3GPP TS 29.229 V14.2.0 (2017-06)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network and Terminals;
Cx and Dx interfaces based on the Diameter protocol;
Protocol details
(Release 14)

Keywords

UMTS, network

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

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 base protocol as specified in IETF RFC 6733 [28].

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 base protocol as specified in IETF RFC 6733 [28]. Where this is not possible, extensions to Diameter base protocol as specified in IETF RFC 6733 [28] 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".

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

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

[4] IETF RFC 2396: "Uniform Resource Identifiers (URI): generic syntax".

[5] Void.

[6] Void.

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

[8] IETF RFC 3966: "The tel URI for Telephone Numbers".

[9] Void.

[10] Void.

[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".

[13] 3GPP TS 23.003: "Numbering, addressing and identification".

[14] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[15] IETF RFC 4740: "Diameter Session Initiation Protocol (SIP) Application".

[16] 3GPP TS 29.328: "IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents".

[17] IETF RFC 3327: "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[18] 3GPP TS 29.273: "3GPP EPS AAA interfaces".

[19] IETF RFC 4005: "Diameter Network Access Server Application".

[20] IETF RFC 4590: " RADIUS Extension for Digest Authentication".

[21] IETF RFC 4960: "Stream Control Transmission Protocol".

[22] IETF RFC 3162: "RADIUS and IPv6".

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

[24] 3GPP TS 23.380: "IMS Restoration Procedures".

[25] IETF draft-holmberg-sipcore-auth-id-01: "Authorization server identity".

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

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

[27] IETF draft-ietf-dime-load-03: "Diameter Load Information Conveyance".

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

Refer to IETF RFC 6733 [28] 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 [28], 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
DSCP	Differentiated Services Code Point
DRMP	Diameter Routing Message Priority
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
WAF	WebRTC Authentication Function
WWSF	WebRTC Web Server Function

4 General

The Diameter base protocol as specified in IETF RFC 6733 [28] 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 6733 [28] 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 6733 [28]. 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 and the Dx interfaces shall make use of SCTP IETF RFC 4960 [21].

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 or a Diameter Proxy Agent (see 3GPP TS 29.228 [1]), based on the Diameter routing table in the client.

If the next Diameter node is an SLF, then once the 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. If the next Diameter node is a Diameter Proxy Agent, the Diameter Proxy Agent shall determine the destination HSS. The Diameter Proxy Agent, based on the result of this determination of the destination HSS, shall modify the Destination-Realm AVP and Destination-Host AVP of the request appropriately. The Diameter Proxy Agent shall then append a Route-Record AVP to the request and shall send the request to the destination HSS. Consequently, the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by an I-CSCF or an S-CSCF.

If the response is routed back to a Diameter Proxy Agent, the Diameter Proxy Agent shall send the response back to the I-CSCF or S-CSCF without modifying the Origin-Realm AVP and Origin-Host AVP. The response shall contain the Origin-Realm AVP set to the realm of the HSS together with the Origin-Host AVP set to the HSS that sent the response. The S-CSCF shall store the HSS realm and HSS address for each Public Identity, after the first request sent to the User Identity to HSS resolution 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 the application identifier (see chapter 6) in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The vendor identifier value of 3GPP (10415) and ETSI (13019) shall be included in the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and in the Vendor-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

Note: The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that is not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per IETF RFC 6733 [28].

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 16777216 (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 Command Code Format (CCF) specification defined in IETF RFC 6733 [28]. Whenever the definition and use of an AVP is not specified in this document, what is stated in IETF RFC 6733 [28] 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 [28]).

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 16777216 (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, REQ, PXY, 16777216 >
                                      < Session-Id >
                                      [ DRMP ]
                                      { Vendor-Specific-Application-Id }
                                      { Auth-Session-State }
                                      { Origin-Host }
                                      { Origin-Realm }
                                      [ Destination-Host ]
                                      { Destination-Realm }
                                      { User-Name }
                                      [ OC-Supported-Features ]
                                      *[ Supported-Features ]
                                      { Public-Identity }
                                      { Visited-Network-Identifier }
                                      [ User-Authorization-Type ]
                                      [ UAR-Flags ]
                                      *[ 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 Experimental-Result AVP may contain one of the values defined in section 6.2.

Message Format

```
< User-Authorization-Answer> ::=     < Diameter Header: 300, PXY, 16777216 >
                                     < Session-Id >
                                     [ DRMP ]
                                     { Vendor-Specific-Application-Id }
                                     [ Result-Code ]
                                     [ Experimental-Result ]
                                     { Auth-Session-State }
                                     { Origin-Host }
                                     { Origin-Realm }
                                     [ OC-Supported-Features ]
                                     [ OC-OLR ]
                                     *[ Load ]
                                     *[ Supported-Features ]
                                     [ Server-Name ]
                                     [ Server-Capabilities ]
                                     *[ AVP ]
                                     [ Failed-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, REQ, PXY, 16777216 >
                                < Session-Id >
                                [ DRMP ]
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                [ User-Name ]
                                [ OC-Supported-Features ]
                                *[ Supported-Features ]
                                *[ Public-Identity ]
                                [ Wildcarded-Public-Identity ]
                                { Server-Name }
                                { Server-Assignment-Type }
                                { User-Data-Already-Available }
                                [ SCSCF-Restoration-Info ]
                                [ Multiple-Registration-Indication ]
                                [ Session-Priority ]
                                [ SAR-Flags ]
                                *[ 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 Experimental-Result AVP may contain one of the values defined in section 6.2. 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, PXY, 16777216 >
                               < Session-Id >
                               [ DRMP ]
                               { Vendor-Specific-Application-Id }
                               [ Result-Code ]
                               [ Experimental-Result ]
                               { Auth-Session-State }
                               { Origin-Host }
                               { Origin-Realm }
                               [ User-Name ]
                               [ OC-Supported-Features ]
                               [ OC-OLR ]
                               *[ Load ]
                               *[ Supported-Features ]
                               [ User-Data ]
                               [ Charging-Information ]
                               [ Associated-Identities ]
                               [ Loose-Route-Indication ]
                               *[ SCSCF-Restoration-Info ]
                               [ Associated-Registered-Identities ]
                               [ Server-Name ]
                               [ Wildcarded-Public-Identity ]
                               [ Priviledged-Sender-Indication ]
                               [ Allowed-WAF-WWSF-Identities ]
                               *[ AVP ]
```

```
                              [ Failed-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, REQ, PXY, 16777216 >
                              < Session-Id >
                              [ DRMP ]
                              { Vendor-Specific-Application-Id }
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              [ Destination-Host ]
                              { Destination-Realm }
                              [ Originating-Request ]
                              [ OC-Supported-Features ]
                              *[ Supported-Features ]
                              { Public-Identity }
                              [ User-Authorization-Type ]
                              [ Session-Priority ]
                              *[ 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 Experimental-Result AVP may contain one of the values defined in section 6.2.

Message Format

```
<Location-Info-Answer> ::=    < Diameter Header: 302, PXY, 16777216 >
                              < Session-Id >
                              [ DRMP ]
                              { Vendor-Specific-Application-Id }
                              [ Result-Code ]
                              [ Experimental-Result ]
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              [ OC-Supported-Features ]
                              [ OC-OLR ]
                              *[ Load ]
                              *[ Supported-Features ]
                              [ Server-Name ]
                              [ Server-Capabilities ]
                              [ Wildcarded-Public-Identity ]
                              [ LIA-Flags ]
                              *[ AVP ]
                              [ Failed-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 303 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, REQ, PXY, 16777216 >
                                < Session-Id >
                                [ DRMP ]
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Realm }
                                [ Destination-Host ]
                                { User-Name }
                                [ OC-Supported-Features ]
                                *[ Supported-Features ]
                                { 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 Experimental-Result AVP may contain one of the values defined in section 6.2.

