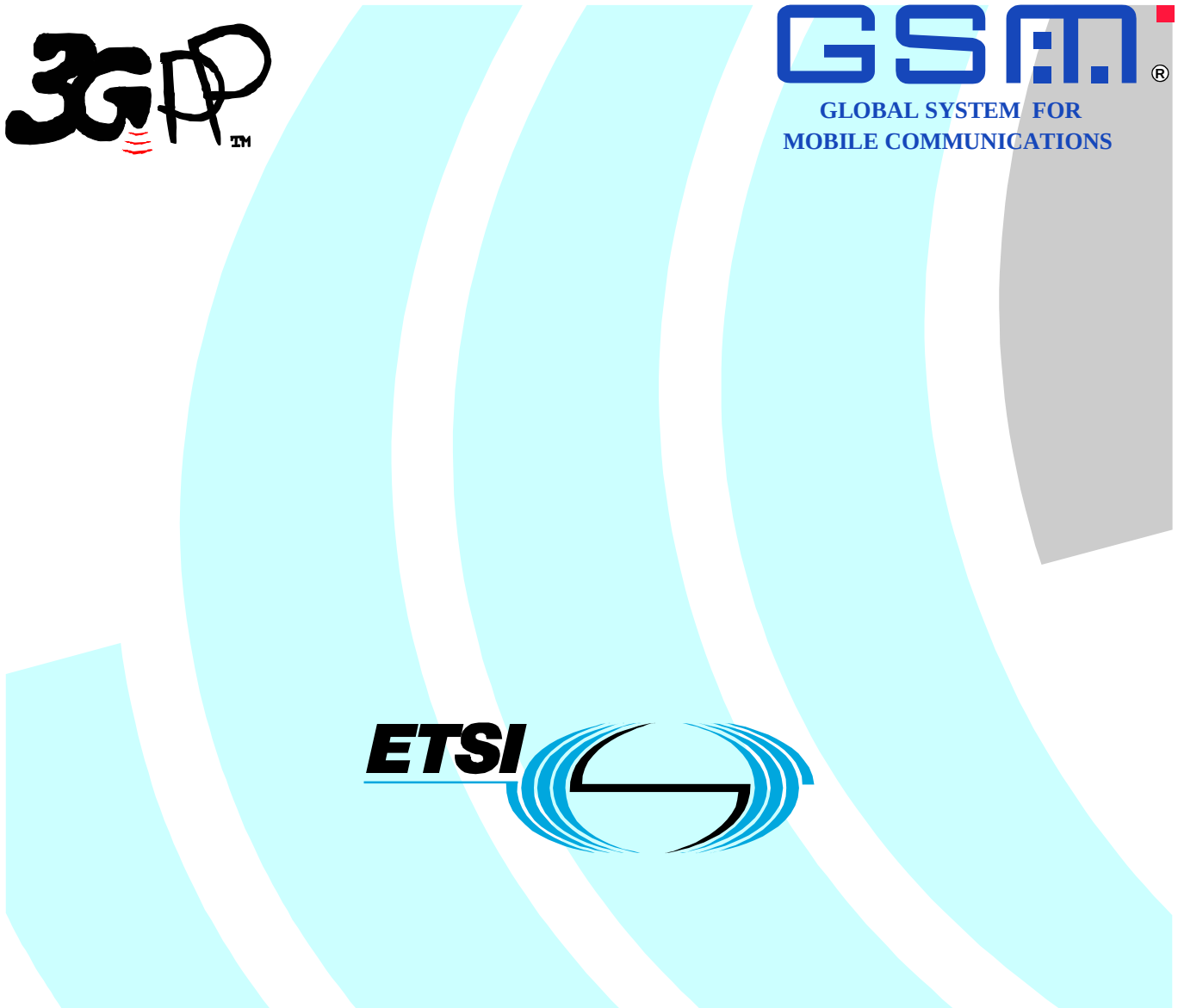
ETSI TS 129 229 V5.6.0 (2003-12)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Cx and Dx interfaces based on the Diameter protocol;
Protocol details
(3GPP TS 29.229 version 5.6.0 Release 5)**



Reference
RTS/TSGN-0429229v560

Keywords
GSM, 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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

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 Cx interface between the I-CSCF/S-CSCF and the HSS.
- The Dx interface between the I-CSCF/S-CSCF and the SLF.

