Network Working Group
INTERNET-DRAFT
Category: Standards Track
Expires: May 2003

Maria-Carmen Belinchon
Miguel-Angel Pallares
Carolina Canales
Ericsson
Peter J. McCann
Lucent
Jaakko Rajaniemi
Nokia

November, 2002

Diameter Multimedia Application
<draft-johansson-aaa-diameter-mm-app-02.txt>

Status of this memo

Abstract

This document specifies a Diameter application that allows to perform the authentication, authorization, and collection of accounting information for Session Initiation Protocol (SIP) services rendered to a client node. This application, combined with the base Diameter protocol and appropriate SIP extensions, allows SIP User Agents (UAs) to obtain services from SIP servers that are connected to a Diameter infrastructure. When combined with the Inter-Domain capability of the base protocol, service may even be obtained from SIP servers that

belong to foreign domains, as would be encountered by roaming mobile nodes.

Note that the specification defined here may be used independently of the authentication technique used for authenticating a node's link layer or network-layer access. In particular, we do not require that the client node was authenticated for access with the use of either the Mobile IP [4] or NASREQ [3] Diameter application.

TABLE OF CONTENTS

1. Introduction

This document specifies a Diameter application that allows to perform the authentication, authorization and collection of accounting information for SIP-based IP multimedia services rendered to a client node. We assume that a client node implements a SIP User Agent (UA) that carries out SIP protocol actions with a SIP server, which in turn relies on the AAA infrastructure for authenticating the client, authorizing it for particular SIP services, and accounting for this usage.

SIP servers can be proxy, redirect, registration, or user agent servers. Additionally, SIP servers may be arranged in arbitrary ways according to the inter-service provider relationships involved in servicing a given client. For example, a mobile node may use a SIP proxy in the visited network, but its SIP messages may be proxied back to a SIP server in the home network that implements call control features. Combined with the Inter-Domain capability of the base protocol, this extension would allow such mobile terminals to receive service from foreign service providers according to their location and subscription profile. Any or all of the SIP servers may need to

independently authenticate the client, authorize service, and account for usage.

Authentication must take place at the time the user agent registers with the SIP server (or chain of SIP proxies and servers) or at any other moment agreed by the entities involved in the authentication (e.g., at SIP session initiation). The particular algorithm used to authenticate a SIP user agent client is a matter of policy agreement between the user agent client, the SIP server, and the home AAA server. This document supports the WWW-Authenticate methods Basic and Digest, which are supported by SIP. In addition to authenticating the user agent client, such a method could also be used to generate or distribute keys for subsequent SIP-layer message integrity and privacy. The specification of such an algorithm, and its embedding in SIP, is outside the scope of this document.

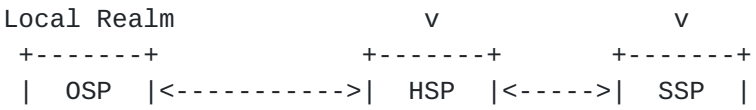
Authorization for SIP services may take many forms. For example, a proxy may need to know that the user agent client is authorized to register, but from then on it may simply pass messages through to other SIP servers. However, a SIP server that implements call control features may need a richer and more complete description of the services to which the user has subscribed.

Accounting for SIP services is on a per-call basis. An accounting record contains a SIP Call-ID, any SDP that was exchanged to set up the call, the duration of the call, and any resources that were consumed on behalf of the call (such as number of bytes exchanged between the parties). Note that accounting for resources may require the SIP server to interact with other network entities, such as media gateways, for the collection of this information. Such interaction is outside the scope of this document. Some example scenarios, inspired by the emerging wireless applications of SIP, are given in Section 2. Sections 3, 4 and 5 address the Diameter Multimedia Application's specific commands, result codes, and AVPs, respectively. Section 7 gives IANA considerations.

1.1 Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [10].

2 Description of a SIP network architecture


Local Realm
v
v
OSP
HSP
SSP

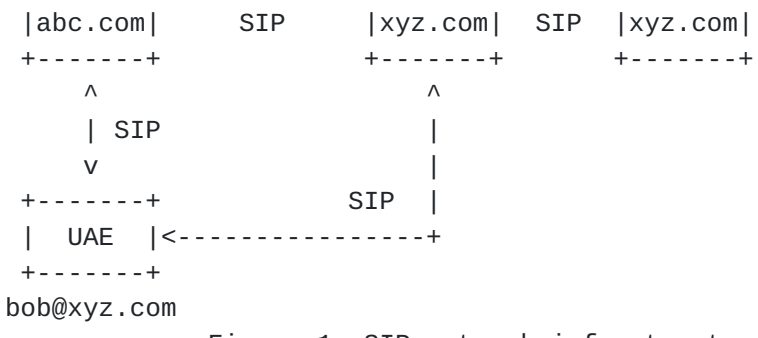


Figure 1: SIP network infrastructure

Figure 1 above illustrates the nodes involved in a SIP multimedia network architecture, according to the requirements in [1]. The home realm (xyz.com) is comprised of a Diameter AAA server, at least one home entry SIP proxy (HSP) which is the gateway SIP proxy seen by the rest of the world, and any number of serving SIP proxy (SSP) nodes. These SSP nodes may be deployed piecemeal for various reasons such as but not limited to load balancing, scalability, and offering distinct, separate services.

