International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3229

(08/2016)

SERIES Q: SWITCHING AND SIGNALLING

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

Signalling requirements and protocol at the M2 interface between the transport location management physical entity and the handover decision and control physical entity

Recommendation ITU-T Q.3229

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.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.3229

Signalling requirements and protocol at the M2 interface between the transport location management physical entity and the handover decision and control physical entity

Summary

Recommendation ITU-T Q.3229 specifies the protocol for the interface between the transport location management physical entity (TLM-PE) of the network attachment control entity (NACE) and the handover decision and control physical entity (HDC-PE) of the mobility management and control entity (MMCE). M2 interface provides information from the TLM-PE to the HDC-PE to support the security association. This Recommendation supports information flows providing the keying material via the M2 reference point as specified in Recommendation ITU-T Y.2018.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3229	2016-08-29	11	11.1002/1000/12985

Keywords

Handover decision and control physical entity, HDC-PE, mobility management and control entity, MMCE, M2 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.3229

Signalling requirements and protocol at the M2 interface between the transport location management physical entity and the handover decision and control physical entity

1 Scope

This Recommendation specifies the protocol for the interface between the transport location management physical entity (TLM-PE) of the network attachment control entity (NACE) and the handover decision and control physical entity (HDC-PE) of the mobility management and control entity (MMCE). M2 interface provides information from the TLM-PE to the HDC-PE to support the security association. This Recommendation supports information flows providing the keying material via the M2 reference point as specified in [ITU-T Y.2018].

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 Y.3230 (2012), *Signalling requirements and protocol at the M13 interface between the transport location management and network information distribution physical entities*.

[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 terms defined elsewhere:

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

– international mobile station identity;

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

3.1.2 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

ABNF Augmented Backus-Naur Form

AM-FE Access Management Functional Entity

AM-PE Access Management Physical Entity

AVP Attribute-Value Pair

CPE Customer Premises Equipment

HDC-FE Handover Decision and Control Functional Entity

HDC-PE Handover Decision and Control Physical Entity

IP Internet Protocol

IPsec IP security protocol

MLM-FE Mobile Location Management Functional Entity

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

NGN Next Generation Network

SCTP Stream Control Transmission Protocol

TAA-FE Authentication and Authorization Functional Entity

TAA-PE Transport Authentication and Authorization Physical Entity

TLM-FE Location Management Functional Entity

TLM-PE Transport Location Management Physical Entity

UE User Equipment

5 Conventions

None.

6 M2 interface

6.1 Overview

The network attachment control function (NACF) manages transport resource subscription information between authentication and authorization functional entity (TAA-FE) and transport location management functional entity (TLM-FE). This information includes the keying material within mobility service parameters in addition to the transport subscriber identifier. The M2 interface allows distributing the keying material from the TLM-FE to the handover decision and control physical entity (HDC-FE) defined in the stage 2 specifications [ITU-T Y.2014] and [ITU-T Y.2018]. Mobility service parameters information flow is used on the M2 reference point. This information flow provides the keying material to support the security association required between the HDC-FE and the user equipment (UE). Figure 6-1 shows the M2 reference point between the transport location management physical entity (TLM-PE) and handover decision and control physical entity (HDC-PE).

