3GPP2 X.S0016-312
Version 1.0
Version Date: June 2004

MMS MM1 Stage 3

Using SIP

Revision: 0

No Text.

MMS MM1 STAGE 3 USING SIP

Contents

List of Figures

List of Tables

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project 2 (3GPP2).

Revision History

Revision		Date
Rev. 0	Initial Publication	June 2004

1 Introduction

This specification outlines a SIP realization of the MMS MM1. This SIP-based MM1 protocol is intended as a part of the MMS system described in the MMS Overview document [X.S0016-000]. It fulfills the MMS Stage 2 functions (see [X.S0016-200]) for Message Submission, Message Notification, Message Acknowledgement, Message Retrieval, Message Delivery Reporting and Message Read Reporting.

1.1 Scope

This specification defines a technical realization of the MMS MM1 interface for Message Submission, Message Notification, Message Acknowledgement, Message Retrieval, Message Delivery Reporting and Message Read Reporting.

1.2 References

3GPP2

[S.R0064] S.R0064 Multimedia Messaging Services (MMS) Stage 1 Requirement. http://www.3gpp2.org/

[X.S0016-000] X.S0016-000-B 3GPP2 Multimedia Messaging System MMS Specification Overview, Revision B. http://www.3gpp2.org/

TIA-934-000-B 3GPP2 Multimedia Messaging System MMS Specification Overview, Revision B.

[X.S0016-200] X.S0016-200 MMS Stage 2, Functional Specifications, Revision 0. http://www.3gpp2.org/

TIA-934-200 MMS Stage 2, Functional Specifications, Revision 0.

[X.S0013-002] X.S0013.2 IP Multimedia Subsystem - Stage-2. http://www.3gpp2.org/

TIA-973.002 IP Multimedia Subsystem - Stage-2

3GPP

[3GPP-23.228] 3GPP TS 23.228 V5.8.0 “IP Multimedia Subsystem (IMS) Stage 2”, 3GPP, http://www.3gpp.org/

IETF

[RFC1630] RFC 1630, Universal Resource Identifiers in WWW, June 1994, IETF. http://www.ietf.org/rfcs/rfc1630

[RFC2234] RFC 2234, augmented BNF for Syntax Specifications: ABNF, November 1997, IETF. http://www.ietf.org/rfcs/rfc2234

[RFC2246] RFC 2246, The TLS Protocol Version 1.0, IETF. http://www.ietf.org/rfcs/rfc2246

[RFC2387] RFC 2387, The MIME Multipart/Related Content-type, IETF. http://www.ietf.org/rfc/rfc2387

[RFC2616] RFC 2616, Hypertext Transfer Protocol HTTP/1.1, June 1999, IETF. http://www.ietf.org/rfc/rfc2616

[RFC2632] RFC 2632, S/MIME Version 3 Certificate Handling, June 1999, IETF. http://www.ietf.org/rfc/rfc2632

[RFC2633] RFC 2633, S/MIME Version 3 Message Specification, June 1999, IETF. http://www.ietf.org/rfc/rfc2633

[RFC2634] RFC 2634, Enhanced Security Services for S/MIME, June 1999, IETF. http://www.ietf.org/rfc/rfc2634

[RFC2732] RFC 2732, Format for Literal IPv6 Addresses in URL's, December 1999, IETF. http://www.ietf.org/rfcs/rfc2732

[RFC2818] RFC 2818, HTTP over TLS, May 2000, IETF. http://www.ietf.org/rfcs/rfc2818

[RFC3156] RFC 3156, MIME Security with OpenPGP, August 2001, IETF. http://www.ietf.org/rfc/rfc3156

[RFC3261] RFC 3261, "The Session Initiation Protocol". June 2002, IETF, http://www.ietf.org/rfc/rfc3261

[RFC3310] RFC 3310, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) ".September 2002, IETF, http://www.ietf.org/rfc/rfc3310

[RFC3428] RFC 3428 "SIP Extension for Instant Messaging", December 2002, IETF http://www.ietf.org/rfc/rfc3428

[RFC3608] RFC 3608 "Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration", October 2003, IETF. http://www.ietf.org/rfc/rfc3608

Open Mobile Alliance (OMA) (formerly WAP Forum)

[OMAENC] OMA-WAP-ENC-v1_1; Multimedia Messaging Service; Encapsulation Protocol. http://www.openmobilealliance.org/

[WAP238] WAP-238-WML-20010911-a, Wireless Markup Language version 2 Specification, September 2001, WAP Forum. http://www.openmobilealliance.org/

[WAP248] WAP-248-UAProf-20011020-a, WAG UAProf, November 2001, WAP Forum. http://www.openmobilealliance.org/

World-Wide-Web Consortium (W3C)

[SMIL] SMIL, Synchronized Multimedia Integration Language (SMIL) 2.0 Specification, June 1998, W3C.Terminology. http://www.w3.org/

This document uses the following “verbal forms” and “verbal form definitions”:

1. “shall” and “shall not” identify items of interest that are to be strictly followed and from which no deviation is recommended,
2. “should” and “should not” indicate items of interest that are highly desirable and particularly suitable, without identifying or excluding other items; or (in the negative

form) indicate items of interest that are not desirable, are not particularly suitable, or are not recommended but not prohibited, and

3. "may" and "may not" indicate items of interest that are optional but permissible within the limits of this recommendation.

1.3 Assumptions

This document describes a Stage 3 technical realization for 3GPP2 MMS MM1. It is assumed that the reader is already familiar with the contents of the 3GPP2 MMS Specification Overview (X.S0016-000), MMS Stage 1 [S.R0064], Stage 2 [X.S0016-200], [RFC3261] and [RFC3428] documents.

1.4 Definitions

TBD

1.5 Abbreviations

For the purposes of the present document, the following abbreviations apply in addition to those defined in Stage 2 documents.

DOS	Denial of Service
FDQN	Fully Qualified Domain Name
HSP	Home Serving Proxy
IANA	Internet Assigned Numbers Authority
MIME	Multipurpose Internet Mail Extensions
MM	Multimedia Message
MMS	Multimedia Messaging Service
MSG	Message
OMA	Open Mobile Alliance
RFC	Request for Comments
SIP	Session Initiation Protocol
TLS	Transport Layer Security
UA	User Agent
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3C	WWW Consortium
WAP	Wireless Application Protocol

2 Stage 2 Amendments

In addition to MMS Stage 2 [X.S0016-200], this specification requires a mechanism called Registration that must be accomplished by the MMS UA before utilizing any MMS functionality. Registration informs the MMS Relay/Server that the MMS UA is available to receive and invoke SIP-Based MMS Services.

In addition to MMS Stage 2 [X.S0016-200], this specification provides a mechanism called User-Initiated De-registration whereby the MMS UA informs the MMS Relay/Server that the MMS UA is no longer available to receive or invoke SIP-Based MMS Services.

In addition to MMS Stage 2 [X.S0016-200], this specification provides a mechanism called *Service Termination* whereby the MMS Relay/Server can inform the MMS UA, after a successful Registration, that SIP-Based MMS Service will no longer be provided.

The MMS Stage 2 [X.S0016-200] does not provide for delivery of MM content in an MM1_Notification.REQ. This specification provides a mechanism (referenced as Direct-Notification) whereby small size MM contents constrained by [RFC3428] may be delivered in the MM1_Notification.REQ.

3 MM1 SIP Stage 3 Description

This section contains definitions, symbols and abbreviations that are used throughout the document.

3.1 Introduction

This specification defines the signaling and procedures for the SIP MM1 implementation option. The MM1 interface is defined as the interface between the MMS UA and the MMS Relay/Server. MM1 provides three basic messaging services: message submission, message retrieval, and message notification. This specification also defines mechanisms for delivery acknowledgement, delivery reporting and read reporting.

Message submission is a mechanism used by the MMS UA to submit a multimedia message. Message notification is the mechanism used to inform the MMS UA about a received message. Message retrieval is a mechanism used by the MMS UA to retrieve a multimedia message. Delivery acknowledgement is the acknowledgement from the MMS UA to the MMS Relay/Server that a MM has been delivered. Delivery reporting permits the originating MMS UA to know when a message delivery has occurred. Read reporting permits the originating MMS UA to know when a message has been read. This specification utilizes SIP [RFC3261] for the message submission, message notification, delivery acknowledgement, delivery reporting and read reporting over the MM1 interface.

3.1.1 MM1 Architecture

Figure 1 depicts a generalized architecture for a SIP realization of the MMS MM1.

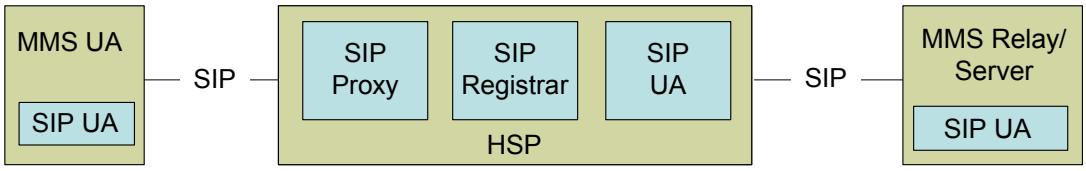

Figure 1 **Architecture for SIP-Based MMS MM1**

The functionality of the architecture elements are:

- Home Serving Proxy (HSP) - consists of three functional entities, a SIP Proxy, a SIP Registrar and a SIP UA. The SIP Registrar is a SIP server that terminates and responds to SIP REGISTER requests as defined in [RFC3261]. The SIP Proxy provides primary SIP routing as defined in [RFC3261] to handle routing of SIP messages between the MMS UA and the MMS Relay/Server. For the purposes of executing application dispatch (e.g., 3rd party Registration Request to the MMS Relay/Server) the HSP implements the SIP UA functionality as defined in [RFC3261]. For 3GPP IMS [3GPP-23.228] and 3GPP2 IMS [X.P0013.2] networks the HSP is equivalent to the S-CSCF.
- MMS UA – the functionality of the MMS UA is defined in [X.S0016-200]. For 3GPP2 IMS [X.P0013.2] and 3GPP IMS [3GPP-23.228] networks the MMS UA is implemented by the User Equipment (UE)

- MMS Relay/Server - the functionality of the MMS Relay/Server is defined in [X.S0016-200]. For 3GPP2 IMS [X.P0013.2] and 3GPP IMS [3GPP-23.228] networks the MMS Relay/Server is implemented by the Application Server (AS).

