3GPP TSG CN Plenary Meeting #13 **Tdoc NP-010628**
Kyoto, JAPAN, 12th – 14th December 2001

Source:	**CN4**
Title:	**3GPP TS 29.229 IP Cx interface based on the Diameter protocol; Protocol details**
Agenda item:	**9.1**
Document for:	**Imformation**

This document contains **3GPP TS 29.229-v1.0.0 IP Cx interface based on the Diameter protocol; Protocol details Rel-5**. It has been agreed by TSG CN WG4, and are forwarded to TSG CN Plenary meeting #14 for information.

3GPP TS 29.229 V1.0.0 (2001-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; Cx Interface based on the Diameter protocol; Protocol details; (Release 5)

Keywords
Diameter, AVP, command-code, Cx

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.

Introduction

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 HSS.

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

2 References

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

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

[1] 3GPP TS 23.228: “IP Multimedia (IM) Subsystem – Stage 2”

[2] 3GPP TS 24.228 “Signalling flows for the IP Multimedia call control based on SIP and SDP”

[3] 3GPP TS 29.228 “IP Multimedia Subsystem Cx interface; signalling flows and message contents”

[4] 3GPP TS 23.002 “Network Architecture”

[5] 3GPP TS 33.203 “Access security for IP based services”

[6] 3GPP TS 33.210 “Network Domain Security: IP Network Layer Security”

[7] ITU-T Recommendation E.164: "Numbering plan for the ISDN era"

[8] draft-ietf-sip-rfc2543bis-05: “SIP: Session Initiation Protocol”, work in progress

[9] IETF RFC 2279: "UTF-8, a transformation format of ISO 10646"

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

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

[12] draft-ietf-aaa-diameter-07.txt, “Diameter Base Protocol”, work in progress

[13] draft-sip-aaa-reqs-02.txt, “AAA requirements for IP telephony/multimedia”, work in progress

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

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

[16] draft ietf-aaa-diameter-nasreq-07.txt, “Diameter NASREQ Extensions”, work in progress

3 Definitions, symbols and abbreviations

3.1 Definitions

Refer to [12] for the definitions of some terms used in this document.

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

Serving SIP proxy in the Home network: SIP server serving the particular user. Corresponds to S-CSCF in 3GPP.

Attribute-Value Pair: see [12], 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.

Location: the information about which SIP server the user is registered in.

Registration: SIP-registration.

Home entry SIP Proxy: corresponds to I-CSCF in 3GPP

Outbound SIP Proxy in the Visited network: corresponds to P-CSCF in 3GPP.

Security information: information needed to establish security association between two entities. In the case of 3GPP this is the authentication vector.

Server: SIP-server.

User data: user profile data.

3.2 Abbreviations

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

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

4 General

The Diameter Base Protocol as specified in [12] and Diameter Multimedia application as specified in clause 6 shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and event codes specified in clause 5 of this specification. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) are unmodified.

Note: This specification has been drafted according with the last known status of the Diameter protocol. The specification of Diameter is work in progress in IETF. Thus some inconsistencies, changes in notation, correction of minor mistakes, change of character of some AVPs (from mandatory to optional or vice-versa), etc. are expected during the development of this specification and until Diameter becomes RFC, something that is expected to happen during October, 2001.

5 Use of the Diameter protocol

5.1 Introduction to methodology

This specification defines a subset of the Diameter Base Protocol and the subset of the Diameter Multimedia Application for the Cx interface.

In the sending direction, the support of a command or AVP means that the implementation is able to send this command or AVP (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the command or AVP.

As a consequence, commands and AVP tables in this clause are not the same as the tables describing the syntax of a PDU in the reference Diameter standards.

The status codes used in this clause are described in table 5.1.

Table 5.1: Key to status codes

Status code	Status name	Meaning
M	Mandatory	The capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement).
O	Optional	The capability may or may not be supported. It is an implementation choice.
n/a	Not applicable	It is impossible to use the capability. No answer in the support column is required.
X	Prohibited (excluded)	It is not allowed to use the capability. This is more common for a profile.
c <integer>	Conditional	The requirement on the capability ("m", "o", "n/a" or "x") depends on the support of other **optional or conditional** items. <integer> is the identifier of the conditional expression.
o.<integer>	qualified optional	For mutually exclusive or selectable options from a set. <integer> is the identifier of the group of options, and the logic of selection of the options.
I	Irrelevant	Capability outside the scope of the given specification. Normally, this notation should be used in a base specification ICS proforma only for transparent parameters in received PDUs. However, it may be useful in other cases, when the base specification is in fact based on another standard.

5.2 Diameter Base Protocol

With exceptions listed in the following subclauses the Diameter Base Protocol defined by IETF shall apply.

5.2.1 Securing Diameter Messages

For secure transport of Diameter messages, see TS 33.210 [6].

5.2.2 Accounting functionality

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

Note: The definition of the charging and accounting architecture is being defined by SA2. SA5 is considering Diameter for other interfaces to do charging and accounting.

5.2.3 Use of sessions

Both between I-CSCF and HSS and between S-CSCF and 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-authorisation 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 [12]. 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.

5.2.4 Transport protocol

Diameter messages over the Cx interface shall make use of SCTP.

