

3GPP2 X.S0016-330

Version 1.0

Version Date: June 2004



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

MMS MM3 Stage 3 for Internet Mail Exchange Revision: 0

COPYRIGHT

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

Revision History

Revision	Date	Description/Title	Source
1.0	June, 2004	Initial publication	Editor

No Text.

CONTENTS

1	Introduction	1
1.1	Scope	1
1.2	References.....	1
1.3	Terminology	2
1.4	Definitions	3
1.5	Abbreviations	4
1.6	Assumptions	4
2	Stage 2 Amendments.....	4
3	MM3 Stage 3 Description.....	5
3.1	Introduction (Informative).....	5
3.2	Stage 3 Specification (Normative).....	5
3.2.1	Sending MMs	5
3.2.2	Receiving messages.....	5
3.2.3	MM3 Mappings	6
3.2.4	Report Generation and Conversion.....	16
3.2.5	Message Delivery.....	22
4	Security Considerations.....	22

TABLE OF TABLES

Table 2-1: Abstract messages for exchanging MMs in MM3	4
Table 3-1: MM3 Mappings	7
Table 3-2: Importance Mappings (MMS to Internet Message)	10
Table 3-3: X-Priority Mappings (MMS to Internet Message).....	10
Table 3-4: Priority Mappings (Internet Message to MMS)	15
Table 3-5: Delivery Report Mapping from MMS to Internet Message	17
Table 3-6: Delivery Report Mapping from Internet Message to MMS	18
Table 3-7: Read Report Mapping from MMS to Internet Message	20
Table 3-8: Disposition Report Mapping from Internet Message to MMS.	21

1 **Foreword**

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

4 **1 Introduction**

5 Note that in the text of this document, a distinction is made between use
6 of “SMTP” or “Simple Mail Transfer Protocol”, and “ESMTP” or “Extended
7 Simple Mail Transfer Protocol”: when the term “ESMTP” or “Extended” is
8 used, it indicates use of extended features of SMTP; that is, those beyond
9 the facilities of RFC 821. (These extended facilities may be in RFC 2821
10 or in other RFCs, as indicated by the specific RFC reference used; note
11 that the name of the RFC 2821 reference is “SMTP” because that is the
12 official title of the RFC.)

13 **1.1 Scope**

14 This specification describes how to use MM3 to exchange messages with
15 Internet mail systems. This includes translation between MMS and
16 Internet Mail messages using Extended Simple Mail Transfer Protocol
17 [SMTP] and Internet mail format [Msg-Fmt]. This protocol is a Stage 3 on
18 reference point MM3 to exchange messages with systems in Internet
19 Message format.

20 Note that MM3 can also be used for interworking with other systems,
21 such as SMS and access to external mail stores. This specification does
22 not address these other uses of MM3; it is only concerned with Internet
23 mail interworking and specifically exchange of messages between MMS
24 and Internet mail systems.

25 **1.2 References**

26 OMA

27 [OMA-MMS] OMA-WAP-MMS-ENC-v1_3-20030716

28

29 3GPP2

30 [Stage_2] MMS Stage 2, Functional Specification, X.S0016-200/

31 [Stage_1] Multimedia Messaging Services (MMS) Stage 1 Require-
32 ments, S.R0064.

33 TIA

34 [Stage_2] MMS Stage 2, Functional Specification, TIA-934-200.

35

1 IETF

2 [Msg-Encap] “Proposed Standard for Message Encapsulation”,
3 Rose, Stefferud, RFC 934, January 1985.

4 [DSN-SMTP] “SMTP Service Extension for Delivery Status Notifica-
5 tions”, Moore, RFC 3461, January 2003.

6 [Report-Fmt] “The Multipart/Report Content Type for the Reporting
7 of Mail System Administrative Messages”, Vaudreuil, RFC 3462,
8 January 2003

9 [DSN-Msg] “An Extensible Message Format for Delivery Status Noti-
10 fications”, Moore, Vaudreuil, RFC 3464, January 2003.

11 [MDN] “An Extensible Message Format for Message Disposition No-
12 tifications”, Fajman, RFC 2298, March 1998.

13 [Submission] “Message Submission”, Gellens, Klensin, RFC 2476,
14 December 1998.

