

Mapping Between the Multimedia Messaging Service (MMS) and Internet Mail

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed and any of which I become aware will be disclosed, in accordance with [RFC 3668](#) ([BCP 79](#)).

By submitting this Internet-Draft, I accept the provisions of [Section 3 of RFC 3667](#) ([BCP 78](#)).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt> The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

The cellular telephone industry has defined a service known as the Multimedia Messaging Service (MMS). This service uses formats and protocols which are similar to, but differ in key ways from those used in Internet mail.

This document specifies how to exchange messages between these two services, including mapping information elements as used in MMS X-Mms-* headers as well as delivery and disposition reports, to and from that used in ESMTP and Internet message headers.

Table of Contents

1	Introduction	3
1.1	Scope	3
1.2	Conventions Used in this Document	4
1.3	Definitions	4
1.4	Abbreviations	5
1.5	Assumptions	6
2	Mapping Between MMS and Internet Mail	6
2.1	Mapping Specification	6
2.1.1	MMS to Internet Mail	6
2.1.2	Internet Mail to MMS	7
2.1.3	MMS Information Element Mappings	7
2.1.3.1	Table 1: MM3 Mappings	8
2.1.3.2	Conversion of messages from MMS to Internet format	10
2.1.3.2.1	Table 2: Importance Mappings (MMS to Internet	14
2.1.3.2.2	Table 3: X-Priority Mappings (MMS to Internet	14
2.1.3.3	Conversion of messages from Internet to MMS format	17
2.1.3.3.1	Table 4: Priority Mappings (Internet Message t	18
2.1.4	Report Generation and Conversion	20
2.1.4.1	Delivery Report Mapping from MMS to Internet Messa	20
2.1.4.1.1	Table 5: Delivery Report Mappings (MMS to Inte	21
2.1.4.2	Delivery Report Mapping from Internet Message to M	22
2.1.4.2.1	Table 6: Delivery Report Mappings (Internet Me	23
2.1.4.3	Read Report Mapping from MMS to Internet Message .	24
2.1.4.3.1	Table 7: Read Report Mappings (MMS to Internet	25
2.1.4.4	Disposition Report Mapping from Internet Message t	26
2.1.4.4.1	Table 8: Disposition Report Mappings (Internet	26
2.1.5	Message Delivery	27
3	Security Considerations	27
4	Normative References	29
5	Informative References	30
6	Author's Address	31
	Intellectual Property Statement	31
	Full Copyright Statement	32
	Disclaimer	32

[1](#) Introduction[1.1](#) Scope

This document describes how to exchange messages with Internet mail systems. This includes translation between MMS (as defined by 3GPP/3GPP2/OMA) and Internet Mail messages using Extended Simple Mail Transfer Protocol [[SMTP](#)] and Internet message format [[Msg-Fmt](#)].

This also includes translation between delivery and disposition reports as used in MMS and in Internet mail ([[DSN-Msg](#)] and [[MDN](#)]).

Gellens

[Page 3]

Expires October 2005

Internet Draft

Mapping Between MMS and Internet Mail

April 2005

The MMS architecture [[Stage 2](#)] and specifications [[Stage 3](#)] refer to interfaces as reference points named MMx. For example, MM1 is the client-server interface, MM4 is the server-server interface, and MM3 is an interface to "external" or non-MMS systems. The specification in this document can be used for message exchange between any system which uses Internet Message formats and protocols and an MMS system; from the perspective of the MMS system, reference point MM3 is used.

This document includes support for voice messages specified by the Voice Profile for Internet Mail [[VPIM](#)]. The VPIM specification allows voice messages to be exchanged between voice mail systems using Internet mail format [[Msg-Fmt](#)] and transported via Extended Simple Mail Transfer Protocol [[SMTP](#)]. Thus, the MMS MM3 interface supports the ability to exchange voice messages between an MMS system and a voice mail system. Note that such use is distinct from voice media being part of a user-composed multimedia message.

Note that MM3 can also be used for interworking with "external" (non-MMS) systems other than Internet mail, such as Short Messaging Service (SMS) and access to external mail stores (such as a voice mail system). This specification does not address these other uses or sub-interfaces of MM3; it is only concerned with Internet mail interworking and specifically exchange of messages.

All MM3 Stage 2 [[Stage 2](#)] functions are supported except for reply charging and sender address hiding, which may be addressed in future extensions.

[1.2](#) Conventions Used in this Document

The key words "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [[KEYWORDS](#)].

Note that in the text of this document, a distinction is made between use of "SMTP" or "Simple Mail Transfer Protocol", and "ESMTP" or "Extended Simple Mail Transfer Protocol": when the term "ESMTP" or "Extended" is used, it indicates use of extended features of SMTP; that is, those beyond the facilities of [RFC 821](#). (These extended facilities may be in [RFC 2821](#) or in other RFCs, as

indicated by the specific RFC reference used; note that the name of the [RFC 2821](#) reference is "SMTP" because that is the official title of the RFC.)