3.1.2 MM1 Abstract Transactions

Figure 2 depicts the abstract transactions that have been defined in MMS Stage 2 [X.S0016-200]. The Submission, Retrieval, Notification, Delivery acknowledgement, Delivery Reporting, and Read Reporting abstract transactions are mapped to corresponding SIP commands and features in the sections below.

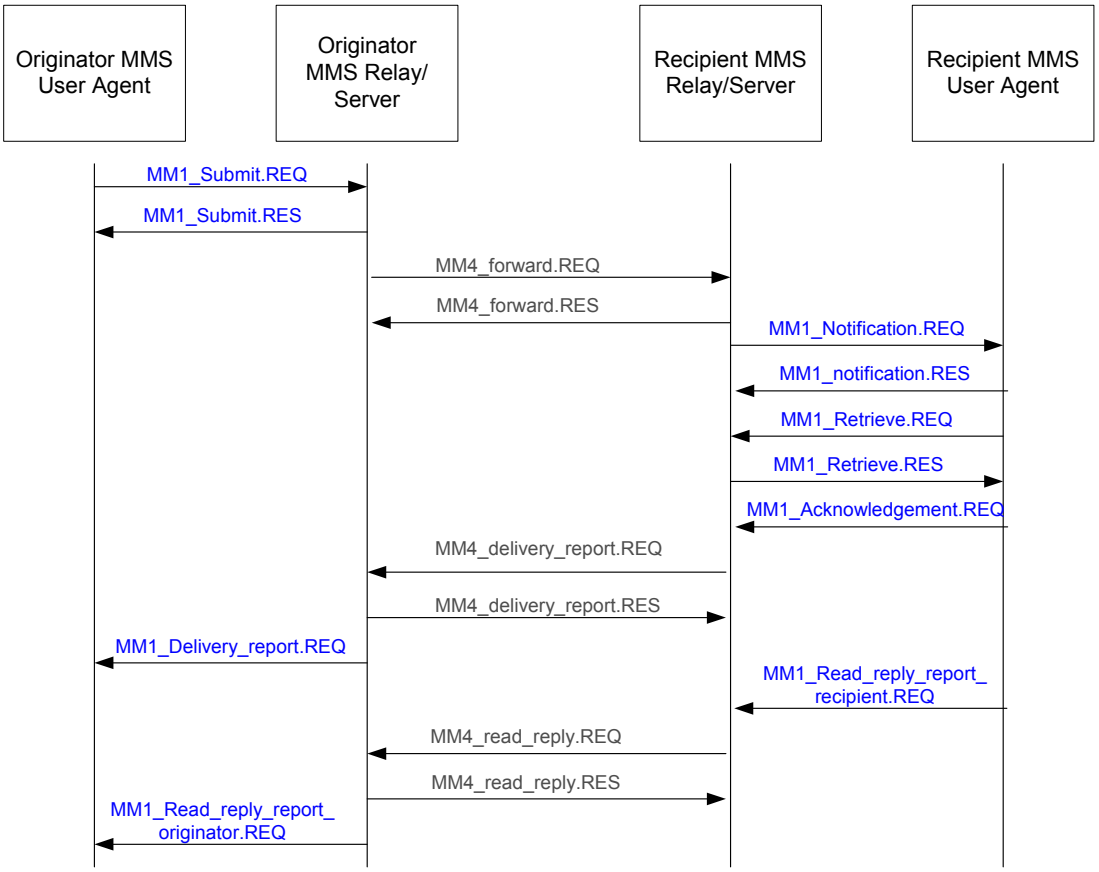

Figure 2 **Abstract Transaction Call Flows**

3.2 MM1 SIP-Based Functions

SIP provides a protocol that fulfills the Message Submission, Message Notification, Delivery Acknowledgement, Delivery Reporting and Read Reporting functions. The specific SIP usage to fulfill these functions is described separately. The abstract message flows for these functions are described in [X.S0016-200].

Before utilizing any MMS functionality defined in this specification an MMS UA shall first register with the HSP. Registration allows the HSP to learn the current location (e.g., contact address) of the MMS UA.

The MMS UA and the MMS Relay/Server shall support the "MESSAGE" method (referred as SIP MESSAGE request in this document). Unless stated otherwise the SIP MESSAGE request and responses shall follow the syntax and the processing details (from both the MMS UA and MMS Server perspective) as defined in [RFC3428].

Unless stated otherwise the SIP REGISTER request and responses shall follow the syntax and the processing details (from the MMS UA, HSP, and MMS Relay/Server perspective) as defined in [RFC3261]. The MMS UA and HSP shall support the SIP extension for Service-Route discovery as defined in [RFC3608].

3.2.1 SIP Registration

SIP Registration activities include initial registration, user-initiated re-registration, and user-initiated de-registration.

When an MMS UA connects to the network, it shall send a SIP REGISTER Request to a HSP indicating, among other things, a contact for the user. The HSP shall implement the SIP registrar functionality as defined in [RFC3261]. The MMS Relay/Server shall be able to terminate the REGISTER method in order to discover the registration status of the user.

3.2.1.1 Initial Registration and User-initiated Re-registration

The MMS UA shall register with the HSP prior to initializing any SIP MMS functionality. Upon the completion of a successful Registration, the HSP shall send a third-party SIP REGISTER Request to the MMS Relay/Server containing the public user identity of the MMS UA. The SIP-MESSAGE exchange is used to inform MMS UA of availably of MMS Service. The SIP-MESSAGE exchange is also used to provide HTTP URI that will be used by MMS UA for storing indirect MM content. Figure 3 shows a message flow for Initial Registration and User-initiated Re-registration.

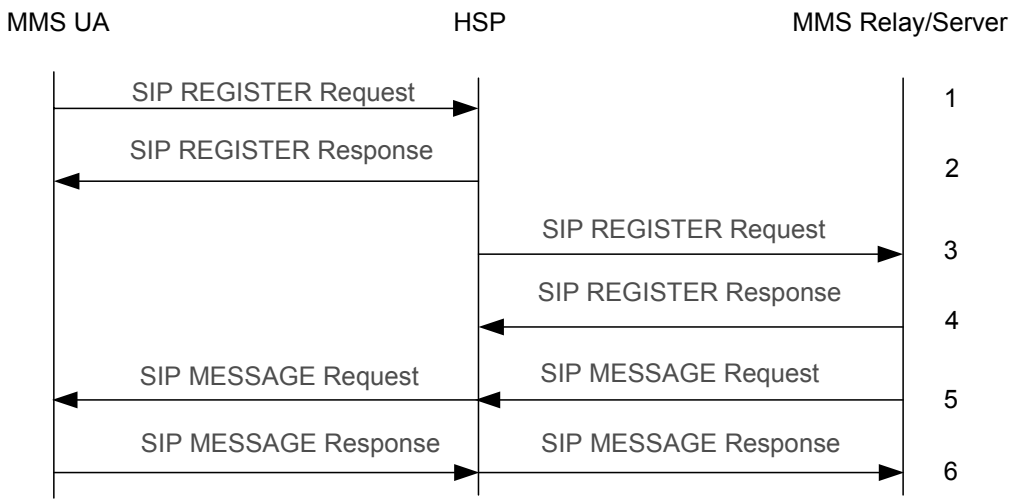

Figure 3 **Initial Registration and User-initiated Re-registration**

3.2.1.1.1 SIP REGISTER Request (MMS UA -> HSP)

The SIP REGISTER Request is defined in [RFC3261]. A MMS UA uses the SIP REGISTER method to inform the HSP of its current communications addresses (i.e., Contact addresses). SIP REGISTER Requests shall be authenticated (see Section 3.3).

The MMS UA shall only initiate a subsequent SIP REGISTER Request when it has received a SIP REGISTER Response from the HSP for the ongoing registration, or the previous SIP REGISTER Request has timed out. On sending the SIP REGISTER Request, the MMS UA shall, at a minimum, populate the SIP REGISTER Request header fields as given in Table 1 .

SIP Header	Comments
From	shall be set to the SIP URI that contains the public user identity to be registered.
To	shall be set to the SIP URI that contains the public user identity to be registered.
Contact	set to include SIP URI(s) containing the IP address of the MMS UA or FQDN. If the UE specifies its FQDN in the Contact header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address of the MMS UA.
Expires, or the expires parameter of the Contact header	set to the value of 600 000 seconds as the value desired for the duration of the registration. The HSP might decrease the duration of the registration. Registration attempts with a registration period of less than a predefined minimum value defined in the HSP will be rejected with a 423 (Interval Too Brief) response.
Request-URI	set to the SIP URI of the domain name of the home network
Authorization header	if the MMS UA has previously established a security association with the HSP (e.g., previously responded to a digest challenge for which the security parameters are still valid) then the Authorization header contains the “security parameters”.

Table 1 **SIP REGISTER Request Header (MMS UA) for Initial Registration**

3.2.1.1.2 SIP REGISTER Response (HSP - > MMS UA)

The service provider defines the minimum and maximum times for each registration. Upon receipt of the SIP REGISTER Request the HSP shall:

1. Identify the user by the identity as received in the To header and check how many authentications are ongoing for this user. The HSP may (based on service provider policy) reject the SIP REGISTER Request by sending a 403 (Forbidden) SIP REGISTER Response, if there is an ongoing authentication. The response may include a Warning header containing the warn-code 399.
2. If there is no ongoing authentication, check if the MMS UA needs to be authenticated. If the MMS UA has not previously responded to a digest challenge the HSP shall challenge the user by send a 401 (Unauthorized) SIP REGISTER Response to the MMS UA
3. If the Call-ID of the SIP REGISTER Request matches with the Call-ID of the 401 (Unauthorized) SIP REGISTER Response sent previously to the MMS UA the HSP shall determine if the security parameters in the Authorization header are valid.
    i. If the security parameters are valid and the expiration timer from the MMS UA is too short to be accepted the HSP shall reject the SIP-REGISTER Request with a 423 (Interval too Brief) SIP-REGISTER Response, containing the Min-Expires header with the minimum registration time the HSP will accept.

