Workgroup: dispatch
Internet-Draft:
draft-mahy-dispatch-immi-content-00
Published: 7 March 2022
Intended Status: Informational
Expires: 8 September 2022
Authors: R. Mahy
Wire

Inside MLS Message Interop (IMMI) instant message content

Abstract

This document defines a profile intended for instant messaging interoperability of messages end-to-end encrypted inside the MLS (Message Layer Security) Protocol. It adapts prior work (CPIM) to work well in the MLS context.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 8 September 2022.

Table of Contents

1. Terminology
2. Introduction
3. Overview
   3.1. Naming schemes
   3.2. Negotiation of MIME types
   3.3. CPIM and MIME headers
4. Example
   4.1. Original Message
   4.2. Reply
   4.3. Reaction
   4.4. Mentions
   4.5. Edit
   4.6. Delete
   4.7. Expiring
   4.8. Knock
   4.9. Read Receipt
   4.10. Attachments
   4.11. Conferencing
5. IMMI CPIM profile
   5.1. CPIM headers
   5.2. Definition of message/immi-disposition-notification
   5.3. Required and Recommended MIME types
6. IANA Considerations
   6.1. MIME subtype registration of message/immi-disposition-notification
7. Security Considerations
8. Normative References
9. Informative References

Author's Address

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2219].

The terms MLS client, MLS group, and KeyPackage have the same meanings as in the MLS protocol [I-D.ietf-mls-protocol].

2. Introduction

MLS [I-D.ietf-mls-protocol] is a group key establishment protocol motivated by the desire for group chat with efficient end-to-end encryption. While one of the motivations of MLS is interoperable standards-based secure messaging, the MLS protocol does not define or prescribe any format for the encrypted "application messages" encoded by MLS. The development of MLS was strongly motivated by the

needs of a number of Instant Messaging (IM) systems, which encrypt messages end-to-end using variations of the Double Ratchet protocol [].

End-to-end encrypted instant messaging was also a motivator for the Common Protocol for Instant Messaging (CPIM) [RFC3862], however the model used at the time assumed standalone encryption of each message using a protocol such as S/MIME [RFC8551] or PGP [RFC3156] to interoperate between IM protocols such as SIP [RFC3261] and XMPP [RFC6120]. For a variety of practical reasons, interoperable end-to-end encryption between IM systems was never deployed commercially.

There are now several vendors prepared to implement MLS. In order to enable interoperable messaging conveyed "inside" MLS application messages, some additional specification and some minor changes are required. Also, the expectation of what constitutes basic features common across multiple IM systems has grown. It would be beneficial to provide an interoperable format for these additional features as well. Most of these features can be implemented using a profile which describes how to use already-defined URIs, message headers, and MIME types.

This proposal assumes that MLS clients can advertise MIME types they support and that MLS clients can determine what MIME types are required to join a specific MLS group. A companion proposal [I-D.mahy-dispatch-immi-mls-mime] defines two MLS extensions which meets this requirement. It would allow implementations to define groups with different MIME type requirements and it would allow MLS clients to send extended or proprietary messages that would be interpreted by some members of the group while assuring that an interoperable end-to-end encrypted baseline is available to all members, even when the group spans multiple systems or vendors.

Below is a list of some features commonly found in IM group chat systems:

*plain text and rich text messaging
*delivery notifications
*read receipts
*replies
*reactions
*edit or delete previously sent messages
*expiring messages
*knock / ping
*shared files/audio/videos
*calling / conferencing

3. Overview

3.1. Naming schemes

IM systems have a number of types of identifiers. Not all systems use every type:

- *client/device identifier (internal representation)
- *user identifier
- *handle identifier (external, friendly representation)
- *group conversation identifier
- *group or or channel name (external, friendly representation)
- *team identifier (less common)

One user may have multiple clients (for example a mobile and a desktop client). A handle may refer to a single user or it may redirect to multiple users. In some systems, the user identifier is a handle. In other systems the user identifier is an internal representation, for example a UUID. Handles may be changed/renamed, but hopefully internal user identifiers do not. Unqualified handles are often prefixed with a commercial at-sign ("@").

