

Network Working Group
Internet-Draft
Updates: 3462, 3464, 3798, 3886 (if approved)
Expires: January 10, 2006

B. Lilly
July 2005

Extensible Message Application Interchange Language (EMAIL) --
Part Two: Syntax, Semantics, and Media Types
draft-lilly-extensible-internet-message-format-p02-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright © The Internet Society (2005).

Abstract

The Internet Message Format originally formally specified in RFC 561 has been extended in some ways and for some purposes which have posed difficulties for some desirable operations such as digitally signed messages, have led to clutter in message content which in turn has led user agent implementers to suppress display of some originator message content, leading in some cases to user confusion, surprise, and embarrassment. This memo is part of a multi-document series that specifies an extensible message format which is intended to facilitate operations hampered by extensions to the current format and to reduce clutter in the user-to-user message content. This memo defines and provides registration information for media types relevant to the extensible message format.

Table of Contents

- 1. Introduction..... 3
- 2. Multipart/email..... 3
 - 2.1. Semantics..... 3
 - 2.2. Syntax..... 3
 - 2.3. Media Type Registration..... 5
- 3. Message/email..... 7
 - 3.1. Semantics..... 7
 - 3.2. Syntax..... 7
 - 3.3. Media Type Registration..... 8
- 4. Security Considerations..... 9
- 5. Internationalization Considerations..... 9
- 6. IANA Considerations..... 9
- Appendix A. Disclaimers..... 9
- Normative References..... 10
- Informative References..... 10
- Author's Address..... 11

1. Introduction

This memo will introduce two new media types which are used in the construction of an extensible message format. Semantics of each media type will be presented in prose, syntax will be presented in accompanying normative prose, incorporating keywords defined in [N1.BCP14], and media type registration data will be presented using the form specified in [I1.MediaReg].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in [N1.BCP14],

2. Multipart/email

2.1. Semantics

The multipart/email media type denotes an extensible wrapper which contains a message, separate transport markings, and may contain ancillary information. It can be thought of as roughly equivalent to the "envelope" of a physical message. Unlike many physical envelopes, the multipart/email wrapper has separate compartments for the originator's message, routing and filing instructions, transport markings, classification schemes, etc. Also unlike most physical messages, the wrapper provides for multiple representations of originator content, providing a backward-compatible migration path which may be used to resolve limitations of RFC 561/680/724/733/822/2822 Internet message format [I2.RFC561], [I3.RFC680], [I4.RFC724], [I5.RFC733], [I6.STD11], [I7.RFC2822].

2.2. Syntax

The general syntax follows multipart media syntax as specified in section 5.1.1 of [N2.RFC2046]. There must be at least one body part, and exactly one body part MUST have type multipart/alternative. That multipart/alternative part MUST itself contain at least one body part and all body parts within that multipart/alternative part must have message type. An example of a simple case would have a single part of type message/rfc822. Each body part within the multipart/alternative part contains end-to-end, user-to-user content formatted according to the rules of the corresponding message type. As specified in [N2.RFC2046] section 5.1.4, order of parts within the multipart/alternative part is significant. Order of body parts within the multipart/email wrapper is not significant.

Aside from the required multipart/alternative composite media type containing the end-to-end message format(s), other media types enclosed in the multipart/email wrapper comprise ancillary data. It is RECOMMENDED that media types defined to hold ancillary data be defined as subtypes of the message top-level MIME type to permit both structured (as fields) and unstructured content. Some initial types will be proposed in a companion document [TBD]. The multipart/email wrapper SHOULD NOT directly contain a component of type message/rfc822; end-to-end message content is wrapped in the multipart/alternative component to provide extensibility.

