Network Working Group
Request for Comments: 4740
Category: Standards Track

M. Garcia-Martin, Ed.
Nokia
M. Belinchon
M. Pallares-Lopez
C. Canales-Valenzuela
Ericsson
K. Tammi
Nokia

November 2006

Diameter Session Initiation Protocol (SIP) Application

Status of This Memo

Copyright Notice

Abstract

This document specifies the Diameter Session Initiation Protocol (SIP) application. This is a Diameter application that allows a Diameter client to request authentication and authorization information. This application is designed to be used in conjunction with SIP and provides a Diameter client co-located with a SIP server, with the ability to request the authentication of users and authorization of SIP resources usage from a Diameter server.

Table of Contents

1. Introduction

This document specifies the Diameter Session Initiation Protocol (SIP) application. This is a Diameter application that allows a Diameter client to request authentication and authorization information to a Diameter server for SIP-based IP multimedia services (see [RFC3261] about SIP). Furthermore, this Diameter SIP application provides the Diameter client with functions that go beyond the typical authorization and authentication, such as the ability to download or receive updated user profiles, or rudimentary routing functions that can assist a SIP server in finding another SIP server allocated to the user.

We assume that the SIP server (such as SIP proxy server, registrar, redirect server, or alike) and the Diameter client are co-located in the same node, so that the SIP server is able to receive and process SIP requests and responses. In turn, the SIP server relies on the Authentication, Authorization, and Accounting (AAA) infrastructure for authenticating the SIP request and authorizing the usage of particular SIP services.

This document provides Diameter procedures to implement certain required functionality when SIP is the protocol chosen to initiate and tear down multimedia sessions or when SIP is used for other non-session-related applications. However, this document does not mandate any particular mapping of SIP procedures to Diameter SIP application procedures, nor does it mandate any particular sequence of events between SIP and Diameter. This document provides useful examples to show the interaction between SIP and the Diameter SIP application in order to achieve the desired functionality.

This application does not require and is not related to other authentication services provided by the Diameter Mobile IPv4 [RFC4004] or the Diameter Network Access Server [RFC4005] applications.

This Diameter SIP application is loosely related to the Diameter credit-control application [RFC4006]. Although both applications are independent, the Diameter SIP application is able to supply the addresses of credit-control servers that will be implementing the Diameter credit-control application [RFC4006].

Section 5 discusses assumptions and configurations assumed by this document.

Section 6 provides the reader with informative descriptions of the Diameter SIP application commands and responses and with some guidance about their linkage with SIP procedures.

Advertisement of this application is specified in Section 7.

Section 8 provides a normative description of all the new Diameter commands defined by this specification.

This application extends the Result-Code Attribute-Value-Pair (AVP) with some new values. Further information is described in Section 10.

This application defines some new AVPs. All these AVPs are described in Section 9.

Some extra information about authentication is provided in Section 11.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] and indicate requirement levels for compliant implementations.

3. Definitions

For the purpose of this document, the following terms and definitions apply:

Node: an addressable device attached to a computer network that implements SIP functionality, Diameter functionality, or a combination of both.

For the purpose of this document, the following terms and definitions given in RFC 3261 [RFC3261] Section 6, apply:

- Address-of-Record (AOR)
- Outbound proxy
- Proxy
- Registrar
- Server (SIP server)
- User Agent (UA)
- User Agent Client (UAC)
- User Agent Server (UAS)

For the purpose of this document, the following terms and definitions given in RFC 3588 [RFC3588] Section 1.3, apply:

- Authorization
- Authentication
- Attribute-Value Pair (AVP)
- Diameter Client
- Diameter Server
- Home Realm
- Redirect Agent
- User

4. Acronyms

AKA: Authentication and Key Agreement
LIR: Location-Info-Request
LIA: Location-Info-Answer
MAR: Multimedia-Auth-Request
MAA: Multimedia-Auth-Answer
PPR: Push-Profile-Request
PPA: Push-Profile-Answer
RTR: Registration-Termination-Request
RTA: Registration-Termination-Answer
SAR: Server-Assignment-Request
SAA: Server-Assignment-Answer
SL: Subscriber Locator
UAR: User-Authorization-Request
UAA: User-Authorization-Answer

5. Applicability Statement

This document assumes a general architecture where a Home Realm is composed of one or more nodes implementing Diameter or SIP functions. Users are issuing SIP requests to access SIP resources. For each particular user, the Home Realm needs to authenticate and authorize the usage of those resources and/or the route to the appropriate node. We assume that the database containing the user-related data is located outside the SIP node that requires authorization. Data belonging to different users may be stored in different nodes in the Home Realm, but we assume that all the data related to a particular user is stored in a single node.

> Note: Central to the architecture is the fact that the user data is stored in a single point in the network. This restriction does not mandate a particular implementation, e.g., it is possible to implement clusters of databases operating in mirror mode to provide redundancy. The property required by this specification is that the user data the Diameter server has access to is stored safely in what is seen, from the external point of view, as a single user database.

This document allows several configurations of the Home Realm. In one configuration, a SIP server (proxy, registrar, etc.) is allocated to a user for the purpose of triggering and executing services. The allocation of the SIP server may be done dynamically, e.g., at the time the user registers in the network. This configuration requires a SIP server, typically located at the edge of the network, that is able to allocate another SIP server for the user and that also supports routing of SIP requests and responses towards that allocated SIP server. Both SIP server nodes implement a Diameter client.

In another configuration, the address of a SIP outbound proxy is configured (by means outside the scope of this specification) into the SIP User Agent. The outbound Diameter client in the SIP outbound proxy node authenticates the user, requests authorization for SIP requests, and performs accounting activities.

6. Overview of Operation

This section provides an informative description of how the Diameter SIP application can be used together with SIP. This section is not intended to mandate any specific usage of the Diameter SIP application nor does it mandate a specific mapping between SIP and Diameter messages. We provide a collection of examples that show how the required AAA functionality can be achieved in conjunction with SIP.

6.1. General Architecture

The Diameter SIP application can be used in a SIP environment where an interface to a AAA infrastructure is required to authenticate and authorize the usage of SIP resources. This application provides support for SIP User Agents and proxies that implement and use HTTP Digest authentication [RFC2617], which is the authentication mechanism mandated by SIP [RFC3261]. The application is extensible and, if need arises, it can be extended to provide support for other authentication mechanisms or extensions to HTTP Digest authentication when they occur.

This application provides limited support for accounting services as follows: the Diameter server is able to provide the addresses of accounting severs to the Diameter client. Figure 1, below, shows a general overview of the integration of the SIP architecture with the AAA architecture.

According to Figure 1, there are one or more SIP User Agents (UAs) that initiate or terminate SIP traffic through one or more SIP servers. Both SIP servers implement a Diameter client that supports the Diameter application described in this specification.

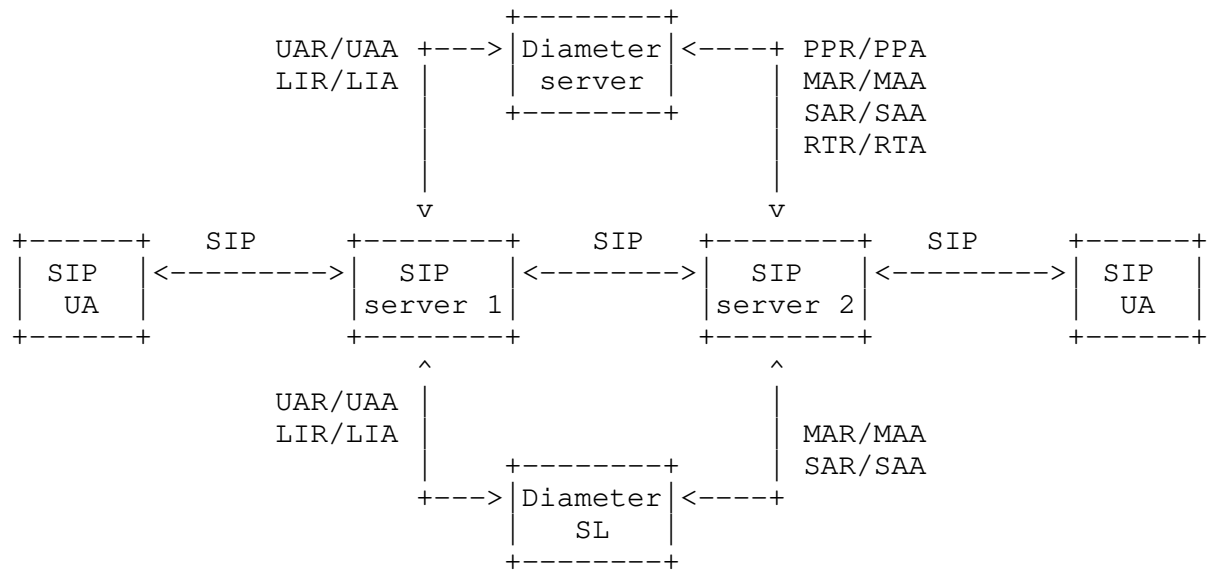

Figure 1: Architecture of the Diameter application for SIP

In Figure 1, it can be seen that SIP server 1 sends different Diameter commands and receives different responses than those sent and received by SIP server 2. This is because SIP server 1 in Figure 1 is located at the edge of a network, and its main task is to locate SIP server 2. SIP server 2 is requesting and receiving authentication and authorization data from the Diameter server and is not located at the edge of the network.

This Diameter application assumes that all the data pertaining to a given user is stored in a single Diameter server. For redundancy purposes, several Diameter servers can be configured in a redundancy fashion, in which case all of them keep the data synchronized and operate externally as a single Diameter server.

With respect to SIP server 1 in Figure 1, the Diameter SIP application provides support for the existence of a farm of these servers, typically configured through one or more DNS records that point to several hosts (this is a typical configuration in common SIP deployments). There is no requirement for these types of servers to keep state related to the Diameter SIP application.

The Diameter SIP application provides support for a feature that allows an administrative domain to provide a collection of SIP servers 2 (as per Figure 1). Once the user registers for the first time, one of these SIP servers is selected and all the SIP requests related to the user are processed by the same SIP server.

The Diameter Subscriber Locator (SL) serves the purpose of locating the Diameter server that contains the user-related data. Its functionality is based on the Diameter redirect mechanism and is further described in Section 6.8.

It should be noted that this document does not mandate any particular SIP/AAA architecture. However, the Diameter SIP application provides the functionality needed to accommodate all the different architectures where SIP and Diameter are used.

The following subsections provide an informative overview of the Diameter SIP application, its commands, and a possible interaction with SIP signaling.

6.2. Diameter Server Authenticates the User

This is the generic mechanism to authenticate users. In this approach, we show an example of an administrative network where the Diameter server is authenticating SIP user requests. This could be the case of a medium-size network where the Diameter server is keeping user records and authenticating SIP requests to perform a certain transaction. We have chosen to show a SIP REGISTER request in the example, but the SIP server could request authentication of any other SIP request.

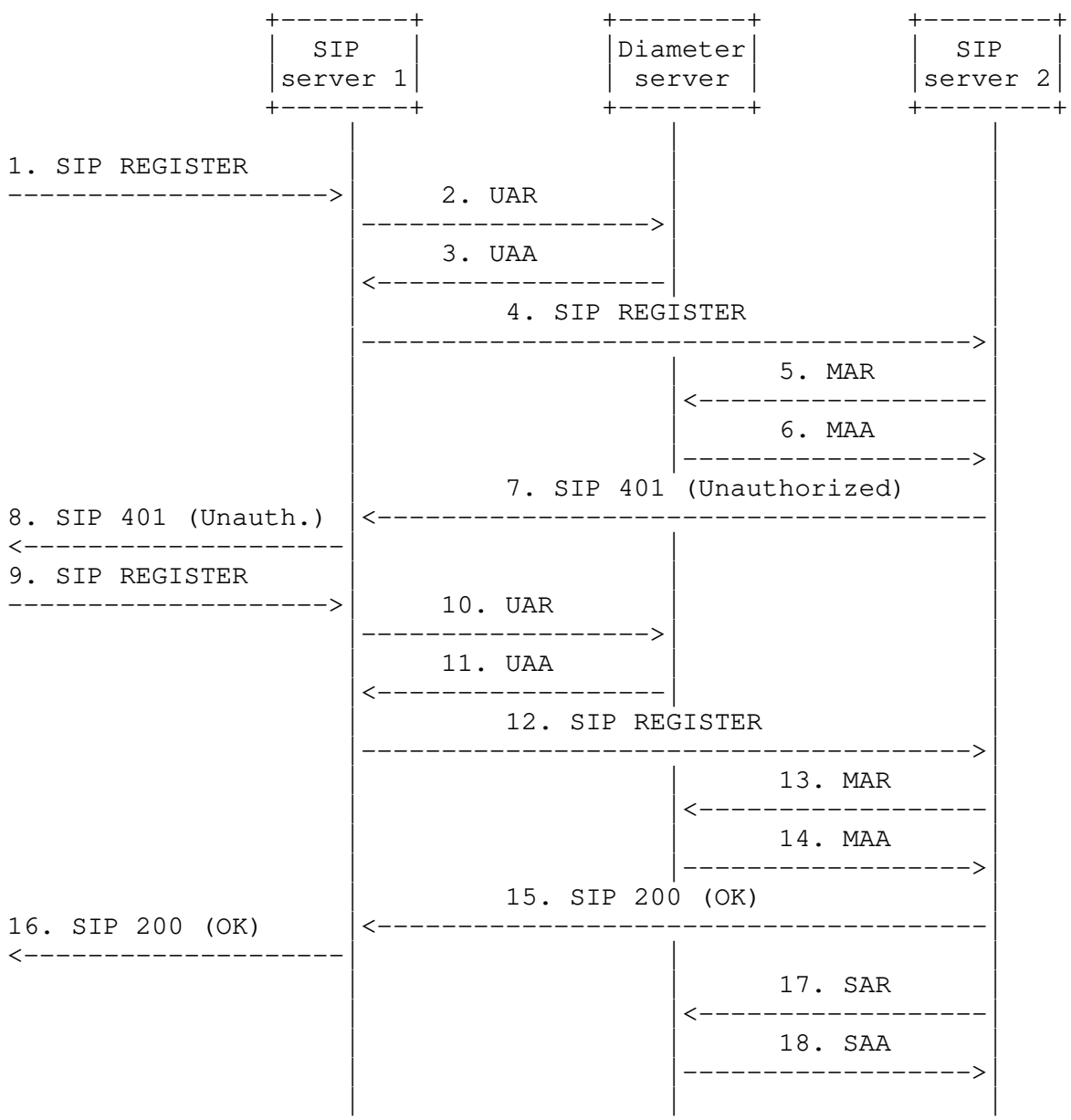

Figure 2: Authentication performed in the Diameter server

According to Figure 2, a SIP User Agent Client (UAC) sends a SIP REGISTER request (step 1) to SIP server 1, which receives the SIP request. In Figure 2, we assume that this SIP server is located at the edge of the administrative home domain. The Diameter client in SIP server 1 contacts its Diameter server by sending a Diameter User-Authorization-Request (UAR) message (step 2) to determine if this user is allowed to receive service, and if so, request the

address of a local SIP server capable of handling this user. The Diameter server answers with a Diameter User-Authorization-Answer (UAA) message (step 3), which indicates a list of capabilities that SIP server 1 may use to select an appropriate SIP server (SIP server 2) and/or a SIP or SIPS URI pointing to SIP server 2.

SIP server 1 forwards the SIP REGISTER request (step 4) to an appropriate SIP server (SIP server 2). Then the Diameter client in SIP server 2 requests user authentication from the Diameter server by sending a Diameter Multimedia-Auth-Request (MAR) message (step 5). This request also serves to make the Diameter server aware of the SIP or SIPS URI of SIP server 2, so as to return subsequent requests for the same user to the same SIP server 2. The Diameter server responds with a Diameter Multimedia-Auth-Answer (MAA) message (step 6) with Result-Code AVP set to the value DIAMETER_MULTI_ROUND_AUTH. The Diameter server also generates a nonce and includes a challenge in the MAA message. SIP server 2 uses that challenge to map into the WWW-Authenticate header in the SIP 401 (Unauthorized) response (step 7), which is sent back to SIP server 1 and then to the SIP UAC (step 8).

SIP server 1 receives a next SIP REGISTER request containing the user credentials (step 9). Note that SIP server 1 does not need to keep a state, and even more, there is no guarantee that the SIP request arrives at the same SIP server 1; there could be a farm of SIP servers 1 operating in redundant configuration. The Diameter client in SIP server 1 contacts the Diameter server by sending a Diameter UAR message (step 10) to determine the SIP server allocated to the user. The Diameter server sends the SIP or SIPS URI of SIP server 2 in a Diameter UAA message (step 11).

