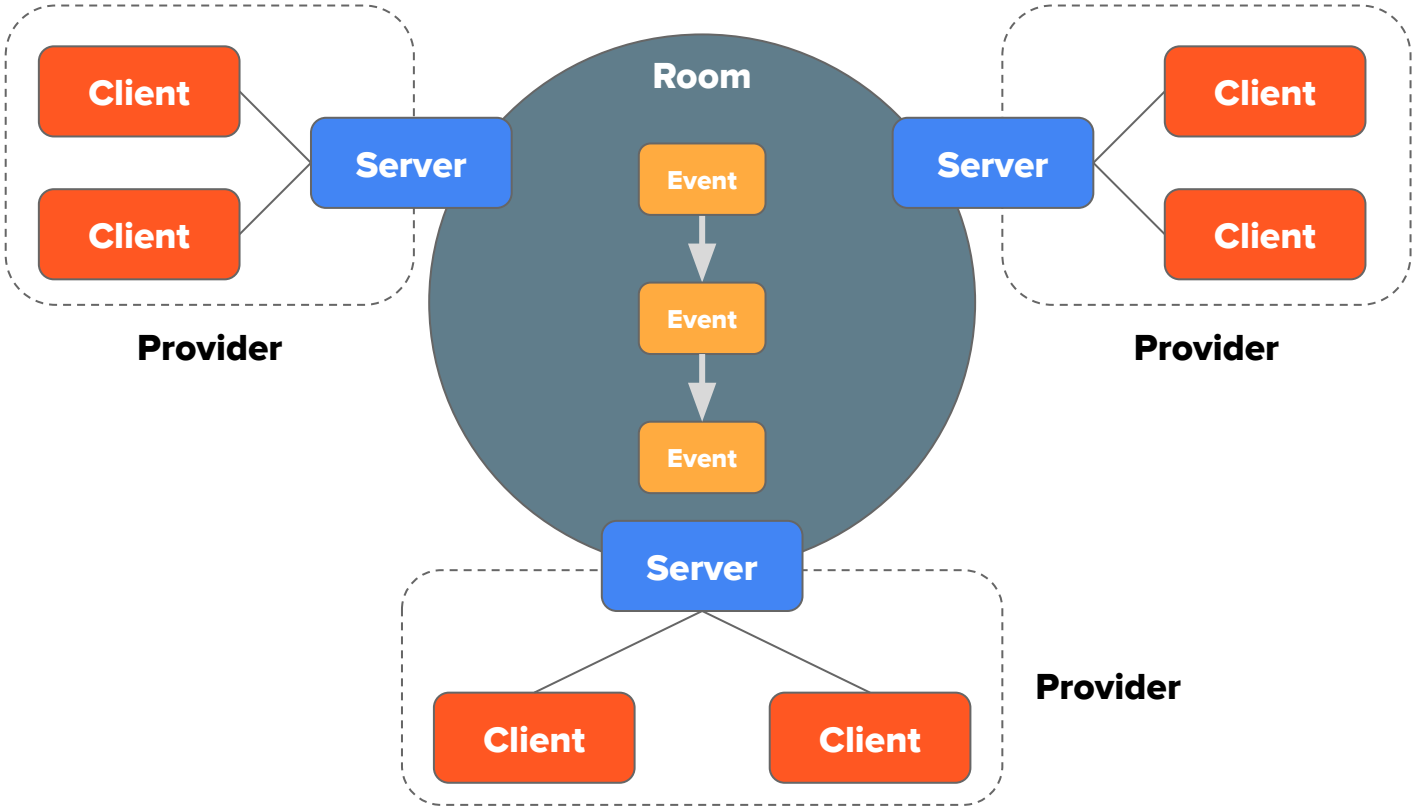
MIMI Architecture

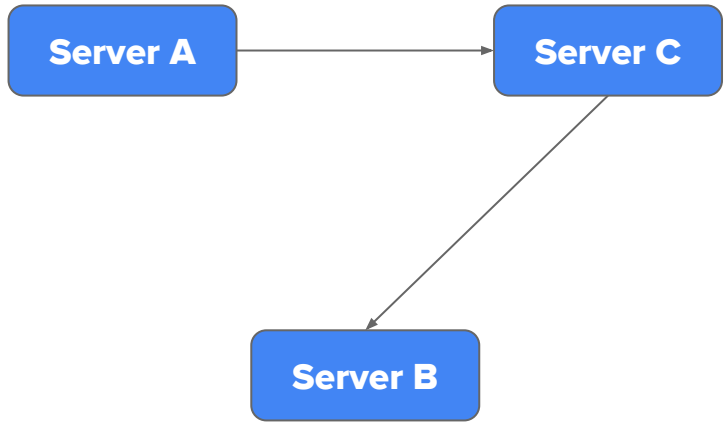
Richard Barnes
IETF 118, November 2023

CSSSC


Client
Client
Server
Provider
Room
Event
Event
Event
Server