If the security parameters are valid the HSP shall create a registration entry for the user as defined in [RFC3261} and respond with a 200 (OK). The 200 (OK) response shall include a Service-Route header field as defined in [RFC3608] containing the SIP URI identifying the HSP. The HSP shall send a third-party SIP REGISTER Request to the MMS Relay/Server (see Section 3.2.1.1.4).

ii. If the security parameters are invalid the HSP shall either
   1. respond with a 401 (Unauthorized) SIP REGISTER Response containing a new digest challenge to initiate a further authentication attempt; or
   2. respond with a 403 (Forbidden) SIP REGISTER Response if the authentication attempt is to be abandoned).

The syntax of the SIP REGISTER Response is defined in [RFC3261].

Upon receiving a 200 (OK) response to the SIP REGISTER Request, the MMS UA shall:

1. store the expiration time from the SIP REGISTER Response.
2. store the list of Service-Route headers contained in the Service-Route header field [SCVRT]. The MMS UA shall use the Service-Route headers to build a route set (inserted as Route header) when generating SIP MESSAGE Request sent to the MMS Relay/Server.

When a 401 (Unauthorized) response to a SIP REGISTER Request is received the MMS UA shall resend the SIP REGISTER Request with an Authorization header that answers the challenge.

On receiving a 423 (Interval Too Brief) response to the SIP REGISTER Request, the MMS UA shall send another SIP REGISTER Request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

3.2.1.1.3 SIP REGISTER Request (HSP - > MMS Relay/Server)

Upon sending a 200 (OK) response to the SIP REGISTER Request to the MMS UA, the HSP shall send a third-party SIP REGISTER Request to the MMS Relay/Server associated with the public user identity used in the SIP REGISTER Request from the MMS UA. The procedure to obtain the SIP URI for the MMS Relay/Server is outside the scope of this document. A HSP uses the SIP REGISTER method to inform the MMS Relay/Server about the registration status of the MMS UA.

On sending the SIP REGISTER Request the HSP shall, at a minimum, populate the SIP REGISTER Request header fields as given in Table 2 .

SIP Header	Comments
Request-URI	shall contain the MMS Relay/Server SIP URI
From	shall contain the HSP SIP URI
To	shall contain the public user identity of the MMS UA for which the third-party SIP REGISTER Request is being sent (e.g., for 3GPP2 IMS or 3GPP IMS this might be an implicitly registered public user identity, as configured by the operator);
Contact	shall contain theHSP's SIP URI
Expires	shall contain the same value as in the 200 (OK) response sent to the SIP REGISTER Request from the MMS UA (see section 3.2.1.1.2)

Table 2 **SIP REGISTER Request (SIP Registrar) for Initial Registration**

3.2.1.1.4 SIP REGISTER Response (MMS Relay/Server -> HSP)

Upon receipt of the SIP REGISTER Request the MMS Relay/Server shall determine if the public user identity in the To header is a valid (note the definition of valid is outside the scope of this document) MMS subscriber.

- if the public user identity is valid the MMS Relay/Server shall respond with a 200 (OK) response for the SIP REGISTER Request. The MMS Relay/Server shall store the expiration time of the registration and the contact information.
- if the public user identity is invalid or if the MMS Relay/Server decides to deny service for the MMS UA, then the MMS Relay/Server shall send a 403 (Forbidden) response to the HSP.

Upon receiving the SIP-REGISTER Response from the MMS Relay/Server, the HSP shall process the response as a SIP User Agent as defined in [RFC3261].

3.2.1.1.5 SIP-MESSAGE Request (MMS Relay/Server ->MMS UA)

Upon receipt of the SIP-REGISTER Request the MMS Relay/Server shall determine if the public user identity in the To header is a valid (note the definition of valid is outside the scope of this document) MMS subscriber.

- if the public user identity is valid the MMS Relay/Server shall send a SIP-MESSAGE Request to the MMS UA. The MMS Relay/Server shall, at a minimum, populate the SIP-MESSAGE Request header fields as given in Table 3.

SIP Header	Comments
Request-URI	shall contain the public user identity of the MMS UA.
From	shall contain the MMS Relay/Server SIP URI
To	shall contain the public user identity of the MMS UA
Content-Type	shall be set to “application/vnd.3gpp2.mms.sip”. In the MIME body the parameters shall be set to: version = “Version=0” msg-field = “Msg=Registration” msg-status = “Status=registered”
Route	shall contain the SIP URI of the HSP as received in the third-party REGISTER request.
Call-Info	shall be set to an HTTP URI allocated for the MMS UA to store indirect contents. The header field shall include the following parameters: purpose=ci-uri expiration set to the same value as the Expires header field in the 200 (OK) response sent to the SIP-REGISTER Request from the MMS UA (see section 3.2.1.1.2)

Table 3 **SIP-MESSAGE Request Header (MMS Service registered by MMS Relay/Server)**

- if the public user identity is invalid or if the MMS Relay/Server decides to deny service for the MMS UA, then the MMS Relay/Server shall send a SIP-MESSAGE Request to the MMS UA. The MMS Relay/Server shall, at a minimum, populate the SIP-MESSAGE Request header fields as given in Table 4.

SIP Header	Comments
Request-URI	shall contain the public user identity of the MMS UA.
From	shall contain the MMS Relay/Server SIP URI
To	shall contain the public user identity of the MMS UA
Content-Type	shall be set to "application/vnd.3gpp2.mms.sip". In the MIME body the parameters shall be set to: version = "Version=0" msg-field = "Msg=Registration" msg-status = "Status=denied" the msg-reason parameter should be set as appropriate.
Route	shall contain the SIP URI of the HSP as received in the third-party REGISTER request.

Table 4 **SIP MESSAGE Request Header (MMS Relay/Server Service denied by MMS Relay/Server)**

3.2.1.1.6 SIP MESSAGE Response (MMS UA _> MMS Relay/Server)

Upon receipt of a SIP MESSAGE Request that contain a Content-Type set to application/vnd.3gpp2.mms.sip the MMS UA shall:

- if the "status-type" parameter set to "denied" :
  1. assume that the Registration for the MMS services has failed. Note if the MMS UA had previously received a SIP REGISTER Response with a 200 (OK) status code, from the HSP (see Section 3.2.1.1.2), then the MMS UA shall assume that it is still registered with the HSP.
  2. send an appropriate response [RFC3261][RFC3428] to the MMS Relay/Server.

- if the "status-type" parameter set to ""registered"
  1. the MMS UA shall assume that it is presently registered for MMS services for the length of time set in the Call-Info header
  2. store the HTTP URI in the Call-Info header.
  3, send an appropriate response [RFC3261] to the MMS Relay/Server.

3.2.1.2 User-Initiated De-registration

The MMS UA can deregister at any time. Prior to sending a SIP REGISTER Request for deregistration, the MMS UA shall conclude any ongoing MM1 SIP-Based functions. Figure 4 shows a message flow for user-initiated de-registration.

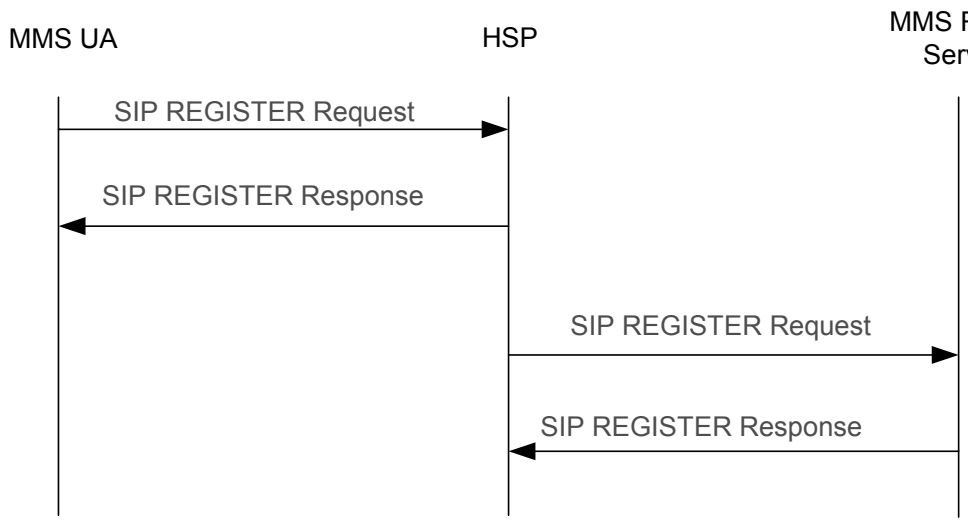

Figure 4 **User-Initiated De-registration**

3.2.1.2.1 SIP REGISTER Request (MMS UA)

On sending the SIP REGISTER Request the MMS UA shall, at a minimum, populate the SIP REGISTER Request header fields as given in Table 5 .

SIP Header	Comments
From	shall be set to the SIP URI that contains the public user identity to be de-registered.
To	shall be set to the SIP URI that contains the public user identity to be de-registered.
Contact	set to include SIP URI(s) containing the IP address of the MMS UA or FQDN. If the UE specifies its FQDN in the Contact header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address of the MMS UA.
Expires, or the expires parameter of the Contact header	set to a value of zero
Request-URI	set to the SIP URI of the domain name of the home network
Authorization header	contains the “security parameters”

Table 5 **SIP REGISTER Request Headers (MMS-UA) for Deregistration**

3.2.1.2.2 SIP REGISTER Response (HSP)

Upon receipt of the SIP REGISTER Request with the Expires header containing a value of zero, the HSP shall:

1. Identify the user by the identity as received in the To header and check how many authentications are ongoing for this user. The HSP may (based on service provider policy) reject the SIP REGISTER Request by sending a 403 (Forbidden) SIP REGISTER Response, if there is an ongoing authentication. The response may include a Warning header containing the warn-code 399.