Message Format

```
< Multimedia-Auth-Answer > ::= < Diameter Header: 303, PXY, 16777216 >
                                < Session-Id >
                                [ DRMP ]
                                { Vendor-Specific-Application-Id }
                                [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ User-Name ]
                                [ OC-Supported-Features ]
                                [ OC-OLR ]
                                *[ Load ]
                                *[ Supported-Features ]
                                [ Public-Identity ]
                                [ SIP-Number-Auth-Items ]
                                *[SIP-Auth-Data-Item ]
                                *[ AVP ]
                                [ Failed-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, REQ, PXY, 16777216 >
                                        < Session-Id >
                                        [ DRMP ]
                                        { Vendor-Specific-Application-Id }
                                        { Auth-Session-State }
                                        { Origin-Host }
                                        { Origin-Realm }
                                        { Destination-Host }
                                        { Destination-Realm }
                                        { User-Name }
                                        [ Associated-Identities ]
                                        *[ Supported-Features ]
                                        *[ 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 Experimental-Result AVP may contain one of the values defined in section 6.2.

Message Format

```
<Registration-Termination-Answer> ::=  < Diameter Header: 304, PXY, 16777216 >
                                       < Session-Id >
                                       < Session-Id >
                                       [ DRMP ]
                                       { Vendor-Specific-Application-Id }
                                       [ Result-Code ]
                                       [ Experimental-Result ]
                                       { Auth-Session-State }
                                       { Origin-Host }
                                       { Origin-Realm }
                                       [ Associated-Identities ]
                                       *[ Supported-Features ]
                                       *[ Identity-with-Emergency-Registration ]
                                       *[ AVP ]
                                       [ Failed-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 and for SIP Digest authentication the authentication data of a multimedia user in the Diameter Multimedia client whenever a modification has occurred in the subscription data or digest password that constitutes the data used by the client.

Message Format

```
< Push-Profile-Request > ::=  < Diameter Header: 305, REQ, PXY, 16777216 >
                              < Session-Id >
                              [ DRMP ]
                              { Vendor-Specific-Application-Id }
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
*[ Supported-Features ]
[ User-Data ]
[ Charging-Information ]
[ SIP-Auth-Data-Item ]
[ Allowed-WAF-WWSF-Identities ]
*[ 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 Experimental-Result AVP may contain one of the values defined in section 6.2.

Message Format

```
< Push-Profile-Answer > ::=     < Diameter Header: 305, PXY, 16777216 >
                                < 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 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

Result codes 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 the 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 Void

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 or a wildcarded identity 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 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 or the Public Identity type received in the request is not allowed for the indicated 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.

6.2.2.10 Void

6.2.2.11 DIAMETER_ERROR_FEATURE_UNSUPPORTED (5011)

A request application message was received indicating that the origin host requests that the command pair would be handled using a feature which is not supported by the destination host.

6.2.2.12 DIAMETER_ERROR_SERVING_NODE_FEATURE_UNSUPPORTED (5012)

This error is used when the HSS supports the P-CSCF-Restoration-mechanism feature, but none of the user serving node(s) supports it, as described by 3GPP TS 23.380 [24] clause 5.4.

6.3 AVPs

The following table describes the Diameter AVPs defined by 3GPP 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) if not otherwise indicated.

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	600	6.3.1	OctetString	M, V				No
Public-Identity	601	6.3.2	UTF8String	M, V				No
Server-Name	602	6.3.3	UTF8String	M, V				No
Server-Capabilities	603	6.3.4	Grouped	M, V				No
Mandatory-Capability	604	6.3.5	Unsigned32	M, V				No
Optional-Capability	605	6.3.6	Unsigned32	M, V				No
User-Data	606	6.3.7	OctetString	M, V				No
SIP-Number-Auth-Items	607	6.3.8	Unsigned32	M, V				No
SIP-Authentication-Scheme	608	6.3.9	UTF8String	M, V				No
SIP-Authenticate	609	6.3.10	OctetString	M, V				No
SIP-Authorization	610	6.3.11	OctetString	M, V				No
SIP-Authentication-Context	611	6.3.12	OctetString	M, V				No
SIP-Auth-Data-Item	612	6.3.13	Grouped	M, V				No
SIP-Item-Number	613	6.3.14	Unsigned32	M, V				No
Server-Assignment-Type	614	6.3.15	Enumerated	M, V				No
Deregistration-Reason	615	6.3.16	Grouped	M, V				No
Reason-Code	616	6.3.17	Enumerated	M, V				No
Reason-Info	617	6.3.18	UTF8String	M, V				No
Charging-Information	618	6.3.19	Grouped	M, V				No
Primary-Event-Charging-Function-Name	619	6.3.20	DiameterURI	M, V				No
Secondary-Event-Charging-Function-Name	620	6.3.21	DiameterURI	M, V				No
Primary-Charging-Collection-Function-Name	621	6.3.22	DiameterURI	M, V				No
Secondary-Charging-Collection-Function-Name	622	6.3.23	DiameterURI	M, V				No
User-Authorization-Type	623	6.3.24	Enumerated	M, V				No
User-Data-Already-Available	624	6.3.26	Enumerated	M, V				No
Confidentiality-Key	625	6.3.27	OctetString	M, V				No
Integrity-Key	626	6.3.28	OctetString	M, V				No
Supported-Features	628	6.3.29	Grouped	V	M			No
Feature-List-ID	629	6.3.30	Unsigned32	V			M	No
Feature-List	630	6.3.31	Unsigned32	V			M	No
Supported-Applications	631	6.3.32	Grouped	V			M	No
Associated-Identities	632	6.3.33	Grouped	V			M	No
Originating-Request	633	6.3.34	Enumerated	M,V				No
Wildcarded-Public-Identity	634	6.3.35	UTF8String	V			M	No
SIP-Digest-Authenticate	635	6.3.36	Grouped	V			M	No
Digest-Realm	104 NOTE 3	6.3.37	UTF8String	M			V	No
Digest-Algorithm	111 NOTE 3	6.3.39	UTF8String	M			V	No
Digest-QoP	110 NOTE 3	6.3.40	UTF8String	M			V	No
Digest-HA1	121 NOTE 3	6.3.41	UTF8String	M			V	No
UAR-Flags	637	6.3.44	Unsigned32	V			M	No
Loose-Route-Indication	638	6.3.45	Enumerated	V			M	No
SCSCF-Restoration-Info	639	6.3.46	Grouped	V			M	No
Path	640	6.3.47	OctetString	V			M	No
Contact	641	6.3.48	OctetString	V			M	No
Subscription-Info	642	6.3.49	Grouped	V			M	No
Call-ID-SIP-Header	643	6.3.49.1	OctetString	V			M	No
From-SIP-Header	644	6.3.49.2	OctetString	V			M	No
To-SIP-Header	645	6.3.49.3	OctetString	V			M	No
Record-Route	646	6.3.49.4	OctetString	V			M	No
Associated-Registered-Identities	647	6.3.50	Grouped	V			M	No
Multiple-Registration-Indication	648	6.3.51	Enumerated	V			M	No
Restoration-Info	649	6.3.52	Grouped	V			M	No

Session-Priority	650	6.3.56	Enumerated	V			M	No
Identity-with-Emergency-Registration	651	6.3.57	Grouped	V			M	No
Priviledged-Sender-Indication	652	6.3.58	Enumerated	V			M	No
LIA-Flags	653	6.3.59	Unsigned32	V			M	No
OC-Supported-Features	621 NOTE 4	6.3.60	Grouped				M, V	No
OC-OLR	623 NOTE 4	6.3.61	Grouped				M, V	No
Initial-CSeq-Sequence-Number	654	6.3.62	Unsigned32	V			M	No
SAR-Flags	655	6.3.63	Unsigned32	V			M	No
Allowed-WAF-WWSF-Identities	656	6.3.64	Grouped	V			M	No
WebRTC-Authentication-Function-Name	657	6.3.65	UTF8String	V			M	No
WebRTC-Web-Server-Function-Name	658	6.3.66	UTF8String	V			M	No
DRMP	301 NOTE 5	6.3.67	Enumerated				M, V	No
Load	NOTE 6	6.3.68	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 IETF RFC 6733 [28].

