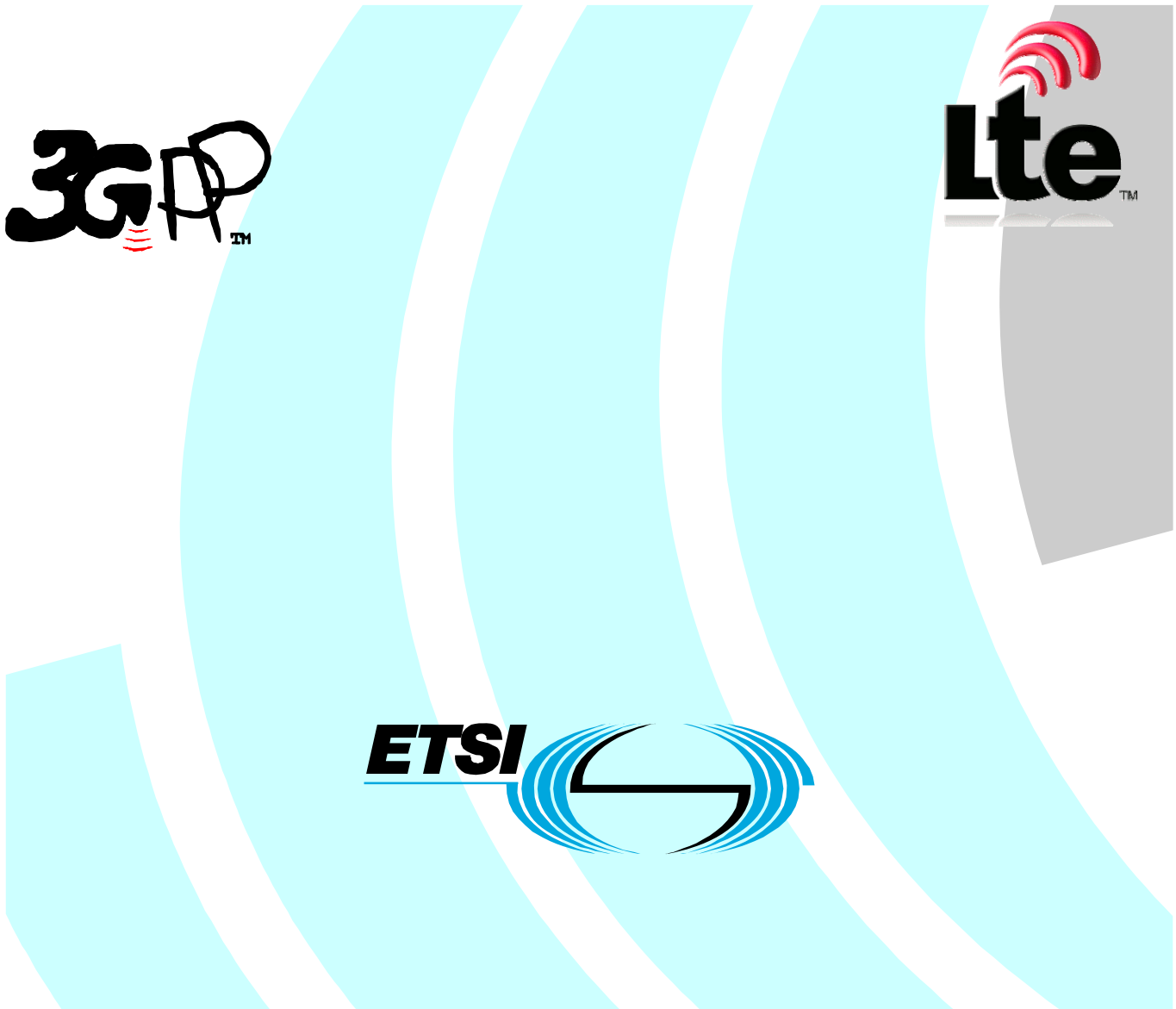
ETSI TS 129 329 V9.4.0 (2011-01)

Technical Specification

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 9.4.0 Release 9)



Reference
RTS/TSGC-0429329v940

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

IPRs essential or potentially essential to the present document 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 (http://webapp.etsi.org/IPR/home.asp).

