

1 3GPP2 X.S0013-006-0  
2 Version 2.0  
3 Version Date: July 2005  
4  
5



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

---

6 ***All-IP Core Network Multimedia Domain***  
7 ***Cx Interface Based on the Diameter Protocol;***  
8 ***Protocol Details***

9  
10  
11  
12  
13  
14  
15

**COPYRIGHT**

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at [secretariat@3gpp2.org](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.

---

16

- 1
- 2
- 3

**All-IP Core Network Multimedia Domain  
Cx Interface Based on the Diameter Protocol;  
Protocol Details**

**Contents**

1			
2			
3			
4			
5			
6	1	Scope .....	1
7	2	References .....	1
8	3	Definitions, symbols and abbreviations.....	1
9	3.1	Definitions.....	1
10	3.2	Abbreviations.....	2
11	4	General .....	2
12	5	Use of the Diameter base protocol.....	2
13	5.1	Securing Diameter Messages.....	2
14	5.2	Accounting functionality .....	2
15	5.3	Use of sessions .....	2
16	5.4	Transport protocol .....	3
17	5.5	Routing considerations.....	3
18	5.6	Advertising Application Support .....	3
19	6	Diameter application for Cx interface .....	3
20	6.1	Command-Code values .....	4
21	6.1.1	User-Authorization-Request (UAR) Command .....	4
22	6.1.2	User-Authorization-Answer (UAA) Command.....	5
23	6.1.3	Server-Assignment-Request (SAR) Command .....	5
24	6.1.4	Server-Assignment-Answer (SAA) Command.....	6
25	6.1.5	Location-Info-Request (LIR) Command .....	6
26	6.1.6	Location-Info-Answer (LIA) Command.....	7
27	6.1.7	Multimedia-Auth-Request (MAR) Command.....	7
28	6.1.8	Multimedia-Auth-Answer (MAA) Command .....	7
29	6.1.9	Registration-Termination-Request (RTR) Command.....	8
30	6.1.10	Registration-Termination-Answer (RTA) Command.....	8
31	6.1.11	Push-Profile-Request (PPR) Command.....	9
32	6.1.12	Push-Profile-Answer (PPA) Command .....	9
33	6.2	Experimental-Result-Code AVP values .....	9
34	6.2.1	Success .....	10
35	6.2.1.1	DIAMETER_FIRST_REGISTRATION (2001).....	10
36	6.2.1.2	DIAMETER_SUBSEQUENT_REGISTRATION (2002).....	10
37	6.2.1.3	DIAMETER_UNREGISTERED_SERVICE (2003).....	10
38	6.2.1.4	DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED (2004).....	10
39	6.2.1.5	DIAMETER_SERVER_SELECTION (2005) .....	10

1	6.2.2	Permanent Failures .....	10
2	6.2.2.1	DIAMETER_ERROR_USER_UNKNOWN (5001).....	10
3	6.2.2.2	DIAMETER_ERROR_IDENTITIES_DONT_MATCH (5002).....	11
4	6.2.2.3	DIAMETER_ERROR_IDENTITY_NOT_REGISTERED (5003).....	11
5	6.2.2.4	DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004).....	11
6	6.2.2.5	DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED (5005).....	11
7	6.2.2.6	DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED (5006).....	11
8	6.2.2.7	DIAMETER_ERROR_IN_ASSIGNMENT_TYPE (5007).....	11
9	6.2.2.8	DIAMETER_ERROR_TOO_MUCH_DATA (5008).....	11
10	6.2.2.9	DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA (5009).....	11
11	6.2.2.10	DIAMETER_MISSING_USER_ID (5010).....	11
12	6.3	AVPs .....	11
13	6.3.1	Visited-Network-Identifier AVP .....	12
14	6.3.2	Public-Identity AVP .....	13
15	6.3.3	Server-Name AVP.....	13
16	6.3.4	Server-Capabilities AVP .....	13
17	6.3.5	Mandatory-Capability AVP.....	13
18	6.3.6	Optional-Capability AVP .....	13
19	6.3.7	User-Data AVP.....	13
20	6.3.8	SIP-Number-Auth-Items AVP.....	13
21	6.3.9	SIP-Authentication-Scheme AVP.....	13
22	6.3.10	SIP-Authenticate AVP.....	14
23	6.3.11	SIP-Authorization AVP.....	14
24	6.3.12	SIP-Authentication-Context AVP.....	14
25	6.3.13	SIP-Auth-Data-Item AVP.....	14
26	6.3.14	SIP-Item-Number AVP .....	14
27	6.3.15	Server-Assnment-Type AVP .....	14
28	6.3.16	Deregistration-Reason AVP .....	15
29	6.3.17	Reason-Code AVP.....	16
30	6.3.18	Reason-Info AVP .....	16
31	6.3.19	Charging-Information AVP.....	16
32	6.3.20	Primary-Event-Charging-Function-Name AVP .....	16
33	6.3.21	Secondary-Event-Charging-Function-Name AVP .....	16
34	6.3.22	Primary-Charging-Collection-Function-Name AVP .....	16
35	6.3.23	Secondary-Charging-Collection-Function-Name AVP .....	16
36	6.3.24	User-Authorization-Type AVP.....	17
37	6.3.25	Void.....	17