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 29.228 “IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents (Release 5)”

[2] 3GPP TS 33.210 “3G Security; Network Domain Security; IP Network Layer Security (Release 5)”

[3] IETF RFC 3261 "SIP: Session Initiation Protocol"

[4] IETF RFC 2396: “Uniform Resource Identifiers (URI): generic syntax”

[5] IETF RFC 2960 “Stream Control Transmission Protocol”

[6] IETF RFC 3588 “Diameter Base Protocol”

[7] IETF RFC 2234 “Augmented BNF for syntax specifications”

[8] IETF RFC 2806 “URLs for Telephone Calls”

[9] void

[10] IETF RFC 3309: “SCTP Checksum Change”

[11] 3GPP TS 29.329 “Sh Interface based on the Diameter protocol; protocol details”

[12] IETF RFC 3589 “Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5”

3 Definitions, symbols and abbreviations

3.1 Definitions

Refer to IETF RFC 3588 [6] 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 [6], it corresponds to an Information Element in a Diameter message.

Diameter Multimedia client: a client that implements the Diameter Multimedia application. The client is one of the communicating Diameter peers that usually initiate transactions. Examples in 3GPP are the I-CSCF and S-CSCF.

Diameter Multimedia server: a server that implements the Diameter Multimedia application. A Diameter Multimedia server that also supported the NASREQ and MobileIP applications would be referred to as a Diameter server. An example of a Diameter Multimedia server in 3GPP is the HSS.

Registration: SIP-registration.

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
ABNF	Augmented Backus-Naur Form
AVP	Attribute-Value Pair
CN	Core Network
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IANA	Internet Assigned Numbers Authority
I-CSCF	Interrogating CSCF
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
NDS	Network Domain Security
RFC	Request For Comments
S-CSCF	Serving CSCF
SCTP	Stream Control Transport Protocol
SIP	Session Initiation Protocol
SLF	Server Locator Function
UCS	Universal Character Set
URL	Uniform Resource Locator
UTF	UCS Transformation Formats

4 General

The Diameter Base Protocol as specified in IETF RFC 3588 [6] 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 5 of this specification. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) are unmodified.

5 Use of the Diameter base protocol

With the clarifications listed in the following subclauses the Diameter Base Protocol defined by IETF RFC 3588 [6] shall apply.

5.1 Securing Diameter Messages

For secure transport of Diameter messages, see 3GPP TS 33.210 [2].

5.2 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used on the Cx interface.

5.3 Use of sessions

Both between the I-CSCF and the HSS and between the S-CSCF and the HSS Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

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 [6]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

5.4 Transport protocol

Diameter messages over the Cx interface shall make use of SCTP IETF RFC 2960 [5] and shall utilise the new SCTP checksum method specified in RFC 3309 [10].

5.5 Routing considerations

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

If an I-CSCF or S-CSCF knows the address/name of the HSS for a certain user, both the Destination-Realm and Destination-Host AVPs shall be present in the request. Otherwise, only the Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node, e.g. the SLF (see 3GPP TS 29.228 [1]), based on the Diameter routing table in the client. Once the redirector function (SLF) has returned the address or the destination HSS (using Redirect-Host AVP), the redirected request to the HSS shall include both Destination-Realm and Destination-Host AVPs. Consequently, the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by an I-CSCF or an S-CSCF. The S-CSCF shall store the address of the HSS for each user, after a first request sent to the redirector function.

Requests initiated by the HSS towards an S-CSCF shall include both Destination-Host and Destination-Realm AVPs. The HSS obtains the Destination-Host AVP to use in requests towards an S-CSCF, from the Origin-Host AVP received in previous requests from the S-CSCF. Consequently, the Destination-Host AVP is declared as mandatory in the ABNF for all requests initiated by the HSS.

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

5.6 Advertising Application Support

The HSS, S-CSCF and I-CSCF shall advertise support of the Diameter Multimedia Application by including the value of 3GPP(10415) in the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and by including the value of 3GPP (10415) in the Vendor-Id AVP and the value of the application identifier (see chapter 6) in the Auth-Application-Id AVP, both in the Vendor-Specific-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

6 Diameter application for Cx interface

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

- to exchange location information
- to authorize a user to access the IMS
- to exchange authentication information
- to download and handle changes in the user data stored in the server

The Cx 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 Cx/Dx interface application is 167772151 (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 IETF RFC 2234 [7], according to the rules in IETF RFC 3588 [6]. Whenever the definition and use of an AVP is not specified in this document, what is stated in IETF RFC 3588 [6] shall apply.

