International Telecommunication Union

ITU-T Q.3228

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(08/2016)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

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

Signalling requirements and protocol at the M1 interface between the transport location management physical entity and the mobile location management physical entity (P)

Recommendation ITU-T Q.3228

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

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.3709
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.3616
Service and session control protocols – supplementary services based on SIP-IMS	Q.3617–Q.3639
NGN applications	Q.3700–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099

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

Recommendation ITU-T Q.3228

Signalling requirements and protocol at the M1 interface between the transport location management physical entity and the mobile location management physical entity (P)

Summary

Recommendation ITU-T Q.3228 provides the protocol for the interface between the TLM-PE of the NACE and the MLM-PE (P) of the MMCE. M1 interface allows distribution of information from the TLM-PE to the MLM-PE (P). This Recommendation supports information flows across the M1 reference point as specified in Recommendation ITU-T Y.2018.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3228	2016-08-29	11	11.1002/1000/12984

Keywords

Mobile location management physical entity, MLM-PE(P), M1 interface, TLM-PE, transport location management physical entity

---

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Q.3228

Signalling requirements and protocol at the M1 interface between the transport location management physical entity and the mobile location management physical entity (P)

1 Scope

This Recommendation specifies the protocol for the M1 interface [ITU-T Y.2014] between the TLM-PE and the MLM-PE (P). The M1 reference point supports delivery of the information, including mobility service.

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 Q.3230] Recommendation ITU-T Q.3230 (2012), *Signalling requirements and protocol at the M13 interface between the transport location management and network information distribution physical entities.*

[ITU-T Q.3232] Recommendation ITU-T Q.3232 (2014), *Signalling requirements and protocol at the Nc interface between the transport location management physical entity and the transport authentication and authorization physical entity.*

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

[ITU-T Y.2018] Recommendation ITU-T Y.2018 (2009), *Mobility management and control framework and architecture within the NGN transport stratum.*

[ETSI TS 129 229] ETSI TS 129 229 V13.0.0 (2016), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (3GPP TS 29.229 version 13.0.0 Release 13).*

[ETSI TS 129 329] ETSI TS 129 329 V12.6.0 (2016), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329 version 12.6.0 Release 12).*

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

[ETSI ES 283 035] ETSI ES 283 035 V3.1.1 (2015), *Network Technologies (NTECH); Network Attachment; e2 interface based on the DIAMETER protocol.*

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 security association [b-IETF RFC 2401]: A simplex "connection" that affords security services to the traffic carried by it.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3GPP 3rd Generation Partnership Project

AAA Authentication, Authorization and Accounting

AM-PE Access Management Physical Entity

ABNF Augmented Backus-Naur Form

AVP Attribute-Value Pair

CPE Customer Premises Equipment

HDC-PE Handover Decision and Control Physical Entity

IP Internet Protocol

IPsec IP security protocol

MLM-PE Mobile Location Management Physical Entity

MMCE Mobility Management and Control Entity

MMCF Mobility Management and Control Function

NACE Network Attachment Control Entity

NACF Network Attachment Control Function

NAC-PE Network Access Configuration Physical Entity

NGN Next Generation Network

SCTP Stream Control Transmission Protocol

TAA-PE Transport Authentication and Authorization Physical Entity

TLM-PE Transport Location Management Physical Entity

TUP-PE Transport User Profile Physical Entity

UE User Equipment

5 Conventions

None.

6 M1 interface

6.1 Overview

This information flow is used to distribute several types of information from the TLM-PE to the MLM-PE(P) defined in the stage 2 specification [ITU-T Y.2014] and [ITU-T Y.2018]. The M1 interface allows the exchange of information about mobility service parameters.

