International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3221

(10/2008)

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 the service control entity and the transport location management physical entity (S-TC1 interface)

Recommendation ITU-T Q.3221

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.3221

Requirements and protocol at the interface between the service control entity and the transport location management physical entity (S-TC1 interface)

Summary

Recommendation ITU-T Q.3221 provides the signalling requirements and protocol for the interface between the service control entities (SCEs) in the services stratum and the transport location management physical entity (TLM-PE) in the network attachment control function block of the next generation network (NGN) release 1. This protocol can be used to retrieve the location information attached by the user equipment. It satisfies the requirements for information flows across the S-TC1 reference point as specified in Recommendation ITU-T Y.2014.

Source

Recommendation ITU-T Q.3221 was approved on 14 October 2008 by ITU-T Study Group 11 (2005-2008) under Recommendation ITU-T A.8 procedure.

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.3221

Requirements and protocol at the interface between the service control entity and the transport location management physical entity (S-TC1 interface)

1 Scope

This Recommendation defines the requirements and protocol for the interface between the transport location management physical entity (TLM-PE) and the service control entity of ITU-T NGN release 1.

At the stage of NGN release 1 [ITU-T Y.2012], this Recommendation is applicable to the interface between TLM-PE and SCE.

1.1 Relationship

Work for this Recommendation is based on the context of [ITU-T Y.2014] and [ITU-T Y.2012]; this Recommendation satisfies the requirements for information flows across the S-TC1 reference point as specified in [ITU-T Y.2014] and the functional requirements 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 (2006), *Functional requirements and architecture of the NGN release 1*.

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2008), *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 TS 129 209] ETSI TS 129 209 V6.7.0 (2007), *Universal Mobile Telecommunications System (UMTS); Policy control over Gq interface*.

[ETSI TS 129 229] ETSI TS 129 229 V7.8.0 (2008), *Cx and Dx interfaces based on the Diameter protocol*; *Protocol details*.

[ETSI TS 129 329] ETSI TS 129 329 V6.7.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Sh interface based on the Diameter protocol*; *Protocol details*.

[ETSI TS 187 003] ETSI TS 187 003 V1.7.1 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture*.

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

[ETSI ES 283 035] ETSI ES 283 035 V2.5.1 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the Diameter protocol*.

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

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

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

[IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

3 Definitions

This Recommendation defines the following terms:

3.1 attribute-value pair (AVP): An attribute-value pair corresponds to an information element in a Diameter message. Source of definition is [IETF RFC 3588].

3.2 mobility: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment. Source of definition is [b-ITU-T Y.2001].

NOTE 1 – The degree of service availability may depend on several factors including the access network capabilities, service level agreements between the user's home network and the visited network (if applicable), etc. Mobility includes the ability of telecommunication with or without service continuity [b-ITU-T Y.2001].

NOTE 2 – In [b-ITU-T Y.2001] this is called generalized mobility.

3.3 nomadism: The ability of the user to change their network access point. When changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no service continuity or hand-over used. Source of definition is [b-ITU-T Q.1706].

NOTE – It is assumed that normal usage pattern is that users shut down their service session before attaching to a different access point.

3.4 roaming: This is the ability of users to access services according to their user profile while outside of their subscribed home network, i.e., by using an access point of a visited network. This requires the capability for access to the visited network, the existence of an interface between home network and visited network, as well as a roaming agreement between the respective network operators. Source of definition is [b-ITU-T Q.1706].

3.5 service control entity (SCE): Element of the service layer architecture offering applications that require information about the characteristics of the IP-connectivity session used to access such applications.

3.6 single sign-on: The ability to use an authentication assertion from one network operator/service provider to another operator/provider for a user either accessing a service or roaming into a visited network. Source of definition is [b-ITU-T Y.2201].

3.7 subscriber: The person or organization responsible for concluding contracts for the services subscribed to and for paying for these services. Source of definition is [b-ITU-T M.3050.1].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABNF Augmented Backus-Naur Form

AM-PE Access Management Physical Entity

AVP Attribute-Value Pair

CPE Customer Premises Equipment

IMPI IMS Private User Identity

IMPU IMS Public User Identity

IMS IP Multimedia Subsystem

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

RACE Resource and Admission Control Entity

RACF Resource and Admission Control Functions

SCE Service Control Entity

SCF Service Control Functions

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

5 S-TC1 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 made accessible to other control functions and applications through two interfaces (see Figure 5-1):

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

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

This Recommendation specifies the protocol for the S-TC1 interface.

In this Recommendation, a service control entity (SCE) is defined as a generic term representing any element of the service layer architecture. It offers applications requiring information on the characteristics of the IP-connectivity session being used to access the applications. One example of a service control entity is the P-CSC-PE in the service control functions.

5.2 S-TC1 reference model

The S-TC1 interface, as shown in Figure 5-1, is defined between the SCE and the TLM-PE.

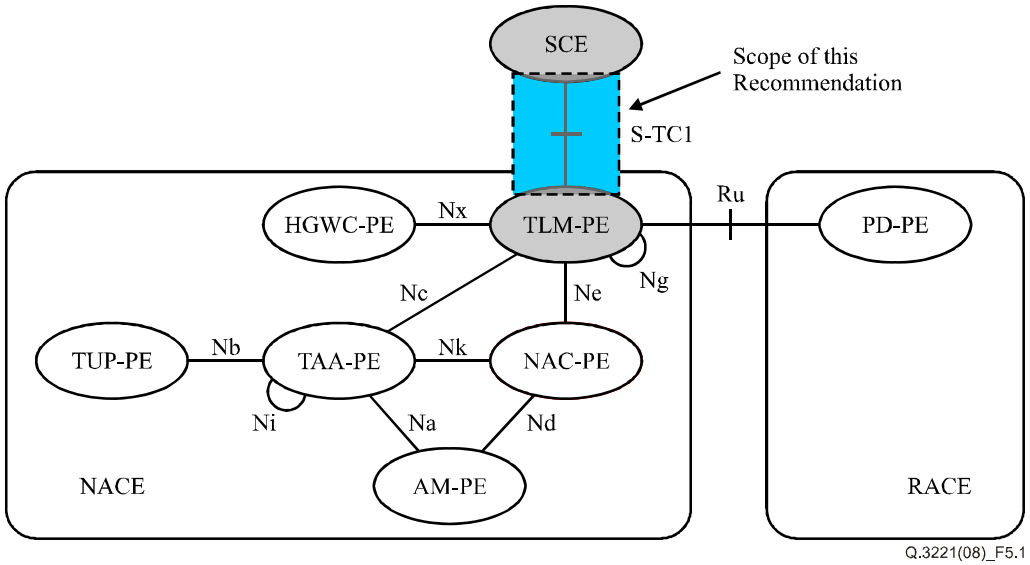

Figure 5-1 – S-TC1 reference model

5.3 Physical entities and capabilities

5.3.1 Transport location management physical entity (TLM-PE)

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

The TLM-PE is able to correlate the information received from the NAC-PE and the TAA-PE based on the logical connection identifier.