The mobile node in this scenario (bob@xyz.com) may either connect directly to its HSP, or via an outbound SIP server (OSP) in the local realm. In larger networks, registrations MAY be routed to different HSPs, potentially even for a subsequent SIP registration for the same user, and thus HSPs are usually stateless.

The next few sections will describe in detail the different modes of operation that are available to such an infrastructure. These options may be either administratively configured to suit local policies, or determined dynamically by the network. For the purposes of authentication and authorization, the procedures involved when using a OSP are a superset of the procedures involved in the absence of a OSP, and therefore we will skip a needless explanation of the latter scenario.

2.1 User authentication by SSP

An operator with a large base of installed SIP servers may wish to minimize the impact of modifying SIP servers to interact with Diameter AAA servers. This can be achieved by allowing SIP servers to retain the functionality of authentication, rather than exporting this capability to the AAA server. However, it should be noted that this mode will not leverage the extensive array of authentication and authorization services which will already be present regardless in diameter servers. Below follows an example of a SIP user registration using the SSP authentication mode.


HSP
AAA
SSP

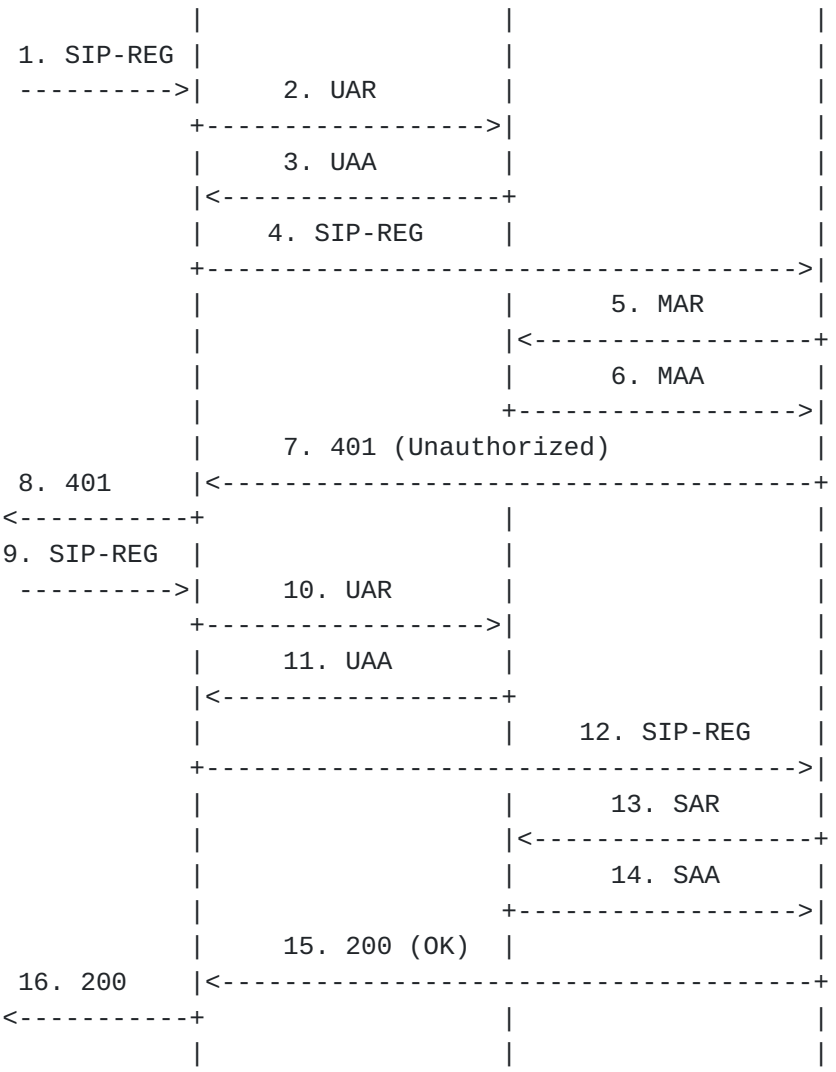


Figure 2: Authentication performed by the SSP

In this scenario, a user sends a SIP registration to the home domain. The HSP will contact its local diameter server with a "User-Authorization-Request" (UAR) to authorize if this user is allowed to receive service, and if so, request the identity of a local SIP server capable of handling this user. The diameter server will respond with a "User-Authorization-Answer" (UAA), which will inform about the result of the user authorization request in the Result-Code AVP. The result values are defined in section 4 in addition to the values defined in [2]. When the authorization successes, the UAA will indicate either the identity of a local SIP server or a list of capabilities from which the HSP will select the SSP.

If the result falls into the success category, then the HSP will forward the registration request to the appropriate SSP. The SSP will then request authentication parameters from the diameter server through a "Multimedia-Auth-Request" (MAR). This request MAY also

serve to identify the SSP, so as to return subsequent registration requests of the same user to the same SSP. The diameter server will respond with a "Multimedia-Auth-Answer" (MAA), which will include all

parameters necessary for the designated authentication algorithm associated with the user. The SSP will then create the 401 (Unauthorized) message, including the authentication material needed by the mobile user to prove his/her identity.

