Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 March 2026

S. Dutta
Independent

16 September 2025

SIME: Srijal's Integrated Mail Extensions
draft-srijal-sime-protocol-00

Abstract

This document specifies the SIME protocol, a decentralized, atomic protocol for inter-domain mail transmission and entity-to-entity communication. It defines packet types, headers, MX/SRV-based trust verification, TCP-based delivery, and SIME Extensions for attachments. All servers act as Domain Authorities (DA), and inter-domain transactions are governed by atomic protocol rules.

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 20 March 2026.

Table of Contents

1. Introduction 2
2. Terminology 2
3. Overview of SIME Protocol 3
4. Packet Types 3
5. Headers 3
6. Authentication and Login 4
7. Message Flow 4
8. Atomic Protocol Rules 4
9. Inter-Domain Transactions 5
10. Error Codes 5
11. Security Considerations 5
12. MX/SRV Verification 5
13. SIME Extensions for Attachments 6
14. Packet Syntax 6
15. Example Message Flow 6
16. Normative References 6
Appendix A. Authors' Addresses 7
Author's Address 7

1. Introduction

SIME (Srijal's Integrated Mail Extensions) is a decentralized protocol designed to provide reliable messaging between users in different Domain Authorities (DA). Each DA manages its own user authentication and registration rules. Atomic protocol enforcement ensures inter-domain transactions follow strict compatibility, reliability, and security rules.

All SIME traffic is conducted over TCP to ensure reliable delivery.

2. Terminology

DA (Domain Authority) - Server managing a domain and its users

ID - Disposable session identifier (e.g., JWT)

Transaction ID - Identifier assigned per transaction session

TCP - Transmission Control Protocol (mandatory transport)

MAIL Packet - Packet containing mail messages

CONV Packet - Packet for general communication

MX/SRV Record - DNS record or SRV record pointing to server endpoint for inter-domain verification

3. Overview of SIME Protocol

- Users authenticate with their DA and receive disposable IDs.

- Communication is TCP-only to prevent packet loss.

- Two primary packet types: CONV and MAIL.

- Inter-domain transactions require MX/SRV verification to ensure messages reach the correct DA server.

- Atomic rules enforce uniformity; non-compliant servers are rejected.

4. Packet Types

CONV Packets:

Used for login and general communications:

```
LOGIN <username> <password>
START TRANSACTION <ID>
CONV <payload>
```

Figure 1

MAIL Packets:

Used for sending messages:

```
PREPARE HEADERS <transact_id> X-Mailed-Type-Render: <TXT|MD|HTML>; RECIPIENT: user@domain
PREPARE MESSAGE <transact_id> <content>
END TRANSACTION <transact_id>
```

Figure 2

5. Headers

- SENDER: Originating user (user@domain)

- RECIPIENT: Destination user (user@domain)

- X-Mailed-Type-Render: TXT | MD | HTML

- Optional headers may be added via SIME Extensions

6. Authentication and Login

Users initiate login via CONV packet:

LOGIN <username> <password>

Figure 3

Server responses:

SUCCESS LOGIN : <ID>
ERROR AUTH

Figure 4

Disposable IDs are required for subsequent packets.

7. Message Flow

1. User logs in: CONV Packet → LOGIN → SUCCESS LOGIN : <ID>

2. User initiates transaction: CONV Packet → START TRANSACTION <ID>

3. Server validates ID:

- Success → returns transaction acknowledgment

- Failure → returns ERROR AUTH

4. User sends MAIL packet:

- PREPARE HEADERS <transact_id> ...

- PREPARE MESSAGE <transact_id> <content>

5. User ends transaction: END TRANSACTION <transact_id>

6. Server responds with SENT or appropriate error.

8. Atomic Protocol Rules

- No version negotiation; all inter-domain servers must implement the exact protocol.

- Non-compliant servers are rejected.

- Transactions must be atomic: either all steps succeed or fail.