NOTE 1a: 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 2: Depending on the concrete command.

NOTE 3: The value of these attributes is defined in IETF RFC 4590 [20].

NOTE 4: The value of these attributes is defined in IETF RFC 7683 [23].

NOTE 5: The value of this attribute is defined in IETF RFC 7944 [26].

NOTE 6: The value of this attribute is defined in IETF draft-ietf-dime-load-03 [27].

6.3.1 Visited-Network-Identifier AVP

The Visited-Network-Identifier AVP is of type OctetString. This AVP contains an identifier that helps the HSS to identify the visited network (e.g. the visited network domain name). Coding of octets is H-PLMN operator specific. The I-CSCF maps a received P-Visited-Network-ID onto an Octet String value that is consistently configured in I-CSCF and HSS to uniquely identify the visited network.

6.3.2 Public-Identity AVP

The Public-Identity AVP 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 3966 [8]). Both SIP URL and TEL URL shall be in canonical form, as described in 3GPP TS 23.003 [13].

6.3.3 Server-Name AVP

The Server-Name AVP 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 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: 603 10415>

        *[Mandatory-Capability]
```

*[Optional-Capability]

*[Server-Name]

*[AVP]

6.3.5 Mandatory-Capability AVP

The Mandatory-Capability AVP is of type Unsigned32. Each value included in this AVP can be used to represent a single determined mandatory capability or a set of capabilities of an S-CSCF, as described in 3GPP TS 29.228 [1] (section 6.7).

6.3.6 Optional-Capability AVP

The Optional-Capability AVP is of type Unsigned32. Each value included in this AVP can be used to represent a single determined optional capability or a set of capabilities of an S-CSCF, as described in 3GPP TS 29.228 [1] (section 6.7).

6.3.7 User-Data AVP

The User-Data AVP 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 is of type Unsigned32.

When used in a request, the SIP-Number-Auth-Items indicates the number of authentication vectors 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 SIP-Auth-Data-Item AVPs provided by the Diameter server.

6.3.9 SIP-Authentication-Scheme AVP

The Authentication-Scheme AVP is of type UTF8String and indicates the authentication scheme used in the authentication of SIP messages. The following values are defined:

- "Digest-AKAv1-MD5": it indicates IMS-AKA authentication scheme.

NOTE 1: The S-CSCF uses the "Digest-AKAv1-MD5" authentication scheme towards the HSS for Digest-AKAv1 and Digest-AKAv2 versions, since they require from the HSS the same procedures that are already supported.

- "SIP Digest": it indicates SIP Digest authentication scheme.
- "NASS-Bundled": it indicates NASS Bundled authentication scheme.
- "Early-IMS-Security": it indicates GPRS-IMS-Bundled authentication scheme.
- "Unknown": it indicates that the authentication scheme to be used is unknown at this point.

6.3.10 SIP-Authenticate AVP

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

It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN. The Authentication Information has a fixed length of 32 octets; the 16 most significant octets shall contain the RAND, the 16 least significant octets shall contain the AUTN.

6.3.11 SIP-Authorization AVP

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

When included in an Authentication Request, it shall contain the concatenation of RAND, as sent to the terminal, and AUTS, as received from the terminal. RAND and AUTS shall both be binary encoded. See 3GPP TS 33.203 [3] for further details about RAND and AUTS. The Authorization Information has a fixed length of 30 octets; the 16 most significant octets shall contain the RAND, the 14 least significant octets shall contain the AUTS.

When included in an Authentication Request Response, it shall contain, binary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.

6.3.12 SIP-Authentication-Context AVP

The SIP-Authentication-Context AVP is of type OctectString.

6.3.13 SIP-Auth-Data-Item AVP

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

AVP format

```
SIP-Auth-Data-Item :: = < AVP Header : 612 10415 >

                [ SIP-Item-Number ]

                [ SIP-Authentication-Scheme ]

                [ SIP-Authenticate ]

                [ SIP-Authorization ]

                [ SIP-Authentication-Context ]

                [ Confidentiality-Key ]

                [ Integrity-Key ]

                [ SIP-Digest-Authenticate ]

                [ Framed-IP-Address ]

                [ Framed-IPv6-Prefix ]

                [ Framed-Interface-Id ]

                * [ Line-Identifier ]

                * [AVP]
```

6.3.14 SIP-Item-Number AVP

The SIP-Item-Number AVP is of type Unsigned32.

6.3.15 Server-Assignment-Type AVP

The Server-Assignment-Type AVP is of type Enumerated, and indicates the type of server update, request or notification 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 and to retrieve the S-CSCF restoration information for a registered Public User Identity, 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 or update of the S-CSCF Restoration Information.

UNREGISTERED_USER (3)

The request is generated in the following cases:

- The S-CSCF received a request for a Public Identity that is not registered, or
- An AS sent an originating request on behalf of a Public Identity that is not registered, or
- The S-CSCF identified a P-CSCF failure for a Public User Identity that is registered with only one Private User Identity and started the P-CSCF Restoration procedure including the P-CSCF Restoration Indication in the request to the HSS.

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 request is generated in the following cases:

- The S-CSCF, due to administrative reasons or network issues, has performed the de-registration of an identity.
- The S-CSCF identified a P-CSCF failure for a Public User Identity that is registered with more than one Private User Identity and started the P-CSCF Restoration procedure including the P-CSCF Restoration Indication in the request to the HSS.

AUTHENTICATION_FAILURE (9)

The authentication of a user has failed.

AUTHENTICATION_TIMEOUT (10)

The authentication timeout has occurred.

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.

AAA_USER_DATA_REQUEST (12)

Used in the SWx protocol, defined in 3GPP TS 29.273 [18]. This value is not used in the Cx protocol.

PGW_UPDATE (13)

Used in the SWx protocol, defined in 3GPP TS 29.273 [18]. This value is not used in the Cx protocol.

RESTORATION (14)

Used in the SWx protocol, defined in 3GPP TS 29.273 [18]. This value is not used in the Cx protocol.

6.3.16 Deregistration-Reason AVP

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

AVP format

```
Deregistration-Reason :: = < AVP Header : 615 10415 >

                { Reason-Code }

                [ Reason-Info ]

                * [AVP]
```

6.3.17 Reason-Code AVP

The Reason-Code AVP 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 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 is of type Grouped, and contains the addresses of the charging functions.

AVP format

```
Charging-Information :: = < AVP Header : 618 10415 >

                [ 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 is of type DiameterURI. This AVP contains the address of the Primary Online Charging Function. The receiving network element shall extract the FQDN of the DiameterURI in this AVP and may use it as content of the Destination-Host AVP for the Diameter accounting requests. The parent domain of the FQDN in the DiameterURI shall be used as Destination-Realm. The number of labels used for the Destination-Realm shall be determined before the Charging Information is provisioned and may be a configuration option.

NOTE: A FQDN is an absolute domain name including a subdomain and its parent domain. The subdomain and the parent domain contain one or more labels separated by dots.

6.3.21 Secondary-Event-Charging-Function-Name AVP

The Secondary-Event-Charging-Function-Name AVP is of type DiameterURI. This AVP contains the address of the Secondary Online Charging Function. The Destination-Host and Destination-Realm values for the Diameter accounting requests should be extracted from the DiameterURI in the way indicated in clause 6.3.20.

6.3.22 Primary-Charging-Collection-Function-Name AVP

The Primary-Charging-Collection-Function-Name AVP is of type DiameterURI. This AVP contains the address of the Primary Charging Data Function. The Destination-Host and Destination-Realm values for the Diameter accounting requests should be extracted from the DiameterURI in the way indicated in clause 6.3.20.