Likewise, group conversation identifiers could be internal or external representations, whereas group names or channel names are often external friendly representations. Unqualified channel names are often prefixed with a hash character ("#"). Some systems have an additional level of hierarchy with a team identifier under which groups/channels can be organized and authorized.

This proposal relies on URIs for naming and identifiers. All the example use the im: URI scheme (defined in [RFC3862]), but any instant messaging scheme is acceptable.

3.2. Negotiation of MIME types

As most IM systems are proprietary, standalone systems, it is useful to allow clients to send and receive proprietary formats among themselves. Using the multipart/alternative MIME wrapper, clients can send a message using the basic functionality described in this document AND a proprietary format for same-vendor clients simultaneously over the same group with end-to-end encryption.

[I-D.mahy-dispatch-immi-mls-mime] contains the actual MLS extensions useful for negotiating MIME types. The profile in this document requires support for receiving message/cpim, text/plain, text/markdown, and multipart MIME. All other mime types (including some recommended in this profile) are optional.

Example sending this profile and proprietary messaging protocol simultaneously.

```
Content-type: multipart/alternative
```

3.3. CPIM and MIME headers

We assume that an MLS group is already established and that either out-of-band or using the MLS protocol or MLS extensions that the following is known to every member of the group:

- The membership of the group (via MLS).
- The identity of any MLS client which sends an application message (via MLS).
- The MLS group ID (via MLS)
- The human readable name(s) of the MLS group, if any (out-of-band or extension).
- Which MIME types are mandatory to implement (proposed extension).
- For each member, the MIME types each supports (proposed extension).

For all messages the message header equivalent of To (the MLS group) and Sender fields (MLS sender) is already known and is therefore redundant. Every message contains a message/cpim header which includes the From, DateTime, and Message-ID fields. The From field contains the external, user-friendly representation of the Sender.

Messages sent to an MLS group are delivered to every member of the group active during the epoch in which the message was sent.

It is also mandatory to understand are the following MIME headers:

- Content-Type
- Content-Disposition
- Content-Length

4. Example

4.1. Original Message

In this example, Alice Smith sends a rich-text (Markdown) [RFC7763] message to the Engineering Team MLS group. The following values are implied as if headers were present:

- Implied Sender header from MLS sender: im:3b52249d-68f9-45ce-8bf5-c799f3cad7ec-0003@example.com
- Implied To header from MLS group: "Engineering Team" im:9dc867ca-3a01-4385-bb69-1573601c3c0c@example.com

```
Content-type: message/cpim

From: <im:alice-smith@example.com>
DateTime: 2022-02-08T22:13:45-00:00
Message-ID: <28fd19857ad7@example.com>

Content-Type: text/markdown;charset=utf-8

Hi everyone, we just shipped release 2.0. __Good work__!
```

4.2. Reply

A reply message looks similar, but contains an In-Reply-To CPIM header with the ID of the original message. The implied To header is the same all example messages in this section. The implied Sender header is always the MLS sender, and will not be shown in subsequent example messages.

```
Content-type: message/cpim

From: <im:bob-jones@example.com>
DateTime: 2022-02-08T22:13:57-00:00
Message-ID: <e701beee59f9@example.com>
In-Reply-To: <28fd19857ad7@example.com>

Content-Type: text/markdown;charset=utf-8

Right on! _Congratulations_ 'all!
```

4.3. Reaction

A reaction, uses the reaction Content-Disposition token defined in [RFC9078]. This Content-Disposition token indicates that the intended disposition of the contents of the message is a reaction.

