[MS-XJRNL]:
Journal Record Message File Format

Intellectual Property Rights Notice for Open Specifications Documentation

Revision Summary

Date	Revision History	Revision Class	Comments
04/04/2008	0.1		Initial Availability.
04/25/2008	0.2		Revised and updated property names and other technical content.
06/27/2008	1.0		Initial Release.
08/06/2008	1.01		Revised and edited technical content.
09/03/2008	1.02		Revised and edited technical content.
12/03/2008	1.03		Updated IP notice.
04/10/2009	2.0		Updated technical content and applicable product releases.
07/15/2009	3.0	Major	Revised and edited for technical content.
11/04/2009	3.1.0	Minor	Updated the technical content.
02/10/2010	3.2.0	Minor	Updated the technical content.
05/05/2010	3.2.1	Editorial	Revised and edited the technical content.
08/04/2010	4.0	Major	Significantly changed the technical content.
11/03/2010	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
03/18/2011	4.0	No change	No changes to the meaning, language, and formatting of the technical content.
08/05/2011	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/07/2011	4.1	Minor	Clarified the meaning of the technical content.
01/20/2012	5.0	Major	Significantly changed the technical content.
04/27/2012	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
07/16/2012	5.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2012	6.0	Major	Significantly changed the technical content.
02/11/2013	6.0	No change	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction

The Journal Record Message File Format is used to format information about an e-mail message that is sent through the server. The Journal Record Message File Format extends the protocols specified in [RFC2045] and [RFC2046].

Sections 1.7 and 2 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in RFC 2119. All other sections and examples in this specification are informative.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

ASCII
Augmented Backus-Naur Form (ABNF)
Coordinated Universal Time (UTC)
distinguished name (DN)

The following terms are defined in [MS-OXGLOS]:

blind carbon copy (Bcc) recipient
body part
carbon copy (Cc) recipient
character set
distribution list
header
MIME content-type
MIME message
Multipurpose Internet Mail Extensions (MIME)
recipient
Simple Mail Transfer Protocol (SMTP)
To recipient

The following terms are specific to this document:

body: The contents of a body part or an entire message that contains several body parts, as described in [RFC2045].

encoding: A process that specifies a Content-Transfer-Encoding for transforming character data from one form to another.

MIME attachment: A body part that is in a MIME message, for example, an email message or a file that is attached to an email message.

recipient forwarding: A feature that enables a message to be redirected to a different email address, which is referred to as the "forwarded address," from the address to which it is sent originally. Depending on the implementation, a message can be redirected to the forwarded address without sending a copy to the original email address, or the original email address can additionally receive a copy of the message.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

References to Microsoft Open Specifications documentation do not include a publishing year because links are to the latest version of the technical documents, which are updated frequently. References to other documents include a publishing year when one is available.

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-OXMSG] Microsoft Corporation, "Outlook Item (.msg) File Format".

[MS-OXOABK] Microsoft Corporation, "Address Book Object Protocol".

[RFC2045] Freed, N., and Borenstein, N., "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996, http://ietf.org/rfc/rfc2045.txt

[RFC2046] Freed, N., and Borenstein, N., "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996, http://ietf.org/rfc/rfc2046.txt

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt

[RFC2821] Klensin, J., "Simple Mail Transfer Protocol", STD 10, RFC 2821, April 2001, http://www.ietf.org/rfc/rfc2821.txt

[RFC2822] Resnick, P., Ed., "Internet Message Format", STD 11, RFC 2822, April 2001, http://www.ietf.org/rfc/rfc2822.txt

[RFC5234] Crocker, D., Ed., and Overell, P., "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008, http://www.rfc-editor.org/rfc/rfc5234.txt

1.2.2 Informative References

[MSFT-WPXTJ] Microsoft Corporation, "White Paper: Exchange 2007 Transport Journaling", September 2007, http://technet.microsoft.com/en-us/library/bb738122(EXCHG.80).aspx

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary".

[MS-OXGLOS] Microsoft Corporation, "Exchange Server Protocols Master Glossary".

[MS-OXPROTO] Microsoft Corporation, "Exchange Server Protocols System Overview".

1.3 Overview

Journal record messages are **MIME messages** produced by the server that capture information about other (non-journal record) messages sent through the server. These non-journal record messages are referred to as original messages. Metadata about the original message is contained in the **Envelope-Part** structure in the Journal Record Message File Format. This format allows an administrator, for example, to log and review the **recipient (1)** of every outgoing message.

For background information about how journaling works, see [MSFT-WPXTJ].

1.3.1   Body Text of the Journal Record Message

The **body** text of the journal record message lists the e-mail addresses of the sender and recipients (1) of the original message, the subject, the Internet **Message-ID** field, and certain other metadata about the original message. The body text is referred to as the **Envelope-Part** structure of the journal record message.

