

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3230

(08/2012)

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 M13
interface between the transport location
management and network information
distribution physical entities**

Recommendation ITU-T Q.3230



ITU-T Q-SERIES RECOMMENDATIONS
SWITCHING AND SIGNALLING

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

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

Recommendation ITU-T Q.3230

Signalling requirements and protocol at the M13 interface between the transport location management and network information distribution physical entities

Summary

Recommendation ITU-T Q.3230 provides the protocol for the interface between the transport location management physical entity (TLM-PE) of the network attachment control entity (NACE) and the network information distribution physical entity (NID-PE) of the mobility management control entity (MMCE). The M13 interface provides the keying material, derived from the user equipment (UE) authentication procedure, in support of the security association required between the NID-PE and the UE. This Recommendation supports information flows providing the keying material via the M13 reference point as specified in Recommendation ITU-T Y.2018.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3230	2012-08-13	11

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	2
3.1 Terms defined elsewhere	2
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	3
6 M13 interface.....	3
6.1 Overview	3
6.2 M13 reference model.....	3
6.3 Physical entities and capabilities	4
7 Signalling requirements	4
7.1 Network selection key transfer indication.....	5
8 Description of procedure	5
8.1 General	5
8.2 Procedure on the M13 interface	5
9 Use of Diameter base protocol	7
9.1 Securing Diameter messages.....	7
9.2 Accounting functionality	7
9.3 Use of sessions	8
9.4 Transport protocol	8
9.5 Routing considerations	8
9.6 Advertising application support	8
10 Message specification.....	9
10.1 Commands.....	9
10.2 Experimental-Result-Code AVP values	10
10.3 AVPs.....	10
10.4 Use of namespaces	11
11 Security considerations.....	11
Bibliography.....	12

Recommendation ITU-T Q.3230

Signalling requirements and protocol at the M13 interface between the transport location management and network information distribution physical entities

1 Scope

This Recommendation defines the protocol for the M13 interface between the transport location management physical entity (TLM-PE) and the network information distribution physical entity (NID-PE). The M13 reference point provides the keying material derived from the user equipment (UE) authentication procedure.

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.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*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [ETSI ES 283 034] ETSI ES 283 034 V2.2.0 (2008), *Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the Diameter protocol*.
- [ETSI TS 129 229] ETSI TS 129 229 V9.3.0 (2010), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (3GPP TS 29.229 version 9.3.0 Release 9) 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 (3GPP TS 29.329 version 6.7.0 Release 6)*.
- [IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.
- [IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

- international mobile station identity;
- actual location of the mobile station (e.g., PLMN, MSC area, location area, as required).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABNF	Augmented Backus-Naur Form
AM-PE	Access Management Physical Entity
AVP	Attribute-Value Pair
CEA	Capabilities-Exchange-Answer
CER	Capabilities-Exchange-Request
CPE	Customer Premises Equipment
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
HDC-PE	Handover Decision and Control Physical Entity
HGWC-PE	Home Gateway Configuration Physical Entity
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IPSec	IP Security protocol
MLM-PE	Mobile Location Management Physical Entity
MMCE	Mobility Management Control Entity
NACE	Network Attachment Control Entity
NACF	Network Attachment Control Functions
NAC-PE	Network Access Configuration Physical Entity
NID-PE	Network Information Distribution Physical Entity
NIR-PE	Network Information Repository Physical Entity
PD-PE	Policy Decision Physical Entity
PLMN	Public Land Mobile Network
PNA	Push-Notification-Answer

PNR	Push-Notification-Request
RACE	Resource Admission and Control Entity
RFC	Request For Comments
SCE	Service Control Entity
SCTP	Stream Control Transmission Protocol
TAA-PE	Transport Authentication and Authorization Physical Entity
TLM-PE	Transport Location Management Physical Entity
TRC-PE	Transport Resource Control Physical Entity
TUP-PE	Transport User Profile Physical Entity
UE	User Equipment
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

5 Conventions

None.

6 M13 interface

6.1 Overview

The network attachment control entity (NACE) maintains information about the keying material derived from the user equipment (UE) authentication procedure. This information is stored in the transport location management physical entity (TLM-PE) and is pushed to the network information distribution physical entity (NID-PE) in the mobility management control entity (MMCE).