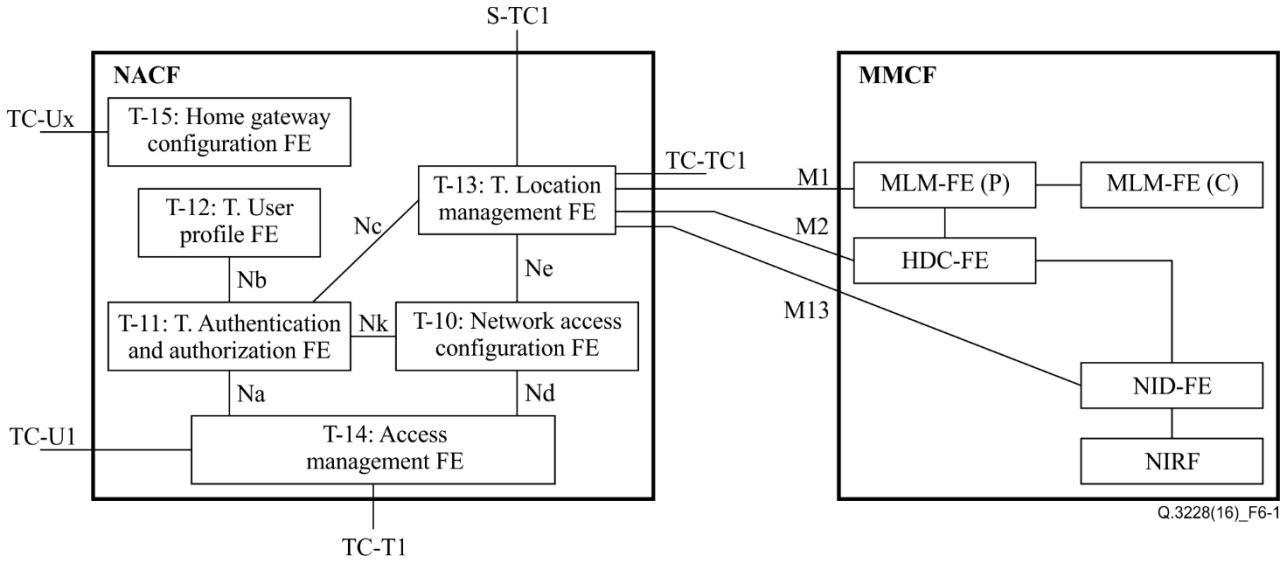

Figure 6-1 – Reference points between the NACF and the MMCF [ITU-T Y.2018]

6.2 Physical entities

6.2.1 Transport location management physical entity (TLM-PE)

The TLM-PE is assumed to be able to contact the NAC-PE via an internal reference point to obtain the persistent and temporary IP addresses.

In the host-based mobility case, the information passed from the TLM-PE includes the keying material derived from the UE authentication procedure to support the security association between the MLM-PE(P) and the UE. Also, it may include mobility service user ID, persistent IP address of the user, and binding between mobile user ID and persistent IP address. In the case of network-based mobility, the transferred information includes the identifier or persistent address, the address of the MLM-PE(C) instance for this connection, and may include the lower tunnel end point address and other parameters relating to mobility service.

6.2.2 Mobility location management physical entity (MLM-PE)

When the TLM-PE indicates network-based mobility service to the MLM-PE(P), this indication will trigger the mobile location registration procedure, and indirectly trigger handover.

7 Signalling requirements

Reference point M1 allows the TLM-PE to interact with the MLM-PE(P) for pushing mobility service parameters, such as keying material and anchor address. The TLM-PE holds keying material, anchor address, etc. in the mobility service parameters information shown in Table 7-1 and pushes keying material to MLM-PE(P).

The M1 reference point should allow information exchange as follows:

– information about mobility service parameters is pushed by the TLM-PE to MLM-PE(P).

Table 7-1 – Information about mobility service parameters in TLM-PE

Parameter	Description	Received from
Address of MLM-PE(C)	The address of the instance of the MLM-PE containing the mobile address binding information.	NAC-PE
Address of MLM-PE(P)	The address of the MLM-PE instance which sends the location registration.	
Keying Material	The material used for the security association between the UE and MMCE.	TAA-PE
Mobility Protocol Type	The type of mobility protocol, such as host-based or network-based mobility.	
Anchor point address	The upper tunnel end point address, from the point of view of the UE.	
Tunnel end point address	The tunnelling end point address for the network node which works as UE's proxy (lower tunnel end point).	

The following information flows shall be used on the M1 interface:

– Indication of host-based mobility;

– Indication of network-based mobility.

Figure 7-1 shows the information flows between the TLM-PE and the MLM-PE(P) through the M1 interface.

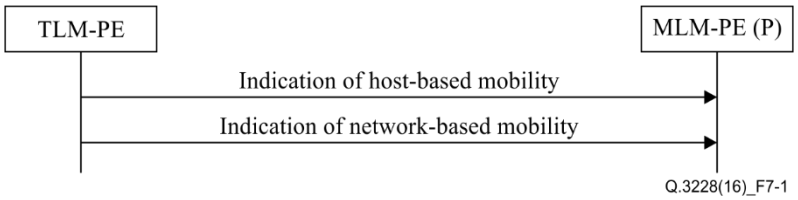

Figure 7-1 – Information flow

7.1 Indication of host-based mobility

In the host-based mobility case, the transferred information includes the keying material derived from the UE authentication procedure, in support of the security association required between the MLM-PE(P) and the UE. The information passed from the TLM-PE to the MLM-PE(P) may also include:

– mobility service user ID;

– persistent IP address of the user;

– binding between mobile user ID and persistent IP address.