The command codes for the Cx/Dx interface application are taken from the range allocated by IANA in IETF RFC 3589 [12] as assigned in this specification. For these commands, the Application-ID field shall be set to 167772151 (application identifier of the Cx/Dx 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-Authorization-Request	UAR	300	6.1.1
User-Authorization-Answer	UAA	300	6.1.2
Server-Assignment-Request	SAR	301	6.1.3
Server-Assignment-Answer	SAA	301	6.1.4
Location-Info-Request	LIR	302	6.1.5
Location-Info-Answer	LIA	302	6.1.6
Multimedia-Auth-Request	MAR	303	6.1.7
Multimedia-Auth-Answer	MAA	303	6.1.8
Registration-Termination-Request	RTR	304	6.1.9
Registration-Termination-Answer	RTA	304	6.1.10
Push-Profile-Request	PPR	305	6.1.11
Push-Profile-Answer	PPA	305	6.1.12

6.1.1 User-Authorization-Request (UAR) Command

The User-Authorization-Request (UAR) command, indicated by the Command-Code field set to 300 and the ‘R’ bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia server in order to request the authorization of the registration of a multimedia user.

Message Format

```
< User-Authorization-Request> ::=   < Diameter Header: 300, 167772151, REQ, PXY >
                                    < Session-Id >
                                    { Vendor-Specific-Application-Id }
                                    { Auth-Session-State }
                                    { Origin-Host }
                                    { Origin-Realm }
                                    [ Destination-Host ]
                                    { Destination-Realm }
                                    { User-Name }
                                    { Public-Identity }
                                    { Visited-Network-Identifier }
                                    [ User-Authorization-Type ]
                                    *[ AVP ]
                                    *[ Proxy-Info ]
                                    *[ Route-Record ]
```

6.1.2 User-Authorization-Answer (UAA) Command

The User-Authorization-Answer (UAA) command, indicated by the Command-Code field set to 300 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the User-Authorization-Request command. The Result-Code AVP or Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in IETF RFC 3588 [6].

Message Format

```
< User-Authorization-Answer> ::=   < Diameter Header: 300, 167772151 >
                                   < Session-Id >
                                   { Vendor-Specific-Application-Id }
                                   [ Result-Code ]
                                   [Experimental-Result ]
                                   { Auth-Session-State }
                                   { Origin-Host }
                                   { Origin-Realm }
                                   [ Server-Name ]
                                   [ Server-Capabilities ]
                                   *[ AVP ]
                                   *[ Proxy-Info ]
                                   *[ Route-Record ]
```

6.1.3 Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR) command, indicated by the Command-Code field set to 301 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia server in order to request it to store the name of the server that is currently serving the user.

Message Format

```
<Server-Assignment-Request> ::= < Diameter Header: 301, 167772151, REQ, PXY >
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                [ User-Name ]
                                *[ Public-Identity ]
                                { Server-Name }
```

{ Server-Assignment-Type }
{ User-Data-Request-Type }
{ User-Data-Already-Available }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.4 Server-Assignment-Answer (SAA) Command

The Server-Assignment-Answer (SAA) command, indicated by the Command-Code field set to 301 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Server-Assignment-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in IETF RFC 3588 [6]. If Result-Code or Experimental-Result does not inform about an error, the User-Data AVP shall contain the information that the S-CSCF needs to give service to the user.

Message Format

<Server-Assignment-Answer> ::= < Diameter Header: 301, 167772151 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[User-Data]
[Charging-Information]
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.5 Location-Info-Request (LIR) Command

The Location-Info-Request (LIR) command, indicated by the Command-Code field set to 302 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia server in order to request name of the server that is currently serving the user.

Message Format

<Location-Info-Request> ::= < Diameter Header: 302, 167772151, REQ, PXY >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
{ Public-Identity }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.6 Location-Info-Answer (LIA) Command

The Location-Info-Answer (LIA) command, indicated by the Command-Code field set to 302 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Location-Info-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in IETF RFC 3588 [6].

Message Format

<Location-Info-Answer> ::= < Diameter Header: 302, 167772151 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Server-Name]
[Server-Capabilities]
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.7 Multimedia-Auth-Request (MAR) Command

The Multimedia-Auth-Request (MAR) command, indicated by the Command-Code field set to 4 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia server in order to request security information.