6.3.23 Secondary-Charging-Collection-Function-Name AVP

The Secondary-Charging-Collection-Function-Name AVP is of type DiameterURI. This AVP contains the address of the Secondary Charging Data Function. The Destination-Host and Destination-Realm for the Diameter accounting requests values should be extracted from the DiameterURI in the way indicated in clause 6.3.20.

6.3.24 User-Authorization-Type AVP

The User-Authorization-Type AVP 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 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 Void

6.3.26 User-Data-Already-Available AVP

The User-Data-Already-Available AVP 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 is of type OctetString, and contains the Confidentiality Key (CK).

6.3.28 Integrity-Key AVP

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

6.3.29 Supported-Features AVP

The Supported-Features AVP is of type Grouped. If this AVP is present it may inform the destination host about the features that the origin host supports for the application. The Feature-List AVP contains a list of supported features of the origin host. The Vendor-Id AVP and the Feature-List-ID AVP shall together identify which feature list is carried in the Supported-Features AVP for the Application-ID present in the command header.

Where a Supported-Features AVP is used to identify features that have been defined by 3GPP, the Vendor-Id AVP shall contain the vendor ID of 3GPP. Vendors may define proprietary features, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Features AVP is used to identify features that have been defined by a vendor other than 3GPP, it shall contain the vendor ID of the specific vendor in question.

If there are multiple feature lists defined by the same vendor and the same application, the Feature-List-ID AVP shall differentiate those lists from one another. The destination host shall use the value of the Feature-List-ID AVP to identify the feature list.

AVP format

```
Supported-Features ::=  < AVP header: 628 10415 >
                        { Vendor-Id }
                        { Feature-List-ID }
                        { Feature-List }
                        *[AVP]
```

6.3.30 Feature-List-ID AVP

The Feature-List-ID AVP is of type Unsigned32 and it contains the identity of a feature list.

6.3.31 Feature-List AVP

The Feature-List AVP is of type Unsigned32 and it contains a bit mask indicating the supported features of an application. When the bit set, indicates the corresponding feature is supported by the application. For the Cx application, the meaning of the bits has been defined in 7.1.1.

6.3.32 Supported-Applications AVP

The Supported-Applications AVP is of type Grouped and it contains the supported application identifiers of a Diameter node.

AVP format

```
Supported-Applications ::= < AVP header: 631 10415 >
                          *[ Auth-Application-Id ]
*[ Acct-Application-Id ]
*[ Vendor-Specific-Application-Id ]
*[ AVP ]
```

6.3.33 Associated-Identities AVP

The Associated-Identities AVP is of type Grouped and it contains the private user identities associated to an IMS subscription.

AVP format

```
Associated-Identities ::= < AVP header: 632, 10415 >
                          *[ User-Name ]
                          *[ AVP ]
```

6.3.34 Originating-Request AVP

The Originating-Request AVP is of type Enumerated. The following value is defined:

ORIGINATING (0)

> This value indicates to the HSS that the request is related to an AS originating SIP request in the Location-Information-Request operation.

6.3.35 Wildcarded-Public-Identity AVP

The Wildcarded-Public-Identity AVP is of type UTF8String. This AVP contains a Wildcarded PSI or Wildcarded Public User Identity stored in the HSS. The syntax of the contents of this AVP is described in 3GPP TS 23.003 [13].

6.3.36 SIP-Digest-Authenticate AVP

The SIP-Digest-Authenticate is of type Grouped and it contains a reconstruction of either the SIP WWW-Authenticate or Proxy-Authentication header fields specified in IETF RFC 2617 [14].

AVP format

```
SIP-Digest-Authenticate ::= < AVP Header: 635 10415>
                          { Digest-Realm }
                           [ Digest-Algorithm ]
                          { Digest-QoP }
                          { Digest-HA1}
                          *[ AVP ]
```

6.3.37 Digest-Realm AVP

The Digest-Realm AVP is defined in IETF RFC 4740 [15].

6.3.38 Void

6.3.39 Digest-Algorithm AVP

The Digest-Algorithm AVP is defined in IETF RFC 4740 [15].

6.3.40 Digest-QoP AVP

The Digest-QoP AVP is defined in IETF RFC 4740 [15].

6.3.41 Digest-HA1 AVP

The Digest-HA1 AVP is defined in IETF RFC 4740 [15].

6.3.42 Line-Identifier AVP

The Line-Identifier AVP is of type OctetString. This AVP has Vendor Id ETSI (13019) and AVP code 500. This AVP contains a fixed broadband access line identifier associated with the user.

6.3.43 Wildcarded-IMPU AVP

The Wildcarded-IMPU AVP is of type UTF8String. This AVP contains a Wildcarded Public User Identity stored in the HSS. The syntax of the contents of this AVP is described in 3GPP TS 23.003 [13].

Note: This AVP is used by Sh interface as specified in the 3GPP TS 29.328 [16] and 3GPP TS 29.329 [11].

6.3.44 UAR-Flags AVP

The UAR-Flags AVP is of type Unsigned32 and it contains a bit mask. The meaning of the bits is defined in the following table:

Table 6.3.44.1: UAR-Flags

Bit	Name	Description
0	IMS Emergency Registration	This bit, when set, indicates that the request corresponds to an IMS Emergency Registration.
Bits not defined in this table shall be cleared by the sending I-CSCF and discarded by the receiving HSS.		

6.3.45 Loose-Route-Indication AVP

The Loose-Route-Indication AVP is of type Enumerated and indicates to the S-CSCF whether or not the loose route mechanism is required to serve the registered Public User Identities. The following values are defined:

LOOSE_ROUTE_NOT_REQUIRED (0)

LOOSE_ROUTE_REQUIRED (1)

6.3.46 SCSCF-Restoration-Info AVP

The SCSCF-Restoration-Info AVP is of type Grouped and it contains the information required for an S-CSCF to handle the requests for a user.

AVP format

```
SCSCF-Restoration-Info ::= < AVP Header: 639, 10415>
                           { User-Name }
                           1*{ Restoration-Info }
                           [ SIP-Authentication-Scheme ]
                            *[ AVP ]
```

6.3.47 Path AVP

The Path AVP is of type OctetString and it contains a comma separated list of SIP proxies in the Path header as defined in IETF RFC 3327 [17].

6.3.48 Contact AVP

The Contact AVP is of type OctetString and it contains the Contact Addresses and Parameters in the Contact header as defined in IETF RFC 3261 [11].

6.3.49 Subscription-Info AVP

The Subscription-Info AVP is of type Grouped and it contains the UE's subscription information. The Contact AVP contains the Contact Address and Parameters in the Contact header of the subscription request.

AVP format

```
Subscription-Info ::= < AVP Header: 642, 10415>
                            { Call-ID-SIP-Header }
                            { From-SIP-Header }
                            { To-SIP-Header }
                            { Record-Route }
                            {Contact}
                            *[ AVP ]
```

6.3.49.1 Call-ID-SIP-Header AVP

The Call-ID-SIP-Header AVP is of type OctetString and it contains the information in the Call-ID header as defined in IETF RFC 3261 [11].

6.3.49.2 From-SIP-Header AVP

The From-SIP-Header AVP is of type OctetString and it contains the information in the From header as defined in IETF RFC 3261 [11].

6.3.49.3 To-SIP-Header AVP

The To-SIP-Header AVP is of type OctetString and it contains the information in the To header as defined in IETF RFC 3261 [11].

6.3.49.4 Record-Route AVP

The Record-Route AVP is of type OctetString and it contains a comma separated list of Record Route header(s) as defined in IETF RFC 3261 [11].

6.3.50 Associated-Registered-Identities AVP

The Associated-Registered-Identities AVP is of type Grouped and it contains the Private User Identities registered with the Public User Identity received in the request command.