15 [SMTP] “Simple Mail Transfer Protocol”, Klensin, RFC 2821, April
16 2001.

17 [Msg-Fmt] “Internet Message Format”, Resnick, RFC 2822, April
18 2001.

19 [Deliver-By] “Deliver By SMTP Service Extension”, Newman, RFC
20 2852, June 2000.

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

24 [Codes] “SMTP Service Extension for Returning Enhanced Error
25 Codes”, Freed, RFC 2034, October 1996.

26 [StartTLS] “SMTP Service Extension for Secure SMTP over Trans-
27 port Layer Security”, Hoffman, RFC 3207, February 2002

28 [Auth] “SMTP Service Extension for Authentication”, Myers, RFC
29 2554, March 1999

30 [PGP] “MIME Security with OpenPGP”, Elkins, Del Torto, Levien,
31 Roessler, RFC 3156, August 2001

32 [SMIME] “S/MIME Version 3 Message Specification”, Ramsdell,
33 RFC 2633, June 1999

34 [IPSec] “Security Architecture for the Internet Protocol”, Kent, At-
35 kinson, RFC 2401, November 1998

36 **1.3 Terminology**

37 This document uses the following “verbal forms” and “verbal form defini-
38 tions”:

- 1 1. “shall” and “shall not” identify items of interest that are to be strictly
2 followed and from which no deviation is recommended,
- 3 2. “should” and “should not” indicate items of interest that are highly
4 desirable and particularly suitable, without identifying or excluding
5 other items; or (in the negative form) indicate items of interest that
6 are not desirable, are not particularly suitable, or are not recom-
7 mended but not prohibited, and
- 8 3. “may” and “may not” indicate items of interest that are optional but
9 permissible within the limits of this recommendation.

10 **1.4 Definitions**

11 For the purposes of the present document, the terms and definitions de-
12 fined in 3GPP2, MMS Stage 1 Requirements [Stage_1] and MMS Stage 2
13 Functional Description [Stage_2] and the following apply:

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 Message Disposition Notification	Feedback information to an originator User Agent by a recipient User Agent about 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 infor-

	mation 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

1 **1.5 Abbreviations**

2 For the purposes of this document, the abbreviations defined in
3 [Stage_1], [Stage_2] and the following apply:

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 Users Agents and processes them; either delivering them locally or relaying to an MTA.
MTA	Mail Transfer Agent. A server which implements [SMTP]

4 **1.6 Assumptions**

5 It is assumed that the reader is already familiar with the contents of the
6 3GPP2 MMS Stage 1 [Stage_1], and Stage 2 [Stage_2] documents. It is
7 also assumed that the reader is familiar with Internet mail, especially
8 RFC 2821 [SMTP] and RFC 2822 [Msg-Fmt].

9 **2 Stage 2 Amendments**

10 All MM3 Stage 2 [Stage_2] functions are supported except for reply charg-
11 ing. Sender address hiding may be used but is not recommended with-
12 out security assurances which are beyond the scope of this specification
13 (see Section 4).

14 The following abstract messages are defined for the Internet Email Ex-
15 change use of MM3:

16 **Table 2-1: Abstract messages for exchanging MMs in MM3**

MM3_forward.REQ	Request	Sending Server -> Receiving Server
MM3_forward.RES	Response	Receiving Server -> Sending Server

17 Note that relay of normal messages as well as relay and generation of de-
18 livery and disposition reports are handled within the forward request ab-
19 stract message.

20 The forward request and forward response abstract messages are realized
21 using an [SMTP] transaction; the forward request is realized using [SMTP]
22 commands from the sending system to the receiving system; the forward

1 response is realized using [SMTP] response codes, including the extended
2 codes specified in [Codes].

3

4 **3 MM3 Stage 3 Description**

5 **3.1 Introduction (Informative)**

6 This section defines the interworking between MMS Relay/Servers and
7 Internet Mail servers using ESMTP. That is, information elements are
8 exchanged using standard Internet Message [Msg-Fmt] header fields and
9 standard ESMTP [SMTP] elements to the maximum possible extent.

10 SMTP and Internet mail extensions are used for features such as delivery
11 reports, message expiration, discovery of server support for optional fea-
12 tures, etc.