The content in the sample message is a single Unicode heart character (U+2665). Discovering the range of characters each implementation could render as a reaction can occur out-of-band and is not within the scope of this proposal. However, an implementation which receives a reaction character string it does not recognize could render the reaction as a reply, possibly prefixing with a localized string such as "Reaction: ". Note that a reaction could theoretically even be another media type (ex: image, audio, or video), although not currently implemented in major instant messaging systems.

```
Content-type: message/cpim

From: <im:cathy-washington@example.com>
DateTime: 2022-02-08T22:13:57-00:00
Message-ID: <1a771ca1d84f@example.com>
In-Reply-To: <28fd19857ad7@example.com>

Content-Type: text/plain;charset=utf-8
Content-Disposition: reaction

♥
```

4.4. Mentions

In instant messaging systems and social media, a mention allows special formatting and behavior when a name, handle, or tag associated with a known group is encountered, often when prefixed with a commercial-at "@" character for mentions of users or a hash "#" character for groups or tags. A message which contains a mention may trigger distinct notifications on the IM client.

We can convey a mention by linking the user, handle, or tag URI in Markdown or HTML rich content. For example, a mention using Markdown is indicated below.

```
Content-type: message/cpim

From: <im:cathy-washington@example.com>
DateTime: 2022-02-08T22:14:03-00:00
Message-ID: <4dcab7711a77@example.com>

Content-Type: text/markdown;charset=utf-8

Kudos to [@Alice Smith](im:alice-smith@example.com)
for making the release happen!
```

The same mention using HTML [W3C.CR-html52-20170808] is indicated below.

```
Content-type: message/cpim

From: <im:cathy-washington@example.com>
DateTime: 2022-02-08T22:14:03-00:00
Message-ID: <4dcab7711a77@example.com>

Content-Type: text/html;charset=utf-8

<p>Kudos to <a href="im:alice-smith@example.com">@Alice
Smith</a> for making the release happen!</p>
```

4.5. Edit

Unlike with email messages, it is common in IM systems to allow the sender of a message to edit or delete the message after the fact. Typically the message is replaced in the user interface of the receivers (even after the original message is read) but shows a visual indication that it has been edited.

We reuse the Supersedes header from MIXER [RFC2156], because the semantics are correct: the message included in the body is a replacement for the message with the superseded message ID.

Here Bob Jones corrects a typo in his original message:

```
Content-type: message/cpim

From: <im:bob-jones@example.com>
DateTime: 2022-02-08T22:13:57-00:00
Message-ID: <89d3472622a4@example.com>
Supersedes: <e701beee59f9@example.com>

Content-Type: text/markdown;charset=utf-8

Right on! _Congratulations_ y'all!
```

4.6. Delete

In IM systems, a delete means that the author of a specific message has retracted the message, regardless if other users have read the message or not. Typically a placeholder remains in the user interface showing that a message was deleted. Replies which reference a deleted message typically hide the quoted portion and reflect that the original message was deleted.

If Bob deleted his message instead of modifying it, we would represent it using the Supersedes header with an empty body, as shown below.

```
Content-type: message/cpim

From: <im:bob-jones@example.com>
DateTime: 2022-02-08T22:13:57-00:00
Message-ID: <89d3472622a4@example.com>
Supersedes: <e701beee59f9@example.com>

Content-Length: 0
```

4.7. Expiring

Expiring messages are designed to be deleted automatically by the receiving client at a certain time whether they have been read or not. As with manually deleted messages, there is no guarantee that a uncooperative client or a determined user will not save the content of the message, however most clients respect the convention.

MIXER defines an Expires header which is also used sent simply by including an Expires header in the CPIM message body.

To avoid using two different date header syntaxes, we define an ExpiresDateTime header, which uses the same date/time format as CPIM's DateTime header. The semantics of the header are that the message is automatically deleted by the receiving clients at the indicated time without user interaction or network connectivity necessary.

```
Content-type: message/cpim

From: <im:alice-smith@example.com>
DateTime: 2022-02-08T22:49:03-00:00
Message-ID: <5c95a4dfddab@example.com>
ExpiresDateTime: 2022-02-08T22:59:03-00:00

Content-Type: text/markdown;charset=utf-8

__*VPN GOING DOWN*__
I'm rebooting the VPN in ten minutes unless anyone objects.
```

4.8. Knock

A knock or ping is message sent to get the attention of a user or a group of users. It might be sent when a user has not responded to direct messages or mentions, or in a group when something requires the attention of everyone quickly (ex: a serious unusual situation like a major system outage).