AVP format

```
Associated-Registered-Identities ::= < AVP header: 647, 10415 >
```

```
                    *[ User-Name ]

                    *[ AVP ]
```

6.3.51 Multiple-Registration-Indication

The Multiple-Registration-Indication AVP is of type Enumerated and indicates to the HSS whether or not the request is related to a multiple registration. The following values are defined:

NOT_MULTIPLE_REGISTRATION (0)

MULTIPLE_REGISTRATION (1)

6.3.52 Restoration-Info AVP

The Restoration-Info AVP is of type Grouped and it contains the information related to a specific registration required for an S-CSCF to handle the requests for a user. The Contact AVP contains the Contact Address and Parameters in the Contact header of the registration request.

AVP format

```
Restoration-Info ::= < AVP Header: 649, 10415>

                    { Path }

                    { Contact }

                    [ Initial-CSeq-Sequence-Number ]

                    [ Call-ID-SIP-Header ]

                    [ Subscription-Info ]

                    *[ AVP ]
```

6.3.53 Framed-IP-Address AVP

The Framed-IP-Address AVP is defined in IETF RFC 4005 [19].

6.3.54 Framed-IPv6-Prefix AVP

The Framed-IPv6-Prefix AVP is defined in IETF RFC 4005 [19], and it shall be encoded as defined in IETF RFC 3162 [22].

6.3.55 Framed-Interface-Id AVP

The Framed-Interface-Id AVP is defined in IETF RFC 4005 [19].

6.3.56 Session-Priority AVP

The Session-Priority AVP is of type Enumerated and indicates to the HSS the session's priority. The following values are defined:

PRIORITY-0 (0)

PRIORITY-1 (1)

PRIORITY-2 (2)

PRIORITY-3 (3)

PRIORITY-4 (4)

PRIORITY-0 is the highest priority.

The value of the AVP when sent to the HSS is mapped from the value received by the CSCF as described in 3GPP TS 24.229 table A.162. The mapping is operator specific.

This AVP may be placed as close to the Diameter header as possible in order to potentially allow optimized processing at the receiver.

6.3.57 Identity-with-Emergency-Registration AVP

The Identity-with-Emergency-Registration AVP is of type Grouped and it contains a pair of private/public user identities which are emergency registered.

AVP format

```
Identity-with-Emergency-Registration ::= < AVP header: 651, 10415 >
                              { User-Name }
                              { Public-Identity }
                              *[ AVP ]
```

6.3.58 Priviledged-Sender-Indication AVP

The Priviledged-Sender-Indication AVP is of type Enumerated and indicates to the S-CSCF whether or not the Private User Identity shall be considered as a priviledged sender. The following values are defined:

NOT_PRIVILEDGED_SENDER (0)PRIVILEDGED_SENDER (1)

6.3.59 LIA-Flags

The LIA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 6.3.59.1.

Table 6.3.59.1: LIA-Flags

Bit	Name	Description
0	PSI Direct Routing Indication	This bit, when set, indicates the request corresponds to PSI Direct Routing, what implies that HSS returns an AS name in Server-Name AVP.
NOTE: Bits not defined in this table shall be cleared by the sending HSS and discarded by the receiving I-CSCF.		

6.3.60 OC-Supported-Features

The OC-Supported-Features AVP is of type Grouped and it is defined in IETF RFC 7683 [23]. This AVP is used to support Diameter overload control mechanism.

6.3.61 OC-OLR

The OC-OLR AVP is of type Grouped and it is defined in IETF RFC 7683 [23]. This AVP is used to support Diameter overload control mechanism.

6.3.62 Initial-CSeq-Sequence-Number AVP

The Initial-CSeq-Sequence-Number AVP is of type Unsigned32, and it contains the sequence number of the CSeq header field contained in the initial successful REGISTER request, as defined in IETF RFC 3261 [11].

6.3.63 SAR-Flags

The SAR-Flags AVP is of type Unsigned32 and it contains a bit mask. The meaning of the bits is defined in the following table:

Table 6.3.63.1: SAR-Flags

Bit	Name	Description
0	P-CSCF Restoration Indication	This bit, when set, indicates that the P-CSCF-Restoration-mechanism feature shall be executed, as described in 3GPP TS 23.380 [24], subclause 5.4. This AVP is optionally present only when Server-Assignment-Type takes the value ADMINISTRATIVE_DEREGISTRATION or UNREGISTERED_USER.
Note: Bits not defined in this table shall be cleared by the sending S-CSCF and discarded by the receiving HSS.		

6.3.64 Allowed-WAF-WWSF-Identities AVP

The Allowed-WAF-WWSF-Identities AVP is of type Grouped and contains the addresses of the WAFs and WWSFs allowed for the subscription.

AVP format

```
Allowed-WAF-WWSF-Identities :: = < AVP Header : 656 10415 >

              *[ WebRTC-Authentication-Function-Name ]

              *[ WebRTC-Web-Server-Function-Name ]

              *[ AVP]
```

6.3.65 WebRTC-Authentication-Function-Name AVP

The WebRTC-Authentication-Function-Name AVP is of type UTF8String and contains the address of a WAF allowed for the subscription. For the format of the string see IETF draft-holmberg-sipcore-auth-id-01 [25].

6.3.66 WebRTC-Web-Server-Function-Name AVP

The WebRTC-Web-Server-Function-Name AVP is of type UTF8String and contains the address of a WWSF allowed for the subscription. For the format of the string see IETF draft-holmberg-sipcore-auth-id-01 [25].

6.3.67 DRMP AVP

The DRMP AVP is of type Enumerated and it is defined in IETF RFC 7944 [26]. This AVP allows the HSS/SLF and the S-CSCF/I-CSCF 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.

6.3.68 Load

The Load AVP is of type Grouped and it is defined in IETF draft-ietf-dime-load-03 [27]. 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 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 5001-5011. 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 16777216 for the 3GPP Cx interface application.

7 Special Requirements

7.1 Version Control

New functionality - i.e. functionality beyond the Rel-5 standard - shall be introduced by post-Rel-5 versions of this specification to the Diameter applications as follows:

1. If possible, the new functionality shall be defined optional.
2. If backwards incompatible changes can not be avoided, the new functionality should be introduced as a feature, see 7.1.1.
3. If the change would be backwards incompatible even as if it was defined as a feature, a new version of the interface shall be created by changing the application identifier of the Diameter application, see 7.1.2.

7.1.1 Defining a new feature

The base functionality for the Cx is the 3GPP Rel-5 standard and a feature is an extension to that functionality. A feature is a functional entity that has a significant meaning to the operation of a Diameter application i.e. a single new parameter without a substantial meaning to the functionality of the Diameter endpoints should not be defined to be a new feature. If the support for a feature is defined mandatory in a post-Rel-5 versions of this specification, the feature concept enables interworking between Diameter endpoints regardless of whether they support all, some or none of the features of the application. Features should be defined so that they are independent from one another.

The content of a feature shall be defined as a part of the specification of the affected application messages. If new AVPs are added to the commands because of the new feature, the new AVPs shall have the ‘M’ bit cleared and the AVP shall not be defined mandatory in the command ABNF. The support for a feature may be defined to be mandatory behaviour of a node.

As an option to defining a feature, an extension to S-CSCF functionality for post-Rel-5 version may be defined as part of the list of mandatory capabilities that is used by the I-CSCF during the process of selecting an S-CSCF, as described in 3GPP TS 29.228 [1]. Any new feature should be taken into account in the definition of the list of mandatory and optional S-CSCF capabilities. Guidelines for the definition of S-CSCF Capabilities are described in 3GPP TS 29.228 [1].