6 Diameter Multimedia application

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

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

Note: It is intended that in the future this subchapter can be turned into a reference to an IETF RFC. In order to make that possibility feasible, the way this Diameter application is formulated pursues that objective.

Note: This specification will contain a subset of the actual Diameter Multimedia Application to be developed in IETF, which scope could be wider than the use that 3GPP makes use of.

6.1 Command-Code values

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

Note: More Command Codes could be added and some could disappear. The assignment of names to the Command Codes is also tentative and subject to change. Particularly, it has to be checked whether there is conflict between the command names defined here and the ones defined in the Diameter base protocol and its applications defined in IETF (NASREQ, MobileIP).

Every command is defined by means of the ABNF syntax [14], according to the rules in [12]. Whenever the definition and use of an AVP is not specified in this document, what is stated in [12] shall apply.

The following Command Codes are defined in this specification:

Table 6.1.1: Command-Code values

Command-Name	Source	Destination	Abbreviation	Code	Section	Cx message
Registration-Authorisation-Request	I-CSCF	HSS	RAR	TBD	6.1.1	Cx-Query + Cx-Select-Pull
Registration-Authorisation-Answer	HSS	I-CSCF	RAA	TBD	6.1.2	Cx-Query Resp + Cx-Select-Pull Resp
Server-Assignment-Request	S-CSCF	HSS		TBD	6.1.3	Cx-Put + Cx-Pull
Server-Assignment-Answer	HSS	S-CSCF	SAA	TBD	6.1.4	Cx-Put Resp + Cx-Pull Resp
Location-Info-Request	I-CSCF	HSS	LIR	TBD	6.1.5	Cx-Location-Query
Location-Info-Answer	HSS	I-CSCF	LIA	TBD	6.1.6	Cx-Location-Query Resp
Multimedia-Auth-Request	S-CSCF	HSS	MAR	TBD	6.1.7	Cx-AuthDataReq
Multimedia-Auth-Answer	HSS	S-CSCF	MAA	TBD	6.1.8	Cx-AuthDataResp
Registration-Termination-Request	HSS	S-CSCF	RTR	TBD	6.1.9	Cx-Deregister
Registration-Termination-Answer	S-CSCF	HSS	RTA	TBD	6.1.10	Cx-Deregister Resp
Push-Profile-Request	HSS	S-CSCF	PPR	TBD	6.1.11	(Subscription update procedure)
Push-Profile-Answer	S-CSCF	HSS	PPA	TBD	6.1.12	(Subscription update procedure)

Note1: The columns entitled “Source”, “Destination” and “Cx message” are provisional, the information that they contain will be finally placed in 29.228. At this stage, they have been included here for the sake of the clarity of this specification. The column “Cx message” contain the stage 2 names of the operations being mapped to commands in this specification.

6.1.1 Registration-Authorisation-Request (RAR) Command

The Registration-Authorisation-Request (RAR) command, indicated by the Command-Code field set to TBD 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 authorisation of the registration of a multimedia user. The server shall validate whether the private and public identities belong to the same user. In addition, the server shall check whether the user is already registered and/or whether the user is authorised to register in the network where the user is roaming.

- Visited-Network-Identifier

Message Format

< Registration-Authorisation-Request> ::= < Diameter Header: TBD, R >

< Session-Id >
{ Auth-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
{ Public-Identity }
{ Visited-Network-Identifier }
*[AVP]
*[Proxy-Info]
*[Route-Record]

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.1.1: AVP values for command RAR

AVP	Status	Value
User-Name	M	This AVP contains the private user identity in the form of a NAI.
Public-Identity	M	It contains the public user identity in the form of SIP-URL or TEL-URL.
Visited-Network-Identifier	M	It contains an identifier that helps the home network to identify the visited network.

6.1.2 Registration-Authorisation-Answer (RAA) Command

The Registration-Authorisation-Answer (RAA) command, indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Registration-Authorisation-Request command. The Result-Code AVP may contain one of the values defined in section 6.2 in addition to the values defined in [12].

If the user has been authorised to register and a server is already assigned, the Server-Name AVP shall contain the SIP URL of the server, so that the client can forward the registration request to it. The Server-Capability AVP shall not be present.

If the user has been authorised to register and a server has not been assigned yet, the Server-Name AVP shall not be present. Instead, one Server-Capabilities AVP may be present, containing the capabilities that the Diameter Multimedia client shall use for the selection of the server that will perform the control of the services for the multimedia user. The Server-Capabilities AVP may be absent if, according to the user profile content, the user does not need any specific capabilities from the S-CSCF.

Message Format

< Registration-Authorisation-Answer> ::= < Diameter Header: TBD, A >
< Session-Id >
{ Auth-Application-Id }
{ Result-Code }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Server-Name]
[Server-Capabilities]
*[AVP]
*[Proxy-Info]
*[Route-Record]

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.2.1: AVP values for command RAA

AVP	Status	Value
Server-Name	O	It contains the SIP URL of the S-CSCF where the user is registered.
Server-Capability	O	It contains the information that will help the I-CSCF in the selection of the S-CSCF.
Result-Code	M	See Table 6.1.2.2