Client
Client
Provider
Server
Client
Client
Provider

CSSSC

- 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**

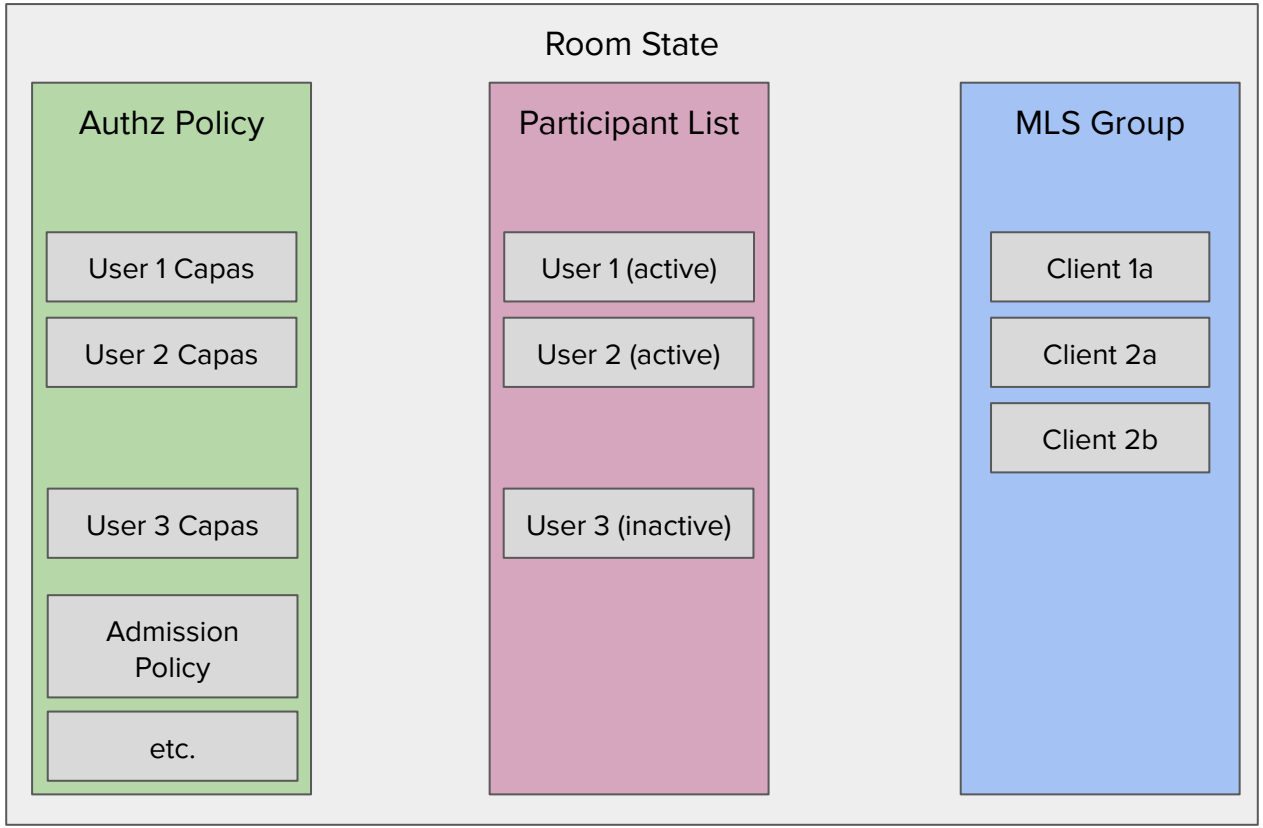
A room has a **state**, which has a few components:

