More Instant Messaging Interoperability
Internet-Draft
Intended status: Informational
Expires: 21 October 2026

R. Mahy

19 April 2026

Conveying the More Instant Messaging Interoperability Message ID in Messaging Layer Security Additional Authenticated Data
draft-mahy-mimi-msgid-aad-02

Abstract

The More Instant Messaging Interoperability (MIMI) content format defines a MIMI Message ID, communicated only to members of the Messaging Layer Security (MLS) group in which the message was sent. This document defines a way to share a Message ID in the MLS Additional Authenticated Data (AAD) so it is visible to MIMI providers.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://rohanmahy.github.io/mimi-msgid-aad/draft-mahy-mimi-msgid-aad.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-mahy-mimi-msgid-aad/.

Discussion of this document takes place on the More Instant Messaging Interoperability mailing list (mailto:mimi@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/mimi/. Subscribe at https://www.ietf.org/mailman/listinfo/mimi/.

Source for this draft and an issue tracker can be found at https://github.com/rohanmahy/mimi-msgid-aad.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Many messaging protocols and formats have a Message ID. The MIMI content format defines how to calculate a MIMI Message ID (See Section 3.3 of [I-D.ietf-mimi-content]) for an application/mimi-content application message. A MIMI Message ID is currently only shared end-to-end encrypted with members of the MLS [RFC9420] group in which the message was sent. This document defines an optional mechanism to share a Message ID in the MLS AAD, so it is visible to intermediary providers. This greatly facilitates debugging and troubleshooting, but causes a modest reduction in privacy.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Mechanism

This document defines a new Safe AAD message_id component as described in Section 4.9 of [I-D.ietf-mls-extensions].

When the content of an MLS application message is a MIMI content message (media type application/mimi-content), if the message_id component is present inside SafeAAD.aad_items, it MUST contain the MIMI content Message ID calculated as described in Section 3.3 of [I-D.ietf-mimi-content].

> To the extent that other application formats or media types have a Message ID, the Message ID for an application message of that type or format MAY be conveyed in this extension, using a message ID appropriate to the media type of the content.

4. Security Considerations

An attacker or provider with access to a fragment of message history, and the message logs of a MIMI provider in the path of a message could potentially learn more about the participants of a particular MIMI room or the room’s corresponding MLS group if it can see message IDs.

5. IANA Considerations

5.1. message_id MLS Component Type

This document registers a new MLS Component Type in the Specification Required range with the following template:

* Value: TBD (suggested value 0x0040)
* Name: message_id
* Where: AD
* Recommended: Y
* Reference: RFC XXXX

6. Normative References

[I-D.ietf-mimi-content]
Mahy, R., "More Instant Messaging Interoperability (MIMI) message content", Work in Progress, Internet-Draft, draft-ietf-mimi-content-08, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-mimi-content-08>.

[I-D.ietf-mls-extensions]
Robert, R., "The Messaging Layer Security (MLS) Extensions", Work in Progress, Internet-Draft, draft-ietf-mls-extensions-09, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-extensions-09>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/rfc/rfc9420>.

Acknowledgments

TODO acknowledge.

Author’s Address

Rohan Mahy
Email: rohan.mahy@gmail.com