Table 6.1.2.2: Result-Code AVP values for command RAA

Result-Code AVP value	Condition	Defined in
DIAMETER_USER_UNKNOWN (5001)	The RAR message was received for a user that is unknown.	[12]
DIAMETER_AVP_UNSUPPORTED (5002)	The RAR message was received with one or more AVPs not recognised or supported (e.g. invalid format in the identifier) and marked with the mandatory bit. RAA shall contain one or more Failed-AVP AVPs (see [12]) containing the AVPs that causes the failure.	[12]
IDENTITIES_DONT_MATCH (5xxx, TBD)	The private (User-Name AVP) and public identities received in the request message do not match.	6.2.2.1
DIAMETER_AUTHORISATION_REJECTED (5004)	The user is not authorised to register.	[12]
ROAMING_NOT_ALLOWED (5xxx, TBD)	The user is not allowed to roam in the visited network.	6.2.2.3
AUTHORISED_FIRST_REGISTRATION (2xxx, TBD)	The user is authorised to register. The user was not registered yet. Server-Name shall not be returned. One Server-Capabilities AVP may be returned.	6.2.1.1
AUTHORISED_REGISTERED	The user is authorised to register. The user was already registered. The name of the server where the user is registered shall be returned in the Server-Name AVP. No Server-Capabilities AVP shall be returned.	6.2.1.2

6.1.3 Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR) command, indicated by the Command-Code field set to TBD 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.

In case that there may be an S-CSCF already assigned for the user the decision that the HSS takes to overwrite or not the existing S-CSCF name depends on the registration status of the user, as defined in TS 29.228 [3].

Message Format

```
<Server-Assignment-Request> ::= < Diameter Header: TBD, R >
                                < Session-Id >
                                { Auth-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
```

{ Destination-Host }
{ Destination-Realm }
[User-Name]
{ Public-Identity }
[Server-Name]
{ Server-Assignment-Type }
*[AVP]
*[Proxy-Info]
*[Route-Record]

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.3.1: AVP values for command SAR

AVP	Status	Value
User-Name	O	If present, this AVP contains the private user identity in the form of a NAI.
Public-Identity	M	It contains the public user identity in the form of SIP-URL or TEL-URL.
Server-Name	O	It contains the SIP URL of the S-CSCF where the user is being registered. Depending on the concrete value of Server-Assignment-Type AVP this AVP may be absent.
Server-Assignment-Type	M	This AVP indicates the situation under which the operation is being issued, from the point of view of the S-CSCF (e.g. first registration, re-registration, authentication failure). See 6.3.13.

6.1.4 Server-Assignment-Answer (SAA) Command

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

Message Format

<Server-Assignment-Answer> ::= < Diameter Header: TBD, A >
< Session-Id >
{ Auth-Application-Id }
{ Result-Code }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Data]
*[AVP]
*[Proxy-Info]
*[Route-Record]

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.4.1: AVP values for command SAA

AVP	Status	Value
Result-Code	M	See Table 6.1.4.2
User-Data	O	This AVP contains the data stored in the HSS to serve the user, which exact content is described in TS 29.228 [3].

Table 6.1.4.2: Result-Code AVP values for command SAA

Result-Code AVP value	Condition	Defined in
DIAMETER_USER_UNKNOWN (5001)	The SAR message was received for a user that is unknown.	[12]
DIAMETER_AVP_UNSUPPORTED (5002)	The SAR message was received with one or more AVPs not recognised or supported (e.g. invalid format in the identities) and marked with the mandatory bit. SAA shall contain one or more Failed-AVP AVPs (see [12]) containing the AVPs that causes the failure.	[12]
IDENTITIES_DONT_MATCH (5xxx, TBD)	The private (User-Name AVP) and public identities received in the request message do not match.	6.2.2.1
IDENTITY_ALREADY_REGISTERED (5xxx, TBD)	The identity is already registered.	6.2.2.4
DIAMETER_SUCCESS	The request succeeded.	[12]
DIAMETER_UNABLE_TO_COMPLY (5014)	The request to update the name of the server failed.	[12]

6.1.5 Location-Info-Request (LIR) Command

- The Location-Info-Request (LIR) command, indicated by the Command-Code field set to TBD 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: TBD, R >
< Session-Id >
{ Auth-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ Public-Identity }
*[AVP]
*[Proxy-Info]
*[Route-Record]

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.7.1: AVP values for command LIR

AVP	Status	Value
Public-Identity	M	It contains the public user identity in the form of SIP-URL or TEL-URL.

6.1.6 Location-Info-Answer (LIA) Command

The Location-Info-Answer (LIA) command, indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Location-Info-Request command. The Result-Code AVP may contain one of the values defined in section 6.2 in addition to the values defined in [12].

If the user is registered, the Server-Name AVP shall contain the SIP URL of the server. The Server-Capabilities AVP shall not be present.

If the user is not registered yet, the Server-Name AVP shall not be present. Instead, in case that the user can be given service even in that situation, one Server-Capabilities AVP may be present, containing the capabilities that the Diameter Multimedia client shall use for the selection of the server that will perform the control of the services for the multimedia user. The Server-Capabilities AVP may be absent if, according to the user profile content, the user does not need any specific capabilities from the S-CSCF.