We represent a knock as a text/plain body containing a single CRLF with the alert Content-Disposition token (defined in [RFC3261]).

```
Content-type: message/cpim

From: <im:alice-smith@example.com>
DateTime: 2022-02-08T22:13:45-00:00
Message-ID: <c1a3375bfe3f@example.com>

Content-Type: text/plain
Content-Disposition: alert
```

4.9. Read Receipt

In instant messaging systems, read receipts typically generate a distinct indicator for each message. In some systems, the number of users in a group who have read the message is subtly displayed and the list of users who read the message is available on further inspection.

Of course, Internet mail has support for read receipts as well, but the existing message disposition notification mechanism defined for email in [RFC8098] is unfortunately inappropriate in this context.

- notifications can be sent by intermediaries
- only one notification can be sent about a single message per recipient
- a human-readable version of the notification is expected
- each notification can refer to only one message
- it is extremely verbose

The proposed format below, message/immi-disposition-notification is sent by one member of an MLS group to the entire group and can refer to multiple messages. There is one IMMI-Disposition line per message, with the disposition of the original message in a parameter. As the disposition at the recipient changes, the disposition can be updated in a subsequent notification.

```
Content-type: message/cpim

From: <im:bob-jones@example.com>
DateTime: 2022-02-09T07:57:13-00:00
Message-ID: <7e924c2e6ee5@example.com>

Content-Disposition: notification
Content-type: message/immi-disposition-notification

IMMI-Disposition: <4dcab7711a77@example.com>;dispo=read
IMMI-Disposition: <285f75c46430@example.com>;dispo=read
IMMI-Disposition: <c5e0cd6140e6@example.com>;dispo=read
IMMI-Disposition: <5c95a4dfddab@example.com>;dispo=expired
```

4.10. Attachments

The message/external-body MIME Type is a convenient way to present a URL to download an attachment which should not be rendered inline.

```
Content-Type: message/external-body; access-type="URL";
 URL="https://example.com/storage/bigfile.m4v";
 size=708234961
```

4.11. Conferencing

Joining a conference via URL is also possible. The link could be rendered to the user, requiring a click. Alternatively another Content-Disposition could be specified to more automatic actions. However further calling and conferencing functionality is out-of-scope of this document.

```
Content-Type: message/external-body; access-type="URL";
 URL="https://example.com/join/12345"
```

5. IMMI CPIM profile

We define a profile of CPIM for instant messaging within MLS. The grammar uses Augmented Backus-Naur Form (BNF) [RFC5234].

5.1. CPIM headers

The following CPIM headers are required:

- *From: the identity of message sender. for example im:alice@example.com this identity could be pseudonymous or anonymous if the group policy allows.
- *DateTime: the date and time in a reasonable format, as specified in CPIM.
- *Message-ID: a message ID which is unique across domains.
- *Content-type: As is from CPIM.
- *In-Reply-To: Refers to the previous Message-ID. Same semantics as in [RFC5322].
- *Supersedes: Refers to the previous Messsage-ID. Similar semantics to header of the same name in MIXER. Content-Disposition: The intended handling of the message. The two required dispositions are render and reaction.
- *Content-Length:

For clarity the grammar for the headers not already included in CPIM are formulated below.

```
msg-id-header-line = msg-id-header ":" SP msg-id CRLF
msg-id-header = "Message-ID"   ; case-sensitive

in-reply-to-header-line = in-reply-to-header ":" SP msg-id CRLF
in-reply-to-header = "In-Reply-To"   ; case-sensitive

supersedes-header-line = supersedes-header ":" SP msg-id CRLF
supersedes-header = "Supersedes"   ; case-sensitive


msg-id = "<" id-left "@" id-right ">"

id-left  = dot-atom-text
id-right = dot-atom-text / no-fold-literal

dot-atom-text   =   1*atext *("." 1*atext)

atext = ALPHA / DIGIT / atom-symbol

atom-symbol = "!" / "#" / "$" / "%" / "&" / "'" / "*" / "+" / "-" /
              "/" / "=" / "?" / "^" / "_" / "`" / "{" / "|" / "}" / "~"

no-fold-literal = "[" *dtext "]"

dtext = %d33-90 / %d94-126 ; Printable US-ASCII
                           ; excluding "[", "]", and "\"
```