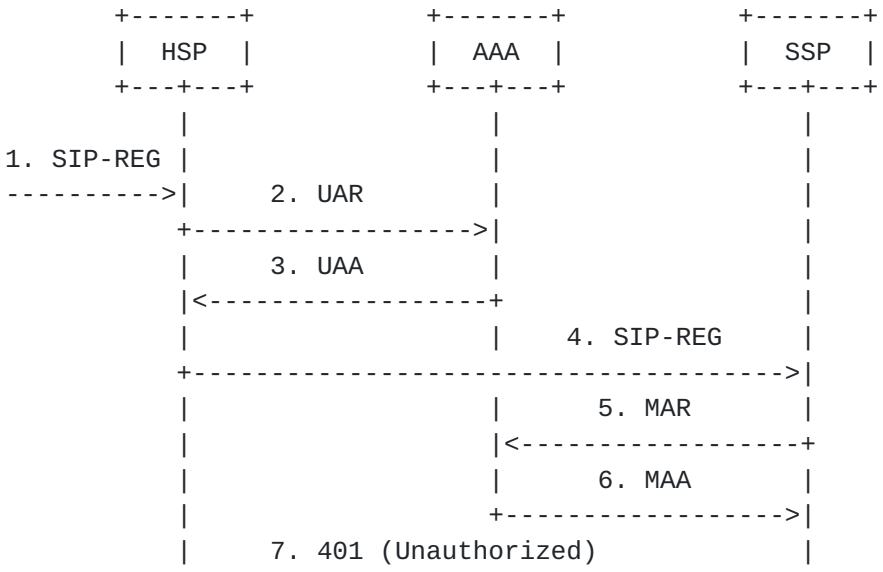
When the subsequent SIP registration is received from the user, the HSP (assumed to be stateless) will once again contact the diameter server with a UAR to determine to which SSP to forward the registration. The HSP will then forward the SIP registration to the SSP node. The SSP node performed the authentication in the previous registration request by means of MAR/MAA, so at this point it is not necessary to ask for it again, instead, it will contact the AAA server by means of a Server-Assignment-Request (SAR) requesting it to store the name of the server that is currently serving the user.

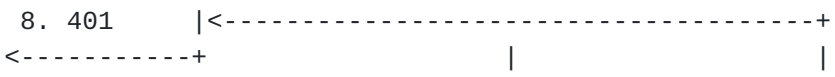
The AAA server will respond with a "Server-Assignment-Answer" (SAA). If the Result-Code does not inform about an error, the User-Data AVP shall contain the information that the SSP needs to give service to the user.

The SSP will produce then a 200 (OK) message, and send it to the HSP. The HSP will then forward the 200 (OK) message towards the mobile user.

2.2 User authentication by AAA server

A different approach in deploying SIP networks is to allow the Diameter server to perform the actual authentication. In addition to leveraging the robust authentication services offered by the AAA server, it will reduce the number of messages sent in the network.




8. 401

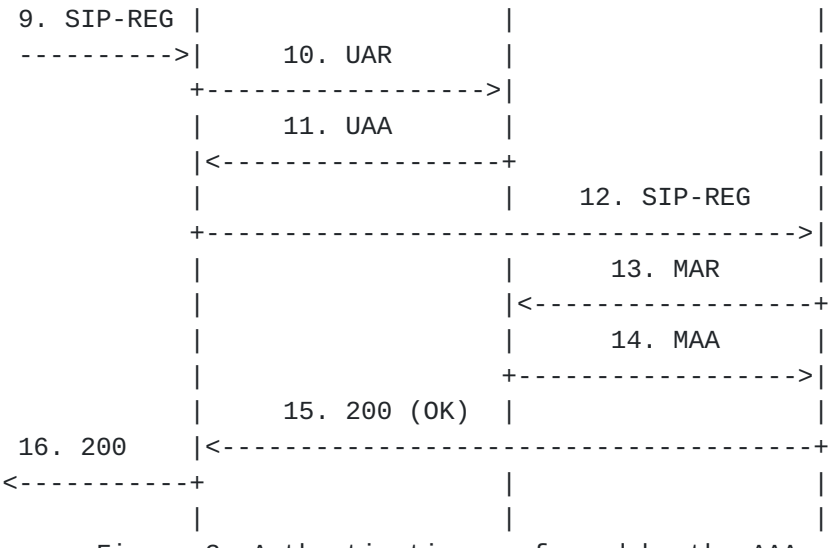


Figure 3: Authentication performed by the AAA server

In this scenario, the user will send a SIP register message to it's home domain. When the HSP receives this request, it will contact its local diameter server with a "User-Authorization-Request" (UAR) to determine if this user is allowed to receive service and if so, request the identity of a local SIP server capable of handling this user, as described in the previous section. The diameter server will respond with a "User-Authorization-Answer" (UAA), which will indicate a list of capabilities from which the HSP will use to select the SSP.