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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

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

Contents

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 Diameter.

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. Where this is not possible, extensions to Diameter 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] IETF RFC 3588 "Diameter Base Protocol"

[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 "

3 Definitions, symbols and abbreviations

3.1 Definitions

Refer to IETF RFC 3588 [4] 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 3588 [4], 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
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

The Diameter Base Protocol as specified in IETF RFC 3588 [4] 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 section 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 section 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 rules in IETF RFC 3588 [4]. 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.

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	Section
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 >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                *[ Supported-Features ]
                                { User-Identity }
                                [ Wildcarded-PSI ]
                                [ Wildcarded-IMPU ]
                                [ Server-Name ]
                                *[ Service-Indication ]
                                *{ Data-Reference }
                                *[ Identity-Set ]
                                [ Requested-Domain ]
                                [ Current-Location ]
                                *[ DSAI-Tag ]
                                [ Session-Priority ]
                                [ Requested-Nodes ]
                                [ User-Name ]
                                *[ 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 section 6.2 or in 3GPP TS 29.229 [6].

Message Format

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

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 section 6.2 or in 3GPP TS 29.229 [6].

Message Format

< Profile-Update-Answer > ::=< Diameter Header: 307, PXY, 16777217 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Wildcarded-PSI]
[Wildcarded-IMPU]
*[Supported-Features]

*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

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 >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
***[Supported-Features]**
{ User-Identity }
[Wildcarded-PSI]
[Wildcarded-IMPU]
***[Service-Indication]**
[Send-Data-Indication]
[Server-Name]
{ Subs-Req-Type }
***{ Data-Reference }**
***[Identity-Set]**
[Expiry-Time]
***[DSAI-Tag]**
[One-Time-Notification]
*[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 section 6.2 or in 3GPP TS 29.229 [6].

Message Format

< Subscribe-Notifications-Answer > ::= < Diameter Header: 308, PXY, 16777217 >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
[Result-Code]
[Experimental-Result]
{ Origin-Host }
{ Origin-Realm }
[Wildcarded-PSI]
[Wildcarded-IMPU]
***[Supported-Features]**
[User-Data]
[Expiry-Time]
*[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 >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
***[Supported-Features]**
{ User-Identity }
[Wildcarded-PSI]
[Wildcarded-IMPU]
{ 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 section 6.2 or in 3GPP TS 29.229 [6].

Message Format

< Push-Notification-Answer > ::=< Diameter Header: 309, PXY, 16777217 >
< Session-Id >
{ 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 section 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.

6.2.3 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 the repository data at the HSS could not be completed because the related repository data is currently being updated by another entity.

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**	**Section 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-PSI	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
Note: 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].								

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.

AVP format

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

[Public-Identity]

[MSISDN]

*[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)

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

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-PSI AVP

See 3GPP TS 29.229 [6] clause 6.3.35.

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 6.3.15.

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 (23)