The TLM-PE may also store the identity of the user/CPE to which the IP address has been allocated (information received from the TAA-PE) as well as the user network QoS profile and user preferences regarding the privacy of the location information. In case it does not store the identity/profile of the user/CPE, the TLM-PE shall be able to retrieve this information from the TAA-PE.

The TLM-PE registers the association between the IP address allocated to the CPE and related network location information provided by the NAC-PE (e.g., access line identifier). The TLM-PE interfaces with the NAC-PE to derive the association between the IP address allocated by the NAC-PE to the end user equipment and the identity of the logical access used by the attached user equipment (i.e., logical connection identifier).

The TLM-PE may provide the SCE with user network profile information through the TLM-PE of the visited network to support mobility when the user is nomadic.

Similarly, the TLM-PE is able to provide the SCE with user network profile information through the 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].

5.3.2 Service control entity (SCE)

In this Recommendation, the SCE is used as a generic term representing any element of the service layer architecture. SCE offers applications requiring information on the characteristics of the IP-connectivity session being used to access the applications. The SCE shall use the S-TC1 interface to get connection-related information with TLM-PE. One example of a SCE is the P-CSC-PE. The SCE requests for location information from TLM-PE, which in turn responds to location queries [ITU-T Y.2012]. The SCE needs network session information such as IP-connectivity status, access network type from TLM-PE and device information such as terminal type.

Moreover, the SCE needs to know the RACE contact point to get resources for a service. Specifically, the P-CSC-PE needs to know the address of the PD-PE to send a QoS request for a service. The PD-PE will check between the QoS request sent from the SCE and QoS profile stored in TUP-PE and determine whether the requested QoS is applicable to the service.

The SCE requests the user network QoS profile and user preferences regarding the privacy of location information.

In addition, the SCE requests location information to provide nomadism for mobility. In cases wherein the access network technologies are identical and are owned by the same access network operator, service continuity or handover may be supported.

Finally, the SCE requests location information for bundled authentication [ETSI TS 187 003].

6 Signalling requirements

This reference point enables applications and service control functions to retrieve network location information from the 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 TLM-PE depends on the requestor.

The following information flows are used on this interface:

– Information query request/response
– Event registration request/response
– Notification event request/response

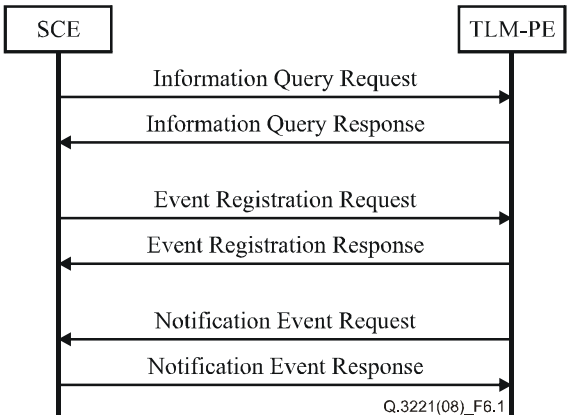

Figure 6-1 – Information flow

6.1 Information query

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

Table 6-1 – Information query request (SCE → TLM-PE)

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
SCE identity	The identifier of the requesting service control entity.

The information query response information flow contains the following information (see Table 6-2)

Table 6-2 – Information query response (TLM-PE → SCE)

Transport subscriber identifier (optional)	A globally unique identifier for the attached CPE. (Note 1).
Location information (optional) (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 CPE is attached.
IP connectivity status (optional)	Whether IP connectivity to/from the user equipment is currently available.
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.	

6.2 Event registration

The event registration request information flow contains the following information (see Table 6-3)

Table 6-3 – Event registration request (SCE → TLM-PE)

Subscription duration	Duration for which the subscription for a particular event will be active.
Transport subscriber identifier (optional)	A globally unique identifier of the attached CPE.
Event	Event-Type (e.g., user logon event) and format for event relay/notification description.
Globally unique IP address information (optional)	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).
SCE identity (optional)	The identity of the requesting service control entity.

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

Table 6-4 – Event registration response (TLM-PE → SCE)

Update action	Administrative action/information for an event: e.g., ACTIVATED (event registration successfully received and event notification for "Event" activated).
Transport subscriber identifier	A globally unique identifier for the attached CPE.
Event	Event-Type (e.g., user logon event)
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).

6.3 Notification event

The notification event request information flow contains the following information (see Table 6-5).

Table 6-5 – Notification event request (TLM-PE → SCE)

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.
Event	Event-Type (e.g., user logon event)

The notification event response information flow contains the following information (see Table 6-6).

Table 6-6 – Notification event response (SCE → TLM-PE)

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.
Event	Event-Type
Result	Result code (e.g., success, permanent failure, etc.)

7 Description of procedures

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 the 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 TLM-PE – SCE interface

7.2.1 Information query

7.2.1.1 Overview

This procedure is used by a SCE to retrieve from the 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 7-1 and 7-2 detail the involved information elements as defined in the NACE and their mapping to Diameter AVPs.

Table 7-1 – Information query request

Information element name	Mapping to Diameter AVP	Cat.	Description
Unique IP address	Globally-unique-address	C	This information element contains: – The IP address of the user equipment used by the subscriber for which profile information is being pushed. – The addressing domain in which the IP address is significant.
Address realm			
Transport subscriber identifier	User-Name	C	The user that is attached to the network.
SCE identity	SCE-Application-Identifier	M	Identifies the SCE originating the request.
Requested items	Requested-Information	O	The list of items requested by the SCE.

Table 7-2 – Information query response

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code/ Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for other errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Transport subscriber identifier	User-Name	O	The user that is attached to the network.
Location information	Location-Information	O	Location information (or a pointer to such information) in a form that is suitable for the requesting application.
RACE contact point	RACE-Contact-Point	O	The FQDN or IP address of the RACE where resource request shall be sent (i.e., PD-PE address).
Access transport network type	Access-Network-Type	O	The type of access network over which IP connectivity is provided to the user equipment.
CPE type	CPE-Type	O	The type of user equipment to which the IP address was allocated.
IP connectivity status	IP-connectivity-status	O	The status of IP connectivity to/from the user equipment.
Physical connection identifier	Physical-Connection-Identifier	O	A local identifier for physical connection of access transport network to which 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	Logical-Connection-Identifier	O	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 attached CPE.

7.2.1.2 Procedure at the SCE side

The SCE 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. The Address-Realm AVP shall be obtained from predefined configuration data in SCE. In case of configuration data, all terminal equipments served by a SCE have the same addressing domain.

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

3) The Requested-Information AVP shall be present if specific information is requested and shall be absent if all available information is requested.

The requested information AVP may be absent or present, depending on requests. In Annex A, there are some examples of scenarios which show the requested information AVP is used in S-TC1.