Once it forwards the initial SIP registration to the appropriate SSP, the SSP will then request user authentication from the Diameter server through a "Multimedia-Auth-Request" (MAR). This request MAY also serve to identify the SSP, so as to return subsequent registration requests to the same SSP. The Diameter server will then respond with a "Multimedia-Auth-Answer" (MAA) with Result-Code equal to DIAMETER_MULTI_ROUND_AUTH and the challenge information, which the SSP will use to map into the WWW-authentication header in the SIP 401 unauthorized and send back to the HSP.

When the subsequent SIP registration is received from the user, the HSP will once again contact the diameter server with a UAR to determine to which SSP to forward the registration. The HSP will then forward the SIP registration to the SSP node, which will then extract the relevant authentication parameters, and include these in a MAR message to the AAA server. This request MAY also serve to identify the SSP, so as to return subsequent registration requests to the same SSP. At this point, the Diameter server will be able to authenticate the user, and upon success, will return a MAA with Result-Code equal to DIAMETER_SUCCESS and include user profile information, which the SSP will use to give service to the user, the SSP will then produce a 200 (OK) message and send it to the HSP, which will then forward it

to the mobile user.

2.3 Invitation

When a registered user wishes to invite another registered user, it will send a SIP Invite request to the home domain (HSP) of the invitee.

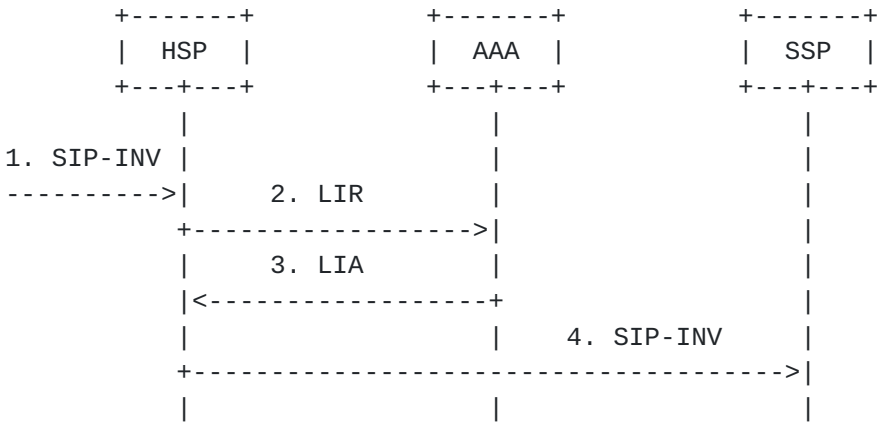


Figure 5. A SIP Invite request

In this scenario, when a user, say Bob, contacts the HSP to invite another user, say Mary, the MaryÆs HSP will issue a diameter "Location-Info- Request" (LIR) message to the AAA server to request the identity of the SSP currently assigned to Mary. The AAA server will respond with a diameter "Location-Info-Answer" (LIA), indicating the appropriate SSP, and the HSP will forward the SIP Invite message directly to the named SSP.

2.4 User Profile Updating

Whenever a modification in the user profile has occurred, the AAA server and SSP must synchronize their user profile data.

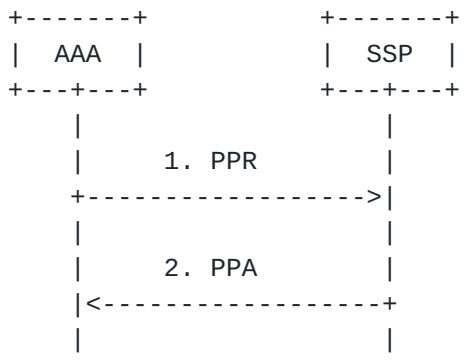


Figure 6. User profile update initiated by AAA server

The AAA server sends a Push-Profile-Request (PPR) to the serving SIP

server to which the user is registered. The PPR message contains a SIP-User-Data AVP, a SIP-User-Name AVP, and zero or more SIP-Public-

Identity AVPs. The presence of the SIP-User-Name AVP without any SIP- Public-Identity AVPs serves to indicate that the entire user profile associated with the SIP-User-Name AVP should be updated. A PPR with a SIP-User-Name AVP and one or more SIP-Public-Identity AVPs serves to indicate that the user profile data associated with each of the SIP- Public-Identity AVPs should be updated.

2.5 User registration termination

Termination of an entire user registration can be achieved by one of two mechanisms. In the event that NO_STATE_MAINTAINED (i.e NO Diameter user session-id is maintained) has been indicated in a prior Auth-Session-State AVP, termination is handled with a Session-Termination-Request (if it is initiated by the SSP/HSP) or with a Registration-Termination-Request (if it is initiated by the AAA).

On the other hand, if STATE_MAINTAINED has been indicated in a prior Auth-Session-State AVP, the use of Session-Termination-Request (STR) and Abort-Session-Request (ASR) messages as defined in the base protocol are used to terminate an entire user registration.

Reasons for terminating a user registration could be due to the expiration of the SIP registration timer in the SIP server, a user initiated SIP de-registration, or a AAA-initiated de-registration as a result of administrative reasons.