Message Format

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

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.8.1: AVP values for command LIA

AVP	Status	Value
Server-Name	O	It contains the SIP URL of the S-CSCF where the user is registered.
Server-Capabilities	O	It contains the information that will help the I-CSCF in the selection of the S-CSCF.
Result-Code	M	See Table 6.1.8.2

Table 6.1.8.2: Result-Code AVP values for command LIA

Result-Code AVP value	Condition	Defined in
DIAMETER_USER_UNKNOWN (5001)	The LIR message was received for a user that is unknown.	[12]
DIAMETER_AVP_UNSUPPORTED (5002)	The LIR message was received with one or more AVPs not recognised or supported (e.g. invalid format in the identities) and marked with the mandatory bit. LIA shall contain one or more Failed-AVP AVPs (see [12]) containing the AVPs that causes the failure.	[12]
DIAMETER_SUCCESS	The request succeeded. The name of the server where the user is registered shall be returned in the Server-Name AVP. No Server-Capability AVPs shall be returned.	[12]

IDENTITY_NOT_REGISTERED_SERVICES (2xxx, TBD)	The request contained an identity not registered, but the user to which this identity belongs can receive service in this situation. The Server-Name AVP shall not be returned. One Server-Capabilities AVP may be returned.	6.2.1.3
IDENTITY_NOT_REGISTERED (5xxx, TBD)	The request contained an identity not registered and the user to which this identity belongs cannot receive service in this situation. No Server-Name AVP or Server-Capabilities AVP shall be returned.	6.2.2.2

6.1.7 Multimedia-Auth-Request (MAR) Command

The Multimedia-Auth-Request (MAR) command, indicated by the Command-Code field set to TBD 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-Authentication-Request > ::= < Diameter Header: TBD, REQUEST >
< Session-Id >
{ Auth-Application-Id }
[Auth-Session-State]
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[Destination-Host]
[User-Name]
[Public-Identity]
[Authentication-Scheme]
[Authentication-Parameters]
[Number-Authentication-Items]
[Server-Name]
* [AVP]
* [Proxy-Info]
* [Route-Record]

The following table contains the values for the case where the S-CSCF request one or more authentication vectors:

Table 6.1.9.1: AVP values for command MAR

AVP	Status	Value
User-Name	M	It contains the private user identity in the form of a NAI
Public-Identity	M	It contains the public user identity in the form of SIP-URL or TEL-URL.
Authentication-Scheme	M	EAP
Authentication-Parameters	M	EAP-Response/Identity packet containing the private user identity, base64 encoded.
Number-Authentication-Items	M	It indicates the number of authentication vectors that are requested.
Server-Name	O	When this AVP is present in the request, it is to indicate that the user has not been authenticated by the S-CSCF yet. In case that there may be an S-CSCF already assigned for the user the decision that the HSS takes to overwrite or not the existing S-CSCF name depends on the registration status of the user, as defined in TS 29.228 [3].

The following table describes the AVP's for the case where the S-CSCF reports a synchronisation failure and requests fresh authentication vectors:

Table 6.1.9.2: AVP values for command MAR – synchronization failure

AVP	Status	Value
User-Name	M	It contains the private user identity in the form of a NAI.
Public-Identity	M	It contains the public user identity in the form of SIP-URL or TEL-URL.
Authentication-Scheme	M	EAP
Authentication-Parameters	M	EAP-Response packet containing AUTS and RAND, base 64 encoded.
Number-Authentication-Items	M	It indicates the number of authentication vectors that are requested.

6.1.8 Multimedia-Auth-Answer (MAA) Command

The Multimedia-Auth-Answer (MAA) command, indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Auth-Request command. The Result-Code AVP may contain one of the values defined in section 6.2 in addition to the values defined in [12].

Message Format

< Multimedia-Auth-Answer > ::= < Diameter Header: TBD, ANSWER >
< Session-Id >
{ Auth-Application-Id }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Public-Identity]
[Error-Reporting-Host]
[Number-Authentication-Items]
* [Authentication-Data-Item]
[Auth-Session-State]
* [AVP]
* [Proxy-Info]
* [Route-Record]

The following table contains mandatory values for some of the AVPs:

Table 6.1.10.1: AVP values for command MAA

AVP	Status	Value
User-Name	M	It contains the private user identity in the form of a NAI.
Public-Identity	M	It contains the public user identity in the form of SIP-URL or TEL-URL.
Number-Authentication-Items	M	It indicates the number of authentication vectors provided by the HSS.
Authentication-Data-Item	M	This AVP shall always be present except in the case that the HSS is not able to generate the vectors.
▪ Item-Number	M	Sequence number for the vector
▪ Authentication-Scheme	M	EAP
▪ Authentication-Parameters	M	EAP-Request packet containing RAND, AUTN, XRES, base64 encoded
▪ NAS-Session-Key	M	

-NAS-Key-Direction		BIDIRECTIONAL
-NAS-Key-Type		CIPHER_KEY
-NAS-Key		Confidentiality Key (CK)
▪ NAS-Session-Key	M	
-NAS-Key-Direction		BIDIRECTIONAL
-NAS-Key-Type		INTEGRITY_KEY
-NAS-Key		Integrity Key (IK)
Result-Code	M	See table 6.1.10.2

Note that the values currently defined for NAS-Key-Binding AVP in Diameter NASREQ application are not suitable for Multimedia. At present NAS-Key-Binding is mandatory in NAS-Session-Key, although it has been proposed in the IETF AAA WG to make it optional.

