ETSI TS 129 329 V15.2.0 (2019-10)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Sh interface based on the Diameter protocol;
Protocol details
(3GPP TS 29.329 version 15.2.0 Release 15)

Reference
RTS/TSGC-0429329vf20

Keywords
GSM,LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 5
1 Scope 6
2 References 6
3 Definitions, symbols and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 General 7
5 Use of the Diameter base protocol 7
6 Diameter application for Sh interface 7
6.1 Command-Code values 8
6.1.1 User-Data-Request (UDR) Command 8
6.1.2 User-Data-Answer (UDA) Command 9
6.1.3 Profile-Update-Request (PUR) Command 9
6.1.4 Profile-Update-Answer (PUA) Command 10
6.1.5 Subscribe-Notifications-Request (SNR) Command 10
6.1.6 Subscribe-Notifications-Answer (SNA) Command 11
6.1.7 Push-Notification-Request (PNR) Command 12
6.1.8 Push-Notifications-Answer (PNA) Command 12
6.2 Result-Code AVP values 13
6.2.1 Success 13
6.2.2 Permanent Failures 13
6.2.2.1 DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED (5100) 13
6.2.2.2 DIAMETER_ERROR_OPERATION_NOT_ALLOWED (5101) 13
6.2.2.3 DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ (5102) 13
6.2.2.4 DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED (5103) 13
6.2.2.5 DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED (5104) 13
6.2.2.6 DIAMETER_ERROR_TOO_MUCH_DATA (5008) 13
6.2.2.7 DIAMETER_ERROR_TRANSPARENT_DATA OUT_OF_SYNC (5105) 13
6.2.2.8 DIAMETER_ERROR_FEATURE_UNSUPPORTED (5011) 13
6.2.2.9 DIAMETER_ERROR_SUBS_DATA_ABSENT (5106) 13
6.2.2.10 DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA (5107) 14
6.2.2.11 DIAMETER_ERROR_DSAI_NOT_AVAILABLE (5108) 14
6.2.2.12 DIAMETER_ERROR_IDENTITIES_DONT_MATCH (5002) 14
6.2.3 Transient Failures 14
6.2.3.1 DIAMETER_USER_DATA_NOT_AVAILABLE (4100) 14
6.2.3.2 DIAMETER_PRIOR_UPDATE_IN_PROGRESS (4101) 14
6.3 AVPs 15
6.3.1 User-Identity AVP 16
6.3.2 MSISDN AVP 16
6.3.3 User-Data AVP 16
6.3.4 Data-Reference AVP 16
6.3.5 Service-Indication AVP 17
6.3.6 Subs-Req-Type AVP 17
6.3.7 Requested-Domain AVP 18
6.3.7A Requested-Nodes AVP 18
6.3.8 Current-Location AVP 18
6.3.9 Server-Name AVP 18
6.3.10 Identity-Set AVP 18
6.3.11 Supported-Features AVP 18

6.3.12 Feature-List-ID AVP 19
6.3.13 Feature-List AVP 19
6.3.14 Supported-Applications AVP 19
6.3.15 Public-Identity AVP 19
6.3.16 Expiry-Time AVP 19
6.3.17 Send-Data-Indication AVP 19
6.3.18 DSAI-Tag AVP 19
6.3.19 Wildcarded-Public-Identity AVP 19
6.3.20 Wildcarded-IMPU AVP 19
6.3.21 Session-Priority AVP 19
6.3.22 One-Time-Notification AVP 19
6.3.23 Serving-Node-Indication AVP 20
6.3.24 Repository-Data-ID AVP 20
6.3.25 Sequence-Number AVP 20
6.3.26 Pre-paging-Supported AVP 20
6.3.27 Local-Time-Zone-Indication AVP 20
6.3.28 UDR-Flags 20
6.3.29 Call-Reference-Info AVP 21
6.3.30 Call-Reference-Number AVP 21
6.3.31 AS-Number AVP 21
6.3.32 OC-Supported-Features 21
6.3.33 OC-OLR 21
6.3.34 DRMP AVP 21
6.3.35 Load 21
6.4 Use of namespaces 21
6.4.1 AVP codes 21
6.4.2 Experimental-Result-Code AVP values 22
6.4.3 Command Code values 22
6.4.4 Application-ID value 22
7 Special Requirements 23
7.1 Version Control 23
Annex A (informative): Change history 24
History 27

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines a transport protocol for use in the IP multimedia (IM) Core Network (CN) subsystem based on the Diameter base protocol as specified in IETF RFC 6733 [15].

The present document is applicable to:

- The Sh interface between an AS and the HSS.
- The Sh interface between an SCS and the HSS.

Whenever it is possible this document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of Diameter base protocol as specified in IETF RFC 6733 [15]. Where this is not possible, extensions to the Diameter base protocol as specified in IETF RFC 6733 [15] are defined within this document.

2 References

The following documents contain provisions, which through reference in this text constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 29.328 "IP Multimedia (IM) Subsystem Sh interface; signalling flows and message contents".

[2] 3GPP TS 33.210 "3G Security; Network Domain Security; IP Network Layer Security".

[3] IETF RFC 2960 "Stream Control Transmission Protocol".

[4] Void.

[5] IETF RFC 2234 "Augmented BNF for syntax specifications".

[6] 3GPP TS 29.229 "Cx and Dx Interfaces based on the Diameter protocol; protocol details".

[7] IETF RFC 3589 "Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5".

[8] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[9] 3GPP TR 33.978 "Security aspects of early IP Multimedia Subsystem (IMS) (Release 6)".

[10] 3GPP TS 29.364 "IMS Application Server Service Data Descriptions for AS interoperability".

[11] 3GPP TS 29.002 "Mobile Application Part (MAP) specification".

[12] IETF RFC 7683: "Diameter Overload Indication Conveyance".