3 Command Codes

This section will define the specific message formats used by this diameter application.

3.1 User-Authorization-Request (UAR) Command

The User-Authorization-Request (UAR), indicated by the Command-Code field set to TBD and the 'R' bit set in the Command Flags field, is sent by an HSP node, acting as a Diameter client, to a AAA server in order to request authorization of a mobile user.

Message Format

```
< User-Authorization-Request > ::= Diameter Header: TBD: REQ, PXY >
                                   < Session-ID >
                                   < Auth-Application-Id >
                                   { Auth-Session-State }
                                   { Origin-Host }
                                   { Origin-Realm }
                                   [ Destination-Host ]
                                   { Destination-Realm }
```

{ SIP-User-Name }
{ SIP-Public-Identity }

```
                                { Visited-Network-Identifier }
                                [ User-Authorization-Type ]
                                * [ AVP ]
                                * [ Proxy-Info ]
                                * [ Route-Record ]
```

3.2 User-Authorization-Answer (UAA) Command

The User-Authorization-Answer (UAA), indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by a AAA server in response to the User-Authorization-Request command. The Result-Code AVP may contain one of the values defined in section 4 in addition to the values defined in [2].

If the user has not previously been authorized, the UAA will make use of the Server-Capabilities AVP to convey information needed by the HSP to select an appropriate SSP.

If the user has already been authorized and a server has already been assigned which is still valid for the user's service profile, the SIP-Server-Name AVP MUST be present which contains the SIP URL of the currently assigned server, so that the HSP can forward the registration request to it.

If the user has already been authorized, and a server has already been assigned which may not be valid for the user's service profile, two pieces of information must be returned to allow the HSP to decide what action to take. First, the Server-Name AVP MUST be present which contains the SIP URL of the currently assigned server. Second, the Server-Capabilities AVP MUST present which contains information to allow the HSP to select an appropriate SIP server.

Message Format

```
< User-Authorization-Answer > ::= < Diameter Header: TBD: PXY >
                                < Session-Id >
                                { Auth-Application-Id }
                                { Auth-Session-State }
                                [ Result-Code ]
                                { Origin-Host }
                                { Origin-Realm }
                                [ SIP-Server]
                                [ Authorization-Lifetime ]
                                [ Auth-Grace-Period ]
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

3.3 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.

Message Format

```
<Server-Assignment-Request> ::= < Diameter Header: TBD, REQ, PXY>
                                < Session-Id >
                                { Auth-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                [ SIP-User-Name ]
                                *[ SIP-Public-Identity ]
                                [ SIP-Server ]
                                { SIP-Server-Assignment-Type }
                                { User-Data-Request-Type }
                                { User-Data-Already-Available }
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

3.4 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 4 in addition to the values defined in [2]. If Result-Code does not inform about an error, the User-Data AVP shall contain the information that the S-CSCF needs to give service to the user.

Message Format

```
<Server-Assignment-Answer> ::=  < Diameter Header: TBD: PXY >
                                < Session-Id >
                                { Auth-Application-Id }
                                [ Result-Code ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ SIP-User-Data ]
                                [ Charging-Information ]
                                [ Auth-Grace-Period ]
```

```
                                [ Authorization-Lifetime ]
                                *[ AVP ]
                                *[ Proxy-Info ]
```

```
                                *[ Route-Record ]
```

3.5 Location-Info-Request (LIR) Command

The Location-Info-Request (LIR), indicated by the Command-Code field set to TBD and the 'R' bit set in the Command Flags field, is sent by a HSP node, acting as a Diameter client, to a Diameter server in order to request the identity of SIP server currently associated with a particular user.

Message Format

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

3.6 Location-Info-Answer (LIA) Command

The Location-Info-Answer (LIA), indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by a Diameter server in response to a Location-Info-Request. If the user in the request is currently registered in the AAA server, the answer will include the identity of the SIP server currently associated with the user. The Result-Code AVP may contain one of the values defined in section 4 in addition to the values defined in [2].

Message Format

```
< Location-Info-Answer > ::= < Diameter Header: TBD: PXY >
                              < Session-Id >
                              { Auth-Application-Id }
                              [ Result-Code ]
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              [ SIP-Server ]
                              [ Auth-Grace-Period ]
                              [ Authorization-Lifetime ]
                              *[ AVP ]
                              *[ Proxy-Info ]
```

*[Route-Record]

3.7 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 an SSP node, acting as a Diameter client, to a server in order to request the authentication of a mobile user. The Diameter client uses information found in the SIP Request to construct the AVPs that are to be included as part of the MAR.

Message Format

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

3.8 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 the server in response to the Multimedia-Auth-Request command. The Result-Code AVP may contain one of the values defined in section 4 in addition to the values defined in [2].

