The proxy request is delivered to the TAA-PE in the home network.

2-3) The TAA-PE in the home network authenticates and authorizes at the NACE level. It returns the NACE authentication data back.

2-4) The TAA-PE sends the authentication response to the AM-PE in order to configure the forwarding table in the AM-PE.

2-5) The AM-PE sends the attachment ACK to inform of the starting of the packet forwarding at the AM-PE.

3-1) The UE sends IP configuration request to the NAC-PE after authentication.

3-2) The NAC-PE performs IP configuration procedure and returns the IP address.

4-1) The NAC-PE sends binding update to the TLM-PE by using the assigned IP address.

4-2 to 4-3) The TLM-PE stores the association of the IP address and line identifier. The TLM-PE in the NACE holds a binding between the IP address and the location information (contains the line identifier or the access point location information), which the user holds per the xDSL or WLAN connectivity.

5-1) The TLM-PE in the visited network registers its location to the TLM-PE in the home network in order to indicate its location.

5-2) The TLM-PE in the home network sends the result to the TLM-PE in the visited network.

6) The UE sends a SIP REGISTER message to the SCE to use services.

7-1) The SCE requests the location information to its home TLM-PE.

7-2) The TLM-PE in the home network sends a request of location to the TLM-PE in the visited network by proxy.

7-3) The TLM-PE in the visited network sends the location information of the UE.

7-4) The TLM-PE in the home network sends the location information to the SCE.

6.1 Location registration

The location registration request information flow contains the following information (see Table 6-1).

Table 6-1 – Location registration request (local TLM-PE → home TLM-PE)

Information element	Explanation
Globally Unique IP Address Information	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).
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.
Attached Access Domain Name	The access domain name or the provider's name of the network.
Index of Local NACE	The address of the local NACE the user belongs to, which is registered by TLM-PE.

The location registration response information flow contains the following information (see Table 6-2).

Table 6-2 – Location registration response (home TLM-PE → local TLM-PE)

Information element	Explanation
Globally Unique IP Address Information	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).
Transport Subscriber Identifier	A globally unique identifier for the attached CPE.
Result	Result code (e.g., success, permanent failure, etc.).

6.2 Information query

The information query request information flow contains the following information (see Table 6-3).

Table 6-3 – Information query request (home TLM-PE → local TLM-PE)

Information element	Explanation
Globally Unique IP Address Information	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).
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.
Requested Items	The item list to the requested information.
Attached Access Domain Name	The access domain name or the provider's name of the network.
Index of Local NACE	The address of the local NACE the user belongs to, which is registered by TLM-PE.

The information query response information flow contains the following information (see Table 6-4).

Table 6-4 – Information query response (local TLM-PE → home TLM-PE)

Information element	Explanation
Transport Subscriber Identifier (optional)	A globally unique identifier for the attached CPE (see Note 1).
Location Information (optional) (see Note 2)	Location information (or a pointer to such information) in a form that is suitable for the requesting service control entity.
RACE Contact Point (optional)	The FQDN or IP address of the RACE where resource request shall be sent (i.e., PD-PE address).
CPE Type (optional)	The type of CPE.
Type of Access Transport (optional)	The type of access network to which the CPE is attached.
IP Connectivity Status (optional)	Whether IP connectivity to/from the user equipment is currently available.

Table 6-4 – Information query response (local TLM-PE → home TLM-PE)

Information element	Explanation
Physical Connection Identifier (optional)	A local identifier for physical connection of access transport network that the CPE is attached to (e.g., IP address of PE-FE device, and MAC address or link ID and physical port).
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). It can be used to locate the layer 2 connection and pertinent network devices for a particular CPE requesting the access transport resource.
NOTE 1 – This identifier may be used by the SCE when interacting with the RACE. NOTE 2 – Location information disclosure depends on the requesting application and the subscriber's privacy restrictions. Privacy restrictions are defined in the privacy indicator stored in the TLM-PE.	

7 Description of procedure

7.1 General

The following clauses describe the realization of the functional procedures defined in the NACE specifications, using Diameter commands described in clause 9. This involves describing a mapping between information elements defined in the NACE specification and Diameter AVPs.

In the tables that describe this mapping, each information element is marked as (M) mandatory, (C) conditional or (O) optional [ETSI ES 283 035].

7.2 Procedure on the Ng interface

7.2.1 Location registration

7.2.1.1 Overview

Location registration procedure is used by a local TLM-PE to notify the home TLM-PE of the occurrence of the location binding information.

Location registration request/answer is mapped to the commands Push-Notifications-Request/ Answer in the Diameter application specified in Sh interface [ETSI TS 129 329]. Tables 7-1 and 7-2 detail the involved information elements as defined in the NACE and their mapping to Diameter AVPs.

Table 7-1 – Mapping of location registration request to Diameter AVP

Information element name	Diameter AVP	Category
Unique IP Address	Globally-Unique-Address	C
Address Realm		
Transport Subscriber Identifier	User-Name	C
Attached Access Domain Name	Access-Domain-Name	M
Index of Local NACE	Local-NACE-Contact-Point	M

Table 7-2 – Mapping of location registration response to Diameter AVP

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

7.2.1.2 Procedure at the local TLM-PE

The local TLM-PE shall request the Location Registration Request by including the following information elements:

1) At least, a Globally-Unique-Address or a User-Name AVP shall be included. The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP.