13 **3.2 Stage 3 Specification (Normative)**

14 This specification defines the Internet Mail Exchange implementation op-
15 tion for MM3.

16 **3.2.1 Sending MMs**

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

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

24 Section 3.2.3 lists the mappings between X-Mms-* headers and Internet
25 Message header fields and ESMTP values.

26 Delivery and read report MMs should be converted to standard Internet
27 Message report format (multipart/report). In addition to converting
28 Internet Message reports, the MMS Relay/Server shall generate delivery
29 and read report MMs for received MMs as appropriate. See section 3.2.4
30 for more information.

31 **3.2.2 Receiving messages**

32 When receiving a message from an Internet mail system the MMS Re-
33 lay/Server may convert incoming messages to the MM format used within
34 the receiving system.

35 The MMS Relay/Server may convert control information received from the
36 External Server into appropriate information elements of an MM.

1 Section 3.2.3 lists the mappings between X-Mms-* headers and Internet
2 Message header fields and ESMTP values.

3 Standard Internet Message report format (multipart/report) messages
4 may be converted to delivery or read report MMs, as appropriate. In ad-
5 dition to converting report MMs, the MMS Relay/Server shall generate
6 standard Internet Message delivery and disposition reports for received
7 Internet messages as appropriate. See section 3.2.4 for more informa-
8 tion.

9 **3.2.3 MM3 Mappings**

10

11 The MM3 mappings between MMS elements and ESMTP/Internet Mes-
12 sages elements (either [SMTP] parameters, [Msg-Fmt] headers, or both) are
13 detailed below. The “MMS Headers” are from [OMA-MMS]. Note that
14 only information elements which need to be mapped are listed. [Msg-
15 Fmt] headers not listed here should be passed unaltered.

1 **Table 3-1: MM3 Mappings**

Information element	[SMTP] Elements	[Msg-Fmt] Headers	MMS Headers
3GPP MMS Version	N/a	N/a	X-Mms-3GPP-MMS-Version::
Message Type (of PDU)	N/a	N/a	X-Mms-Message-Type:
Transaction ID	N/a	N/a	X-Mms-Transaction-ID:
Message ID	ENVID [DSN-SMTP]	Message-ID:	X-Mms-Message-ID: Message-id:
Recipient(s) address	RCPT TO addresses	To:, Cc:, or omitted (Bcc:)	To:, Cc:, Bcc:
Sender address	MAIL FROM address user-originated MMS; NB: shall set MAIL FROM to null ("<>") for all automatically-generated MMS	From: (may set to locally-generated value to hide sender identity in anonymous messages when receiving system does not support anonymous messages)	From:
Content type		Content-Type:	Content-type:
Message class	Class=auto: shall set MAIL FROM to null ("<>").	May set 'Precedence: bulk' on class=auto.	X-Mms-Message-Class:
Date and time		Date:	Date:
Time of Expiry	DELIVER-BY [Deliver-By]		X-Mms-Expiry:
Earliest delivery time	(not an MM3 feature)		X-Mms-Delivery-Time:
Delivery report request	DSN [DSN-SMTP]; should also specify recipient address as ORCPT; should also specify ENVID		X-Mms-Delivery-Report:
Priority		Importance: X-Priority:	X-Mms-Priority:
Sender visibility	X-ANONYMOUS (see text below)		X-Mms-Sender-Visibility:
Read reply request		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:
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		Subject:	Subject:
Forward counter		Resent-Count:	

Previously-sent-by		Resent-From:	X-Mms-Previously-Sent-By:
Previously-sent-date and-time		Resent-Date:	X-Mms-Previously-Sent-Date:
Trace data		Received:	
Content		<message body>	

1

2 *3.2.3.1 Conversion of messages from MMS to Internet format*3 **3GPP MMS Version**