Message Format

```
< Multimedia-Auth-Answer > ::= < Diameter Header: TBD, PXY >
                               < Session-Id >
                               { Auth-Application-Id }
                               [ Result-Code ]
                               { Auth-Session-State }
                               { Origin-Host }
                               { Origin-Realm }
                               [ SIP-User-Name ]
                               [ SIP-Public-Identity ]
                               [ SIP-Number-Auth-Items ]
```

```
                                * [ SIP-Auth-Data-Item ]
                                [ SIP-User-Data ]
```

```
                                [ Authorization-Lifetime ]
                                [ Auth-Grace-Period ]
                                * [ AVP ]
                                * [ Proxy-Info ]
                                * [ Route-Record ]
```

3.9 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, REQ,
PXY >
                                < Session-Id >
                                { Auth-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Host }
                                { Destination-Realm }
                                { SIP-User-Name }
                                *[ SIP-Public-Identity ]
                                { DeRegistration-Reason }
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

3.10 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 4 in addition to the values defined in [2].

Message Format

```
<Registration-Termination-Answer> ::=  < Diameter Header: TBD, PXY >
                                < Session-Id >
                                { Auth-Application-Id }
                                [ Result-Code ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
```

```
                        [ Auth-Grace-Period ]
                        [ Authorization-Lifetime ]
                        *[ AVP ]
```

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

3.11 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.

Message Format

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

3.12 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 4 in addition to the values defined in [2].

Message Format

```
< Push-Profile-Answer > ::=< Diameter Header: 10415: 305 >
                                < Session-Id >
                                { Auth-Application-Id }
                                [Result-Code ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                *[ AVP ]
```

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

4 Result Code AVP values

This section defines new Result codes in addition to the values defined in [2].

4.1 Success

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

DIAMETER_FIRST_REGISTRATION 2xxx
The user was not previously registered, and has now been authorized by the AAA server. Information necessary to select an appropriate SSP SHOULD be included in the message.

DIAMETER_SUBSEQUENT_REGISTRATION 2xxx
The user has been previously registered, and has now been re-authorized by the AAA server. The identity of the SSP to which the user is currently registered SHOULD be included in the message.

DIAMETER_SEPARATE_REGISTRATION 2xxx
The user has been previously registered, but with a different public identifier (and associated service profile). The identity of the SSP to which the user is currently registered MUST be included in the message, and in the event a new SSP must be assigned (based on the new service profile), information necessary to select an appropriate SSP MUST be included in the message as well.

DIAMETER_UNREGISTERED_SERVICE 2xxx
The user is not currently registered, but the requested service can still be granted to the user.

4.2 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.

DIAMETER_ERROR_ROAMING_NOT_ALLOWED 5xxx
This error code is used to indicate that there is no multimedia roaming agreement between the home and visited networks.

DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED 5xxx
The identity being registered has already a server assigned and the registration status does not allow that it is overwritten.

DIAMETER_ERROR_IDENTITY_NOT_REGISTERED	5xxx

This error code is used to inform that the received public identity has not been registered before and the user to which this identity belongs cannot be given service in this situation.

DIAMETER_ERROR_IDENTITIES_DONT_MATCH 5xxx
The value in one of the Public-Identity AVPs does not correspond to the user specified in the SIP-User-Name AVP.

5 Diameter AVP values

The following sections define the AVPs used in this diameter application.

5.1 SIP-Server AVP

The SIP-Server AVP (AVP code TBD) is of type Grouped. This AVP MAY be used by the HSP to assist in the selection of a SSP.

```
SIP-Server ::= < AVP Header: TBD >
               { SIP-Server-Name }
             * [ SIP-Server-Capability ]
             * [ AVP ]
```

5.1.1 SIP-Server-Name AVP

The SIP-Server-Name AVP (AVP Code TBD) is of type UTF8String. This AVP contains a SIP-URL (as defined in [5] and [6]) used to identify a SIP server.

The HSP MAY include the SIP-Server-Name AVP to inform the Diameter server which SSP to use for the SIP user or the SIP-Server-Name AVP MAY be used by the Diameter server to inform the HSP that the SIP UA client is assigned at the following SSP server.

5.1.2 SIP-Server-Capability AVP

The SIP-Capability AVP (AVP Code TBD) is of type Grouped. This AVP is used to indicate support for particular SIP capability, and contains the information to assist the HSP in the selection of an SSP.

```
SIP-Capability ::= < AVP Header: TBD >
                   *[ Mandatory-Capability ]
                   *[ Optional-Capability ]
                   *[ AVP ]
```

5.1.2.1 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 single determined mandatory capability of an SSP. Each mandatory capability available in an individual operatorÆs network shall be allocated a unique value. The allocation of these values to individual capabilities is an operator issue.

5.1.2.2 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 single determined optional capability of an SSP. Each optional capability available in an individual operatorÆs network shall be allocated a unique value. The allocation of these values to individual capabilities is an operator issue.

5.2 SIP-Public-Identity AVP

The SIP-Public-Identity AVP (AVP Code TBD) is of type OctetString, encoded in the UTF-8 format. The syntax of this AVP corresponds either to a SIP URL (with the format defined in [5] and [6]) or a TEL URL (with the format defined in [7]).

This AVP contains the SIP public identity of a user in the IMS.

The Diameter client (HSP or SSP) 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 SIP-Public-Identity AVP.

5.3 SIP-Visited-Network-Identifier AVP

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

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

REGISTRATION (1)

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

RE_REGISTRATION (2)
The request corresponds to the re-registration of an identity.