1.3.2   Original Message

The original message is attached as a **MIME attachment** to the **Envelope-Part** structure. This is referred to as the **Original-Message-Part** structure of the journal record message. How the **Original-Message-Part** structure is attached to the **Envelope-Part** structure is fully described in [RFC2045] and [RFC2046].

1.4   Relationship to Protocols and Other Structures

The journal record MIME message conforms to [RFC2045] and [RFC2046]. [RFC2045] describes how messages with a **MIME content-type** of message/rfc822 might be nested recursively as MIME attachments. The outermost message/rfc822 **body part** of the journal record message contains the **Envelope-Part** structure as the body.

The **Envelope-Part** structure is encoded using the mechanisms described in [RFC2045], such as the Content-Transfer-Encoding mechanism, which specifies details such as the **character set** and **encoding** used for the data in the **Envelope-Part** structure. The mechanism for decoding the **Envelope-Part** structure is described in [RFC2045] section 6.

The following figure shows how the **Envelope-Part** structure is placed in relation to the various other structures in the journal record MIME message.

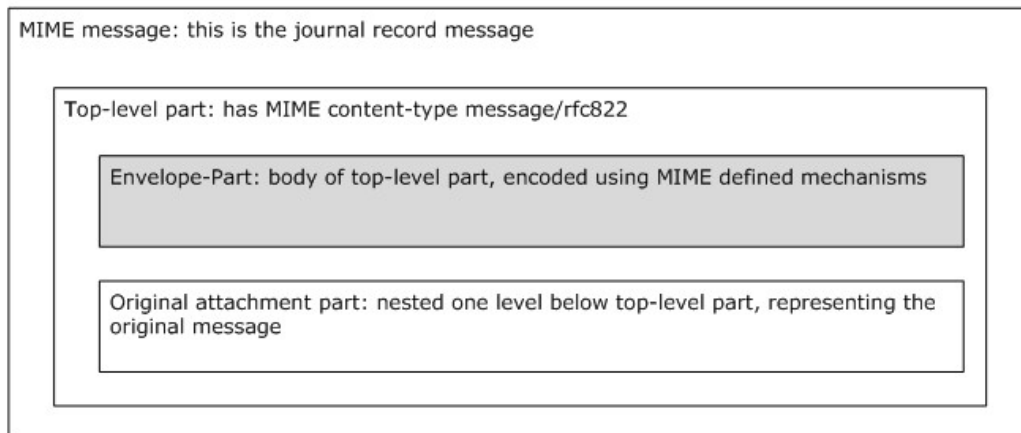

Figure 1: MIME structure of a journal record message

For conceptual background information and overviews of the relationships and interactions between this and other protocols, see [MS-OXPROTO].

1.5 Applicability Statement

Applications can use this format to create and consume journal record messages.

1.6 Versioning and Localization

None.

1.7 Vendor-Extensible Fields

None.

2 Structures

The Journal Record Message File Format extends the structures defined in [RFC2045] and [RFC2046] by defining a structure called the **Envelope-Part** structure, which is embedded within the MIME message.

2.1 Envelope-Part Structure

The **Envelope-Part** structure is the body text of the journal record message. The **Envelope-Part** structure contains metadata about the original message. The format of the **Envelope-Part** structure is specified by using the **Augmented Backus-Naur Form (ABNF)** notation, as specified in [RFC5234]. The format is a series of field/value pairs on CRLF-terminated lines. The format, prior to the application of any **MIME** encoding, is as follows.

```
<Envelope-Part>          = <sender> CRLF
                            [<sent-on-behalf> CRLF]
                            (<subject> CRLF <message-id> CRLF) / (<message-id> CRLF <subject>
CRLF)
                            [<label> CRLF]
                            [<mailbox-owner> CRLF]
                            1*<recipient-specification>
                            [<sent-time> CRLF]
                            [<received-time> CRLF]

<sender>                 = "Sender:" SP <reverse-path>
<sent-on-behalf>         = "On-Behalf-Of:" SP <on-behalf-path>
<subject>                = "Subject:" SP <subject-string>
<message-id>             = "Message-ID:" SP <msg-id>
<label>                  = "Label:" SP 1*255CHAR
<mailbox-owner>          = "Mailbox:" SP <mailbox-owner-address>
<recipient-specification> = <recipient-p2-type> ":" SP <forward-path>
                            ["," SP <redirection-type> ":" SP <original-forward-path>] CRLF
<sent-time>              = "SentUtc:" SP <sent-time-string>
<received-time>          = "ReceivedUtc:" SP <received-time-string>

<recipient-p2-type>      = "Bcc" / "To" / "Cc" / "Recipient"
<redirection-type>       = "Expanded" / "Forwarded"
```

2.1.1 sender Field

Within the **sender** field, the **reverse-path** field MUST be set to the e-mail address of the sender of the original message. The **reverse-path** field MUST be formatted as one of the following:

- A **Simple Mail Transfer Protocol (SMTP)** e-mail address, as specified in [RFC2821].

