MIMI Architecture

Richard Barnes
IETF 118, November 2023
● Each room is hosted at a hub server
● All communications go via the hub
  ○ Messages
  ○ State changes
  ○ Ancillary things like KeyPackage fetches
● Anticipate that not every server will be willing to talk to every other server
  ○ A and B might not be willing to talk directly
  ○ But if users from A and B are in a room hosted at C...
  ○ A needs to be able to talk to B via C
Terminology

The unit of MIMI functionality is a room

A room has a state, which has a few components:

- An authorization policy
- A list of users who are participants in the room
- An MLS group, including a list of clients who are members of the group

Participants can either be active or inactive. Active participants have at least one client that is a member of the MLS group.

⚠ Earlier discussions covered a “policy envelope”. Needs more refinement.
Terminology Illustrated

Authz Policy
- User 1 Capas
- User 2 Capas
- User 3 Capas
- Admission Policy
- etc.

Participant List
- User 1 (active)
- User 2 (active)
- User 3 (inactive)

MLS Group
- Client 1a
- Client 2a
- Client 2b
A user may be a participant only if allowed by the authorization policy.

A client may be a member of the MLS group only if its user is a participant in the room.
Different aspects of the state are managed via separate “control” sub-protocols.

To ensure everyone agrees on state, it is included in the MLS key schedule:
- E.g., as a GroupContext extension
- If clients don’t agree, they can’t communicate

Each Commit must reflect the current room state.
Order of Operations

Preemption + Confirmation require some coupling between control protocols

- User must be on PList before clients added to MLS
- Clients must be removed from MLS before user leaves PList

Sending control messages together will help keep things organized.
**Lego* Bricks**

* from Danish *leg godt* = “play well” [Wikipedia]

<table>
<thead>
<tr>
<th>Message Format</th>
<th>(Application Logic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Protection</td>
<td>E2EE (MLS Group)</td>
</tr>
</tbody>
</table>

Transport (Events)
Lego* Bricks

* from Danish *leg godt* = “play well” [Wikipedia]