2. If there is no ongoing authentication, check if the MMS UA needs to be authenticated. If the MMS UA has not previously responded to a digest challenge the HSP shall challenge the user by send a 401 (Unauthorized) SIP REGISTER Response to the MMS UA
3. If the Call-ID of the SIP REGISTER Request matches with the Call-ID of the 401 (Unauthorized) SIP REGISTER Response sent previously to the MMS UA the HSP shall determine if the security parameters in the Authorization header are valid.
   i. If the security parameters are valid the HSP shall remove the registration entry for the user as defined in [RFC3261} and respond with a 200 (OK). The 200 (OK) response shall include a Service-Route header field as defined in [RFC3608] containing the SIP URI identifying the HSP. The HSP shall send a third-party SIP REGISTER Request to the MMS Relay with the Expires header containing a value of zero.
   ii. If the security parameters are invalid the HSP shall either
      1. respond with a 401 (Unauthorized) SIP REGISTER Response containing a new digest challenge to initiate a further authentication attempt; or
      2. respond with a 403 (Forbidden) SIP REGISTER Response if the authentication attempt is to be abandoned).

Upon receiving the 200 (OK) response to the SIP REGISTER Request, the MMS UA shall remove all registration details.

3.2.1.2.3 SIP REGISTER Request (HSP)

Upon sending a 200 (OK) response to the MMS UA, the HSP shall send a SIP REGISTER Request to the MMS Relay/Server associated with the public user identity of the MMS UA. The HSP uses the SIP REGISTER method to inform the MMS Relay/Server that the public user identity of the MMS UA has been de-registered.

The HSP shall, at a minimum, populate the SIP REGISTER Request header fields as given in Table 6 .

SIP Header	Comments
Request-URI	shall contain the MMS Relay/Server SIP URI
From	shall contain the SIP Registrar SIP URI
To	shall contain the public user identity of the MMS UA for which the third-party SIP REGISTER Request is being sent (e.g., for 3GPP2 IMS or 3GPP IMS this might be an implicitly registered public user identities, as configured by the operator);
Contact	shall contain the SIP Registrar's SIP URI
Expires	shall contain a value of zero

Table 6 **SIP REGISTER Request Headers (SIP Registrar) for Deregistration**

3.2.1.2.4 SIP REGISTER Response (MMS Relay/Server)

Upon receipt of the SIP REGISTER Request the MMS Relay/Server shall deregister the public user identity found in the To header field.

The MMS Relay/Server shall respond with the appropriate response [RFC3261].

3.2.2 Service Termination

The MMS Relay/Server can terminate services for a MMS UA at anytime. Prior to initiating service termination with a MMS UA the MMS Relay/Server shall terminate all on-going MM1 SIP-Based Functions. Service Termination does not change the registration status with the HSP.

Figure 5 shows a message flow for Service Termination.

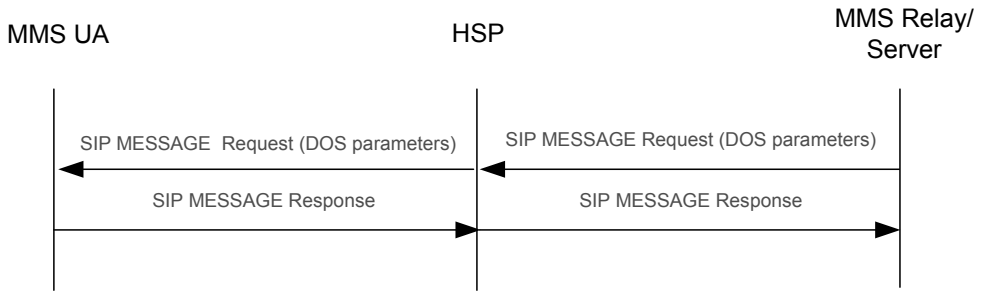

Figure 5 **Service Termination**

3.2.2.1 SIP MESSAGE Request (MMS Relay/Server)

The MMS Relay/Server shall send a SIP MESSAGE Request to the MMS UA. The MMS Relay/Server shall, at a minimum, populate the SIP MESSAGE Request header fields as given in Table 7.

SIP Header	Comments
Request-URI	shall contain the public user identity of the MMS UA.
From	shall contain the MMS Relay/Server SIP URI
To	shall contain the public user identity of the MMS UA
Content-Type	shall be set to “application/vnd.3gpp2.mms.sip”. In the MIME body the parameters shall be set to: version = “Version=0” msg-field = “Msg=Termination” msg-status = “Status=terminated” the msg-reason parameter should be set as appropriate.
Route	shall contain the SIP URI of the HSP as received in the third-party SIP REGISTER request.

Table 7 **SIP MESSAGE Request Header (MMS Relay/Server)**

3.2.2.2 SIP MESSAGE Response (MMS UA)

Upon receipt of a SIP MESSAGE Request that contains a Content-Type set to “application/vnd.3gpp2.mms.sip.status” the MMS UA shall:

1. follow the recommended action in Appendix B2.
2. send an appropriate response [RFC3261] [RFC3428] to the MMS Relay/Server.

3.2.3 Message Submission

The procedure for message submission depends upon the content size of the MM. In cases where the actual MM content is small only MM Submission (see Section 3.2.3.1) is required. The definition of small is determined by provider policy, subject to the size constraints in [RFC3428].

3.2.3.1 MM Submission

MM Submission is used by the MMS UA to inform the MMS Relay/Server that it desires to send an MM. MM Submission consists of two steps: 1) submitting the submission request and 2) receiving confirmation of the submission request. The request contains either a small MM or an indirect reference to an MM (e.g., for large MMs).

Table 8 specifies the mapping of abstract MM1 Submit messages [X.S0016-200] to the appropriate SIP operations.

Abstract Messages	Mapping	Direction
MM1_Submit.REQ	SIP MESSAGE Request	MMS UA -> MMS Relay/Server
MM1_Submit.RES	SIP MESSAGE Request	MMS Relay/Server -> MMS UA

Table 8 **Mapping of MM1 Submit abstract messages**

The message flow MM Submission is given in Figure 6.

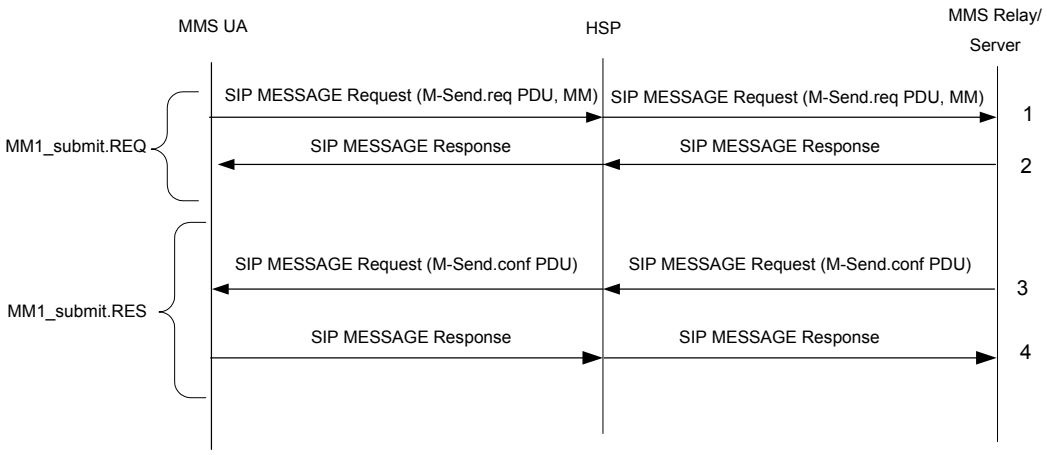

Figure 6 **Message flow for MM Submission**

3.2.3.1.1 SIP MESSAGE Request (MMS UA -> MMS Server)

The MMS UA shall send a SIP MESSAGE Request to the MMS Relay/Server. The payload of the SIP MESSAGE Request contains a multipart/related MIME type [RFC2387] including two parts.. One part will be of Content-Type “application/vnd.wap.mms-message and contain the M-Send.req PDU which is defined in [OMAENC]. The other part of the multipart MIME contains either the MM contents or an indirect reference to the MM contents. If the MM Content is included then the appropriate content-type is used. If an indirect reference to the MM Content (e.g., HTTP URI) is used, then the Content-Type is set to “message/external-body” and a URI that refers to the MM content is included. The SIP MESSAGE Request structure is shown Figure 7.

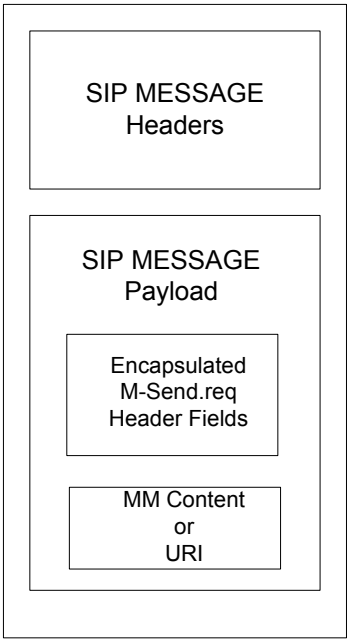

Figure 7 **SIP MESSAGE Request for MM Submission (M-Send.req)**

3.2.3.1.2 SIP MESSAGE Response (MMS Relay/Server -> MMS UA)

After receiving a SIP MESSAGE Request, the MMS Relay/Server shall send an appropriate response [RFC3261] [RFC3428] to the MMS UA.

3.2.3.1.3 SIP MESSAGE Request (MMS Relay/Server -> MMS UA)

After processing the SIP MESSAGE Request payload received from the MMS UA, the MMS Relay/Server shall send a SIP MESSAGE Request to the MMS UA. The payload of the SIP MESSAGE Request includes the MIME type application/vnd.wap.mms-message which includes the M-Send.conf header fields as described in [OMAENC]. The M-Send.conf header fields are encoded according to the binary encoding described in [OMAENC]. Figure 8 shows the SIP MESSAGE Request message structure sent from the MMS Relay/Server to the MMS UA.

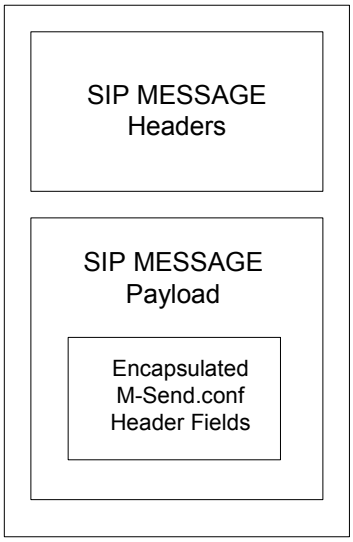

Figure 8 **SIP MESSAGE Request for MM Submission (M-Send.conf)**

3.2.3.1.4 SIP MESSAGE Response (MMS UA -> MMS Relay/Server)

After receiving a SIP MESSAGE Request, the MMS UA shall send an appropriate response [RFC3261] [RFC3428] to the MMS Relay/Server.