1	6.3.26	User-Data-Already-Available AVP .....	17
2	6.3.27	Confidentiality-Key AVP .....	17
3	6.3.28	Integrity-Key AVP .....	18
4	<b>6.4</b>	<b>Use of namespaces .....</b>	<b>18</b>
5	6.4.1	AVP codes .....	18
6	6.4.2	Experimental-Result-Code AVP values .....	18
7	6.4.3	Command Code values .....	18
8	6.4.4	Application-ID value .....	18
9			

1 **Foreword**

2 | This document contains portions of material copied from 3GPP document number 29.229 [5.10.0](#). The  
 3 copyright on the 3GPP document is owned by the Organizational Partners of 3GPP (ARIB - Association of  
 4 Radio Industries and Businesses, Japan; CCSA – China Communications Standards Association, China;  
 5 ETSI - European Telecommunications Standards Institute; ATIS - Alliance for Telecommunications  
 6 Industry Solutions, USA; TTA - Telecommunications Technology Association, Korea; and TTC –  
 7 Telecommunication Technology Committee, Japan), which have granted license for reproduction and for  
 8 use by 3GPP2 and its Organizational Partners.

9

10 **Revision History**

Revision	Changes	Date
0, v1.0	Initial Publication	December 2003
0, v2.0	Version Update	July 2005

11

12

## 1 Scope

The present document defines a transport protocol for use in the IP multimedia (IM) Core Network (CN) subsystem based on Diameter.

The present document is applicable to: The Cx interface between the I-CSCF/S-CSCF and the HSS.

Whenever it is possible this document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of Diameter. Where this is not possible, extensions to Diameter are defined within this document.

## 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

[1] 3GPP2 X.S0013-005-[0 v2.0](#), “IP Multimedia (IM) Subsystem Cx interface; signalling flows and message contents”

[2] 3GPP2 S.[RS0086-A](#), “IMS Security Framework”

[3] IETF RFC 3261, “SIP: Session Initiation Protocol”

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

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

[6] IETF RFC 3588, “Diameter Base Protocol”

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

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

[9] void

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

[11] 3GPP2 X.S0013-011-[0 v2.0](#), “Sh Interface based on the Diameter protocol; protocol details”

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

## 3 Definitions, symbols and abbreviations

### 3.1 Definitions

Refer to [6] for the definitions of some terms used in this document.

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

**Attribute-Value Pair:** see [6], it corresponds to an Information Element in a Diameter message.

**Diameter Multimedia client:** The client is one of the communicating Diameter peers that usually initiate transactions

1 **Diameter Multimedia server:** A Diameter Multimedia server that also supported the NASREQ and  
 2 MobileIP applications would be referred to as a Diameter server.

3 **Registration:** SIP-registration.

4 **Server:** SIP-server.

5 **User data:** user profile data.