6.2 M13 reference model

This clause describes the M13 reference architecture. Figure 6-1 can be used as an initial architecture illustration:

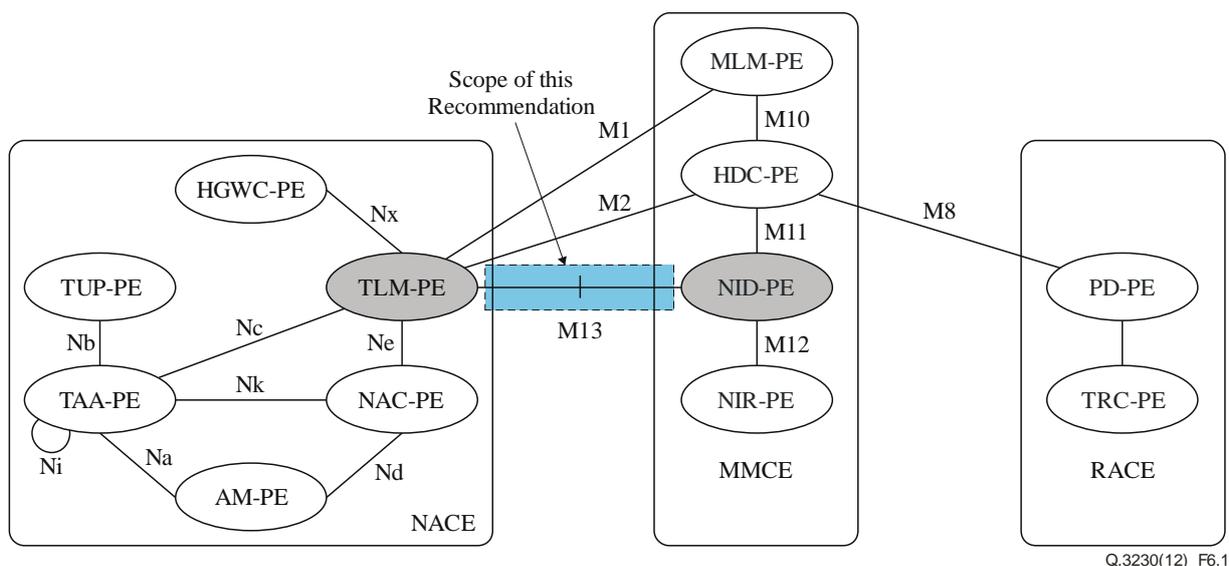


Figure 6-1 – M13 reference model

6.3 Physical entities and capabilities

6.3.1 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 agreement with the requester and on user preferences regarding the privacy of its location.

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

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

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

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

6.3.2 NID-PE

The NID-PE communicates with the entity making the handover decision during the network discovery phase. The handover decision may be made by either the UE or the handover decision and control physical entity (HDC-PE). The NID-PE has the following responsibilities:

- Distributing handover policy, which is a set of operator-defined rules and preferences that affect the handover decisions taken by the UE or HDC-PE.
For example, a handover policy can indicate that vertical handover from E-UTRAN access to WLAN access is not allowed. It can also indicate, e.g., that WiMAX access is preferable to WLAN access.
- Distributing other information provided by the NIR-PE.

The functionality of the NID-PE is further detailed in clause 6.4 of [ITU-T Y.2018].

7 Signalling requirements

The M13 reference point allows the TLM-PE to interact with the NID-PE for pushing mobility service parameters such as keying material, in support of the security association required between the NID-PE and the UE.

The M13 reference point is an intra-domain reference point.

The M13 reference point allows information exchange as follows:

- The mobility service parameters information is pushed by the TLM-PE to the NID-PE (see Figure 7-1).

For further information, refer to clause 8.5.3 of [ITU-T Y.2014].

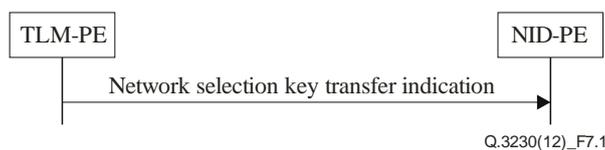


Figure 7-1 – Information flow

7.1 Network selection key transfer indication

This information flow provides the keying material derived from the UE authentication procedure, in support of the security association required between the NID-PE and the UE. This security association is required for the ongoing network selection and decision process subsequent to attachment.

The network selection key transfer indication flow contains the following information shown in Table 7-1.