[13] IETF RFC 7944: "Diameter Routing Message Priority".

[14] IETF RFC 8583: "Diameter Load Information Conveyance".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[15] IETF RFC 6733: "Diameter Base Protocol".

[16]] 3GPP TS 29.336: "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications".

3 Definitions, symbols and abbreviations

3.1 Definitions

Refer to IETF RFC 6733 [15] for the definitions of some terms used in this document.

For the purposes of the present document, the following terms and definitions apply.

Attribute-Value Pair: see IETF RFC 6733 [15], it corresponds to an Information Element in a Diameter message.

Server: SIP-server.

User data: user profile data.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization and Accounting
AS	Application Server
ABNF	Augmented Backus-Naur Form
AVP	Attribute-Value Pair
CN	Core Network
DRMP	Diameter Routing Message Priority
DSCP	Differentiated Services Code Point
HSS	Home Subscriber Server
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
NDS	Network Domain Security
RFC	Request For Comment
SCTP	Stream Control Transport Protocol
UCS	Universal Character Set
URL	Uniform Resource Locator
UTF	UCS Transformation Formats

4 General

he Diameter base protocol as specified in IETF RFC 6733 [15] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and event codes specified in clause 6 of this specification. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) are unmodified.

5 Use of the Diameter base protocol

The same clarifications of clause 5 of 3GPP TS 29.229 [6] shall apply to the Sh interface. An exception is that the application identifier for this application is defined in chapter 6.

6 Diameter application for Sh interface

This clause specifies a Diameter application that allows a Diameter server and a Diameter client:

- to download and update transparent and non-transparent user data
- to request and send notifications on changes on user data

The Sh interface protocol is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

The Diameter application identifier assigned to the Sh interface application is 16777217 (allocated by IANA).

6.1 Command-Code values

This clause defines Command-Code values for this Diameter application.

Every command is defined by means of the ABNF syntax (as defined in RFC 2234 [5]), according to the Command Code Format (CCF) specification defined in IETF RFC 6733 [15]. Whenever the definition and use of an AVP is not specified in this document, what is stated in 3GPP TS 29.229 [6] shall apply.

NOTE: As the Diameter commands described in this specification have been defined based on the former specification of the Diameter base protocol, the Vendor-Specific-Application-Id AVP is still listed as a required AVP (an AVP indicated as {AVP}) in the command code format specifications defined in this specification to avoid backward compatibility issues, even if the use of this AVP has been deprecated in the new specification of the Diameter base protocol (IETF RFC 6733 [15]).

The command codes for the Sh interface application are taken from the range allocated by IANA in IETF RFC 3589 [7] as assigned in this specification. For these commands, the Application-ID field shall be set to 16777217 (application identifier of the Sh interface application, allocated by IANA).

The following Command Codes are defined in this specification:

Table 6.1.1: Command-Code values

Command-Name	Abbreviation	Code	Clause
User-Data-Request	UDR	306	6.1.1
User-Data-Answer	UDA	306	6.1.2
Profile-Update-Request	PUR	307	6.1.3
Profile-Update-Answer	PUA	307	6.1.4
Subscribe-Notifications-Request	SNR	308	6.1.5
Subscribe-Notifications-Answer	SNA	308	6.1.6
Push-Notification-Request	PNR	309	6.1.7
Push-Notification-Answer	PNA	309	6.1.8

6.1.1 User-Data-Request (UDR) Command

The User-Data-Request (UDR) command, indicated by the Command-Code field set to 306 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request user data.

Message Format

```
< User-Data -Request> ::=   < Diameter Header: 306, REQ, PXY, 16777217 >
                            < Session-Id >
                            [ DRMP ]
                            { Vendor-Specific-Application-Id }
                                        { Auth-Session-State }
                                        { Origin-Host }
                                        { Origin-Realm }
                                        [ Destination-Host ]
                            { Destination-Realm }
                                        *[ Supported-Features ]
                                        { User-Identity }
                                        [ Wildcarded-Public-Identity ]
                                        [ Wildcarded-IMPU ]
                                        [ Server-Name ]
```

***[Service-Indication]**
***{ Data-Reference }**
***[Identity-Set]**
[Requested-Domain]
[Current-Location]
***[DSAI-Tag]**
[Session-Priority]
[User-Name]
[Requested-Nodes]
[Serving-Node-Indication]
[Pre-paging-Supported]
[Local-Time-Zone-Indication]
[UDR-Flags]
[Call-Reference-Info]
[OC-Supported-Features]
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.2 User-Data-Answer (UDA) Command

The User-Data-Answer (UDA) command, indicated by the Command-Code field set to 306 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the User-Data-Request command. The Experimental-Result AVP may contain one of the values defined in clause 6.2 or in 3GPP TS 29.229 [6].

Message Format

< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777217 >
< Session-Id >
[DRMP]
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
***[Supported-Features]**
[Wildcarded-Public-Identity]
[Wildcarded-IMPU]
[User-Data]
[OC-Supported-Features]
[OC-OLR]
*[Load]
*[AVP]
[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

6.1.3 Profile-Update-Request (PUR) Command

The Profile-Update-Request (PUR) command, indicated by the Command-Code field set to 307 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to update user data in the server.

Message Format

< Profile-Update-Request > ::= < Diameter Header: 307, REQ, PXY, 16777217 >
< Session-Id >
[DRMP]
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }

[Destination-Host]
{ Destination-Realm }
***[Supported-Features]**
{ User-Identity }
[Wildcarded-Public-Identity]
[Wildcarded-IMPU]
[User-Name]
***{** Data-Reference **}**
{ User-Data }
[OC-Supported-Features]
*[AVP]
*[Proxy-Info]
*[Route-Record]

NOTE: More than one Data-Reference AVP may be present in the message only if both the AS and the HSS support the Update-Eff-Enhance feature. How the AS knows whether the HSS supports the Update-Eff-Enhance feature is implementation issue, e.g. the AS can get the information from a previous PUA message.