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 section 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 section 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 and SNR / SNA command pairs. If both the HSS and the AS support this feature and if multiple subscriptions to notifications are associated with a Public User Identity, the HSS may combine the notifications for multiple Data References and Service Indications into a single notification message. Similarly the User Data Request / Answer will allow multiple data references and Service Indications and Identity Sets. The User Data Answer will be able to combine DataReference items resulting in the User Data Answer contents including a single XML document with the separable XML sections populated. Additionally, this feature allows concurrent subscriptions to different Identity Sets.
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	In	Out
June 2002	CN#16	NP-020266			Version 2.0.1 present in CN#16 for approval	2.0.1	5.0.0
Sep 2002	CN#17	NP-020450	2	1	Cancellation of subscriptions to notifications	5.0.0	5.1.0
Sep 2002	CN#17	NP-020450	3	1	Addition of AVPs to User-Data-Request	5.0.0	5.1.0
Dec 2002	CN#18	NP-020592	6	-	Error handling in HSS when being updated with too much data	5.1.0	5.2.0
Mar 2003	CN#19	NP-030102	005	1	Initial Filter Criteria	5.2.0	5.3.0
Mar 2003	CN#19	NP-030102	007	2	Update after Diameter has become RFC	5.2.0	5.3.0
Mar 2003	CN#19	NP-030102	011	-	Missing code-point in Data-Reference AVP	5.2.0	5.3.0
Mar 2003	CN#19	NP-030102	013	-	Registration State Alignment	5.2.0	5.3.0
Mar 2003	CN#19	NP-030102	008	-	Correction of the Application Server Identification type for Initial Filter Criteria usage	5.2.0	5.3.0
Mar 2003	CN#19	NP-030102	009	-	Clarification on Sh interface for charging purposes	5.2.0	5.3.0
Jun 2003	CN#20	NP-030216	014	1	Co-ordination of Update of Repository Data	5.3.0	5.4.0
Jun 2003	CN#20	NP-030216	015	1	Command code correction for UDA plus editorial corrections	5.3.0	5.4.0
Jun 2003	CN#20	NP-030216	016	-	Correction on Current-Location AVP values	5.3.0	5.4.0
Jun 2003	CN#20	NP-030216	018	-	Correction to the use of User-Identity	5.3.0	5.4.0
Jun 2003	CN#20	NP-030216	019	1	Correction to the use of Data-Reference	5.3.0	5.4.0
Dec 2003	CN#22				Editorial changes in application IDs and references [4] and [7].	5.4.0	5.4.1
Mar 2004	CN#23	NP-040135	031	1	Add MSISDN to set of Data that may be downloaded	5.4.1	5.5.0
Mar 2004	CN#23	NP-040055	032	2	Introduction of 'Identity-Set' AVP	5.5.0	6.0.0
Jun 2004	CN#24	NP-040216	037	-	Correction to description of Data Reference AVP value 10	6.0.0	6.1.0
Jun 2004	CN#24	NP-040216	035	1	Correction of reference for definition of MSISDN	6.0.0	6.1.0
Sep 2004	CN#25	NP-040394	043	-	Incorrect Data-Reference AVP in Subscriber Notification Answer Command	6.1.0	6.2.0
Sep 2004	CN#25	NP-040395	046	1	Application version control	6.1.0	6.2.0
Sep 2004	CN#25	NP-040394	041	1	Public-Identity is unspecified for the Sh interface	6.1.0	6.2.0
Sep 2004	CN#25	NP-040395	045	1	Single Public_Identity required in Grouped User-Identity AVP	6.1.0	6.2.0
Sep 2004	CN#25	NP-040394	049	-	Correction of the Application-Id code	6.1.0	6.2.0
Sep 2004	CN#25	NP-040412	051	1	Re-numbering of 3GPP specific AVP codes	6.1.0	6.2.0
Dec 2004	CN#26	NP-040578	053	-	Sh ABNF corrections	6.2.0	6.3.0