4 The 'X-Mms-3GPP-MMS-Version:.' header, if present, should be removed.

5 **Message Type (of PDU)**

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

7 **Transaction ID**

8 The 'X-Mms-Transaction-ID:.' header, if present, should be removed.

9 **Message ID**

10 An 'X-Mms-Message-ID:.' header, if present, should be retained.

11 The 'Message-ID:.' header shall be retained. If not present it shall be cre-
12 ated, with a unique value. If an 'X-Mms-Message-ID:.' header is present
13 and a 'Message-ID:.' header is not, the value of the 'X-Mms-Message-ID:.'
14 header may be used in creating the 'Message-ID:.' header.15 The message ID should be transmitted in the ESMTP envelope as the
16 ENVID parameter, as specified in [DSN-SMTP].17 **Recipient(s) address**18 The address of each recipient shall be transmitted in the ESMTP envelope
19 as a RCPT TO value. All disclosed recipients should also appear in a 'To:.'
20 or 'Cc:.' header. At least one 'To:.' or 'Cc:.' header should be present. If all
21 recipients are undisclosed, a 'To:.' header may be created that contains a
22 comment, for example 'To: (undisclosed recipients)'. The 'To:.' header
23 should not appear more than once. The 'Cc:.' header should not appear
24 more than once.

25 Each recipient address shall obey the length restrictions per [SMTP].

26 Current Internet message format requires that only 7-bit US-ASCII char-
27 acters be present. Other characters (for example, non-7-bit characters in
28 a phrase part of an address header) must be encoded according to [Hdr-
29 Enc]. Note that it would be possible to define an ESMTP extension to

1 permit transmission of unencoded 8-bit characters, but in the absence of
2 such an extension [Deliver-By] shall be used.

3 ***Sender address***

4 The address of the message sender should appear in the 'From:' header,
5 unless address hiding has been requested. If address hiding has been
6 requested, the 'From:' header may contain a comment to this effect, for
7 example, 'From: (anonymous sender)'.

8 The address of the message sender for all user-generated messages ('X-
9 Mms-Message-Class: personal') should be transmitted in the [SMTP] envelope as the
10 MAIL FROM value unless address hiding has been requested and the receiving server
11 is not known to support address hiding.

12 The 'From:' header and the MAIL FROM value may set to a locally-
13 generated value to hide the sender identity in anonymous messages when
14 the receiving system does not support anonymous messages. Locally
15 generated addressed may be internally mapped to the actual address to
16 allow replies to anonymous messages, but such mapping is beyond the
17 scope of this specification.

18 Because of the risk of mail loops, it is critical that the MAIL FROM be set
19 to null ("<>") for all automatically-generated MMs ('X-Mms-Message-Class:
20 auto'). The MAIL FROM value shall be set to null for all automatically -
21 generated messages.

22 The sender address shall obey the length restrictions of [SMTP].

23 ***Content type***

24 The 'Content-Type:' header should be preserved. Content types not in
25 widespread use in the Internet may be converted into those that are,
26 when such conversion can be done without loss of content. For example,
27 SMIL messages may be converted into widely-supported multi-
28 part/related with multipart/html.

29 ***Message class***

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

34 ***Time of Expiry***

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

36 The remaining time until the message is considered expired should be
37 transmitted in the ESMTP envelope by using the DELIVER-BY extension,
38 as specified in [Deliver-By].

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

6 ***Earliest delivery time***

7 The 'X-Mms-Delivery-Time:' header, if present, should be removed.
 8 Future delivery is a message submission, not message relay feature.

9 ***Delivery report request***

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

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

18 ***Priority***

19 The message sender's importance value should be transmitted using an
 20 'Importance:' header (although currently not all Internet mail clients sup-
 21 port this header).

22 An 'X-Priority:' header may be used in addition. Although not standard-
 23 ized, most email applications support the 'X-Priority:' header, and use an
 24 'X-Priority' value of 3 for messages with "normal" priority. More important
 25 messages have lower values and less important message have higher val-
 26 ues. In most cases, urgent messages have an X-Priority value of 1.

27 Suggested mappings:

28 **Table 3-2: Importance Mappings (MMS to Internet Message)**

X-Mms-Priority: High	Importance: High
X-Mms-Priority: Normal	<i>omit</i>
X-Mms-Priority: Low	Importance: Low

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

30 **Table 3-3: X-Priority Mappings (MMS to Internet Message)**

X-Mms-Priority: High	X-Priority: 2 (high)
X-Mms-Priority: Normal	<i>omit</i>
X-Mms-Priority: Low	X-Priority: 4 (low)

- 1 Normal priority messages should omit the 'X-Priority:' header.
2 The 'X-Mms-Priority:' header, if present, should be removed.