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

Table 7.1.1: Features of Feature-List-ID 1 used in Cx

Feature bit	Feature	M/O	Description
0	SiFC	O	Shared iFC sets This feature is applicable for the SAR/SAA and PPR/PPA command pairs. If both the HSS and the S-CSCF support this feature, subsets of Initial Filter Criteria may be shared by several service profiles and the HSS shall download the shared iFC sets implicitly by downloading the unique identifiers of the shared iFC sets to the S-CSCF. By means of a locally administered database, the S-CSCF then maps the downloaded identifiers onto the shared iFC sets. If the DSAI feature, as defined in 3GPP TS 29.328 [16], is also active with the shared iFC sets feature then the HSS shall behave as described below: If the DSAI feature is active with the shared iFC sets feature and if all the iFCs bounding to a Shared iFC set are not masked by the DSAI, the HSS shall download the unique identifier of the shared iFC set to the S-CSCF. If some iFCs or all the iFCs bounding to a shared iFC set are masked by the DSAI, the HSS shall not download the identifier of the shared iFC set. Instead the HSS shall - download the remaining non masked iFCs of the shared iFC set explicitly or - download suitable identifiers of other shared iFC sets, i.e. those covering exactly the remaining non masked iFCs and which do not contain masked iFCs or - download a combination of identifiers of shared iFC sets and explicit iFCs which cover exactly the remaining non masked iFCs. If the S-CSCF does not support this feature, the HSS shall not download identifiers of shared iFC sets. Instead as a default behavior the HSS shall (by means of a locally administered database) download the iFCs of a shared iFC set explicitly. If the HSS does not support this feature, no special default behaviour is required for the S-CSCF. Note: In using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and HSSs consistent.
1	AliasInd	M	Alias Indication This feature is applicable for the SAR/SAA and PPR/PPA command pairs. If both the HSS and the S-CSCF support this feature, different aliases groups may be sent within the same service profile. Identities within the same service profile that are aliases shall be sent with identical alias group ID. If the S-CSCF does not support this feature, the HSS shall send within the service profile only those identities that are aliases. Public User Identities that are not aliases of each other shall be sent in different service profiles even if these service profiles have exactly the same Core Network Service Authorization, Initial Filter Criteria, and Shared iFC Set information and these service profiles only differ in the contained Public User Identities. This is done in order to allow backwards compatibility since part of the handling of aliases in the S-CSCF was there before this indication was required and it applied to identities that share the same service profile and implicit registration set. In this case, the S-CSCF does not provide any additional treatment of aliases than that which existed before this indication was required. If the HSS does not support this feature, no special default behaviour is required for the S-CSCF. Note: All identities included in a single SAA or PPR command are always within one implicit registration set.
2	IMSRestorationInd	O	IMS Restoration Indication This feature is applicable for the UAR/UAA, LIR/LIA, SAR/SAA command pairs. If both the HSS and the I-CSCF support this feature, in case the S-CSCF currently assigned in the HSS to the Public User Identity cannot be contacted the I-CSCF shall trigger the assignment of a new S-CSCF. If both the HSS and the S-CSCF support this feature, the S-CSCF shall send S-CSCF Restoration Information to the HSS. The HSS shall send this information element in SAA to the S-CSCF when required. If the S-CSCF does not support this feature, the HSS shall not send the IMS Restoration Information to the S-CSCF.

3	P-CSCF-Restoration-mechanism	O	HSS-based P-CSCF Restoration mechanism. This feature is applicable for the SAR/SAA command pair. If both the HSS and the S-CSCF support this feature, the S-CSCF shall send the P-CSCF-Restoration-Indication in SAR-Flags AVP to the HSS when required as described by 3GPP TS 23.380 [24] clause 5.4. If the HSS does not support this feature, the S-CSCF shall not send the P-CSCF-Restoration-Indication to HSS.
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 origin host may discover the supported features of the destination host with the dynamic discovery mechanism defined in 7.2 or via local O&M interfaces.

7.1.2 Changing the version of the interface

The version of an interface shall be changed by a future version of this specification only if there is no technically feasible means to avoid backwards incompatible changes to the Diameter application, i.e. to the current version of the interface. However, if the incompatible changes can be capsulated within a feature, there is no need to change the version of the interface. The versioning of an interface shall be implemented by assigning a new application identifier for the interface. This procedure is in line with the Diameter base protocol (see IETF RFC 3588) which defines that if an incompatible change is made to a Diameter application, a new application identifier shall be assigned for the Diameter application.

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

Table 7.1.2: Application identifiers used in Cx

Application identifier	First applied
16777216	3GPP Rel-5

The origin host may discover which versions of an interface the destination host supports within the capabilities exchange (i.e. CER/CEA command), via the error messages defined in the chapter 7.3 or via local O&M interfaces.

7.2 Supported features

Features that are not indicated in the Supported-Features AVPs within a given application message shall not be used to construct that message. A request application message shall always be compliant with the list of supported features indicated in the Supported-Features AVPs within the application message. If a feature does not have an effect on constructing an application message, the message is by definition compliant with the feature. If no features are indicated in the application message, no features - i.e. no extensions to Rel-5 - shall be used to construct the application message. An answer application message shall always indicate in the Supported-Features AVPs the complete set of features supported by the sender of the answer application message. An answer application message shall be compliant with the features commonly supported by the sender of the request and answer application messages.

The sender of a request application message shall discover for a given application message pair which features a destination host supports as described in 7.2.1. The discovered features of one command pair may be applicable to other command pairs within the application. Different commands within an application may support a different set of features. After discovering the features a destination host supports for a given application message pair, the sender of the request application message may store the information on the supported features of the destination host and it may use the features the destination host supports to construct the subsequent request application messages sent to the destination host.

7.2.1 Dynamic discovery of supported features

When sending a request application message to a destination host whose supported features the sender does not know, the request application message shall include the Supported-Features AVP containing the set of features required to process the request and generate the answer. An exception to this is where the origin host does not use any features to construct the request application message and it is not prepared to accept an answer application message which is constructed by making use of any features. For this exception the origin host need not include the Supported-Features AVP within the message.

The Supported-Features AVP within a request application message shall always have the 'M' bit set and within an answer application message the AVP shall never have the 'M' bit set. An exception to this is where the origin host does not use any supported feature to construct the request application message but is prepared to accept an answer application message which is constructed by making use of supported features. For this exception it is optional for the origin host to set the 'M' bit of the Supported-Features AVP within the request application message.

On receiving a request application message, the destination host shall do one of the following:

- If it supports all features indicated in the Supported-Features AVPs within the request message, the answer application message shall include Supported-Features AVPs identifying the complete set of features that it supports. The Experimental-Result-Code AVP shall not be set to DIAMETER_ERROR_FEATURE_UNSUPPORTED.

- If the request application message does not contain any Supported-Features AVPs, the answer application message shall include either Supported-Features AVPs identifying the complete set of features that it supports or, if it does not support any features, no Supported-Features AVPs shall be present. The Experimental-Result-Code AVP shall not be set to DIAMETER_ERROR_FEATURE_UNSUPPORTED.

- If it does not support all the features indicated in the Supported-Features AVPs with the 'M' bit set, it shall return the answer application message with the Experimental-Result-Code AVP set to DIAMETER_ERROR_FEATURE_UNSUPPORTED and it shall include also Supported-Features AVPs containing lists of all features that it supports.

- If it does not support Supported-Features AVP and it receives a request application message containing Supported-Features AVPs with the 'M' bit set, it will return the answer application message with the Result-Code AVP set to DIAMETER_AVP_UNSUPPORTED and a Failed-AVP AVP containing at least one Supported-Features AVP as received in the request application message.

If an answer application message is received with the Experimental-Result-Code AVP set to DIAMETER_ERROR_FEATURE_UNSUPPORTED or with the Result-Code AVP set to DIAMETER_AVP_UNSUPPORTED, the sender of the request application message may, based on the information in the received Supported-Features AVP or the lack of the AVP in the message, re-send the Diameter message containing only the common supported features.