3.2.3.2 Message Submission for Large MM

For large MM content, the process of message submission requires two steps:

1. The MMS UA uploads the MM content to the storage location provided by the MMS Relay/Server during registration period
2. MM Submission, given in Section 3.2.3.1 is performed.

3.2.3.2.1 Uploading an MM

The MM content is uploaded to the storage location provided during registration using an HTTP PUT method [RFC2616]. If the MMS Relay/Server is not part of a trusted domain then Secure HTTP (HTTPS) [RFC2818] shall be used between the MMS UA and the MMS Relay/Server for the HTTP PUT Method. The message flow for the uploading operation is given in Figure 9.

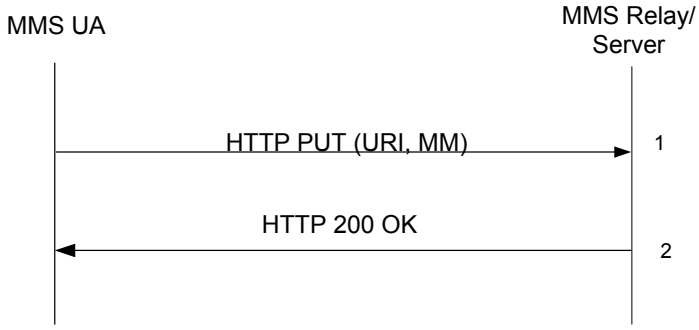

Figure 9 **Message Flow for Uploading a MM**

3.2.3.2.1.1 HTTP PUT (MMS UA -> MMS Relay/Server)

The MMS UA shall send an HTTP PUT [RFC2616] to the MMS Relay/Server containing the URI received from the MMS Relay/Server during the registration period and the MM content.

3.2.3.2.1.2 HTTP PUT Response (MMS Relay/Server -> MMS UA)

When successful, the MMS Relay/Server responds with an HTTP 200 OK response.

3.2.4 Message Notification

After an MMS UA has successfully registered with the HSP and the HSP informed the MMS Relay/Server about the registration status of the MMS UA, the MMS Relay/Server shall notify the MMS UA of any MMs that are available. This specification defines two message notification mechanisms: Direct-Notification and Indirect-Notification. The Direct-Notification mechanism contains the MM content within the MM1_Notification.REQ and the Indirect-Notification uses an indirect reference (i.e., standard URI as defined in [RFC2396]) to the MM content in the MM1_Notification.REQ.

Table 9 specifies the mapping of abstract MM1 Notification messages [X.S0016-200] to the appropriate SIP operations.

Abstract Messages	Mapping	Direction
MM1_notification.REQ	SIP MESSAGE request	MMS Server -> MMS UA
MM1_notification.RES	SIP MESSAGE request	MMS UA -> MMS Server

Table 9 **Mapping of MM1 Notification abstract messages**

3.2.4.1 Direct-Notification

In cases where the actual MM content is small Direct-Notification may be used. The definition of small is determined by provider policy, subject to the size constraints in [RFC3428]. The message flow for Direct-Notification is shown in Figure 10.

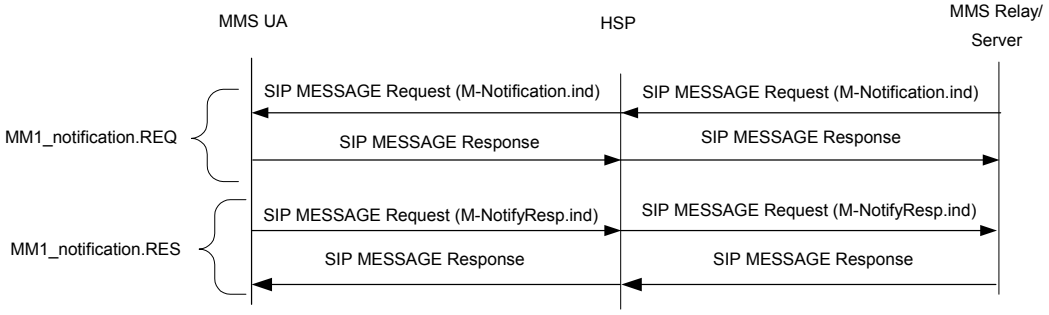

Figure 10 **Direct-Notification Message Flow**

3.2.4.2 Indirect- Notification

In the more common case, the actual MM content is stored on the MMS Relay/Server or on a separate content server, and the MMS notification contains a field indicating the size of the MM content and a pointer to the message content that can be used by the MMS UA to retrieve the content. Message notification using a pointer to the message content is defined as Indirect-Notification. Message flows for Indirect-Notification are shown in Figure 11 and Figure 12. The details of the MM1_retrieve.REQ

and MM1_retrieve.RES (as shown in Figure 11 and Figure 12) are given in Section 3.2.5. The details of MM1_Acknowledgement.REQ (as shown in) will be addressed in Section 3.2.6.

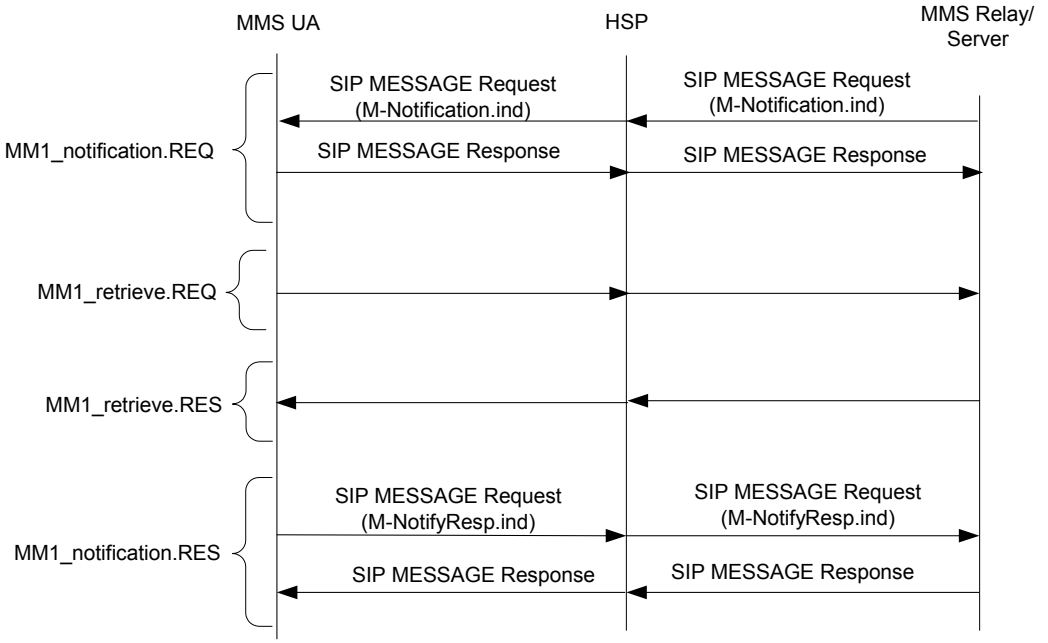

Figure 11 **Indirect-Notification Message Flow (Immediate Retrieval of MM)**

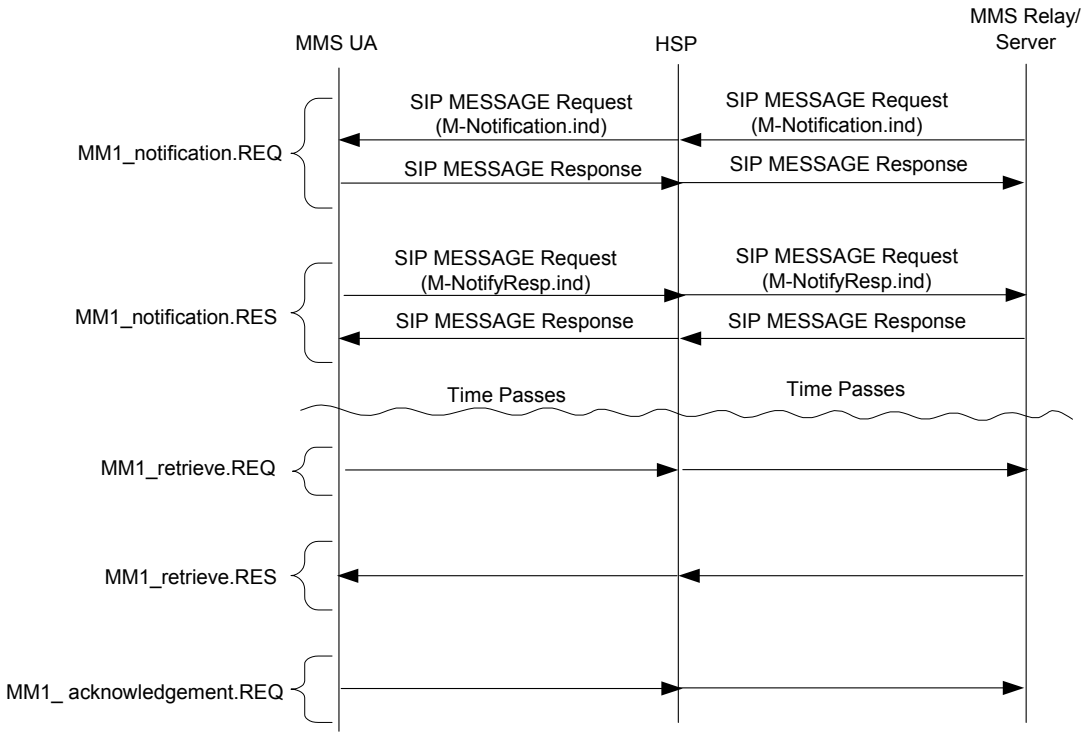

Figure 12 **Indirect-Notification Message Flow (Delayed Retrieval of MM)**

3.2.4.3 SIP MESSAGE Request (MMS Server -> MMS UA)

When the MMS Relay/Server receives an MM for a registered user it shall send a SIP MESSAGE Request to the MMS UA. When constructing the SIP MESSAGE Request the MMS Relay/Server shall map certain M-Notification.ind header fields [OMAENC] and other information into SIP MESSAGE Header fields as described in Table 10.