Message Format

< Multimedia-Auth-Request > ::= < Diameter Header: 303, 167772151, REQ >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[Destination-Host]
{ User-Name }
{ Public-Identity }
[SIP-Auth-Data-Item]
[SIP-Number-Auth-Items]
{ Server-Name }
* [AVP]
* [Proxy-Info]
* [Route-Record]

6.1.8 Multimedia-Auth-Answer (MAA) Command

The Multimedia-Auth-Answer (MAA) command, indicated by the Command-Code field set to 303 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Auth-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in IETF RFC 3588 [6].

Message Format

< Multimedia-Auth-Answer > ::= < Diameter Header: 303, 167772151 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Public-Identity]
[SIP-Number-Auth-Items]
*** [SIP-Auth-Data-Item]**
* [AVP]
* [Proxy-Info]
* [Route-Record]

6.1.9 Registration-Termination-Request (RTR) Command

The Registration-Termination-Request (RTR) command, indicated by the Command-Code field set to 304 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia server to a Diameter Multimedia client in order to request the de-registration of a user.

Message Format

<Registration-Termination-Request> ::= < Diameter Header: 304, 167772151, REQ >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
***[Public-Identity]**
{ DeRegistration-Reason }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.10 Registration-Termination-Answer (RTA) Command

The Registration-Termination-Answer (RTA) command, indicated by the Command-Code field set to 304 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Registration-Termination-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in IETF RFC 3588 [6].

Message Format

<Registration-Termination-Answer> ::= < Diameter Header: 304, 167772151 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.11 Push-Profile-Request (PPR) Command

The Push-Profile-Request (PPR) command, indicated by the Command-Code field set to 305 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia server to a Diameter Multimedia client in order to update the subscription data of a multimedia user in the Diameter Multimedia client whenever a modification has occurred in the subscription data that constitutes the data used by the client.

Message Format

< Push-Profile-Request > ::= < Diameter Header: 305, 167772151, REQ >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
{ User-Data }

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

6.1.12 Push-Profile-Answer (PPA) Command

The Push-Profile-Answer (PPA) command, indicated by the Command-Code field set to 305 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Push-Profile-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in IETF RFC 3588 [6].

Message Format

< Push-Profile-Answer > ::=< Diameter Header: 305, 167772151 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[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. 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

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

6.2.1.1 DIAMETER_FIRST_REGISTRATION (2001)

The HSS informs the I-CSCF that:

- The user is authorized to register this public identity;
- A S-CSCF shall be assigned to that user.

6.2.1.2 DIAMETER_SUBSEQUENT_REGISTRATION (2002)

The HSS informs the I-CSCF that:

- The user is authorized to register this public identity;
- A S-CSCF is already assigned and there is no need to select a new one.

6.2.1.3 DIAMETER_UNREGISTERED_SERVICE (2003)

The HSS informs the I-CSCF that:

- The public identity is not registered but has services related to unregistered state;
- A S-CSCF shall be assigned to the user.

6.2.1.4 DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED (2004)

The HSS informs to the S-CSCF that:

- The de-registration is completed;
- The S-CSCF name is not stored in the HSS.

6.2.1.5 DIAMETER_SERVER_SELECTION (2005)

The HSS informs the I-CSCF that:

- The user is authorized to register this public identity;
- A S-CSCF is already assigned for services related to unregistered state;
- It may be necessary to assign a new S-CSCF to the user.

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_UNKNOWN (5001)

A message was received for a user that is unknown.

6.2.2.2 DIAMETER_ERROR_IDENTITIES_DONT_MATCH (5002)

A message was received with a public identity and a private identity for a user, and the server determines that the public identity does not correspond to the private identity.

6.2.2.3 DIAMETER_ERROR_IDENTITY_NOT_REGISTERED (5003)

A query for location information is received for a public identity that has not been registered before. The user to which this identity belongs cannot be given service in this situation.

6.2.2.4 DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)

The user is not allowed to roam in the visited network.

6.2.2.5 DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED (5005)

The identity being registered has already a server assigned and the registration status does not allow that it is overwritten.

6.2.2.6 DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED (5006)

The authentication scheme indicated in an authentication request is not supported.

6.2.2.7 DIAMETER_ERROR_IN_ASSIGNMENT_TYPE (5007)

The identity being registered has already the same server assigned and the registration status does not allow the server assignment type.

6.2.2.8 DIAMETER_ERROR_TOO_MUCH_DATA (5008)

The volume of the data pushed to the receiving entity exceeds its capacity.