The TAA-PE obtains these mobility service parameters from an AAA entity in the mobile subscriber's home network. How the TAA-PE determines that mobility service is to be provided and that mobility service parameters are required is out of the scope of this Recommendation.

The contents of the "indication of host-based mobility" primitive described in [ITU-T Y.2018] are shown in Table 7-2.

Table 7-2 – Indication of host-based mobility (TLM-PE → MLM-PE(P))

Information element	Explanation
Transport subscriber identifier (optional) (Note)	The user/UE identifier authenticated for attachment.
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Persistent IP address information (optional) (Note)	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Keying material	The material used for the security association between the UE and MLM-PE(P).
RACE contact point (optional)	The FQDN or IP address of the RACE entity where the resource requests are required to be sent (i.e., PD-PE address).
Anchor point address (optional)	The upper tunnel end point address, from the point of view of the UE.
NOTE – Either the UE identifier or the persistent IP address must be present.	

7.2 Indication of network-based mobility

The transferred information in the case of network-based mobility includes the identifier or persistent address, the address of the MLM-PE(C) instance for this connection, and may include the lower tunnel end point address and other parameters relating to mobility service. The "indication of network-based mobility" primitive described in [ITU-T Y.2018] is shown in Table 7-3.

When the TLM-PE indicates network-based mobility service to the MLM-PE(P), this indication will trigger the mobile location registration procedure, and indirectly trigger handover.

Table 7-3 – Indication of network-based mobility (TLM-PE → MLM-PE(P))

Information element	Explanation
Transport subscriber identifier (optional) (Note 1)	The user/UE identifier authenticated for attachment.
Mobility service subscriber identifier	The user/UE identifier authenticated for mobility services. This will be the same as the transport subscriber identifier in the integrated scenario.
Persistent IP address information (optional) (Note 1)	A set of IP address information used for locating the mobile UE.
– Unique IP address	The persistent IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Address of MLM-PE(C)	The address of the instance of the MLM-PE containing the mobile address binding information.
Tunnel end-point address (optional) (Note 2)	The tunnelling end point address for the network node which works as UE's proxy (lower tunnel end point).
RACE contact point (optional)	The FQDN or IP address of the RACE entity where resource requests shall be sent (i.e., PD-FE address).

Table 7-3 – Indication of network-based mobility (TLM-PE → MLM-PE(P))

Information element	Explanation
Anchor point address (optional)	The upper tunnel end point address, from the point of view of the UE.
NOTE 1 – Either the UE identifier or the persistent IP address must be present. NOTE 2 – If the tunnel end-point address is statically provisioned or the MLM-PE can obtain it with its own mechanisms, this information is not required.	

8 Description of procedures

8.1 General

The following clauses describe the realization of the functional procedures defined in the NACE [ITU-T Y.2014] and MMCE specifications [ITU-T Y.2018] using Diameter commands described in clause 10. They include mapping between the information elements defined in the NACE specification and the Diameter attribute-value pairs (AVPs).

In the tables that describe this mapping (Tables 8-1 to 8-4), each information element is marked as (M) mandatory, (C) conditional, or (O) optional [ETSI ES 283 035].

8.2 Procedures on the M1 interface

This procedure is used to push mobility service parameters from the TLM-PE to the MLM-PE. This information flow occurs from the UE authentication procedure to connect the security association between UE and MLM-PE(P) to distribute mobility service information.

8.2.1 Indication of host-based mobility

This procedure is mapped to the Push-Notifications-Request/Answer commands in the Diameter application specified in clause 10. Tables 8-1 and 8-2 detail the involved information elements as defined in the NACE specification [ITU-T Y.2014] and their mapping to Diameter AVPs.