### 6 **3.2 Abbreviations**

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

8	AAA	Authentication, Authorization and Accounting
9	ABNF	Augmented Backus-Naur Form
10	AVP	Attribute-Value Pair
11	CN	Core Network
12	CSCF	Call Session Control Function
13	HSS	Home Subscriber Server
14	IANA	Internet Assigned Numbers Authority
15	I-CSCF	Interrogating CSCF
16	IETF	Internet Engineering Task Force
17	IMS	IP Multimedia Subsystem
18	RFC	Request For Comments
19	S-CSCF	Serving CSCF
20	SCTP	Stream Control Transport Protocol
21	SIP	Session Initiation Protocol
22	UCS	Universal Character Set
23	URL	Uniform Resource Locator
24	UTF	UCS Transformation Formats

## 25 **4 General**

26 The Diameter Base Protocol as specified in [6] shall apply except as modified by the defined support of the  
 27 methods and the defined support of the commands and AVPs, result and event codes specified in clause 6  
 28 of this specification. Unless otherwise specified, the procedures (including error handling and unrecognised  
 29 information handling) are unmodified.

## 30 **5 Use of the Diameter base protocol**

31 With the clarifications listed in the following subclauses, the Diameter Base Protocol defined by IETF [6]  
 32 shall apply.

### 33 **5.1 Securing Diameter Messages**

34 For secure transport of Diameter messages, see [2].

### 35 **5.2 Accounting functionality**

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

### 38 **5.3 Use of sessions**

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

1 The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation  
2 of implicitly terminated sessions.

3 The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value  
4 NO\_STATE\_MAINTAINED (1), as described in [6]. As a consequence, the server does not maintain any  
5 state information about this session and the client does not need to send any session termination request.  
6 Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or  
7 responses.

## 8 **5.4 Transport protocol**

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

## 11 **5.5 Routing considerations**

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

13 If an I-CSCF or S-CSCF knows the address/name of the HSS for a certain user, both the Destination-Realm  
14 and Destination-Host AVPs shall be present in the request. Otherwise, only the Destination-Realm AVP  
15 shall be present and the command shall be routed to the next Diameter node based on the Diameter routing  
16 table in the client. Consequently, the Destination-Host AVP is declared as optional in the ABNF for all  
17 requests initiated by an I-CSCF or an S-CSCF. The S-CSCF shall store the address of the HSS for each  
18 user, after a first request sent to the redirector function.

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

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

## 24 **5.6 Advertising Application Support**

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

29 and by including the The vendor identifier value of 3GPP (10415) shall be included in the Supported-  
30 Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and  
31 in the Vendor-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-  
32 Exchange-Request and Capabilities-Exchange-Answer commands. and the value of the application  
33 identifier (see chapter 6) in the Auth-Application-Id AVP, both in the Vendor-Specific-Application-Id AVP  
34 of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer command.

35 Note: The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-  
36 Answer commands that is not included in the the Vendor-Specific-Application-Id AVPs as  
37 described above shall indicate the manufacturer of the Diameter node as per [6].

## 38 **6 Diameter application for Cx interface**

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

- 41 - to exchange location information
- 42 - to authorize a user to access the IMS

- 1 - to exchange authentication information  
 2 - to download and handle changes in the user data stored in the server  
 3 The Cx interface protocol is defined as an IETF vendor specific Diameter application, where the vendor is  
 4 3GPP. The vendor identifier assigned by IANA to 3GPP ( [http://www.iana.org/assignments/enterprise-](http://www.iana.org/assignments/enterprise-numbers)  
 5 [numbers](http://www.iana.org/assignments/enterprise-numbers)) is 10415.  
 6 The Diameter application identifier assigned to the Cx interface protocol is [16777216167772151](#).

## 7 **6.1 Command-Code values**

8 This section defines Command-Code values for this Diameter application.

9 Every command is defined by means of the ABNF syntax [7], according to the rules in [6]. Whenever the  
 10 definition and use of an AVP is not specified in this document, what is stated in [6] shall apply.