3 ***Sender visibility***

4 Requests for sender address hiding may be transmitted in the ESMTP
5 envelope by using the X-ANONYMOUS extension. The request is made
6 by adding "X-ANONYMOUS" to the MAIL FROM command. Servers
7 which support address hiding may advertise this by including X-
8 ANONYMOUS in their EHLO response.

9 Note that even if servers claim to support address hiding, there is no
10 technical guarantee that it will be properly honored; servers shall not
11 trust other servers to support this without a basis which is beyond the
12 scope of this specification (such as business relationships).

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

14 ***Read reply request***

15 A request for a read reply should be transmitted using a 'Disposition-
16 Notification-To:' header as specified in [MDN].

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

18 ***Reply-charging***

19 Reply charging permission and acceptance are complex issues requiring
20 both user agent and server support. Misapplied reply charging may
21 cause incorrect billing. Until the security issues have been properly ad-
22 dressed, reply charging should not be honored when using this interface.

23 The 'X-Mms-Reply-Charging:', 'X-Mms-Reply-Charging-Deadline:', 'X-
24 Mms-Reply-Charging-Size:', and 'X-Mms-Reply-Charging-ID:' headers
25 may be removed. Messages containing a reply-charging usage request
26 ('X-Mms-Reply-Charging-ID:' and 'X-Mms-Reply-Charging: Accepted' or
27 'X-Mms-Reply-Charging: Accepted (text only)' headers) should be rejected.

28 ***Subject***

29 The 'Subject:' header shall be preserved. Current Internet message for-
30 mat requires that only 7-bit US-ASCII characters be present. Other
31 characters must be encoded according to [Hdr-Enc]. Note that it would
32 be possible to define an ESMTP extension to permit transmission of un-
33 encoded 8-bit characters, but in the absence of such an extension [Hdr-
34 Enc] shall be used.

35 ***Resending/Forwarding***

36 In MMS a message may be *resent* or *forwarded*, the difference being that
37 if the message has been downloaded then sending it to another address

1 is considered forwarding, while sending a message that has not been
2 downloaded is considered to be resending.

3 In Internet mail there are two primary ways of sending a previously re-
4 ceived message to a new recipient: forwarding and resending. Forward-
5 ing is when a user creates a new message containing the original mes-
6 sages, either simply embedded within the text, or delineated. Embedded
7 messages generally have each original line preceded by a quote symbol
8 ('>'), surround the original text with a preceding and trailing line which
9 starts with hyphens as per [Msg-Encap], such as '--- begin forwarded
10 text' and '--- end forwarded text', or encapsulate the original message as
11 a 'message/rfc822' content type, perhaps within a 'multipart/mixed' mes-
12 sages. (This last method offers more robust delineation.) Resending is
13 when the original message is unaltered except for the possible addition of
14 'resent-' headers to explain the resending to the new recipient.

15 A message may be resent more than once; each time new 'resent-' head-
16 ers may be added at the top of the message. Thus, if more than one se-
17 ries of 'resent-' headers are present, the original series is the last; the
18 most recent is the first.

19 **Forward counter**

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

23 **Previously-sent Information**

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

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

28 Any 'X-Mms-Previously-Sent-By:' and 'X-Mms-Previously-Sent-Date'
29 headers, if present, should be removed. The information contained in
30 them should be translated into 'From:', 'Resent-To:', 'Resent-From:', 'Re-
31 sent-Date:', and 'Resent-Count:' headers. The original sender of the mes-
32 sages should appear in the 'From:' header; the original recipient(s) should
33 appear in the 'To:' header; the time and date the message was originally
34 sent should appear in the 'Date:' header. The most recent sender should
35 appear in the top-most 'Resent-From:' header; the most recent recipi-
36 ent(s) should appear in the top-most 'Resent-To:' header; the time and
37 date the message was most recently sent should appear in the top-most
38 'Resent-Date:' header.

39 **'Received:' Headers**

1 Each system that processes a message should add a 'Received:' header as
 2 per [SMTP]. A message may be rejected if the number of 'Received:'
 3 headers exceeds a locally-defined maximum, which shall be no less than
 4 100.