Case 1) shows NACE-SCE bundled authentication scenario in fixed access network. In bundled authentication, the network authentication implies service authentication. After successful NACE authentication, access line information is stored to TUP-PE. This line information is compared with that of SUP-PE in service authentication. In bundled authentication environment, P-CSC-PE shall send information request to TLM-PE to request line information by using IP address as a key of Requested-Information AVP. TLM-PE will fetch line information corresponding to the IP address and send the line information as location information response.

Case 2) shows NACE-SCE bundled authentication scenario in both fixed and mobile access network. SCE will request authentication data as a Requested-Information AVP. The Requested-Information AVP will be authentication data bound to IP address. Because access point information varies in mobile access network, bundled authentication shall be completed by checking authentication data between TUP-PE and SUP-PE.

Case 3) shows the case in which SCE requests address of PD-PE for QoS service. SCE needs QoS policy to provide QoS-based service and TLM-PE keeps the contact point of policy server that is PD-PE. P-CSC-PE sends information query to TLM-PE to request the address of PD-PE in Requested-Information AVP. TLM-PE will send back to P-CSC-PE with the address of PD-PE as information response.

Case 4) shows a scenario of location-based service. When a user is looking for a hospital, location-based service will recommend a closest hospital geographically. To recognize the user's location, the service will make use of the user's authentication data, IP address and line information.

7.2.1.3 Procedure at the TLM-PE side

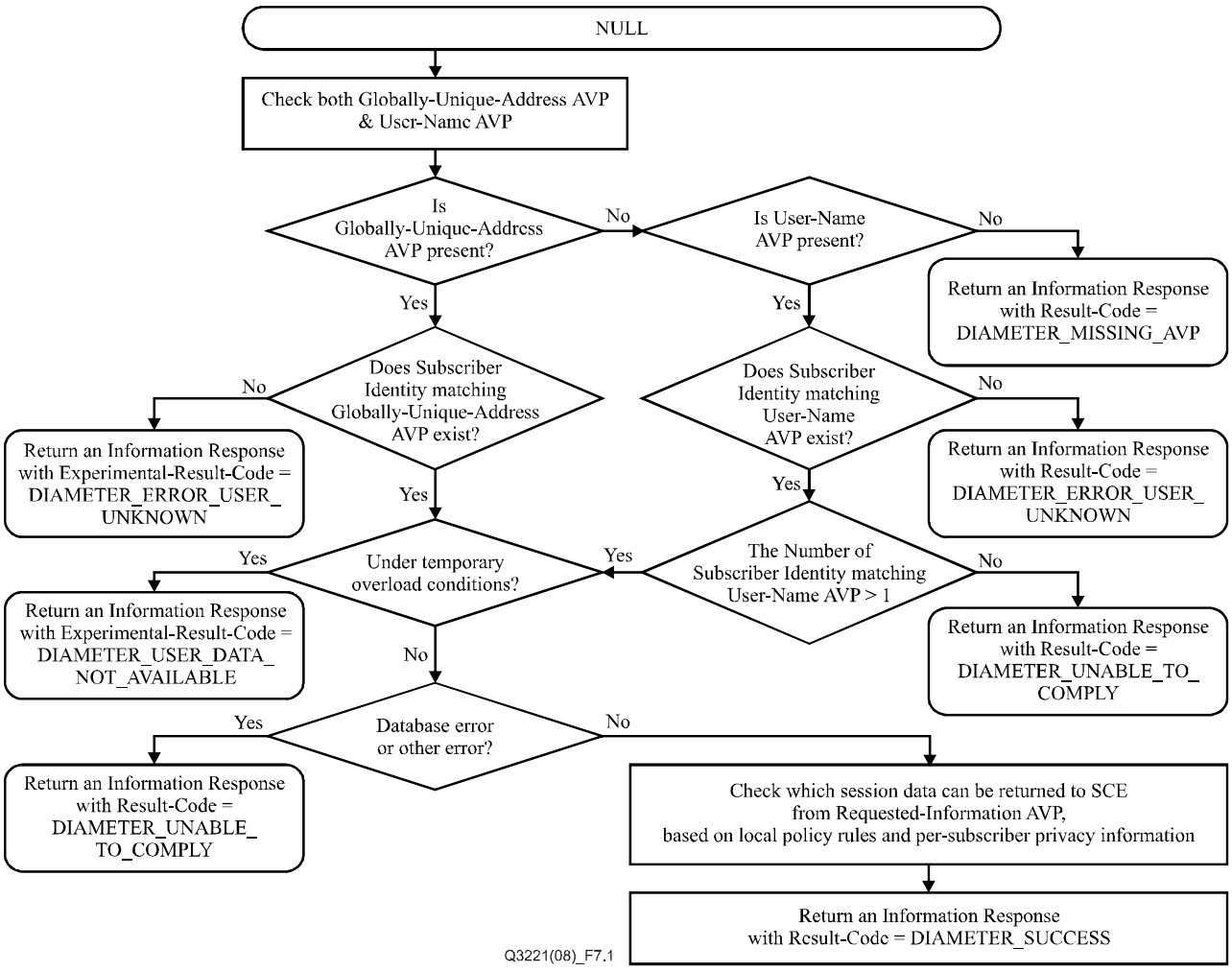

Figure 7-1 – Procedure side for location query on the TLM-PE side

1) First, check both Globally-Unique-Address AVP and 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 Result-Code set to DIAMETER_MISSING_AVP and stop this procedure.
5) If more than one record include 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 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 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. The SCE may retry retrieving the required information at a later stage. Otherwise, go to the next step.

8) 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 the Result-Code to DIAMETER_UNABLE_TO_COMPLY.

9) Check which session data can be returned to the SCE, based on local policy rules and per-subscriber privacy information stored in the TLM-PE. If the session data to be retrieved is currently being updated by another entity, the 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 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.

7.2.2 Event registration

7.2.2.1 Overview

This procedure is used by an SCE to subscribe with the TLM-PE to a particular event. This procedure is mapped to the commands Subscribe-Notifications-Request/Answer defined in the Diameter application specified in Sh interface [ETSI TS 129 329]. Tables 7-3 and 7-4 detail the involved information elements as identified in the NACE and their mapping to Diameter AVPs.

Table 7-3 – Event registration request

Information element name	Mapping to Diameter AVP	Cat.	Description
	Subs-Req-Type	M	Indicates whether the SCE is willing to subscribe or unsubscribe to the notification of the event.
Unique IP address	Globally-unique-Address	C	This information element contains: – The IP address of the user equipment used by the subscriber for which profile information is being pushed. – The addressing domain in which the IP address is significant.
Address realm			
Transport subscriber identifier	User-Name	C	The user that is attached to the network.
Subscription duration	Expiry-Time	O	Duration for which the subscription to the event will be active.
Event	Event-Type	M	The type of event to be monitored.
SCE identity	SCE-Application-Identifier	M	Identifies the SCE originating the request.

Table 7-4 – Event registration response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code/ Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for other errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
	Expiry-Time	O	Acknowledges the absolute time at which the subscription expires.