11 The command codes for the Cx interface application are taken from the range allocated by IANA in [12] as  
 12 assigned in this specification. For these commands, the Application-ID field shall be set to  
 13 [16777216167772151](#) (application identifier of the Cx interface application).

14 The following Command Codes are defined in this specification:

15 **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

16

### 17 **6.1.1 User-Authorization-Request (UAR) Command**

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

21 Message Format

22 `< User-Authorization-Request > ::= < Diameter Header: 300, 16777216167772151, REQ,`  
 23 `PXY, 16777216 >`  
 24 `< Session-Id >`

```

1           { Vendor-Specific-Application-Id }
2           { Auth-Session-State }
3           { Origin-Host }
4           { Origin-Realm }
5           [ Destination-Host ]
6           { Destination-Realm }
7           { User-Name }
8           { Public-Identity }
9           { Visited-Network-Identifier }
10          [ User-Authorization-Type ]
11          *[ AVP ]
12          *[ Failed-AVP ]
13          *[ Proxy-Info ]
14          *[ Route-Record ]
15

```

### 16 6.1.2 User-Authorization-Answer (UAA) Command

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

21 Message Format

```

22          < User-Authorization-Answer > ::= < Diameter Header: 300, PXY, 16777216+167772151
23          >
24          < Session-Id >
25          { Vendor-Specific-Application-Id }
26          [ Result-Code ]
27          [ Experimental-Result ]
28          { Auth-Session-State }
29          { Origin-Host }
30          { Origin-Realm }
31          [ Server-Name ]
32          [ Server-Capabilities ]
33          *[ AVP ]
34          *[ Proxy-Info ]
35          *[ Route-Record ]

```

### 36 6.1.3 Server-Assignment-Request (SAR) Command

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

40 Message Format

```

41          <Server-Assignment-Request> ::= < Diameter Header: 301, 16777216+167772151, REQ, PXY,
42          16777216 >
43          < Session-Id >
44          { Vendor-Specific-Application-Id }
45          { Auth-Session-State }
46          { Origin-Host }
47          { Origin-Realm }
48          [ Destination-Host ]
49          { Destination-Realm }
50          [ User-Name ]

```

```

1      * [ Public-Identity ]
2      [ Server-Name ]
3      { Server-Assignment-Type }
4      { User-Data-Request-Type }
5      { User-Data-Already-Available }
6      * [ AVP ]
7      * [ Failed-AVP ]
8      * [ Proxy-Info ]
9      * [ Route-Record ]

```

#### 10 6.1.4 Server-Assignment-Answer (SAA) Command

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

17 Message Format

```

18      <Server-Assignment-Answer> ::=          < Diameter Header: 301, PXY, 16777216167772151
19      >
20      < Session-Id >
21      { Vendor-Specific-Application-Id }
22      [ Result-Code ]
23      [ Experimental-Result ]
24      { Auth-Session-State }
25      { Origin-Host }
26      { Origin-Realm }
27      [ User-Name ]
28      [ User-Data ]
29      [ Charging-Information ]
30      * [ AVP ]
31      * [ Proxy-Info ]
32      * [ Route-Record ]

```

#### 33 6.1.5 Location-Info-Request (LIR) Command

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

37 Message Format

```

38      <Location-Info-Request> ::=          < Diameter Header: 302, 16777216167772151, REQ, PXY,
39      16777216 >
40      < Session-Id >
41      { Vendor-Specific-Application-Id }
42      { Auth-Session-State }
43      { Origin-Host }
44      { Origin-Realm }
45      [ Destination-Host ]
46      { Destination-Realm }
47      { Public-Identity }
48      * [ AVP ]
49      * [ Proxy-Info ]
50      * [ Route-Record ]

```

### 1 **6.1.6 Location-Info-Answer (LIA) Command**

2 The Location-Info-Answer (LIA) command, indicated by the Command-Code field set to 302 and the 'R'  
3 bit cleared in the Command Flags field, is sent by a server in response to the Location-Info-Request  
4 command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section  
5 6.2 in addition to the values defined in [6].