2) The Access-Domain-Name AVP and the Local-NACE-Contact-Point shall be present.

7.2.1.3 Procedure at the home TLM-PE

Upon reception of a Location Registration Request, the home TLM-PE shall:

1) Check both the Globally-Unique-Address AVP and the User-Name AVP.

2) If the Globally-Unique-Address AVP is present, go to step 6). Otherwise, go to the next step.

3) If the Globally-Unique-Address AVP is absent, but the User-Name AVP is present, go to step 5). Otherwise, go to the next step.

4) Because both the Globally-Unique-Address AVP and the User-Name AVP are absent, return a Location Registration Response with Result-Code set to DIAMETER_MISSING_AVP and stop this procedure. If the Access-Domain-Name AVP and the Local-NACE-Contact Point AVP are absent, return a Location Registration Response with Result-Code set to DIAMETER_MISSING_AVP and stop this procedure.

5) If more than one record includes the same subscriber identity matching the value of the User-Name AVP and no Globally-Unique-Address AVP is included, return a Location Registration Response with Result-Code set to DIAMETER_UNABLE_TO_COMPLY and stop this procedure. Otherwise, go to the next step.

6) Under temporary overload conditions, the home TLM-PE shall stop processing the request and return a Location Registration Response with the Experimental-Result-Code set to DIAMETER_USER_DATA_NOT_AVAILABLE and stop this procedure. Otherwise, go to the next step.

7) If the home TLM-PE cannot fulfill the received request for reasons not stated in the above steps, e.g., due to database error, it shall stop processing the request and set the Result-Code to DIAMETER_UNABLE_TO_COMPLY.

8) The Access-Domain-Name AVP and the Local-NACE-Contact Point AVP are stored in the home TLM-PE and the home TLM-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS in the Location Registration Response and stop this procedure.

7.2.2 Information query

7.2.2.1 Overview

The information query procedure is used by a home TLM-PE to retrieve, from the local TLM-PE, location information and other data related to an access session. This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in Sh interface [ETSI TS 129 329]. Tables 7-3 and 7-4 detail the involved information elements as defined in the NACE and their mapping to Diameter AVPs.

Table 7-3 – Mapping of information query request to Diameter AVP

Information element name	Diameter AVP	Category
Unique IP Address	Globally-Unique-Address	C
Address Realm		
Transport Subscriber Identifier	User-Name	C
Requested Items	Requested-Information	O
Attached Access Domain Name	Access-Domain-Name	M
Index of Local NACE	Local-NACE-Contact-Point	M

Table 7-4 – Mapping of information query response to Diameter AVP

Information element name	Diameter AVP	Category
Result	Result-Code/Experimental-Result	M
Transport Subscriber Identifier	User-Name	O
Location Information	Location-Information	O
RACE contact point	RACE-Contact-Point	O
Access Transport Network Type	Access-Network-Type	O
CPE Type	CPE-Type	O
IP Connectivity status	IP-connectivity-status	O
Physical Connection Identifier	Physical-Connection-Identifier	O
Logical Connection Identifier	Logical-Connection-Identifier	O

7.2.2.2 Procedure at the home TLM-PE

The home TLM-PE shall request the Information Query Request by including the following information elements:

1) Either a Globally-Unique-Address AVP or a User-Name AVP will be present. The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value and an Address-Realm AVP.
2) The Access-Domain-Name AVP and the Local-NACE-Contact-Point shall be present.
3) The Requested-Information AVP shall be present if specific information is requested, and shall be absent if all available information is requested.

7.2.2.3 Procedure at the local TLM-PE

Upon reception of an Information Query Request, the home TLM-PE shall:

1) Check both the Globally-Unique-Address AVP and the User-Name AVP.
2) If the Globally-Unique-Address AVP is present, go to step 6) to use this information as a key to retrieve the requested session information. Otherwise, go to the next step.
3) If the Globally-Unique-Address AVP is absent, but the User-Name AVP is present, go to step 5) to use the latter information as a key to retrieve the requested session information. Otherwise, go to the next step.
4) Because both the Globally-Unique-Address AVP and the User-Name AVP are absent, return an Information Query Response with a Result-Code set to DIAMETER_MISSING_AVP and stop this procedure. If the Access-Domain-Name AVP and the Local-NACE-Contact-Point AVP are absent, return an Information Query Response with Result-Code set to DIAMETER_MISSING_AVP and stop this procedure.

5) If more than one record includes the same subscriber identity matching the value of the User-Name AVP and no Globally-Unique-Address AVP is included, return an Information Query Response with Result-Code set to DIAMETER_UNABLE_TO_COMPLY and stop this procedure. Otherwise, go to the next step.

6) If no session record is stored for the Globally-Unique-Address AVP or the User-Name AVP, return an Information Query Response with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN and stop this procedure. Otherwise, go to the next step.

7) Under temporary overload conditions, the local TLM-PE shall stop processing the request and return an Information Query Response with the Experimental-Result-Code set to DIAMETER_USER_DATA_NOT_AVAILABLE and stop this procedure. Otherwise, go to the next step.

8) If the local TLM-PE cannot fulfill the received request for reasons not stated in the above steps, e.g., due to database error, it shall stop processing the request and set the Result-Code to DIAMETER_UNABLE_TO_COMPLY.