5 **Content**

6 The message content appears in the message body. Note that Internet
 7 message format requires that line-endings be encoded as CR LF, thus
 8 charset encodings that do not have this property cannot be used in text/*
 9 body parts. (They may be used in other body parts, but only when they
 10 are suitable encoded or when binary transmission has been negotiated.)
 11 In particular, MMS allows UTF-16, while Internet message format does
 12 not. UTF-16 encoding shall be transcoded to UTF-8 or another charset
 13 and encoding which is suitable for use in Internet message for-
 14 mat/protocols.

15 3.2.3.2 *Conversion of messages from Internet to MMS format*

16 **3GPP MMS Version**

17 An 'X-Mms-3GPP-MMS-Version:' header should be added.

18 **Message Type (of PDU)**

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

21 **Transaction ID**

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

24 **Message ID**

25 The 'Message-ID:' header shall be retained. If not present it shall be cre-
 26 ated, with a unique value. If the 'Message-ID:' header does not exist, but
 27 the ESMTP envelop contains an ENVID value (as specified in [DSN-
 28 SMTP]), it may be used as the message ID.

29 An 'X-Mms-Message-ID:' header should be added. The Message ID may
 30 be used to construct the value.

31 **Recipient(s) address**

32 'To:' and 'Cc:' headers shall be retained.

33 Each recipient contained in the [SMTP] envelope (RCPT TO values) shall
 34 be considered a recipient of the message. Recipients who appear in ad-
 35 dress headers but not the ESMTP envelope shall be ignored. Recipients

1 who appear in the [SMTP] envelope but do not appear in headers are con-
2 sidered “blind” (bcc) recipients; such recipients shall not be added to
3 message headers (including address and trace headers) unless there is
4 only one recipient total.

5 ***Sender address***

6 The ‘From:’ header shall be retained.

7 If address hiding has been requested, the ‘From:’ header may contain a
8 comment to this effect, for example, ‘From: (anonymous sender)’.

9 ***Content type***

10 The ‘Content-Type:’ header should be preserved.

11 ***Message class***

12 An ‘X-Mms-Message-Class: personal’ header should be created for all re-
13 ceived messages with a non-null return path (MAIL FROM value in the
14 [SMTP] envelope). An ‘X-Mms-Message-Class: auto’ header may be cre-
15 ated for messages with a null return path.

16 ***Time of Expiry***

17 An ‘X-Mms-Expiry:’ header should be created if the message contains a
18 relative time to expiration in the DELIVER-BY extension, as specified in
19 [Deliver-By].

20 ***Earliest delivery time***

21 An ‘X-Mms-Delivery-Time:’ header should not be created. If a message
22 arrives via [SMTP] relay containing an earliest time of delivery in the
23 AFTER extension, it may be rejected. If a message is submitted via Mes-
24 sages Submission [Submission] containing an earliest time of delivery in
25 the AFTER extension, it shall be retained until the delivery time arrives,
26 or it may be immediately rejected. It shall not be delivered or further re-
27 layed prior to the delivery time.

28 ***Delivery report request***

29 An ‘X-Mms-Delivery-Report:’ header should be created for messages
30 which request ‘success’ or ‘none’ delivery status notification by use of the
31 DSN extension as specified in [DSN-SMTP]. Requests for ‘delay’ notifica-
32 tions or non-default actions, such as that only the message headers
33 should be returned, cannot be mapped onto MMS headers and thus
34 should be ignored.

35 ***Priority***

1 'X-Priority:' and/or 'Importance:' headers, if present, should be replaced
2 with an 'X-Mms-Priority:' header. Suggested mappings:

3 **Table 3-4: 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)	<i>Omitted</i>
Importance: Normal	<i>Omitted</i>
X-Priority: 4 (low)	X-Mms-Priority: Low
Importance: Low	X-Mms-Priority: Low
X-Priority: 5 (lowest)	X-Mms-Priority: Low

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

5 ***Sender visibility***

6 Requests for sender address hiding may be received in the SMTP envelope by X-ANONYMOUS extension. Servers which support address hiding may advertise this by including X-ANONYMOUS in their EHLO response. A message received which includes X-ANONYMOUS in the MAIL FROM command has requested address hiding.

11 Note that even if servers claim to support address hiding, there is no technical guarantee that it will be properly honored; servers should not trust other servers to support this without a basis which is beyond the scope of this specification (such as business relationships).

15 Requests for sender address hiding may be reflected in the created MM by adding an 'X-Mms-Sender-Visibility:' header.

17 ***Read reply request***

18 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.