#### 6 Message Format

```
7 | <Location-Info-Answer> ::= < Diameter Header: 302, PXY, 16777216+67772151>
8 | < Session-Id >
9 | { Vendor-Specific-Application-Id }
10 | [ Result-Code ]
11 | [ Experimental-Result ]
12 | { Auth-Session-State }
13 | { Origin-Host }
14 | { Origin-Realm }
15 | [ Server-Name ]
16 | [ Server-Capabilities ]
17 | *[ AVP ]
18 | *[ Failed-AVP ]
19 | *[ Proxy-Info ]
20 | *[ Route-Record ]
```

### 21 **6.1.7 Multimedia-Auth-Request (MAR) Command**

22 The Multimedia-Auth-Request (MAR) command, indicated by the Command-Code field set to 303 and the  
23 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia  
24 server in order to request security information.

#### 25 Message Format

```
26 | < Multimedia-Auth-Request > ::= < Diameter Header: 303, 16777216+67772151, REQ, PXY,
27 | 16777216 >
28 | < Session-Id >
29 | { Vendor-Specific-Application-Id }
30 | { Auth-Session-State }
31 | { Origin-Host }
32 | { Origin-Realm }
33 | { Destination-Realm }
34 | [ Destination-Host ]
35 | { User-Name }
36 | { Public-Identity }
37 | [ SIP-Auth-Data-Item ]
38 | –[ SIP-Number-Auth-Items ]
39 | { Server-Name }
40 | * [ AVP ]
41 | * [ Proxy-Info ]
42 | * [ Route-Record ]
```

### 43 **6.1.8 Multimedia-Auth-Answer (MAA) Command**

44 The Multimedia-Auth-Answer (MAA) command, indicated by the Command-Code field set to 303 and the  
45 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Auth-Request  
46 command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section  
47 6.2 in addition to the values defined in [6].

#### 48 Message Format

```
49 | < Multimedia-Auth-Answer > ::= < Diameter Header: 303, PXY, 16777216+67772151 >
50 | < Session-Id >
```

```

1           { Vendor-Specific-Application-Id }
2           [ Result-Code ]
3           [ Experimental-Result ]
4           { Auth-Session-State }
5           { Origin-Host }
6           { Origin-Realm }
7           [ User-Name ]
8           [ Public-Identity ]
9           [ SIP-Number-Auth-Items ]
10          * [ SIP-Auth-Data-Item ]
11          * [ AVP ]
12          * [ Failed-AVP ]
13          * [ Proxy-Info ]
14          * [ Route-Record ]

```

### 15 6.1.9 Registration-Termination-Request (RTR) Command

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

19 Message Format

```

20          <Registration-Termination-Request> ::= < Diameter Header: 304, 16777216167772151, REQ,
21          PXY, 16777216 >
22          < Session-Id >
23          { Vendor-Specific-Application-Id }
24          { Auth-Session-State }
25          { Origin-Host }
26          { Origin-Realm }
27          { Destination-Host }
28          { Destination-Realm }
29          { User-Name }
30          * [ Public-Identity ]
31          { DeRegistration-Reason }
32          * [ AVP ]
33          * [ Proxy-Info ]
34          * [ Route-Record ]

```

### 35 6.1.10 Registration-Termination-Answer (RTA) Command

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

40 Message Format

```

41          <Registration-Termination-Answer> ::= < Diameter Header: 304, PXY,
42          16777216167772151>
43          < Session-Id >
44          { Vendor-Specific-Application-Id }
45          [ Result-Code ]
46          [ Experimental-Result ]
47          { Auth-Session-State }
48          { Origin-Host }
49          { Origin-Realm }
50          * [ AVP ]
51          * [ Failed-AVP ]