9) Check which session data can be returned to the home TLM-PE, based on local policy rules and per-subscriber privacy information stored in the local TLM-PE. If the session data to be retrieved is currently being updated by another entity, the local TLM-PE may delay the response message until the update has been completed and shall include in the response message the updated data requested. The requested operation shall take place and the local TLM-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS and the session data in the Information Query Response and stop this procedure.

8 Use of Diameter-based protocol

With the clarifications listed in the following clauses, the Diameter Base Protocol defined by [IETF RFC 3588] shall apply.

8.1 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 [b-IETF RFC 3554].

8.2 Accounting functionality

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

8.3 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 3588].

The Diameter-based 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 or responses the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in [IETF RFC 3588]. 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.

8.4 Transport protocol

Diameter messages over the Ng interface shall make use of stream control transport protocol (SCTP) [IETF RFC 2960] and shall utilize the new SCTP checksum method specified in [IETF RFC 3309].

8.5 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 Ng interface, the local TLM-PE acts as a Diameter server and the home TLM-PE acts as the Diameter client.

Requests initiated by the local TLM-PE towards a home TLM-PE shall include both Destination-Host and Destination-Realm AVPs. The local TLM-PE obtains the Destination-Host AVP to use in requests towards a home TLM-PE from configuration data and/or the subscriber profile. Consequently, the Destination-Host AVP is declared as mandatory in the Augmented Backus-Naur Form (ABNF) for all requests initiated by the TLM-PE. Destination-Realm AVP is declared as mandatory in the ABNF for all requests.

8.6 Advertising application support

The Capabilities-Exchange-Request (CER) and the Capabilities-Exchange-Answer (CEA) commands are specified in [IETF RFC 3588]. The Diameter-base application identifier (0) shall be used in the Diameter message header of these messages.

If both home and local TLM-PE indicate support of the Ng application, then the Ng application identifier (16777263) shall be used in the Diameter message header of all subsequent messages exchanged within this association.

Support of the Ng 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 Ng (16777263).

The home TLM-PE and the local TLM-PE are required to advertise the support of AVPs specified in the Diameter related documents of 3GPP, ETSI and ITU-T, 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.

Table 8-1 – Vendor identifiers for Ng

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

NOTE – The Vendor-Id AVP included in Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer (CEA) 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 3588].

9 Message specification

9.1 Commands

This Recommendation re-uses the four Diameter commands identified in Table 9-1 which are defined in [ETSI TS 129 329]. Other commands are ignored by the local TLM-PE and the home TLM-PE.

Table 9-1 – Command code

Command	Abbreviation	Defining reference	Command code	See clause
Push-Notification-Request	PNR	[ETSI TS 129 329]	309	9.1.1
Push-Notification-Answer	PNA	[ETSI TS 129 329]	309	9.1.2
User-Data-Request	UDR	[ETSI TS 129 329]	306	9.1.3
User-Data-Answer	UDA	[ETSI TS 129 329]	306	9.1.4

9.1.1 Push-Notification-Request (PNR) command

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

Message format:

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777263>
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                [ Globally-Unique-Address ]
                                [ User-Name ]
                                { Access-Domain-Name }
                                { Local-NACE-Contact-Point }
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

9.1.2 Push-Notification-Answer (PNA) 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 (PNR) command. The Experimental-Result AVP may contain one of the values defined in clause 9.2.

Message format:

```
< Push-Notification-Answer > ::= < Diameter Header: 309, PXY, 16777263>
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                *[ AVP ]
```

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

9.1.3 User-Data-Request (UDR) command

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

Message format:

```
< User-Data-Request > ::= < Diameter Header: 306, REQ, PXY, 16777263>
                              < Session-Id >
                              { Vendor-Specific-Application-Id }
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              [ Destination-Host ]
                              { Destination-Realm }
                              [ Globally-Unique-Address ]
                              [ User-Name ]
                              [ Requested-Information ]
                              { Access-Domain-Name }
                              { Local-NACE-Contact-Point }
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

9.1.4 User-Data-Answer (UDA) command

The User-Data-Answer (UDA) command, indicated by the Command-Code field set to 306 and the "R" bit cleared in the Command Flags field, is sent by a server in response to the User-Data-Request command. This command is defined in [ETSI TS 129 329] and used with additional AVPs defined in this Recommendation. The Experimental-Result AVP may contain one of the values defined in clause 9.2.

Message format:

```
< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777263>
                              < Session-Id >
                              { Vendor-Specific-Application-Id }
                              [ Result-Code ]
                              [ Experimental-Result ]
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              [ User-Name ]
                              [ Physical-Connection-Identifier ]
                              [ Logical-Connection-Identifier ]
                              [ Access-Network-Type ]
                              [ Location-Information ]
                              [ RACE-Contact-Point ]
                              [ CPE-Type ]
                              [ IP-Connectivity-status ]
                              *[ AVP ]
                              *[ Failed-AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

9.2 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.

9.2.1 Experimental-Result-Code AVP values imported from [ETSI TS 129 229]

This clause defines the specific values of the Experimental-Result-Code AVP imported from [ETSI TS 129 229] (the 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.

9.3 Attribute value pairs (AVPs)

The following tables summarize the AVPs used in this Recommendation. These are, in addition to the AVPs, defined in [IETF RFC 3588].