21 ***Subject***

22 The 'Subject:' header shall be preserved.

23 ***Resending/Forwarding***

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

26 ***'Received:' Headers***

1 Each system that processes a message should add a 'Received:' header as
 2 per [SMTP]. A message may be rejected if the number of 'Received:'
 3 headers exceeds a locally-defined maximum, which shall be no less than
 4 100.

5 **Content**

6 The message content appears in the message body.

7 **3.2.4 Report Generation and Conversion**

8 The format of standard Internet Message systems use the *multi-*
 9 *part/report* MIME type for delivery and disposition reports (often called
 10 "read reports") as specified in [Report-Fmt]. This format is a two- or-
 11 three-part MIME message, one part is a structured format describing the
 12 event being reported in an easy-to-parse format. Specific reports have a
 13 format which is built on [Report-Fmt]. Delivery reports are specified in
 14 [DSN-Msg]. Message disposition reports, which include read reports, are
 15 specified in [MDN].

16 By contrast, MMS reports are plain text, with no defined structure speci-
 17 fied. This makes it difficult to convert from an MMS report to a standard
 18 Internet report.

19 An MMS Relay/Server supporting Internet Message exchange using MM3
 20 shall convert reports received from one side (MMS or Internet mail) des-
 21 tined for the other. In addition, reports shall be generated as appropriate
 22 for messages received from either side of the MM3 interface. For exam-
 23 ple, if an MM to be sent via MM3 is not deliverable, a delivery status MM
 24 shall be generated. Likewise, if an Internet message is received via MM3
 25 that cannot be further relayed or delivered, a delivery status [DSN-Msg]
 26 shall be generated.

27 When creating delivery or disposition reports from MMS reports, the
 28 MMS report should be parsed to determine the reported event and time,
 29 status, and the headers of the referenced (original) message. These ele-
 30 ments, once determined, are used to populate the subparts of the deliv-
 31 ery or disposition report. The first subpart is of type *text/plain*, and con-
 32 tains a human-readable explanation of the event. This text may include
 33 a statement that the report was synthesized based on an MMS report.
 34 The second subpart is of type *report/delivery-status* (for delivery reports)
 35 or *report/disposition-notification* (for disposition reports). This second
 36 part contains a structured itemization of the event. The third subpart is
 37 of type *message/rfc822* and includes the headers and optionally the body
 38 of the referenced (original) message.

- 1 3.2.4.1 *Delivery Report Mapping from MMS to Internet Message*
 2 The following table maps information elements from MMS delivery reports
 3 to the format specified in [DSN-Msg].

4 **Table 3-5: Delivery Report Mapping from MMS to Internet Message**

Information Element	MMS Delivery Report Element	[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
Delivery status of original message	X-Mms-Status:	Action and Status fields of 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: <ul style="list-style-type: none"> • delivered (used for

Information Element	MMS Delivery Report Element	[DSN-Msg] Element
		<p>MMS status values ‘retrieved’ and ‘rejected’, depending on ‘Status’ code).</p> <ul style="list-style-type: none"> 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)

1

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

- 4 • Top-level header field ‘To:’ should be the [SMTP] return-path of the
5 message whose status is being reported.
- 6 • Top-level header field ‘From:’ should be the address of the recipient
7 that the delivery-report concerns.
- 8 • The first part of the [DSN-Msg] should include the MM Status Text
9 field that would have been generated for an MM1 delivery-report.

10 3.2.4.2 *Delivery Report Mapping from Internet Message to MMS*

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

13 **Table 3-6: Delivery Report Mapping from Internet Message to MMS**

Information Element	MMS Delivery Report Element	[DSN-Msg] Element
ID of the original message (object of delivery report)	Message-ID:	‘Original-Envelope-ID’ field of per-message fields. If not available,

Information Element	MMS Delivery Report Element	[DSN-Msg] Element
		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.
Date and time the message was handled	Date:	'Date:' header field value of top-level
Delivery status of original message	X-Mms-Status: 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' shall not be used (ignore DSNs with 'Action' value 'delayed')	'Action' and 'Status' fields of per-recipient section

Information Element	MMS Delivery Report Element	[DSN-Msg] Element
Status Text		Text in first part (human-readable part)