Then SIP server 1 forwards the SIP REGISTER request to SIP server 2 (step 12). SIP server 2 extracts the credentials from the SIP REGISTER request. The Diameter client in SIP server 2 sends those credentials in a Diameter MAR message (step 13) to the Diameter server. At this point, the Diameter server is able to authenticate the user, and upon success, returns a Diameter MAA message (step 14) with the AVP Result-Code set to the value DIAMETER_SUCCESS.

Then SIP server 2 generates a SIP 200 (OK) response (step 15), which is forwarded to SIP server 1 and eventually to the SIP UAC (step 16).

If the Diameter client in SIP server 2 is interested in downloading the user profile information or is required to store the address of the SIP server in the Diameter server, then the Diameter client sends a Diameter SAR message (step 17) to the Diameter server. The Diameter server replies with a Diameter SAA message (step 18) that contains the requested user profile information and the

acknowledgement of the SIP server address storage. These actions are needed when the SIP server has to retrieve a user profile used to provide services to the served user, or when the SIP server keeps a state for the user, so the Diameter server needs to store the SIP server's address.

6.3. Delegating Final Authentication Check to the SIP Server

An operator with a large base of installed SIP servers may wish to minimize the number of round-trips between the Diameter client and the Diameter server. We provide support for a mechanism where the Diameter server delegates the final authentication check to the SIP server, thereby saving a round-trip. Section 14.1 discusses the security considerations of this scenario.

It must noted that this scenario is not applicable when the Diameter server is configured to use a session MD5 (MD5-sess) algorithm, because the Diameter server requires the client nonce to compute the H(A1) before sending it to the Diameter client. However, the client nonce might not be available at that time.

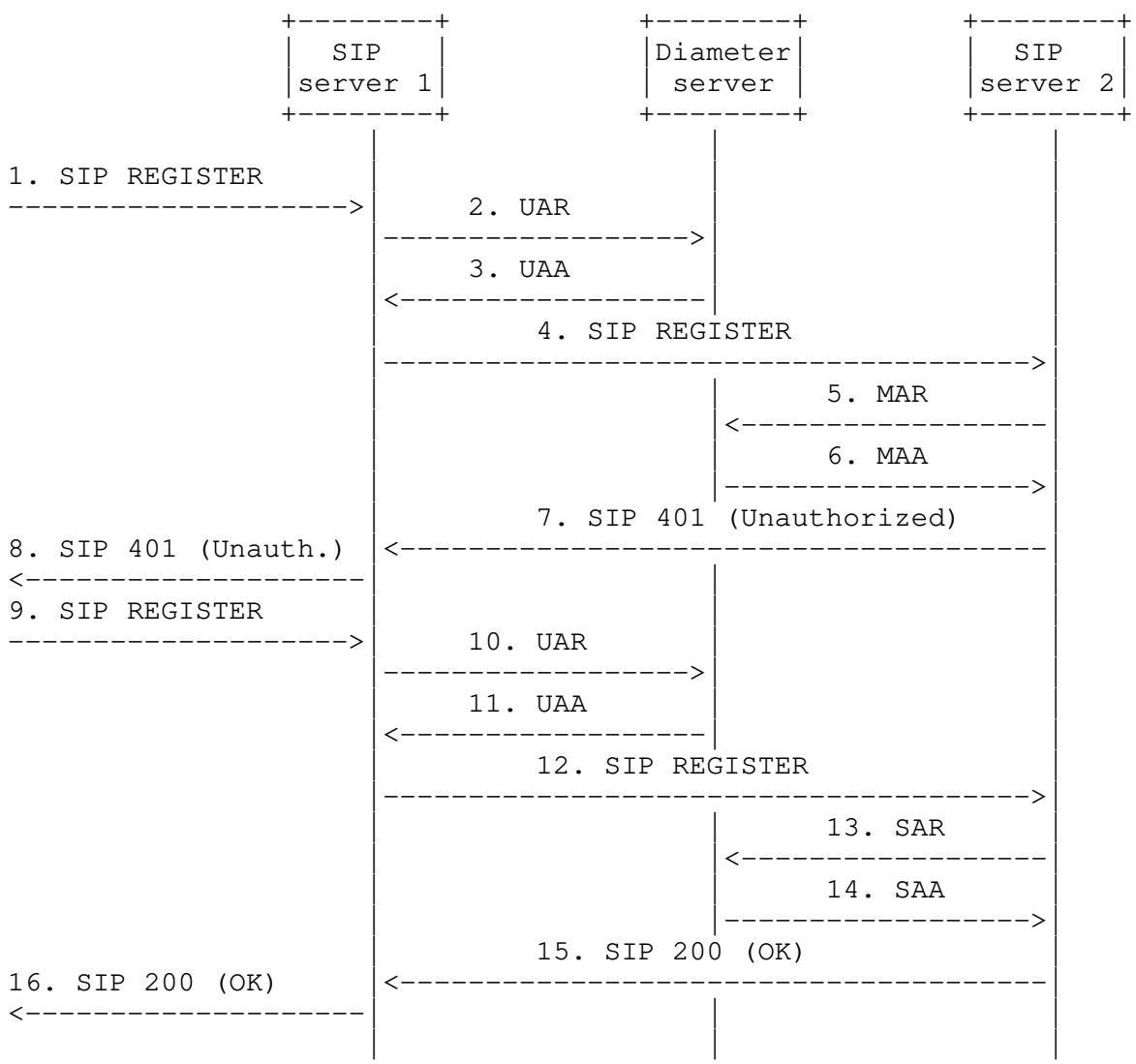

Figure 3: Delegation of authentication to the SIP server

Figure 3 shows an example where a SIP server is dynamically allocated to serve a SIP User Agent with the support of the Diameter server. This may be the case of certain architectures, such as that of the 3rd Generation Partnership Project (3GPP) IP Multimedia Core Network Subsystem.

A first SIP server receives a SIP REGISTER request (step 1) whose target is the home network domain. In Figure 3, we assume that this SIP server is located at the edge of the administrative home domain. The Diameter client in this SIP server requests authorization from the Diameter server to proceed with the registration, by sending a

Diameter User-Authorization-Request (UAR) message (step 2). The message includes, among other Attribute-Value-Pairs (AVPs), the SIP Address-Of-Record (AOR) that is included in the SIP REGISTER request. The Diameter server verifies the SIP AOR and, if it is a valid defined user in the home network, authorizes the registration to proceed. The Diameter server responds with a Diameter User-Authorization-Answer (UAA) message (step 3), which informs the Diameter client/SIP server about the result of the user authorization. In case of a successful authorization, the Diameter UAA message indicates the address of a local SIP server (SIP server 2 in Figure 3) and/or a list of capabilities that SIP server 1 may use to select an appropriate SIP server 2.

When the authorization is successful, SIP server 1 forwards the SIP REGISTER request (step 4) to the appropriate SIP server (SIP server 2). The Diameter client in SIP server 2 requests authentication parameters by sending a Diameter Multimedia-Auth-Request (MAR) message (step 5) to the Diameter server. This request also makes the Diameter server aware of the SIP or SIPS URI of SIP server 2, so as to return subsequent requests of the same user to the same SIP server 2. The Diameter server responds with a Diameter Multimedia-Auth-Answer (MAA) message (step 6), which includes a nonce and all the rest of the parameters necessary for the designated authentication algorithm associated with the user. Among others, the MAA message includes a Digest-HA1 AVP that contains H(A1) (as defined in RFC 2617 [RFC2617]), and that allows the Diameter client to calculate the expected response. Then the Diameter client can compare this expected response with the response to the challenge sent from the SIP UA. The absence of the Digest-HA1 AVP in MAA indicates that authentication and authorization take place in the Diameter server, as per the scenario described in Section 6.2.

SIP server 2 creates a SIP 401 (Unauthorized) SIP response (step 7) based on the challenge included in the MAA message, including the authentication material needed by the SIP User Agent Client (UAC) to include the appropriate credentials. SIP server 1 forwards the SIP response to the SIP UAC (step 8).

The SIP server 1 receives the next SIP REGISTER request containing the user credentials (step 9). Because SIP server 1 does not need to keep a state (and there is no guarantee that the SIP request arrives to the same SIP server 1), the Diameter client in SIP server 1 contacts the Diameter server again by sending a Diameter UAR message (step 10) to determine the SIP server allocated to the user. The Diameter server sends the SIP or SIPS URI of SIP server 2 in a Diameter UAA message (step 11).

SIP server 1 forwards the SIP REGISTER request to SIP server 2 (step 12). SIP server 2 validates the credentials by comparing the response supplied by the SIP UA with the expected response calculated by the SIP server 2 (based on the H(A1) received from the Diameter server).

If the credentials are valid, SIP server 2 sends a Diameter Server-Assignment-Request (SAR) message (step 13) requesting the Diameter server to confirm the completion of the authentication procedure and to confirm the SIP or SIPS URI of the SIP server that is currently serving the user. The Diameter SAR message also serves the purpose of requesting that the Diameter server send the user profile to the SIP server. The Diameter server responds with a Diameter Server-Assignment-Answer (SAA) message (step 14). If the Result-Code AVP value does not inform SIP Server 2 of an error, the SAA message can include zero or more SIP-User-Data AVPs containing the information that SIP server 2 needs in order to provide a service to the user.

SIP server 2 generates a SIP 200 (OK) response (step 15), which is forwarded to SIP server 1 and eventually to the SIP UAC (step 16).

6.4. SIP Server Requests Authentication and Authorization

Figure 4 depicts a typical scenario where a stateless SIP proxy requests authentication information and authorization to a Diameter server, for the purpose of providing SIP routing services to a SIP User Agent. The SIP proxy server may be configured as an outbound SIP proxy, so that all the requests initiated by the SIP UA traverse the SIP proxy.

According to Figure 4, a SIP User Agent sends a SIP request to its outbound SIP proxy server. In this case, the message is a SIP INVITE request (see step 1), but it could be any other SIP request. We assume that this SIP request does not contain any credentials at this time. The outbound SIP proxy server needs to authenticate and authorize the proxy services offered to the user. The Diameter client in the SIP server sends a Multimedia-Auth-Request (MAR) message (step 2). The Diameter server generates a nonce and sends a Multimedia-Auth-Answer (MAA) message (step 3) that includes the nonce and the rest of the data necessary for the SIP server to challenge the user, typically with HTTP Digest Authentication indicated in the MAA message. This data enables the SIP server to create a SIP 407 (Proxy Authentication Required) response (step 4) that contains a challenge. The SIP UA creates a new INVITE request (step 5) that contains the credentials. The Diameter client in the SIP server sends the credentials to the Diameter server in a new Diameter MAR message (step 6). The Diameter server validates the credentials and

authorize the SIP transaction in a Diameter MAA message (step 7). The SIP server forwards the SIP INVITE request to its destination (step 8) as per regular SIP procedures. Eventually, the session setup is confirmed with a SIP 200 (OK) response (step 9) that is forwarded to the SIP UA (step 10). The session setup is complete.

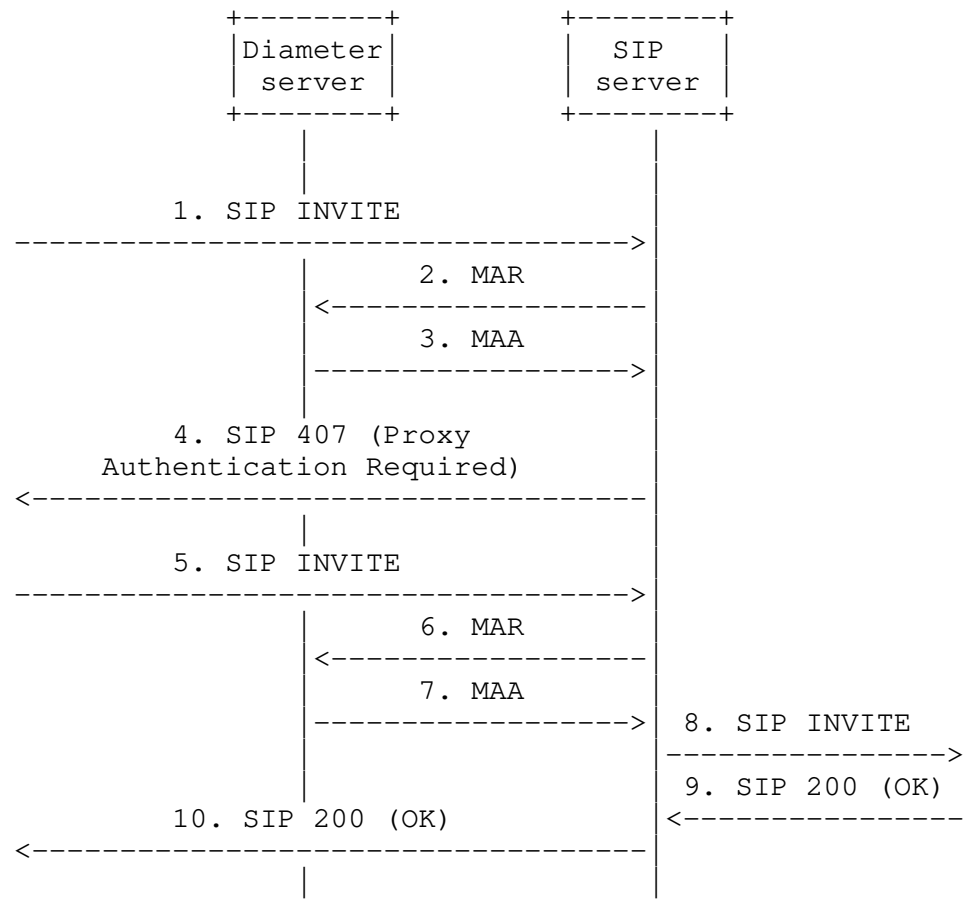

Figure 4: SIP server requests authorization

6.5. Locating the Recipient of the SIP Request

Figure 5 shows the scenario where SIP server 1 may be configured as a SIP edge proxy server, processing SIP traffic at the edge of a network. SIP server 1 receives a SIP INVITE request (step 1). SIP server 1 needs to find the address of SIP server 2, which is serving the recipient of the SIP request. The Diameter client in SIP server 1 sends a Diameter Location-Info-Request (LIR) message (step 2) to the Diameter server. The Diameter server responds with a Diameter Location-Info-Answer (LIA) message (step 3) that contains the SIP or

SIPS URI of SIP server 2. SIP server 1 then forwards the SIP INVITE to SIP server 2 (step 4). SIP server 2 eventually forwards the SIP INVITE to the appropriate UAS (step 5).

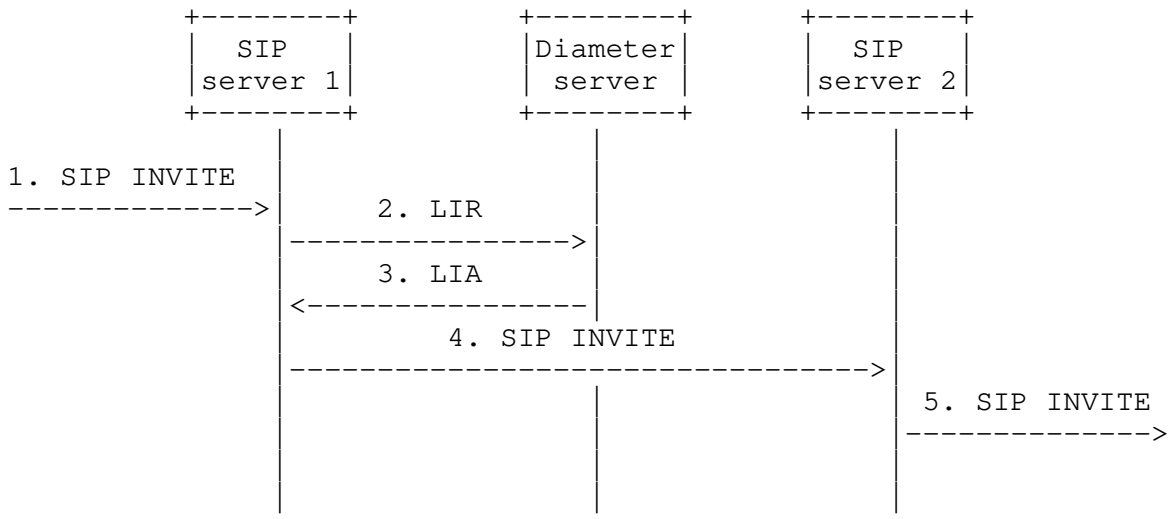

Figure 5: Locating the SIP server of the recipient

Although the example shows the connection between a SIP INVITE request and the Diameter LIR message, any SIP request other than REGISTER (such as SUBSCRIBE, OPTIONS, etc.) would trigger the same Diameter message. (A SIP REGISTER request will trigger a Diameter UAR message, as indicated in Figure 2 and Figure 3.)