Table 8-1 – Indication of host-based mobility

Information Element name	Mapping to Diameter AVP	Category
	Mobility-Protocol-Type	M
Mobility service subscriber identifier	User-Name	M
Transport subscriber identifier	User-Name	C
Persistent IP address	Globally-Unique-Address	C
Keying material	Keying-Material	M
RACE address	RACE-Contact-Point	O
Anchor point address	Anchor-Point-Address	O

Table 8-2 – Indication of host-based mobility response

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

8.2.1.1 Procedure at the TLM-PE side

The TLM-PE shall deliver the Indication of host-based mobility by including the following information elements:

(1) At a minimum, a User-Name AVP for a transport subscriber identifier or a Globally-Unique-Address AVP shall be included conditionally. The Globally-Unique-Address AVP shall contain a Frame-IP-Address AVP or a Frame-IPv6-Prefix AVP, and an Address-Realm AVP.

(2) A RACE-Contact-Point AVP or an Anchor-Point-Address AVP may be included optionally.

(3) The Mobility-Protocol-Type AVP, the User-Name AVP for a Mobility service subscriber identifier, and the Keying-Material AVP shall be present.

8.2.1.2 Procedure at the MLM-PE side

Upon reception of the Indication of host-based mobility, the MLM-PE shall:

(1) If User-Name AVP for transport subscriber is present, go to step (4). Otherwise, go to the next step.

(2) If User-Name AVP for transport subscriber is absent, but Globally-Unique-Address AVP is present, go to step (4). Otherwise, go to the next step.

(3) If both User-Name AVP for transport subscriber and Globally-Unique-Address AVP are absent, return Indication of host-based mobility response with Result-Code set to DIAMETER_MISSING_AVP.

(4) If no session record is stored for the User-Name AVP or Globally-Unique-Address AVP, return network selection key transfer indication response with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN. Otherwise, go to the next step.

(5) If Mobility-Protocol-Type AVP is present, go to step the next step. Otherwise, return indication of host-based mobility response with Result-Code set to DIAMETER_MISSING_AVP.

(6) If User-Name AVP for Mobility service is present, go to step the next step. Otherwise, return indication of host-based mobility response with Result-Code set to DIAMETER_MISSING_AVP.

(7) If Keying-Material AVP is present, go to step the next step. Otherwise, return indication of host-based mobility response with Result-Code set to DIAMETER_MISSING_AVP.

(8) Under temporary overload conditions, the MLM-PE shall stop processing the request and return a network selection key transfer indication response with the Experimental-Result-Code set to DIAMETER_USER_DATA_NOT_AVAILABLE. Otherwise, go to the next step.

(9) If the MLM-PE cannot fulfil the received request for reasons not stated in the above-mentioned steps, e.g., due to database error, it shall stop processing the request and, return a network selection key transfer indication response with the Result-Code set to DIAMETER_UNABLE_TO_COMPLY. Otherwise, go to the next step.

(10) The MLM-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS in the indication of host-based mobility response.

8.2.2 Indication of network-based mobility

This procedure is mapped to the commands Push-Notifications-Request/Answer in the Diameter application specified in clause 10. Tables 8-3 and 8-4 detail the relevant information elements as defined in the NACE specification [ITU-T Y.2014] and their mapping to Diameter AVPs.

Table 8-3 – Indication of network-based mobility

Information element name	Mapping to Diameter AVP	Category
	Mobility-Protocol-Type	M
Mobility service subscriber identifier	User-Name	M
Transport subscriber identifier	User-Name	C
Persistent IP address	Globally-Unique-Address	C
Address of MLM-PE(C)	Central-MLM-PE-Contact-Point	M
Tunnel end-point address	Tunnel-End-Point-Address	O
Address of RACE	RACE-Contact-Point	O
Address of anchor point	Anchor-Point-Address	O

Table 8-4 – Indication of network-based mobility response

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

8.2.2.1 Procedure at the TLM-PE side

The TLM-PE shall deliver the indication of network-based mobility by including the following information elements:

(1) At a minimum, a User-Name AVP for a transport subscriber identifier or a Globally-Unique-Address AVP shall be included conditionally. The Globally-Unique-Address AVP shall contain a Frame-IP-Address AVP or a Frame-IPv6-Prefix AVP, and an Address-Realm AVP.

(2) A Tunnel-End-Point-Address AVP or a RACE-Contact-Point AVP or an Anchor-Point-Address AVP may be included optionally.

(3) The Mobility-Protocol-Type AVP, the User-Name AVP for a mobility service subscriber identifier, and the Central-MLM-PE-Contact-Point AVP shall be present.

8.2.2.2 Procedure at the MLM-PE side

Upon reception of the Indication of host-based mobility, the MLM-PE shall:

(1) If User-Name AVP for transport subscriber is present, go to step (4). Otherwise, go to the next step.