1

2 **3.2.4.3** *Read Report Mapping from MMS to Internet Message*3 The following table maps information elements from MMS read reports to
4 the format specified in [MDN].5 **Table 3-7: Read Report Mapping from MMS to Internet Message**

Information Element	MMS Read Report Element	[MDN] Element
ID of the original message (object of read report)	Message-ID:	'Original-Envelope-ID' field (use value of ENVID from ESMTP envelope of original message 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-

Information Element	MMS Read Report Element	[MDN] Element
		type' value 'deleted')
Status Text		Text in first part (human-readable part)

1

2 When an MMS Relay/Server generates an [MDN] in response to a mes-
3 sage received using ESMTP on MM3:

- 4 • Top-level header field 'To:' should be value of the 'Disposition-
5 Notification-To:' header field of the message whose disposition is being
6 reported.
- 7 • Top-level header field 'From:' should be the address of the recipient
8 that the read report concerns.

9 3.2.4.4 *Disposition Report Mapping from Internet Message to MMS*

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

12 **Table 3-8: Disposition Report Mapping from Internet Message to**
13 **MMS**

Information Element	MMS Read Report Element	[MDN] 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
Disposition of message being re-	X-Mms-Read-Status:	disposition-field

Information Element	MMS Read Report Element	[MDN] Element
ported	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)

1 **3.2.5 Message Delivery**

2 Within Internet mail, when ESMTP is used and delivery reports are re-
3 quested [DSN-SMTP], delivery is considered to be acceptance of a mes-
4 sage by the final server, that is, the server closest to the recipient. When
5 an MMS Relay/Server receives a message using ESMTP and a delivery
6 report is requested, the MMS Relay/Server may consider the message de-
7 livered when it has been sent to the MMS User Agent.

8 **4 Security Considerations**

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

14 The following messaging-related security threats can be identified:

- 15 • Misidentification of message source.
- 16 • Message interception (unauthorized disclosure of contents).
- 17 • Unauthorized disclosure of message sender or recipient.
- 18 • Message modification (by adversary).
- 19 • Message replay.
- 20 • Traffic analysis (determining who is communicating with whom).

1 There are existing mechanisms used to protect email traffic against some
2 of these threats, such as:

- 3 • Use of SSL/TLS (via [StartTLS]) to address disclosure and modifica-
4 tion in transit between adjacent servers.
- 5 • SMTP Authentication [Auth] can be used to protect against mis-
6 identification of message source.
- 7 • Use of end-to-end security mechanisms such as [PGP] or S/MIME
8 [SMIME] to protect message contents.
- 9 • Use of [IPSec] to address disclosure and modification in transit be-
10 tween adjacent servers.

11 These mechanisms should be employed whenever the required infra-
12 structure is available, e.g., a certificate infrastructure is necessary to
13 support S/MIME, or user agent support for PGP is available. Enabling
14 SMTP Authentication [Auth] and STARTTLS [StartTLS] are easy measures
15 to deploy and should be used.

16 Since MMS does not include a clear separation between in-transit enve-
17 lope and message content, there are increased risks of unauthorized dis-
18 closure information, and additional challenges in protecting data. For ex-
19 ample, Bcc recipients do not normally appear in the message content,
20 only in the envelope; care must be taken in the gateway function to en-
21 sure that Bcc recipients which do appear are deleted from the message
22 content.

23 Some MMS features contain inherently more risk than others. For exam-
24 ple, reply charging and sender address hiding. The reply charging
25 mechanism requires a high degree of trust between entities with little
26 technical basis. Deliberate or accidental abuse of this trust can result in
27 unexpected or unauthorized charges. For example, a sender may be
28 charged for unauthorized replies, or a sender may be charged for a reply
29 which the author thought would be paid for the recipient. A sender's
30 identity may be disclosed in violation of a request for this to be blocked.
31 The identity of recipients may be disclosed to other recipients (or even
32 non-recipients) for a message in which the sender intended for the recipi-
33 ents not to be disclosed.

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

38 Mechanisms can be developed to protect against various threats, how-
39 ever, these are not included in this version of this specification. It is
40 strongly recommended that features such as reply charging and sender
41 identity hiding **not** be used across carrier domains, and be used within
42 carrier domains only with full understanding of the risks involved.