The scenario described in this section is also applicable in case an outbound SIP server is not interested in authenticating the user, but is required to locate a further SIP server to route the outbound SIP requests. In this case, the outbound SIP server is mapped to SIP server 1 as shown in Figure 5.

6.6. Update of the User Profile

The Diameter SIP application provides a mechanism for a Diameter server to asynchronously download a user profile to a SIP server whenever there is an update of such user profile. It must be noted that the Diameter server also attaches the user profile to the Diameter Server-Assignment-Answer (SAA) message. This is valid for most of the daily situations; however, the administrator may decide to update or modify the user profile for a particular user, due to, e.g., new services made available to the user. This may involve mechanisms outside the scope of this specification, such as human

intervention, in the Diameter server. In this situation, the Diameter server is able to push the new user profile into the SIP server allocated to the user.

The scenario is illustrated in Figure 6. When the user profile changes, the Diameter server sends a Diameter Push-Profile-Request (PPR) message (step 1) to the Diameter client in the SIP server allocated to that user (SIP server 2 in the examples). The Diameter PPR message contains one or more SIP-User-Data AVPs, a User-Name AVP and zero or more SIP-AOR AVPs. The Diameter client in SIP server 2 acknowledges the Diameter PPR message by sending a Diameter Push-Profile-Answer (PPA) message (step 2) to the Diameter server.

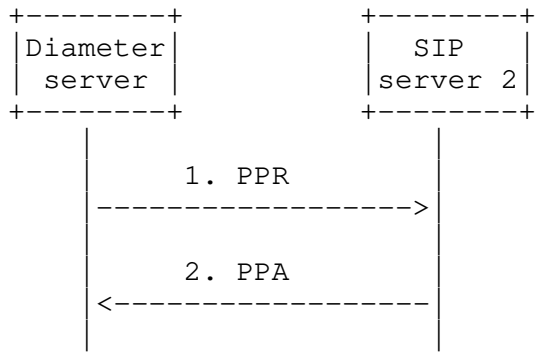

Figure 6: Diameter server pushes an update of the user profile

6.7. SIP Soft State Termination

SIP can create soft states in SIP nodes based on events such as SIP registrations or SIP event subscriptions. These states are periodically refreshed, and cease to exist if they are not refreshed. Additionally, an administrative action can be taken to terminate a SIP soft state, or the SIP UA can explicitly terminate a SIP soft state.

The Diameter base protocol offers a mechanism to create and delete states in Diameter nodes. These states are called Diameter user sessions. The Diameter server decides whether to use a Diameter user session as a mechanism to map to a SIP soft state. If the Diameter server decides to use Diameter user sessions, the termination of a Diameter user session implies the termination of the corresponding SIP soft state (e.g., registration, event subscription), and vice versa. If the Diameter server does not use Diameter user sessions, this Diameter SIP application offers specific commands to manage the SIP soft states. Implementations compliant with this specification MUST support both mechanisms of session management.

We provide support for both Diameter client- and Diameter server-initiated session termination. Depending on whether Diameter sessions are used, termination of a SIP soft state can be achieved by one of the following methods:

- When the Diameter client (SIP proxy) wants to terminate the SIP soft state and Diameter user sessions are not maintained (i.e., the Auth-Session-State AVP has been previously set to NO_STATE_MAINTAINED), the Diameter client MUST send a Server-Assignment-Request (SAR) message with the SIP-Server-Assignment-Type AVP (Section 9.4) set to any of the deregistration values: TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION, TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME, USER_DEREGISTRATION_STORE_SERVER_NAME, ADMINISTRATIVE_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA.

- When the Diameter client (SIP proxy) wants to terminate the SIP soft state and Diameter user sessions are maintained (i.e., the Auth-Session-State AVP has been previously set to STATE_MAINTAINED), the Diameter client MUST send a Session-Termination-Request (STR) message as per regular procedures according to RFC 3588 [RFC3588].

- When the Diameter server wants to terminate the SIP soft state and Diameter user sessions are not maintained (i.e., the Auth-Session-State AVP has been previously set to NO_STATE_MAINTAINED), the Diameter server MUST send a Registration-Termination-Request (RTR) message (see Section 8.9).

- When the Diameter server wants to terminate the SIP soft state and Diameter user sessions are maintained (i.e., the Auth-Session-State AVP has been previously set to STATE_MAINTAINED), the Diameter server MUST send an Abort-Session-Request (ASR) message as per regular procedures according to RFC 3588 [RFC3588].

6.8. Diameter Server Discovery

The basic architecture assumption of this document is that all the data related to a user is stored in a unique Diameter server. Contrary to general opinion, this does not create a single point of failure. It is assumed that Diameter servers are configured in a redundant fashion in an attempt to mitigate the single-point-of-failure problem.

In large networks, where the number of users may be significantly high, there might be a need to scale the number of Diameter servers. All the data associated with a user is still stored in one Diameter

server (typically, operating in a redundant configuration), but the data associated with different users may reside in different Diameter servers.

Although this configuration scales well, it introduces a new problem, namely: given the user's SIP AOR as an input, how to determine which of various Diameter servers is storing the data for that particular SIP AOR. We solve this problem with inspiration from the Diameter redirection mechanism specified in RFC 3588 [RFC3588]. We include in the architecture a new Diameter node that, for the purpose of this document, is known as Diameter Subscriber Locator (SL). The Diameter SL contains a database or routing tables that map SIP AORs to Diameter server URIs. A particular Diameter server URI points to the actual Diameter server that stores all the data related to a particular SIP AOR, and in consequence, to the user who owns the SIP AOR. The Diameter SL acts in a similar way to a Diameter Redirect Agent, dispatching Diameter requests (e.g., providing the redirection URI in the answer). The Diameter SL can redirect all the request pertaining to a user by setting the Redirect-Host-Usage AVP with a value ALL_USER, as specified in RFC 3588 [RFC3588].

The Diameter SL can be replicated in different nodes along the network, for the purpose of building scalability and redundancy. The database or routing tables have to be consistent across all these different Diameter SLs, so that equal Diameter requests will produce equal Diameter answers, no matter which Diameter SL processes the request.

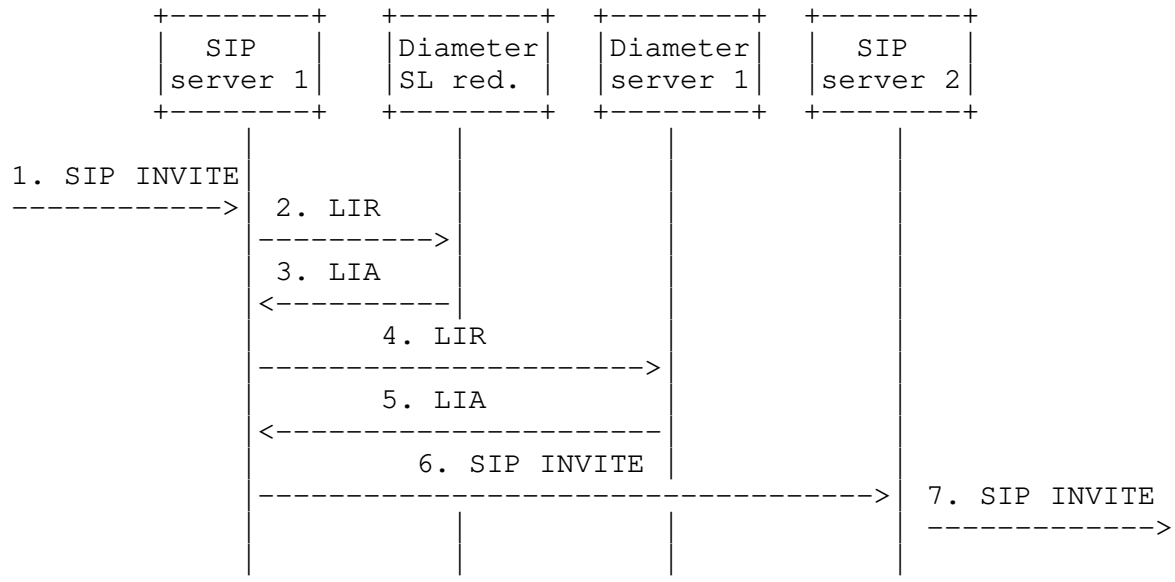

Figure 7: Locating a Diameter server. SL redirecting requests

Figure 7 shows an example of operation of a Diameter SL acting in redirect mode. SIP server 1 receives an INVITE request (step 1) addressed (in the SIP Request-URI) to a user for which the Diameter client in SIP server 1 does not possess routing information. In other words, the Diameter client in SIP server 1 does not know the URI of the Diameter server 1. The Diameter client sends a Diameter LIR message (step 2) to any of the Diameter SLs configured in the network. The address of those SLs is assumed to be pre-provisioned in the Diameter client. The Diameter SL, based on the contents of the SIP-AOR AVP and its own routing tables, determines the Diameter server that stores the information allocated to such user. Then it builds a Diameter LIA message (step 3) that includes a Result-Code AVP set to DIAMETER_REDIRECT_INDICATION and one Redirect-Host AVP, whose value is set to the URI of the Diameter server that stores the information related to such user. Then the Diameter client in SIP server 1 builds a new LIR message (step 4) addressed to the Diameter server received in the Redirect-Host AVP. The rest of the procedure is completed as described in previous sections.

7. Advertising Application Support

Diameter implementations conforming to this specification MUST advertise its support by including an Auth-Application-Id AVP in the Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer (CEA) commands, according to the Diameter base protocol, RFC 3588 [RFC3588]. This Auth-Application-Id AVP MUST be set to the value of this Diameter SIP application (Section 13.1 indicates the actual value allocated by IANA).

8. Diameter SIP Application Command Codes

All the Diameter implementations conforming to this specification MUST implement and support the list of Diameter commands listed in Table 1.

Command Name	Abbr.	Code	Reference
User-Authorization-Request	UAR	283	Section 8.1
User-Authorization-Answer	UAA	283	Section 8.2
Server-Assignment-Request	SAR	284	Section 8.3
Server-Assignment-Answer	SAA	284	Section 8.4
Location-Info-Request	LIR	285	Section 8.5
Location-Info-Answer	LIA	285	Section 8.6
Multimedia-Auth-Request	MAR	286	Section 8.7
Multimedia-Auth-Answer	MAA	286	Section 8.8
Registration-Termination-Request	RTR	287	Section 8.9
Registration-Termination-Answer	RTA	287	Section 8.10
Push-Profile-Request	PPR	288	Section 8.11
Push-Profile-Answer	PPA	288	Section 8.12

Table 1: Defined command codes

Sections defining commands contain the Message Format for that particular command. The Message Formats included in this document are defined as per Section 3.2 of RFC 3588 [RFC3588].

8.1. User-Authorization-Request (UAR) Command

The User-Authorization-Request (UAR) is indicated by the Command-Code set to 283 and the Command Flags' 'R' bit set. The Diameter client in a SIP server sends this command to the Diameter server to request authorization for the SIP User Agent to route a SIP REGISTER request. Because the SIP REGISTER request implicitly carries a permission to bind an AOR to a contact address, the Diameter client uses the Diameter UAR as a first authorization request towards the Diameter server to authorize the registration. For instance, the Diameter server can verify that the AOR is a legitimate user of the realm.

The Diameter client in the SIP server requests authorization for one of the possible values defined in the SIP-User-Authorization-Type AVP (Section 9.10).

The user name used for authentication of the user is conveyed in a User-Name AVP (defined in the Diameter base protocol, RFC 3588 [RFC3588]). The location of the authentication user name in the SIP

REGISTER request varies depending on the authentication mechanism. When the authentication mechanism is HTTP Digest as defined in RFC 2617 [RFC2617], the authentication user name is found in the "username" directive of the SIP Authorization header field value. This Diameter SIP application only provides support for HTTP Digest authentication in SIP; other authentication mechanisms are not currently supported.

The SIP or SIPS URI to be registered is conveyed in the SIP-AOR AVP (Section 9.8). Typically this SIP or SIPS URI is found in the To header field value of the SIP REGISTER request that triggered the Diameter UAR message.

The SIP-Visited-Network-Id AVP indicates the network that is providing SIP services (e.g., SIP proxy functionality or any other kind of services) to the SIP User Agent.

The Message Format of the UAR command is as follows:

```
<UAR> ::= < Diameter Header: 283, REQ, PXY >
          < Session-Id >
          { Auth-Application-Id }
          { Auth-Session-State }
          { Origin-Host }
          { Origin-Realm }
          { Destination-Realm }
          { SIP-AOR }
          [ Destination-Host ]
          [ User-Name ]
          [ SIP-Visited-Network-Id ]
          [ SIP-User-Authorization-Type ]
        * [ Proxy-Info ]
        * [ Route-Record ]
        * [ AVP ]
```

8.2. User-Authorization-Answer (UAA) Command

The User-Authorization-Answer (UAA) is indicated by the Command-Code set to 283 and the Command Flags' 'R' bit cleared. The Diameter server sends this command in response to a previously received Diameter User-Authorization-Request (UAR) command. The Diameter server indicates the result of the requested registration authorization. Additionally, the Diameter server may indicate a collection of SIP capabilities that assists the Diameter client to select a SIP proxy to the AOR under registration.

In addition to the values already defined in RFC 3588 [RFC3588], the Result-Code AVP may contain one of the values defined in Section 10.1.

Whenever the Diameter server fails to process the Diameter UAR message, it MUST stop processing and return the relevant error in the Diameter UAA message. When there is success in the process, the Diameter server MUST set the code to DIAMETER_SUCCESS in the Diameter UAA message.

If the Diameter server requires a User-Name AVP value to process the Diameter UAR request, but the Diameter UAR message did not contain a User-Name AVP value, the Diameter server MUST set the Result-Code AVP value to DIAMETER_USER_NAME_REQUIRED (see Section 10.1.2) and return it in a Diameter UAA message. Upon reception of this Diameter UAA message with the Result-Code AVP value set to DIAMETER_USER_NAME_REQUIRED, the SIP server typically requests authentication by sending a SIP 401 (Unauthorized) or SIP 407 (Proxy Authentication Required) response back to the originator.

When the authorization procedure succeeds, the Diameter server constructs a User-Authorization-Answer (UAA) message that MUST include (1) the address of the SIP server already assigned to the user name, (2) the capabilities needed by the SIP server (Diameter client) to select another SIP server for the user, or (3) a combination of the previous two options.

If the Diameter server is already aware of a SIP server allocated to the user, the Diameter UAA message contains the address of that SIP server.

The Diameter UAA message contains the capabilities required by a SIP server to trigger and execute services. It is required that these capabilities are present in the Diameter UAA message due to the possibility that the Diameter client (in the SIP server) allocates a different SIP server to trigger and execute services for that particular user.

If a User-Name AVP is present in the Diameter UAR message, then the Diameter server MUST verify the existence of the user in the realm, i.e., the User-Name AVP value is a valid user within that realm. If the Diameter server does not recognize the user name received in the User-Name AVP, the Diameter server MUST build a Diameter User-Authorization-Answer (UAA) message and MUST set the Result-Code AVP to DIAMETER_ERROR_USER_UNKNOWN.

If a User-Name AVP is present in the Diameter UAR message, then the Diameter server MUST authorize that User-Name AVP value is able to register the SIP or SIPS URI included in the SIP-AOR AVP. If this authorization fails, the Diameter server must set the Result-Code AVP to DIAMETER_ERROR_IDENTITIES_DONT_MATCH and send it in a Diameter User-Authorization-Answer (UAA) message.

Note: Correlation between User-Name and SIP-AOR AVP values is required in order to avoid registration of a SIP-AOR allocated to another user.

If there is a SIP-Visited-Network-Id AVP in the Diameter UAR message, and the SIP-User-Authorization-Type AVP value received in the Diameter UAR message is set to REGISTRATION or REGISTRATION& CAPABILITIES, then the Diameter server SHOULD verify whether the user is allowed to roam into the network specified in the SIP-Visited-Network-Id AVP in the Diameter UAR message. If the user is not allowed to roam into that network, the Diameter AAA server MUST set the Result-Code AVP value in the Diameter UAA message to DIAMETER_ERROR_ROAMING_NOT_ALLOWED.