NOTE: This error code is also used in 3GPP TS 29.329 [11].

6.2.2.9 DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA (5009)

The S-CSCF informs HSS that the received subscription data contained information, which was not recognised or supported.

6.3 AVPs

The following table describes the Diameter AVPs defined for the Cx interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

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 Encr.**
Visited-Network-Identifier	1	6.3.1	OctetString	M, V				No
Public-Identity	2	6.3.2	UTF8String	M, V				N
Server-Name	3	6.3.3	UTF8String	M,V				No
Server-Capabilities	4	6.3.4	Grouped	M, V				No
Mandatory-Capability	5	6.3.5	Unsigned32	M, V				No
Optional-Capability	6	6.3.6	Unsigned32	M, V				No
User-Data	7	6.3.7	OctetString	M, V				No
SIP-Number-Auth-Items	8	6.3.8	Unsigned32	M, V				No
SIP-Authentication-Scheme	9	6.3.9	UTF8String	M, V				No
SIP-Authenticate	10	6.3.10	OctetString	M, V				No
SIP-Authorization	11	6.3.11	OctetString	M, V				No
SIP-Authentication-Context	12	6.3.12	OctetString	M, V				No
SIP-Auth-Data-Item	13	6.3.13	Grouped	M, V				No
SIP-Item-Number	14	6.3.14	Unsigned32	M, V				No
Server-Assignment-Type	15	6.3.15	Enumerated	M, V				No
Deregistration-Reason	16	6.3.16	Grouped	M, V				No
Reason-Code	17	6.3.17	Enumerated	M, V				No
Reason-Info	18	6.3.18	UTF8String	M, V				No
Charging-Information	19	6.3.19	Grouped	M, V				No
Primary-Event-Charging-Function-Name	20	6.3.20	DiameterURI	M, V				No
Secondary-Event-Charging-Function-Name	21	6.3.21	DiameterURI	M, V				No
Primary-Charging-Collection-Function-Name	22	6.3.22	DiameterURI	M, V				No

Secondary-Charging-Collection-Function-Name	23	6.3.23	DiameterURI	M, V				No
User-Authorization-Type	24	6.3.24	Enumerated	M, V				No
User-Data-Request-Type	25	6.3.25	Enumerated	M, V				No
User-Data-Already-Available	26	6.3.26	Enumerated	M, V				No
Confidentiality-Key	27	6.3.27	OctetString	M, V				No
Integrity-Key	28	6.3.28	OctetString	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 IETF RFC 3588 [6]. NOTE 2: Depending on the concrete command.								

6.3.1 Visited-Network-Identifier AVP

The Visited-Network-Identifier AVP (AVP Code 1) is of type OctetString. This AVP contains an identifier that helps the home network to identify the visited network (e.g. the visited network domain name).

6.3.2 Public-Identity AVP

The Public-Identity AVP (AVP Code 2) is of type UTF8String. This AVP contains the public identity of a user in the IMS. The syntax of this AVP corresponds either to a SIP URL (with the format defined in IETF RFC 3261 [3] and IETF RFC 2396 [4]) or a TEL URL (with the format defined in IETF RFC 2806 [8]).

6.3.3 Server-Name AVP

The Server-Name 3 (AVP Code 3) is of type UTF8String. This AVP contains a SIP-URL (as defined in IETF RFC 3261 [3] and IETF RFC 2396 [4]), used to identify a SIP server (e.g. S-CSCF name).

6.3.4 Server-Capabilities AVP

The Server-Capabilities AVP (AVP Code 4) is of type Grouped. This AVP contains information to assist the I-CSCF in the selection of an S-CSCF.

AVP format

Server-Capabilities ::= <AVP header: TBD>

*[Mandatory-Capability]

*[Optional-Capability]

*[Server-Name]

*[AVP]

6.3.5 Mandatory-Capability AVP

The Mandatory-Capability AVP (AVP Code 5) is of type Unsigned32. The value included in this AVP can be used to represent a single determined mandatory capability of an S-CSCF. Each mandatory capability available in an individual operator's network shall be allocated a unique value. The allocation of these values to individual capabilities is an operator issue.

6.3.6 Optional-Capability AVP

The Optional-Capability AVP (AVP Code 6) is of type Unsigned32. The value included in this AVP can be used to represent a single determined optional capability of an S-CSCF. Each optional capability available in an individual operator's network shall be allocated a unique value. The allocation of these values to individual capabilities is an operator issue.