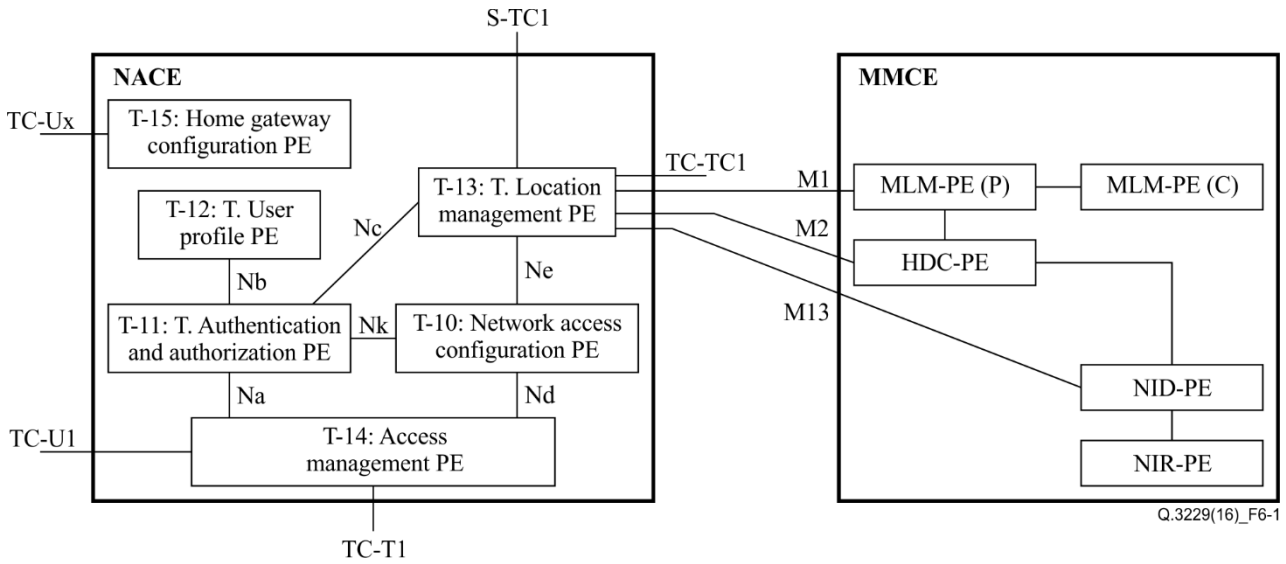

Figure 6-1 – Reference points between the NACE and the MMCE [ITU-T Y.2018]

6.2 Physical entities

Table 6-1 indicates the mapping from the functional entities to the physical entities implementing them.

Table 6-1 – Mapping from functional to physical entities concerned with the M2 reference point

Functional entity	Abbrev.	Physical entity	Abbrev.
Network attachment control functions	NACF	Network attachment control entity	NACE
Mobility management and control functions	MMCF	Mobility management and control entity	MMCE
Transport location management functional entity	TLM-FE	Transport location management physical entity	TLM-PE
Transport authentication and authorization functional entity	TAA-FE	Transport authentication and authorization physical entity	TLM-PE
Access management functional entity	AM-FE	Access management physical entity	AM-PE
Handover decision and control functional entity	HDC-FE	Handover decision and control physical entity	HDC-PE
Mobile location management functional entity	MLM-FE	Mobile location management physical entity	MLM-PE

6.2.1 Transport location management physical entity (TLM-PE)

The TLM-PE identifies the current network location of a UE and keeps track of it as it moves. When the point of attachment of a UE is changed in network, TLM-PE updates the association between the UE's IP address and related network location information and the association between network location information and geographical location information. When a UE is attached to a new access network, the new TLM-PE allocates a new temporary IP address, stores the location information and may inform service control function of the updated binding information.

The TLM-PE delivers the mobility service subscriber identifier in addition to the keying material as the network selection key transfer indication. When a mobile user hands over from the serving AM-PE to the target AM-PE, the TAA-PE will receive the user authentication request from the target AM-PE and derive an authentication key for it. The TLM-PE informs the HDC-PE of the keying material related to mobility service authentication.

6.2.2 Handover decision and control physical entity (HDC-PE)

The HDC-PE has three sub-functions: handover decision, layer 2 handover control, and layer 3 handover control. The HDC-PE is responsible for triggering handover and invoking handover action. The security association is required for the ongoing network selection and decision process subsequent to attachment.

7 Signalling requirements

Reference point M2 supports the "network selection key transfer indication" primitive as the keying material for the security association required between the HDC-PE and the UE. The TLM-PE holds keying material in the mobility service parameters information shown in Table 7-1 and pushes keying material to HDC-PE.

The M2 reference point should allow information exchange as follows: mobility service parameters information is pushed by the TLM-PE to HDC-PE.

Table 7-1 – Mobility service parameters information 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 flow shall be used on the M2 interface:

– Network selection key transfer indication

Figure 7-1 shows the information flow between the TLM-PE and the HDC-PE through the M2 interface.

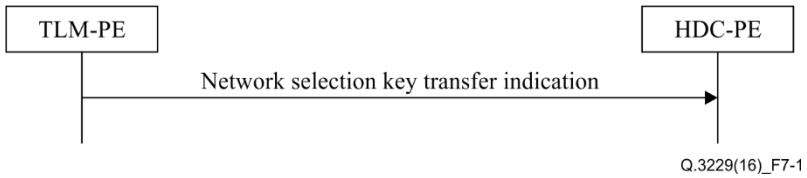

Figure 7-1 – Information flow

7.1 Network selection key transfer indication

In the case of host-based mobility, IP configuration procedure is executed after the authentication procedure. During this procedure, the TLM-PE transfers keying material to the HDC-PE for network discovery and selection. In the case of network-based mobility, key material is transferred to the HDC-PE during the mobility location management procedure. The network selection key transfer indication information flow described in [ITU-T Y.2018] contains keying material shown in Table 7-2.

Table 7-2 – Network selection key transfer indication (TLM-PE → HDC-PE)

Information element	Description
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.
Keying material	The material used for security association between the UE and HDC-PE.

The network discovery and decision procedure is performed before handover. After the UE attaches to a new network, TAA-PE informs HDC-PE of network selection key transfer indication via TLM-PE, which means previous handover is completed. UE moves and determines that another handover is required, so HDC-PE triggers handover procedures.