UNREGISTERED_USER (3)
The request is generated because the SSP received an INVITE for a public identity that is not registered.

TIMEOUT_DEREGISTRATION (4)
The SIP registration timer of an identity has expired.

USER_DEREGISTRATION (5)
The SSP has received a user initiated de-registration request.

TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME (6)
The SIP registration timer of an identity has expired. The S-CSCF keeps the user data stored in the SSP and requests AAA to store the SSP name.

USER_DEREGISTRATION_STORE_SERVER_NAME (7)
The SSP has received a user initiated de-registration request. The SSP keeps the user data stored in the SSP and requests AAA to store the SSP name.

ADMINISTRATIVE_DEREGISTRATION (8)
The SSP, due to administrative reasons, has performed the de-registration of an identity.

AUTHENTICATION_FAILURE (9)
The authentication of a user has failed.

AUTHENTICATION_TIMEOUT (10)
The authentication timeout has expired.

5.5 SIP-Auth-Data-Item AVP

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

```
    SIP-Auth-Data-Item :: = < AVP Header : TBD >
                            [ SIP-Item-Number ]
                            [ SIP-Authentication-Scheme ]
                            [ SIP-Authenticate ]
                            [ SIP-Authorization ]
                            [ SIP-Authentication-Info ]
                            [ SIP-Authentication-Context ]
                          * [ NAS-Session-Key ]
```

* [AVP]

5.5.1 SIP-Item-Number AVP

The SIP-Item-Number (AVP code TDB) is of type Unsigned32, and is included in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value (such as 1) should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value (such as 13).

5.5.2 SIP-Authentication-Scheme AVP

The SIP-Authentication-Scheme AVP (AVP code TBD) is of type UTF8String and indicates the authentication scheme used in the authentication of SIP messages. Current values are "Basic" and "Digest", defined in [8].

5.5.3 SIP-Authenticate AVP

The SIP-Authenticate AVP (AVP code TBD) is of type UTF8String and contains the data portion of the WWW-Authenticate or Proxy-Authenticate SIP headers if present in a SIP response.

5.5.4 SIP-Authorization AVP

The SIP-Authorization AVP (AVP code TBD) is of type UTF8String and contains the data portion of the Authorization or Proxy-Authorization SIP headers if present in a SIP request.

5.5.5 SIP-Authentication-Info AVP

The SIP-Authentication-Info AVP (AVP Code TBD) is of type OctetString and contains additional authentication information sent by the AAA server in case of Digest authentication. It follows the format defined in RFC2617 for the Authentication-Info Header (sect 3.2.3). The content of this AVP is to be mapped to the SIP Authentication-Info header upon reception by the SIP server.

5.5.6 SIP-Authentication-Context AVP

The SIP-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 SIP-Authentication-Context AVP would be carrying such information.

5.6 SIP-Number-Auth-Items AVP

The SIP-Number-Auth-Items AVP (AVP Code TBD) is of type Unsigned32 and indicates the number of authentication and/or authorization vectors provided by the Diameter server.

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

5.7 SIP-User-Data AVP

The SIP-User-Data AVP (AVP Code TBD) is of type OctetString, and MUST NOT be interpreted by the Diameter protocol. This AVP contains the user profile data required for a SIP server to give service to a user.

5.8 NAS-Session-Key AVP

The NAS-Session-Key AVP is defined in [3].

5.9 NAS-Key-Binding AVP

The NAS-Key-Binding AVP is defined in [3].

5.10 SIP-Deregistration-Reason AVP

The SIP-Deregistration-Reason AVP (AVP Code TBD) is of type Grouped, and indicates the reason for a deregistration operation.

Message format

```
SIP-Deregistration-Reason::= < AVP Header: TBD >
                              { SIP-Reason-Code }
                              [ SIP-Reason-Info ]
                              * [ AVP ]
```

5.10.1 Reason-Code AVP

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

PERMANENT_TERMINATION (0)

NEW_SERVER_ASSIGNED (1)
SERVER_CHANGE (2)
REMOVE_SSP (3)

5.10.2 Reason-Info AVP

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

5.11 Charging-Information AVP

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

AVP format
Charging-Information :: = < AVP Header : TBD >
[Primary-Event-Charging-Function-Name]
[Secondary-Event-Charging-Function-Name]
[Primary-Charging-Collection-Function-Name]
[Secondary-Charging-Collection-Function-Name]
*[AVP]

5.11.1 Primary-Event-Charging-Function-Name AVP

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

5.11.2 Secondary -Event-Charging-Function-Name AVP

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

5.11.3 Primary-Charging-Collection-Function-Name AVP

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

5.11.4 Secondary -Charging-Collection-Function-Name AVP

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

5.12 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. HSP determines this from the Expires 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. HSP determines this from the Expires field in the SIP REGISTER method if it is equal to zero.

REGISTRATION_AND_CAPABILITIES (3)
This value is used in case of initial registration or re-registration and when the HSP explicitly requests SSP capability information from the AAA.

5.13 User-Data-Request-Type AVP

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

COMPLETE_PROFILE (0)
This value is used to request from the AAA the complete user profile corresponding to one or more public identities.