6.3.7 User-Data AVP

The User-Data AVP (AVP Code 7) is of type OctetString. This AVP contains the user data required to give service to a user. The exact content and format of this AVP is described in 3GPP TS 29.228 [1].

6.3.8 SIP-Number-Auth-Items AVP

The SIP-Number-Auth-Items AVP (AVP code 8) is of type Unsigned32 and indicates the number of authentication vectors provided by the Diameter server.

When used in a request it indicates the number of SIP-Auth-Data-Item's the S-CSCF is requesting. This can be used, for instance, when the client is requesting several pre-calculated authentication vectors. In the answer message the SIP-Number-Auth-Items AVP indicates the actual number of items provided by the Diameter server.

6.3.9 SIP-Authentication-Scheme AVP

The Authentication-Scheme AVP (AVP code 9) is of type UTF8String and indicates the authentication scheme used in the authentication of SIP messages.

6.3.10 SIP-Authenticate AVP

The SIP-Authenticate AVP (AVP code 10) is of type OctetString and contains the data portion of the WWW-Authenticate or Proxy-Authenticate SIP headers that are to be present in a SIP response.

6.3.11 SIP-Authorization AVP

The SIP-Authorization AVP (AVP code 11) is of type OctetString and contains the data portion of the Authorization or Proxy-Authorization SIP headers suitable for inclusion in a SIP request.

6.3.12 SIP-Authentication-Context AVP

The SIP-Authentication-Context AVP (AVP code 12) is of type OctectString, and contains authentication-related information relevant for performing the authentication but that is not part of the SIP authentication headers.

Some mechanisms (e.g. PGP, digest with quality of protection set to auth-int defined in IETF RFC 2617, digest with predictive nonces or sip access digest) request that part or the whole SIP request is passed to the entity performing the authentication. In such cases the SIP-Authentication-Context AVP would be carrying such information.

6.3.13 SIP-Auth-Data-Item AVP

The SIP-Auth-Data-Item (AVP code 13) is of type Grouped, and contains the authentication and/or authorization information for the Diameter client.

AVP format

SIP-Auth-Data-Item :: = < AVP Header : TBD >

[SIP-Item-Number]

[SIP-Authentication-Scheme]

[SIP-Authenticate]

[SIP-Authorization]

[SIP-Authentication-Context]

[Confidentiality-Key]

[Integrity-Key]

* [AVP]

6.3.14 SIP-Item-Number AVP

The SIP-Item-Number AVP (AVP code 14) is of type Unsigned32, and is included in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.

6.3.15 Server-Assignment-Type AVP

The Server-Assignment-Type AVP (AVP code 15) is of type Enumerated, and indicates the type of server update being performed in a Server-Assignment-Request operation. The following values are defined:

NO_ASSIGNMENT (0)

This value is used to request from HSS the user profile assigned to one or more public identities, without affecting the registration state of those identities.

REGISTRATION (1)

The request is generated as a consequence of a first registration of an identity.

RE_REGISTRATION (2)

The request corresponds to the re-registration of an identity.

UNREGISTERED_USER (3)

The request is generated because the S-CSCF received an INVITE for a public identity that is not registered.

TIMEOUT_DEREGISTRATION (4)

The SIP registration timer of an identity has expired.

USER_DEREGISTRATION (5)

The S-CSCF has received a user initiated de-registration request.

TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME (6)

The SIP registration timer of an identity has expired. The S-CSCF keeps the user data stored in the S-CSCF and requests HSS to store the S-CSCF name.

USER_DEREGISTRATION_STORE_SERVER_NAME (7)

The S-CSCF has received a user initiated de-registration request. The S-CSCF keeps the user data stored in the S-CSCF and requests HSS to store the S-CSCF name.

ADMINISTRATIVE_DEREGISTRATION (8)

The S-CSCF, due to administrative reasons, has performed the de-registration of an identity.

AUTHENTICATION_FAILURE (9)

The authentication of a user has failed.

AUTHENTICATION_TIMEOUT (10)

The authentication timeout has expired.

DEREGISTRATION_TOO_MUCH_DATA (11)

The S-CSCF has requested user profile information from the HSS and has received a volume of data higher than it can accept.

6.3.16 Deregistration-Reason AVP

The Deregistration-Reason AVP (AVP code 16) is of type Grouped, and indicates the reason for a de-registration operation.