The TLM-PE monitors events related to access sessions. Monitoring of a particular event on a particular session is activated when at least one application function has subscribed to be notified of the occurrence of the event. Subscription to an event may be done implicitly (i.e., through management operations) or explicitly using the event registration/deregistration request. Subscription to an event ceases when one of the following conditions is met:

– Expiry of the subscription duration.

– Removal of the session record from the TLM-PE.

– Receipt of an explicit request to unsubscribe.

7.2.2.2 Procedure at the SCE side

The SCE shall populate the event registration request as follows:

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

2) Insert either a Globally-Unique-Address or a User-Name AVP. The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP. The Address-Realm AVP shall be included and set either using configuration data (in which case all user equipment served by the SCE is assumed to belong to the same addressing domain) or from the physical or logical interface over which was received a related service request.

3) The SCE-Application-Identifier AVP shall be present.

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

5) The Expiry-Time AVP may be present.

7.2.2.3 Procedure at the TLM-PE side

Upon reception of an event registration/deregistration request, the TLM-PE shall, in the following order:

1) Based on the contents of the SCE-Application-Identifier AVP, check whether the SCE is allowed to request monitoring of events. If not, return an event registration response with Result-Code set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED.

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

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

4) If both the Globally-Unique-Address AVP and the User-Name AVP are absent, return an event registration/deregistration response with the Result-Code AVP set to DIAMETER_MISSING_AVP.

5) If no stored session record matches the Globally-Unique-Address AVP or the User-Name AVP and the requested event differs from USER-LOGON, return an event registration response with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN. If the Subs-Req-Type AVP indicates that this is a request to subscribe to the notification of events, the TLM-PE shall check whether the requested event can be reported to the SCE, based on local policy rules and per-subscriber privacy information received from the TAA-PE. If the SCE is not allowed to request monitoring of the event, return an event registration/deregistration response with Result-Code set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED. If the SCE is allowed to request monitoring of the event, the TLM-PE shall:

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

   – Include in the event registration response an Expiry-Time AVP with the absolute time at which the subscription expires in the case of a successful subscription. This time may be earlier than the requested expiry time. If the TLM-PE includes this AVP, then no notification shall be sent to the SCE after the expiration time. If the TLM-PE does not include this AVP, that indicates an unlimited subscription.

   – Set the Result-Code to DIAMETER_SUCCESS and return an event registration/deregistration response.

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

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

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 the Result-Code to DIAMETER_UNABLE_TO_COMPLY.

7.2.3 Notification event

7.2.3.1 Overview

This procedure is used by a TLM-PE to notify the SCE of the occurrence of a particular event.
This procedure is mapped to the commands Push-Notifications-Request/Answer in the Diameter application specified in Sh interface [ETSI TS 129 329]. Tables 7-5 and 7-6 detail the involved information elements as defined in the NACE and their mapping to Diameter AVPs.

Table 7-5 – Notification event request

Information element name	Mapping to Diameter AVP	Cat.	Description
Unique IP address	Globally-unique-Address	C	This information element contains: – The IP address of the user equipment used by the subscriber for which profile information is being pushed. – The addressing domain in which the IP address is significant.
Address realm			
Transport subscriber identifier	User-Name	C	The user that is attached to the network.
SCE identity	SCE-Application-Identifier	M	Identifies the SCE originating the request.
Event	Event-Type	M	The type of event to be monitored.
	[AVP]	O	AVPs carrying TLM-PE information associated to the reported event.

Table 7-6 – Notification event response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code/ Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for other errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

7.2.3.2 Procedure at the TLM-PE side

When a monitored event is detected on a particular access session, the TLM-PE issues an event notification request to each of the application functions having registered to this event.

The event notification request is populated as follows:

1) A least a Globally-Unique-Address or a User-Name AVP shall be included. The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP. The Address-Realm AVP shall be included and set either using configuration data (in which case all terminal equipment served by the SCE belongs to the same addressing domain) or from the physical or logical interface over which was received a related service request.
2) The SCE-Application-Identifier AVP shall be present.
3) One or more occurrence of the Event-Type AVP indicating the type of events being notified.

Based on local policy rules and per-subscriber privacy information previously received from the TAA-PE, the TLM-PE may also include additional information in the event registration/deregistration request. Table 7-7 provides an indication of the AVPs that may be returned for each event.

Table 7-7 – Request-Information to AVP mapping

Event	AVP
USER-LOGON	IP-Connectivity-Status
LOCATION-INFORMATION-CHANGED	Location-Information
RACE-CONTACT-POINT-CHANGED	RACE-Contact-Point
ACCESS-NETWORK-TYPE-CHANGED	Access-Network-Type
CPE-TYPE-CHANGED	CPE-Type
LOGICAL-CONNECTION-IDENTIFIER-CHANGED	Logical-Connection-Identifier
PHYSICAL-CONNECTION-IDENTIFIER-CHANGED	Physical-Connection-Identifier
DEFAULT-CONFIGURATION-CHANGED	Default-Configuration
TRANSPORT-RESOURCE-SUBSCRIPTION-CHANGED	Transport-Resource-Subscription
IP-ADDRESS-CHANGED	Globally-Unique-Address
USER-LOGOFF	IP-Connectivity-Status

7.2.3.3 Procedure at the SCE side

Upon reception of a notification event request, the SCE shall:

1) If neither the globally unique identifier contained in the Globally-Unique-Address AVP nor the subscriber identifier contained in the User-Name AVP are known, return a notification event response with a Result-Code AVP value set to DIAMETER_ERROR_USER_UNKNOWN.
2) If the event type contained in the Event-Type AVP is not known, return a notification event response with a Result-Code AVP value set to DIAMETER_INVALID_AVP_VALUE.
3) If the event type contained in the Event-Type AVP is known but was not expected, return a notification event response with a Result-Code AVP value set to DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA.

If the SCE cannot process the event for reasons not stated in the above steps, return a notification event response with a Result-Code AVP value set to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code AVP set to DIAMETER_SYSTEM_UNAVAILABLE. In the latter case, the TLM-PE is expected to retry after a provisioned time period. After a provisioned number of unsuccessful retries, the TLM-PE is expected to delete the SCE-Identity from the list of application functions registered to the event.

Otherwise, the event shall be processed and the SCE shall return the Result-Code AVP set to DIAMETER_SUCCESS in the notification event response.

8 Use of the Diameter base 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 [IETF RFC 3554].

8.2 Accounting functionality

Accounting functionality (accounting session state machine, related command codes and AVPs) is not used on the S-TC1 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.

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 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 S-TC1 interface shall make use of 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 defined over the S-TC1 interface, the TLM-PE acts as a Diameter server and the SCE acts as the Diameter client.

If a SCE knows the address/name of the TLM-PE for a certain user, both the Destination-Realm and Destination-Host AVPs shall be present in the request. Otherwise, only the Destination-Realm AVP shall be present and the command shall be routed to a proxy TLM-PE, based on the Diameter routing table in the client. The proxy TLM-PE shall act as a Diameter relay as described in [IETF RFC 3588].