Table 6.1.10.2: Result-Code AVP values for command MAA

Result-Code AVP value	Condition	Defined in
DIAMETER_USER_UNKNOWN (5001)	The MAR message was received for a user that is unknown.	[12]
DIAMETER_AVP_UNSUPPORTED (5002)	The MAR message was received with one or more AVPs not recognised or supported (e.g. invalid format in the identities) and marked with the mandatory bit. MAA shall contain one or more Failed-AVP AVPs (see [12]) containing the AVPs that causes the failure.	[12]
IDENTITIES_DONT_MATCH (5xxx, TBD)	The private (User-Name AVP) and public identities received in the request message do not match.	6.2.2.1
DIAMETER_SUCCESS	The request succeeded. One or more Security-Information AVPs containing authentication vectors shall be returned.	[12]
DIAMETER_UNABLE_TO_COMPLY (5014)	The request failed.	[12]

6.1.9 Registration-Termination-Request (RTR) Command

The Registration-Termination-Request (RTR) command, indicated by the Command-Code field set to TBD 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: TBD, R >
< Session-Id >
{ Auth-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }

{ Public-Identity }
*[AVP]
*[Proxy-Info]
*[Route-Record]

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.11.1: AVP values for command RTR

AVP	Status	Value
User-Name	M	It contains the private user identity in the form of a NAI.
Public-Identity	M	It contains the public user identity in the form of SIP-URL or TEL-URL.
Destination-Host	M	It contains the specific Diameter Multimedia client which originated the last update of the name of the multimedia server stored in the server for a given multimedia user. The address of the Diameter Multimedia client is the same as the Origin-Host AVP in the message sent from the client.

6.1.10 Registration-Termination-Answer (RTA) Command

The Registration-Termination-Answer (RTA) command, indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Registration-Termination-Request command. The Result-Code AVP may contain one of the values defined in section 6.2 in addition to the values defined in [12].

Message Format

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

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.12.1: AVP values for command RTA

AVP	Status	Value
Result-Code	M	See Table 6.1.12.2

Table 6.1.12.2: Result-Code AVP values for command RTA

Result-Code AVP value	Condition	Defined in
DIAMETER_USER_UNKNOWN (5001)	The RTR message was received for a user that is unknown.	[12]
DIAMETER_AVP_UNSUPPORTED (5002)	The RTR message was received with one or more AVPs not recognised or supported (e.g. invalid format in the identities) and marked with the mandatory bit. RTA shall contain one or more	[12]

	Failed-AVP AVPs (see [12]) containing the AVPs that causes the failure.	
IDENTITIES_DONT_MATCH (5xxx, TBD)	The private (User-Name AVP) and public identities received in the request message do not match.	6.2.2.1
DIAMETER_SUCCESS	The request succeeded. The user was successfully de-registered.	[12]
DIAMETER_UNABLE_TO_COMPLY (5014)	The request failed.	[12]

6.1.11 Push-Profile-Request (PPR) Command

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

Message Format

< Push-Profile-Request > ::= < Diameter Header: TBD, R >
< Session-Id >
{ Auth-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
{ Public-Identity }
{ User-Data }
*[AVP]
*[Proxy-Info]
*[Route-Record]

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.13.1: AVP values for command PPR

AVP	Status	Value
User-Name	M	It contains the private user identity in the form of a NAI.
Public-Identity	M	It contains the public user identity in the form of SIP-URL or TEL-URL.
User-Data	M	This AVP contains the data stored in the HSS to serve the user, which exact content is described in TS 29.228 [3].
Destination-Host	M	It contains the specific Diameter Multimedia client which originated the last update of the name of the multimedia server stored in the server for a given multimedia user. The address of the Diameter Multimedia client is the same as the Origin-Host AVP in the message sent from the client.

6.1.12 Push-Profile-Answer (PPA) Command

The Push-Profile-Answer (PPA) command, indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Push-Profile-Request command. The Result-Code AVP may contain one of the values defined in section 6.2 in addition to the values defined in [12].

Message Format

< Push-Profile-Answer > ::=< Diameter Header: TBD, A >
< Session-Id >
{ Auth-Application-Id }
{ Result-Code }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[AVP]
*[Proxy-Info]
*[Route-Record]

The following table contains the values for the Diameter Multimedia Application specific AVPs:

Table 6.1.14.1: AVP values for command PPA

AVP	Status	Value
Result-Code	M	See Table 6.1.14.2

Table 6.1.14.2: Result-Code AVP values for command UDA

Result-Code AVP value	Condition	Defined in
DIAMETER_USER_UNKNOWN (5001)	The PPR message was received for a user that is unknown.	[12]
DIAMETER_AVP_UNSUPPORTED (5002)	The PPR message was received with one or more AVPs not recognised or supported (e.g. invalid format in the identities) and marked with the mandatory bit. PPA shall contain one or more Failed-AVP AVPs (see [12]) containing the AVPs that causes the failure.	[12]
IDENTITIES_DONT_MATCH (5xxx, TBD)	The private (User-Name AVP) and public identities received in the request message do not match.	6.2.2.1
DIAMETER_SUCCESS	The request succeeded.	[12]
DIAMETER_UNABLE_TO_COMPLY (5014)	The request failed.	[12]

6.2 Result-Code AVP values

This section defines new Result-Code [12] values that must be supported by all Diameter implementations that conform to this specification.

6.2.1 Success

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

6.2.1.1 AUTHORISED_FIRST_REGISTRATION (2xxx, TBD)

The user is authorised to register in this server. The user was not registered yet.