Gellens

[Page 4]

Expires October 2005

Internet Draft

Mapping Between MMS and Internet Mail

April 2005

[1.3](#) Definitions

-----	-----
Anonymous Remailer	A service which accepts messages and resends them to their intended recipient, masking information about the original sender.
-----	-----
Body	The portion of an SMTP message's Content following the Header (that is, following the first blank line). The Body may contain structured parts and sub-parts, each of which may have their own Header and Body. The Body contains information intended for the message recipient (human or software).
-----	-----
Content	The portion of an SMTP message that is delivered. The Content consists of a Header and a Body.
-----	-----
Disposition Report	Feedback information to an originator User Agent by a recipient User Agent about
Message Disposition Notification	handling of an original message. This may include notification that the message was or was not read, was deleted unread, etc.
-----	-----
Envelope	The portion of an SMTP message not included in the Content; that is, not in the Header nor in the Body. Envelope information only exists while the message is in transit, and contains information used by SMTP agents (MTAs).
-----	-----
Header	The first part of an SMTP message's Content. The Header is separated from the Body by a blank line. The Header consists of Fields (such as "To:"), also known as Header Fields or Headers. The message Header contains information used by User Agents.
-----	-----

Gateway Function	An agent which acts as both MMSC and MTA and/or MSA.
-----	-----
User Agent	An MMS or Email user agent
-----	-----

Gellens [Page 5] Expires October 2005

Internet Draft Mapping Between MMS and Internet Mail April 2005

1.4 Abbreviations

-----	-----
ESMTP	Extended Simple Mail Transfer Protocol. The use of features and capabilities added to SMTP since RFC 821 .
-----	-----
MSA	Message Submission Agent. A server which accepts messages from User Agents and processes them; either delivering them locally or relaying to an MTA.
-----	-----
MTA	Mail Transfer Agent. A server which implements [SMTP] .
-----	-----

1.5 Assumptions

It is assumed that the reader is already familiar with the contents of the 3GPP2 MMS Specification Overview [\[Overview\]](#), MMS Stage 1 (requirements) [\[Stage 1\]](#) and Stage 2 (architecture and abstract messages) [\[Stage 2\]](#), and 3GPP/3GPP2 Stage 3 (protocols) [\[Stage 3\]](#) documents. It is also assumed that the reader is familiar with Internet mail, especially [RFC 2821](#) [\[SMTP\]](#) and [RFC 2822](#) [\[Msg-Fmt\]](#).

2 Mapping Between MMS and Internet Mail

This section defines the interworking between MMS Relay/Servers and External Servers using native ESMTP. That is, information elements are exchanged using standard Internet Message [\[Msg-Fmt\]](#) header fields and standard [\[SMTP\]](#) elements.

SMTP and Internet mail extensions are used for features such as delivery reports, message expiration, discovery of server support for optional features, etc.

2.1 Mapping Specification

2.1.1 MMS to Internet Mail

When sending a message to an Internet mail system the MMS Relay/Server MUST convert the MM if required, and MUST comply with the requirements of [\[SMTP\]](#) (for example, use of a null return-path for automatically-generated messages).

The MMS Relay/Server SHOULD use the information elements associated with the MM to define the control information (Internet Message header fields and ESMTP values) needed for the transfer protocol.

Gellens

[Page 6]

Expires October 2005

Internet Draft

Mapping Between MMS and Internet Mail

April 2005

[Section 2.1.3](#) lists the mappings between X-Mms-* headers and Internet Message header fields and ESMTP values.

Delivery and read report MMs SHOULD be converted to standard Internet Message report format (multipart/report). In addition to converting Internet Message reports, the MMS Relay/Server MUST generate delivery and read report MMs for received messages as appropriate. See [section 2.1.4](#) for more information.

2.1.2 Internet Mail to MMS

When receiving a message from an Internet mail system the MMS Relay/Server MAY convert incoming messages to the MM format used within the receiving system.

The MMS Relay/Server MAY convert control information received from the Internet mail server into appropriate information elements of an MM.

[Section 2.1.3](#) lists the mappings between X-Mms-* headers and Internet Message header fields and ESMTP values.

Standard Internet Message report format (multipart/report) messages MAY be converted to delivery or read report MMs, as appropriate. In addition to converting report MMs, the MMS Relay/Server MUST generate standard Internet Message delivery and disposition reports for received Internet messages as appropriate. See [section 2.1.4](#) for more information.

2.1.3 MMS Information Element Mappings

The mappings between MMS elements and ESMTP/Internet Message elements (either [\[SMTP\]](#) parameters, [\[Msg-Fmt\]](#) headers, or both) are summarized in the table below, and detailed in subsequent sections. The "MMS Headers" are from [\[OMA-MMS\]](#). Note that only information elements which need to be mapped are listed. [\[Msg-Fmt\]](#) headers not listed here SHOULD be passed unaltered

2.1.3.1 Table 1: MM3 Mappings

Information Elem	[SMTP] Element	[Msg-Fmt] Header	MMS Header
3GPP MMS Version	N/A	N/A	X-Mms-Version:
Message Type (of PDU)	N/A	N/A	X-Mms-Message- Type:
Transaction ID	N/A	N/A	X-Mms-Transact ion-Id:
Message ID	ENVID [DSN-SMTP]	Message-ID:	X-Mms-Message- Id: Message-ID:

Recipient address(es)	RCPT TO address(es)	To:, Cc:, or omitted (Bcc)	To:, Cc:, Bcc:
Sender's address	MAIL FROM address if user-originated; MUST set MAIL FROM to null ("<>") for all automatically-generated MMs	From: (MAY set to locally-generated value to hide sender identity)	From:
Content type	N/A	Content-Type: For voice messages compliant to VPIM , see Note 2	Content-type:
=====	=====	=====	=====