Table 9-2 describes the Diameter AVPs that are used within this Recommendation that have been defined by ETSI [ETSI ES 283 035], providing their AVP code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs identified in the following table shall be set to ETSI (13019). These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI ES 283 035].

Table 9-2 – Diameter AVPs imported from [ETSI ES 283 035]

Attribute name	AVP code	Clause defined	Value type (Note 2)	AVP flag rules (Note 1)				May encrypt
				Must	May	Should not	Must not	
Location-Information	350	9.3.4	Grouped	V	M			Y
RACE-Contact-Point	351	9.3.5	DiameterIdentity	V	M			Y
CPE-Type	352	9.3.6	OctetString	V	M			Y
Requested-Information	353	9.3.2	Enumerated	V			M	Y
NOTE 1 – The AVP header bit denoted as 'M' indicates whether support of the AVP is required. The AVP header bit denoted as 'V' indicates whether the optional Vendor-Id field is present in the AVP header. For further details, see [IETF RFC 3588]. NOTE 2 – The value types are defined in [IETF RFC 3588].								

Table 9-3 describes the Diameter AVPs defined by the e4 interface protocol [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 9-3 shall be set to ETSI (13019).

Table 9-3 – 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	9.3.1	Grouped	M,V				Y
Logical-Connection-Identifier	302	9.3.9	OctetString	V	M			Y
Access-Network-Type	306	9.3.3	Grouped	V	M			Y
IP-Connectivity-Status	305	9.3.7	Enumerated	V	M			Y
Physical-Connection-Identifier	313	9.3.8	UTF8String	V	M			Y

Table 9-4 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 9-4 – 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	
Access-Domain-Name	1030	9.3.10	OctetString	M,V				Y
Local-NACE-Contact-Point	1031	9.3.11	DiameterIdentity	M,V				Y

9.3.1 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]
```

9.3.2 Requested-Information AVP

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

- SUBSCRIBER-ID (0).
- LOCATION-INFORMATION (1).
- RACE-CONTACT-POINT (2).
- ACCESS-NETWORK-TYPE (3).
- CPE-TYPE (4).
- LOGICAL-CONNECTION-IDENTIFIER (5).
- PHYSICAL-CONNECTION-IDENTIFIER (6).
- ACCESS-NETWORK-TYPE (7).

- DEFAULT-CONFIGURATION (8).
- TRANSPORT-RESOURCE-SUBSCRIPTION (9).
- IP-CONNECTIVITY-STATUS (10).

9.3.3 Access-Network-Type AVP

The Access-Network-Type AVP (AVP code 306 13019) is of type Grouped; it indicates the type of port on which the user equipment is connected and the type of aggregation network.

AVP format:

```
Access-Network-Type ::= < AVP Header: 306 13019 >
       {NAS-Port-Type}
       [Aggregation-Network-Type]
```

9.3.4 Location-Information AVP

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

AVP format:

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

9.3.5 RACE-Contact-Point AVP

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

9.3.6 CPE-Type AVP

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

9.3.7 IP-Connectivity-Status AVP

The IP-Connectivity-Status AVP (AVP code 305 13019) is of type Enumerated.

The following values are defined:

- IP-CONNECTIVITY-ON (0).
- IP-CONNECTIVITY-LOST (1).

9.3.8 Physical-Connection-Identifier AVP

The Physical-Connection-Identifier 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.

9.3.9 Logical-Connection-Identifier AVP

The Logical-connection-identifier AVP (AVP code 302 13019) is of type OctetString. This AVP contains either a Circuit-ID (as defined in [IETF RFC 3046]) or a technology independent identifier.

NOTE – In the xDSL/ATM case, the logical access ID may explicitly contain the identity of the VP and the VC carrying the traffic.

9.3.10 Access-Domain-Name AVP

The Access-Domain-Name AVP (ITU-T AVP code 1030 11502) is of type OctetString, and provides information about the access domain name or the provider's name of the network.

9.3.11 Local-NACE-Contact-Point AVP

The Local-NACE-Contact-Point AVP (ITU-T AVP code 1031 11502) is of type DiameterIdentity and identifies the Local NACE the user belongs to which is registered by the TLM-PE.

9.4 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).

9.4.1 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 9.3.

9.4.2 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 9.2.

9.4.3 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.

9.4.4 Application-ID value

This Recommendation defines the Ng Diameter application with application ID 16777263. The vendor identifier assigned by IANA to ITU-T (http:/www.iana.org/assignments/enterprise-numbers) is 11502.

10 Security considerations

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

Clause 8.1 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 3588].

Appendix I

Scenarios using Ng interface

(This appendix does not form an integral part of this Recommendation)

I.1 Location information service from the home network with DHCP-based network attachment

I.1.1 Access scenarios for location registration request/response

This clause provides high-level information flows using Ng interface that define the location registration and the information query between the home TLM-PE and the local TLM-PE.

The NACE relies on several stages in the network attachment process. Figure I.1 shows the high-level information flows and the procedures of NACE. This figure also shows the basic network attachment procedure in the home access domain. Depending on the access domain, some additional stages for the location registration at the home TLM-PE can be applied as shown in Figure I.2.

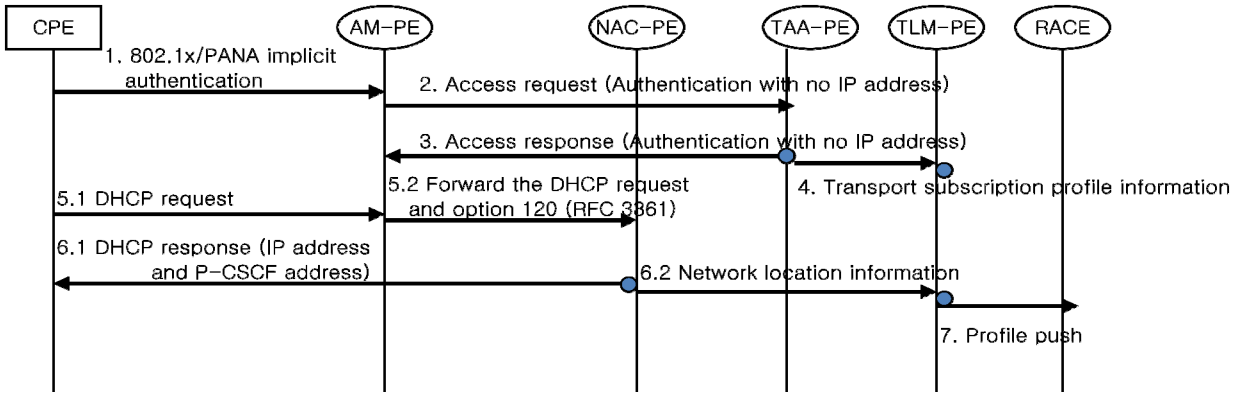

Figure I.1 – Information flows for location registration