6.2.1.2 AUTHORISED_REGISTERED (2xxx, TBD)

The user is authorised to register in this server. The user was already registered (same or another public identity).

6.2.1.3 IDENTITY_NOT_REGISTERED_SERVICES (2xxx, TBD)

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

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 IDENTITIES_DONT_MATCH (5xxx, TBD)

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.

6.2.2.2 IDENTITY_NOT_REGISTERED (5xxx, TBD)

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.

6.2.2.3 ROAMING_NOT_ALLOWED (5xxx, TBD)

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

6.2.2.4 IDENTITY_ALREADY_REGISTERED (5xxx, TBD)

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

6.3 3G AVPs

The following table describes the Diameter AVPs defined in the 3G extension, their AVP Code values, types, possible flag values and whether the AVP may be encrypted.

Table 6.3.1: 3G Extension AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
Visited-Network-Identifier	TBD	6.3.1	OctetString	M			V	N
Public-Identity	TBD	6.3.2	OctetString	M			V	N
Server-Name	TBD	6.3.3	OctetString	M			V	N
Server-Capabilities	TBD	6.3.4	Grouped	M			V	N
Mandatory-Capability	TBD	6.3.5	Unsigned32	M			V	N
Optional-Capability	TBD	6.3.6	Unsigned32	M			V	N
User-Data	TBD	6.3.7	FFS	M			V	N
Number-Authentication-Items	TBD	6.3.8	Unsigned32	M			V	N

Authentication-Scheme	TBD	6.3.9	UTF8String	M			V	N
Authentication-Parameters	TBD	6.3.10	UTF8String	M			V	N
Authentication-Context	TBD	6.3.11	OctetString	M			V	N
Authentication-Data-Item	TBD	6.3.12	Grouped	M			V	N
Item-Number	TBD	6.3.13	Unsigned32	M			V	N
Server-Assignment-Type	TBD	6.3.14	Enumerated	M			V	N

Note: The rules for the setting of flags for these AVPs is FFS. It may depend on the application of the fallback mechanism described in Annex A.

6.3.1 Visited-Network-Identifier AVP

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

6.3.2 Public-Identity AVP

The Public-Identity AVP (AVP Code TBD) 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 [8] and [10]) or a TEL URL (with the format defined in [15]).

6.3.3 Server-Name AVP

The Server-Name AVP (AVP Code TBD) is of type UTF8String. This AVP contains a SIP-URL (as defined in [8] and [10]), used to identify a SIP server (e.g. S-CSCF name).

6.3.4 Server-Capabilities AVP

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

AVP format

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

*[Mandatory-Capability]

*[Optional-Capability]

*[Server-Name]

*[AVP]

6.3.5 Mandatory-Capability AVP

The Mandatory-Capability AVP (AVP Code TBD) is of type Unsigned32. The value included in this AVP can be used to represent a determined mandatory capability of an S-CSCF. The exact meaning of each value is an operator issue.

6.3.6 Optional-Capability AVP

The Optional-Capability AVP (AVP Code TBD) is of type Unsigned32. The value included in this AVP can be used to represent a determined optional capability of an S-CSCF. The exact meaning of each value is an operator issue.

6.3.7 User-Data AVP

The User-Data AVP (AVP Code TBD) is of type FFS. This AVP contains the user data required to give service to a user.

Note: the exact content and format of this AVP shall be described in TS 29.228.

6.3.8 Number-Authentication-Items AVP

The Number-Authentication-Items AVP (AVP code TBD) is of type Unsigned32.

When used in a request it indicates the number of Authentication-Data-Items the Diameter client is requesting. This can be used, for instance, when the client is requesting several pre-calculated authentication vectors from a back-end server. In the answer message the Number-Authentication-Items AVP indicates the actual number of items provided by the Diameter server.

6.3.9 Authentication-Scheme AVP

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

6.3.10 Authentication-Parameters AVP

The Authentication-Parameters AVP (AVP code TBD) is of type UTF8String, and contains the comma-separated list of attribute-value pairs that carry the parameters necessary for achieving authentication via a specific scheme. The contents of this format depend on the authentication scheme used.

6.3.11 Authentication-Context AVP

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

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

6.3.12 Authentication-Data-Item AVP

The Authentication-Data-Item (AVP code TDB) is of type Grouped, and contains the authentication information for the Diameter client.

Authentication-Data-Item :: = < AVP Header : TBD >

[Item-Number]

[Authentication-Scheme]

[Authentication-Parameters]

*[NAS-session-key]

* [AVP]

6.3.13 Item-Number AVP

The Item-Number AVP (AVP code TBD) is of type Unsigned32, and indicates to the client, which is the position the item occupies in a multiple occurrence of the Authentication-Data-Item AVP. The significance of the order depends on the specific authentication mechanism. It can be useful, as well, when several challenges belonging to different schemes are to be presented to the end-user.

6.3.14 Server-Assignment-Type AVP

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

NO_ASSIGNMENT	0
REGISTRATION	1
RE_REGISTRATION	2
UNREGISTERED_USER	3
TIMEOUT_DEREGISTRATION	4
USER_DEREGISTRATION	5
AUTHENTICATION-FAILURE	6

6.4 Interaction with IETF

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

This specification assigns the values TBD from the Command Code namespace defined in [12]. See section 6.1 for the assignment of the namespace in this specification.