6.1.4 Profile-Update-Answer (PUA) Command

The Profile-Update-Answer (PUA) command, indicated by the Command-Code field set to 307 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Profile-Update-Request command. The Experimental-Result AVP may contain one of the values defined in clause 6.2 or in 3GPP TS 29.229 [6].

Message Format

< Profile-Update-Answer > ::=< Diameter Header: 307, PXY, 16777217 >
< Session-Id >
[DRMP]
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Wildcarded-Public-Identity]
[Wildcarded-IMPU]
[Repository-Data-ID]
[Data-Reference **]**
*[Supported-Features]
[OC-Supported-Features]
[OC-OLR]
*[Load]
*[AVP]
[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

NOTE: The Data-Reference AVP may be present in the message only if both the AS and the HSS support the Update-Eff-Enhance feature.

6.1.5 Subscribe-Notifications-Request (SNR) Command

The Subscribe-Notifications-Request (SNR) command, indicated by the Command-Code field set to 308 and the 'R' bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request notifications of changes in user data.

Message Format

```
< Subscribe-Notifications-Request > ::=    < Diameter Header: 308, REQ, PXY, 16777217 >
                                             < Session-Id >
                                           [ DRMP ]
                                           { Vendor-Specific-Application-Id }
                                           { Auth-Session-State }
                                           { Origin-Host }
                                           { Origin-Realm }
                                           [ Destination-Host ]
                                    { Destination-Realm }
                                           *[ Supported-Features ]
                                           { User-Identity }
                                           [ Wildcarded-Public-Identity ]
                                           [ Wildcarded-IMPU ]
                                           *[ Service-Indication ]
                                           [ Send-Data-Indication ]
                                           [ Server-Name ]
                                           { Subs-Req-Type }
                                           *{ Data-Reference }
                                           *[ Identity-Set ]
                                           [ Expiry-Time ]
                                           *[ DSAI-Tag ]
                                           [One-Time-Notification]
                                           [ User-Name ]
                                           [ OC-Supported-Features ]
                                    *[ AVP ]
                                    *[ Proxy-Info ]
                                    *[ Route-Record ]
```

6.1.6 Subscribe-Notifications-Answer (SNA) Command

The Subscribe-Notifications-Answer command, indicated by the Command-Code field set to 308 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Subscribe-Notifications-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in clause 6.2 or in 3GPP TS 29.229 [6].

Message Format

```
< Subscribe-Notifications-Answer > ::=    < Diameter Header: 308, PXY, 16777217 >
                                            < Session-Id >
                                          [ DRMP ]
                                          { Vendor-Specific-Application-Id }
                                          { Auth-Session-State }
                                          [ Result-Code ]
                                          [ Experimental-Result ]
                                          { Origin-Host }
                                          { Origin-Realm }
                                          [ Wildcarded-Public-Identity ]
                                          [ Wildcarded-IMPU ]
                                          *[ Supported-Features ]
                                          [ User-Data ]
                                          [ Expiry-Time ]
                                          [ OC-Supported-Features ]
                                          [ OC-OLR ]
                                          *[ Load ]
                                          *[ AVP ]
                                          [ Failed-AVP ]
                                          *[ Proxy-Info ]
                                          *[ Route-Record ]
```

6.1.7 Push-Notification-Request (PNR) Command

The Push-Notification-Request (PNR) command, indicated by the Command-Code field set to 309 and the 'R' bit set in the Command Flags field, is sent by a Diameter server to a Diameter client in order to notify changes in the user data in the server.

Message Format

< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777217 >
< Session-Id >
[DRMP]
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
***[Supported-Features]**
{ User-Identity }
[Wildcarded-Public-Identity]
[Wildcarded-IMPU]
[User-Name]
{ User-Data }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.8 Push-Notifications-Answer (PNA) Command

The Push-Notifications-Answer (PNA) command, indicated by the Command-Code field set to 309 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Push-Notification-Request command. The Experimental-Result AVP may contain one of the values defined in clause 6.2 or in 3GPP TS 29.229 [6].

Message Format

< Push-Notification-Answer > ::=< Diameter Header: 309, PXY, 16777217 >
< Session-Id >
[DRMP]
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
***[Supported-Features]**
*[AVP]
[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

6.2 Result-Code AVP values

This clause defines new result code values that must be supported by all Diameter implementations that conform to this specification. The result codes defined in 3GPP TS 29.229 [6] are also applicable. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and Result-Code AVP shall be absent.

6.2.1 Success

Result codes that fall within the Success category are used to inform a peer that a request has been successfully completed.

No result codes within this category have been defined so far.

6.2.2 Permanent Failures

Errors that fall within the Permanent Failures category are used to inform the peer that the request failed, and should not be attempted again.

6.2.2.1 DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED (5100)

The data received by the AS is not supported or recognized.

6.2.2.2 DIAMETER_ERROR_OPERATION_NOT_ALLOWED (5101)

The requested operation is not allowed for the user

6.2.2.3 DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ (5102)

The requested user data is not allowed to be read.

6.2.2.4 DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED (5103)

The requested user data is not allowed to be modified.

6.2.2.5 DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED (5104)

The requested user data is not allowed to be notified on changes.

6.2.2.6 DIAMETER_ERROR_TOO_MUCH_DATA (5008)

The size of the data pushed to the receiving entity exceeds its capacity. This error code is defined in 3GPP TS 29.229 [6].

6.2.2.7 DIAMETER_ERROR_TRANSPARENT_DATA OUT_OF_SYNC (5105)

The request to update the repository data at the HSS could not be completed because the requested update is based on an out-of-date version of the repository data. That is, the sequence number in the Sh-Update Request message, does not match with the immediate successor of the associated sequence number stored for that repository data at the HSS. It is also used where an AS tries to create a new set of repository data when the identified repository data already exists in the HSS.