- A **distinguished name (DN) (1)** address formatted according to the following ABNF notation. The format for x500-dn is specified in [MS-OXOABK] section 2.2.1.1.

  <distinguished-name-address> = "[EX:" x500-dn "]"

2.1.2 subject Field

Within the **subject** field, the **subject-string** field MUST contain the data from the "Subject" **header (2)** of the original message. This header (2) is specified in [RFC2822].

The value of the **subject-string** field can consist of characters outside the **ASCII** character set range, as specified in [RFC2045] and [RFC2046]. The MIME content-type header (2) of the respective body part in which the **Envelope-Part** structure is embedded MUST specify the character set to use to interpret the value of the **subject-string** field in accordance with the MIME specifications [RFC2045] and [RFC2046].

2.1.3 message-id Field

Within the **message-id** field, the **msg-id** field MUST contain the value of the **Message-ID** field, as specified in [RFC2822] section 3.6.4, of the original message.

2.1.4 recipient-specification Field

The **recipient-specification** field contains information about the recipients (1) of the original message. This field can have one or more occurrences.

2.1.4.1 recipient-p2-type Field

The **recipient-p2-type** field MUST be set with a value from the following table.

Value	Meaning
Bcc	The recipient (1) listed in the **forward-path** field is addressed as a **blind carbon copy (Bcc) recipient**.
To	The recipient (1) listed in the **forward-path** field is addressed as a **To recipient**.
Cc	The recipient (1) listed in the **forward-path** field is addressed as a **carbon copy (Cc) recipient**.
Recipient	The server is unable to determine how the recipient (1) is addressed.

2.1.4.2 forward-path Field

The **forward-path** field MUST be set to the e-mail address of a recipient (1) of the original message. This address MUST be formatted in one of the following formats:

▪ An SMTP e-mail address, as specified in [RFC2821].

▪ A DN (1) address, as specified in section 2.1.1.<1>

Neither format is preferred over the other. The choice of format is left to the implementation.

2.1.4.3 redirection-type Field

The value of the **redirection-type** field MUST be set to either "Expanded" or "Forwarded".

2.1.4.3.1 Expanded Value

The **redirection-type** field, when set to "Expanded", indicates that the sender of the message sent it originally to the address specified by the value of the **original-forward-path** field, which was the address of a **distribution list**. This distribution list was then expanded to one or more recipients (1), perhaps expanding nested recipients (1) repeatedly until all recipients (1) were non-distribution list recipients (1). Each of these expanded recipients (1) is listed in the **forward-path** field of an occurrence of the **recipient-specification** field.

2.1.4.3.2 Forwarded Value

The **redirection-type** field, when set to "Forwarded", indicates that the recipient (1) indicated by the **original-forward-path** field was configured for **recipient forwarding**. The message was forwarded to the recipient (1) indicated by the **forward-path** field.

2.1.4.4 original-forward-path Field

The **original-forward-path** field contains the e-mail address of the recipient (1) that was redirected to the address contained in the **forward-path** field. The address contained in the **original-forward-path** field MUST be formatted in one of the following formats:

- An SMTP e-mail address, as specified in [RFC2821].

- A DN (1) address, as specified in section 2.1.1.<2>

Neither format is preferred over the other. The choice of format is left to the implementation.

The **original-forward-path** field, although syntactically identical to the **forward-path** field, has different semantics. The appearance of the **redirection-type** and **original-forward-path** fields in an occurrence of the **recipient-specification** field indicates that the original message was sent to the recipient (1) with the address contained in the **original-forward-path** field and the server did one of the following:

- Changed the recipient (1) address to the address contained in the **forward-path** field.

- Added a new recipient (1) with the address contained in the **forward-path** field due to the recipient (1) with the address contained in the **original-forward-path** field being present.

If the **redirection-type** and **original-forward-path** fields are omitted, the server did not have information about what type of forwarding or expansion was done on the recipient (1) when it generated the journal record message.

2.1.5 label Field

The **label** field is optional. If present, this field MUST contain a text value, the contents of which are implementation-specific.

2.1.6 sent-on-behalf Field

The **sent-on-behalf** field is optional. If this field is present, it contains the e-mail address of the sending mailbox owner. This e-mail address MUST be different from the address contained in the **reverse-path** field. This address MUST be formatted in one of the following formats:

- An SMTP e-mail address, as specified in [RFC2821].

- A DN (1) address, as specified in section 2.1.1.

Neither format is preferred over the other. The choice of format is left to the implementation.