=====	=====	=====	=====
Information Elem	RFC 2821 Element	RFC 2822 Header	MMS Header
=====	=====	=====	=====
Message class	Class=auto: MUST set MAIL FROM to null ("<>").	MAY set 'Precedence: bulk' on class=auto	X-Mms-Message-Class:
Date and time of submission	N/A	Date:	Date:
Time of expiry	DELIVER-BY [Deliver-By]	N/A	X-Mms-Expiry:
Earliest delivery time	(only for submission; not relay)	N/A	X-Mms-Delivery-Time:
Delivery report request	DSN [DSN-SMTP] SHOULD also specify recipient address as ORCPT; SHOULD	N/A	X-Mms-Delivery-Report:

	also specify ENVID		
Importance (a/k/a "priority")	N/A	Importance: X-Priority:	X-Mms- Priority:
Sender visib- ility	N/A	N/A	X-Mms-Sender- Visibility:
Read reply request	N/A	Disposition- Notification -To: MDN	X-Mms-Read- Reply:
Reply-charging permission	(not currently supported)	(not currently supported)	X-Mms-Reply- Charging:
Reply-charging permission deadline	(not currently supported)	(not currently supported)	X-Mms-Reply- Charging- Deadline:
Reply-charging permission limitation	(not currently supported)	(not currently supported)	X-Mms-Reply- Charging- Size:
=====	=====	=====	=====

Information Elem	RFC 2821 Element	RFC 2822 Header	MMS Header
Reply-charging usage request	(not currently supported)	(not currently supported)	X-Mms-Reply- Charging- Id:
Reply-charging usage reference	(not currently supported)	(not currently supported)	X-Mms-Reply- Charging:
Subject	N/A	Subject:	Subject:
Forward counter	N/A	Resent-Count:	(Not sup- ported)
Previously-sent- by	N/A	Resent-From:	X-Mms-Previous ly-Sent-By:

Previously-sent-date and-time	N/A	Resent-Date:	X-Mms-Previously-Sent-Date:
Hop/host trace	N/A	Received:	(Not supported)
Sensitivity	N/A	Sensitivity: see Note 1	N/A
Content	N/A	<message body>	<message body>
=====	=====	=====	=====

Note 1: The [\[VPIM\]](#) 'Sensitivity' header element indicates the privacy requested by the message originator (values are "personal" or "private"); a message recipient MUST NOT forward a message with a 'Sensitivity' header.

Note 2: A MIME-Version header with a comment of "Voice 2.0" indicates that the voice message conforms to [\[VPIM\]](#).

2.1.3.2 Conversion of messages from MMS to Internet format

3GPP MMS Version

The 'X-Mms-Version:' header, if present, SHOULD be removed.

Gellens

[Page 10]

Expires October 2005

Internet Draft

Mapping Between MMS and Internet Mail

April 2005

Message Type (of PDU)

The 'X-Mms-Message-Type:' header, if present, SHOULD be removed.

Transaction ID

The 'X-Mms-Transaction-Id:' header, if present, SHOULD be removed.

Message ID

An 'X-Mms-Message-Id:' header, if present, SHOULD be retained.

The 'Message-Id:' header MUST be retained. If not present it MUST be created, with a unique value. If an 'X-Mms-Message-Id:' header

is present and a 'Message-Id:' header is not, the value of the 'X-Mms-Message-Id:' header MAY be used in creating the 'Message-Id:' header.

The message ID SHOULD be transmitted in the ESMTP envelope as the ENVID parameter, as specified in [[DSN-SMTP](#)].

Recipient(s) address

The address of each recipient MUST be transmitted in the SMTP envelope as a RCPT TO value. All disclosed recipients SHOULD also appear in a 'To:' or 'Cc:' header. At least one 'To:' or 'Cc:' header MUST be present. If all recipients are undisclosed, a 'To:' header MAY be created that contains a comment, for example 'To: (undisclosed recipients)'. The 'To:' header SHOULD NOT appear more than once. The 'Cc:' header SHOULD NOT appear more than once.

Each recipient address MUST obey the length restrictions per [[SMTP](#)].

Current Internet message format requires that only 7-bit US-ASCII characters be present in addresses. Other characters (for example, non-7-bit characters in a phrase part of an address header) MUST be encoded according to [[Hdr-Enc](#)]. Note that it would be possible to define an SMTP extension to permit transmission of unencoded 8-bit characters, but in the absence of such an extension [[Hdr-Enc](#)] MUST be used.

Sender address

The address of the message sender SHOULD appear in the 'From:' header, unless address hiding has been requested. If address hiding has been requested, the 'From:' header MAY contain a comment to this effect, for example, 'From: (anonymous sender)'.

The address of the message sender for all user-generated messages ('X-Mms-Message-Class: Personal') SHOULD be transmitted in the SMTP envelope as the MAIL FROM value unless address hiding has been requested and the receiving server is not known and trusted to support address hiding.

The 'From:' header and the MAIL FROM value MAY be set to a locally-generated value to hide the sender identity in anonymous messages when the receiving system does not support anonymous messages. Locally generated addresses MAY be internally mapped to

the actual address to allow replies to anonymous messages, but such mapping is beyond the scope of this specification, as is a mechanism for discovering and requesting support for anonymous messages.

Because of the risk of mail loops, it is critical that the MAIL FROM be set to null ("<>") for all automatically-generated MMs (such as 'X-Mms-Message-Class: Auto'). The MAIL FROM value MUST be set to null for all automatically-generated messages. This includes reports, "out-of-office" replies, etc.

Current Internet message format requires that only 7-bit US-ASCII characters be present in addresses. Other characters (for example, non-7-bit characters in a phrase part of an address header) MUST be encoded according to [[Hdr-Enc](#)]. Note that it would be possible to define an SMTP extension to permit transmission of unencoded 8-bit characters, but in the absence of such an extension [[Hdr-Enc](#)] MUST be used.

The sender address MUST obey the length restrictions of [[SMTP](#)].

Content type

The 'Content-Type:' header SHOULD be preserved. Content types not in widespread use in the Internet MAY be converted into those that are, when such conversion can be done without significant loss of content. For example, SMIL messages MAY be converted into widely-supported multipart/related with multipart/html. When such conversion is done, the 'Content-Type:' header MUST be updated if it is no longer correct.