If the SIP-User-Authorization-Type AVP value received in the Diameter UAR message is set to REGISTRATION or REGISTRATION&CAPABILITIES, then the Diameter server SHOULD verify whether the SIP-AOR AVP value is authorized to register in the Home Realm. Where the SIP AOR is not authorized to register in the Home Realm, the Diameter server MUST set the Result-Code AVP to DIAMETER_AUTHORIZATION_REJECTED and send it in a Diameter UAA message.

When the SIP-User-Authorization-Type AVP is not present in the Diameter UAR message, or when it is present and its value is set to REGISTRATION, then:

- If the Diameter server is not aware of any previous registration of the user name (including registrations of other SIP AORs allocated to the same user name), then the Diameter server does not know of any SIP server allocated to the user. In this case, the Diameter server MUST set the Result-Code AVP value to DIAMETER_FIRST_REGISTRATION in the Diameter UAA message, and the Diameter server SHOULD include the required SIP server capabilities in the SIP-Server-Capabilities AVP value in the Diameter UAA message. The SIP-Server-Capabilities AVP assists the Diameter client (SIP server) to select an appropriate SIP server for the user, according to the required capabilities.

- In some cases, the Diameter server is aware of a previously assigned SIP server for the same or different SIP AORs allocated to the same user name. In these cases, re-assignment of a new SIP

server may or may not be needed, depending on the capabilities of the SIP server. The Diameter server MUST always include the allocated SIP server URI in the SIP-Server-URI AVP of the UAA message. If the Diameter server does not return the SIP capabilities, the Diameter server MUST set the Result-Code AVP in the Diameter UAA message to DIAMETER_SUBSEQUENT_REGISTRATION. Otherwise (i.e., if the Diameter server includes a SIP-Server-Capabilities AVP), then the Diameter server MUST set the Result-Code AVP in the Diameter UAA message to DIAMETER_SERVER_SELECTION. Then the Diameter client determines, based on the received information, whether it needs to select a new SIP server.

When the SIP-User-Authorization-Type AVP value received in the Diameter UAR message is set to REGISTRATION&CAPABILITIES, then Diameter Server MUST return the list of capabilities in the SIP-Server-Capabilities AVP value of the Diameter UAA message, it MUST set the Result-Code to DIAMETER_SUCCESS, and it MUST NOT return a SIP-Server-URI AVP. The SIP-Server-Capabilities AVP enables the SIP server (Diameter client) to select another appropriate SIP server for invoking and executing services for the user, depending on the required capabilities. The Diameter server MAY leave the list of capabilities empty to indicate that any SIP server can be selected.

When the SIP-User-Authorization-Type AVP value received in the Diameter UAR message is set to DEREGISTRATION, then:

- If the Diameter server is aware of a SIP server assigned to the SIP AOR under deregistration, the Diameter server MUST set the Result-Code AVP to DIAMETER_SUCCESS and MUST set the SIP-Server-URI AVP value to the known SIP server, and return them in the Diameter UAA message.

- If the Diameter server is not aware of a SIP server assigned to the SIP AOR under deregistration, then the Diameter server MUST set the Result-Code AVP in the Diameter UAA message to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED.

The Message Format of the UAA command is as follows:

```
<UAA> ::= < Diameter Header: 283, PXY >
          < Session-Id >
          { Auth-Application-Id }
          { Auth-Session-State }
          { Result-Code }
          { Origin-Host }
          { Origin-Realm }
          [ SIP-Server-URI ]
```

```
                  [ SIP-Server-Capabilities ]
                  [ Authorization-Lifetime ]
                  [ Auth-Grace-Period ]
                  [ Redirect-Host ]
                  [ Redirect-Host-Usage ]
                  [ Redirect-Max-Cache-Time ]
                * [ Proxy-Info ]
                * [ Route-Record ]
                * [ AVP ]
```

8.3. Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR) command is indicated by the Command-Code set to 284 and the Command Flags' 'R' bit set. The Diameter client in a SIP server sends this command to the Diameter server to indicate the completion of the authentication process and to request that the Diameter server store the URI of the SIP server that is currently serving the user. The main functions of the Diameter SAR command are to inform the Diameter server of the URI of the SIP server allocated to the user, and to store or clear it from the Diameter server. Additionally, the Diameter client can request to download the user profile or part of it.

During the registration procedure, a SIP server becomes assigned to the user. The Diameter client in the assigned SIP server MUST include its own URI in the SIP-Server-URI AVP of the Server-Assignment-Request (SAR) Diameter message and send it to the Diameter server. The Diameter server then becomes aware of the allocation of the SIP server to the user name and the server's URI.

The Diameter client in the SIP server MAY send a Diameter SAR message because of other reasons. These reasons are identified in the SIP-Server-Assignment-Type AVP (Section 9.4) value. For instance, a Diameter client in a SIP server may contact the Diameter server to request deregistration of a user, to inform the Diameter server of an authentication failure, or just to download the user profile. For a complete description of all the SIP-Server-Assignment-Type AVP values, see Section 9.4.

Typically the reception of a SIP REGISTER request in a SIP server will trigger the Diameter client in the SIP server to send the Diameter SAR message. However, if a SIP server is receiving other SIP request, such as INVITE, and the SIP server does not have the user profile, the Diameter client in the SIP server may send the Diameter SAR message to the Diameter server in order to download the user profile and make the Diameter server aware of the SIP server assigned to the user.

The user profile is an important piece of information that dictates the behavior of the SIP server when triggering or providing services for the user. Typically the user profile is divided into:

- Services to be rendered to the user when the user is registered and initiates a SIP request.
- Services to be rendered to the user when the user is registered and a SIP request destined to that user arrives to the SIP proxy.
- Services to be rendered to the user when the user is not registered and a SIP request destined to that user arrives to the SIP proxy.

The SIP-Server-Assignment-Type AVP indicates the reason why the Diameter client (SIP server) contacted the Diameter server. If the Diameter client sets the SIP-Server-Assignment-Type AVP value to REGISTRATION, RE_REGISTRATION, UNREGISTERED_USER, NO_ASSIGNMENT, AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT, the Diameter client MUST include exactly one SIP-AOR AVP in the Diameter SAR message.

The SAR message MAY contain zero or more SIP-Supported-User-Data-Type AVPs. Each of them contains a type of user data understood by the SIP server. This allows the Diameter client to provide an indication to the Diameter server of the different format of user data understood by the SIP server. The Diameter server uses this information to select one or more SIP-User-Data AVPs that will be included in the SAA message.

The Message Format of the SAR command is as follows:

```
<SAR> ::= < Diameter Header: 284, REQ, PXY >
          < Session-Id >
          { Auth-Application-Id }
          { Auth-Session-State }
          { Origin-Host }
          { Origin-Realm }
          { Destination-Realm }
          { SIP-Server-Assignment-Type }
          { SIP-User-Data-Already-Available }
          [ Destination-Host ]
          [ User-Name ]
          [ SIP-Server-URI ]
        * [ SIP-Supported-User-Data-Type ]
        * [ SIP-AOR ]
        * [ Proxy-Info ]
        * [ Route-Record ]
        * [ AVP ]
```

8.4. Server-Assignment-Answer (SAA) Command

The Server-Assignment-Answer (SAA) is indicated by the Command-Code set to 284 and the Command Flags' 'R' bit cleared. The Diameter server sends this command in response to a previously received Diameter Server-Assignment-Request (SAR) command. The response may include the user profile or part of it, if requested.

In addition to the values already defined in RFC 3588 [RFC3588], the Result-Code AVP may contain one of the values defined in Section 10.1.

The Result-Code AVP value in the Diameter SAA message may indicate a success or an error in the execution of the Diameter SAR command. If Result-Code AVP value in the Diameter SAA message does not contain an error code, the SAA message MAY include one or more SIP-User-Data AVPs that typically contain the profile of the user, indicating services that the SIP server can provide to that user.

The Diameter server MAY include one or more SIP-Supported-User-Data-Type AVPs, each one identifying a type of user data format supported in the Diameter server. If there is not a common supported user data type between the Diameter client and the Diameter server, the Diameter server SHOULD declare its list of supported user data types by including one or more SIP-Supported-User-Data-Type AVPs in a Diameter SAA message. This indication is merely for debugging reasons, since there is not a fallback mechanism that allows the Diameter client to retrieve the profile in a supported format.

If the Diameter server requires a User-Name AVP value to process the Diameter SAR request, but the Diameter SAR message did not contain a User-Name AVP value, the Diameter server MUST set the Result-Code AVP value to DIAMETER_USER_NAME_REQUIRED (see Section 10.1.2) and return it in a Diameter SAA message. Upon reception of this Diameter SAA message with the Result-Code AVP value set to DIAMETER_USER_NAME_REQUIRED, the SIP server typically requests authentication by generating a SIP 401 (Unauthorized) or SIP 407 (Proxy Authentication Required) response back to the originator.

If the User-Name AVP is included in the Diameter SAR message, upon reception of the Diameter SAR message, the Diameter server MUST verify the existence of the user in the realm, i.e., the User-Name AVP value is a valid user within that realm. If the Diameter server does not recognize the user name received in the User-Name AVP, the Diameter server MUST build a Diameter Server-Assignment-Answer (SAA) message and MUST set the Result-Code AVP to DIAMETER_ERROR_USER_UNKNOWN.

Then the Diameter server MUST authorize that User-Name AVP value is a valid authentication name for the SIP or SIPS URI included in the SIP-AOR AVP of the Diameter SAR message. If this authorization fails, the Diameter server must set the Result-Code AVP to DIAMETER_ERROR_IDENTITIES_DONT_MATCH and send it in a Diameter Server-Assignment-Answer (SAA) message.

After successful execution of the Diameter SAR command, the Diameter server MUST clear the "authentication pending" flag and SHOULD move the temporarily stored SIP server URI to permanent storage.

The actions of the Diameter server upon reception of the Diameter SAR message depend on the value of the SIP-Server-Assignment-Type:

- If the SIP-Server-Assignment-Type AVP value in the Diameter SAR message is set to REGISTRATION or RE_REGISTRATION, the Diameter server SHOULD verify that there is only one SIP-AOR AVP. Otherwise, the Diameter server MUST answer with a Diameter SAA message with the Result-Code AVP value set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and MUST NOT include any SIP-User-Data AVP. If there is only one SIP-AOR AVP and if the SIP-User-Data-Already-Available AVP value is set to USER_DATA_NOT_AVAILABLE, then the Diameter server SHOULD include one or more user profile data with the SIP or SIPS URI (SIP-AOR AVP) and all other SIP identities associated with that AVP in the SIP-User-Data AVP value of the Diameter SAA message. On selecting the type of user data, the Diameter server SHOULD take into account the supported formats at the SIP server (SIP-Supported-User-Data-Type AVP in the SAR message) and the local policy. Additionally, the Diameter server MUST set the Result-Code AVP value to DIAMETER_SUCCESS in the Diameter SAA message. The Diameter server considers the SIP AOR authenticated and registered.

- If the SIP-Server-Assignment-Type AVP value in the Diameter SAR message is set to UNREGISTERED_USER, then the Diameter server MUST store the SIP server address included in the SIP-Server-URI AVP value. The Diameter server will return the SIP server address in Diameter Location-Info-Answer (LIA) messages. If the SIP-User-Data-Already-Available AVP value is set to USER_DATA_NOT_AVAILABLE, then the Diameter server SHOULD include one or more user profile data associated with the SIP or SIPS URI (SIP-AOR AVP) and associated identities in the SIP-User-Data AVP value of the Diameter SAA message. On selecting the type of user data, the Diameter server SHOULD take into account the supported formats at the SIP server (SIP-Supported-User-Data-Type AVP in the SAR message) and the local policy. The Diameter server MUST set the Result-Code AVP value to DIAMETER_SUCCESS. The Diameter

server considers the SIP AOR UNREGISTERED, but with a SIP server allocated to trigger and provide services for unregistered users. Note that in case of UNREGISTERED_USER (SIP-Server-Assignment-Type AVP), the Diameter server MUST verify that there is only one SIP-AOR AVP. Otherwise, the Diameter server MUST answer the Diameter SAR message with a Diameter SAA message, and it MUST set the Result-Code AVP value to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and MUST NOT include any SIP-User-Data AVP.
If the User-Name AVP was not present in the Diameter SAR message and the SIP-AOR is not known for the Diameter server, the Diameter server MUST NOT include a User-Name AVP in the Diameter SAA message and MUST set the Result-Code AVP value to DIAMETER_ERROR_USER_UNKNOWN.

- If the SIP-Server-Assignment-Type AVP value in the Diameter SAR message is set to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA, or ADMINISTRATIVE_DEREGISTRATION, the Diameter server MUST clear the SIP server address associated with all SIP AORs indicated in each of the SIP-AOR AVP values included in the Diameter SAR message. The Diameter server considers all of these SIP AORs as not registered. The Diameter server MUST set the Result-Code AVP value to DIAMETER_SUCCESS in the Diameter SAA message.

- If the SIP-Server-Assignment-Type AVP value in the Diameter SAR message is set to TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME or USER_DEREGISTRATION_STORE_SERVER_NAME, the Diameter server MAY keep the SIP server address associated with the SIP AORs included in the SIP-AOR AVP values of the Diameter SAR message, even though the SIP AORs become unregistered. This feature allows a SIP server to request that the Diameter server remain an assigned SIP server for those SIP AORs (SIP-AOR AVP values) allocated to the same user name, and avoid SIP server assignment. The Diameter server MUST consider all these SIP AORs as not registered. If the Diameter server honors the request of the Diameter client (SIP server) to remain as an allocated SIP server, then the Diameter server MUST keep the SIP server assigned to those SIP AORs allocated to the username and MUST set the Result-Code AVP value to DIAMETER_SUCCESS in the Diameter SAA message. Otherwise, when the Diameter server does not honor the request of the Diameter client (SIP server) to remain as an allocated SIP server, the Diameter server MUST clear the SIP server name assigned to those SIP AORs and it MUST set the Result-Code AVP value to DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED in the Diameter SAA message.

- If the SIP-Server-Assignment-Type AVP value in the Diameter SAR message is set to NO_ASSIGNMENT, the Diameter server SHOULD first verify that the SIP-Server-URI AVP value in the Diameter SAR message is the same URI as the one assigned to the SIP-AOR AVP value. If they differ, then the Diameter server MUST set the Result-Code AVP value to DIAMETER_UNABLE_TO_COMPLY in the Diameter SAA message. Otherwise, if the SIP-User-Data-Already-Available AVP value is set to USER_DATA_NOT_AVAILABLE, then the Diameter server SHOULD include the user profile data with the SIP or SIPS URI (SIP-AOR AVP) and all other SIP identities associated with that AVP in the SIP-User-Data AVP value of the Diameter SAA message. On selecting the type of user data, the Diameter server SHOULD take into account the supported formats at the SIP server (SIP-Supported-User-Data-Type AVP in the SAR message) and the local policy.

- If the SIP-Server-Assignment-Type AVP value in the Diameter SAR message is set to AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT, the Diameter server MUST verify that there is exactly one SIP-AOR AVP in the Diameter SAR message. If the number of occurrences of the SIP-AOR AVP is not exactly one, the Diameter server MUST set the Result-Code AVP value to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES in the Diameter SAA message, and SHOULD not take further actions. If there is exactly one SIP-AOR AVP in the Diameter SAR message, the Diameter server MUST clear the address of the SIP server assigned to the SIP AOR allocated to the user name, and the Diameter server MUST set the Result-Code AVP value to DIAMETER_SUCCESS in the Diameter SAA message. The Diameter server MUST consider the SIP AOR as not registered.

The Message Format of the SAA command is as follows:

```
<SAA> ::= < Diameter Header: 284, PXY >
          < Session-Id >
          { Auth-Application-Id }
          { Result-Code }
          { Auth-Session-State }
          { Origin-Host }
          { Origin-Realm }
        * [ SIP-User-Data ]
          [ SIP-Accounting-Information ]
        * [ SIP-Supported-User-Data-Type ]
          [ User-Name ]
          [ Auth-Grace-Period ]
          [ Authorization-Lifetime ]
          [ Redirect-Host ]
          [ Redirect-Host-Usage ]
```

```
                [ Redirect-Max-Cache-Time ]
              * [ Proxy-Info ]
              * [ Route-Record ]
              * [ AVP ]
```

8.5. Location-Info-Request (LIR) Command

The Location-Info-Request (LIR) is indicated by the Command-Code set to 285 and the Command Flags' 'R' bit set. The Diameter client in a SIP server sends this command to the Diameter server to request routing information, e.g., the URI of the SIP server assigned to the SIP-AOR AVP value allocated to the users.