AVP format

Deregistration-Reason :: = < AVP Header : TBD >

{ Reason-Code }

[Reason-Info]

* [AVP]

6.3.17 Reason-Code AVP

The Reason-Code AVP (AVP code 17) is of type Enumerated, and defines the reason for the network initiated de-registration. The following values are defined:

PERMANENT_TERMINATION (0)

NEW_SERVER_ASSIGNED (1)

SERVER_CHANGE (2)

REMOVE_S-CSCF (3)

The detailed behaviour of the S-CSCF is defined in 3GPP TS 29.228 [1].

6.3.18 Reason-Info AVP

The Reason-Info AVP (AVP code 18) is of type UTF8String, and contains textual information to inform the user about the reason for a de-registration.

6.3.19 Charging-Information AVP

The Charging-Information (AVP code 19) is of type Grouped, and contains the addresses of the charging functions.

AVP format

Charging-Information :: = < AVP Header : TBD >

[Primary-Event-Charging-Function-Name]

[Secondary-Event-Charging-Function-Name]

{ Primary-Charging-Collection-Function-Name }

[Secondary-Charging-Collection-Function-Name]

*[AVP]

6.3.20 Primary-Event-Charging-Function-Name AVP

The Primary-Event-Charging-Function-Name AVP (AVP Code 20) is of type DiameterURI. This AVP contains the address of the Primary Event Charging Function.

6.3.21 Secondary-Event-Charging-Function-Name AVP

The Secondary-Event-Charging-Function-Name AVP (AVP Code 21) is of type DiameterURI. This AVP contains the address of the Secondary Event Charging Function.

6.3.22 Primary-Charging-Collection-Function-Name AVP

The Primary-Charging-Collection-Function-Name AVP (AVP Code 22) is of type DiameterURI. This AVP contains the address of the Primary Charging Collection Function.

6.3.23 Secondary-Charging-Collection-Function-Name AVP

The Secondary-Charging-Collection-Function-Name AVP (AVP Code 23) is of type DiameterURI. This AVP contains the address of the Secondary Charging Collection Function.

6.3.24 User-Authorization-Type AVP

The User-Authorization-Type AVP (AVP code 24) is of type Enumerated, and indicates the type of user authorization being performed in a User Authorization operation, i.e. UAR command. The following values are defined:

REGISTRATION (0)

This value is used in case of the initial registration or re-registration. I-CSCF determines this from the Expires field or expires parameter in Contact field in the SIP REGISTER method if it is not equal to zero.

This is the default value.

DE_REGISTRATION (1)

This value is used in case of the de-registration. I-CSCF determines this from the Expires field or expires parameter in Contact field in the SIP REGISTER method if it is equal to zero.

REGISTRATION_AND_CAPABILITIES (2)

This value is used in case of initial registration or re-registration and when the I-CSCF explicitly requests S-CSCF capability information from the HSS. The I-CSCF shall use this value when the user's current S-CSCF, which is stored in the HSS, cannot be contacted and a new S-CSCF needs to be selected

6.3.25 User-Data-Request-Type AVP

The User-Data-Request-Type AVP (AVP code 25) is of type Enumerated, and indicates the type of user profile the S-CSCF is requesting from the HSS. The following values are defined:

COMPLETE_PROFILE (0)

This value is used to request from the HSS the complete user profile corresponding to one or more public identities.

REGISTERED_PROFILE (1)

This value is used to request from the HSS the registered part of the user profile corresponding to one or more public identities.

UNREGISTERED_PROFILE (2)

This value is used to request from the HSS the unregistered part of the user profile corresponding to one or more public identities.

6.3.26 User-Data-Already-Available AVP

The User-Data-Already-Available AVP (AVP code 26) is of type Enumerated, and indicates to the HSS whether or not the S-CSCF already has the part of the user profile that it needs to serve the user. The following values are defined:

USER_DATA_NOT_AVAILABLE (0)

The S-CSCF does not have the data that it needs to serve the user.

USER_DATA_ALREADY_AVAILABLE (1)

The S-CSCF already has the data that it needs to serve the user.

6.3.27 Confidentiality-Key AVP

The Confidentiality-Key (AVP code 27) is of type OctetString, and contains the Confidentiality Key (CK).

6.3.28 Integrity-Key AVP

The Integrity-Key (AVP code 28) is of type OctetString, and contains the Integrity Key (IK).

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 values 1-28 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 2001-2005 and 5001-5009. See section 6.2.