6.2.2.8 DIAMETER_ERROR_FEATURE_UNSUPPORTED (5011)

See 3GPP TS 29.229 [6] clause 6.2.2.11.

6.2.2.9 DIAMETER_ERROR_SUBS_DATA_ABSENT (5106)

The Application Server requested to subscribe to changes to Repository Data that is not present in the HSS.

6.2.2.10 DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA (5107)

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

6.2.2.11 DIAMETER_ERROR_DSAI_NOT_AVAILABLE (5108)

The Application Server addressed a DSAI not configured in the HSS.

6.2.2.12 DIAMETER_ERROR_IDENTITIES_DONT_MATCH (5002)

See 3GPP TS 29.229 [6]

6.2.3 Transient Failures

Errors that fall within the transient failures category are those used to inform a peer that the request could not be satisfied at the time that it was received. The request may be able to be satisfied in the future.

6.2.3.1 DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

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

6.2.3.2 DIAMETER_PRIOR_UPDATE_IN_PROGRESS (4101)

The request to update data at the HSS could not be completed for one of the following reasons:

- If the Data Reference is Repository Data, then the related Repository Data is currently being updated by another entity;
- If the Data Reference is other than Repository Data, then the related data is currently being updated.

6.3 AVPs

The following table describes the Diameter AVPs defined for the Sh interface protocol, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted.

Table 6.3.1: Diameter Multimedia Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encrypt**
User-Identity	700	6.3.1	Grouped	M, V				No
MSISDN	701	6.3.2	OctetString	M, V				No
User-Data	702	6.3.3	OctetString	M, V				No
Data-Reference	703	6.3.4	Enumerated	M, V				No
Service-Indication	704	6.3.5	OctetString	M, V				No
Subs-Req-Type	705	6.3.6	Enumerated	M, V				No
Requested-Domain	706	6.3.7	Enumerated	M, V				No
Current-Location	707	6.3.8	Enumerated	M, V				No
Identity-Set	708	6.3.10	Enumerated	V			M	No
Expiry-Time	709	6.3.16	Time	V			M	No
Send-Data-Indication	710	6.3.17	Enumerated	V			M	No
Server-Name	602	6.3.9	UTF8String	M, V				No
Supported-Features	628	6.3.11	Grouped	V	M			No
Feature-List-ID	629	6.3.12	Unsigned32	V			M	No
Feature-List	630	6.3.13	Unsigned32	V			M	No
Supported-Applications	631	6.3.14	Grouped	V			M	No
Public-Identity	601	6.3.15	UTF8String	M, V				No
DSAI-Tag	711	6.3.18	OctetString	M, V				No
Wildcarded-Public-Identity	634	6.3.19	UTF8String	V			M	No
Wildcarded-IMPU	636	6.3.20	UTF8String	V			M	No
Session-Priority	650	6.3.21	Enumerated	V			M	No
One-Time-Notification	712	6.3.22	Enumerated	V			M	No
Requested-Nodes	713	6.3.7A	Unsigned32	V			M	No
Serving-Node-Indication	714	6.3.23	Enumerated	V			M	No
Repository-Data-ID	715	6.3.24	Grouped	V			M	No
Sequence-Number	716	6.3.25	Unsigned32	V			M	No
Pre-paging-Supported	717	6.3.26	Enumerated	V			M	No
Local-Time-Zone-Indication	718	6.3.27	Enumerated	V			M	No
UDR-Flags	719	6.3.28	Unsigned32	V			M	No
Call-Reference-Info	720	6.3.29	Grouped	V			M	No
Call-Reference-Number	721	6.3.30	OctetString	V			M	No
AS-Number	722	6.3.31	OctetString	V			M	No
OC-Supported-Features	621 NOTE 3	6.3.32	Grouped				M, V	No
OC-OLR	623 NOTE 3	6.3.33	Grouped				M, V	No
DRMP	301 NOTE 4	6.3.34	Enumerated				M, V	No
Load	NOTE 5	6.3.35	Grouped				M, V	No

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see 3GPP TS 29.229 [6].
NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.
NOTE 3: The value of these attributes is defined in IETF RFC 7683 [12].
NOTE 4: The value of this attribute is defined in IETF RFC 7944 [13].
NOTE 5: The value of this attribute is defined in IETF RFC 8583 [14].

The following table specifies the Diameter AVPs re-used by the Sh interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within Sh.

Table 6.3/2: Sh re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
External-Identifier	3GPP TS 29.336 [16]		Must set
NOTE 1: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies.			
NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.			

6.3.1 User-Identity AVP

The User-Identity AVP is of type Grouped. This AVP contains either a Public- Identity AVP or an MSISDN AVP or an External-Identifier AVP.

AVP format

User-Identity ::= <AVP header: 700 10415>

[Public-Identity]

[MSISDN]

[External-Identifier]

*[AVP]

6.3.2 MSISDN AVP

The MSISDN AVP is of type OctetString. This AVP contains an MSISDN, in international number format as described in ITU-T Rec E.164 [8], encoded as a TBCD-string, i.e. digits from 0 through 9 are encoded 0000 to 1001; 1111 is used as a filler when there is an odd number of digits; bits 8 to 5 of octet n encode digit 2n; bits 4 to 1 of octet n encode digit 2(n-1)+1.

6.3.3 User-Data AVP

The User-Data AVP is of type OctetString. This AVP contains the user data requested in the UDR/UDA, SNR/SNA and PNR/PNA operations and the data to be modified in the PUR/PUA operation. The exact content and format of this AVP is described in 3GPP TS 29.328 [1] Annex C as Sh-Data.