2.1.7 mailbox-owner Field

The **mailbox-owner** field is optional. If this field is present, the **mailbox-owner-address** field contains the SMTP e-mail address of the sending mailbox owner.

2.1.8   sent-time Field

The **sent-time** field is optional. If this field is present, it contains the **sent-time-string** field, which contains a string that indicates the date and time, in **Coordinated Universal Time (UTC)**, that the original message was sent. The exact format of the string contained in the **sent-time-string** field is left to the implementation.

The **sent-time** field can begin with either "SentUtc" or "Sent".<3> The meaning is the same regardless of which string is used.

2.1.9   received-time Field

The **received-time** field is optional. If this field is present, it contains the **received-time-string** field, which contains a string that indicates the date and time, in **UTC**, that the original message was received. The exact format of the string contained in the **received-time-string** field is left to the implementation.

The **received-time** field can begin with either "ReceivedUtc" or "Received".<4> The meaning is the same regardless of which string is used.

2.2   Original-Message-Part Structure

The **Original-Message-Part** structure MUST contain one of the following:

- A MIME attachment of type message/rfc822.

- A .msg file, as specified in [MS-OXMSG].

Neither format is preferred over the other. The choice of format is left to the implementation.

3 Structure Examples

The following is an example of the **Envelope-Part** structure contained in a journal record message, followed by an explanation of the various syntax elements. Note that the line numbers are not present in the actual **Envelope-Part** structure but are shown here so that the structure can be discussed line by line.

```
1 Sender: sender@contoso.com
2 Subject: Sample Message
3 Message-ID: <12345@contoso.com>
4 To: dl-to-member1@contoso.com, Expanded: dl-to@contoso.com
5 To: dl-to-member2@contoso.com, Expanded: dl-to@contoso.com
6 Cc: fwd@contoso.com, Forwarded: user@contoso.com
7 Bcc: dl-bcc-member@contoso.com, Expanded: dl-bcc@contoso.com
8 Bcc: fwd2@contoso.com, Forwarded: user2@contoso.com
9 Recipient: user-unk@contoso.com
```

1. The sender of the original message was sender@contoso.com.

2. The subject of the original message was "Sample Message".

3. The value of the **Message-ID** field, as specified in [RFC2822] section 3.6.4, of the original message was "12345@contoso.com".

4. The original message was sent to dl-to@contoso.com as a To recipient, which is a distribution list that was expanded to dl-to-member1@contoso.com and dl-to-member2@contoso.com (captured in line 5) by the server.

5. See (4).

6. The original message was sent to user@contoso.com as a Cc recipient, which was changed by the e-mail server to fwd@contoso.com because recipient forwarding was configured. user@contoso.com did not receive a copy of the message because there is no occurrence of the **recipient-specification** field where user@contoso.com was listed in the **forward-path** field.

7. The original message was sent by the mail client to dl-bcc@contoso.com as a Bcc recipient, which is a distribution list that was expanded to dl-bcc-member@contoso.com.

8. The original message was sent to user2@contoso.com as a Bcc recipient, which was rewritten by the e-mail server to fwd2@contoso.com because recipient forwarding was configured. user2@contoso.com did not receive a copy of the message because there is no occurrence of the **recipient-specification** field where user2@contoso.com was listed in the **forward-path** field.

9. Finally, there is no information about whether user-unk@contoso.com was sent the original message as a To recipient, Cc recipient, or Bcc recipient. It is also not known whether this recipient (1) received the message due to distribution list expansion, recipient forwarding, or being directly addressed by the sender. The value of the **recipient** field indicates that the server was only able to capture that user-unk@contoso.com was a recipient (1) of the message and no further recipient (1) metadata was available.

4 Security

4.1 Security Considerations for Implementers

This format does not implement or concern itself with security but relies on the underlying e-mail transport software and e-mail storage software to provide security as applicable.

4.2 Index of Security Fields

None.

5   Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft Exchange Server 2007

- Microsoft Exchange Server 2010

- Microsoft Exchange Server 2013

- Microsoft Office Outlook 2007

- Microsoft Outlook 2010

- Microsoft Outlook 2013

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

<1> Section 2.1.4.2: Exchange 2007 does not support the DN (1) address format for the **forward-path** field.

<2> Section 2.1.4.4: Exchange 2007 does not support the DN (1) address format for the **original-forward-path** field.

<3> Section 2.1.8: Exchange 2007 begins the **sent-time** field with "Sent". Exchange 2010 and Exchange 2013 begin the **sent-time** field with "SentUtc".

<4> Section 2.1.9: Exchange 2007 begins the **received-time** field with "Received". Exchange 2010 and Exchange 2013 begin the **received-time** field with "ReceivedUtc".

6 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

7 Index

Release: February 11, 2013