Data Element	SIP Header	Comments
M-Notification.ind .From	From	May be a TEL URL, or encoded into a SIP URL. If From is not included in the MM Notification headers, the SIP header should include "anonymous" in the user part.
M-Notification.ind .Subject	Subject	
M-Notification.ind.X-Mms-Expiry	Expires	Should also include a Date header indicating the time and date the MESSAGE request was sent.
Response Destination	Reply-To	URL indicating logical destination for response message.

Table 10 **SIP MESSAGE Header Field Mapping (Notification.REQ)**

The SIP MESSAGE Payload is a multipart MIME containing two parts, in no particular order. One part is of Content-Type application/vnd.wap.mms-message and contains the M-Notification.ind header fields as described in [OMAENC]. The M-Notification.ind header fields are encoded according to the binary encoding described in [OMAENC]. The X-Mms-Content-Location field of M-Notification.ind should contain a URL with the scheme of “cid:” containing a reference to the Content-ID header of the MM Content. The other part contains either the MM contents (i.e., Direct-Notification) or an indirect reference to the MM contents (i.e., Indirect-Notification). If Direct-Notification is used then the appropriate Content-Type is used and the MM content is included. If Indirect-Notification is used the Content-Type is set to “message/external-body” and a URL that refers to the MM content is included. The SIP MESSAGE Request message structure for Direct-Notification is shown in Figure 13 and for Indirect-Notification in Figure 14.

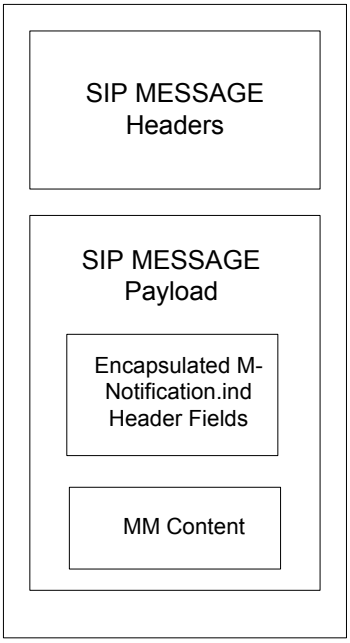

Figure 13 **SIP MESSAGE Request for Direct-Notification (M-Notification.ind)**

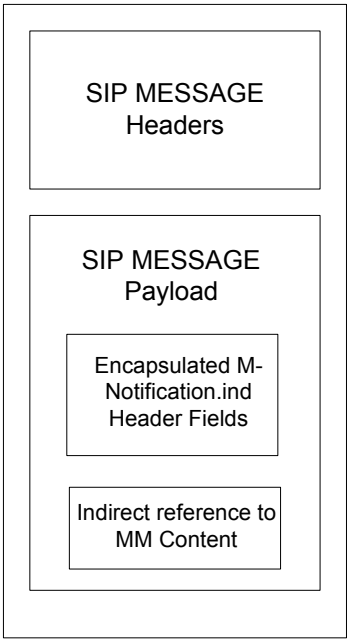

Figure 14 **SIP MESSAGE Request for Indirect-Notification (M-Notification.ind)**

3.2.4.4 SIP MESSAGE Response (MMS UA -> MMS Server)

After receiving a SIP MESSAGE Request, the MMS UA shall send an appropriate response [RFC3261] [RFC3428] to the MMS Relay/Server.

3.2.4.5 SIP MESSAGE Request (MMS UA -> MMS Server)

After sending the response discussed in Section 3.2.4.4, the MMS UA processes the SIP MESSAGE Payload (see Section 3.2.4.3) received from the MMS Relay/Server. After processing, the MMS UA

shall send a SIP MESSAGE Request to the MMS Relay/Server. If the SIP MESSAGE Payload contained an Indirect-Notification it is up to the MMS UA to decide whether to send the SIP MESSAGE Request immediately after sending the response for the SIP MESSAGE Request (see Figure 11) or after retrieval of the MM content from the indicated MM content location (see Figure 12).

The payload of the SIP MESSAGE Request includes the MIME type application/vnd.wap.mms-message which includes the M-NotifyResp.ind header fields as described in [OMAENC]. The M-NotifyResp.ind header fields are encoded according to the binary encoding described in [OMAENC]. Figure 15shows the SIP MESSAGE Request message structure sent from the MMS UA to the MMS Server.

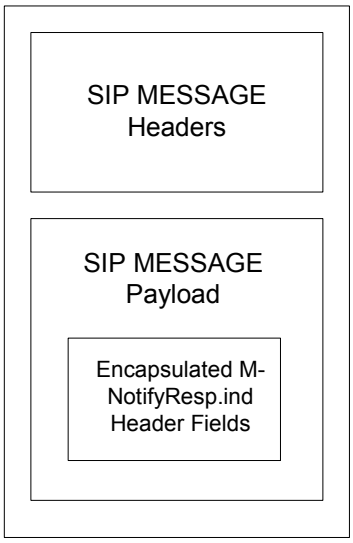

Figure 15 **SIP MESSAGE Request Structure (NotifyResp.ind)**

3.2.4.6 SIP MESSAGE Response (MMS Server -> MMS UA)

After receiving a SIP MESSAGE Request, the MMS Relay/Server shall send an appropriate response [RFC3261] [RFC3428] to the MMS UA.

3.2.5 Retrieval of Multimedia Message

The retrieval of a Multimedia message may be accomplished either before or after the MM1_notification.RES occurs, depending on whether the MMS UA decides to perform an immediate retrieval (see Figure 11) or a deferred retrieval (see Figure 12) of the MM.

Table 11 specifies the mapping of the abstract MM1 Retrieval messages [X.S0016-200] to the appropriate HTTP operations.

Abstract Messages	Mapping	Direction
MM1_Retrieve.REQ	HTTP GET	MMS UA -> MMS Relay/Server
MM1_Retrieve.RES	HTTP 200 OK	MMS Relay/Server -> MMS UA

Table 11 **Mapping of MM1 Retrieval of MM abstract messages**

3.2.5.1 Retrieve of MM Message Flow

The message flow for retrieve of a MM is shown in Figure 16.

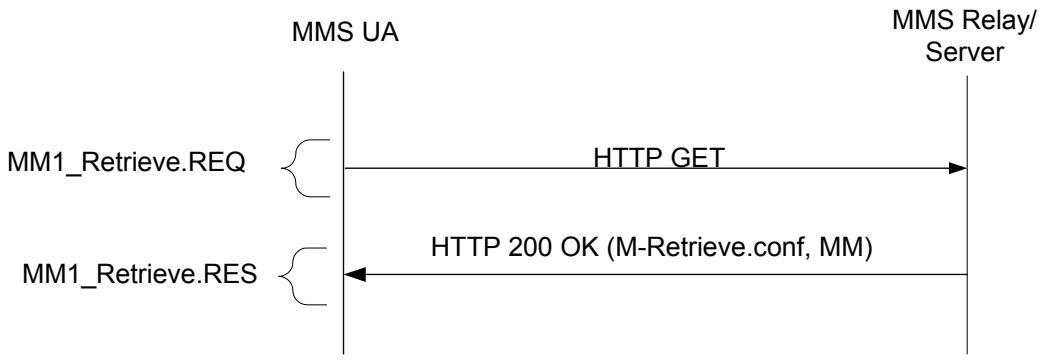

Figure 16 **Retrieval of Multimedia Message**

3.2.5.2 HTTP GET (MMS UA -> MMS Relay/Server)

The MMS UA shall send an HTTP GET [RFC2616] to the MMS Relay/Server containing a URI that indicates the location of the MM to be retrieved.

3.2.5.3 HTTP 200 OK (MMS Relay/Server -> MMS UA)

When successful, the MMS Relay/Server responds with an HTTP 200 OK response that shall contain a M-Retrieve.conf PDU [OMAENC] containing MMS headers and the MM.

If the URI supplied in the HTTP GET can not be resolved, a network or server fault may be returned. For example, if the MMS Relay/Server deletes the MM from the store, making the requested MM unavailable, it is expected that the HTTP GET would generate an HTTP Status Code of 404 (Not Found) [RFC 2616].

3.2.6 Delivery Acknowledgement

If a message acknowledgement is requested, the MMS UA shall respond with a Delivery Acknowledgement to the MMS Relay/Server that supports the specific MMS UA. The message acknowledgement confirms successful message retrieval to the MMS Relay/Server.

Table 12 specifies the mapping of abstract MM1 Delivery Acknowledgement message [X.S0016-200] to the appropriate SIP operation.

Abstract Messages	Mapping	Direction
MM1_Acknowledgement.REQ	SIP MESSAGE request	MMS UA -> MMS Relay/Server

Table 12 **Mapping of MM1 Delivery Acknowledgement abstract message**

3.2.6.1 Delivery Acknowledgement Message Flow

The message flow for Delivery Acknowledgement is shown in Figure 17.

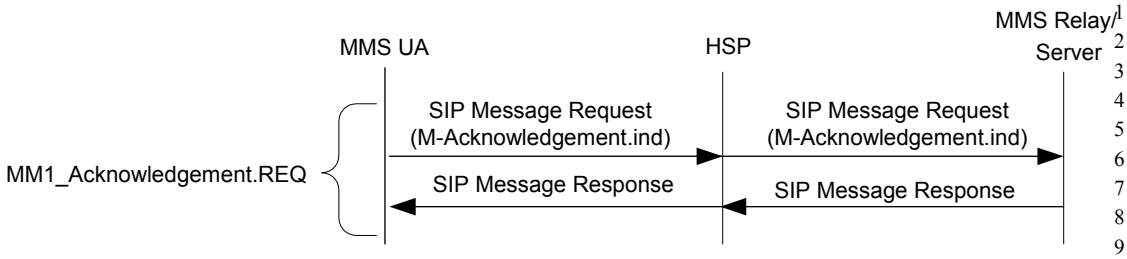

Figure 17 **Delivery Acknowledgement Message Flow**

3.2.6.2 SIP MESSAGE Request (MMS UA -> MMS Relay/Server)

The payload of the SIP MESSAGE Request includes the MIME type application/vnd.wap.mms-message which includes the M-Acknowledgement.ind header fields as described in [OMAENC]. The M-Acknowledgement.ind header fields are encoded according to the binary encoding described in [OMAENC]. Figure 18 shows the SIP MESSAGE Request message structure sent from the MMS UA to the MMS Relay/Server.