Message class

The 'X-Mms-Message-Class:' header MAY be retained. A 'Precedence: bulk' header MAY be inserted for class=auto or class=advertisement. See 'Sender Address' above. (Class=personal and class=informational do not require special handling.)

Time of Expiry

The 'X-Mms-Expiry:' header, if present, SHOULD be removed.

The remaining time until the message is considered expired SHOULD be transmitted in the ESMTP envelope by using the DELIVER-BY extension,

as specified in [[Deliver-By](#)].

Note that the ESMTP DELIVER-BY extension carries time remaining until expiration; each server decrements the value by the amount of time it has possessed the message. The 'X-Mms-Expiry:' header may contain either the absolute time at which the message is considered expired or the relative time until the message is considered expired.

Earliest delivery time

The 'X-Mms-Delivery-Time:' header, if present, SHOULD be removed.

Future delivery is a message submission, not message relay feature.

Delivery report request

Requests for delivery status notifications (DSNs) SHOULD be transmitted in the ESMTP envelope by using the DSN extension as specified in [[DSN-SMTP](#)] to request "success" or "none" notification (depending on the value of the 'X-Mms-Delivery-Report' header). When the NOTIFY extension is used, the unaltered recipient address SHOULD be transmitted as the ORCPT value, and the original message ID SHOULD be transmitted as the ENVID value.

The 'X-Mms-Delivery-Report:' header, if present, SHOULD be removed.

Importance

The message sender's importance value (also called "priority", although this can be confused with class-of-service values) SHOULD be transmitted using an 'Importance:' header (although currently not all Internet mail clients support this header).

An 'X-Priority:' header MAY be used in addition. Although not standardized, most email applications support the 'X-Priority:' header, and use an 'X-Priority' value of 3 for messages with "normal" priority. More important messages have lower values and less important messages have higher values. In most cases, urgent messages have an X-Priority value of 1.

Suggested mappings:

[2.1.3.2.1](#) **Table 2:** Importance Mappings (MMS to Internet Message)

----- -----
'X-Mms-Priority: High' 'Importance: High'
----- -----
'X-Mms-Priority: Normal' [omit]
----- -----
'X-Mms-Priority: Low' 'Importance: Low'
----- -----

Normal priority messages should omit the 'Importance:' header.

[2.1.3.2.2](#) **Table 3:** X-Priority Mappings (MMS to Internet Message)

----- -----
'X-Mms-Priority: High' 'X-Priority: 2 (high)'
----- -----
'X-Mms-Priority: Normal' [omit]
----- -----
'X-Mms-Priority: Low' 'X-Priority: 4 (low)'
----- -----

Normal priority messages SHOULD omit the 'X-Priority:' header.

The 'X-Mms-Priority:' header, if present, SHOULD be removed.

Sender visibility

Support for sender address hiding is not included in this version of the mapping document.

The 'X-Mms-Sender-Visibility:' header, if present, SHOULD be removed.

Read reply request

A request for a read reply SHOULD be transmitted using a 'Disposition-Notification-To:' header as specified in [[MDN](#)].

The 'X-Mms-Read-Reply:' header, if present, SHOULD be removed.

Reply-charging

Reply charging permission and acceptance are complex issues requiring both user agent and server support. Misapplied reply charging may cause incorrect billing. Until the security issues have been properly addressed, reply charging SHOULD NOT be honored

when using this interface.

The 'X-Mms-Reply-Charging:', 'X-Mms-Reply-Charging-Deadline:', 'X-Mms-Reply-Charging-Size:', and 'X-Mms-Reply-Charging-Id:' headers MAY be removed. Messages containing a reply-charging usage request ('X-Mms-Reply-Charging-Id:' and 'X-Mms-Reply-Charging: accepted' or 'X-Mms-Reply-Charging: accepted (text only)' headers) SHOULD be rejected.

Subject

The 'Subject:' header MUST be preserved. Current Internet message format requires that only 7-bit US-ASCII characters be present. Other characters must be encoded according to [\[Hdr-Enc\]](#). Note that it would be possible to define an SMTP extension to permit transmission of unencoded 8-bit characters, but in the absence of such an extension [\[Hdr-Enc\]](#) must be used.

Resending/Forwarding

In MMS a message may be resent or forwarded, the difference being that if the message has been downloaded then sending it to another address is considered forwarding, while sending a message that has not been downloaded is considered to be resending.

In Internet mail there are two primary ways of sending a previously received message to a new recipient: forwarding and resending. Forwarding is when a user creates a new message containing the original message, either simply embedded within the text, or delineated. Embedded messages generally have each original line preceded by a quote symbol ('>'), surround the original text with a preceding and trailing line which starts with hyphens as per [\[Msg-Encap\]](#), such as '--- begin forwarded text' and '--- end forwarded text', or encapsulate the original message as a 'message/rfc822' content type, perhaps within a 'multipart/mixed' message. (This last method offers more robust delineation.) Resending is when the original message is unaltered except for the addition of 'Resent-' headers to explain the resending to the new recipient.

A message may be resent more than once; each time new 'Resent-' headers SHOULD be added at the top of the message. Thus, if more than one series of 'Resent-' headers are present, the original series is the last; the most recent is the first.

Forward counter

The 'Resent-Count:' header MAY be used to track the number of times the message has been resent. Note that loop control is often done by counting 'Received' headers, which are more general than 'Resent-' headers.

Previously-sent Information

A 'Resent-From:' header MAY be added to indicate the address of the user who directed the message to be resent.

A 'Resent-Date:' header SHOULD be added to indicate the time and date that the message was resent.