7.3 Interface versions

The sender of the request application message may discover which versions of an interface a destination host supports together with the capabilities exchange (i.e. CER/CEA command pair) and with error mechanisms defined to the application messages in 7.3.1. The sender of the request application message should store information on all versions of the interface the destination host supports. The sender of the request application message should use the latest common version of the application supported by the destination host to send the request.

If the receiver of the request application message itself or the versions of the interface it supports are not yet known, the sender of the request application message should use the latest supported version of the interface of the Diameter peer (i.e. Diameter proxy, redirect or relay agent) discovered during the capabilities exchange. If the Diameter peer is a redirect or relay agent, which advertises the 0xffffffff as an application identifier, the sender of the request application message shall use its own latest supported version of the interface when initiating the request.

7.3.1 Discovery of supported interface versions

When a Diameter agent receives a request application message and the Diameter agent doesn't find any upstream peer that would support the application identifier indicated in the request, the Diameter agent shall return the result code DIAMETER_UNABLE_TO_DELIVER and it may also return the list of the application identifiers, which are supported by the destination host of the request application message. The supported application identifiers are carried in the answer application message in the Supported-Applications grouped AVP.

Message format for the answer application message (based on the RFC 3588, section 7.2) is as follows:

```
<answer-message> ::=  < Diameter Header: code, ERR [PXY] >
                    0*1< Session-Id >
                       { Origin-Host }
                       { Origin-Realm }
                       { Result-Code }
                       [ Origin-State-Id ]
                       [ Error-Reporting-Host ]
                       [ Proxy-Info ]
                       [ Supported-Applications ]
                       * [ AVP ]
```

If the receiver of a request application message does not support the application identifier indicated in the message, it shall return the result code DIAMETER_APPLICATION_UNSUPPORTED and it may also return the list of all application identifiers it supports. The supported application identifiers are carried in the Supported-Applications grouped AVP. The error message format is as specified above.

If an answer application message is received with Result-Code AVP set to DIAMETER_UNABLE_TO_DELIVER or Experimental-Result-Code AVP set to DIAMETER_APPLICATION_UNSUPPORTED and the message contains the Supported-Applications AVP, the receiver of the answer application message may select, based on the information in the Supported-Applications AVP, the latest common version of the interface with the destination host and re-send the Diameter message with a structure conforming to the ABNF of that release.

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
Mar 2003	CN#19	NP-030101	012	1	Update TS 29.229 after Diameter has become RFC	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	015	1	Clarification on Re-allocation of S-CSCF	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	018	1	Handling of non supported data in the S-CSCF when the profile is being updated.	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	014	-	Correction to the values of User-Authorizatin-Type AVP	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	013	-	Replacement of the NAS-Session-Key AVP	5.2.0	5.3.0
Jun 2003	CN#20	NP-030215	019	-	Conditionality of User-Name AVP in Server-Assignment-Answer	5.3.0	5.4.0
Sep 2003	CN#21	NP-030383	022	1	Critical Correction on the PPR command code	5.4.0	5.5.0
Dec 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
Dec 2003	CN#22	NP-030500	027	-	User-Authorization-Type	5.5.0	5.6.0
Dec 2003	CN#22	NP-030518	029	-	Clarification of inclusion of elements in Charging Information	5.5.0	5.6.0
Dec 2003	CN#22				Application IDs and references updated	5.5.0	5.6.0
Mar 2004	CN#23	NP-040055	035	-	Error for no identification in SAR command	5.6.0	6.0.0
Jun 2004	CN#24	NP-040215	037	1	Update of the charging addresses from HSS	6.0.0	6.1.0
Jun 2004	CN#24	NP-040215	043	-	Multimedia-Auth-Request (MAR) Command Message Format Corrections	6.0.0	6.1.0
Jun 2004	CN#24	NP-040215	050	2	Use of Vendor-Id by 3GPP	6.0.0	6.1.0
Sep 2004	CN#25	NP-040395	065	2	Application version control	6.1.0	6.2.0
Sep 2004	CN#25	NP-040401	056	-	Optimization of User Profile Download	6.1.0	6.2.0
Sep 2004	CN#25	NP-040396	058	-	Simplification of the User Profile Split concept	6.1.0	6.2.0
Sep 2004	CN#25	NP-040401	061	-	Correction of the Application-Id code	6.1.0	6.2.0
Sep 2004	CN#25	NP-040412	063	1	Re-numbering of 3GPP specific AVP codes	6.1.0	6.2.0
Dec 2004	CN#26	NP-040523	070	-	Cx ABNF corrections	6.2.0	6.3.0
Mar 2005	CN#27	NP-050030	078	2	Correction of authentication-related AVPs	6.3.0	6.4.0
Mar 2005	CN#27	NP-050037	079	-	TEL-URI reference update	6.3.0	6.4.0
Mar 2005	CN#27	NP-050030	082	1	Introduction of Failed-AVP	6.3.0	6.4.0
Jun 2005	CT#28	CP-050086	087	-	Correction of reference	6.4.0	6.5.0
Jun 2005	CT#28	CP-050086	089	1	Editorial corrections	6.4.0	6.5.0
Jun 2005	CT#28	CP-050086	088	2	Corrections to message parameters	6.4.0	6.5.0
Sep 2005	CT#29	CP-050440	091	2	Private identities on the Cx	6.5.0	6.6.0
Sep 2005	CT#29	CP-050282	093	1	Charging-Information correction	6.5.0	6.6.0
Sep 2005	CT#29	CP-050296	094	-	Error code cleanup	6.5.0	6.6.0
Dec 2005	CT#30	CP-050611	095	1	Removal of overhead in Private Identities handling in RTR	6.6.0	6.7.0
Dec 2005	CT#30	CP-050611	098	1	Incorrect Definition of Supported-Applications AVP	6.6.0	6.7.0
Jan 2006					Rel-7 version was created because of ETSI TISPAN references.	6.7.0	7.0.0
Mar 2006	CT#31	CP-060084	0099	-	Supported Features Text missing	7.0.0	7.1.0
Jun 2006	CT#32	CP-060302	0108	-	S-CSCF reselection removal	7.1.0	7.2.0
Jun 2006	CT#32	CP-060308	0110	3	Definition of new Feature for Cx	7.1.0	7.2.0
Sep 2006	CT#33	CP-060417	0114	3	AS originating requests on behalf of a user	7.2.0	7.3.0
Sep 2006	CT#33	CP-060405	0118	2	Correction of discovery of supported features in Sh and Cx	7.2.0	7.3.0
Sep 2006	CT#33	CP-060417	0119	1	Sharing feature support information between command pairs	7.2.0	7.3.0
Dec 2006	CT#34	CP-060566	0124	1	Optimization of handling of Wildcarded PSIs	7.3.0	7.4.0
Mar 2007	CT#35	CP-070020	0125	1	M-bit in SupportedFeatures AVP	7.4.0	7.5.0
Sep 2007	CT#37	CP-070520	0129	-	Misalignment of Mandatory Items in the MAR	7.5.0	7.6.0
Nov 2007	CT#38	CP-070744	0132	6	Add alias as a new feature	7.6.0	7.7.0
Nov 2007	CT#38	CP-070755	0130	4	Updates to 29.229 for Digest on the Cx interface	7.7.0	8.0.0
Mar 2008	CT#39	CP-080022	0138	2	Update 29.229 for Supporting NASS-Bundled-Authentication	8.0.0	8.1.0
Mar 2008	CT#39	CP-080019	0139	-	SIP Digest password push	8.0.0	8.1.0
Mar 2008	CT#39	CP-080019	0141	2	Wildcarded Public User Identities	8.0.0	8.1.0
Jun 2008	CT#40	CP-080261	0145	1	Correction to the behavior of the HSS defined in the SiFC feature	8.1.0	8.2.0
Jun 2008	CT#40	CP-080261	0146	2	Realm and Host to be used for Charging	8.1.0	8.2.0
Sep 2008	CT#41	CP-080456	0149	1	Emergency Public User Identity Removal	8.2.0	8.3.0
Sep 2008	CT#41	CP-080460	0155	1	Support of "Loose-Route" indication from HSS	8.2.0	8.3.0
Sep 2008	CT#41	CP-080463	0156	1	Cx Impacts of IMS Restoration Procedures	8.2.0	8.3.0
Sep 2008	CT#41	CP-080463	0158		Add IMS Restoration as a new feature	8.2.0	8.3.0
Sep 2008	CT#41	CP-080463	0159	1	Addition of Registered Private Identities in SAA	8.2.0	8.3.0

