Workgroup: MIMI BoF
Internet-Draft:
draft-mahy-mimi-problem-outline-02
Published: 13 March 2023
Intended Status: Informational
Expires: 14 September 2023
Authors: R. Mahy
Wire

More Instant Messaging Interoperability (MIMI) problem outline

Abstract

Instant Messaging interoperability requirements have changed dramatically since the last IETF activity in the space. This document presents an outline of problems that need to be addressed to make possible interoperability of modern Instant Messaging systems. The goal of this problem outline is to point at more detailed drafts which spawn discussion and eventually spur the IETF standards process.

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 14 September 2023.

Table of Contents

1. Overview

The IETF has been working on Instant Messaging Interoperability since the late 1990s. At the time, different groups within IETF proposed separate protocol suites (SIMPLE, APEX, and XMPP) because the community could not come to consensus on a single protocol (arguably due to a lack of consensus on the additional requirements which made these proposals unique). In the interests of interoperability, the IMPP Working Group developed a general framework for interoperability [RFC3860], and the Common Presence and Instant Messaging (CPIM) Message Format [RFC3862], an interoperability format that could pass through gateways among these protocols, even when end-to-end encrypted.

The CPIM model assumed standalone encryption of each message using a protocol such as S/MIME [RFC8551] or PGP [RFC3156]. This model was not widely adopted, but many Instant Messaging systems around this time frame began to add optional end-to-end encryption with OTR (Off The Record) [OTR], and eventually incorporated variants of the Double Ratchet protocol [DoubleRatchet], originally popularized by Signal.

Today, group chats are the norm, most modern instant messaging systems are end-to-end encrypted (many by default or always) using a variant of DoubleRatchet, and the typical feature set includes a plethora of features not included in CPIM: plain text and rich text messaging, delivery notifications, read receipts, replies, reactions, editing or deleting previously sent messages, and expiring messages. Almost all systems provide a way to share files/audio/videos, and many support calling and/or conferencing features (often using WebRTC). Some IM vendors are implementing MLS [I-D.ietf-mls-protocol], a group key establishment protocol motivated by the desire for group chat with efficient end-to-end encryption.

Unfortunately, federation of these IM systems is still rare and interoperability of the major IM systems in almost non-existent. It would be incredibly beneficial to provide interoperable best practices and solutions which IM vendors can incorporate into modern IM systems. Indeed, large customers and governments are already putting pressure on these IM vendors. The European Union's Digital Markets Act Article 7 [DMA] is a recent motivator as well.

Instant Messaging interoperability requirements have changed dramatically since the IETF last activity in the space. This document presents an outline of problems that need to be addressed to make possible interoperability of modern Instant Messaging systems. The goal of this problem outline is to point at more detailed drafts which spur discussion and eventually spur the IETF standards process.

The larger goals of MIMI (More Instant Messaging Interoperability) are to start discussion; gather requirements common to many IM systems, focusing on the most immediate needs first; develop requirements and frameworks; and eventually to identify and evaluate existing solutions to these specific problems; and to assemble standards and technology which already largely exist into profiles and best current practices. Where special expertise in another Working Group or standards body is required, that work would be delegated to the specialty group.

2. Interoperability Problem Areas

2.1. Naming schemes

IM systems have a number of identifiers with different characteristics which are relevant for interoperability.

- *Domain identitifer
- *Handle identifier
- *User or Account identifier

*Client or Device identifier
*Group Chat or Channel identifier
*Group, Conversation, or Session identifiers
*Team or Workspace identifier

These identifiers are discussed in detail in [I-D.mahy-mimi-identity] as well as how they can be represented using URIs.

2.2. End-to-end IM Identity

The largest and most widely deployed Instant Messaging (IM) systems support end-to-end message encryption using a variant of the Double Ratchet protocol [DoubleRatchet] popularized by Signal and the companion X3DH [X3DH] key agreement protocol. Many vendors are also keen to support the Message Layer Security (MLS) protocol [I-D.ietf-mls-protocol] and architecture [I-D.ietf-mls-architecture]. These protocols provide confidentiality of sessions (with Double Ratchet) and groups (with MLS) once the participants in a conversation have been identified. However, the current state of most systems require the end user to manually verify key fingerprints or blindly trust their instant messaging service not to add and remove participants from their conversations. This problem is exacerbated when these systems federate or try to interoperate.

This problem space is explored in [I-D.mahy-mimi-identity], and a specific architecture is described in [I-D.barnes-mimi-identity-arch].

2.3. Discovery

2.3.1. Domain-level service discovery

The discovery of IM services using DNS SRV records is described in [RFC3861].