Any 'X-Mms-Previously-Sent-By:' and 'X-Mms-Previously-Sent-Date' headers, if present, SHOULD be removed. The information contained in them SHOULD be translated into 'From:', 'Resent-To:', 'Resent-From:', 'Resent-Date:', and 'Resent-Count:' headers. The original sender of the message SHOULD appear in the 'From:' header; the original recipient(s) SHOULD appear in the 'To:' header; the time and date the message was originally sent SHOULD appear in the 'Date:' header. The most recent sender SHOULD appear in the top-most 'Resent-From:' header; the most recent recipient(s) SHOULD appear in the top-most 'Resent-To:' header; the time and date the message was most recently sent SHOULD appear in the top-most 'Resent-Date:' header.

'Received:' Headers

Each system that processes a message SHOULD add a 'Received:' header as per [\[SMTP\]](#). A message MAY be rejected if the number of 'Received:' headers exceeds a locally-defined maximum, which MUST conform to [\[SMTP\] section 6.2](#) and SHOULD be no less than 100.

Privacy

Note that MMS systems do not currently support the 'Privacy' header field as described by [\[VPIM\]](#).

Content

The message content appears in the message body. Note that Internet message format requires that line-endings be encoded as CR LF, thus charset encodings that do not have this property cannot be used in text/* body parts. (They MAY be used in other body parts, but only when they are suitable encoded or when binary transmission has been negotiated.) In particular, MMS allows UTF-16, while Internet

message format does not. UTF-16 encoding MUST be translated to UTF-8 or another charset and encoding which is suitable for use in Internet message format/protocols.

Gellens

[Page 16]

Expires October 2005

Internet Draft

Mapping Between MMS and Internet Mail

April 2005

2.1.3.3 Conversion of messages from Internet to MMS format

3GPP MMS Version

An 'X-Mms-Mms-Version:' header SHOULD be added.

Message Type (of PDU)

An 'X-Mms-Message-Type:' header SHOULD be used in accordance with the specific MMS interface (e.g., MM1, MM4).

Transaction ID

An 'X-Mms-Transaction-Id:' header SHOULD be used in accordance with the specific MMS interface (e.g., MM1, MM4).

Message ID

The 'Message-Id:' header MUST be retained. If not present it MUST be created, with a unique value. If the 'Message-Id:' header does not exist, but the SMTP envelop contains an ENVID value (as specified in [[DSN-SMTP](#)]), it MAY be used to construct the value.

Recipient(s) address

'To:' and 'Cc:' headers MUST be retained.

Each recipient contained in the SMTP envelope (RCPT TO values) MUST be considered a recipient of the message. Recipients who appear in address headers but not the SMTP envelope MUST be ignored.

Recipients who appear in the [[SMTP](#)] envelope but do not appear in headers are considered "blind" (Bcc) recipients; such recipients MUST NOT be added to message headers (including address and trace headers) unless there is only one recipient total.

Sender address

The 'From:' header MUST be retained.

Content type

The complete 'Content-Type:' header (including any parameters)

SHOULD be preserved.

Message class

Gellens

[Page 17]

Expires October 2005

Internet Draft

Mapping Between MMS and Internet Mail

April 2005

An X-Mms-Message-Class: personal' header SHOULD be created for all received messages with a non-null return path (MAIL FROM value in the SMTP envelope). An X-Mms-Message-Class: auto' header MAY be created for messages with a null return path.

Time of Expiry

An 'x-Mms-Expiry:' header SHOULD be created if the message contains a relative time to expiration in the DELIVER-BY extension, as specified in [[Deliver-By](#)].

Earliest delivery time

An 'X-Mms-Delivery-Time:' header SHOULD NOT be created. If a message arrives via ESMTP relay containing an earliest time of delivery in the AFTER extension, it MAY be rejected. If a message is submitted via Message Submission [[Submission](#)] containing an earliest time of delivery in the AFTER extension, it MUST either be retained until the delivery time arrives, or it may be immediately rejected. It MUST NOT be delivered or further relayed prior to the delivery time.

Delivery report request

An 'X-Mms-Delivery-Report:' header SHOULD be created for messages which request 'success' or 'none' delivery status notification by use of the DSN extension as specified in [[DSN-SMTP](#)]. Requests for 'delay' notifications or non-default actions, such as that only the message headers should be returned, cannot be mapped onto MMS headers and thus SHOULD be ignored.

Priority

An 'X-Priority:' or 'Importance:' header, if present, SHOULD be replaced with an 'X-Mms-Priority:' header. Suggested mappings:

[2.1.3.3.1](#) **Table 4:** Priority Mappings (Internet Message to MMS)

-----	-----
'X-Priority: 1 (highest)'	'X-Mms-Priority: High'
-----	-----
'X-Priority: 2 (high)'	'X-Mms-Priority: High'
-----	-----
'Importance: High'	'X-Mms-Priority: High'
-----	-----
'X-Priority: 3 (normal)'	[omitted]
-----	-----
'Importance: Normal'	[omitted]
-----	-----

Gellens

[Page 18]

Expires October 2005

Internet Draft

Mapping Between MMS and Internet Mail

April 2005

'X-Priority: 4 (low)'	'X-Mms-Priority: Low'
-----	-----
'Importance: Low'	'X-Mms-Priority: Low'
-----	-----
'X-Priority: 5 (lowest)'	'X-Mms-Priority: Low'
-----	-----

Normal priority messages SHOULD omit the 'X-Mms-Priority:' header.

Sender visibility

Support for sender address hiding is not currently supported.

Read reply request

A request for a read reply contained in a 'Disposition-Notification-To:' header as specified in [[MDN](#)] SHOULD be replaced with an 'X-Mms-Read-Reply:' header.

Subject

The 'Subject:' header MUST be preserved.

Resending/Forwarding

One or more sets of 'Resent-' headers, if present, SHOULD be mapped to 'To:', 'From:', 'Date:', and 'X-Mms-Previously-Sent-' headers.