Table 7-1 – Network selection key transfer indication (TLM-PE → NID-PE)

Information Element	Explanation
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 NID-PE.

8 Description of procedure

8.1 General

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

In the tables that describe this mapping, each information element is marked as (M) Mandatory, (C) Conditional or (O) Optional. See [ETSI ES 283 034].

8.2 Procedure on the M13 interface

8.2.1 Network selection key transfer indication

8.2.1.1 Overview

This procedure is used by the TLM-PE to notify the NID-PE of the occurrence of the keying material information.

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

Table 8-1 – Network selection key transfer indication request

Information Element name	Mapping to Diameter AVP	Category
Unique IP Address	Globally-Unique-Address	C
Address Realm		
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

8.2.1.2 Procedure at the TLM-PE

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

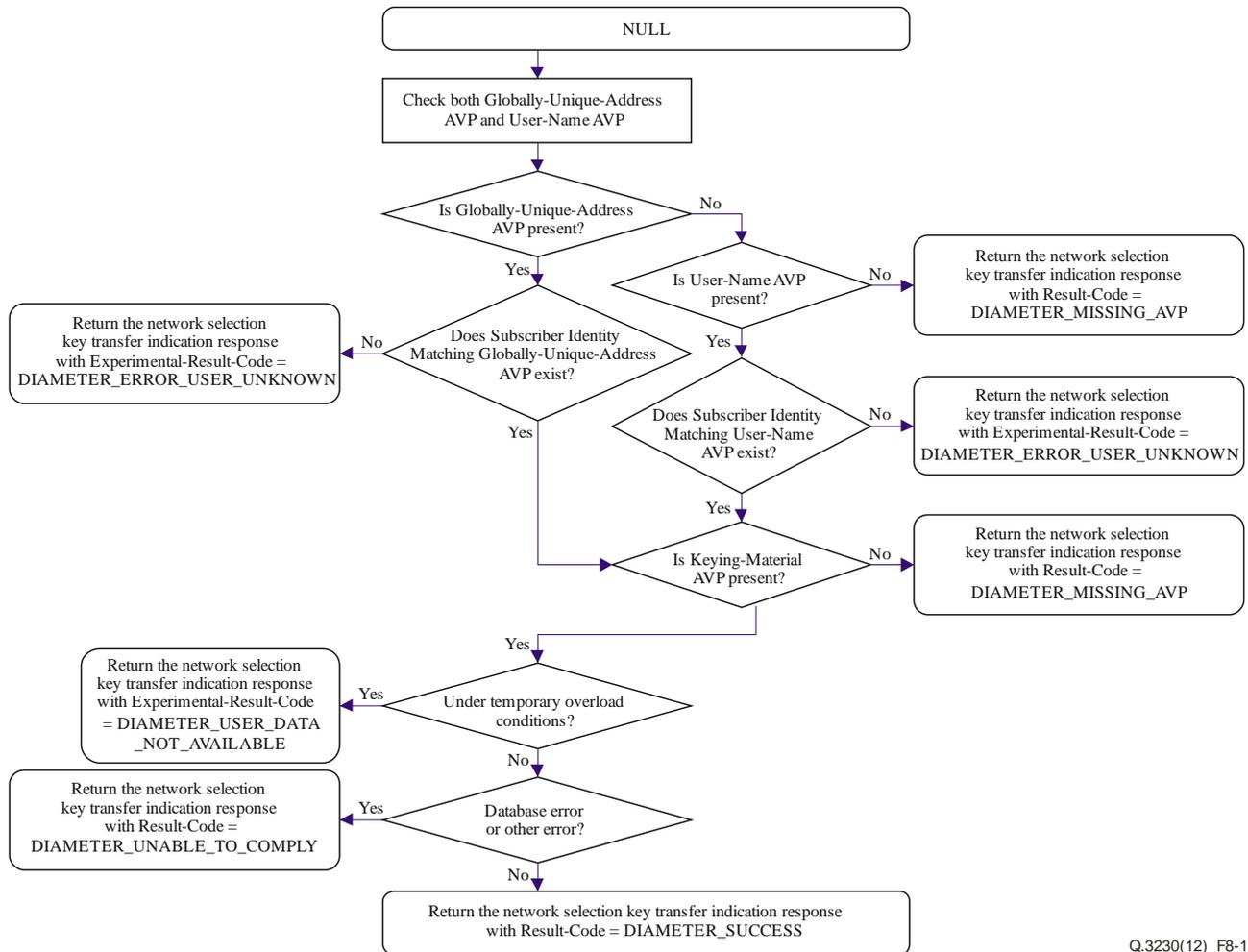
- 1) At a minimum, a Globally-Unique-Address AVP or a User-Name AVP shall be included. The Globally-Unique-Address AVP shall contain a Frame-IP-Address AVP or a Frame-IPv6-Prefix AVP, and an Address-Realm AVP.
- 2) The Keying-Material AVP shall be present.