```



1    **6.2.1    Success**

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

4    **6.2.1.1            DIAMETER\_FIRST\_REGISTRATION (2001)**

5    The HSS informs the I-CSCF that:

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

8

9    **6.2.1.2            DIAMETER\_SUBSEQUENT\_REGISTRATION (2002)**

10   The HSS informs the I-CSCF that:

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

13   **6.2.1.3            DIAMETER\_UNREGISTERED\_SERVICE (2003)**

14   The HSS informs the I-CSCF that:

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

17

18   **6.2.1.4            DIAMETER\_SUCCESS\_SERVER\_NAME\_NOT\_STORED (2004)**

19   The HSS informs to the S-CSCF that :

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

22   **6.2.1.5            DIAMETER\_SERVER\_SELECTION (2005)**

23   The HSS informs the I-CSCF that:

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

27   **6.2.2    Permanent Failures**

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

30   **6.2.2.1            DIAMETER\_ERROR\_USER\_UNKNOWN (5001)**

31   A message was received for a user that is unknown.

1     **6.2.2.2           DIAMETER\_ERROR\_IDENTITIES\_DONT\_MATCH (5002)**

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

4     **6.2.2.3           DIAMETER\_ERROR\_IDENTITY\_NOT\_REGISTERED (5003)**

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

7     **6.2.2.4           DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED (5004)**

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

9     **6.2.2.5           DIAMETER\_ERROR\_IDENTITY\_ALREADY\_REGISTERED (5005)**

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

12    **6.2.2.6           DIAMETER\_ERROR\_AUTH\_SCHEME\_NOT\_SUPPORTED (5006)**

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

14    **6.2.2.7           DIAMETER\_ERROR\_IN\_ASSIGNMENT\_TYPE (5007)**

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

17    **6.2.2.8           DIAMETER\_ERROR\_TOO\_MUCH\_DATA (5008)**

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

19    NOTE: This error code is also used in [11].

20    **6.2.2.9           DIAMETER\_ERROR\_NOT\_SUPPORTED\_USER\_DATA (5009)**

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

23    **6.2.2.10           DIAMETER\_MISSING\_USER\_ID (5010xxx)**

24    The HSS informs the S-CSCF that the message did not contain a Private-Id and/or a Public-Id and so the  
25    message could not be processed.

26    **6.3    AVPs**

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

30                   **Table 6.3.1: Diameter Multimedia Application AVPs**

Attribute Name	AVP Code	Section defined	Value Type	AVP Flag rules				May Encr.
				Must	May	Should not	Must not	
Visited-Network-Identifier	600+	6.3.1	OctetString	M, V				No

Public-Identity	<a href="#">6012</a>	6.3.2	UTF8String	M, V			No
Server-Name	<del>6023</del>	6.3.3	UTF8String	M, V			No
Server-Capabilities	<a href="#">6034</a>	6.3.4	Grouped	M, V			No
Mandatory-Capability	<del>6045</del>	6.3.5	Unsigned32	M, V			No
Optional-Capability	<a href="#">6056</a>	6.3.6	Unsigned32	M, V			No
User-Data	<del>6067</del>	6.3.7	OctetString	M, V			No
SIP-Number-Auth-Items	<a href="#">6078</a>	6.3.8	Unsigned32	M, V			No
SIP-Authentication-Scheme	<del>6089</del>	6.3.9	UTF8String	M, V			No
SIP-Authenticate	<del>60940</del>	6.3.10	OctetString	M, V			No
SIP-Authorization	<del>61044</del>	6.3.11	OctetString	M, V			No
SIP-Authentication-Context	<del>61142</del>	6.3.12	OctetString	M, V			No
SIP-Auth-Data-Item	<del>61243</del>	6.3.13	Grouped	M, V			No
SIP-Item-Number	<a href="#">61344</a>	6.3.14	Unsigned32	M, V			No
Server-Assignment-Type	<del>61445</del>	6.3.15	Enumerated	M, V			No
Deregistration-Reason	<del>61546</del>	6.3.16	Grouped	M, V			No
Reason-Code	<del>61647</del>	6.3.17	Enumerated	M, V			No
Reason-Info	<del>61748</del>	6.3.18	UTF8String	M, V			No
Charging-Information	<del>61849</del>	6.3.19	Grouped	M, V			No
Primary-Event-Charging-Function-Name	<del>61920</del>	6.3.20	DiameterURI	M, V			No
Secondary-Event-Charging-Function-Name	<del>62024</del>	6.3.21	DiameterURI	M, V			No
Primary-Charging-Collection-Function-Name	<del>62122</del>	6.3.22	DiameterURI	M, V			No
Secondary-Charging-Collection-Function-Name	<del>62223</del>	6.3.23	DiameterURI	M, V			No
User-Authorization-Type	<del>62324</del>	6.3.24	Enumerated	M, V			No
User-Data-Already-Available	<del>62426</del>	6.3.26	Enumerated	M, V			No
Confidentiality-Key	<del>62527</del>	6.3.27	OctetString	M, V			No
Integrity-Key	<del>62628</del>	6.3.28	OctetString	M, V			No
<u>User-Data-Request-Type</u>	<a href="#">627</a>	<a href="#">6.3.25</a>	<u>Enumerated</u>	<u>M, V</u>			<u>No</u>