6.4.3 Command Code values

This specification assigns the values 300-305 from the range allocated by IANA to 3GPP in IETF RFC 3589 [12].

6.4.4 Application-ID value

IANA has allocated the value 167772151 for the 3GPP Cx interface application.

7 Special Requirements

7.1 Version Control

It shall be possible to identify/negotiate which version of IMS the application is supporting. The current Diameter draft does not support differentiation of versions within an application with the reasoning that for a new application version just a new application ID is required. The same approach is followed by 3GPP as described in the section 5.6.

If the new application ID mechanism for capability exchange is not enough in the future versions of the Cx specifications, the principle on how the version control is done is following. When the peer node receives the Capabilities-Exchange-Request messagecommand with the additional AVPs indicating the added supported functionality of the requesting node, if the receiving node supports some or all of the functionalities it shall send the corresponding AVPs indicating the supported functionality to the requesting node, which then knows that the added

capabilities the peer node supports. If the peer node does not recognize some or all of the additional capabilities it shall discard the AVPs and it shall not send those AVPs to the original requestor.

As an example of this mechanism, an additional AVP could indicate the supported command version, e.g. the version of the Multimedia-Auth command (Multimedia-Auth-Version AVP). If updates to the Multimedia-Auth command are supported by the node initiating the capability exchange, it includes Multimedia-Auth-Version AVP into the Capabilities-Exchange-Request command in indicating the version supported. If the peer node supports the version, it will send in the Capabilities-Exchange-Answer command the Multimedia-Auth-Version AVP with the same version number.

The exact mechanism and AVPs needed for the version control are decided when the exact update to the Cx application is needed.

Annex A (informative): Change history

Date	TSG #	TSG Doc.	CR#	Rev	Subject/Comment	In	Out
Jun 2002	CN#16	NP-020265			Version 2.0.0 approved at CN#16	2.0.0	5.0.0
Sep 2002	CN#17	NP-020449	001		Add a reference to the new IETF RFC on SCTP checksum	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	003		Wrong format of Charging Function Addresses	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	005		Editorial mistake in the definition of command MAA	5.0.0	5.1.0
Dec 2002	CN#18	NP-020587	006	-	Addition of User-Name AVP to SAA	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	007	-	Editorial correction of SIP-Auth-Data-Item AVP definition	5.1.0	5.2.0
Dec 2002	CN#18	NP-020589	008	1	Clarification of REGISTRATION_AND_CAPABILITIES value	5.1.0	5.2.0
Dec 2002	CN#18	NP-020588	009	-	Correction in charging information	5.1.0	5.2.0
Dec 2002	CN#18	NP-020590	010	1	Error handling in S-CSCF when receiving too much data	5.1.0	5.2.0
March 2003	CN#19	NP-030244	012	1	Update TS 29.229 after Diameter has become RFC	5.2.0	5.3.0
March 2003	CN#19	NP-030277	015	1	Clarification on Re-allocation of S-CSCF	5.2.0	5.3.0
March 2003	CN#19	NP-030237	018	1	Handling of non supported data in the S-CSCF when the profile is being updated.	5.2.0	5.3.0
March 2003	CN#19	NP-030079	014	-	Correction to the values of User-Authorizatin-Type AVP	5.2.0	5.3.0
March 2003	CN#19	NP-030077	013	-	Replacement of the NAS-Session-Key AVP	5.2.0	5.3.0
June 2003	CN#20	NP-030215	019	-	Conditionality of User-Name AVP in Server-Assignment-Answer	5.3.0	5.4.0
September 2003	CN#21	NP-030383	022	1	Critical Correction on the PPR command code	5.4.0	5.5.0
December 2003	CN#22	NP-030500	021	1	The S-CSCF name needs to be checked always in MAR and SAR	5.5.0	5.6.0
December 2003	CN#22	NP-030500	027	-	User-Authorization-Type	5.5.0	5.6.0
December 2003	CN#22	NP-030518	029	-	Clarification of inclusion of elements in Charging Information	5.5.0	5.6.0
December 2003	CN#22				Application IDs and references updated	5.5.0	5.6.0

History

Document history		
V5.0.0	June 2002	Publication
V5.1.0	September 2002	Publication
V5.2.0	December 2002	Publication
V5.3.0	March 2003	Publication
V5.4.0	June 2003	Publication
V5.5.0	September 2003	Publication
V5.6.0	December 2003	Publication