The Message Format of the LIR command is as follows:

```
    <LIR> ::= < Diameter Header: 285, REQ, PXY >
              < Session-Id >
              { Auth-Application-Id }
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              { Destination-Realm }
              { SIP-AOR }
              [ Destination-Host ]
            * [ Proxy-Info ]
            * [ Route-Record ]
            * [ AVP ]
```

8.6. Location-Info-Answer (LIA) Command

The Location-Info-Answer (LIA) is indicated by the Command-Code set to 285 and the Command Flags' 'R' bit cleared. The Diameter server sends this command in response to a previously received Diameter Location-Info-Request (LIR) command.

In addition to the values already defined in RFC 3588 [RFC3588], the Result-Code AVP may contain one of the values defined in Section 10.1. When the Diameter server finds an error in processing the Diameter LIR message, the Diameter server MUST stop the process of the message and answer with a Diameter LIA message that includes the appropriate error code in the Result-Code AVP value. When there is no error, the Diameter server MUST set the Result-Code AVP value to DIAMETER_SUCCESS in the Diameter LIA message.

One of the errors that the Diameter server may find is that the SIP-AOR AVP value is not a valid user in the realm. In such cases, the Diameter server MUST set the Result-Code AVP value to DIAMETER_ERROR_USER_UNKNOWN and return it in a Diameter LIA message.

If the Diameter server cannot process the Diameter LIR command, e.g., due to a database error, the Diameter server MUST set the Result-Code AVP value to DIAMETER_UNABLE_TO_COMPLY and return it in a Diameter LIA message. The Diameter server MUST NOT include any SIP-Server-URI or SIP-Server-Capabilities AVP in the Diameter LIA message.

The Diameter server may or may not be aware of a SIP server assigned to the SIP-AOR AVP value included in the Diameter LIR message. If the Diameter server is aware of a SIP server allocated to that particular user, the Diameter server MUST include the URI of such SIP server in the SIP-Server-URI AVP and return it in a Diameter LIA message. This is typically the situation when the user is either registered, or unregistered but a SIP server is still assigned to the user.

When the Diameter server is not aware of a SIP server allocated to the user (typically the case when the user unregistered), the Result-Code AVP value in the Diameter LIA message depends on whether the Diameter server is aware that the user has services defined for unregistered users:

- Those users who have services defined for unregistered users may require the allocation of a SIP server to trigger and perhaps execute those services. Therefore, when the Diameter server is not aware of an assigned SIP server, but the user has services defined for unregistered users, the Diameter server MUST set the Result-Code AVP value to DIAMETER_UNREGISTERED_SERVICE and return it in a Diameter LIA message. The Diameter server MAY also include a SIP-Server-Capabilities AVP to facilitate the SIP server (Diameter client) with the selection of an appropriate SIP server with the required capabilities. Absence of the SIP-Server-Capabilities AVP indicates to the SIP server (Diameter client) that any SIP server is suitable to be allocated for the user.

- Those users who do not have service defined for unregistered users do not require further processing. The Diameter server MUST set the Result-Code AVP value to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED and return it to the Diameter client in a Diameter LIA message. The SIP server (Diameter client) may return the appropriate SIP response (e.g., 480 (Temporarily unavailable)) to the original SIP request.

The Message Format of the LIA command is as follows:

```
<LIA> ::= < Diameter Header: 285, PXY >
          < Session-Id >
          { Auth-Application-Id }
          { Result-Code }
```

```
                  { Auth-Session-State }
                  { Origin-Host }
                  { Origin-Realm }
                  [ SIP-Server-URI ]
                  [ SIP-Server-Capabilities ]
                  [ Auth-Grace-Period ]
                  [ Authorization-Lifetime ]
                  [ Redirect-Host ]
                  [ Redirect-Host-Usage ]
                  [ Redirect-Max-Cache-Time ]
                * [ Proxy-Info ]
                * [ Route-Record ]
                * [ AVP ]
```

8.7. Multimedia-Auth-Request (MAR) Command

The Multimedia-Auth-Request (MAR) command is indicated by the Command-Code set to 286 and the Command Flags' 'R' bit set. The Diameter client in a SIP server sends this command to the Diameter server to request that the Diameter server authenticate and authorize a user attempt to use some SIP service (in this context, SIP service can be something as simple as a SIP subscription or using the proxy services for a SIP request).

The MAR command may also register the SIP server's own URI to the Diameter server, so that future LIR/LIA messages can return this URI. If the SIP server is acting as a SIP registrar (see examples in Sections 6.2 and 6.3), its Diameter client MUST include a SIP-Server-URI AVP in the MAR command. In any other cases (see example in Section 6.4), its Diameter client MUST NOT include a SIP-Server-URI AVP in the MAR command.

The SIP-Method AVP MUST include the SIP method name of the SIP request that triggered this Diameter MAR message. The Diameter server can use this AVP to authorize some SIP requests depending on the method.

The Diameter MAR message MUST include a SIP-AOR AVP. The SIP-AOR AVP indicates the target of the SIP request. The value of the AVP is extracted from different places in SIP request, depending on the semantics of the SIP request. For SIP REGISTER messages the SIP-AOR AVP value indicates the intended public user identity under registration, and it is the SIP or SIPS URI populated in the To header field value (addr-spec as per RFC 3261 [RFC3261]) of the SIP REGISTER request. For other types of SIP requests, such as INVITE, SUBSCRIBE, MESSAGE, etc., the SIP-AOR AVP value indicates the intended destination of the request. This is typically populated in the Request-URI of the SIP request. Extracting the SIP-AOR AVP value

from the proper SIP header field is the Diameter client's responsibility. Extensions to SIP (new SIP methods or new semantics) may require the SIP-AOR to be extracted from other parts of the request.

If the SIP request includes some sort of authentication information, the Diameter client MUST include the user name, extracted from the authentication information of the SIP request, in the User-Name AVP value.

The Message Format of the MAR command is as follows:

```
<MAR> ::= < Diameter Header: 286, REQ, PXY >
          < Session-Id >
          { Auth-Application-Id }
          { Auth-Session-State }
          { Origin-Host }
          { Origin-Realm }
          { Destination-Realm }
          { SIP-AOR }
          { SIP-Method }
          [ Destination-Host ]
          [ User-Name ]
          [ SIP-Server-URI ]
          [ SIP-Number-Auth-Items ]
          [ SIP-Auth-Data-Item ]
        * [ Proxy-Info ]
        * [ Route-Record ]
        * [ AVP ]
```

8.8. Multimedia-Auth-Answer (MAA) Command

The Multimedia-Auth-Answer (MAA) is indicated by the Command-Code set to 286 and the Command Flags' 'R' bit cleared. The Diameter server sends this command in response to a previously received Diameter Multimedia-Auth-Request (MAR) command.

In addition to the values already defined in RFC 3588 [RFC3588], the Result-Code AVP may contain one of the values defined in Section 10.1.

If the Diameter server requires a User-Name AVP value to process the Diameter MAR request, but the Diameter MAR message did not contain a User-Name AVP value, the Diameter server MUST set the Result-Code AVP value to DIAMETER_USER_NAME_REQUIRED (see Section 10.1.2) and return it in a Diameter MAA message. The Diameter server MAY include a SIP-Number-Auth-Items AVP and one or more SIP-Auth-Data-Item AVPs with authentication information (e.g., a challenge). Upon reception

of this Diameter MAA message with the Result-Code AVP value set to DIAMETER_USER_NAME_REQUIRED, the SIP server typically requests authentication by generating a SIP 401 (Unauthorized) or SIP 407 (Proxy Authentication Required) response back to the originator.

If the User-Name AVP is present in the Diameter MAR message, the Diameter server MUST verify the existence of the user in the realm, i.e., the User-Name AVP value is a valid user within that realm. If the Diameter server does not recognize the user name received in the User-Name AVP, the Diameter server MUST build a Diameter Multimedia-Auth-Answer (MAA) message and MUST set the Result-Code AVP to DIAMETER_ERROR_USER_UNKNOWN.

If the SIP-Methods AVP value of the Diameter MAR message is set to REGISTER and a User-Name AVP is present, then the Diameter server MUST authorize that User-Name AVP value is able to use the URI included in the SIP-AOR AVP. If this authorization fails, the Diameter server must set the Result-Code AVP to DIAMETER_ERROR_IDENTITIES_DONT_MATCH and send it in a Diameter Multimedia-Auth-Answer (MAA) message.

> Note: Correlation between User-Name and SIP-AOR AVP values is only required for SIP REGISTER request, to prevent a user from registering a SIP-AOR allocated to another user. In other types of SIP requests (e.g., INVITE), the SIP-AOR indicates the intended destination of the request, rather than the originator of it.

The Diameter server MUST verify whether the authentication scheme (SIP-Authentication-Scheme AVP value) indicated in the grouped SIP-Auth-Data-Item AVP is supported or not. If that authentication scheme is not supported, then the Diameter server MUST set the Result-Code AVP to DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED and send it in a Diameter Multimedia-Auth-Answer (MAA) message.

If the SIP-Number-Auth-Items AVP is present in the Diameter MAR message, it indicates the number of authentication data items that the Diameter client is requesting. It is RECOMMENDED that the Diameter server, when building the Diameter MAA message, includes a number of SIP-Auth-Data-Item AVPs that are a subset of the authentication data items requested by the Diameter client in the SIP-Number-Auth-Items AVP value of the Diameter MAR message.

If the SIP-Server-URI AVP is present in the Diameter MAR message, then the Diameter server MUST compare the stored SIP server (assigned to the user) with the SIP-Server-URI AVP value (received in the Diameter MAR message). If they don’t match, the Diameter server MUST temporarily save the newly received SIP server assigned to the user, and MUST set an "authentication pending" flag for the user. If they

match, the Diameter server shall clear the "authentication pending" flag for the user.

In any other situation, if there is a success in processing the Diameter MAR command and the Diameter server stored the SIP-Server-URI, the Diameter server MUST set the Result-Code AVP value to DIAMETER_SUCCESS and return it in a Diameter MAA message.

If there is a success in processing the Diameter MAR command, but the Diameter server does not store the SIP-Server-URI because the AVP was not present in the Diameter MAR command, then the Diameter server MUST set the Result-Code AVP value to either:

1. DIAMETER_SUCCESS_AUTH_SENT_SERVER_NOT_STORED, if the Diameter server is sending authentication credentials to create a challenge.

2. DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED, if the Diameter server successfully authenticated the user and authorized the SIP server to proceed with the SIP request.

Otherwise, the Diameter server MUST set the Result-Code AVP value to DIAMETER_UNABLE_TO_COMPLY, and it MUST NOT include any SIP-Auth-Data-Item AVP.

The Message Format of the MAA command is as follows:

```
    <MAA> ::= < Diameter Header: 286, PXY >
              < Session-Id >
              { Auth-Application-Id }
              { Result-Code }
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              [ User-Name ]
              [ SIP-AOR ]
              [ SIP-Number-Auth-Items ]
            * [ SIP-Auth-Data-Item ]
              [ Authorization-Lifetime ]
              [ Auth-Grace-Period ]
              [ Redirect-Host ]
              [ Redirect-Host-Usage ]
              [ Redirect-Max-Cache-Time ]
            * [ Proxy-Info ]
            * [ Route-Record ]
            * [ AVP ]
```

8.9. Registration-Termination-Request (RTR) Command

The Registration-Termination-Request (RTR) command is indicated by the Command-Code set to 287 and the Command Flags' 'R' bit set. The Diameter server sends this command to the Diameter client in a SIP server to indicate to the SIP server that one or more SIP AORs have to be deregistered. The command allows an operator to administratively cancel the registration of a user from a centralized Diameter server.

The Diameter server has the capability to initiate the deregistration of a user and inform the SIP server by means of the Diameter RTR command. The Diameter server can decide whether only one SIP AOR is going to be deregistered, a list of SIP AORs, or all the SIP AORs allocated to the user.

The absence of a SIP-AOR AVP in the Diameter RTR message indicates that all the SIP AORs allocated to the user identified by the User-Name AVP are being deregistered.

The Diameter server MUST include a SIP-Deregistration-Reason AVP value to indicate the reason for the deregistration.

The Message Format of the RTR command is as follows:

```
<RTR> ::= < Diameter Header: 287, REQ, PXY >
          < Session-Id >
          { Auth-Application-Id }
          { Auth-Session-State }
          { Origin-Host }
          { Origin-Realm }
          { Destination-Host }
          { SIP-Deregistration-Reason }
          [ Destination-Realm ]
          [ User-Name ]
        * [ SIP-AOR ]
        * [ Proxy-Info ]
        * [ Route-Record ]
        * [ AVP ]
```

8.10. Registration-Termination-Answer (RTA) Command

The Registration-Termination-Answer (RTA) is indicated by the Command-Code set to 287 and the Command Flags' 'R' bit cleared. The Diameter client sends this command in response to a previously received Diameter Registration-Termination-Request (RTR) command.

In addition to the values already defined in RFC 3588 [RFC3588], the Result-Code AVP may contain one of the values defined in Section 10.1.

If the SIP server (Diameter client) requires a User-Name AVP value to process the Diameter RTR request, but the Diameter RTR message did not contain a User-Name AVP value, the Diameter client MUST set the Result-Code AVP value to DIAMETER_USER_NAME_REQUIRED (see Section 10.1.2) and return it in a Diameter RTA message.

The SIP server (Diameter client) applies the administrative deregistration to each of the URIs included in each of the SIP-AOR AVP values, or, if there is no SIP-AOR AVP present in the Diameter RTR request, to all the URIs allocated to the User-Name AVP value.

The value of the SIP-Deregistration-Reason AVP in the Diameter RTR command has an effect on the actions performed at the SIP server (Diameter client):

- If the value is set to PERMANENT_TERMINATION, then the user has terminated his/her registration to the realm. If informing the interested parties (e.g., subscribers to the "reg" event [RFC3680]) about the administrative deregistration is supported through SIP procedures, the SIP server (Diameter client) will do so. The Diameter Client in the SIP Server SHOULD NOT request a new user registration. The SIP server clears the registration state of the deregistered AORs.

- If the value is set to NEW_SIP_SERVER_ASSIGNED, the Diameter server informs the SIP server (Diameter client) that a new SIP server has been allocated to the user, due to some reason. The SIP server, if supported through SIP procedures, will inform the interested parties (e.g., subscribers to the "reg" event [RFC3680]) about the administrative deregistration at this SIP server. The Diameter client in the SIP server SHOULD NOT request a new user registration. The SIP server clears the registration state of the deregistered SIP AORs.

- If the value is set to SIP_SERVER_CHANGE, the Diameter server informs the SIP server (Diameter client) that a new SIP server has to be allocated to the user, e.g., due to user's capabilities requiring a new SIP server, or not enough resources in the current SIP server. If informing the interested parties about the administrative deregistration is supported through SIP procedures (e.g., subscriptions to the "reg" event [RFC3680]), the SIP server will do so. The Diameter client in the SIP Server SHOULD NOT request a new user registration. The SIP server clears the registration state of the deregistered SIP AORs.

- If the value is set to REMOVE_SIP_SERVER, the Diameter server informs the SIP server (Diameter client) that the SIP server will no longer be bound in the Diameter server with that user. The SIP server can delete all data related to the user.

The Message Format of the RTA command is as follows:

```
<RTA> ::= < Diameter Header: 287, PXY >
          < Session-Id >
          { Auth-Application-Id }
          { Result-Code }
          { Auth-Session-State }
          { Origin-Host }
          { Origin-Realm }
          [ Authorization-Lifetime ]
          [ Auth-Grace-Period ]
          [ Redirect-Host ]
          [ Redirect-Host-Usage ]
          [ Redirect-Max-Cache-Time ]
        * [ Proxy-Info ]
        * [ Route-Record ]
        * [ AVP ]
```

8.11. Push-Profile-Request (PPR) Command

The Push-Profile-Request (PPR) command is indicated by the Command-Code set to 288 and the Command Flags' 'R' bit set. The Diameter server sends this command to the Diameter client in a SIP server to update either the user profile of an already registered user in that SIP server or the SIP accounting information. This allows an operator to modify the data of a user profile or the accounting information and push it to the SIP server where the user is registered.

Each user has a user profile associated with him/her and other accounting information. The profile or the accounting information may change with time, e.g., due to addition of new services to the user. When the user profile or the accounting information changes, the Diameter server sends a Diameter Push-Profile-Request (PPR) command to the Diameter client in a SIP server, in order to start applying those new services.