6.3.4 Data-Reference AVP

The Data-Reference AVP is of type Enumerated, and indicates the type of the requested user data in the operation UDR and SNR. Its exact values and meaning is defined in 3GPP TS 29.328 [1]. The following values are defined (more details are given in 3GPP TS 29.328 [1]):

RepositoryData (0)

IMSPublicIdentity (10)

IMSUserState (11)

S-CSCFName (12)

InitialFilterCriteria (13)

This value is used to request initial filter criteria relevant to the requesting AS

LocationInformation (14)

UserState (15)

ChargingInformation (16)

MSISDN (17)

PSIActivation (18)

DSAI (19)

ServiceLevelTraceInfo (21)

IPAddressSecureBindingInformation (22)

ServicePriorityLevel (23)

SMSRegistrationInfo (24)

UEReachabilityForIP (25)

TADSinformation (26)

STN-SR (27)

UE-SRVCC-Capability (28)

ExtendedPriority (29)

CSRN (30)

ReferenceLocationInformation (31)

IMSI (32)

IMSPrivateUserIdentity (33)

NOTE: Value 20 is reserved.

6.3.5 Service-Indication AVP

The Service-Indication AVP is of type OctetString. This AVP contains the Service Indication that identifies a service or a set of services in an AS and the related repository data in the HSS. Standardized values of Service-Indication identifying a standardized service or set of services in the AS and standardized format of the related repository data are defined in 3GPP TS 29.364 [10].

6.3.6 Subs-Req-Type AVP

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

Subscribe (0)

This value is used by an AS to subscribe to notifications of changes in data.

Unsubscribe (1)

This value is used by an AS to unsubscribe to notifications of changes in data.

6.3.7 Requested-Domain AVP

The Requested-Domain AVP is of type Enumerated, and indicates the access domain for which certain data (e.g. user state) are requested. The following values are defined:

CS-Domain (0)

The requested data apply to the CS domain.

PS-Domain (1)

The requested data apply to the PS domain.

6.3.7A Requested-Nodes AVP

The Requested-Nodes AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 6.3.7A/1:

Table 6.3.7A/1: Requested-Nodes

Bit	Name	Description
0	MME	The requested data apply to the MME
1	SGSN	The requested data apply to the SGSN
2	3GPP-AAA-SERVER-TWAN	The requested data apply to the 3GPP AAA Server for TWAN
3	AMF	The requested data apply to the AMF (for 3GPP access)

6.3.8 Current-Location AVP

The Current-Location AVP is of type Enumerated, and indicates whether an active location retrieval has to be initiated or not:

DoNotNeedInitiateActiveLocationRetrieval (0)

The request indicates that the initiation of an active location retrieval is not required.

InitiateActiveLocationRetrieval (1)

It is requested that an active location retrieval is initiated.

6.3.9 Server-Name AVP

The Server-Name contains a SIP-URL used to identify an AS. See 3GPP TS 29.229 [6] for further description of this AVP.

6.3.10 Identity-Set AVP

The Identity-Set AVP is of type Enumerated and indicates the requested set of IMS Public Identities. The following values are defined:

ALL_IDENTITIES (0)

REGISTERED_IDENTITIES (1)

IMPLICIT_IDENTITIES (2)

ALIAS_IDENTITIES (3)

6.3.11 Supported-Features AVP

See 3GPP TS 29.229 [6] clause 6.3.29.

6.3.12 Feature-List-ID AVP

See 3GPP TS 29.229 [6] clause 6.3.30.

6.3.13 Feature-List AVP

See 3GPP TS 29.229 [6] clause 6.3.31.

6.3.14 Supported-Applications AVP

See 3GPP TS 29.229 [6] clause 6.3.32.

6.3.15 Public-Identity AVP

The Public-Identity AVP contains a Public User Identity. See 3GPP TS 29.229 [6] for the definition of this AVP.

6.3.16 Expiry-Time AVP

The Expiry-Time AVP is of type Time. This AVP contains the expiry time of subscriptions to notifications in the HSS.

6.3.17 Send-Data-Indication AVP

The Send-Data-Indication AVP is of type Enumerated. If present it indicates that the sender requests the User-Data. The following values are defined:

USER_DATA_NOT_REQUESTED (0)

USER_DATA_REQUESTED (1)

6.3.18 DSAI-Tag AVP

The DSAI-Tag AVP is of type OctetString. This AVP contains the DSAI-Tag identifying the instance of the Dynamic Service Activation Information being accessed for the Public Identity.

6.3.19 Wildcarded-Public-Identity AVP

See 3GPP TS 29.229 [6] clause 6.3.35 for the definition of theWildcarded-Public-Identity AVP. This AVP only contains a Wildcarded PSI over Sh interface.

6.3.20 Wildcarded-IMPU AVP

See 3GPP TS 29.229 [6] clause 6.3.43.

6.3.21 Session-Priority AVP

See 3GPP TS 29.229 [6] clause 6.3.56.

6.3.22 One-Time-Notification AVP

The One-Time-Notification AVP is of type Enumerated. If present it indicates that the sender requests to be notified only one time. The following values are defined:

ONE_TIME_NOTIFICATION_REQUESTED (0)

This AVP is only applicable to UE reachability for IP (25)

6.3.23 Serving-Node-Indication AVP

The Serving-Node-Indication AVP is of type Enumerated. If present it indicates that the sender does not require any location information other than the Serving Node Addresses/Identities requested (e.g. MME name, VLR number). Other location information (e.g. Global Cell ID, Tracking Area ID) may be absent. The following values are defined:

ONLY_SERVING_NODES_REQUIRED (0)

6.3.24 Repository-Data-ID AVP

The Repository-Data-ID AVP is of type Grouped. This AVP shall contain a Service-Indication AVP and a Sequence-Number AVP.