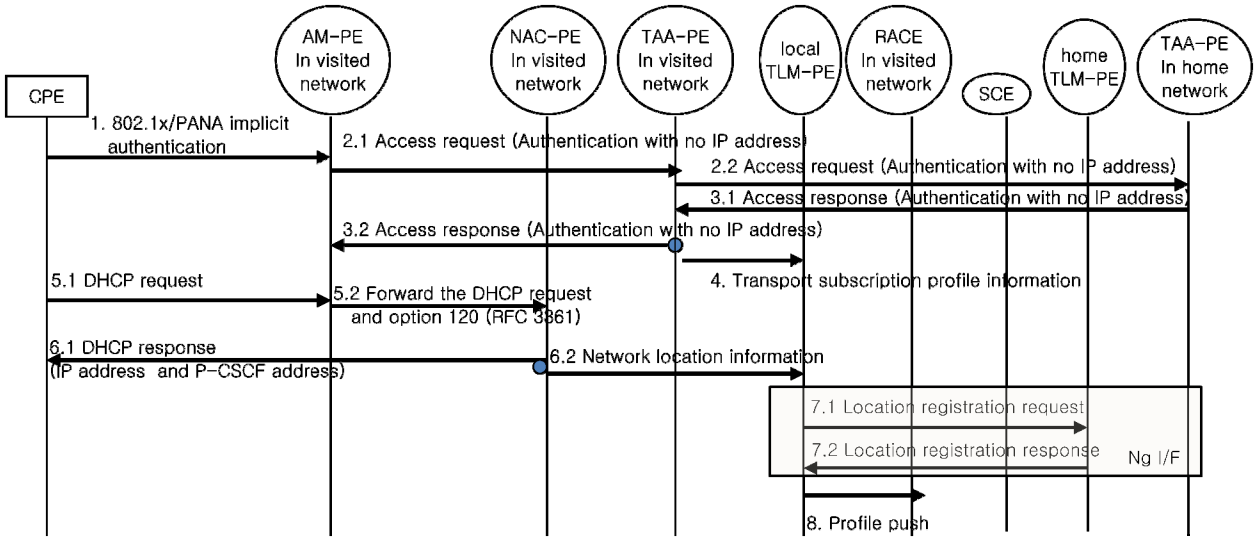

Figure I.2 – Additional information flows for location registration at the home TLM-PE

In the first stage of the network attachment process, the CPE will be authenticated and authorized. In step 1, CPE initiates authentication based on [b-IETF RFC 5191]. In step 2, AM-PE relays and translates PPP request to an access request to the TAA-PE for authentication. It occurs prior or during the IP address allocation procedure (step 2). The authentication process relies on the mechanisms and identities described in clauses 6, 7 and 8 in [ITU-T Y.2014]. Step 2 involves the authorization for access to the network based on the transport subscription profile. In step 2.1, a specific transport subscription profile, related e.g., to QoS, may be also downloaded from the home NGN network to the visited NGN network (from the TAA-PE-server to the TAA-PE-proxy mode).

When the authentication is successful and the CPE is authorized to use access network resources, configuration of access network based on the transport subscription profile is performed in step 5. During step 6.1, the NAC-PE allocates the IP configuration information and provides it to the user equipment/CPE. This mapping information between the allocated IP configuration information and the logical connection identifier is forwarded to the TLM-PE (via the Ne reference point) in step 6.2, which correlates this with the transport subscriber identifier and the transport subscription profile. It also implies that the specific transport subscription profile information for the authenticated user be required to be forwarded to the TLM-PE via the Nc reference point. The profile information includes at least the logical connection identifier (i.e., line ID), the transport subscriber identifier and the transport resource subscription information, which may be the QoS profile downloaded from the home NGN network or a default configuration profile, and the identification of the edge PE-PE device.

The local TLM-PE may also register to the home TLM-PE, the association between the transport location information received from the NAC-PE and the geographical location information in step 7.1. In step 8, the TLM-PE pushes the binding information to the RACE via the TC-TC1 reference point to configure the line with the transport subscription profile information.

I.1.2 Access scenarios for information query request/response

The service control entities (SCEs) can retrieve information about the characteristics of the IP-connectivity session used to access (e.g., network location information) from the TLM-PE. When the user/CPE moves in the different access domain, the service control functions access the TLM-PE in the visited network for location information via a proxy-TLM-PE in the home network as shown in Figure I.3. The form of location information that is provided by the TLM-PE depends on the requestor.

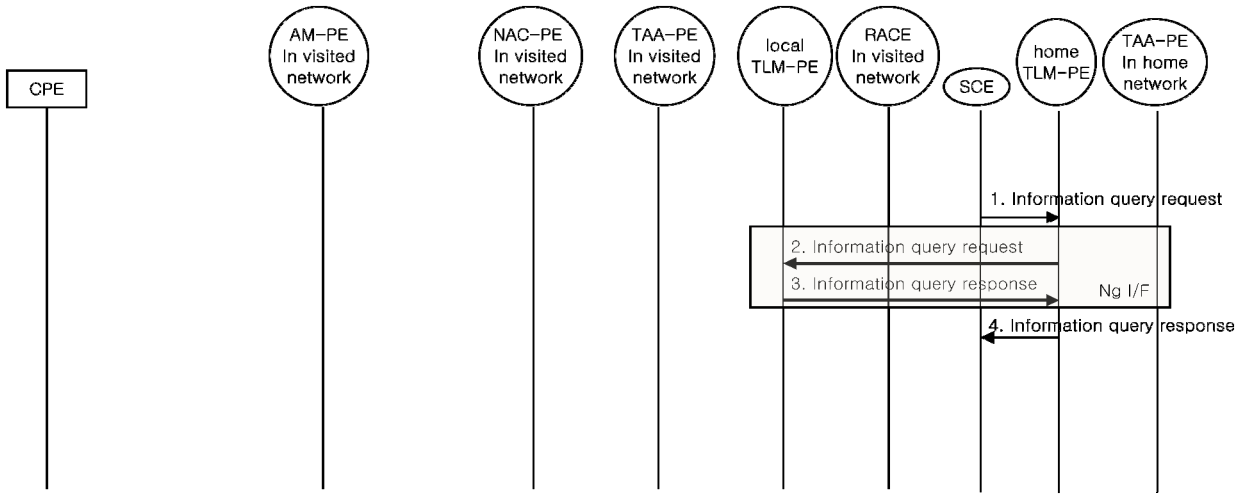

Figure I.3 – Information flows for information query

I.2 NACE-SCE bundled authentication

I.2.1 Case 1: NACE-SCE bundled authentication based on line information