Using the notation given in [I8.Intro], the simple case example has the following structure:

```
multipart/email 0
  multipart/alternative 1
    message/rfc822 1.1
      text/plain 1.1.1
    close delimiter 1
  close delimiter 0
```

Note that the message/rfc822 part within the multipart/alternative part need not be a simple message; it MAY be a complex MIME message. An OpenPGP [I9.RFC3156] signed and encrypted message body with ancillary information generated by the originator's MUA could have the following structure:

```
multipart/email 0
  multipart/alternative 1
    message/rfc822 1.1
      multipart/encrypted 1.1.1
        application/pgp-encrypted 1.1.1.1
        application/octet-stream 1.1.1.2
      close delimiter 1.1.1
    close delimiter 1
  message/omua 2
  close delimiter 0
```

In the example above, the message body is encrypted, but the header is not. That may leave some information accessible to an eavesdropper. Alternatively, the encrypted content could include an entire message/rfc822 media type object, and the plaintext header could consist of placeholder fields. Note that details of the signing and encryption operations are not specified by this media type, and may have vulnerabilities. The media type provides a mechanism to isolate the end-to-end content from signature-breaking operations performed by transport agents; by itself the media type provides no guarantees of security or privacy for that content, nor can it protect against damage caused by non-compliant transport or transport-related agents. In particular, the layered aspect of signing and encryption used by some mechanisms leaves content open to vulnerabilities such as signature replacement, eavesdropping, and/or surreptitious forwarding.

2.3. Media Type Registration

Type name: multipart

Subtype name: email

Required parameters:

boundary: per [N2.RFC2046] section 5.1.1

version: An unsigned decimal integer number indicating the version of the media type specification. The value corresponding to this specification is 1.

A version value change requires a new specification. A specification revision entailing any of the following means that a new version is REQUIRED:

- addition of a mandatory part
- specification such that existence or content of some part affects processing or display of the message as a whole or of any part other than the specific part whose existence or content is concerned

A media type definition suitable as an optional part does not require a new version of multipart/email unless the second item above applies.

Once a mandatory part is added to the specification (with a corresponding new version), that part MUST NOT subsequently be made optional. That prohibition is necessary to ensure backward compatibility of new versions. Consequently, addition of a mandatory part is a change that should not be made lightly.

Optional parameters: none

Encoding considerations: Encoding MUST be one of 7bit, 8bit, or binary per section 6.4 of [N3.RFC2045] and section 5.1 of [N2.RFC2046]. Encoding specified via a Content-Transfer-Encoding field MUST be consistent with enclosed media type domains and with the [N3.RFC2045] and [N2.RFC2046] requirements noted above.

Restrictions on usage: none

Security considerations: Making it easier for users and applications to find specific information necessarily makes it easier for attackers to find such information.

Separating the end-to-end message information from transport markings facilitates digital signing and/or encryption of that communication, including header information, impeding

eavesdropping and similar attacks. It facilitates confidentiality, data integrity, and data origin authentication when used with message security mechanisms applied to the end-to-end message contained within the wrapper.

This media type does not address security issues such as inappropriate usage and denial of service.

Content could be moved from one wrapper to another, or unsigned content in the wrapper could be added, elided, or modified by an attacker. Specification of optional content formats SHOULD make provision for signing and/or encryption of that content if security or privacy are concerns.

Interoperability considerations: Because the format of an EMAIL message is a MIME object, it can be handled by MIME-capable user agents, or by non-MIME-aware agents via an external package such as metamail [I10.Metamail]. Initially, many agents will not recognize the multipart/email type, and will treat it as multipart/mixed in accordance with [N2.RFC2046] section 5.1.3. That is reasonable, since the multipart/email type is in fact treated like multipart/mixed, but carries the semantics of a wrapped message and has specific message-related specifications. A wrapped message of type message/rfc822 contained within the multipart/alternative wrapper will be recognized (some existing UAs, tested prior to publication of the initial draft of this document, display the message inline, others may require that the MIME part be selected). Alternative new message subtypes, both for compartmentalizing ancillary data and for alternative end-to-end message content formatting which are unrecognized are treated as equivalent to application/octet-stream, per [N2.RFC2046] section 5.2.4. Some UAs in fact present that content inline, although that is non-conforming behavior [I11.RFC2049] (section 2, paragraph labeled "(4)").