- 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

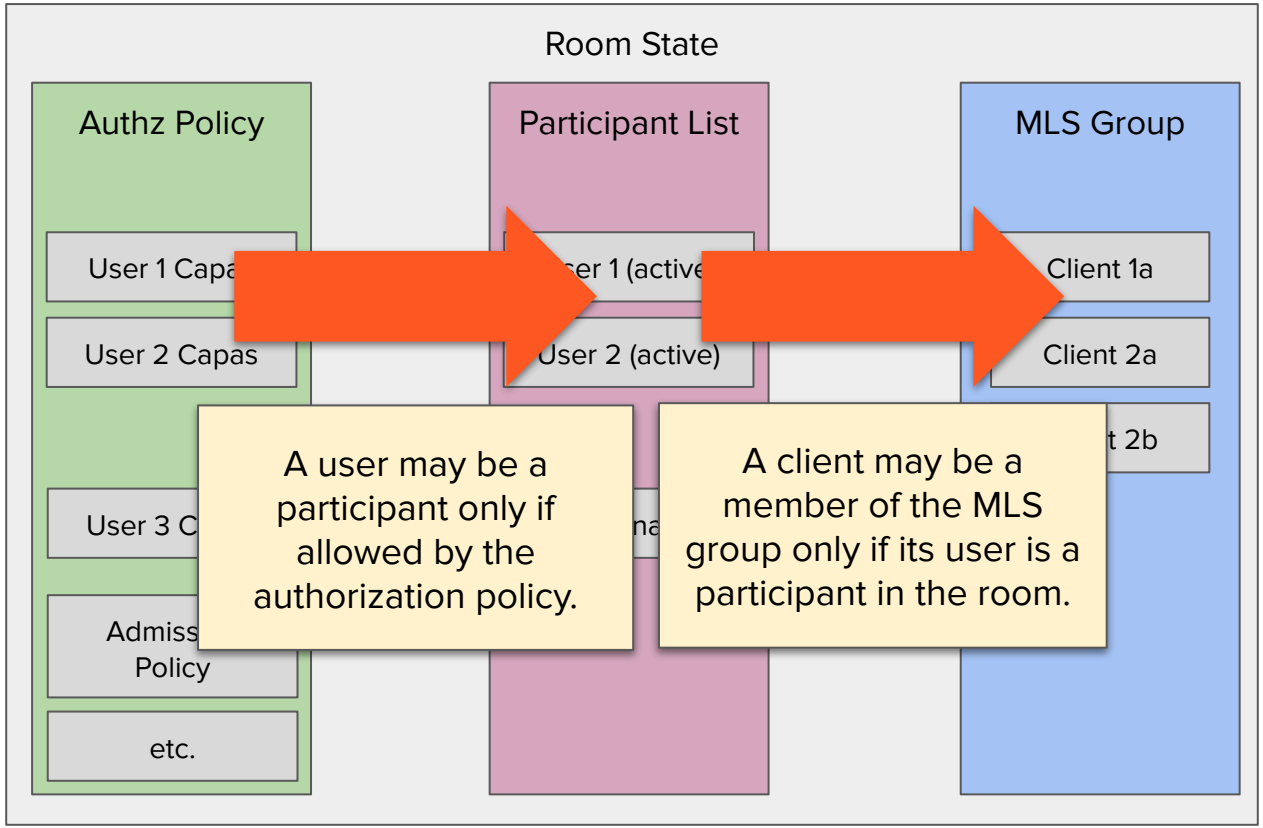
Participants can either be **active** or **inactive**. Active participants have at least one client that is a member of the MLS group.

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

Terminology Illustrated



Preemption


Room State
Authz Policy
Participant List
MLS Group
User 1 Capa
User 2 Capas
User 3 C
Admiss
Policy
etc.
er 1 (active
User 2 (active)
Client 1a
Client 2a
t 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.