Sep 2008	CT#41	CP-080460	0160	1	Add Assigned S-CSCF name to SAA	8.2.0	8.3.0
Dec 2008	CT#42	CP-080708	0163		Removal of Digest Domain	8.3.0	8.4.0
Dec 2008	CT#42	CP-080708	0166	2	Diameter Proxy Agent - an alternative User Identity to HSS resolution mechanism	8.3.0	8.4.0
Mar 2009	CT#43	CP-090026	0167		Multiple Registrations in Registration	8.4.0	8.5.0
Mar 2009	CT#43	CP-090026	0168	1	Restoration Information for Multiple Registrations	8.4.0	8.5.0
Mar 2009	CT#43	CP-090026	0169		Update for Restoration	8.4.0	8.5.0
Mar 2009	CT#43	CP-090051	0170	1	Definition of Server-Assignment-Type values in Cx	8.4.0	8.5.0
Mar 2009	CT#43	CP-090028	0171		Support for GPRS IMS Bundled Authentication (GIBA) in Cx	8.4.0	8.5.0
Mar 2009	CT#43	CP-090025	0172		Use of canonical form for SIP URI/tel URI in Cx interface	8.4.0	8.5.0
Mar 2009	CT#43	CP-090026	0175	1	Comma separated list for Path, Contact and Record-Route AVPs	8.4.0	8.5.0
Jun 2009	CT#44	CP-090484	0176	2	Contact storage in reg event subscription	8.5.0	8.6.0
Jun 2009	CT#44	CP-090303	0177	1	Comma separated list for path AVP	8.5.0	8.6.0
Sep	CT#45	CP-090526	0181		Dx over SCTP	8.6.0	8.7.0
Dec 2009	CT#46	CP-090784	0182	2	SIP Digest AVP Flag Settings	8.7.0	8.8.0
Dec 2009	CT#46	CP-090781	0185	1	Unregistered user clarification	8.7.0	8.8.0
Dec 2009	CT#46	CP-090778	0188	2	Session-Priority AVP	8.7.0	8.8.0
Dec 2009	CT#46	CP-091030	0189		Validity of Feature Bit Value in Feature-List AVP	8.7.0	8.8.0
Dec 2009	CT#46				Upgraded unchanged from Rel-8	8.8.0	9.0.0
Mar 2010	CT#47	CP-100239	0195	1	Wildcarded Public Identity	9.0.0	9.1.0
Mar 2010	CT#47	CP-100031	0199		Wildcarded Public Identities handling	9.0.0	9.1.0
Jun 2010	CT#48	CP-100412	0205	1	Digest AVPs wrongly defined	9.1.0	9.2.0
Sep 2010	CT#49	CP-100447	0207	2	Wildcarded Identities handling	9.2.0	9.3.0
Sep 2010	CT#49	CP-100442	0209	2	Mandatory and optional capabilities handling	9.2.0	9.3.0
Sep 2010	CT#49	CP-100442	0212		Reference to SCTP IETF RFC obsolete	9.2.0	9.3.0
Sep 2010	CT#49	CP-100463	0213	2	Restoration Data Backup	9.2.0	9.3.0
Sep 2010	CT#49	CP-100447	0216		Encoding of Framed-IPv6-Prefix AVP	9.2.0	9.3.0
2011-03	-	-	-	-	Update to Rel-10 version (MCC)	9.3.0	10.0.0
Jun 2011	CT#52	CP-110349	0224	2	Handling of RTR for Emergency Registration	10.0.0	10.1.0
Jun 2011	CT#52	CP-110349	0227		Error in assignment type for backward compatibility scenarios	10.0.0	10.1.0
Jun 2011	CT#52	CP-110349	0230		User-Authorization-Type AVP error in description	10.0.0	10.1.0
Sep 2011	CT#53	CP-110566	0233	1	Priviledged sender	10.1.0	10.2.0
Dec 2011	CT#54	CP-110781	0240	1	Restoration of Wildcarded-IMPU AVP	10.2.0	10.3.0
Dec 2011	CT#54	CP-110812	0235	2	Server Assignment Type AVP definition	10.3.0	11.0.0
Sep 2012	CT#57	CP-120440	0247	1	Emergency registrations do not affect registration status	11.0.0	11.1.0
Dec 2012	CT#58	CP-120743	0251	2	PSI direct routing with restoration procedures	11.1.0	11.2.0
Mar 2013	CT#59	CP-130011	0258	1	Originating-request AVP in LIR	11.2.0	11.3.0
Jun 2013	CT#60	CP-130374	0260	1	Supported-Feature AVP carries list of features specific to the Application-ID	11.3.0	11.4.0
Jun 2013	CT#60	CP-130380	0259	-	Visited Network ID coding	11.4.0	12.0.0
Dec 2013	CT#62	CP-130627	0263	1	Session-Priority AVP	12.0.0	12.1.0
Jun 2014	CT#64	CP-140243	0264	2	Diameter Overload Control Over Cx	12.1.0	12.2.0
Sep 2014	CT#65	CP-140515	0265	1	T-GRUU restoration	12.2.0	12.3.0
Sep 2014	CT#65	CP-140506	0266	2	P-CSCF Restoration indication	12.2.0	12.3.0
Dec 2014	CT#66	CP-140794	0268	2	P-CSCF Restoration mechanism new feature	12.3.0	12.4.0
Dec 2014	CT#66	CP-140794	0270	1	P-CSCF Restoration mechanism new error	12.3.0	12.4.0
Dec 2014	CT#66	CP-140773	0269	-	M-bit clarification	12.3.0	12.4.0
Mar 2015	CT#67	CP-150023	0273	1	SIP-Authentication-Scheme AVP encoding	12.4.0	12.5.0
Jun 2015	CT#68	CP-150261	0274	-	SAR-Flags inclusion in SAR command	12.5.0	12.6.0
Sep 2015	CT#69	CP-150428	0276	1	SIP-Auth-Data-Item sub AVPs clarifications	12.6.0	12.7.0
Sep 2015	CT#69	CP-150436	0275	1	Server-Assignment-Type AVP update to consider P-CSCF Restoration	12.6.0	12.7.0
Dec 2015	CT#70	CP-150754	0279	2	Allowed WAF and/or WWSF Identities	12.7.0	12.8.0
Dec 2015	CT#70	CP-150759	0281	1	Update reference to DOIC new IETF RFC	12.7.0	12.8.0
Dec 2015	CT#70	CP-150768	0282	2	Support of the DRMP AVP over Cx/Dx	12.8.0	13.0.0
2016-12	CT#74	CP-160664	0284	1	Correction to change IETF drmp draft version to official RFC 7944	13.0.0	13.1.0
2016-12	CT#74	CP-160681	0283	1	Load Control	13.1.0	14.0.0
2017-03	CT#75	CP-170048	0285	1	Update of reference for the Diameter base protocol	14.0.0	14.1.0
2017-03	CT#75	CP-170048	0286	-	Cardinality of the Failed-AVP AVP in answer	14.0.0	14.1.0
2017-06	CT’76	CP-171018	0288	1	Support for signaling transport level packet marking	14.1.0	14.2.0