Requests initiated by the TLM-PE towards a SCE shall include both Destination-Host and Destination-Realm AVPs. The TLM-PE obtains the Destination-Host AVP to use in requests towards a SCE from configuration data or information received from the TAA-PE/TUP-PE. 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.

To ensure that messages are routed to the correct application at the destination host, the Diameter message header of each message sent shall contain either the S-TC1 application identifier (16777245) or the e2 application identifier (16777231) as agreed during CER/CEA negotiation. (See clause 8.6)

8.6 Advertising application support

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

If both the SCE and TLM-PE indicate support of the S-TC1 application, then the S-TC1 application identifier (16777245) shall be used in the Diameter message header of all subsequent messages

exchanged within this association. Otherwise, the e2 application identifier (16777231) shall be placed in those headers.

Support of the S-TC1 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 S-TC1 (16777245). Support of the e2 application within the CER/CEA is indicated by supplying an instance of the Vendor-Specific-Application-Id containing a Vendor-Id AVP set to ETSI (13019) and an Auth-Application-Id AVP set to e2 (16777231).

The SCE and TLM-PE shall 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.

Table 8-1 – Vendor identifiers for S-TC1

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 3588].

9 Message specification

9.1 Commands

This Recommendation reuses the Diameter command defined in [ETSI TS 129 329]. Other commands shall be ignored by the SCE and TLM-PE.

Table 9-1 – Command code

Command	Abbreviation	Defining reference	Command code	See clause
User-Data-Request	UDR	ETSI TS 129 329	306	9.1.1
User-Data-Answer	UDA	ETSI TS 129 329	306	9.1.2
Subscribe-Notification-Request	SNR	ETSI TS 129 329	308	9.1.3
Subscriber-Notification-Answer	SNA	ETSI TS 129 329	308	9.1.4
Push-Notification-Request	PNR	ETSI TS 129 329	309	9.1.5
Push-Notification-Answer	PNA	ETSI TS 129 329	309	9.1.6

9.1.1 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, 16777245>
                          < Session-Id >
                          { Vendor-Specific-Application-Id }
                          { Auth-Session-State }
```

```
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                [ Globally-Unique-Address ]
                                [ User-Name ]
                                [ SCE-Application-Identifier ]
                                [ Requested-Information ]
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

9.1.2 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, 16777245>
                                < 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 ]
```

9.1.3 Subscribe-Notification-Request (SNR) command

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

Message format

```
< Subscribe-Notification-Request > ::= < Diameter Header: 308, REQ, PXY,
16777245>
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                { Subs-Req-Type }
                                [ Expiry-Time ]
```

```
                                [ Globally-Unique-Address ]
                                [ User-Name ]
                                [ SCE-Application-Identifier ]
                                *[ Event-Type ]
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

9.1.4 Subscribe-Notification-Answer (SNA) command

The Subscribe-Notification-Answer command, indicated by the Command-Code field set to 308 and the "R" bit cleared in the command flags field, is sent by a server in response to the Subscribe-Notification-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in clause 9.2.

Message format

```
< Subscribe-Notification-Answer > ::= < Diameter Header: 308, PXY, 16777245>
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Expiry-Time ]
                                *[ AVP ]
                                *[ Failed-AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

9.1.5 Push-Notification-Request (PNR) command

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

Message format

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777245>
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                *[ Event-Type ]
                                [ Globally-Unique-Address ]
                                [ User-Name ]
                                [ Access-Network-Type ]
                                [ Location-Information ]
                                [ RACE-Contact-Point ]
                                [ CPE-Type ]
                                [ Logical-connection-identifier ]
                                [ Physical-connection-identifier ]
                                [ Access-Network-Type ]
                                [ Default-Configuration ]
                                *[ Transport-Resource-Subscription ]
                                [ IP-Connectivity-Status]
                                *[ AVP ]
                                *[ Proxy-Info ]
```

```
                                *[ Route-Record ]
```

9.1.6 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 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, 16777245>
                               < Session-Id >
                               { Vendor-Specific-Application-Id }
                               [ Result-Code ]
                               [ Experimental-Result ]
                               { Auth-Session-State }
                               { Origin-Host }
                               { Origin-Realm }
                               *[ AVP ]
                               *[ Failed-AVP ]
                               *[ Proxy-Info ]
                               *[ Route-Record ]
```

9.2 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 subclauses below.

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

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

9.2.2 Experimental-Result-Code AVP values imported from ETSI TS 129 329

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

DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA (5107)

The SCE received a notification of changes of some information to which it is not subscribed.

9.3 AVPs

The following tables summarize the AVPs used in this Recommendation, beyond those defined in the Diameter base protocol [IETF RFC 3588].

Table 9-2 describes the Diameter AVPs that are used within this Recommendation that have been defined by [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 Table 9-2 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 TS 283 035].

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

				AVP flag rules (Note 1)				
Attribute name	**AVP code**	**Clause defined**	**Value type (Note 2)**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Location-Information	350	9.3.5	Grouped	V	M			Y
RACE-Contact-Point	351	9.3.6	DiameterIdentity	V	M			Y
CPE-Type	352	9.3.7	OctetString	V	M			Y
Requested-Information	353	9.3.3	Enumerated	V			M	Y
Event-Type	354	9.3.11	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

				AVP flag rules				
Attribute name	**AVP code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Globally-Unique-Address	300	9.3.1	Grouped	M, V				Y
Logical-Connection-Identifier	302	9.3.10	OctetString	V	M			Y
Access-Network-Type	306	9.3.4	Grouped	V	M			Y
Default-Configuration	303	9.3.14	Grouped	V	M			Y
Transport-Resource-Subscription	304	9.3.15	Grouped	V	M			Y
IP-Connectivity-Status	305	9.3.8	Enumerated	V	M			Y
Physical-Connection-Identifier	313	9.3.9	UTF8String	V	M			Y

Table 9-4 describes the Diameter AVPs defined by the Gq interface protocol [ETSI TS 129 209] 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 129 209]. The Vendor-Id header of all AVPs defined in Table 9-4 shall be set to ETSI (13019).

Table 9-4 – Diameter AVPs imported from ETSI TS 129 209

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				
				Must	May	Should not	Must not	May encrypt
SCE-Application-Identifier	504	9.3.2	OctetString	M, V				Y

Table 9-5 describes the Diameter AVPs defined by the Sh interface protocol [ETSI TS 129 329] 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 129 329]. The Vendor-Id header of all AVPs defined in Table 9-5 shall be set to ETSI (13019).

Table 9-5 – Diameter AVPs imported from ETSI TS 129 329

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				
				Must	May	Should not	Must not	May encrypt
Expiry-Time	709	9.3.13	Time	V			M	Y
Subs-Req-Type	705	9.3.12	Enumerated	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 SCE-Application-Identifier AVP

The SCE-Application-identifier AVP (AVP code 504 13019) is of type OctetString, and it contains information that identifies the particular service that the SCE service session belongs to.

9.3.3 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).

9.3.4 Access-Network-Type AVP

The Access-Network-Type AVP (AVP code 306 13019) is of type Grouped, and 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]
```