5.2. Definition of message/immi-disposition-notification

The grammar below defines the syntax.

```
immi-disposition-notification-body = 1*immi-header-line

immi-header-line = immi-header ":" SP msg-id ";" status CRLF

imm-header = "IMMI-Disposition" ; case-sensitive

status = "dispo" "=" status-value

status-value = "read" /
               "error" /
               "delivered" /
               "expired" /
               "deleted" /
               "hidden"
```

5.3. Required and Recommended MIME types

The following MIME types are REQUIRED:

*message/cpim

*multipart/alternative
*multipart/mixed
*multipart/parallel
*text/plain
*text/markdown

The following MIME types are RECOMMENDED:

*text/html
*message/external-body
*message/immi-disposition-notification
*image/jpeg
*image/png

6. IANA Considerations

6.1. MIME subtype registration of message/immi-disposition-notification

This document proposes registration of a MIME subtype with IANA.

TBC

7. Security Considerations

TBC

8. Normative References

[I-D.ietf-mls-protocol] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", Work in Progress, Internet-Draft, draft-ietf-mls-protocol-12, 11 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-protocol-12>.

[I-D.mahy-dispatch-immi-mls-mime] Mahy, R., "Inside MLS Message Interop (IMMI) MIME type extensions", Work in Progress, Internet-Draft, draft-mahy-dispatch-immi-mls-mime-00, 7 March 2022, <https://datatracker.ietf.org/doc/html/draft-mahy-dispatch-immi-mls-mime-00>.

[RFC2156] Kille, S., "MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME", RFC 2156, DOI

10.17487/RFC2156, January 1998, <https://www.rfc-editor.org/info/rfc2156>.

[RFC2219] Hamilton, M. and R. Wright, "Use of DNS Aliases for Network Services", BCP 17, RFC 2219, DOI 10.17487/RFC2219, October 1997, <https://www.rfc-editor.org/info/rfc2219>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/info/rfc3261>.

[RFC3862] Klyne, G. and D. Atkins, "Common Presence and Instant Messaging (CPIM): Message Format", RFC 3862, DOI 10.17487/RFC3862, August 2004, <https://www.rfc-editor.org/info/rfc3862>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC7763] Leonard, S., "The text/markdown Media Type", RFC 7763, DOI 10.17487/RFC7763, March 2016, <https://www.rfc-editor.org/info/rfc7763>.

9. Informative References

[RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, DOI 10.17487/RFC3156, August 2001, <https://www.rfc-editor.org/info/rfc3156>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <https://www.rfc-editor.org/info/rfc6120>.

[RFC8098] Hansen, T., Ed. and A. Melnikov, Ed., "Message Disposition Notification", STD 85, RFC 8098, DOI

10.17487/RFC8098, February 2017, <https://www.rfc-editor.org/info/rfc8098>.

[RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/info/rfc8551>.

[RFC9078] Crocker, D., Signes, R., and N. Freed, "Reaction: Indicating Summary Reaction to a Message", RFC 9078, DOI 10.17487/RFC9078, August 2021, <https://www.rfc-editor.org/info/rfc9078>.

[W3C.CR-html52-20170808] Faulkner, S., Eicholz, A., Leithead, T., Danilo, A., and S. Moon, "HTML 5.2", World Wide Web Consortium CR CR-html52-20170808, 8 August 2017, <https://www.w3.org/TR/2017/CR-html52-20170808>.

Author's Address

Rohan Mahy
Wire

Email: rohan.mahy@wire.com