8.2.1.3 Procedure at the NID-PE

Upon reception of a network selection key transfer indication request (see Figure 8-1), the NID-PE shall:

- 1) Check both the Globally-Unique-Address AVP and the User-Name AVP.
- 2) If the Globally-Unique-Address AVP is present, go to step 6). Otherwise, go to the next step.
- 3) If the Globally-Unique-Address AVP is absent, but the User-Name AVP is present, go to step 5). Otherwise, go to the next step.
- 4) Because both the Globally-Unique-Address AVP and the User-Name AVP are absent, return a network selection key transfer indication response with Result-Code set to DIAMETER_MISSING_AVP and stop this procedure. Otherwise, go to the next step.
- 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 a network selection key transfer indication 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 network selection key transfer indication response with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN and stop this procedure. Otherwise, go to the next step.
- 7) If the Keying-Material AVP is absent, return a network selection key transfer indication response with the Result-Code set to DIAMETER_MISSING_AVP and stop this procedure. Otherwise, go to the next step.
- 8) Under temporary overload conditions, the NID-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 and stop this procedure. Otherwise, go to the next step.

- 9) If the NID-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 NID-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS in the network selection key transfer indication response and stop this procedure.



Q.3230(12)_F8-1

Figure 8-1 – Procedure for network selection key transfer indication on the NID-PE side

9 Use of Diameter base protocol

With the clarifications listed in the following clauses the Diameter base protocol defined by [IETF RFC 3588] shall apply.

9.1 Securing Diameter messages

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

9.2 Accounting functionality

Accounting functionality (i.e., accounting session state machine, related command codes and AVPs) is not used at the M13 interface.

9.3 Use of sessions

Diameter sessions are implicitly terminated. An implicitly terminated session is one in 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 3588].

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 state information about this session and the client does not need to send a 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 M13 interface shall make use of stream control transmission protocol (SCTP) as specified in [IETF RFC 4960] and shall utilize the new SCTP checksum method also 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 M13 interface, the TLM-PE acts as a Diameter server and the NID-PE acts as a Diameter client.

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

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

If the TLM-PE and NID-PE indicate support of the M13 application, then the M13 application identifier (16777307) shall be used in the Diameter message header of all subsequent messages exchanged within this association.

Support of the M13 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 M13 (16777307).

The TLM-PE and the NID-PE are required to advertise the support of AVPs specified in 3GPP, ETSI, and ITU-T documents by including the values 10415 (3GPP), 13019 (ETSI) and 11502 (ITU-T) in three different instances of the Supported-Vendor-Id AVP in the CER and CEA commands respectively. See Table 9-1 for vendor identifiers for M13.

Table 9-1 – Vendor identifiers for M13

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

NOTE – The Vendor-Id AVP included in CER and CEA commands that are not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per [IETF RFC 3588].

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 NID-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, 16777307>
    < 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, 16777307>
    < 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 clauses below.

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 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 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 10-3 – Diameter AVPs defined in this Recommendation

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
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 NID-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 M13 Diameter application with application ID 16777307. The vendor identifier assigned by IANA to ITU-T is 11502 (<http://www.iana.org/assignments/enterprise-numbers>).

11 Security considerations

The security requirements within the functional requirements and architecture of the network attachment control functions (NACF) are addressed by the security requirements for NGN [ITU-T Y.2701]. The M13 interface shall follow the security requirements of the NACF as specified in [ITU-T Y.2014].

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

Further considerations are provided in the security considerations section of [IETF RFC 3588].

Bibliography

- [b-ITU-T Q.1001] Recommendation ITU-T Q.1001 (1988), *General aspects of public land mobile networks*.
- [b-IETF RFC 3554] IETF RFC 3554 (2003), *On the Use of Stream Control Transmission Protocol (SCTP) with IPSec*.

SERIES OF ITU-T RECOMMENDATIONS

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