A PPR command MAY contain a SIP-Accounting-Information AVP that updates the addresses of the accounting servers. Changes in the addresses of the accounting servers take effect immediately. The Diameter client SHOULD close any existing accounting session with the existing server and start providing accounting information to the newly acquired accounting server.

A PPR command MAY contain zero or more SIP-User-Data AVP values containing the new user profile. On selecting the type of user data, the Diameter server SHOULD take into account the supported formats at the SIP server (SIP-Supported-User-Data-Type AVP sent in a previous SAR message) and the local policy.

The User-Name AVP indicates the user to whom the profile is applicable.

The Message Format of the PPR command is as follows:

```
    <PPR> ::= < Diameter Header: 288, REQ, PXY >
              < Session-Id >
              { Auth-Application-Id }
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              { Destination-Realm }
              { User-Name }
            * [ SIP-User-Data ]
              [ SIP-Accounting-Information ]
              [ Destination-Host ]
              [ Authorization-Lifetime ]
              [ Auth-Grace-Period ]
            * [ Proxy-Info ]
            * [ Route-Record ]
            * [ AVP ]
```

8.12. Push-Profile-Answer (PPA) Command

The Push-Profile-Answer (PPA) is indicated by the Command-Code set to 288 and the Command Flags' 'R' bit cleared. The Diameter client sends this command in response to a previously received Diameter Push-Profile-Request (PPR) command.

In addition to the values already defined in RFC 3588 [RFC3588], the Result-Code AVP may contain one of the values defined in Section 10.1.

If there is no error when processing the received Diameter PPR message, the SIP server (Diameter client) MUST download the received user profile from the SIP-User-Data AVP values in the Diameter PPR message and store it associated with the user specified in the User-Name AVP value.

If the SIP server does not recognize or does not support some of the data transferred in the SIP-User-Data AVP values, the Diameter client in the SIP server MUST return a Diameter PPA message that includes a

Result-Code AVP set to the value DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA.

If the SIP server (Diameter client) receives a Diameter PPR message with a User-Name AVP that is unknown, the Diameter client MUST set the Result-Code AVP value to DIAMETER_ERROR_USER_UNKNOWN and MUST return it to the Diameter server in a Diameter PPA message.

If the SIP server (Diameter client) receives in the SIP-User-Data-Content AVP value (of the grouped SIP-User-Data AVP) more data than it can accept, it MUST set the Result-Code AVP value to DIAMETER_ERROR_TOO_MUCH_DATA and MUST return it to the Diameter server in a Diameter PPA message. The SIP server MUST NOT override the existing user profile with the one received in the PPR message.

If the Diameter server receives the Result-Code AVP value set to DIAMETER_ERROR_TOO_MUCH_DATA in a Diameter PPA message, it SHOULD force a new re-registration of the user by sending to the Diameter client a Diameter Registration-Termination-Request (RTR) with the SIP-Deregistration-Reason AVP value set to SIP_SERVER_CHANGE. This will force a re-registration of the user and will trigger a selection of a new SIP server.

If the Diameter client is not able to honor the command, for any other reason, it MUST set the Result-Code AVP value to DIAMETER_UNABLE_TO_COMPLY and it MUST return it in a Diameter PPA message.

The Message Format of the PPA command is as follows:

```
    <PPA> ::= < Diameter Header: 288, PXY >
              < Session-Id >
              { Auth-Application-Id }
              { Result-Code }
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              [ Redirect-Host ]
              [ Redirect-Host-Usage ]
              [ Redirect-Max-Cache-Time ]
            * [ Proxy-Info ]
            * [ Route-Record ]
            * [ AVP ]
```

9. Diameter SIP Application AVPs

This section defines new AVPs used in this Diameter SIP application. Applications compliant with this specification MUST implement these AVPs.

Table 2 lists the new AVPs defined in this Diameter SIP application. The following abbreviations are used in the Data-Type column:

- DURI: DiameterURI
- E: Enumerated
- G: Grouped
- OS: OctetString
- UTF8S: UTF8String
- U32: Unsigned32

Attribute Name	AVP Code	Reference	Data-Type
SIP-Accounting-Information	368	Section 9.1	G
SIP-Accounting-Server-URI	369	Section 9.1.1	DURI
SIP-Credit-Control-Server-URI	370	Section 9.1.2	DURI
SIP-Server-URI	371	Section 9.2	UTF8S
SIP-Server-Capabilities	372	Section 9.3	G
SIP-Mandatory-Capability	373	Section 9.3.1	U32
SIP-Optional-Capability	374	Section 9.3.2	U32
SIP-Server-Assignment-Type	375	Section 9.4	E
SIP-Auth-Data-Item	376	Section 9.5	G
SIP-Authentication-Scheme	377	Section 9.5.1	E
SIP-Item-Number	378	Section 9.5.2	U32
SIP-Authenticate	379	Section 9.5.3	G
SIP-Authorization	380	Section 9.5.4	G
SIP-Authentication-Info	381	Section 9.5.5	G
SIP-Number-Auth-Items	382	Section 9.6	U32
SIP-Deregistration-Reason	383	Section 9.7	G
SIP-Reason-Code	384	Section 9.7.1	E
SIP-Reason-Info	385	Section 9.7.2	UTF8S
SIP-Visited-Network-Id	386	Section 9.9	UTF8S
SIP-User-Authorization-Type	387	Section 9.10	E
SIP-Supported-User-Data-Type	388	Section 9.11	UTF8S
SIP-User-Data	389	Section 9.12	G
SIP-User-Data-Type	390	Section 9.12.1	UTF8S
SIP-User-Data-Contents	391	Section 9.12.2	OS
SIP-User-Data-Already-Available	392	Section 9.13	E
SIP-Method	393	Section 9.14	UTF8S

Table 2: Defined AVPs

Table 3 expands the table of AVPs included in Section 4.5 of RFC 3588 [RFC3588]. The table indicates the Diameter AVPs defined in this Diameter SIP Application, their possible flag values, and whether the AVP may be encrypted. The acronyms 'M', 'P', and 'V' refer to AVP flags whose semantics are described in RFC 3588 [RFC3588]. The value of the 'Encr' column is also described in RFC 3588 [RFC3588].

Attribute Name	MUST	MAY	SHD NOT	MUST NOT	Encr
SIP-Accounting-Information	M	P		V	N
SIP-Accounting-Server-URI	M	P		V	N
SIP-Credit-Control-Server-URI	M	P		V	N
SIP-Server-URI	M	P		V	N
SIP-Server-Capabilities	M	P		V	N
SIP-Mandatory-Capability	M	P		V	N
SIP-Optional-Capability	M	P		V	N
SIP-Server-Assignment-Type	M	P		V	N
SIP-Auth-Data-Item	M	P		V	N
SIP-Authentication-Scheme	M	P		V	N
SIP-Item-Number	M	P		V	N
SIP-Authenticate	M	P		V	N
SIP-Authorization	M	P		V	N
SIP-Authentication-Info	M	P		V	N
SIP-Number-Auth-Items	M	P		V	N
SIP-Deregistration-Reason	M	P		V	N
SIP-Reason-Code	M	P		V	N
SIP-Reason-Info	M	P		V	N
SIP-Visited-Network-Id	M	P		V	N
SIP-User-Authorization-Type	M	P		V	N
SIP-Supported-User-Data-Type	M	P		V	N
SIP-User-Data	M	P		V	N
SIP-User-Data-Type	M	P		V	N
SIP-User-Data-Contents	M	P		V	N
SIP-User-Data-Already-Available	M	P		V	N
SIP-Method	M	P		V	N

Table 3: Summary of the new AVPs flags

9.1. SIP-Accounting-Information AVP

The SIP-Accounting-Information (AVP Code 368) is of type Grouped, and contains the Diameter addresses of those nodes that are able to collect accounting information.

The SIP-Accounting-Information AVP is defined as follows (per the grouped-avp-def of RFC 3588 [RFC3588]):

```
SIP-Accounting-Information ::= < AVP Header: 368 >
                               * [ SIP-Accounting-Server-URI ]
                               * [ SIP-Credit-Control-Server-URI ]
                               * [ AVP]
```

9.1.1. SIP-Accounting-Server-URI AVP

The SIP-Accounting-Server-URI AVP (AVP Code 369) is of type DiameterURI. This AVP contains the address of a Diameter server that is able to receive SIP-session-related accounting information.

9.1.2. SIP-Credit-Control-Server-URI AVP

The SIP-Credit-Control-Server-URI AVP (AVP Code 370) is of type DiameterURI. This AVP contains the address of a Diameter server that is able to authorize real-time credit control usage. The Diameter Credit-Control Application [RFC4006] may be used for this purpose.

9.2. SIP-Server-URI AVP

The SIP-Server-URI AVP (AVP Code 371) is of type UTF8String. This AVP contains a SIP or SIPS URI (as defined in RFC 3261 [RFC3261]) that identifies a SIP server.

9.3. SIP-Server-Capabilities AVP

The SIP-Server-Capabilities AVP (AVP Code 372) is of type Grouped. The Diameter indicates in this AVP the requirements for a particular SIP capability, so that the Diameter client (SIP server) is able to select another appropriate SIP server to serve the user.

The SIP-Server-Capabilities AVP allows a Diameter client (SIP server) to select another SIP server for triggering or executing services to the user. A user may have enabled some services that require the implementation of certain capabilities in the SIP server that triggers or executes those services. For example, the SIP server that triggers or executes services to this user may need to implement SIP servlets [JSR-000116], Call Processing Language (CPL) [RFC3880], or any other kind of capability. Or perhaps that user belongs to a premium users group that has a certain stringent quality-of-service agreement that requires a fast SIP server. The capabilities required or recommended to a given user are conveyed in the SIP-Server-Capabilities AVP. When it receives them, the Diameter client (SIP server) that does the SIP server selection needs to have the means to find out available SIP servers that meet the required or optional capabilities. Such means are outside the scope of this specification.

Note that the SIP-Server-Capabilities AVP assists the Diameter client (SIP server) to produce a subset of all the available SIP servers to be allocated to the user in the Home Realm; this is the subset that conforms the requirements of capabilities on a per-user basis. Typically this subset will be formed of more than a single SIP

server, so once the subset of those SIP servers is identified, it is possible that several instances of these SIP servers exist, in which case the Diameter client (SIP server) should choose one particular SIP server to execute and trigger services to this user. It is expected that at this point the SIP server (Diameter client) will follow the procedures of RFC 3263 [RFC3263] to allocate one SIP server to the user.

The SIP-Server-Capabilities AVP is defined as follows (per the grouped-avp-def of RFC 3588 [RFC3588]):

```
SIP-Server-Capabilities ::= < AVP Header: 372 >
                            * [ SIP-Mandatory-Capability ]
                            * [ SIP-Optional-Capability ]
                            * [ SIP-Server-URI ]
                            * [ AVP ]
```

9.3.1. SIP-Mandatory-Capability AVP

The SIP-Mandatory-Capability AVP (AVP Code 373) is of type Unsigned32. The value represents a certain capability (or set of capabilities) that have to be fulfilled by the SIP server allocated to the user.

The semantics of the different values are not standardized, as it is a matter of the administrative network to allocate its own semantics within its own network. Each value has to represent a single capability within the administrative network.

9.3.2. SIP-Optional-Capability AVP

The SIP-Optional-Capability AVP (AVP Code 374) is of type Unsigned32. The value represents a certain capability (or set of capabilities) that, optionally, may be fulfilled by the SIP server allocated to the user.

The semantics of the different values are not standardized, as it is a matter of the administrative network to allocate its own semantics within its own network. Each value has to represent a single capability within the administrative network.

9.4. SIP-Server-Assignment-Type AVP

The SIP-Server-Assignment-Type AVP (AVP Code 375) is of type Enumerated and indicates the type of server update being performed in a Diameter Server-Assignment-Request (SAR) operation. The following values are defined:

- NO_ASSIGNMENT (0)
  The Diameter client uses this value to request the user profile of a SIP AOR, without affecting the registration state of that identity.

- REGISTRATION (1)
  First SIP registration of a SIP AOR.

- RE_REGISTRATION (2)
  Subsequent SIP registration of a SIP AOR.

- UNREGISTERED_USER (3)
  The SIP server has received a SIP request (e.g., SIP INVITE) addressed for a SIP AOR that is not registered.

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

- USER_DEREGISTRATION (5)
  The SIP server has received a request to deregister a SIP AOR.

- TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME (6)
  The SIP registration timer of an identity has expired. The SIP server keeps the user data stored and requests the Diameter server to store the SIP server address.

- USER_DEREGISTRATION_STORE_SERVER_NAME (7)
  The SIP server has received a user-initiated deregistration request. The SIP server keeps the user data stored and requests the Diameter server to store the SIP server address.

- ADMINISTRATIVE_DEREGISTRATION (8)
  The SIP server, due to administrative reasons, has deregistered a SIP AOR.

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

- AUTHENTICATION_TIMEOUT (10)
  The authentication timer has expired.

- DEREGISTRATION_TOO_MUCH_DATA (11)
  The SIP server has requested user profile information from the Diameter server and has received a volume of data higher than it can accept.

9.5. SIP-Auth-Data-Item AVP

The SIP-Auth-Data-Item (AVP Code 376) is of type Grouped and contains the authentication and/or authorization information pertaining to a user.

When the Diameter server uses the grouped SIP-Auth-Data-Item AVP to include a SIP-Authenticate AVP, the Diameter server MUST send a maximum of one authentication data item (e.g., in case the SIP request contained several credentials). Section 11 contains a detailed discussion and normative text of the case when a SIP request contains several credentials.

The SIP-Auth-Data-Item AVP is defined as follows (per the grouped-avp-def of RFC 3588 [RFC3588]):

```
SIP-Auth-Data-Item ::= < AVP Header: 376 >
                       { SIP-Authentication-Scheme }
                       [ SIP-Item-Number ]
                       [ SIP-Authenticate ]
                       [ SIP-Authorization ]
                       [ SIP-Authentication-Info ]
                     * [ AVP ]
```

9.5.1. SIP-Authentication-Scheme AVP

The SIP-Authentication-Scheme AVP (AVP Code 377) is of type Enumerated and indicates the authentication scheme used in the authentication of SIP services. RFC 2617 identifies this value as an "auth-scheme" (see Section 1.2 of RFC 2617 [RFC2617]). The only currently defined value is:

- DIGEST (0) to indicate HTTP Digest authentication as specified in RFC 2617 [RFC2617] Section 3.2.1. Derivative work is also considered Digest authentication scheme, as long as the "auth-scheme" is identified as Digest in the SIP headers carrying the HTTP authentication. This includes, e.g., the HTTP Digest authentication using AKA [RFC3310].

Each HTTP Digest directive (parameter) is transported in a corresponding AVP, whose name follows the pattern Digest-*. The Digest-* AVPs are RADIUS attributes imported from the RADIUS Extension for Digest Authentication [RFC4590] namespace, allowing a smooth transition between RADIUS and Diameter applications supporting SIP. The Diameter SIP application goes a step further by grouping the Digest-* AVPs into the SIP-Authenticate, SIP-Authorization, and

SIP-Authentication-Info grouped AVPs that correspond to the SIP WWW-Authenticate/Proxy-Authentication, Authorization/Proxy-Authorization, and Authentication-Info headers fields, respectively.

> Note: Due to the fact that HTTP Digest authentication [RFC2617] is the only mandatory authentication mechanism in SIP, this memo only provides support for HTTP Digest authentication and derivative work such as HTTP Digest authentication using AKA [RFC3310]. Extensions to this memo can register new values and new AVPs to provide support for other authentication schemes or extensions to HTTP Digest authentication.
>
> Note: Although RFC 2617 [RFC2617] defines the Basic and Digest schemes for authenticating HTTP requests, RFC 3261 [RFC3261] only imports HTTP Digest as a mechanism to provide authentication in SIP.

Due to syntactic requirements, HTTP Digest authentication has to escape quote characters in contents of HTTP Digest directives. When translating directives into Digest-* AVPs, the Diameter client or server removes the surrounding quotes where present, as required by the syntax of the Digest-* attributes defined in the "RADIUS Extension for Digest Authentication" [RFC4590].

9.5.2. SIP-Item-Number AVP

The SIP-Item-Number (AVP Code 378) 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 of processing is relevant. The AVP indicates the order in which the Grouped SIP-Auth-Data-Item should be processed. Lower values of the SIP-Item-Number AVP indicate that the whole SIP-Auth-Data-Item SHOULD be processed before other SIP-Auth-Data-Item AVPs that contain higher values in the SIP-Item-Number AVP.