These characteristics (appropriate handling of the wrapper, the embedded multipart/alternative, and the internal message/rfc822 message) are necessary and sufficient to meet the goal of backward compatibility for the purpose of end-to-end communications.

Handling of ancillary information will progress at a rate dependent on the perceived need for such handling; likewise for development, deployment, and recognition of alternative message content formats (with message/rfc822 retained in the multipart/alternative wrapper for the foreseeable future as a fallback for legacy UAs). In the meantime, separation of such ancillary data and transport markings from the end-to-end message content enables end-to-end authentication of that message content without invalidation of digital signatures (because transport, including gateways, is prohibited from modifying the MIME-wrapped end-to-end message per [N2.RFC2046] section 5.2). That feature alone may be instrumental in reduction of the amount of messaging-based fraud which is rampant at the time of writing of this memo.

Published specification: This document.

Applications which use this media type: Any applications using MIME and the Internet Message Format

Additional information:

Magic number(s): None

File extension(s): Files do not require any specific "extension" or suffix. Many are in use as a convenience for mechanized processing of files. File names are orthogonal to the nature of the content. In particular, while a file name or a component of a name may be useful in some types of automated processing of files, the name or component might not be capable of indicating subtleties. This media type SHOULD NOT be assigned a relationship with any file "extension" where content may be untrusted unless there is provision for human judgment which may be used to override that relationship for individual files. Where appropriate, a filename MAY be suggested by a suitable mechanism such as the one specified in [I12.RFC2183] as amended by [I13.RFC2231] and .

Macintosh File Type Code(s): unknown

Person & email address to contact for further information:

Bruce Lilly
blilly@erols.com

Intended usage: COMMON

Author/Change controller: IESG

3. Message/email

3.1. Semantics

The message/email media type holds a complete message consisting of a MIME-conforming message header and a body type containing a multipart/email composite media type. It is similar to message/rfc822 but has the added semantics of the extensible format.

3.2. Syntax

Overall syntax is that of MIME message types and is similar to that of message/rfc822 with a composite MIME body. Note that due to optional extension parts, the content might require 8bit or binary transport.

3.2.1. Usage

The message/email media type may be used in the same places as message/rfc822 provided there are no conflicts which would prevent such use. In particular, it may be used as an alternative to

message/rfc822 in a multipart/report media type [N4.RFC3462] as used by DSNs [I14.RFC3464], MDNs [I15.RFC3798], and MSTNs [I16.RFC3886]. For backward compatibility, a message/email media type which meets the syntax of message/rfc822 MAY be relabeled as message/rfc822 when used in a multipart/report composite media type.

3.3. Media Type Registration

Type name: message

Subtype name: email

Required parameters:

version: An unsigned decimal integer number indicating the version of the media type specification. The value corresponding to this specification is 1.

Optional parameters: none

Encoding considerations: Encoding MUST be one of 7bit, 8bit, or binary per section 6.4 of [N3.RFC2045] and section 5.1 of [N2.RFC2046] . Encoding specified via a Content-Transfer-Encoding field MUST be consistent with enclosed media type domains and with the [N3.RFC2045] and [N2.RFC2046] requirements noted above.

Restrictions on usage: none

Security considerations: As with any message media type, content can be forged or replaced via a man-in-the-middle. Security multiparts [I17.RFC1847] may be used to provide some protection.

Interoperability considerations: This media type will be treated as application/octet-stream by MIME-conforming [I11.RFC2049] implementations which do not recognize the media subtype. In many cases, the content can be saved and treated as message/rfc822 with MIME content.

Published specification: This document.