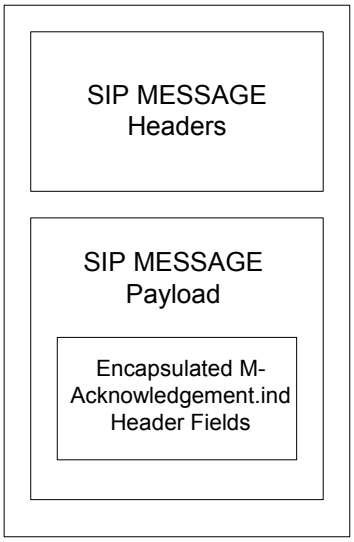

Figure 18 **SIP MESSAGE Request Structure (M-Acknowledgement.ind)**

3.2.6.3 SIP MESSAGE Response (MMS Relay/Server -> MMS UA)

After receiving a SIP MESSAGE Request, the MMS Relay/Server shall send an appropriate response for the SIP MESSAGE Request [RFC3261] [RFC3428] to the MMS UA.

3.2.7 Delivery Reporting

Delivery Reporting informs the originating MMS UA that a message delivery has succeeded. A Delivery Report shall be sent from the MMS Relay/Server to the originator MMS UA when a delivery report has been requested and the recipient MMS Client has not explicitly requested for denial of the report. As for example, the recipient can request for denial of the Delivery Report by using the X-Mms-Report-Allowed field of M-Acknowledge.ind (see Section 3.2.6.2) or M-NotifyResp.ind (see Section 3.2.4.5). There will be a separate delivery report from each recipient.

Table 13 specifies the mapping of the abstract MM1 Delivery Report message [X.S0016-200] to the appropriate SIP operation.

Abstract Messages	Mapping	Direction
MM1_delivery_report.REQ	SIP MESSAGE request	MMS Relay/Server -> MMS UA

Table 13 **Mapping of MM1 Delivery Report abstract message**

3.2.7.1 Delivery Reporting Message Flow

The message flow for Delivery Reporting is shown in Figure 19.

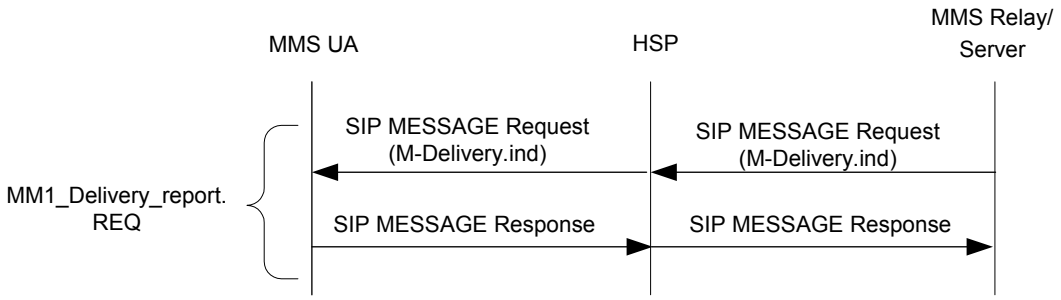

Figure 19 **Delivery Reporting Message Flow**

3.2.7.2 SIP MESSAGE Request (MMS Relay/Server -> MMS UA)

A SIP MESSAGE Request is generated when the MMS Relay/Server is satisfied that it has sufficient information to declare that the MM was delivered or other status can be declared. As such, there may be cases where the MMS Relay/Server makes a decision about the delivery status that may be incorrect (e.g., timer expiry may generate an expiry notice but recipient MMS UA may actually retrieve MM if the read occurred before the MM was deleted).

The payload of the SIP MESSAGE Request includes the MIME type application/vnd.wap.mms-message which includes the M-Delivery.ind header fields as described in [OMAENC]. The M-Delivery.ind header fields are encoded according to the binary encoding described in [OMAENC]. Figure 20 shows the SIP MESSAGE Request message structure sent from the MMS Relay/Server to the MMS UA.

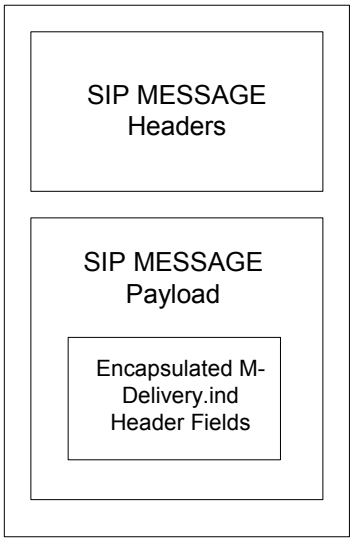

Figure 20 **SIP MESSAGE Request Structure (M-Delivery.ind)**

3.2.7.3 SIP MESSAGE Response (MMS UA -> MMS Relay/Server)

After receiving a SIP MESSAGE Request, the MMS UA shall send an appropriate response [RFC3261] [RFC3428] for the SIP MESSAGE Request to the MMS Relay/Server.

3.2.8 Read Reporting

When the originating MMS UA requests a Read Report for a multimedia message, the receiving MMS UA may send a Read Report message back to it. Table 14 specifies the mapping of abstract MM1 Read Report messages [X.S0016-200] to the appropriate SIP operation.

Abstract Messages	Mapping	Direction
MM1_Read_reply_report_ recipient.REQ	SIP MESSAGE request	MMS UA -> MMS Relay/Server
MM1_Read_reply_report_ Originator.REQ	SIP MESSAGE request	MMS Relay/Server -> MMS UA

Table 14 **Mapping of MM1 Read Report abstract messages**

3.2.8.1 Read Reporting Message Flow

A Read Report originates at the recipient MMS Client and is sent via the recipient MMS Relay/Server to the originating MMS Relay/Server. Upon receiving the Read Report, the originating MMS Relay/Server forwards the Read Report to the originating MMS UA. The message flow for Read Reporting is shown in Figure 21. The details of MM4_read_report.REQ and MM4_read_report.RES are outside the scope of this specification.

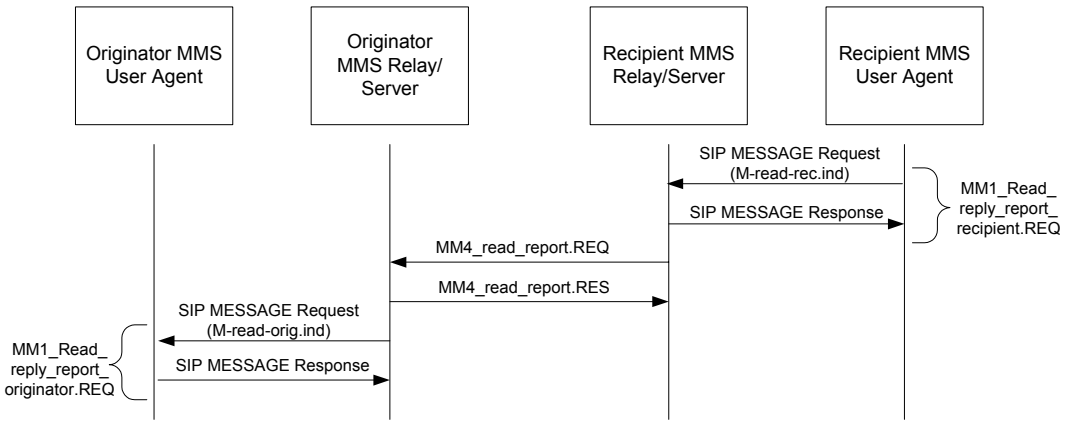

Figure 21 **Read Reporting Message Flow**

3.2.8.2 SIP MESSAGE Request (MMS UA -> MMS Relay/Server)

The payload of the SIP MESSAGE Request includes the MIME type application/vnd.wap.mms-message which includes the M-read-rec.ind header fields as described in [OMAENC]. The M-read-rec.ind header fields are encoded according to the binary encoding described in [OMAENC]. Figure 22 shows the SIP MESSAGE Request message structure sent from the MMS UA to the MMS Relay/Server.

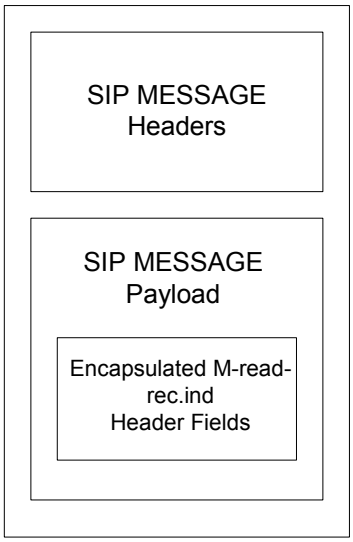

Figure 22 **SIP MESSAGE Request Structure (M-read-rec.ind)**

3.2.8.3 SIP MESSAGE Response (MMS Relay/Server -> MMS UA)

After receiving a SIP MESSAGE Request, the MMS Relay/Server shall send an appropriate response [RFC3261] [RFC3428] for the SIP MESSAGE to the MMS UA.

3.2.8.4 SIP MESSAGE Request (MMS Relay/Server -> MMS UA)

The payload of the SIP MESSAGE Request includes the MIME type application/vnd.wap.mms-message which includes the M-read-orig.ind header fields as described in [OMAENC]. The M-read-orig.ind header fields are encoded according to the binary encoding described in [OMAENC]. Figure

23 shows the SIP MESSAGE Request message structure sent from the MMS Relay/Server to the MMS UA.