REGISTERED_PROFILE (1)
This value is used to request from the AAA 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 AAA the unregistered part of the user profile corresponding to one or more public identities.

5.14 User-Data-Already-Available AVP

The User-Data-Already-Available AVP (AVP code TBD) is of type Enumerated, and indicates to the HSS whether or not the SSP 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 SSP does not have the data that it needs to serve the user.

USER_DATA_ALREADY_AVAILABLE (1)
The SSP already has the data that it needs to serve the user.

6. Authentication Details

Authenticating a mobile user can occur through various mechanisms (http basic or digest authentication have currently been prescribed), with the actual authentication being performed in either the SIP server or the AAA server. The choice of the server will determine the AVPs to be utilized in the SIP-Auth-Data-Item grouped AVP, as well as a few AVPs in the MAR/MAA.

In the event that the SIP server performs the authentication of a mobile user, the MAR from the SIP server to the AAA server will include the SIP-User-Name and SIP-Public-Identity AVPs as necessary, as well a SIP-Number-Auth-Items AVP to indicate how many authentication vectors (the actual contents of the vector are dependent upon the authentication method) are being requested. In the MAA, the AAA server SHOULD indicate how many SIP-Auth-Data-Item AVPs are present with the Number-Auth-Items AVP, and may be different from the amount requested in the MAR. If multiple SIP-Auth-Data-Item AVPs are present, and their ordering is significant, the Item-Number MUST be included in each grouping. The Authentication-Scheme and SIP- Authenticate AVPs will contain data (typically a challenge of some kind) to be used by the mobile user to authenticate itself. The SIP- Authorization AVP will contain the response which is expected from the user. In order to support some auth methods which combine key distribution with authentication, NAS-Session-Key AVPs may be included in the event they were requested by including "SIP crypto node" as one of the Server-Type AVPs in the MAR.

In the event that the AAA server performs the authentication of a mobile user, the MAR from the SIP server will include a single SIP-Auth-Data-Item AVP. The SIP-Authentication-Scheme and SIP Authorization AVPs will contain the relevant parameters from the SIP message if present, and if necessary, the SIP-Authentication-Context AVP will contain any additional information needed to perform the authentication. If the authentication is successful, the MAA will contain a result code indicating success, and if necessary, the SIP-Auth-Data-Item AVP may be included to carry session keys back to the SIP server. If the authentication is unsuccessful due to missing credentials, the MAA will include an SIP-Auth-Data-Item with the SIP-Authentication-Scheme and SIP-Authenticate AVPs containing data (typically a challenge of some kind) to be used by the mobile user to authenticate itself.

7. IANA Considerations

Command Code values are assigned according to the reference [9].

8 References

[1] Loughney, Camarillo, Authentication, Authorization and Accounting Requirements ", draft-ietf-sipping-aaa- req-00.txt, IETF work in progress, August 2002

[2] Calhoun, Akhtar, Arkko, Guttman, Rubens, Zorn, "Diameter Base Pro¡tocol", draft-ietf-aaa-diameter-15.txt, IETF work in progress, October 2002

[3] Calhoun, Bulley, Rubens, Haag, Zorn, "Diameter NASREQ Application", daft-ietf-aaa-diameter-nasreq-09.txt, IETF work in progress, March 2002

[4] Calhoun, Johansson, Perkins, "Diameter Mobile IPv4 Application," draft-ietf-diameter-mobileip-13.txt, IETF work in progress, October 2002

[5] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Ses¡sion Initiation Protocol". RFC 3261, June 2002

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

[7] IETF RFC 2806: "URLs for Telephone Calls"

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

[9] J. Loughney, "Provisional Diameter Command Codes for 3GPP", draft-loughney-aaa-cc-3gpp-00.txt, IETF work in progress, October 2002

[10] IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels"

9 Authors' Addresses

Carolina Canales Phone: +34 913392680
Ericsson Spain Fax: +34 913392538
Via de los Poblados, 13
28033 Madrid
Spain
E-mail: carolina.canales-valenzuela@ece.ericsson.se

Miguel-Angel Pallares Phone: +34 913394222
Ericsson Spain Fax: +34 913392538
Via de los Poblados, 13

28033 Madrid
Spain

E-mail: miguel-angel.pallares-lopez@ece.ericsson.se

Maria-Carmen Belinchon Phone: +34 913393535
Ericsson Spain Fax: +34 913392906
Via de los Poblados, 13
28033 Madrid
Spain
E-mail: maria.c.belinchon@ericsson.com

Peter J. McCann Phone: +1 630 713 9359
Lucent Technologies Fax: +1 630 713 4982
Rm 2Z-305
263 Shuman Blvd
Naperville, IL 60566-7050
USA
E-Mail: mccap@lucent.com

Jaakko Rajaniemi Phone: +358 50 3391387
Nokia Networks Fax: +358 9 51130163
P.O. Box 301
00045 Nokia Group
Finland
E-mail: jaakko.rajaniemi@nokia.com

10. Full Copyright Statement

FITNESS FOR A PARTICULAR PURPOSE.