9. Inter-Domain Transactions

- DA MX/SRV record must point to verified server endpoint.
- Messages are sent only to verified MX/SRV endpoints.
- Servers not listed or failing verification are rejected.

10. Error Codes

- ERROR AUTH : Invalid login/session
- ERROR TRANS : Transaction initiation failure
- ERROR HEADER : Invalid or missing headers
- ERROR MXVER : Inter-domain MX/SRV verification failure
- ERROR PACKET : Malformed packet
- ERROR SEND : Message could not be delivered

11. Security Considerations

- All packets use TCP for reliable delivery.
- Authentication handled per DA; disposable IDs required.
- TLS is recommended for inter-domain traffic.
- Disposable IDs and transaction IDs mitigate replay attacks.
- Inter-domain trust relies on MX/SRV verification; unverified endpoints are rejected.
- Confidentiality and integrity of message content require TLS or optional message signing.
- Reviewers should note that deployment must account for standard-compliant DNS/SRV usage instead of arbitrary IP:PORT MX records.

12. MX/SRV Verification

- Each DA must publish a SIME MX or SRV record specifying its server endpoint.
- Inter-domain messages are routed only to verified endpoints.

- Unverified endpoints are rejected.

13. SIME Extensions for Attachments

- ATTACHMENT: <filename>

- ENCODING: base64 | hex

- Optional metadata headers supported

- Attached in content as: <UNICODE UTF-8: 0xEF 0xBF 0xBF><hex|base64> <encoded attachment><UNICODE UTF-8: 0xEF 0xBF 0xBF>

14. Packet Syntax

```
CONV-PACKET   = LOGIN-PACKET / TRANSACTION-PACKET / GENERAL-CONV
LOGIN-PACKET  = "LOGIN" SP USERNAME SP PASSWORD CRLF
TRANSACTION-PACKET = "START TRANSACTION" SP ID CRLF / CONV SP PAYLOAD CRLF
MAIL-PACKET  = "PREPARE HEADERS" SP TRANSACTION-ID SP HEADER-FIELDS CRLF
               "PREPARE MESSAGE" SP TRANSACTION-ID SP CONTENT CRLF
               "END TRANSACTION" SP TRANSACTION-ID CRLF

USERNAME     = 1*(ALPHA / DIGIT / "-" / "_")
PASSWORD     = 1*(ALPHA / DIGIT / SYMBOL)
TRANSACTION-ID = 1*DIGIT
HEADER-FIELDS = *(HEADER-NAME ":" SP HEADER-VALUE CRLF)
CONTENT      = *(OCTET)
```

Figure 5

15. Example Message Flow

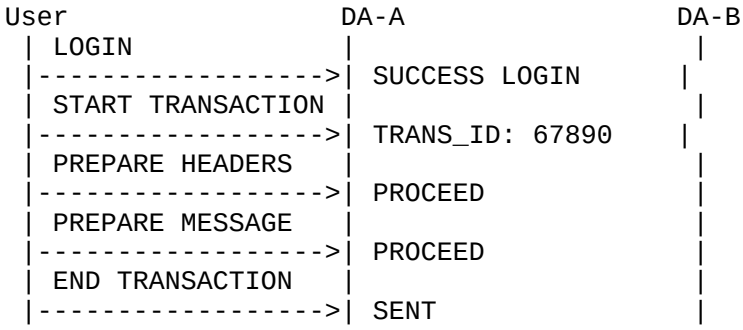

Figure 6

16. Normative References

[RFC793] Postel, J., "Transmission Control Protocol", RFC 793, 1981, <https://www.rfc-editor.org/rfc/rfc793>.

[RFC7519] Jones, M., "JSON Web Token (JWT)", RFC 7519, 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, 2008, <https://www.rfc-editor.org/rfc/rfc5321>.

Appendix A. Authors' Addresses

Srijal Dutta

Email: srijaldutta.official+sime@gmail.com

Author's Address

Srijal Dutta
Independent
Email: srijaldutta.official+sime@gmail.com