'Received:' Headers

Each system that processes a message SHOULD add a 'Received:' header as per [[SMTP](#)]. A message MAY be rejected if the number of 'Received:' headers exceeds a locally-defined maximum, which MUST conform to [[SMTP](#)] [section 6.2](#) and SHOULD be no less than 100.

Sensitivity

The 'Sensitivity:' header field (value = "personal" or "private") [[VPIM](#)] indicates the desire of a voice message originator to send the message contents to the original recipient list with assurance that the message will not be forwarded further by either the messaging system or the actual message recipient(s). Since sensitivity is not an MMS feature, any messages which contain a 'Sensitivity:' header SHOULD NOT be sent to an MMS system. An appropriate extended error response code [[RESP](#)] SHOULD be used in the associated negative delivery status report.

Gellens

[Page 19]

Expires October 2005

Internet Draft

Mapping Between MMS and Internet Mail

April 2005

Content

The message content appears in the message body.

[2.1.4](#) Report Generation and Conversion

Internet Message systems use the multipart/report MIME type for delivery and disposition reports (often called "read reports") as specified in [[Report-Fmt](#)]. This format is a two- or three-part MIME message; one part is a structured format describing the event being reported in an easy-to-parse format. Specific reports have a format which is built on [[Report-Fmt](#)]. Delivery reports are specified in [[DSN-Msg](#)]. Message disposition reports, which include read reports, are specified in [[MDN](#)].

By contrast, MMS reports are plain text, with no defined structure specified. This makes it difficult to convert from an MMS report to a standard Internet report.

An MMS Relay/Server supporting Internet Message exchange using MM3 MUST convert reports received from one side (MMS or Internet mail) destined for the other. In addition, reports MUST be generated as appropriate for messages received from either side of the MM3 interface. For example, if an MM to be sent via MM3 is not deliverable, a delivery status MM shall be generated. Likewise, if an Internet message is received via MM3 that cannot be further relayed or delivered, a delivery status report [[DSN-Msg](#)] MUST be generated.

When creating delivery or disposition reports from MMS reports, the MMS report should be parsed to determine the reported event and time, status, and the headers of the referenced (original) message. These elements, once determined, are used to populate the subparts of the delivery or disposition report. The first subpart is of type text/plain, and contains a human-readable explanation of the event. This text may include a statement that the report was synthesized based on an MMS report. The second subpart is of type report/delivery-status (for delivery reports) or report/disposition-notification (for disposition reports). This second part contains a structured itemization of the event. The third subpart is of type message/rfc822 and includes the headers and optionally the body of the referenced (original) message.

2.1.4.1 Delivery Report Mapping from MMS to Internet Message

Gellens [Page 20] Expires October 2005

Internet Draft Mapping Between MMS and Internet Mail April 2005

The following table maps information elements from MMS delivery reports to the format specified in [DSN-Msg].

2.1.4.1.1 Table 5: Delivery Report Mappings (MMS to Internet Message)

Information Element	MMS Delivery Report Elem	[DSN-Msg] Element
ID of message whose delivery status is being reported	Message-Id:	'Original-Envelope-ID' field of per-message fields (use value of ENVID from ESMTP envelope if available, 'Message-ID:' otherwise).
Recipient address of the original message (object of delivery report)	From:	'Final-Recipient' field of the per-recipient section
Destination address of report	To:	'To:' header field value of top-level. Value taken from [SMTP] envelope return-path of message being reported, not its 'From:' header field.

-----	-----	-----
Date and time the message was handled	Date:	'Date:' header field value of top-level
=====	=====	=====

Gellens [Page 21] Expires October 2005

Internet Draft Mapping Between MMS and Internet Mail April 2005

=====	=====	=====
Information Element	MMS Delivery	[DSN-Msg] Element
	Report Elem	
=====	=====	=====Delivery
status of X-Mms-original message	Action and Status fields of Status:	per-recipient section.
		The 'Action' field indicates if the message was delivered.
		For failed delivery an appropriate 'Status' value shall be included per [DSN-Msg].
		The Action field is set to one of the following values:
		* delivered (used for MMS status values 'retrieved' and 'rejected', depending on 'Status' code).
		* failed (used for MMS status values 'expired' and 'unreachable')

		* delayed MAY be used for MMS
		status value 'deferred'
		* relayed (used for MMS status
		value 'indeterminate')
		* expanded (SHOULD NOT be used)
-----	-----	-----
Status Text		Text in first part (human-readable
		part)
-----	-----	-----

When an MMS Relay/Server generates a [DSN-Msg] in response to a message received using [SMTP] on MM3:

* Top-level header field 'To:' SHOULD be the [SMTP] return-path of the message whose status is being reported.

* Top-level header field 'From:' SHOULD be the address of the recipient that the delivery-report concerns.

* The first part of the [DSN-Msg] SHOULD include the MM Status Text field that would have been generated for an MM1 delivery-report.

Gellens [Page 22] Expires October 2005

Internet Draft Mapping Between MMS and Internet Mail April 2005

2.1.4.2 Delivery Report Mapping from Internet Message to MMS

The following table maps information elements from a delivery report as specified in [DSN-Msg] to the format of an MMS delivery report.

2.1.4.2.1 Table 6: Delivery Report Mappings (Internet Message to MMS)

=====	=====	=====
Information Element	MMS Delivery	[DSN=Msg] Element
	Report Element	
=====	=====	=====
ID of the original	Message-Id:	'Original-Envelope-ID' field of
message (object of		per-message fields. If not
delivery report)		available, the 'Message-ID'
		header field of the message
		being reported, if included in
		the third part, may be
		substituted.