(2) If User-Name AVP for transport subscriber is absent, but Globally-Unique-Address AVP is present, go to step (4). Otherwise, go to the next step.

(3) If both User-Name AVP for transport subscriber and Globally-Unique-Address AVP are absent, return Indication of host-based mobility response with Result-Code set to DIAMETER_MISSING_AVP.

(4) If no session record is stored for the User-Name AVP or Globally-Unique-Address AVP, return network selection key transfer indication response with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN. Otherwise, go to the next step.

(5) If Mobility-Protocol-Type AVP is present, go to step the next step. Otherwise, return Indication of host-based mobility response with Result-Code set to DIAMETER_MISSING_AVP.

(6) If User-Name AVP for Mobility service is present, go to step the next step. Otherwise, return Indication of host-based mobility response with Result-Code set to DIAMETER_MISSING_AVP.

(7) If Central-MLM-PE-Contact-Point AVP is present, go to step the next step. Otherwise, return Indication of host-based mobility response with Result-Code set to DIAMETER_MISSING_AVP.

(8) Under temporary overload conditions, the MLM-PE shall stop processing the request and return a network selection key transfer indication response with the Experimental-Result-Code set to DIAMETER_USER_DATA_NOT_AVAILABLE. Otherwise, go to the next step.

(9) If the MLM-PE cannot fulfil the received request for reasons not stated in the above steps, e.g., due to database error, it shall stop processing the request and, return a network selection key transfer indication response with the Result-Code set to DIAMETER_UNABLE_TO_COMPLY. Otherwise, go to the next step.

(10) The MLM-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS in the Indication of host-based mobility response.

9 Use of Diameter-based protocol

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

9.1 Securing Diameter messages

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

9.2 Accounting functionality

Accounting functionality (accounting session state machine, related command codes and AVPs) is not used at the M1 interface.

9.3 Use of sessions

Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server [IETF RFC 6733].

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

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in [IETF RFC 6733]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

9.4 Transport protocol

Diameter messages over the M1 interface shall make use of SCTP [IETF RFC 4960] and shall utilize the new SCTP checksum method specified in [IETF RFC 4960].

9.5 Routing considerations

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

With regard to the Diameter diameter protocol used at the M1 interface, the TLM-PE acts as a Diameter server and the MLM-PE(P) acts as the Diameter client.

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

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

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

9.6 Advertising application support

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

If TLM-PE and MLM-PE(P) indicate support of the M1 application, then the M1 application identifier (16777352) shall be used in the Diameter message header of all subsequent messages exchanged within this association.

Support of the M1 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 M1 (16777352).

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

Table 9-1 – Vendor identifiers for M1

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

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

10 Message specification

10.1 Commands

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

Table 10-1 – Command code

Command	Abbreviation	Defining reference	Command code	See clause
Push-Notification-Request	PNR	[ETSI TS 129 329]	309	10.1.1
Push-Notification-Answer	PNA	[ETSI TS 129 329]	309	10.1.2

10.1.1 Push-Notification-Request command

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

Message Format:

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777352>
                              < Session-Id >
                              { Vendor-Specific-Application-Id }
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              { Destination-Host }
                              { Destination-Realm }
                              { Mobility-Protocol-Type }
                              [ User-Name ]
                              [ User-Name ]
                              [ Globally-Unique-Address ]
                              [ Keying-Material ]
                              [ RACE-Contact-Point ]
                              [ Anchor-Point-Address ]
                              [ Central-MLM-PE-Contact-Point ]
                              [ Tunnel-End-Point-Address ]
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

10.1.2 Push-Notification-Answer command

The Push-Notification-Answer (PNA) command, indicated by the Command-Code field set to 309 and the "R" bit cleared in the Command Flags field, is sent by a client in response to the Push-Notification-Request command. The Experimental-Result-Code AVP may contain one of the values defined in clause 10.2.

Message Format:

```
< Push-Notification-Answer > ::= < Diameter Header: 309, PXY, 16777352>
                             < Session-Id >
                             { Vendor-Specific-Application-Id }
                             [ Result-Code ]
                             [ Experimental-Result ]
                             { Auth-Session-State }
                             { Origin-Host }
                             { Origin-Realm }
                             *[ AVP ]
                             *[ Failed-AVP ]
                             *[ Proxy-Info ]
                             *[ Route-Record ]
```

10.2 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 following clauses.