Mar 2005	CN#27	NP-050031	057	1	Introduction of Failed AVP	6.3.0	6.4.0
Mar 2005	CN#27	NP-050031	064	-	Sh-Update needs to include Data-Reference to be future proof	6.3.0	6.4.0
Jun 2005	CT#28	CP-050216	069	-	Sh UDR correction	6.4.0	6.5.0
Jun 2005	CT#28	CP-050087	070	-	Correction of references	6.4.0	6.5.0
Jun 2005	CT#28	CP-050087	071	1	Corrections to message parameters	6.4.0	6.5.0
Jun 2005	CT#28	CP-050087	072	1	Miscellaneous Corrections	6.4.0	6.5.0
Jun 2005	CT#28	CP-050216	074	-	Correction to allow realm based routing	6.4.0	6.5.0
Sep 2005	CT#29	CP-050424	075	-	Identity-Set correction	6.5.0	6.6.0
Sep 2005	CT#29	CP-050422	095	1	State the condition for encryption of the Data Reference	6.5.0	6.6.0
Sep 2005	CT#29	CP-050423	097	1	Early IMS Security based protection for the Ut interface	6.5.0	6.6.0
Dec 2005	CT#30	CP-050625	098	3	Notification & Query Efficiency	6.6.0	7.0.0
Dec 2005	CT#30	CP-050625	099	1	Management of subscriptions	6.6.0	7.0.0
Mar 2006	CT#31	CP-060084	0100	1	User-Data in the response to Sh-Subs-Notif	7.0.0	7.1.0
Mar 2006	CT#31	CP-060084	0101	3	New error indications for the Sh-Subs-Notif procedure	7.0.0	7.1.0
Jun 2006	CT#32	CP-060319	0105	2	Sh interface efficiency improvement	7.1.0	7.2.0
Sep 2006	CT#33	CP-060417	0107	2	Introduction of Activation State Information for IMS (DSAI)	7.2.0	7.3.0
Sep 2006	CT#33	CP-060417	0108	-	Addition of AVPs in SNR and SNA	7.2.0	7.3.0
Sep 2006	CT#33	CP-060417	0110	1	Public User Identity Grouping Information	7.2.0	7.3.0
Sep 2006	CT#33	CP-060405	0112	-	Missing Data Reference value	7.2.0	7.3.0
Sep 2006	CT#33	CP-060417	0113	1	Errors to be sent in response to Sh-Notif	7.2.0	7.3.0
Sep 2007	CT#37	CP-070527	0118	-	Define User-Data AVP	7.3.0	7.4.0
Sep 2007	CT#37	CP-070527	0119	1	Wildcarded PSI as key in the Sh Interface	7.3.0	7.4.0
Nov 2007	CT#38	CP-070743	0120	-	ABNF correction for UDR and SNR	7.4.0	7.5.0
Nov 2007	CT#38	CP-070743	0121	1	PNR for Subscriptions to Notifications for all Identity Sets	7.4.0	7.5.0
Mar 2008	CT#39	CP-080019	0122	-	Wildcarded Public User Identities	7.8.0	8.0.0
Jun 2008	CT#40	CP-080267	0123	1	DSAI Corrections	8.0.0	8.1.0
Jun 2008	CT#40	CP-080702	0130	1	Service Indication for standardized services	8.1.0	8.2.0
Jun 2008	CT#40	CP-080883	0132	1	Correction of Identity-Set AVP	8.1.0	8.2.0
Mar 2009	CT#43	CP-090042	0134	1	AliasesRepositoryData removal	8.2.0	8.3.0
Jun 2009	CT#44	CP-090305	0136		Missing data-reference for GIBA	8.3.0	8.4.0
Dec 2009	CT#46	CP-090778	0138		Session-Priority AVP	8.4.0	8.5.0
Dec 2009	CT#46				Upgraded unchanged from Rel-8	8.5.0	9.0.0
Mar 2010	CT#47	CP-100033	0143	1	IP-SM-GW UE reachability handling over Sh	9.0.0	9.1.0
Mar 2010	CT#47	CP-100048	0144	1	Sh handling of T-ADS	9.0.0	9.1.0
Mar 2010	CT#47	CP-100206	0148	3	EPS Subcsriber State and Location Information Request	9.0.0	9.1.0

Jun 2010	CT#48	CP-100275	0149		EPS state and location retrieval	9.1.0	9.2.0
Jun 2010	CT#48	CP-100279	0154	1		9.1.0	9.2.0
Sep 2010	CT#49	CP-100447	0157	1	Correction to the Value of Data-Reference AVP	9.2.0	9.3.0
Sep 2010	CT#49	CP-100454	0160	1	Correction on Requested-Domain	9.2.0	9.3.0
Dec 2010	CT#50	CP-100671	0162	3	C-MSISDN over Sh	9.3.0	9.4.0

History

Document history		
V9.0.0	January 2010	Publication
V9.1.0	April 2010	Publication
V9.2.0	July 2010	Publication
V9.3.0	October 2010	Publication
V9.4.0	January 2011	Publication