9.3.5 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]
```

9.3.6 RACE-Contact-Point AVP

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

9.3.7 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).

9.3.8 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).

9.3.9 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.

9.3.10 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 VC carrying the traffic.

9.3.11 Event-Type AVP

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

- USER-LOGON (0).
- LOCATION-INFORMATION-CHANGED (1)
- RACE-CONTACT-POINT-CHANGED (2)
- ACCESS-NETWORK-TYPE-CHANGED (3)
- CPE-TYPE-CHANGED (4)

- LOGICAL-CONNECTION-IDENTIFIER-CHANGED (5)
- PHYSICAL-CONNECTION-IDENTIFIER-CHANGED (6)
- IP-ADDRESS-CHANGED (7)
- DEFAULT-CONFIGURATION-CHANGED (8)
- TRANSPORT-RESOURCE-SUBSCRIPTION-CHANGED (9)
- USER-LOGOFF (10)

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

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

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

9.3.12 Subs-Req-Type AVP

The Subs-Req-Type AVP (AVP code 705 13019) is of type Enumerated, and indicates the type of the subscription-to-notifications request. The following values are defined:

- SUBSCRIBE (0): This value is used by an SCE to subscribe to notifications of changes in data.
- UNSUBSCRIBE (1): This value is used by an SCE to unsubscribe to notifications of changes in data.

9.3.13 Expiry-Time AVP

The Expiry-Time AVP (AVP code 709 13019) is of type Time. This AVP contains the expiry time of subscriptions to notifications in the TLM-PE.

9.3.14 Default-Configuration AVP

The Default-Configuration AVP (AVP code 303 13019) is of type Grouped.

AVP format

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

9.3.15 Transport-Resource-Subscription AVP

The Transport-Resource-Subscription AVP (AVP code 304 13019) represents Transport-Resource-Subscription element and is of type Grouped.

AVP format

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

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 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. 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 IETF, including those requested by 3GPP.

9.4.4 Application-ID value

This Recommendation defines the S-TC1 Diameter application with application ID 16777245. 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 S-TC1 interface shall follow the security requirements of the NACF.

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 [IETF RFC 3554].

Further considerations along this line are provided in the security considerations section of [IETF RFC 3588], which operators are advised to consult.

Annex A

Scenarios using S-TC1

(This annex forms an integral part of this Recommendation)