-----	-----	-----
Recipient address of the original message (object of delivery report)	From:	If available, the 'Original-Recipient' field of the per-recipient section should be used; otherwise the 'Final-Recipient' field of the per-recipient section is used
-----	-----	-----
Destination address of report	To:	'To:' header field value of top-level.
		Value taken from [SMTP] envelope return-path of message being reported, not its 'From:' header field.
=====	=====	=====

=====	=====	=====
Information Element	MMS Delivery Report Element	[DSN=Msg] Element
=====	=====	=====
Date and time the message was handled	Date:	'Date:' header field value of top-level
-----	-----	-----
Delivery status of original message	X-Mms-Status:	'Action' and 'Status' fields of per-recipient section
	Set to one of the following values:	
	'retrieved' (used for 'Action' value	

	'delivered').	
	'unreachable'	
	(used for 'Action'	
	value 'failed')	
	'forwarded' (used	
	for 'Action' value	
	'relayed')	
	'deferred' MUST	
	NOT be used	
	(ignore DSNs with	
	'Action' value	
	'delayed')	
-----	-----	-----
Status Text		Text in first part (human-
		readable part)
=====	=====	=====

Gellens [Page 24] Expires October 2005

Internet Draft Mapping Between MMS and Internet Mail April 2005

2.1.4.3 Read Report Mapping from MMS to Internet Message

The following table maps information elements from MMS read reports to the format specified in [[MDN](#)].

2.1.4.3.1 Table 7: Read Report Mappings (MMS to Internet Message)

=====	=====	=====
Information Element	MMS Delivery	[DSN-Msg] Element
	Report Elem	
=====	=====	=====

ID of the original message (object of read report)	Message-Id:	'Original-Envelope-ID' field (use value of ENVID from ESMTP envelope if available, 'Message-ID:' otherwise).
-----	-----	-----
Recipient address of the original message	From:	'Final-Recipient' field
-----	-----	-----
Destination address of report	To:	'To:' header field value of top-level.
		Value taken from 'Disposition-Notification-To:' header field of message being reported, not its 'From:' header field.
-----	-----	-----
Date and time the message was handled	Date:	'Date:' header field value of top-level
-----	-----	-----
Disposition of message being reported	X-Mms-Read-Status:	Disposition-field
		For MMS-Read-Status value 'read', use 'disposition-type' value 'displayed'; for MMS-Read-Status value 'Deleted without being read', use 'disposition-type' value 'deleted')
-----	-----	-----
Status Text		Text in first part (human-readable part)
=====	=====	=====

When an MMS Relay/Server generates an [MDN](#) in response to a message received using ESMTP on MM3:

* Top-level header field 'To:' SHOULD be the value of the 'Disposition-Notification-To:' header field of the message whose disposition is being reported .

* Top-level header field 'From:' SHOULD be the address of the recipient that the read report concerns.

2.1.4.4 Disposition Report Mapping from Internet Message to MMS

The following table maps information elements from a disposition report as specified in [MDN] to the format of an MMS read report.

2.1.4.4.1 Table 8: Disposition Report Mappings (Internet Message to MMS)

Information Element	MMS Read Report Element	[DSN=Msg] Element
ID of the original message (object of disposition report)	Message-Id:	'Original-Envelope-ID' field
Recipient address of the original message	From:	'Final-Recipient' field
Destination address of report	To:	'To:' header field value of top-level. Value taken from 'Disposition-Notification-To:' header field of message being reported, not its 'From:' header field.
Date and time the message was handled	Date:	'Date:' header field value of top-level

Information Element	MMS Read Report Element	[DSN=Msg] Element
---------------------	-------------------------	-------------------

=====	=====	
=====Disposition of	X-Mms-Read-Status:	
disposition-field		
message being		
reported	Set to one of the	
	following values:	
	'read' (used for	
	disposition-type	
	value 'displayed')	
	'Deleted without	
	being read' (used	
	for disposition-	
	types 'deleted',	
	'denied' and	
	'failed' when	
	action-mode is	
	'automatic-	
	action')	
-----	-----	-----
Status Text		Text in first part (human-
		readable part)
=====	=====	=====

2.1.5 Message Delivery

Within Internet mail, when ESMTP is used and delivery reports are requested [[DSN-SMTP](#)], delivery is considered to be acceptance of a message by the final server, that is, the server closest to the recipient. When an MMS Relay/Server receives a message using ESMTP and a delivery report is requested, the MMS Relay/Server MAY consider the message delivered when it has been sent to the MMS User Agent.

3 Security Considerations

Data contained within messages should not be automatically trusted. Even within a carrier's network, and certainly within the Internet, various deliberate and accidental attacks or corruptions are possible. For example, routers may contain vulnerabilities which may be exploited, IP traffic may be intercepted and/or modified, etc.

The following messaging-related security threats can be identified:

- * Misidentification of message source.
- * Message interception (unauthorized disclosure of contents).
- * Unauthorized disclosure of message sender or recipient.
- * Message modification (by adversary).
- * Message replay.
- * Traffic analysis (determining who is communicating with whom).

There are existing mechanisms which can be used to protect email traffic against some of these threats, such as:

- * Use of SSL/TLS (via [[StartTLS](#)]) to address disclosure and modification in transit between adjacent servers.
- * SMTP Authentication [[Auth](#)] to protect against misidentification of message source.
- * Use of end-to-end security mechanisms such as [[PGP](#)] or S/MIME [[SMIME](#)] to protect message contents.
- * Use of [[IPSec](#)] to protect against disclosure or modification in transit between servers.

Use of these mechanisms is encouraged. When a message uses end-to-end security mechanisms such as [[PGP](#)] or S/MIME [[SMIME](#)], servers MUST be careful not to accidentally destroy the integrity of the protected content (for example, by altering any text within the region covered by a signature while mapping between MMS and email).