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 [6].

NOTE 2: Depending on the concrete command.

1

### 2 6.3.1 Visited-Network-Identifier AVP

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

### 1 **6.3.2 Public-Identity AVP**

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

### 5 **6.3.3 Server-Name AVP**

6 | The Server-Name AVP (~~AVP Code 3~~) is of type UTF8String. This AVP contains a SIP-URL (as defined in  
7 [3] and [4]), used to identify a SIP server (e.g. S-CSCF name).

### 8 **6.3.4 Server-Capabilities AVP**

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

11 AVP format

```
12 |         Server-Capabilities ::= <AVP header: TBD4-167772151>
13 |             *[Mandatory-Capability]
14 |             *[Optional-Capability]
15 |             *[Server-Name]
16 |             *[AVP]
```

### 17 **6.3.5 Mandatory-Capability AVP**

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

### 22 **6.3.6 Optional-Capability AVP**

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

### 27 **6.3.7 User-Data AVP**

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

### 30 **6.3.8 SIP-Number-Auth-Items AVP**

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

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

### 37 **6.3.9 SIP-Authentication-Scheme AVP**

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

### 1 **6.3.10 SIP-Authenticate AVP**

2 | The SIP-Authenticate AVP (~~AVP code 10~~) is of type OctetString and contains specific parts of the data  
 3 | portion of the WWW-Authenticate or Proxy-Authenticate SIP headers that are to be present in a SIP  
 4 | response. The identification and encoding of the specific parts are defined in [1].

### 5 **6.3.11 SIP-Authorization AVP**

6 | The SIP-Authorization AVP (~~AVP code 11~~) is of type OctetString and contains specific parts of the data  
 7 | portion of the Authorization or Proxy-Authorization SIP headers suitable for inclusion in a SIP request. The  
 8 | identification and encoding of the specific parts are defined in [1].

### 9 **6.3.12 SIP-Authentication-Context AVP**

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

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

### 17 **6.3.13 SIP-Auth-Data-Item AVP**

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

20 | AVP format

```
21 |     SIP-Auth-Data-Item:: = < AVP Header : TBD13-16772151 >
22 |         [ SIP-Item-Number ]
23 |         [ SIP-Authentication-Scheme ]
24 |         [ SIP-Authenticate ]
25 |         [ SIP-Authorization ]
26 |         [ SIP-Authentication-Context ]
27 |         [Confidentiality-Key]
28 |         [Integrity-Key]
29 |         * [AVP]
```

### 30 **6.3.14 SIP-Item-Number AVP**

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

### 36 **6.3.15 Server-Assignment-Type AVP**

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

39 | NO\_ASSIGNMENT (0)

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

3   REGISTRATION (1)

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

5   RE\_REGISTRATION (2)

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

7   UNREGISTERED\_USER (3)

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

10   TIMEOUT\_DEREGISTRATION (4)

11          The SIP registration timer of an identity has expired.

12   USER\_DEREGISTRATION (5)

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

14   TIMEOUT\_DEREGISTRATION\_STORE\_SERVER\_NAME (6)

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

17   USER\_DEREGISTRATION\_STORE\_SERVER\_NAME (7)

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

20   ADMINISTRATIVE\_DEREGISTRATION (8)

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

22   AUTHENTICATION\_FAILURE (9)

23          The authentication of a user has failed.

24   AUTHENTICATION\_TIMEOUT (10)

25          The authentication timeout has expired.

26   DEREGISTRATION\_TOO\_MUCH\_DATA (11)

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

### 29   **6.3.16 Deregistration-Reason AVP**

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

32 | AVP format

33 |       Deregistration-Reason ::= < AVP Header : TBD+6-167772151 >

34 |               { Reason-Code }

35 |               [ Reason-Info ]