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

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

DIAMETER_ERROR_USER_UNKNOWN (5001)

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

DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

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

10.3 Attribute-value pairs

The following tables (Tables 10-2 to 10-5) summarize the AVPs used in this Recommendation. These are, in addition to the AVPs, defined in [IETF RFC 6733].

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

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

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
Globally-Unique-Address	300	10.3.1	Grouped	M,V				Y
NOTE – The AVP flag bit denoted as "M" indicates support of the AVP is required. The AVP flag bit denoted as "V" indicates the optional Vendor-ID field is present in the AVP header.								

Table 10-3 describes the Diameter AVPs 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 10-3 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 10-3 – Diameter AVPs imported from [ETSI ES 283 035]

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
RACE-Contact-Point	351	10.3.2	DiameterIdentity	V	M			Y
NOTE – The AVP flag bit denoted as "M" indicates support of the AVP is required. The AVP flag bit denoted as "V" indicates the optional Vendor-ID field is present in the AVP header.								

Table 10-4 describes the Diameter AVPs defined by [ITU-T Q.3230] and used within this Recommendation. These AVPs are described in this Recommendation for information; however, the

normative detail for these AVPs is contained in [ITU-T Q.3230]. The Vendor-Id header of all AVPs defined in Table 10-4 shall be set to ITU-T (11502).

Table 10-4 – Diameter AVPs imported from [ITU-T Q.3230]

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
Keying-Material	1040	10.3.3	Octet String	M,V				Y

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

Table 10-5 – Diameter AVPs imported from [ITU-T Q.3232]

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
Central-MLM-PE-Contact-Point	1054	10.3.4	DiameterIdentity	V	M			Y
Mobility-Protocol-Type	1056	10.3.5	Enumerated	V	M			Y
Anchor-Point-Address	1057	10.3.6	DiameterIdentity	V	M			Y
Tunnel-End-Point-Address	1058	10.3.7	DiameterIdentity	V	M			Y
NOTE – The AVP flag bit denoted as "M" indicates support of the AVP is required. The AVP flag bit denoted as "V" indicates the optional Vendor-ID field is present in the AVP header.								

10.3.1 Globally-Unique-Address AVP

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

AVP format:

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

10.3.2 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.

10.3.3 Keying-Material AVP

The Keying-Material AVP (AVP code 1040 11502) is of type Octet String, and provides the material used for security association.

10.3.4 Central-MLM-PE-Contact-Point AVP

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

10.3.5 Mobility-Protocol-Type AVP

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

The following values are defined:

- HOST-BASED-MOBILITY (0);
- NETWORK-BASED-MOBILITY (1).

10.3.6 Anchor-Point-Address AVP

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

10.3.7 Tunnel-End-Point-Address AVP

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

10.4 Use of namespaces

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

10.4.1 AVP codes

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

10.4.2 Experimental-Result-Code AVP values

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

10.4.3 Command code values

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

10.4.4 Application-ID value

This Recommendation defines the M1 Diameter application with application ID 16777352. The vendor identifier assigned by IANA to ITU-T is 11502 (http:/www.iana.org/assignments/enterprise-numbers).

11 Security considerations

Security requirements within the functional requirements and architecture of the NACF are addressed by the security requirements for NGN [b-ITU-T Y.2701]. The M1 interface shall follow the security requirements of the network attachment control functions (NACF) [ITU-T Y.2014].

Clause 10.1 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].

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

Appendix I

Mapping to mobility signalling requirements for IMT-2020

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

The ITU-T FG IMT-2020 network is recommended to support distributed network architecture, and optimized routes for application data and signalling data, Control/User-plane functions should be clearly separated with defined interface [b-ITU-T FG IMT-2020].

NGN is also designed to separate control/user-plane functions, and even NACE and MMCE are separated within the control plane to be responsible for the initialization of CPE for accessing the NGN services [ITU-T Y.2014] and the mobile location management [ITU-T Y.2018], respectively. Reference point M1 allows the TLM-PE (NACE) to interact with the MLM-PE (MMCE) for pushing mobility service parameters, such as keying material, and anchor address. Information flows used on the M1 interface may be adapted to the information flows for indicating mobility service types between modular functional entities if functional entities similar to NACE and MMCE are defined according to [b-ITU-T FG IMT-2020].

Bibliography

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

[b-ITU-T FG IMT-2020] FG IMT-2020: *Report on Standards Gap analysis*.

[b-IETF RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; 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, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016