Since MMS does not include a clear separation between in-transit envelope and message content, there are increased risks of unauthorized disclosure of information, and additional challenges in protecting data. For example, Bcc recipients do not normally appear in the message content, only in the envelope; care MUST be taken in the gateway function to ensure that Bcc recipients which do appear are deleted from the message content.

Some MMS features contain inherently more risk than others. For example, reply charging and sender address hiding. The reply charging mechanism requires a high degree of trust between entities with little technical basis. Deliberate or accidental abuse of this trust can result in unexpected or unauthorized charges. For example, a sender may be charged for unauthorized replies, or a

sender may be charged for a reply which the author thought would be paid for by the recipient. A sender's identity may be disclosed in violation of a request for this to be blocked. The identity of recipients may be disclosed to other recipients (or even non-recipients) for a message in which the sender intended for the recipients not to be disclosed.

It is possible to hide the sender's identity from non-recipients using anonymous remailers. It is hard to hide the sender's identity from recipients when the mail is cryptographically signed. In view of anti-spam measures it may be undesirable to hide the sender's identity.

Additional mechanisms can be developed to protect against various threats, however, these are not included in this version of this specification. It is strongly RECOMMENDED that features such as reply charging and sender identity hiding not be used across carrier domains, and be used within carrier domains only with full understanding of the risks involved.

4 Normative References

IETF:

[DSN-Msg] "An Extensible Message Format for Delivery Status Notifications", Moore, Vaudreuil, [RFC 3464](#), January 2003.

[DSN-SMTP] "SMTP Service Extension for Delivery Status Notifications", Moore, [RFC 3461](#), January 2003.

[Hdr-Enc] "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", Moore, [RFC 2047](#), November 1996.

[KEYWORDS] Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), Harvard University, March 1997.

[MDN] "An Extensible Message Format for Message Disposition Notifications", Fajman, [RFC 2298](#), March 1998.

[Msg-Fmt] "Internet Message Format", Resnick, [RFC 2822](#), April 2001.

[Report-Fmt] "The Multipart/Report Content Type for the Reporting of

Mail System Administrative Messages", Vaudreuil, [RFC 3462](#), January 2003

Gellens [Page 29] Expires October 2005

Internet Draft Mapping Between MMS and Internet Mail April 2005

[RESP] Enhanced Mail System Status Codes, Vaudreuil, [RFC 1893](#), January 1996.

[SMTP] "Simple Mail Transfer Protocol", Klensin, [RFC 2821](#), April 2001.

5 Informative References

IETF:

[Auth] "SMTP Service Extension for Authentication", Myers, [RFC 2554](#), March 1999

[BINARY] "SMTP Service Extensions for Transmission of Large and Binary MIME Messages", Vaudreuil, Parsons, [RFC 3030](#), December 2000.

[Codes] "SMTP Service Extension for Returning Enhanced Error Codes", Freed, [RFC 2034](#), October 1996.

[Deliver-By] "Deliver By SMTP Service Extension", Newman, [RFC 2852](#), June 2000.

[Msg-Encap] "Proposed Standard for Message Encapsulation", Rose, Stefferud, [RFC 934](#), January 1985.

[Hdrs] "Common Internet Message Headers", J. Palme, [RFC 2076](#), February 1997.

[IPSec] "Security Architecture for the Internet Protocol", Kent, Atkinson, [RFC 2401](#), November 1998

[PGP] "MIME Security with OpenPGP", Elkins, Del Torto, Levien, Roessler, [RFC 3156](#), August 2001

[SMIME] "S/MIME Version 3 Message Specification", Ramsdell, [RFC 2633](#), June 1999

[StartTLS] "SMTP Service Extension for Secure SMTP over Transport Layer Security", Hoffman, [RFC 3207](#), February 2002

[Submission] "Message Submission", Gellens, Klensin, [RFC 2476](#),

December 1998.

[VPIM] "Voice Profile Internet Mail - Version 2", Vaudreuil, Parsons, [RFC 2421](#), September 1998.

Gellens	[Page 30]	Expires October 2005
Internet Draft	Mapping Between MMS and Internet Mail	April 2005

OMA:

OMA specifications are available at the OMA web site
<<http://www.openmobilealliance.org>>.

[OMA-MMS] OMA-WAP-MMS-ENC-V1_2-20040323-C

3GPP2 and 3GPP:

3GPP2 specifications are available at the 3GPP2 (Third
Generation Partnership Project 2) web site
<<http://www.3gpp2.org>>.

3GPP specifications are available at the 3GPP (Third Generation
Partnership Project) web site <<http://www.3gpp.org>>

[Stage_3] "MMS MM1 Stage 3 using OMA/WAP", X.S0016-310

"MMS MM4 Stage 3 Inter-Carrier Interworking", X.S0016-340

"Multimedia Messaging Service: Functional description; Stage 2", TS
23.140 Release 5.

[Formats] "Multimedia Messaging Service (MMS) Media Format and
Codecs for cdma2000 Spread Spectrum Systems", C.S0045

[Overview] "Multimedia Messaging Services (MMS) Overview",
X.S0016-000

[Stage_1] "Multimedia Messaging Services (MMS); Stage 1",
Requirements, October 2002, S.R0064-0.

[Stage_2] "Multimedia Messaging Service (MMS); Stage 2", Functional
Specification, April 2003, X.S0016-200.

"Multimedia Messaging Service; Media formats and codecs",
TS26.140 Release 5.

6 Author's Address

Randall Gellens
QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121
USA
randy@qualcomm.com

Gellens [Page 31] Expires October 2005

Internet Draft Mapping Between MMS and Internet Mail April 2005

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2004).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Disclaimer

This document and the information contained herein are provided on

an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.