More MIMI Requirements from
draft-mahy-mimi-transport-design-reqs and
(a bit of) draft-mahy-mimi-group-chat

Rohan Mahy
rohan@wire.com
Requirements on what?

- The whole MIMI “system”
- MIMI provider’s “servers”
- MLS message Delivery Service (“DS”) abstract service
- MIMI message “transport protocol”
- MIMI client messaging applications (“clients”)

- draft-mahy-mimi-transport-design-reqs is about implications on the transport protocol and design of the DS

- draft-mahy-mimi-group-chat is about the overall group chat functionality. requirements on the whole system, but a focus on client authorization
mimi-transport-design-reqs
Types of Primitives

• “Locking” style requests
  • submit an MLS Commit “bundle”
  • claim a KeyPackage
  • fetch GroupInfo
• Direct async messages
  • request/grant/revoke consent
  • knock (request an invite)
  • report spam/abuse
  • permission to send messages (request/grant/revoke “voice”)

• “Provisional” messages (ex: application messages, and MLS proposals)
• “Fanout” messages

• Search and Discovery
• Attachments
• Invite links
• Status - only care about the current state
  • is typing
  • presence
mimi-transport-design-reqs

Implications

- Provisional and Fanout messages should be **sent in bulk**. A pair of gatekeepers might send a million messages per minute. Don’t wait for individual responses/acknowledgements.

- There are some modest **ordering requirements** for fanout messages (see next slide)

- **Commits** should be **bundled**/stapled together with GroupInfo and Welcome

- Client should be able to fetch **KeyPackages for several users’s clients** on the same provider

- Explicit **consent** requests/grants/rejections and spam reporting should be **asynchronous**

- **Joining via a link** is so common, we need joining by link to be supported / **interoperable**

- Discovery should be able to indicate it is **searching on a specific field** (i.e. phone number)
Fanout Ordering requirements

- Every message/event needs to be delivered.
- It is desirable that events/messages within a single group are no more than a few hundred messages out-of-order, so the client does not advance its decryption generation counter too far.
- Application messages do not need to be delivered strictly in order.
- Commits within the same group must be in-order relative to each other.
- Proposal referenced in a Commit must be delivered before or with the Commit.
Preview of mimi-group-chat requirements (1/2)

Requirements questions

• What kinds of room policies do we want/need to support in MIMI?
  • types of rooms
  • multi-device support vs. single-device support
  • valid ways to join and leave
  • moderation capabilities
  • logging and history policy
  • anonymity and pseudonymity
  • and more (ex: read receipts, delivery notification)

• What level of support?
  • actively initiate; or
  • another client on another provider can passively participate without breaking the experience.
Preview of mimi-group-chat requirements (2/2)

Types of Rooms

- Member-only/administered rooms — non-controversial
- Fixed membership groups
  - 1:1 DM — non-controversial
  - Group DM — assuming we need to do this
- Open groups — probably?
- Parent-dependent (useful for breakout rooms, for ex)— optional initiation?