36 |               \* [AVP]

### 1    **6.3.17           Reason-Code AVP**

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

- 4       PERMANENT\_TERMINATION (0)
- 5       NEW\_SERVER\_ASSIGNED (1)
- 6       SERVER\_CHANGE (2)
- 7       REMOVE\_S-CSCF (3)

8 | The detailed behaviour of the S-CSCF is defined in [1].

### 9    **6.3.18           Reason-Info AVP**

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

### 12   **6.3.19   Charging-Information AVP**

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

15 | AVP format

```
16 |       Charging-Information ::= < AVP Header : TBD19-167772151 >
17 |           [ Primary-Event-Charging-Function-Name ]
18 |           [ Secondary-Event-Charging-Function-Name ]
19 |           { { Primary-Charging-Collection-Function-Name } }
20 |           [ Secondary-Charging-Collection-Function-Name ]
21 |           *[ AVP ]
```

### 22   **6.3.20   Primary-Event-Charging-Function-Name AVP**

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

### 25   **6.3.21   Secondary-Event-Charging-Function-Name AVP**

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

### 28   **6.3.22   Primary-Charging-Collection-Function-Name AVP**

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

### 31   **6.3.23   Secondary-Charging-Collection-Function-Name AVP**

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

### 6.3.24 User-Authorization-Type AVP

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

#### REGISTRATION (0)

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

This is the default value.

#### DE\_REGISTRATION (1)

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

#### REGISTRATION\_AND\_CAPABILITIES (2)

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

### 6.3.25 ~~VoidUser-Data-Request-Type AVP~~

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

#### ~~COMPLETE\_PROFILE (0)~~

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

#### ~~REGISTERED\_PROFILE (1)~~

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

#### ~~UNREGISTERED\_PROFILE (2)~~

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

### 6.3.26 User-Data-Already-Available AVP

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

#### USER\_DATA\_NOT\_AVAILABLE (0)

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

#### USER\_DATA\_ALREADY\_AVAILABLE (1)

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

### 6.3.27 Confidentiality-Key AVP

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

### 1 **6.3.28 Integrity-Key AVP**

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

## 3 **6.4 Use of namespaces**

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

### 7 **6.4.1 AVP codes**

8 This specification assigns the AVP values ~~1-28~~ from the AVP Code namespace for Diameter vendor-  
9 specific applications. See section 6.3 for the assignment of the namespace in this specification.

### 11 **6.4.2 Experimental-Result-Code AVP values**

12 This specification has assigned Experimental-Result-Code AVP values 2001-2005 and 5001-5009. See  
13 section 6.2.

### 14 **6.4.3 Command Code values**

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

### 16 **6.4.4 Application-ID value**

17 IANA has allocated the value ~~16777216+67772151~~ for the 3GPP<sup>2</sup> Cx interface application.

## 19 **7 Special Requirements**

### 20 **7.1 Version Control**

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

25 ~~If the new application ID mechanism for capability exchange is not enough in the future versions of the Cx  
26 specifications, the principle on how the version control is done is following. When the peer node receives  
27 the Capabilities Exchange Request command with the additional AVPs indicating the added supported  
28 functionality of the requesting node, if the receiving node supports some or all of the functionalities it shall  
29 send the corresponding AVPs indicating the supported functionality to the requesting node, which then  
30 knows that the added capabilities the peer node supports. If the peer node does not recognize some or all of  
31 the additional capabilities it shall discard the AVPs and it shall not send those AVPs to the original  
32 requestor.~~

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

- 1 | ~~The exact mechanism and AVPs needed for the version control are decided when the exact update to the Cx~~
- 2 | ~~application is needed.~~