AVP format

Repository-Data-ID ::= <AVP header: 715 10415>

{Service-Indication}

{Sequence-Number}

*[AVP]

6.3.25 Sequence-Number AVP

The Sequence-Number AVP is of type Unsigned32. This AVP contains a number associated to a repository data.

6.3.26 Pre-paging-Supported AVP

The Pre-paging-Supported AVP is of type Enumerated. It indicates whether the sender supports pre-paging or not. The following values are defined:

PREPAGING_NOT_SUPPORTED (0)

PREPAGING_SUPPORTED (1)

If this AVP is not present in the command, the default value is PREPAGING_NOT_SUPPORTED (0).

6.3.27 Local-Time-Zone-Indication AVP

The Local-Time-Zone-Indication AVP is of type Enumerated. If present it indicates that the Local Time Zone information (time zone and daylight saving time) of the visited network where the UE is attached is requested with or without other location information. The following values are defined:

ONLY_LOCAL_TIME_ZONE_REQUESTED (0)

LOCAL_TIME_ZONE_WITH_LOCATION_INFO_REQUESTED (1)

6.3.28 UDR-Flags

The UDR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in 3GPP TS 29.328 [1].

Table 6.3.28/1: UDR-Flags

Bit	Name
0	Location-Information-EPS-Supported
1	RAT-Type-Requested
NOTE:	Bits not defined in this table shall be cleared by the sender of the request and discarded by the receiver of the request.

6.3.29 Call-Reference-Info AVP

The Call-Reference-Info AVP is of type Grouped. This AVP shall contain a Call-Reference-Number AVP and an AS-Number AVP.

AVP format

Call-Reference-Info ::= <AVP header: 720 10415>

{Call-Reference-Number}

{AS-Number}

*[AVP]

6.3.30 Call-Reference-Number AVP

The Call-Reference-Number AVP is of type OctetString. The exact content and format of this AVP is described in 3GPP TS 29.002 [11].

6.3.31 AS-Number AVP

The AS-Number AVP is of type OctetString. The exact content and format of this AVP corresponds to the gmsc-address parameter described in 3GPP TS 29.002 [11].

6.3.32 OC-Supported-Features

The OC-Supported-Features AVP is of type Grouped and it is defined in IETF RFC 7683 [12]. This AVP is used to support Diameter overload control mechanism.

6.3.33 OC-OLR

The OC-OLR AVP is of type Grouped and it is defined in IETF RFC 7683 [12]. This AVP is used to support Diameter overload control mechanism.

6.3.34 DRMP AVP

The DRMP AVP is of type Enumerated and it is defined in IETF RFC 7944 [13]. This AVP allows the HSS/SLF and the AS/OSA SCS to indicate the relative priority of Diameter messages. The DRMP AVP may be used to set the DSCP marking for transport of the associated Diameter message.

6.3.35 Load

The Load AVP is of type Grouped and it is defined in IETF RFC 8583 [14]. This AVP is used to support the Diameter load control mechanism.

6.4 Use of namespaces

This clause contains the namespaces that have either been created in this specification, or the values assigned to existing namespaces managed by IANA.

6.4.1 AVP codes

This specification assigns the AVP values from the AVP Code namespace managed by 3GPP for its Diameter vendor-specific applications. See clause 6.3 for the assignment of the namespace in this specification.

6.4.2 Experimental-Result-Code AVP values

This specification has assigned Experimental-Result-Code AVP values 4100-4101 and 5100-5105. See clause 6.2.

6.4.3 Command Code values

This specification assigns the values 306-309 from the range allocated by IANA to 3GPP in IETF RFC 3589 [7].

6.4.4 Application-ID value

IANA has allocated the value 16777217 for the 3GPP Sh interface application.

7 Special Requirements

7.1 Version Control

The version control mechanisms specified in 3GPP TS 29.229 [6] clauses 7.1, 7.2 and 7.3 apply to this specification.

The following table of features shall apply to the Sh interface.

Table 7.1.1: Features of feature list 1 used in Sh

Feature bit	Feature	M/O	Description
0	Notif-Eff	M	This feature is applicable to the UDR/UDA, SNR/SNA and PNR/PNA command pairs. It requires support in both the HSS and the AS. If multiple subscriptions to notifications are associated with a Public User Identity, the HSS may combine the notifications for multiple Data References and/or Service Indications and/or Identity Sets into a single Push-Notification-Request message. The User-Data-Request / Answer and the Subscribe-Notifications-Request / Answer allow multiple Data References, Service Indications and Identity Sets. The User-Data-Answer and Push-Notification-Request allow combining multiple DataReference items resulting in the User Data AVP including a single XML document with the separable XML clauses populated.
1	Update-Eff	O	This feature is applicable to the PUR/PUA commands. If both the HSS and the AS support this feature, a PUR command where the Data reference type is Repository Data, may contain an XML document with several Repository Data instances.
2	Update-Eff-Enhance	O	This feature is an enhancement of the Update-Eff feature and requires Update-Eff is supported. It is applicable to the PUR/PUA commands. If both the HSS and the AS support this feature, a PUR command may contain an XML document with several Data instances.
3	Additional-MSISDN	O	This feature is applicable to UDR/UDA commands. It requires support in both HSS and AS. If enabled, it extends the information returned with DataReference=17. Instead of returning only MSISDN, it includes ExtendedMSISDN. See 3GPP TS 29.328 [1] for more information.
Feature bit: The order number of the bit within the Supported-Features AVP, e.g. "1". Feature: A short name that can be used to refer to the bit and to the feature, e.g. "MOM". M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O"). Description: A clear textual description of the feature.			

The following table shall apply to the Sh interface; the column Application identifier lists the used application identifiers on Sh and 3GPP.