Applications which use this media type: Any applications using MIME and the Internet Message Format

Additional information:

Magic number(s): None

File extension(s): Files do not require any specific "extension" or suffix. Many are in use as a convenience for mechanized processing of files. File names are orthogonal to the nature of the content. In particular, while a file name or a component of a name may be useful in some types of automated processing of files, the name or component might not be

capable of indicating subtleties. This media type SHOULD NOT be assigned a relationship with any file "extension" where content may be untrusted unless there is provision for human judgment which may be used to override that relationship for individual files. Where appropriate, a filename MAY be suggested by a suitable mechanism such as the one specified in [I18.RFC2183] as amended by [I13.RFC2231] and .

Macintosh File Type Code(s): unknown

Person & email address to contact for further information:

Bruce Lilly
blilly@erols.com

Intended usage: COMMON

Author/Change controller: IESG

4. Security Considerations

Security considerations relevant to media types are discussed in the media type registration form data in this memo.

5. Internationalization Considerations

This memo raises no new internationalization considerations. It identifies some internationalization issues in general terms, and discusses an approach to those issues, also in general terms.

6. IANA Considerations

Upon approval by the IESG, IANA SHALL register the media types defined in this document.

Appendix A. Disclaimers

This document has exactly one (1) author.

In spite of the fact that the author's given name may also be the surname of other individuals, and the fact that the author's surname may also be a given name for some females, the author is, and has always been, male.

The presence of "or she", "/SHE", "each", "their", and "authors" (plural) in the boilerplate sections of this document is irrelevant.

As noted in the "Status of this Memo" section, this document is an Internet-Draft, and as such is a "work in progress", not a standard. Reference to this document's contents as "this standard" in the boilerplate are inappropriate.

The author of this document is not responsible for the boilerplate text.

Comments regarding the silliness, lack of accuracy, and lack of precision of the boilerplate text should be directed to the IESG, not to the author.

Normative References

- [N1.BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [N2.RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.
- [N3.RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.
- [N4.RFC3462] Vaudreuil, G., "The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages", RFC 3462, January 2003.

Informative References

- [I1.MediaReg] Freed, N. and J. Klensin, "Media Type Specifications and Registration Procedures" (draft-freed-media-type-reg-04.txt), April 2005.
- [I2.RFC561] Bhushan, A., Pogran, K., Tomlinson, R., and J. White, "Standardizing Network Mail Headers", RFC 561, September 1973.
- [I3.RFC680] Myer, T. and D. Henderson, "Message Transmission Protocol", RFC 680, April 1975.
- [I4.RFC724] Crocker, D., Pogran, K., Vittal, J., and D. Henderson, "Proposed official standard for the format of ARPA Network messages", RFC 724, May 1977.
- [I5.RFC733] Crocker, D., Vittal, J., Pogran, K., and D. Henderson, "Standard for the format of ARPA network text messages", RFC 733, November 1977.
- [I6.STD11] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.
- [I7.RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.
- [I8.Intro] Lilly, B., "Extensible Message Application Interchange Language (EMAIL) -- Part One: Introduction and Overview", (draft-lilly-extensible-message-format-p1-00.txt), June 2005.

- [I9.RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, August 2001.

- [I10.Metamail] <http://guppylake.com/~nsb/metamail/mm2.7.tar.Z>

- [I11.RFC2049] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples", RFC 2049, November 1996.

- [I12.RFC2183] Troost, R., Dorner, S., and K. Moore, "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field", RFC 2183, August 1997.

- [I13.RFC2231] Freed, N. and K. Moore, "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", RFC 2231, November 1997.

- [I14.RFC3464] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 3464, January 2003.

- [I15.RFC3798] Hansen, T. and G. Vaudreuil, "Message Disposition Notification", RFC 3798, May 2004.

- [I16.RFC3886] Allman, E., "An Extensible Message Format for Message Tracking Responses", RFC 3886, September 2004.

- [I17.RFC1847] Galvin, J., Murphy, S., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

- [I18.RFC2183] Troost, R., Dorner, S., and K. Moore, "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field", RFC 2183, August 1997.

Author's Address

Bruce Lilly

Email: blilly@erols.com

Full Copyright Statement

Copyright © The Internet Society (2005).

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.

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.

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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