2.3.2. User discovery and discovery of device keying material

TBC.

One vendor mentioned a strawperson outline for user discovery:

*well-known URL with query format on each domain

-search string

ocould be handle, internal user ID, internal device ID; search by anonymous credential?

owhat type of key are you searching for?

okeypackages
ouser keys
odomain keys
-searcher identity and proof of identity (optional)
-rate limiting

The privacy implications of user discovery are of the utmost importance, and may differ widely depending on the specific messaging application.

2.4. Profiles of security protocols to facilitate interoperable end-to-end encryption

Enabling strong user privacy has been a core concern of the IETF for decades, and was the main motivation for the CPIM message format. S/MIME and PGP where proposed for use with instant messaging systems, but never widely adopted. The first broad adoption of end-to-end encryption in messaging was with Off The Record (OTR) [OTR] introduced in 2004, which also included perfect forward secrecy (which protects past communications from future compromises). As OTR was available in XMPP clients, it was possible to use across domains.

2.4.1. Protocols based on Double Ratchet

Signal introduced what is now know as the Double Ratchet protocol in 2013. Today there are over a dozen implementations of variations of Double Ratchet. While the differences among these variations tend to be small, there is little emphasis on interoperability.

Tens of instant messaging applications implement some form of end-to-end encryption using a protocol based on the Double Ratchet protocol. Double Ratchet was originally referred to as Axolotl Ratchet when it was introduced in 2013 and popularized in the Signal application. Most applications using Double Ratchet also use [X3DH] for initial key agreement. However the initial setup of encryption sessions among these applications are often incompatible.

Most implementations of Double Ratchet use a fixed ciphersuite and have no content negotiation or advertisement mechanism.

2.4.2. Instant Messaging using Messaging Layer Security

Messaging Layer Security (MLS) [I-D.ietf-mls-protocol] is a group key agreement protocol with application message encryption and authentication. As described in the MLS architecture [I-D.ietf-mls-architecture], the protocol does not define the

specific behavior of the Distribution Service (DS) or the Authentication Service (AS).

Some specific issues involving the use of MLS is a multi-domain Instant Messaging context are discussed in the MLS federation draft [I-D.ietf-mls-federation].

More documentation on the use of MLS in the Instant Messaging Context: (ex: long-lived persistent groups) would be invaluable.

2.5. Content negotiation

Protocol independent content negotiation is discussed in [RFC2703]. In this framework, content negotiation covers these elements:

- *describing the data resource to be transmitted
- *expressing sender capabilities
- *expressing receiver capabilities
- *a protocol to exchange capabilities

In end-to-end encrypted group messaging, the problem is slightly different; an intermediary should not be able to read the sender's content, let alone change the format of the message for different recipients. Furthermore, in MLS a message in a group is encrypted once for all the recipients in the group, some of whom may be offline and receive the message later. The sender has one opportunity to craft an encrypted message which can be processed by all the members of an MLS group. Rather than have a protocol to exchange capabilities, MLS content advertising insures that each member knows any media types required in the group, knows the content capabilities of every group member at all times, and knows the media type of each received message. Note that the message could be be a container type such as a multipart [RFC2046] expressing different alternative expressions of the same content in a single message.

The requirements for content negotiation are discussed in the MLS architecture document [I-D.ietf-mls-architecture] and a specific content advertisement mechanism for MLS is described in [I-D.ietf-mls-extensions].

2.6. Content format interoperability

The expectation of basic or common features in IM systems has grown. Below is a list of some features commonly found in most IM group chat systems:

- *plain text and rich text messaging
- *mentions
- *delivery notifications

*read receipts
*replies
*reactions
*edit or delete previously sent messages
*expiring messages
*shared files/audio/videos
*calling / conferencing
*message threading

Once messages are encrypted end-to-end there is no further opportunity for content negotiation. Exploring requirements, semantics, and an example common format for messages, which would allow proprietary messages or extensions to be delivered in parallel to the same users is described in [I-D.mahy-mimi-content]. It discusses all of the features above.

2.7. Transport protocol

The protocol used between two different providers needs to be specified. A few different proposals include creating a REST-based protocol [I-D.rosenberg-mimi-protocol], using XMPP [RFC6120], and using a variation of the Matrix protocol.

2.8. Calling and Conferencing

Many IM systems offer 1:1 calling and/or conferencing of real-time audio and video. The majority of these systems use a exchange a session description offer and answer to setup sessions of media transmitted using DTLS-SRTP [RFC5764], including the fingerprint of the DTLS-SRTP self-signed certificate. These messages are typically end-to-end encrypted. During 1:1 calls, the session descriptions (an offer and an answer) are shared for one or more DTLS-SRTP flows which carry the actual media.