A.1 CASE 1: NACE-SCE bundled authentication based on line information

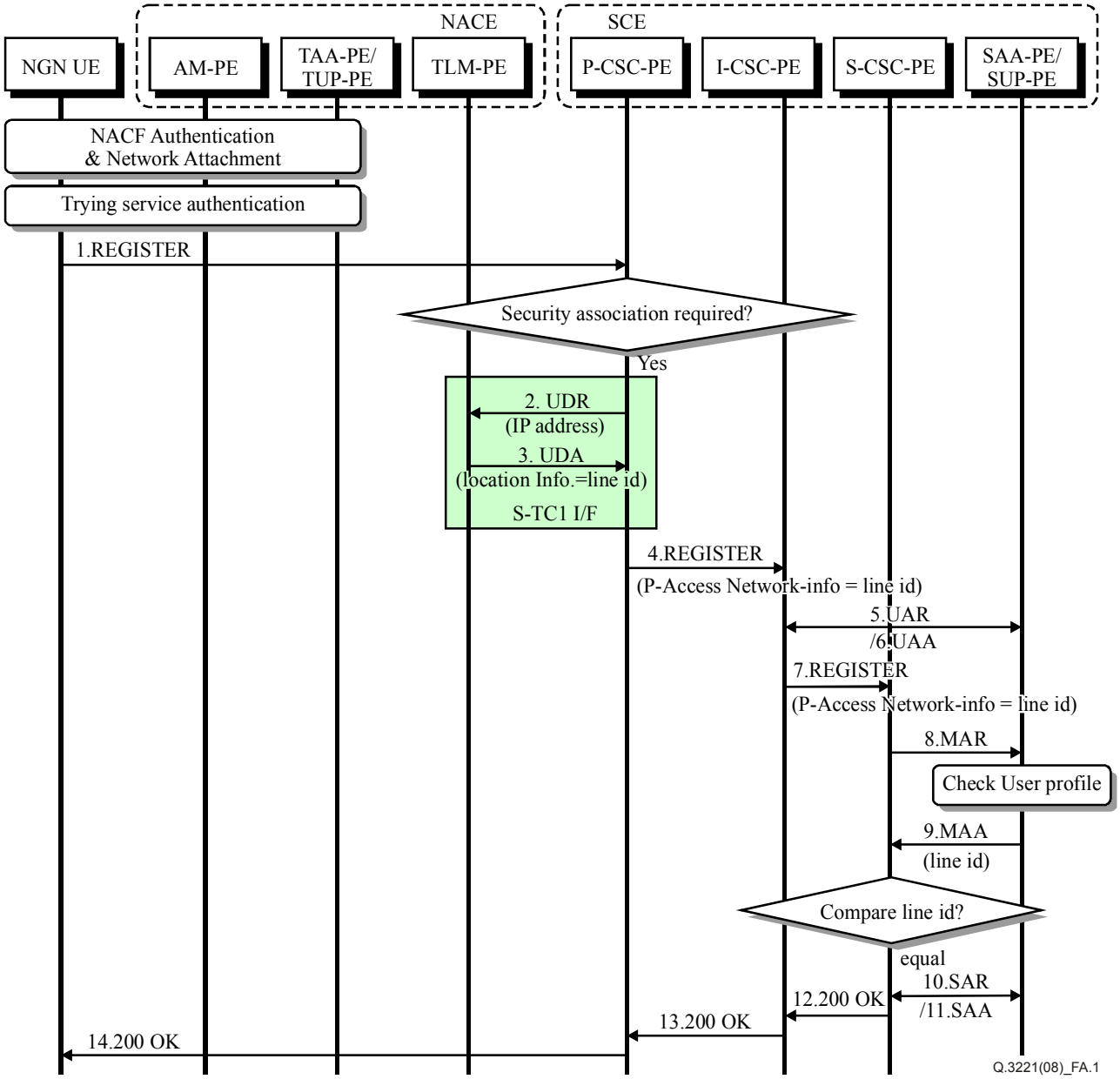

Figure A.1 – NACE-SCE bundled authentication for the fixed access network only

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) 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 TLM-PE over the S-TC1 interface. The key for the query is the IP address used by the UE.

3) The TLM-PE sends the UDA response to the P-CSC-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.

A.2 CASE 2: NACE-SCE bundled authentication based on the authentication context

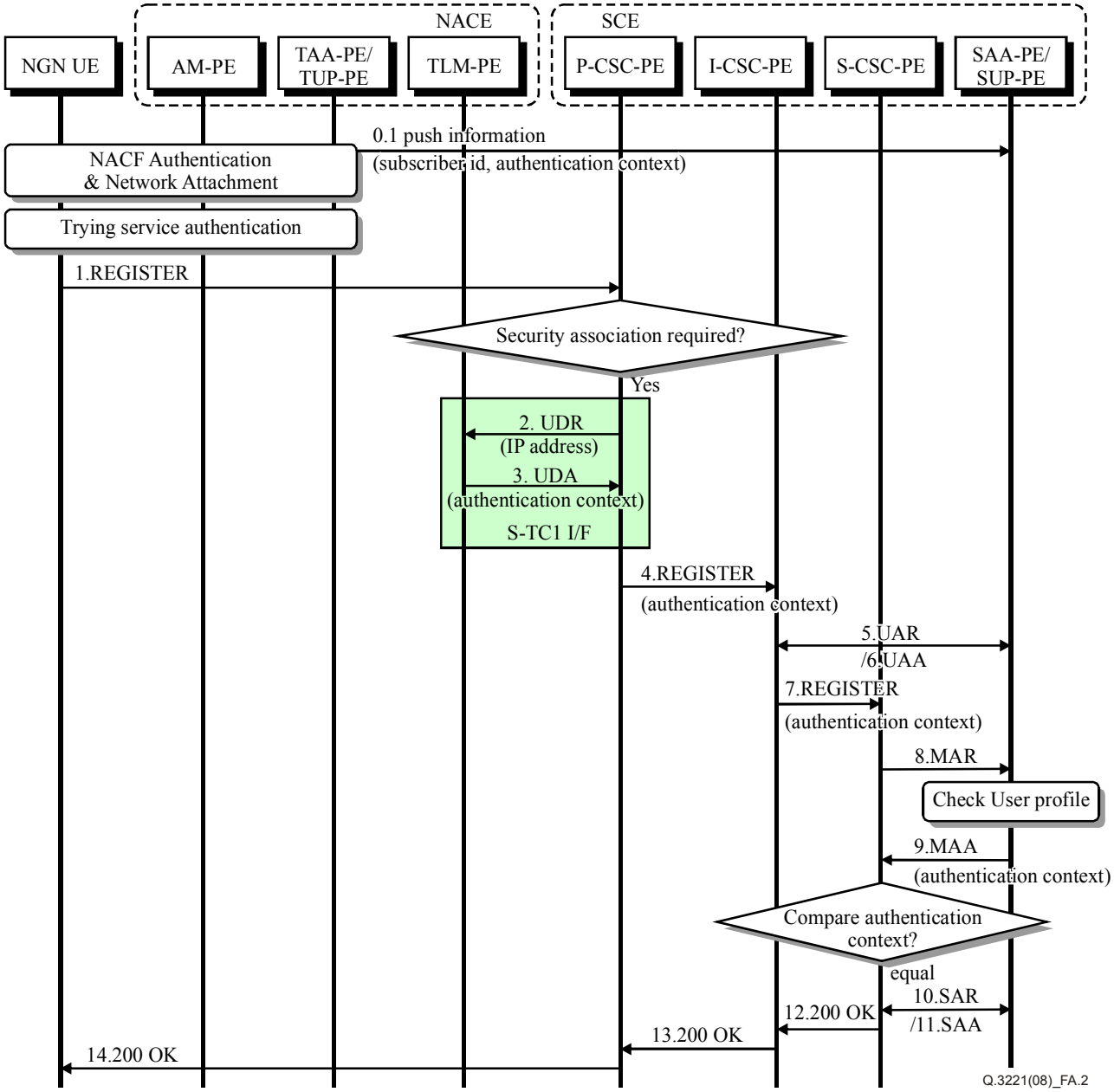

Figure A.2 – NACE-SCE bundled authentication for both fixed and mobile access network

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

Here, the NACE-SCE bundle authentication scenario example applicable, including the mobile access network, will be considered unlike the scenario of clause A.1.

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

0) The UE gets network attachment after the 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 the SCE-user basis. The relationship between subscriber identity and SCE-user identities (IMPI and IMPU) is already known to the SUP-PE.

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

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. The P-CSC-PE performs the UDR request toward the TLM-PE over the S-TC1 interface. The key for the query is the IP address used by the UE.

3) The TLM-PE sends the UDA response to the P-CSC-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 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 SAR message, and SIP 200 OK message is sent to the UE.

A.3 CASE 3: Information of PD-PE in RACE for providing QoS

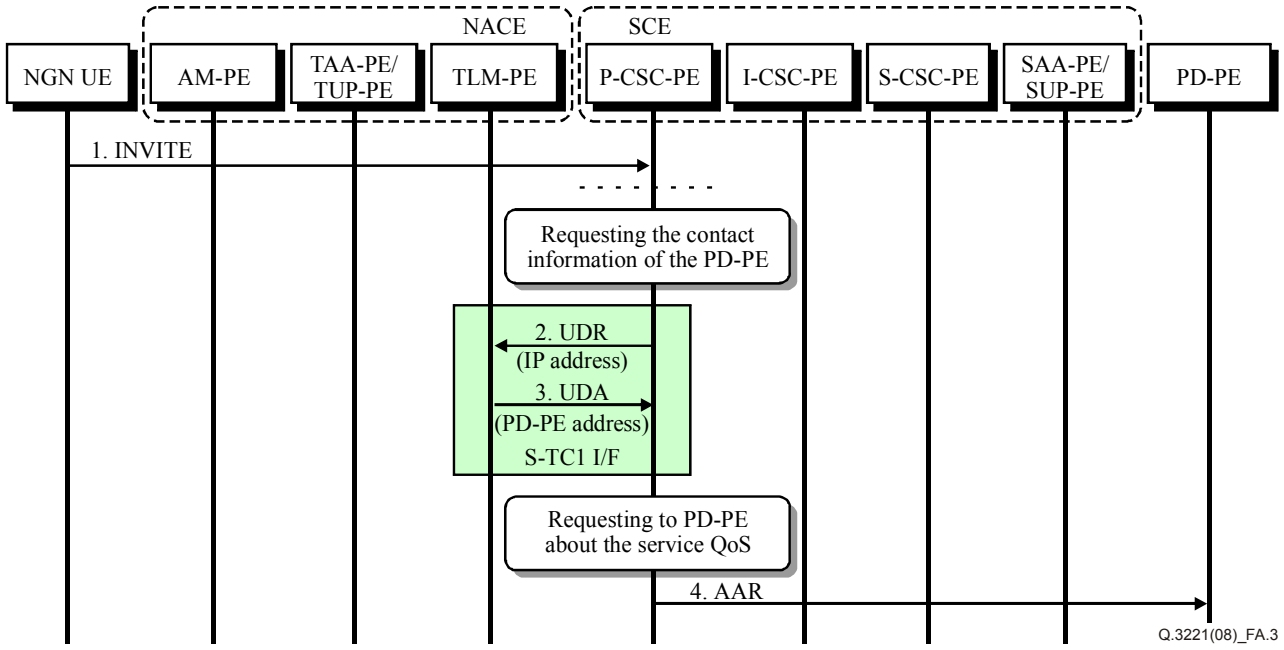

Figure A.3 – Information of PD-PE in RACE for providing QoS

P-CSC-PE has to connect to PD-PE with Diameter for the service QoS request. Therefore, it is necessary to have the contact information of PD-PE. That information can be set up in advance or be inquired from NACE. Here, it is the scenario about the latter method. The latter method has the advantage that when P-CSC-PE is connected to several PD-PEs, PD-PE can be selected dynamically. We assume both that the attachment and authentication about the access network succeeds, and that the SIP register procedure about the service network was completed.

1) The UE or CPE delivers the SIP INVITE message to P-CSC-PE through each attachment device.

2~3) P-CSC-PE requests the contact information of the PD-PE allocated to a user from NACE and is responded.

4) P-CSC-PE requests AAR to PD-PE about the service QoS using the contact information of the PD-PE allotted to a user.

A.4 CASE 4: Location service based on fixed access line information with bundled authentication