6.4.1 AVP codes

This specification assigns the values TBD from the AVP Code namespace defined in [12]. See section 6.3 for the assignment of the namespace in this specification.

Note: This specification may also make use of AVPs defined in other existing extensions to Diameter, fact that would be reflected in this section.

6.4.2 Result-code AVP values

This specification has not assigned any Result-Code AVP value yet.

Note: In case this specification would assign values for the Result-Code AVP value namespace, such assignment would be reflected in section 6.2.

7 Special Requirements

7.1 Version Control

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

Cx interface in an intra-operator interface. The way to implement mechanisms for the control of versions is FFS.

Annex A (informative): Interaction with IETF

A.1 Diameter Multimedia Application RFC

CN4 shall collect the requirements from the procedures described by SAx working groups (SA2 for multimedia procedures, SA3 for security related procedures) and shall detail them until the level of detail required for the implementation of the extension to Diameter.

The companies supporting the IETF approach would work in the Diameter Multimedia Application in IETF.

The progress of the work in IETF (actual content of the IETF draft with the extension) would be included in this specification and used as stage 3 specification of the Cx interface.

A.2 Vendor Specific 3G Extensions to Diameter

All the requirements from 3GPP should be supported by a vendor specific extension. A 3GPP specific extension would be developed in case of trouble to get some requirements approved (first fallback mechanism)

It is quite difficult to establish a time schedule for the work in IETF. 3GPP time schedule would trigger the second fallback mechanism, which would consist in taking the progress reached by the work in IETF (work that would be anyway present in CN4 specifications) and use it to define a vendor specific extension.

Annex B (informative): Change history

Date	TSG #	TSG Doc.	CR#	Rev	Subject/Comment	In	Out
2001-07	CN4#9	N4-010932	-	-	Creation of version 0.1.0	0.0.1	0.1.0
2001-10	CN4#10	N4-011064	-	-	▪ Correction of title following MCC instructions. ▪ Addition of description of implicit termination of sessions to 5.2.6. ▪ Deletion of Authorization-Lifetime AVP in all messages. ▪ Addition of Auth-Session-State AVP to all messages. ▪ “Subscriber” replaced with “user”. ▪ Corrections in result codes tables. ▪ SIR command renamed to MAR (Multimedia Authentication Request) ▪ Public-Identity AVP re-defined	0.1.0	0.2.0
2001-11	CN4#11	N4-011296	-	-	▪ Introduction of authentication messages and AVPs according to N4-011066. ▪ The Server-Capability AVP is now optional in RAA. ▪ Introduction of PPR operation according to N4-011166. ▪ Introduction of capabilities for the selection of S-CSCF according to N4-011065. ▪ Renaming of command Location-Update to Server-Assignment. ▪ Completion of command Server-Assignment according to N4-011169	0.2.0	0.3.0
2001-11	CN4#11	N4-011408	-	-	▪ Introduction of changes agreed in N4-011300, N4-011376, N4-011297, N4-011298, N4-011299.	0.4.0	1.0.0

Annex C (informative): Proposed authentication scheme for the Diameter Multimedia Application (IETF)

This is the description of the commands for the IETF draft. The generalities it includes may not be all necessary for 3GPP.

This proposal tries to give a general support to the authentication framework defined for SIP. The Diameter messages provide a generic container for passing the information in the SIP authentication headers. This approach provides support to currently defined authentication schemes (e.g. basic, digest, eap…) and minimises the impact on the protocol due to the introduction of new schemes.

The framework for SIP authentication parallels that for HTTP [RFC 2617]. This framework provides a simple challenge-response authentication mechanism that may be used by a proxy, server or registrar to challenge a user agent request and by a user agent to provide authentication information. It uses an extensible, case-insensitive token to identify the authentication scheme, followed by a comma-separated list of attribute-value pairs which carry the parameters necessary for achieving authentication via that scheme.

When a server wants to authenticate a user agent request it includes a challenge in the WWW_Authentication header in the following form:

challenge = auth-scheme 1*SP 1#auth-param

auth-scheme = token

auth-param = token "=" (token | quoted-string)

The user agent shall answer the challenge providing an appropriated response containing the following in the Authorization header:

credentials = auth-scheme #auth-param

Two different authentication scenarios are proposed, depending on the roles of the Diameter Multimedia peers:

- In the normal AAA case, where the AAAH is responsible for authenticating the user, the Diameter Multimedia client maps Diameter and SIP messages in the following way:

  SIP REQUEST message with no Authorization header needs to be mapped to Multimedia-Auth-Request (MAR) command.

  Multimedia-Auth-Answer (MAA) command with Result-Code equal to DIAMETER_MULTI_ROUND_AUTH has to be mapped to a SIP 401/407 Response's WWW-Authenticate/Proxy-Authenticate header. The challenge information contained in the MAA is mapped into the Authenticate header.

  SIP REQUEST message with Authorization/Proxy-Authorization header has to be mapped to a MAR command containing the authentication information.

  MAA command with Result-Code DIAMETER_SUCCESS has to be mapped to SIP 200 OK Response.