9.5.3. SIP-Authenticate AVP

The SIP-Authenticate AVP (AVP Code 379) is of type Grouped and contains a reconstruction of either the SIP WWW-Authenticate or Proxy-Authentication header fields specified in RFC 2617 [RFC2617] for the HTTP Digest authentication scheme. Additionally, the AVP may include a Digest-HA1 AVP that contains H(A1) (as defined in RFC 2617 [RFC2617]). H(A1) allows the Diameter client to create an expected response and compare it with the Digest response received from the SIP UA.

The SIP-Authenticate AVP is defined as follows (per the grouped-avp-def of RFC 3588 [RFC3588]):

```
SIP-Authenticate ::= < AVP Header: 379 >
                     { Digest-Realm }
                     { Digest-Nonce }
                     [ Digest-Domain ]
                     [ Digest-Opaque ]
                     [ Digest-Stale ]
                     [ Digest-Algorithm ]
                     [ Digest-QoP ]
                     [ Digest-HA1]
                   * [ Digest-Auth-Param ]
                   * [ AVP ]
```

9.5.4. SIP-Authorization AVP

The SIP-Authorization AVP (AVP Code 380) is of type Grouped and contains a reconstruction of either the SIP Authorization or Proxy-Authorization header fields specified in RFC 2617 [RFC2617] for the HTTP Digest authentication scheme.

The SIP-Authorization AVP is defined as follows (per the grouped-avp-def of RFC 3588 [RFC3588]):

```
SIP-Authorization ::= < AVP Header: 380 >
                      { Digest-Username }
                      { Digest-Realm }
                      { Digest-Nonce }
                      { Digest-URI }
                      { Digest-Response }
                      [ Digest-Algorithm ]
                      [ Digest-CNonce ]
                      [ Digest-Opaque ]
                      [ Digest-QoP ]
                      [ Digest-Nonce-Count ]
                      [ Digest-Method]
                      [ Digest-Entity-Body-Hash ]
                    * [ Digest-Auth-Param ]
                    * [ AVP ]
```

9.5.5. SIP-Authentication-Info AVP

The SIP-Authentication-Info AVP (AVP Code 381) is of type Grouped and contains a reconstruction of the SIP Authentication-Info header specified in RFC 2617 [RFC2617] for the HTTP Digest authentication scheme.

The SIP-Authentication-Info AVP is defined as follows (per the grouped-avp-def of RFC 3588 [RFC3588]):

```
SIP-Authentication-Info ::= < AVP Header: 381 >
                            [ Digest-Nextnonce ]
                            [ Digest-QoP ]
                            [ Digest-Response-Auth ]
                            [ Digest-CNonce ]
                            [ Digest-Nonce-Count ]
                          * [ AVP ]
```

Note that, in some cases, the Digest-Response-Auth AVP cannot be calculated at the Diameter server, but has to be calculated at the Diameter client (SIP server). For example, if the value of the quality of protection (qop) parameter in Digest is set to "auth-int", then the response-digest (rspauth parameter value in Digest) is calculated with the hash of the body of the SIP response, which is not available at the Diameter server. In this case, the Diameter client (SIP server) must calculate the response-digest once the body of the SIP response is calculated.

Therefore, a value of "auth-int" in the Digest-QoP AVP of the SIP-Authentication-Info AVP indicates that the Diameter client (SIP server) MUST compute the Digest "rspauth" parameter value at the Diameter client (SIP server).

9.5.6. Digest AVPs

The following AVPs are RADIUS attributes defined in the RADIUS Extension for Digest Authentication [RFC4590] and imported by this specification: Digest-AKA-Auts, Digest-Algorithm, Digest-Auth-Param, Digest-CNonce, Digest-Domain, Digest-Entity-Body-Hash, Digest-HA1, Digest-Method, Digest-Nextnonce, Digest-Nonce, Digest-Nonce-Count, Digest-Opaque, Digest-QoP, Digest-Realm, Digest-Response, Digest-Response-Auth, Digest-URI, Digest-Username, and Digest-Stale.

9.5.6.1. Considerations about Digest-HA1 AVP

The Digest-HA1 AVP contains the value, pre-calculated at the Diameter server, of H(A1) as defined in RFC 2617 [RFC2617]. The Diameter client can use H(A1) to calculate the expected Digest response, according to this challenge. If the SIP UA is in possession of the credentials, the calculated expected response and the response sent from the SIP UA will match. The Diameter server MAY include this AVP to enable and assist the SIP server in authenticating the SIP UA.

This scenario is not applicable when the Diameter server is configured to use a session MD5 (MD5-sess) algorithm, because the

Diameter server requires the client nonce to compute the H(A1) before sending it to the Diameter client, and the client nonce might not be available when the computation of H(A1) is done. Therefore, if the final authentication is delegated to the Diameter client, it is RECOMMENDED to configure the Diameter server to use algorithms different than MD5-sess in HTTP Digest.

It is up to the Diameter server to include a Digest-HA1 AVP. The Diameter server calculates the Digest H(A1) with the username, password, and realm (and nonce and cnonce, if applicable) as inputs, and places the result in the Digest-HA1 AVP value. For more details of the A1 computation, see RFC 2617 [RFC2617] Section 3.2.2.2. The Diameter client can calculate the Digest expected response with H(A1) as input, as described in RFC 2617 [RFC2617] Section 3.2.2.

Section 11 provides further normative details about the usage of the Digest-HA1 AVP.

9.5.6.2. Considerations about Digest-Entity-Body-Hash AVP

The Digest-Entity-Body-Hash AVP contains a hash of the entity body contained in the SIP message. This hash is required by HTTP Digest with quality of protection set to "auth-int". Diameter clients MUST use this AVP to transport the hash of the entity body when HTTP Digest is the authentication mechanism and the Diameter server requires verification of the integrity of the entity body (e.g., qop parameter set to "auth-int").

The clarifications described in Section 22.4 of RFC 3261 [RFC3261] about the hash of empty entity bodies apply to the Digest-Entity-Body-Hash AVP.

9.5.6.3. Considerations about Digest-Auth-Param AVP

The Digest-Auth-Param AVP is the mechanism whereby the Diameter client and Diameter server can exchange possible extension parameters contained in Digest headers that are either not understood by the Diameter client or for which there are no corresponding stand-alone AVPs. Unlike the previously listed Digest-* AVPs, the Digest-Auth-Param contains not only the value, but also the parameter name, since it is unknown to the Diameter client. The Diameter node MUST insert one Digest parameter/value combination per AVP value. If the Digest header contains several unknown parameters, then the Diameter implementation MUST repeat this AVP and each instance MUST contain one different unknown Digest parameter/value combination. This AVP corresponds to the "auth-param" parameter defined in Section 3.2.1 of RFC 2617 [RFC2617].

Example: Assume that the Diameter server wants the SIP server to send a "foo" parameter with the value set to "bar", so that the SIP server sends that combination in a SIP WWW-Authenticate header field. The Diameter server builds a grouped SIP-Authenticate AVP that contains a Digest-Auth-Param whose value is set to foo="bar". Then the SIP server creates the WWW-Authenticate header field with all the digest parameters (received in Digest-* AVPs) and adds the foo="bar" parameter to that header field.

9.6. SIP-Number-Auth-Items AVP

The SIP-Number-Auth-Items AVP (AVP Code 382) is of type Unsigned32 and indicates the number of authentication and/or authorization credentials that the Diameter server included in a Diameter message.

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

9.7. SIP-Deregistration-Reason AVP

The SIP-Deregistration-Reason AVP (AVP Code 383) is of type Grouped and indicates the reason for a deregistration operation.

The SIP-Deregistration-Reason AVP is defined as follows (per the grouped-avp-def of RFC 3588 [RFC3588]):

```
SIP-Deregistration-Reason ::= < AVP Header: 383 >
                              { SIP-Reason-Code }
                              [ SIP-Reason-Info ]
                            * [ AVP ]
```

9.7.1. SIP-Reason-Code AVP

The SIP-Reason-Code AVP (AVP Code 384) is of type Enumerated and defines the reason for the network initiated deregistration. The following values are defined:

- PERMANENT_TERMINATION (0)
- NEW_SIP_SERVER_ASSIGNED (1)
- SIP_SERVER_CHANGE (2)
- REMOVE_SIP_SERVER (3)

9.7.2. SIP-Reason-Info AVP

The SIP-Reason-Info AVP (AVP Code 385) is of type UTF8String and contains textual information that can be rendered to the user, about the reason for a deregistration.

9.8. SIP-AOR AVP

The SIP-AOR AVP is a RADIUS attribute imported from the RADIUS Extension for Digest Authentication [RFC4590] namespace, allowing a smooth transition between RADIUS and Diameter applications supporting SIP. The SIP-AOR AVP carries the URI of the intended user related to the SIP request (whose location in SIP may vary depending on the actual SIP request and whether the SIP server is acting on Diameter due to a SIP-originated or terminating requests).

The Diameter client (SIP server) uses the value found in a SIP Request-URI or a header field value of the SIP request to construct the SIP-AOR AVP. The selection of a Request-URI or a particular header field to create the value of the SIP-AOR AVP depends on the semantics of the SIP message and whether the SIP server is acting for originating or terminating requests. For instance, when the SIP server receives an INVITE request addressed to the served user (e.g., the SIP server is receiving a terminating SIP request), it maps the SIP Request-URI of the SIP request to this AVP. However, when the SIP server receives an INVITE request originated by the served user, it can map either the P-Asserted-Identity or the From header field values to this AVP. If the SIP server is acting as a SIP registrar, then it maps the To header field of the REGISTER request to the SIP-AOR AVP.

9.9. SIP-Visited-Network-Id AVP

The SIP-Visited-Network-Id AVP (AVP Code 386) is of type UTF8String. This AVP contains an identifier that helps the home network identify the visited network (e.g., the visited network domain name), in order to authorize roaming to that visited network.

9.10. SIP-User-Authorization-Type AVP

The SIP-User-Authorization-Type AVP (AVP Code 387) is of type Enumerated and indicates the type of user authorization being performed in a User Authorization operation, i.e., the Diameter User-Authorization-Request (UAR) command. The following values are defined:

- REGISTRATION (0)
  This value is used for initial registration or re-registration. This is the default value.

- DEREGISTRATION (1)
  This value is used for deregistration.

- REGISTRATION_AND_CAPABILITIES (2)
  This value is used for initial registration or re-registration when the SIP server explicitly requests the Diameter server to get capability information. This capability information helps the SIP server to allocate another SIP server to serve the user.

9.11. SIP-Supported-User-Data-Type AVP

The SIP-Supported-User-Data-Type AVP (AVP Code 388) is of type UTF8String and contains a string that identifies the type of supported user data (user profile, see SIP-User-Data AVP (Section 9.12)) supported in the node. The AVP can be repeated, if the SIP server supports several user data types. In case of repetition, the Diameter client should order the different instances of this AVP according to its preferences.

When the Diameter client inserts this AVP in a SAR message, it allows the Diameter client to provide an indication to the Diameter server of the types of user data supported by the SIP server. The Diameter server, upon inspection of these AVPs, will return a suitable SIP-User-Data AVP (Section 9.12) of the type indicated in the SIP-User-Data-Type AVP (Section 9.12.1).

9.12. SIP-User-Data AVP

The SIP-User-Data AVP (AVP Code 389) is of type Grouped. This AVP allows the Diameter server to transport user-specific data, such as a user profile, to the SIP server (in the Diameter client). The Diameter server selects a type of user data that is understood by the SIP server in the Diameter client, and has been indicated in a SIP-Supported-User-Data-Type AVP. In case the Diameter client indicated support for several types of user data, the Diameter server SHOULD choose the first type supported by the client.

The SIP-User-Data grouped AVP contains a SIP-User-Data-Type AVP that indicates the type of user data included in the SIP-User-Data-Contents-AVP.

The SIP-User-Data AVP is defined as follows (per the grouped-avp-def of RFC 3588 [RFC3588]):

```
SIP-User-Data ::= < AVP Header: 389 >
                  { SIP-User-Data-Type }
                  { SIP-User-Data-Contents }
                * [ AVP ]
```

9.12.1. SIP-User-Data-Type AVP

The SIP-User-Data AVP (AVP Code 390) is of type UTF8String and contains a string that identifies the type of user data included in the SIP-User-Data AVP (Section 9.12).

This document does not specify a convention to characterize the type of user data contained in the SIP-User-Data AVP (Section 9.12). It is believed that in most cases this feature will be used in environments controlled by a network administrator who can configure both the client and server to assign the same value type at the client and server. It is also RECOMMENDED that organizations developing their own profile of SIP-User-Data AVP (Section 9.12) allocate a type based on their canonical DNS name. For instance, organization "example.com" can define several types of SIP-User-Data and allocate the types "type1.dsa.example.com", "type2.dsa.example.com", and so on. This convention will avoid a clash in the allocation of types of SIP-User-Data AVP (Section 9.12).

9.12.2. SIP-User-Data-Contents AVP

The SIP-User-Data-Contents AVP (AVP Code 391) is of type OctetString. The Diameter peers do not need to understand the value of this AVP.

The AVP contains the user profile data required for a SIP server to give service to the user.

9.13. SIP-User-Data-Already-Available AVP

The SIP-User-Data-Already-Available AVP (AVP Code 392) is of type Enumerated and gives an indication to the Diameter server about whether the Diameter client (SIP server) already received the portion of the user profile needed in order to serve the user. The following values are defined:

- USER_DATA_NOT_AVAILABLE (0)
  The Diameter client (SIP server) does not have the data that it needs to serve the user.

- USER_DATA_ALREADY_AVAILABLE (1)
  The Diameter client (SIP server) already has received the data that it needs to serve the user.

9.14. SIP-Method AVP

The SIP-Method-AVP (AVP Code 393) is of type UTF8String and contains the method of the SIP request that triggered the Diameter message. The Diameter server MUST use this AVP solely for authorization of SIP requests, and MUST NOT use it to compute the Digest authentication. To compute the Digest authentication, the Diameter server MUST use the Digest-Method AVP instead.

10. New Values for Existing AVPs

This section defines new values that the Diameter SIP application extends to already existing AVPs.

10.1. Extension to the Result-Code AVP Values

The Result-Code AVP is already defined in RFC 3588 [RFC3588]. In addition to the values already defined in RFC 3588 [RFC3588], the Diameter SIP application defines the following new Result-Code AVP values:

10.1.1. Success Result-Code AVP Values

A Diameter peer uses Result-Code AVP values that fall into the success category to inform the remote peer that a request has been successfully completed.

- DIAMETER_FIRST_REGISTRATION 2003
  The user was not previously registered. The Diameter server has now authorized the registration.

- DIAMETER_SUBSEQUENT_REGISTRATION 2004
  The user is already registered. The Diameter server has now authorized the re-registration.

- DIAMETER_UNREGISTERED_SERVICE 2005
  The user is not currently registered, but the requested service can still be granted to the user.

- DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED 2006
  The request operation was successfully processed. The Diameter server does not keep a record of the SIP server address assigned to the user.

- DIAMETER_SERVER_SELECTION 2007
  The Diameter server has authorized the registration. The user has already been assigned a SIP server, but it may be necessary to select a new SIP server for the user.

- DIAMETER_SUCCESS_AUTH_SENT_SERVER_NOT_STORED 2008
  The requested operation was successfully executed. The Diameter server is sending a number of authentication credentials in the answer message. The Diameter server does not keep a record of the SIP server.

10.1.2. Transient Failures Result-Code AVP Values

A Diameter peer uses a Result-Code AVP value that falls in the transient failures category to inform the remote peer that a request could not be satisfied at the time it was received, but it MAY be satisfied by the Diameter peer in the future.

- DIAMETER_USER_NAME_REQUIRED 4013
  The Diameter request did not contain a User-Name AVP, which is required to complete the transaction. The Diameter peer MAY include a User-Name AVP and attempt the request again.

10.1.3. Permanent Failures Result-Code AVP Values

A Diameter peer uses a Result-Code AVP value that falls into the permanent failure category to inform the remote peer that the request failed and should not be attempted again.

- DIAMETER_ERROR_USER_UNKNOWN 5032
  The SIP-AOR AVP value does not belong to a known user in this realm.

- DIAMETER_ERROR_IDENTITIES_DONT_MATCH 5033
  The value in one of the SIP-AOR AVPs is not allocated to the user specified in the User-Name AVP.

- DIAMETER_ERROR_IDENTITY_NOT_REGISTERED 5034
  A query for location information is received for a SIP AOR that has not been registered before. The user to which this identity belongs cannot be given service in this situation.

- DIAMETER_ERROR_ROAMING_NOT_ALLOWED 5035
  The user is not allowed to roam to the visited network.

- DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED 5036
  The identity being registered has already been assigned a server and the registration status does not allow that it is overwritten.

- DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED 5037
  The authentication scheme indicated in an authentication request is not supported.

- DIAMETER_ERROR_IN_ASSIGNMENT_TYPE 5038
  The SIP server address sent in the SIP-Server-URI AVP value of the Diameter Server-Assignment-Request (SAR) command is the same SIP server address that is currently assigned to the user name, but the SIP-Server-Assignment-Type AVP is not allowed. For example, the user is registered and the Server-Assignment-Request indicates the assignment for an unregistered user.

- DIAMETER_ERROR_TOO_MUCH_DATA 5039
  The Diameter peer in the SIP server receives more data than it can accept. The SIP server cannot overwrite the already stored data.

- DIAMETER_ERROR_NOT SUPPORTED_USER_DATA 5040
  The SIP server informs the Diameter server that the received subscription data contained information that was not recognized or supported.

11. Authentication Details

Authenticating a user can occur through various mechanisms. Currently HTTP Digest authentication is supported. The actual authentication is performed in either the SIP server or the Diameter server.

If the Diameter server wants to assure that authentication will take place in the Diameter server (as opposed to a delegated authentication taking place in the SIP server), it MUST NOT include a Digest-HA1 AVP (part of the grouped SIP-Authenticate AVP, which in turn is part of the SIP-Auth-Data-Item AVP) in a MAA message. The Diameter server MAY include a pre-calculated Digest-HA1 AVP in the MAA message if it wants to delegate authentication of the user to the SIP server.

Note that on systems where the SIP User Agent is using HTTP Digest authentication [RFC2617] inside of Transport Layer Security (TLS) [RFC4346], where only the SIP proxy server has a certificate, delegating authentication to the SIP server (by making Digest-HA1 available to the SIP server) might reduce the load on the Diameter server.

When requesting authentication, the Diameter client indicates in the SIP-Number-Auth-Items AVP value of a Diameter MAR message how many authentication credentials are being requested. In the Diameter MAA message, the Diameter server MAY include more than one SIP-Auth-Data-Item AVP, but it is only useful for the Diameter client if the Digest-QoP AVP was set to 'auth-int' (in the MAR message), and if future authentications will have the same realm. When including more than one SIP-Auth-Data-Item AVP, the Diameter server SHOULD

indicate how many instances of SIP-Auth-Data-Item AVPs are present with the SIP-Number-Auth-Items AVP. This number may be different from the one requested in the Diameter MAR message. If multiple SIP-Auth-Data-Item AVPs are present, and their ordering is significant, the Diameter server MUST include a SIP-Item-Number AVP in each grouping to indicate the order. The SIP-Authentication-Scheme AVP indicates "Digest" and the SIP-Authenticate AVP contains data (typically a challenge of some kind) that the user can use for her authentication. The grouped SIP-Authorization AVP contains the AVPs that conform to the response expected from the user.

If the Diameter server performs the authentication of the user, the Diameter MAR message that the Diameter client sends to the Diameter server MUST include all the authentication credentials supplied by the SIP UA (there might be more than one credential, e.g., different realms, authentication of proxies, etc.). Each credential is inserted in a grouped SIP-Authorization AVP (part of the grouped SIP-Auth-Data-Item AVP). The Diameter client MUST insert a SIP-Number-Auth-Items AVP with the value set to the number of credentials enclosed. If necessary, the Digest-Entity-Body-Hash AVP will contain a hash of the body, needed to perform the authentication. If the authentication is successful, the Diameter MAA message will contain a Result-Code AVP indicating success, and if necessary, the Diameter server MAY include one or more SIP-Auth-Data-Item AVPs to provide further authentication credentials to the SIP server. If the authentication is unsuccessful due to missing credentials, the Diameter MAA message will include a SIP-Auth-Data-Item AVP with the SIP-Authentication-Scheme and SIP-Authenticate AVPs containing data (typically a challenge of some kind) that the user can use to authenticate itself.

There are situations where a SIP request traverses several proxies, and each of the proxies requests to authenticate the SIP UA. In this situation, it is a valid scenario that a SIP request received at a SIP server contains several sets of credentials. The 'realm' directive in HTTP is the key that the Diameter client can use to determine which credential is applicable. Also, none of the realms may be of interest to the Diameter client, in which case the Diameter client MUST consider that no credentials (of interest) were sent. In any case, a Diameter client MUST send zero or exactly one credential to the Diameter server. The Diameter client MUST choose the credential based on the 'realm' directive in the Authorization/Proxy-Authorization header field, and it MUST match the realm of the Diameter client.

It must be noted that nonces are always generated in the Diameter server.

12. Migration from RADIUS

RADIUS offers support for HTTP Digest authentication in the RADIUS Extension for Digest Authentication [RFC4590]. A number of AVPs (the Digest-* AVPs) of this Diameter SIP application are imported from the RADIUS attributes namespace, thus making the migration from RADIUS to Diameter smooth.

Note that the RADIUS Extension for Digest Authentication [RFC4590] provides a more limited scope than this Diameter SIP application. Specifically, the RADIUS extension for Digest Authentication merely provides support for HTTP Digest authentication, whereas the Diameter SIP application provides support for user location, profile downloading and update, etc.

The following sections discuss several configurations in which a gateway translates RADIUS to Diameter and vice versa.

12.1. Gateway from RADIUS Client to Diameter Server

The gateway maps Access-Request messages to MAR request. If a RADIUS Access-Request message contains at least one Digest-* attribute, the gateway maps all Digest-* attributes to the AVPs of a Diameter SIP-Authorization AVP, constructs a MAR message, and sends it to the Diameter server. If the RADIUS Access-Request message does not contain any Digest-* attribute, then the RADIUS client does not want to apply HTTP Digest authentication, in which case, actions at the gateway are outside the scope of this document.

The Diameter server responds with a MAA message. If the MAA message contains a Result-Code AVP set to the value DIAMETER_MULTI_ROUND_AUTH and contains challenge parameters in a SIP-Authenticate AVP, then the gateway translates the AVPs of SIP-Authenticate AVP and puts the resulting RADIUS attributes into an Access-Challenge message. It sends the Access-Challenge message to the RADIUS client.

If the MAA message contains a SIP-Authentication-Info and a Digest-Response AVP, the gateway converts these AVPs to the corresponding RADIUS attributes and constructs a RADIUS message. If the Result-Code AVP is DIAMETER_SUCCESS, an Access-Accept is sent. In all other cases, an Access-Reject is sent.

12.2. Gateway from Diameter Client to RADIUS Server

The Diameter client sends a Diameter MAR message to the gateway. If the MAR message does not contain SIP-Auth-Data-Item AVPs, the gateway constructs an Access-Request message and maps the SIP-AOR and SIP-Method AVPs to RADIUS attributes. The gateway sends the

Access-Request message to the RADIUS server, which will respond with an Access-Challenge. The gateway creates a MAA message with a Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH and maps the Digest-* attributes to Diameter AVPs in a SIP-Authenticate AVP. The gateway sends the resulting MAA to the Diameter client, which will respond with a new MAR.

The gateway checks the SIP-Auth-Data-Item AVPs of this MAR for an AVP where the Digest-Realm AVP matches the locally configured realm value. It takes the AVPs from this SIP-Auth-Data-Item AVP, converts them into the corresponding RADIUS attributes and constructs a RADIUS Access-Request message. The gateway sends the Access-Request message to the RADIUS server. If the RADIUS server responds with an Access-Accept message, the gateway converts the RADIUS attributes to Diameter AVPs, constructs a MAA message with a Result-Code AVP set to DIAMETER_SUCCESS and sends this message to the Diameter client. If the RADIUS server responds with an Access-Reject message, the gateway converts the RADIUS attributes to Diameter AVPs, constructs a MAA message with a Result-Code AVP set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH, and sends this message to the Diameter client.

12.3. Known Limitations

As mentioned earlier, there is not a 100% match between the Diameter SIP application and the RADIUS Extension for Digest Authentication [RFC4590]. In particular, the RADIUS Extension for Digest Authentication [RFC4590] does not offer equivalent functionality to the Diameter UAR/UAA, SAR/SAA, LIR/LIA, RTR/RTA, and PPR/PPA messages defined by this specification.

13. IANA Considerations

This document serves as IANA registration request for a number of items that should be registered in the AAA parameters registry.

13.1. Application Identifier

This document defines a standards-track Application-ID that falls into the Application Identifier standards-track address space defined by RFC 3588 [RFC3588] Section 11.3. This Application-ID has been registered in the Application IDs sub-registry of the AAA parameters registry with the following data:

ID values	Name	Reference
6	Diameter Session Initiation Protocol (SIP) Application	RFC 4740

13.2. Command Codes

This document defines new standard commands whose Command Codes are to be allocated within the standard permanent Command Codes address space defined in RFC 3588 [RFC3588] Section 11.2.1. These command codes should be registered in the Command Codes sub-registry of the AAA parameters registry.

Table 1 in Section 8 contains the detailed list of Command Code names and values that are part of this Diameter application.

13.3. AVP Codes

This document defines new standard AVPs, whose AVP Codes are to be allocated within the AVP Codes address space defined in RFC 3588 [RFC3588] Section 11.4. These AVP codes have been registered in the AVP Codes sub-registry of the AAA parameters registry.

Table 2 in Section 9 contains the detailed list of AVP names and AVP codes that are part of this Diameter application.

13.4. Additional Values for the Result-Code AVP Value

This document defines new standard Result-Code AVP values to be allocated within the Result-Code AVP address space defined in RFC 3588 [RFC3588] Section 14.4.1. These values are listed in the Result-Code AVP values section of the AVP Specific Values sub-registry of the AAA parameters registry.

Section 10.1.1 lists the new Result-Code AVP values that fall into the success category, according to RFC 3588 [RFC3588] Section 7.1.2.

Section 10.1.2 lists the new Result-Code AVP values that fall into the transient failures category, according to RFC 3588 [RFC3588] Section 7.1.4.

Section 10.1.3 lists the new Result-Code AVP values that fall into the permanent failures category, according to RFC 3588 [RFC3588] Section 7.1.5.

13.5. Creation of the SIP-Server-Assignment-Type Section in the AAA Registry

This document defines a new SIP-Server-Assignment-Type AVP (see Section 9.4). This AVP is of type Enumerated. We define an initial set of values that should be registered by IANA. IANA should create a new "SIP-Sever-Assignment-Type AVP values" section under the AVP Specific Values sub-registry of the AAA parameters registry. The initial list of values is listed in Section 9.4.

13.6. Creation of the SIP-Authentication-Scheme Section in the AAA Registry

This document defines a new SIP-Authentication-Scheme AVP (see Section 9.5.1). This AVP is of type Enumerated. We currently define a single value that should be registered by IANA. IANA should create a new "SIP-Authentication-Scheme AVP values" section under the AVP Specific Values sub-registry of the AAA parameters registry. The initial list of values is included in Section 9.5.1.

13.7. Creation of the SIP-Reason-Code Section in the AAA Registry

This document defines a new SIP-Reason-Code AVP (see Section 9.7.1). This AVP is of type Enumerated. We define an initial set of values that should be registered by IANA. IANA should create a new "SIP-Reason-Code AVP values" section under the AVP Specific Values sub-registry of the AAA parameters registry. The initial list of values is listed in Section 9.7.1.

13.8. Creation of the SIP-User-Authorization-Type Section in the AAA Registry

This document defines a new SIP-User-Authorization-Type AVP (see Section 9.10). This AVP is of type Enumerated. We define an initial set of values that should be registered by IANA. IANA should create a new "SIP-User-Authorization-Type AVP values" section under the AVP Specific Values sub-registry of the AAA parameters registry. The initial list of values is listed in Section 9.10.

13.9. Creation of the SIP-User-Data-Already-Available Section in the AAA Registry

This document defines a new SIP-User-Data-Already-Available AVP (see Section 9.13). This AVP is of type Enumerated. We define an initial set of values which should be registered by IANA. IANA should create a new "SIP-User-Data-Already-Available AVP values" section under the AVP Specific Values sub-registry of the AAA parameters registry. The initial list of values is listed in Section 9.13.

14. Security Considerations

This memo does not describe a stand-alone protocol, but a particular application for the Diameter protocol [RFC3588]. Consequently, all the security considerations applicable to Diameter automatically apply to this memo. In particular, Section 13 of RFC 3588 applies to this memo.

This Diameter SIP application allows a Diameter client to use the properties of HTTP Digest authentication [RFC2617] by evaluating or sending to the Diameter server the credentials supplied by a user. The discussion of HTTP Digest authentication in Section 4 of RFC 2617 [RFC2617] is also applicable to this memo.

This Diameter SIP application also allows a Diameter client to use the properties of HTTP Digest authentication using AKA [RFC3310] by evaluating or sending to the Diameter server the credentials supplied by a user. Section 5 of RFC 3310 [RFC3310] is also applicable to this memo.

14.1. Final Authentication Check in the Diameter Client/SIP Server

The Diameter SIP application can be configured to operate in a scenario where the final authentication check is performed in the Diameter client (SIP server). There are a number of security considerations associated to it; all of them are consequences of the requirement to transfer H(A1) from the Diameter server to the Diameter client:

- Both Diameter client and server must trust each other, such as when both client and server belong to the same administrative domain.

- To avoid eavesdroppers, the transport protocol between the Diameter client and server MUST be secured. RFC 3588 [RFC3588] specifies TLS [RFC4346] and IPsec as possible transport protection mechanisms for Diameter.

Due to these security considerations, it is RECOMMENDED to configure the Diameter SIP application to operate in the mode where the final authentication check is performed in the Diameter server.

15. Contributors

The authors would like to thank the following contributors who made substantial contributions to this work:

Pete McCann	Lucent
Jaakko Rajaniemi	Nokia

Wolfgang Beck (Deutsche Telekom AG) provided the text in Section 12, "Migration from RADIUS".

16. Acknowledgements

The authors would like to thank Tony Johansson and Kevin Purser for their invaluable contribution to the start-up of this application and the continuous progress. The authors would like to thank Daniel Warren, Jayshree Bharatia, Kuntal Chowdhury, Jari Arkko, Avi Lior, Wolfgang Beck, Ulrich Wiehe, Cullen Jennings, Anu Leinonen, Glen Zorn, German Blanco, Mikko Aittola, Bert Wijnen, and Sam Hartman for their reviews and valuable comments.

The Diameter SIP application is based on the Diameter application for the Cx interface of the 3GPP IP Multimedia Subsystem [3GPP.29.229]. The authors would like to thank 3GPP Working Group CN4 for this work.

17. References

17.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3310] Niemi, A., Arkko, J., and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC4590] Sterman, B., Sadolevsky, D., Schwartz, D., Williams, D., and W. Beck, "RADIUS Extension for Digest Authentication", RFC 4590, July 2006.

17.2. Informative References

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3680] Rosenberg, J., "A Session Initiation Protocol (SIP) Event Package for Registrations", RFC 3680, March 2004.

[RFC3880] Lennox, J., Wu, X., and H. Schulzrinne, "Call Processing Language (CPL): A Language for User Control of Internet Telephony Services", RFC 3880, October 2004.

[RFC4004] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application", RFC 4004, August 2005.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4006] Hakala, H., Mattila, L., Koskinen, J-P., Stura, M., and J. Loughney, "Diameter Credit-Control Application", RFC 4006, August 2005.

[3GPP.29.229] 3GPP, "Cx and Dx interfaces based on the Diameter protocol; Protocol details", 3GPP TS 29.229 5.12.0, June 2006.

[JSR-000116] Java Community Process, "SIP Servlet API Specification 1.0 Final Release", JSR 000116, March 2003.

Authors' Addresses

Miguel A. Garcia-Martin (Editor)
Nokia
P.O. Box 407
NOKIA GROUP, FIN 00045
Finland

Phone: +358 50 480 4586
EMail: miguel.an.garcia@nokia.com

Maria-Carmen Belinchon
Ericsson
Via de los Poblados 13
Madrid 28033
Spain

Phone: +34 91 339 3535
EMail: maria.carmen.belinchon@ericsson.com

Miguel A. Pallares-Lopez
Ericsson
Via de los Poblados 13
Madrid 28033
Spain

Phone: +34 91 339 4222
EMail: miguel-angel.pallares@ericsson.com

Carolina Canales-Valenzuela
Ericsson
Via de los Poblados 13
Madrid 28033
Spain

Phone: +34 91 339 2680
EMail: carolina.canales@ericsson.com

Kalle Tammi
Nokia
P.O.Box 785
Tampere 33101
Finland

Phone: +358 40 505 8670
EMail: kalle.tammi@nokia.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.