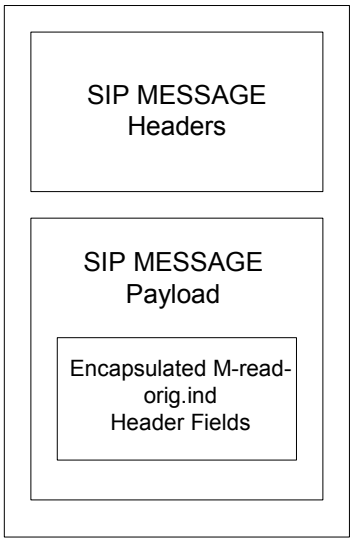

Figure 23 **SIP MESSAGE Request Structure (M-read-orig.ind)**

3.2.8.5 SIP MESSAGE Response (MMS UA -> MMS Relay/Server)

After receiving a SIP MESSAGE Request, the MMS UA shall send an appropriate response [RFC3261] [RFC3428] for the SIP MESSAGE Request to the MMS Relay/Server.

3.3 MMS Security Model

The HSP and the MMS UA shall mutually authenticate all SIP REGISTER Requests. After successful registration, all subsequent SIP messages between the MMS UA and HSP shall be sent using a secure connection (e.g., TLS [RFC2246] as specified in [RFC3261]).

After the MMS UA successfully registers with the HSP, if the MMS Relay/Server is not part of a trusted domain, then the third-party SIP REGISTER Request to the MMS Relay/Server from the HSP (see Section 3.2.1.1.3) shall be mutually authenticated and all subsequent SIP messages between the HSP and the MMS Relay/Server shall be sent using a secure connection (e.g., TLS [RFC2246] as specified in [RFC3261]).

3.3.1 Client Authentication

If client authentication is implemented, it shall be accomplished as described in [RFC3261]. Digest authentication requires a shared secret between the MMS UA and HSP. To avoid a challenge to every SIP Request sent by the client, the HSP might use long-lived nonce values. If a nonce value is re-used for authentication, then the value should be changed periodically (e.g., every 15 minutes or every 100 messages) but this is outside the scope of this specification. If the HSP receives a SIP REGISTER Request that requires authentication, it first checks for the presence of an Authorization header that matches an existing nonce value. If this header field is not present, or if it is present but invalid, or present but using an expired nonce value, the HSP shall challenge the request by sending a 401 (Unauthorized) response to the MMS UA.

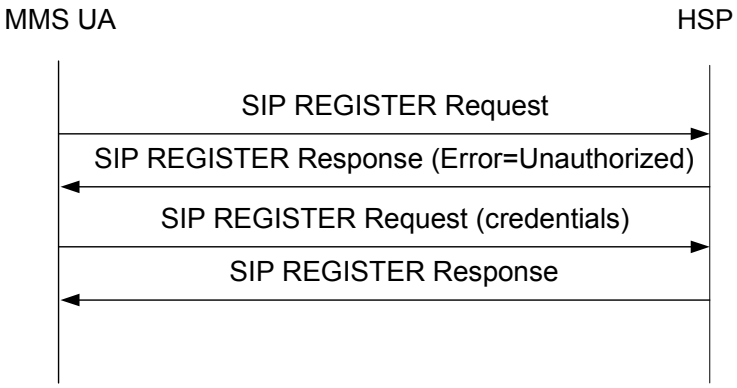

Figure 24 **SIP Registration with MMS UA Authentication**

When a MMS UA that has not previously responded to a digest challenge issues a SIP REGISTER Request, it will not include an Authorization header field. If the MMS UA receives a 401 (Unauthorized) response, it shall re-send the SIP REGISTER Request with an Authorization header that answers the challenge as described in [RFC3261]. When the MMS UA issues subsequent SIP REGISTER Requests and SIP MESSAGE Requests it shall include an Authorization header containing the credentials used when responding to the previous challenge, without waiting for a new challenge. Note that any request that contains a valid Authorization header is authenticated, even if that particular request is not challenged by the HSP.

The HSP should periodically expire the nonce value. The expiration interval is a matter of provider policy, and should be chosen to balance the risk of replay attacks against the message overhead required by digest authentication challenges.

For 3GPP2 IMS [X.P0013.2] and 3GPP IMS [3GPP-23.228] networks the client authentication is based on Digest-AKA as described in [RFC3310].

3.3.2 Server Authentication

If authentication of MMS Relay/Server requests is desired, it may be accomplished using Transport Layer Security [RFC2246] as specified in [RFC3261].

A Sample Application (Informative)

A.1 MMS Direct-Notification Example

This example shows how a message using Direct-Notification is delivered. The actual message is sent as part of F1.

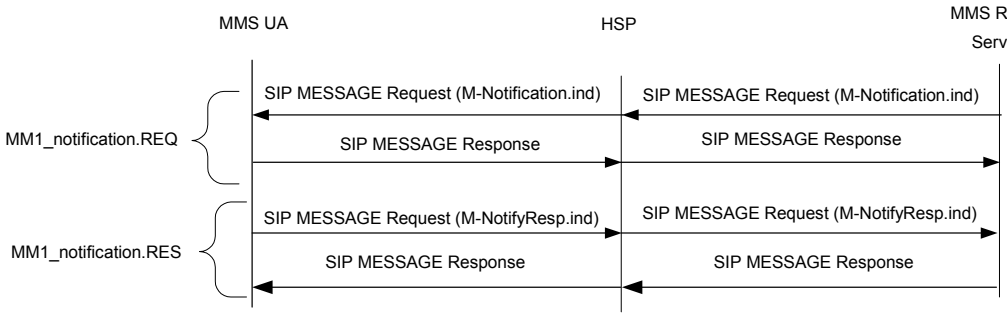

Figure 25 **Direct Notification**

```
F1 MESSAGE  MMS Relay/Server -> MMS UA
   MESSAGE sip:user@example.com SIP/2.0
   Via: SIP/2.0/TCP mms.example.com;branch=z9hG4bK776sgdkse
   Max-Forwards: 70
   From: sip:sender@example.com;tag=49583
   To: sip:user@example.com
   Call-ID: cb03a0s09a2sdfglkj490333
   CSeq: 1 MESSAGE

   Content-Length: NNNN
   Content-Type: Multipart/Related; boundary=example-1
             start="<950120.aaCC@example.com>";
             type=”application/vnd.wap.mms-message”

   --example-1
   Content-Type: application/vnd.wap.mms-message
   Content-ID: 950120.aaCC@example.com

   <…Encoded M-Notification.ind metadata elements…
   X-Mms-Content-Location: cid:94834si4@example.com
   …>

   --example-1

   Content-type: text/html
   Content-Transfer-Encoding: binary
   Content-ID: <cid:94834si4@example.com>

   Hello Watson

   --example-1

F2 200 OK  MMS UA -> MMS Relay/Server
```

```
      SIP/2.0 200 OK
      Via: SIP/2.0/TCP mms.example.com;branch=z9hG4bK776sgdkse;
            received=1.2.3.4
      From: sip:sender@example.com;tag=49394
      To: sip:user@example.com;tag=43kjs8ei
      Call-ID: cb03a0s09a2sdfglkj490333
      CSeq: 1 MESSAGE
      Content-Length: 0

F3 MESSAGE  MMS UA -> MMS Relay/Server
      MESSAGE sip: mms.example.com SIP/2.0
      Via: SIP/2.0/TCP 10.0.0.1;branch=z9hG4bK776sgdidk
      Max-Forwards: 70
      From: sip:user@example.com;tag=94384
      To: sip: mms.example.com
      Call-ID: cb03a0s09a2sdfglkj490333
      CSeq: 1 MESSAGE
      Content-Length: NNNN
      Content-Type: application/vnd.wap.mms-message

      <… M-NotifyResp.ind encoded metadata elements…>


F4 200 OK  MMS Relay/Server -> MMS UA

      SIP/2.0 200 OK
      Via: SIP/2.0/TCP 10.0.0.1;branch=z9hG4bK776sgdidk;
      From: sip:mms. example.com;tag=94384
      To: sip:user@example.com;tag=ab8asdasd9
      Call-ID: cb03a0s09a2sdfglkj490336
      CSeq: 1 MESSAGE
      Content-Length: 0
```

B MM1 SIP Reference Specification (Normative)

B.1 MIME Subtype: vnd.3gpp2.mms.sip

The following subsections define the vnd.3gpp2.mms.sip application subtype.

B.1.1 MIME Registration for application/vnd.3gpp2.mms.sip

MIME media type name: application

MIME subtype name: vnd.3gpp2.mms.sip

Required parameters: none.

Optional parameters: none.

Encoding considerations: This type is only defined for transfer via SIP MESSAGE [RFC3428].

Security considerations: See the Appendix B.1.3 in this document.

Interoperability considerations: none

Published specification: This document.

Applications which use this media: The vnd.3gpp2.mms.sip application subtype supports the exchange of information between a MMS Relay/Server and a MMS UA using SIP as a transport.

Additional information:

1. Magic number(s): N/A
2. File extension(s): N/A
3. Macintosh file type code: N/A

B.1.2 MIME Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in [RFC2234]. The formal syntax for application/vnd.3gpp2.mms.sip is below:

```
message = version
      msg-field
      status-value
      reason-field

version = "Version=" 1*DIGIT CRLF
            ; this document describes version 0

msg-field = "Msg=" msg-type CRLF
msg-type = "Registration"/ "Termination"

msg-status = "Status=" status-type CRLF
status-type = "registered"/"accepted"/"denied"/"terminated"

reason-field = ["Reason ="  msg-reason]
```

```
msg-reason = "congestion"/"accounting"/"identity_not_known"/
             "admin"
```

B.1.3 Security Considerations

Messages using the vnd.3gpp2.mms.sip application subtype should be encrypted and integrity protected using end-to-end mechanisms.

B.2 Clarification of status-type

This section gives more detail about the meaning of the different values that "status-type" (as defined in Appendix B.1.2) and "msg-reason" may have.

status-type	msg-reason	Action by MMS UA
registered	N/A	MMS UA is registered for MMS services.
denied	identity_not_known	MMS UA may attempt to re-register. If the error is repeated the MMS UA may use the information to indicate the error to the user. The MMS UA should take no further action. MMS UA assumes that MMS services are not available.
denied	accounting	The MMS UA may use the information to indicate the error to the user. MMS UA assumes that MMS services are not available.
denied	congestion	If msg-type=Registration the MMS UA should attempt re-registration after some period of time. MMS UA assumes that MMS services are not available.
terminated	accounting	The MMS UA may use the information to indicate the error to the user. MMS UA assumes that MMS services are not available.
terminated	admin	No action by MMS UA. MMS UA assumes that MMS services are not available.

Table 15 **Status Actions**