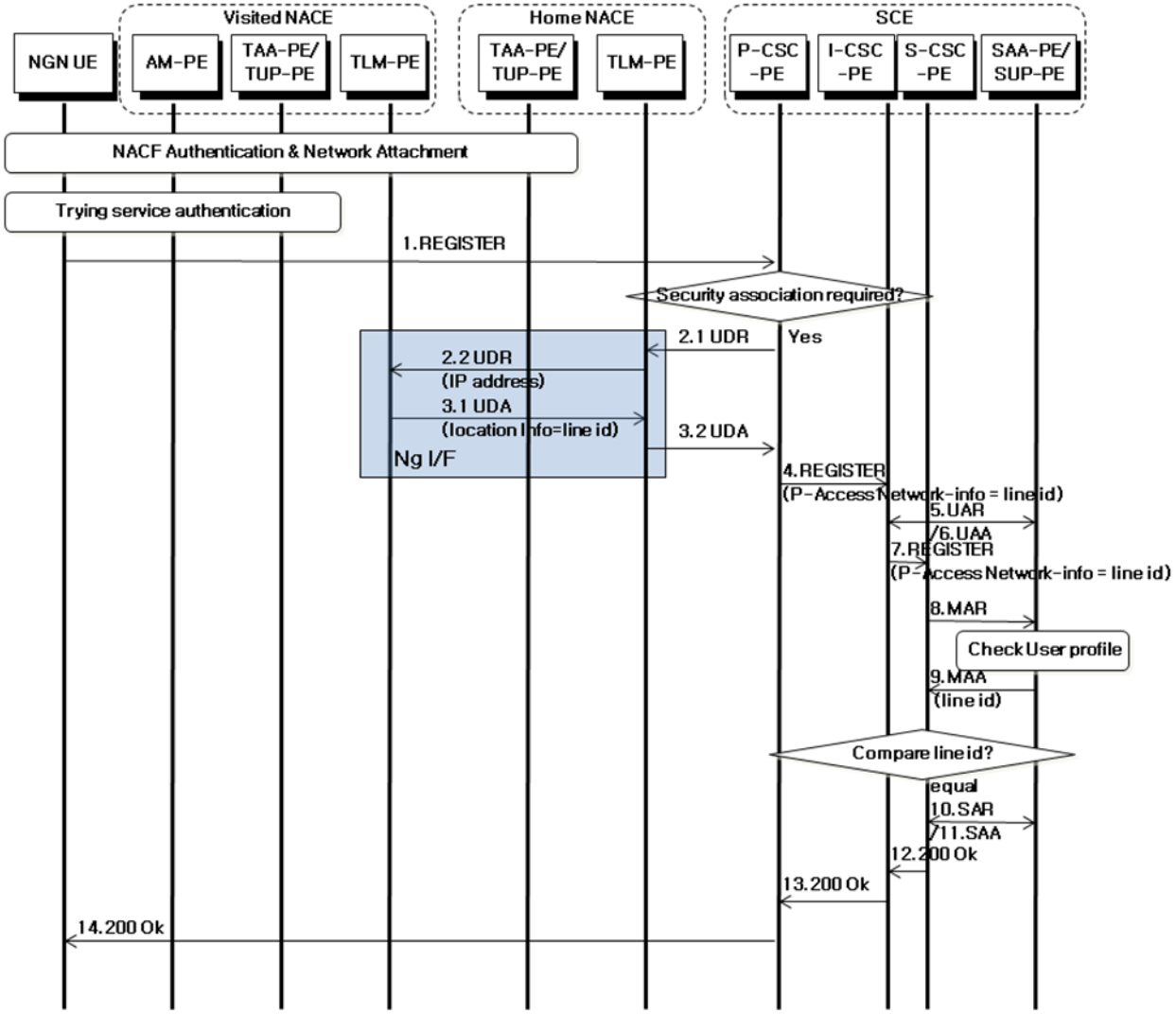

Figure I.4 – NACE-SCE bundled authentication for the fixed access network only

This clause describes how UEs undergo authentication in NACE and simultaneously gain service layer authentication using the single sign-on NACE-SCE bundled authentication with line information.

0) The UE gets network attachment following the authentication at the NACE level. The TLM-PE in the NACE holds a binding between the IP address and the location information (contains the line identifier), held by the user as per the xDSL connectivity. The selection of the authentication (whether NACE-SCE bundled authentication is possible or not) is done at the SUP-PE level on an SCE-user basis.

1) The SIP REGISTER message reaches P-CSC-PE.

2.1-2.2) The P-CSC-PE knows whether or not security association is required at this point, based on the SIP signalling, presence of local policies and L3/L2 address. During the SIP registration, the P-CSC-PE locates the TLM-PE based on the UE's IP address or/and based on the information of the access network from which the P-CSC-PE receives the IP packet. P-CSC-PE performs a UDR request with the local TLM-PE via the home TLM-PE over the S-TC1 interface and the Ng interface. The key for the query is the IP address used by the UE.

3.1-3.2) The local TLM-PE sends the UDA response to the P-CSC-PE via the home TLM-PE including the location information of the UE.

4) The P-CSC-PE appends the NACE location information to the SIP REGISTER message and forwards the REGISTER message to the I-CSC-PE.

5) The I-CSC-PE queries the SUP-PE using the UAR request.

6) The SUP-PE returns a UAA message for selecting the S-CSC-PE.

7) The I-CSC-PE forwards the REGISTER message to the S-CSC-PE.

8) The S-CSC-PE queries the SUP-PE using the MAR request.

9) If line-based NACE bundling is the preferred authentication scheme, the SUP-PE returns a message with the location information of the user identified by IMPI and IMPU.

The S-CSC-PE performs final authentication by comparing the location information embedded in the REGISTER message with the location information received from the SUP-PE. If they match, the user is successfully authenticated.

10-14) If the UE is successfully authenticated, the S-CSC-PE assigns a unique IP address to the SUP-PE using the SAR message, and a SIP 200 OK message is then sent to the UE.

I.2.2 Case 2: NACE-SCE bundled authentication based on the authentication context

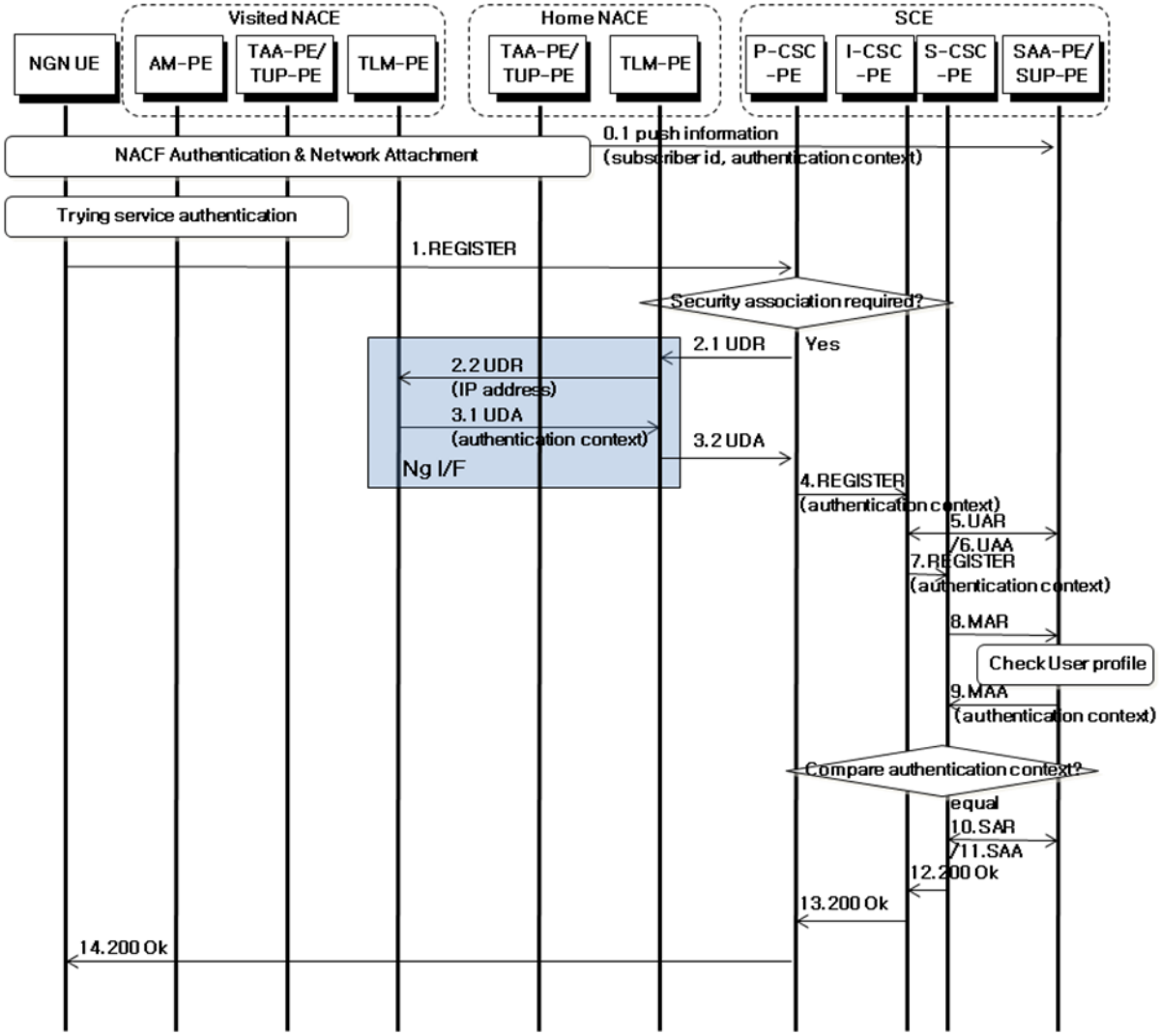

Figure I.5 – NACE-SCE bundled authentication for both the fixed and the mobile access network

This clause describes how UEs authenticate the NACE and simultaneously also gain a service layer authentication using the single sign-on NACE-SCE bundled authentication with a unique context information (for one example, we can use authentication context).

Here, the NACE-SCE bundle authentication scenario example, that is applicable to networks including the mobile access network, will be considered unlike the scenario in I.2.1.