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 (Table 8-1 and Table 8-2), each information element is marked as (M) mandatory, (C) conditional or (O) optional [ETSI ES 283 035].

8.2 Procedures on the M2 interface

8.2.1 Network selection key transfer indication overview

This procedure is used to push keying material information from the TLM-PE to the HDC-PE. This information flow occurs for Security Association (SA) which is a "connection" that affords security service to the traffic.

This procedure is mapped to the commands Push-Notifications-Request/Answer 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 – Network selection key transfer indication

Information element name	Mapping to Diameter AVP	Category
Globally unique IP address	Globally-Unique-Address	C
Transport Subscriber Identifier	User-Name	C
Keying material	Keying-Material	M

Table 8-2 – Network selection key transfer indication response

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

8.2.2 Procedure at the TLM-PE side

The TLM-PE shall request the network selection key transfer indication by including the following information elements:

1) At a minimum, a Globally-Unique-Address AVP or a User-Name AVP shall be included. The Globally-Unique-Address AVP shall contain a Frame-IP-Address AVP or a Frame-IPv6-Prefix AVP, and an Address-Realm AVP.
2) The Keying-Material AVP shall be present.

8.2.3 Procedure at the HDC-PE side

Upon reception of a network selection key transfer indication, the HDC-PE shall:

1) If the Globally-Unique-Address AVP is present, go to step 4). Otherwise, go to the next step.
2) If the Globally-Unique-Address AVP is absent, but the User-Name AVP is present, go to step 4). Otherwise, go to the next step.
3) Because both the Globally-Unique-Address AVP and the User-Name AVP are absent, return a network selection key transfer indication response with Result-Code set to DIAMETER_MISSING_AVP.

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

6) Under temporary overload conditions, the HDC-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.

7) If the HDC-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.

8) The HDC-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS in the network selection key transfer indication response.

9 Use of Diameter-based protocol

The Diameter base protocol [IETF RFC 6733] shall be used for the M2 interface with the clarifications listed in the following clauses.

9.1 Security

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

9.2 Accounting

This functionality (accounting session state machine, related command codes and AVPs) is not used on the M2 interface.

9.3 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. See [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 M2 interface shall make use of stream control transmission protocol (SCTP) specified in [IETF RFC 4960] and shall utilize the new SCTP checksum method specified in [IETF RFC 4960].

9.5 Routing considerations

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

With regard to the Diameter protocol used at the M2 interface, the TLM-PE acts as a Diameter server and the HDC-PE acts as a Diameter client.

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

9.6 Application advertisement

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 the TLM-PE and HDC-PE indicate support of the M2 application, then the M2 application identifier (16777353) shall be used in the Diameter message header of all subsequent messages exchanged within this association.

Support of the M2 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 M2 (16777353).

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

NOTE – A Vendor-Id AVP included in the CER and CEA commands, which is not included in the Vendor-Specific-Application-Id AVPs as described above, indicates 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 the HDC-PE. See the command code in 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 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 the client of changes to the user data in the server. This command is defined in [ETSI TS 129 329] and is used with additional AVPs defined in this Recommendation.

Message Format:

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777353>
                        < Session-Id >
                        { Vendor-Specific-Application-Id }
```

```
                        { Auth-Session-State }
                        { Origin-Host }
                        { Origin-Realm }
                        [ Destination-Host ]
                        { Destination-Realm }
                        [ Globally-Unique-Address ]
                        [ User-Name ]
                        { Keying-Material }
                        *[ AVP ]
                        *[ Proxy-Info ]
                        *[ Route-Record ]
```

10.1.2 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 PNR command. The Experimental-Result AVP may contain one of the values defined in clause 10.2.

Message Format:

```
< Push-Notification-Answer > ::= < Diameter Header: 309, PXY, 16777353>
                        < 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 values 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

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

– DIAMETER_ERROR_USER_UNKNOWN (5001)

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

– DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

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

10.3 AVPs

The following tables (Tables 10-2 and Table 10-3) summarize the AVPs used in this Recommendation. These are, in addition to the AVPs, defined in [IETF RFC 3588].

Table 10-2 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 details for these AVPs are 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

Table 10-3 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 10-3 shall be set to ITU-T (11502).

Table 10-3 – 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	10.3.2	Octet String	M,V				Y

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 Keying-Material AVP

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

10.4 Use of namespaces

This clause contains the values assigned to 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 M2 Diameter application with application ID 16777353. 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 [ITU-T Y.2701]. The M2 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].

Further 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 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 M2 allows the TLM-PE (NACE) to interact with the HDC-PE (MMCE) for the security association required between the HDC-PE and the UE. Information flows used on the M2 interface may be adapted to the information flows for indicating network selection key transfer 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 Q.1001] Recommendation ITU-T Q.1001 (1988), *General aspects of public land mobile networks*.

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

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

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

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

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