Table 7.1.2: Application identifiers used in Sh

Application identifier	First applied
16777217	3GPP Rel-5

Annex A (informative): Change history

Date	TSG #	TSG Doc.	CR#	Rev	Subject/Comment	Out
June 2002	CN#16	NP-020266			Version 2.0.1 present in CN#16 for approval	5.0.0
Sep 2002	CN#17	NP-020450	2	1	Cancellation of subscriptions to notifications	5.1.0
Sep 2002	CN#17	NP-020450	3	1	Addition of AVPs to User-Data-Request	5.1.0
Dec 2002	CN#18	NP-020592	6	-	Error handling in HSS when being updated with too much data	5.2.0
Mar 2003	CN#19	NP-030102	005	1	Initial Filter Criteria	5.3.0
Mar 2003	CN#19	NP-030102	007	2	Update after Diameter has become RFC	5.3.0
Mar 2003	CN#19	NP-030102	011	-	Missing code-point in Data-Reference AVP	5.3.0
Mar 2003	CN#19	NP-030102	013	-	Registration State Alignment	5.3.0
Mar 2003	CN#19	NP-030102	008	-	Correction of the Application Server Identification type for Initial Filter Criteria usage	5.3.0
Mar 2003	CN#19	NP-030102	009	-	Clarification on Sh interface for charging purposes	5.3.0
Jun 2003	CN#20	NP-030216	014	1	Co-ordination of Update of Repository Data	5.4.0
Jun 2003	CN#20	NP-030216	015	1	Command code correction for UDA plus editorial corrections	5.4.0
Jun 2003	CN#20	NP-030216	016	-	Correction on Current-Location AVP values	5.4.0
Jun 2003	CN#20	NP-030216	018	-	Correction to the use of User-Identity	5.4.0
Jun 2003	CN#20	NP-030216	019	1	Correction to the use of Data-Reference	5.4.0
Dec 2003	CN#22				Editorial changes in application IDs and references [4] and [7].	5.4.1
Mar 2004	CN#23	NP-040135	031	1	Add MSISDN to set of Data that may be downloaded	5.5.0
Mar 2004	CN#23	NP-040055	032	2	Introduction of 'Identity-Set' AVP	6.0.0
Jun 2004	CN#24	NP-040216	037	-	Correction to description of Data Reference AVP value 10	6.1.0
Jun 2004	CN#24	NP-040216	035	1	Correction of reference for definition of MSISDN	6.1.0
Sep 2004	CN#25	NP-040394	043	-	Incorrect Data-Reference AVP in Subscriber Notification Answer Command	6.2.0
Sep 2004	CN#25	NP-040395	046	1	Application version control	6.2.0
Sep 2004	CN#25	NP-040394	041	1	Public-Identity is unspecified for the Sh interface	6.2.0
Sep 2004	CN#25	NP-040395	045	1	Single Public_Identity required in Grouped User-Identity AVP	6.2.0
Sep 2004	CN#25	NP-040394	049	-	Correction of the Application-Id code	6.2.0
Sep 2004	CN#25	NP-040412	051	1	Re-numbering of 3GPP specific AVP codes	6.2.0
Dec 2004	CN#26	NP-040578	053	-	Sh ABNF corrections	6.3.0
Mar 2005	CN#27	NP-050031	057	1	Introduction of Failed AVP	6.4.0
Mar 2005	CN#27	NP-050031	064	-	Sh-Update needs to include Data-Reference to be future proof	6.4.0
Jun 2005	CT#28	CP-050216	069	-	Sh UDR correction	6.5.0
Jun 2005	CT#28	CP-050087	070	-	Correction of references	6.5.0
Jun 2005	CT#28	CP-050087	071	1	Corrections to message parameters	6.5.0
Jun 2005	CT#28	CP-050087	072	1	Miscellaneous Corrections	6.5.0
Jun 2005	CT#28	CP-050216	074	-	Correction to allow realm based routing	6.5.0
Sep 2005	CT#29	CP-050424	075	-	Identity-Set correction	6.6.0
Sep 2005	CT#29	CP-050422	095	1	State the condition for encryption of the Data Reference	6.6.0
Sep 2005	CT#29	CP-050423	097	1	Early IMS Security based protection for the Ut interface	6.6.0
Dec 2005	CT#30	CP-050625	098	3	Notification & Query Efficiency	7.0.0
Dec 2005	CT#30	CP-050625	099	1	Management of subscriptions	7.0.0
Mar 2006	CT#31	CP-060084	0100	1	User-Data in the response to Sh-Subs-Notif	7.1.0
Mar 2006	CT#31	CP-060084	0101	3	New error indications for the Sh-Subs-Notif procedure	7.1.0
Jun 2006	CT#32	CP-060319	0105	2	Sh interface efficiency improvement	7.2.0
Sep 2006	CT#33	CP-060417	0107	2	Introduction of Activation State Information for IMS (DSAI)	7.3.0
Sep 2006	CT#33	CP-060417	0108	-	Addition of AVPs in SNR and SNA	7.3.0
Sep 2006	CT#33	CP-060417	0110	1	Public User Identity Grouping Information	7.3.0
Sep 2006	CT#33	CP-060405	0112	-	Missing Data Reference value	7.3.0
Sep 2006	CT#33	CP-060417	0113	1	Errors to be sent in response to Sh-Notif	7.3.0
Sep 2007	CT#37	CP-070527	0118	-	Define User-Data AVP	7.4.0
Sep 2007	CT#37	CP-070527	0119	1	Wildcarded PSI as key in the Sh Interface	7.4.0
Nov 2007	CT#38	CP-070743	0120	-	ABNF correction for UDR and SNR	7.5.0
Nov 2007	CT#38	CP-070743	0121	1	PNR for Subscriptions to Notifications for all Identity Sets	7.5.0
Mar 2008	CT#39	CP-080019	0122	-	Wildcarded Public User Identities	8.0.0
Jun 2008	CT#40	CP-080267	0123	1	DSAI Corrections	8.1.0
Jun 2008	CT#40	CP-080702	0130	1	Service Indication for standardized services	8.2.0
Jun 2008	CT#40	CP-080883	0132	1	Correction of Identity-Set AVP	8.2.0
Mar 2009	CT#43	CP-090042	0134	1	AliasesRepositoryData removal	8.3.0
Jun 2009	CT#44	CP-090305	0136		Missing data-reference for GIBA	8.4.0
Dec 2009	CT#46	CP-090778	0138		Session-Priority AVP	8.5.0
Dec 2009	CT#46				Upgraded unchanged from Rel-8	9.0.0
Mar 2010	CT#47	CP-100033	0143	1	IP-SM-GW UE reachability handling over Sh	9.1.0
Mar 2010	CT#47	CP-100048	0144	1	Sh handling of T-ADS	9.1.0
Mar 2010	CT#47	CP-100206	0148	3	EPS Subcsriber State and Location Information Request	9.1.0
Jun 2010	CT#48	CP-100275	0149		EPS state and location retrieval	9.2.0
Jun 2010	CT#48	CP-100279	0154	1		9.2.0
Sep 2010	CT#49	CP-100447	0157	1	Correction to the Value of Data-Reference AVP	9.3.0
Sep 2010	CT#49	CP-100454	0160	1	Correction on Requested-Domain	9.3.0
Sep 2010	CT#49	CP-100466	0158	2	Usage of IMSI and IMPI for user identification over Sh	10.0.0
Sep 2010	CT#49	CP-100466	0159	3	Location data including only serving node address	10.0.0