- The Diameter peer acting as Multimedia client is the one that performs actual authentication. The Diameter Multimedia server acts as backend authentication server and provides the necessary information to perform the authentication (e.g. challenge/response pairs, one-time-password lists, user certificates…). In this case there is no direct mapping between SIP and Diameter messages. The Diameter client shall use the MAR message to retrieve authentication information whenever it is necessary. Depending on the authentication scheme used, it may be possible for the client to retrieve several pre-computed authentication credentials. In this case the Diameter Result Code AVP corresponds to the retrieval of the authentication information and not to the user authentication result. It is assumed that when this authentication mode is used, the client and the server has pre-configured information about the authentication schemes supported by the client.

C.1Diameter Attributes

This section defines the new AVP required by this application.

C.1.1 Public-Identity AVP

The Public-Identity AVP (AVP Code TBD) is of type OctetString, encoded in the UTF-8 [9] format. 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 RFC 2543 and RFC 2396) or a TEL URL (with the format defined in RFC 2806).

The Diameter Multimedia client uses information found in the header of the SIP messages (e.g. To: field in REGISTER messages or From: field in INVITE messages) to construct the Public-Identity AVP.

C.1.2 Number-Authentication-Items AVP

The Number-Authentication-Items AVP (AVP code TBD) is of type Unsigned32 and indicates the number of authentication vectors provided by the Diameter Server.

When used in a request it indicates the number of Authentication-Data-Items the Diameter client is requesting. This can be used, for instance, when the client is requesting several pre-calculated authentication vectors from a back-end server. In the answer message the Number-Authentication-Items AVP indicates the actual number of items provided by the Diameter server.

C.1.3 Authentication-Scheme AVP

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

C.1.4 Authentication-Parameters AVP

The Authentication-Parameters AVP (AVP code TBD) is of type UTF8String, and contains the comma-separated list of attribute-value pairs that carry the parameters necessary for achieving authentication via a specific scheme. The contents of this format depend on the authentication scheme used.

C.1.5 Authentication-Context AVP

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

Some mechanisms (e.g. PGP, digest with quality of protection set to auth-int [RFC 2617], digest with predictive nonces [7] or sip access digest [8]) request that part or the whole SIP request is passed to the entity performing the authentication. In such cases the Authentication-Context AVP would be carrying such information.

This AVP can be also needed for authorisation purposes.

C.1.6 Authentication-Data-Item AVP

The Authentication-Data-Item (AVP code TDB) is of type Grouped, and contains the authentication information for the Diameter client.

Authentication-Data-Item :: = < AVP Header : TBD >

[Item-Number]

[Authentication-Scheme]

[Authentication-Parameters]

*[NAS-session-key]

* [AVP]

The Item-Number AVP (AVP code TBD) is of type Unsigned32, and indicates the client which is the position the item occupies in a multiple occurrence of the Authentication-Data-Item AVP. The significance of the order depends on the mechanisms. It can be useful, as well, when several challenges belonging to different schemes are to be presented to the end-user.

The Authentication-Scheme AVP is defined above. It indicates the authentication scheme to which the parameters are applicable.

The Authentication-Parameters AVP is defined above. It contains the information the client shall use to authenticate the client (e.g. challenge to be presented to the user), according to the authentication scheme utilised. Usually, the Diameter Multimedia client will use this information in the multimedia signalling messages without modification.

The NAS-Session-Key AVP (see definition in [16]) contains the encryption keys that may be derived from the authentication vectors. The value of this AVP takes precedence over any possible NAS-Session-Key AVP present outside the Authentication-Data-Item AVP.

C.2Diameter Commands

C.2.1 Multimedia-Auth-Request (MAR) Command

The Multimedia-Auth-Request (MAR), indicated by the Command-Code field set to TBD 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 user authentication and authorisation.

Message Format

```
< Multimedia-Auth-Request > ::= < Diameter Header: TBD, REQUEST >
                                < Session-Id >
                                { Auth-Application-Id = TBD}
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Realm }
                                [ Destination-Host ]
                                [ User-Name ]
                                [ Public-Identity ]
                                [ Authentication-Scheme ]
                                [ Authentication-Parameters ]
                                [ Authentication-Context ]
                                [ Number-Authentication-Items ]
                                [ Authorization-Lifetime ]
                                [ Auth-Grace-Period ]
                                [ Auth-Session-State ]
                                [ Session-Timeout ]
                                [ Idle-Timeout ]
                                [ Origin-State-Id ]
                                * [ AVP ]
                                * [ Proxy-Info ]
                                * [ Route-Record ]
```

C.2.2 Multimedia-Auth-Answer (MAA) Command

The Multimedia-Auth-Answer (MAA), indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Auth-Request command.

Message Format

```
< Multimedia-Auth-Answer > ::=  < Diameter Header: TBD, ANSWER >
                                < Session-Id >
                                { Auth-Application-Id }
                                { Result-Code }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Error-Reporting-Host ]
                                [ User-Name ]
                                [ Public-Identity ]
                                [ Number-Authentication-Items ]
                                * [ Authentication-Data-Item ]
                                [ Idle-Timeout ]
                                [ Authorization-Lifetime ]
                                [ Auth-Grace-Period ]
                                [ Auth-Session-State ]
                                [ Re-Auth-Request-Type ]
                                [ Session-Timeout ]
                                [ Origin-State-Id ]
                                * [ AVP ]
                                * [ Proxy-Info ]
                                * [ Route-Record ]
```