For conferences, a client typically contacts a conferencing system which sets up a session between the client and the media forwarder. The client needs to have the URI of the specific conference and support the protocol used to access it, such as WebRTC [RFC8825] or SIP [RFC3261]. To maintain the privacy of the media with respect to the media forwarder, the clients could further encrypt the media using keying material only to clients, for example using WebRTC Insertable Streams.

2.9. Administrative setup of federation

(ex: agreement on certificates, contact information, abuse policies). TBC.

2.10. Authorization features

Is it necessary to standardize IM application authorization features such as moderation roles?

3. IANA Considerations

This document requires no action of IANA.

4. Security Consideration

TBC.

5. Normative References

[I-D.barnes-mimi-identity-arch] Barnes, R. and R. Mahy, "Identity for E2E-Secure Communications", Work in Progress, Internet-Draft, draft-barnes-mimi-identity-arch-00, 24 October 2022, <https://datatracker.ietf.org/doc/html/draft-barnes-mimi-identity-arch-00>.

[I-D.mahy-mimi-content] Mahy, R., "More Instant Messaging Interoperability (MIMI) message content", Work in Progress, Internet-Draft, draft-mahy-mimi-content-02, 13 March 2023, <https://datatracker.ietf.org/api/v1/doc/document/draft-mahy-mimi-content/>.

[I-D.mahy-mimi-identity] Mahy, R., "More Instant Messaging Interoperability (MIMI) Identity Concepts", Work in Progress, Internet-Draft, draft-mahy-mimi-identity-01, 24 October 2022, <https://datatracker.ietf.org/doc/html/draft-mahy-mimi-identity-01>.

[RFC3861] Peterson, J., "Address Resolution for Instant Messaging and Presence", RFC 3861, DOI 10.17487/RFC3861, August 2004, <https://www.rfc-editor.org/info/rfc3861>.

6. Informative References

[DMA] The European Parliament, "REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL", 14 September 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925&qid=1678665640191&from=en>.

[DoubleRatchet] Perrin, T. and M. Marlinspike, "The Double Ratchet Algorithm", 20 November 2016, <https://signal.org/docs/specifications/doubleratchet/>.

[I-D.ietf-mls-architecture] Beurdouche, B., Rescorla, E., Omara, E., Inguva, S., and A. Duric, "The Messaging Layer Security

(MLS) Architecture", Work in Progress, Internet-Draft, draft-ietf-mls-architecture-10, 16 December 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-architecture-10>.

[I-D.ietf-mls-extensions] Robert, R., "The Messaging Layer Security (MLS) Extensions", Work in Progress, Internet-Draft, draft-ietf-mls-extensions-01, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-extensions-01>.

[I-D.ietf-mls-federation] Omara, E. and R. Robert, "The Messaging Layer Security (MLS) Federation", Work in Progress, Internet-Draft, draft-ietf-mls-federation-02, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-federation-02>.

[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-18, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-protocol-18>.

[I-D.rosenberg-mimi-protocol] Rosenberg, J., Jennings, C. F., and S. Nandakumar, "More Instant Messaging Interop (MIMI) Transport Protocol", Work in Progress, Internet-Draft, draft-rosenberg-mimi-protocol-00, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-rosenberg-mimi-protocol-00>.

[OTR] Borisov, N., Goldberg, I., and E. Brewer, "Off-the-Record Communication, or, Why Not To Use PGP", 28 October 2004, <https://otr.cypherpunks.ca/otr-wpes.pdf>.

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

[RFC2703] Klyne, G., "Protocol-independent Content Negotiation Framework", RFC 2703, DOI 10.17487/RFC2703, September 1999, <https://www.rfc-editor.org/info/rfc2703>.

[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>.

[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>.

[RFC3860] Peterson, J., "Common Profile for Instant Messaging (CPIM)", RFC 3860, DOI 10.17487/RFC3860, August 2004, <https://www.rfc-editor.org/info/rfc3860>.

[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>.

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, DOI 10.17487/RFC5764, May 2010, <https://www.rfc-editor.org/info/rfc5764>.

[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>.

[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>.

[RFC8825] Alvestrand, H., "Overview: Real-Time Protocols for Browser-Based Applications", RFC 8825, DOI 10.17487/RFC8825, January 2021, <https://www.rfc-editor.org/info/rfc8825>.

[X3DH] Marlinspike, M. and T. Perrin, "The X3DH Key Agreement Protocol", 4 November 2016, <https://signal.org/docs/specifications/x3dh/>.

Author's Address

Rohan Mahy
Wire

Email: rohan.mahy@wire.com