As to the mobile subscriber, the line information does not exist like the fixed user. Therefore, the subscriber id and the access authentication context need to be delivered towards SUP-PE in case of being authenticated.

0) The UE gets network attachment after authentication at the NACE level.

0.1) The TUP-PE delivers subscriber id and authentication context to the SUP-PE. The selection of the authentication (whether NACE-SCE bundled authentication is possible or not) is done at the SUP-PE level on a SCE-user basis. The relation between the subscriber identity and the SCE-user identities (IMPI and IMPU) is already known to the SUP-PE.

1) The SIP REGISTER message reaches P-CSC-PE.

2.1-2.2) The P-CSC-PE knows whether or not a security association is required at this point, based on the SIP signalling, presence of local policies and L3/L2 address. During the SIP registration, the P-CSC-PE locates the TLM-PE based on the UE's IP address or/and based on the information of the access network from which the P-CSC-PE receives the IP packet. P-CSC-PE performs the UDR request toward the local TLM-PE via the home TLM-PE over the S-TC1 interface and the Ng interface. The key for the query is the IP address used by the UE.

3.1-3.2) The local TLM-PE sends the UDA response to the P-CSC-PE via the home TLM-PE including the authentication context of the UE.

4) The P-CSC-PE appends the authentication context to the SIP REGISTER message and forwards the REGISTER message to the I-CSC-PE.

5) The I-CSC-PE queries the SUP-PE using the UAR request.

6) The SUP-PE returns a UAA message for selecting the S-CSC-PE.

7) The I-CSC-PE forwards the REGISTER message to the S-CSC-PE.

8) The S-CSC-PE queries the SUP-PE using the MAR request.

9) The SUP-PE returns a message with the authentication context of the user identified by the IMPI and IMPU, if Authentication Context-based NACE bundling is the preferred authentication scheme.

   The S-CSC-PE finally authenticates by comparing the authentication context embedded in the REGISTER message with the authentication context received from the SUP-PE. If they match, the user is successfully authenticated.

10-14) If the UE is successfully authenticated, the S-CSC-PE assigns its own IP address to the SUP-PE using the SAR message, and a SIP 200 OK message is then sent to the UE.

Bibliography

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

[b-ITU-T Q.1741.3] Recommendation ITU-T Q.1741.3 (2003), *IMT-2000 references to release 5 of GSM evolved UMTS core network.*

[b-ITU-T Q.1761] Recommendation ITU-T Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems.*

[b-ITU-T Q.3221] Recommendation ITU-T Q.3221 (2008), *Requirements and protocol at the interface between the service control entity and the transport location management physical entity (S-TC1 interface).*

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

[b-IETF RFC 4005] IETF RFC 4005 (2005), *Diameter Network Access Server Application.*

[b-IETF RFC 5191] IETF RFC 5191 (2008), *Protocol for Carrying Authentication for Network Access (PANA).*

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, 2010