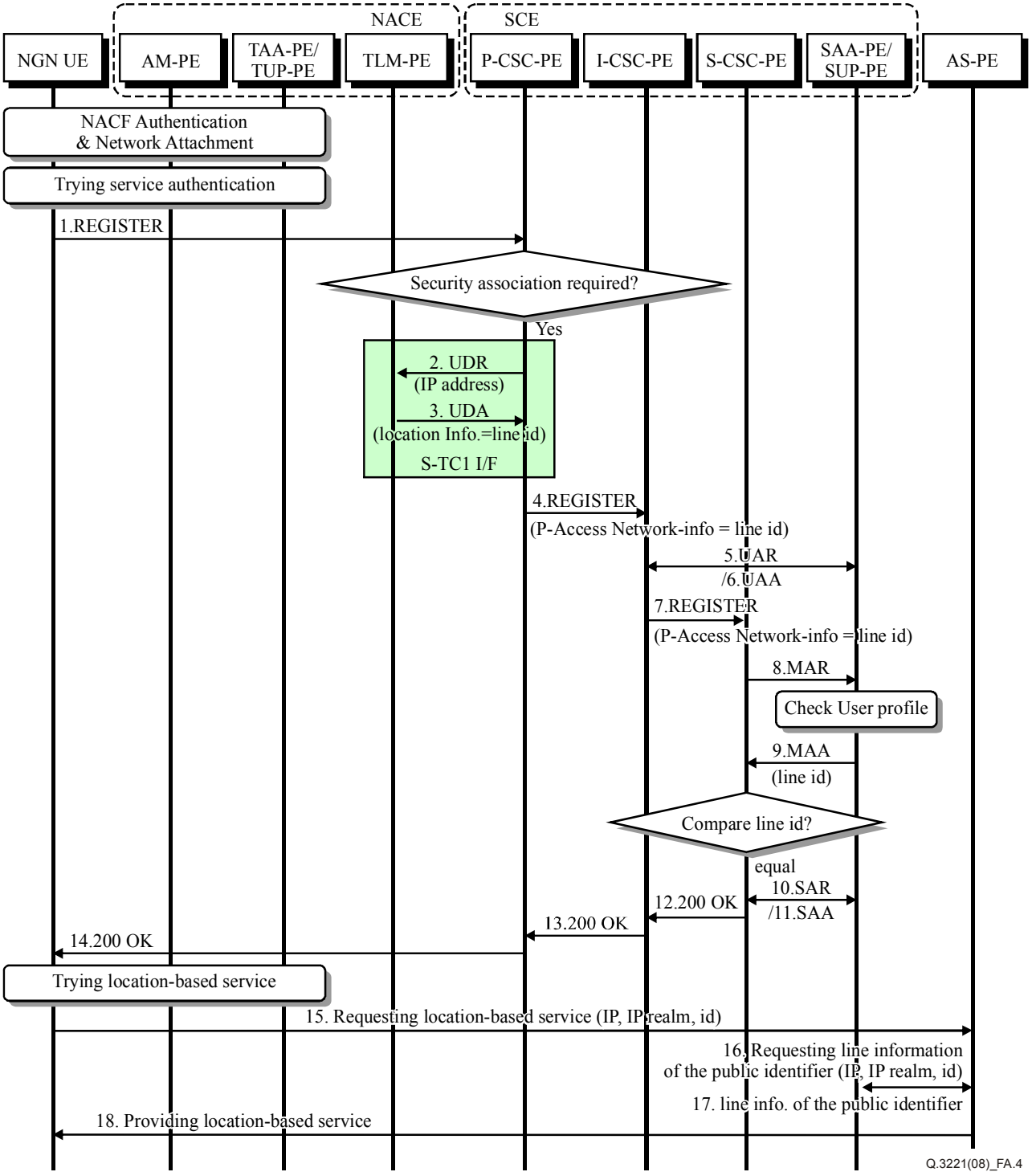

Figure A.4 – Location-based service by using fixed access line information

A location-based service provides a user with a preferable service by gathering and analysing a user's location information. For example, a general advertisement service of Internet portal does not consider a user's geographical location, so some restaurant advertisements are useless to users who live far from the restaurant. Location information may be a line identifier in the fixed access network, an access pointer in the mobile network, and a geographical location in the GPS environment.

This clause describes how a location-based service provider (e.g., restaurant advertisement provider) can provide a service to UEs without explicit service authentication (by making use of bundled authentication).

0) The UE gets network attachment after 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), which the user holds 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 a SCE-user basis.

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

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 a location information query toward the TLM-PE over the S-TC1 interface. The key for the query is the IP address used by the UE.

3) The TLM-PE sends the response to the P-CSC-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) The SUP-PE returns a message with the location information of the user identified by the IMPI and IMPU, if line based NACE bundling is the preferred authentication scheme.

   The S-CSC-PE finally authenticates by comparing the location information embedded in the REGISTER message with 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 its own IP address to the SUP-PE using SAR message and SIP 200 OK message is sent to the UE.

15) A user selects location-based advertisement service through a UE, and the UE sends to AS-PE the IP address, the IP realm and a public identifier which were stored in the UE.

16) AS-PE sends IP address, IP realm and a public identifier to SAA-PE/SUP-PE to get the line information.

17) SAA-PE/SUP-PE sends the line information (such as assigned line identifier) to AS-PE.

18) AS-PE receives the user's line information and applies it to the location-based service.

19) AS-PE gives user a preferable advertisement service by making use of the user's line information.

Bibliography

[b-ITU-T M.3050.1] Recommendation ITU-T M.3050.1 (2007), *Enhanced Telecom Operations Map (eTOM) – The business process framework*.

[b-ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

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	Telephone transmission quality, telephone installations, local line networks
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, 2009