Sep 2010	CT#49	CP-100466	0163	3	Update-Eff feature	10.0.0
Dec 2010	CT#50	CP-100699	0164	2	Enhanced SRVCC	10.1.0
Mar 2011	CT#51	CP-110257	0168	2	MPS over Sh	10.2.0
Mar 2011	CT#51	CP-110075	0170	2	Retrieval of CSRN from HSS	10.2.0
Jun 2011	CT#52	CP-110370	0175	1	Pre-paging Support Indicator for CSRN	10.3.0
Jun 2011	CT#52	CP-110370	0176	1	Clarification on Notif-Eff description for SNR/SNA	10.3.0
Jun 2011	CT#52	CP-110370	0177	-	Missing Repository-Data-ID AVP in PUA	10.3.0
Jun 2011	CT#52	CP-110383	0173	2	Reference Location over Sh interface	11.0.0
Dec 2011	CT#54	CP-110781	0189	-	Correction on Wildcarded Public Identity	11.1.0
Mar 2012	CT#55	CP-120035	0194	2	Update of Multiple Data Instances in Sh-Update	11.2.0
Jun 2012	CT#56	CP-120240	0195	3	Local Time for NPLI	11.3.0
Sep 2012	CT#57	CP-120481	0197		A-MSISDN handling over Sh	11.4.0
Sep 2012	CT#57	CP-120481	0198	1	Local Time Zone	11.4.0
Dec 2012	CT#58	CP-120743	0202	1	EPS LocationInformation Support	11.5.0
Mar 2013	CT#59	CP-130020	0208	1	PS Location Info request with RAT-type	11.6.0
Mar 2013	CT#59	CP-130020	0210	1	Pre-paging-Supported and Local-Time-Zone-Indication AVPs	11.6.0
Mar 2013	CT#59	CP-130031	0200	1	Sh IMSI retrieval	12.0.0
Jun 2013	CT#60	CP-130374	0211	1	MTRR on Sh	12.1.0
Mar 2014	CT#63	CP-140027	0214	1	Multiple notification due to the Update-Eff feature	12.2.0
Jun 2014	CT#64	CP-140262	0217	-	Private User Identity retrieval	12.3.0
Jun 2014	CT#64	CP-140262	0218	-	UE Reachability for IP	12.3.0
Sep 2014	CT#65	CP-140515	0219	-	Session-Priority reference	12.4.0
Sep 2014	CT#65	CP-140509	0220	1	Diameter Overload Control Over Sh	12.4.0
Dec 2014	CT#66	CP-140773	0222	-	M-bit clarification	12.5.0
Dec 2014	CT#66	CP-140779	0223	-	Retrieval of TWAN-Id over Sh	12.5.0
Dec 2014	CT#66	CP-140790	0224	-	DOIC reference update	12.5.0
Dec 2015	CT#70	CP-150759	0226	1	Update reference to DOIC new IETF RFC	12.6.0
Dec 2015	CT#70	CP-150849	0227	4	Support of the DRMP AVP over Sh/Dh	13.0.0
2016-09	CT#73	CP-160431	0228	1	Request to update data while a previous update request is in progress	14.0.0
2016-12	CT#74	CP-160649	0236	1	RAT type included in EPS location information	14.1.0
2016-12	CT#74	CP-160681	0237	1	Load Control	14.1.0
2016-12	CT#74	CP-160664	0239	1	Correction to change IETF drmp draft version to official RFC 7944	14.1.0
2017-03	CT#75	CP-170035	0241	-	Notif-Eff feature description correction	14.2.0
2017-03	CT#75	CP-170035	0245	1	UDR flag description	14.2.0
2017-03	CT#75	CP-170048	0243	1	Update of reference for the Diameter base protocol	14.2.0
2017-03	CT#75	CP-170048	0244	-	Cardinality of the Failed-AVP AVP in answer	14.2.0
2017-06	CT#76	CP-171018	0248	1	Support for signaling transport level packet marking	14.3.0
2017-06	CT#76	CP-171040	0246	1	External Identifier on Sh	15.0.0
2018-06	CT#80	CP-181131	0249	-	Requested Node AMF	15.1.0
2019-09	CT#85	CP-192094	0251	2	draft-ietf-dime-load published as RFC 8583	15.2.0

History

Document history		
V15.1.0	July 2018	Publication
V15.2.0	October 2019	Publication