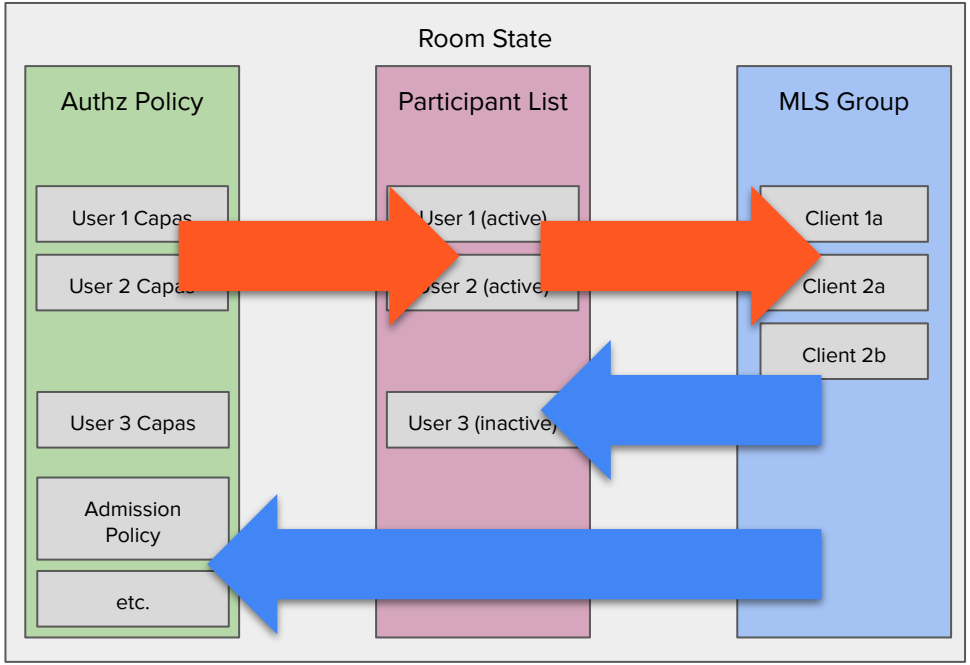
Confirmation

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.

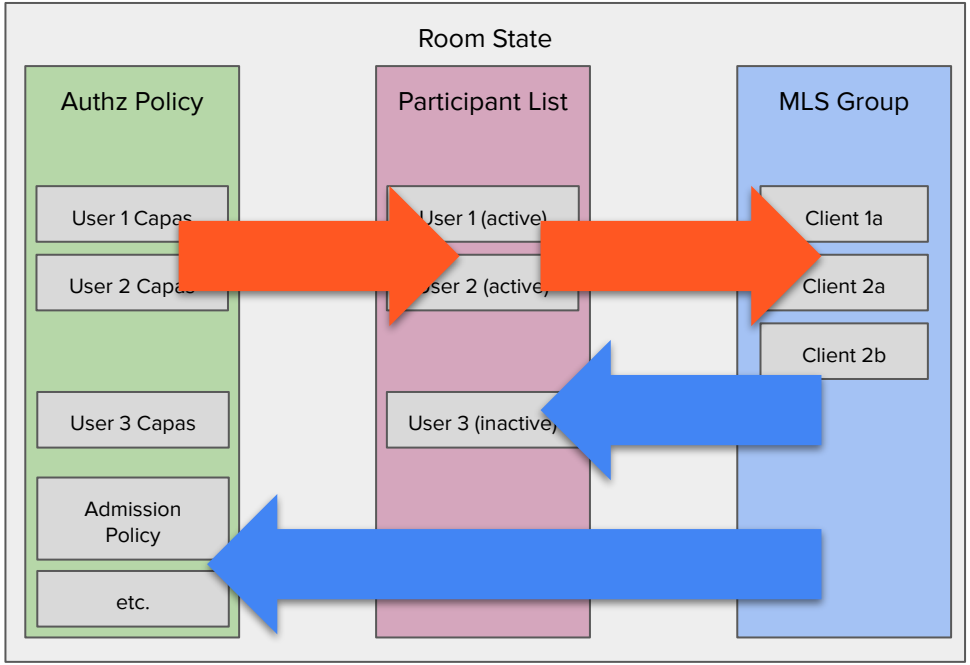


Order of Operations

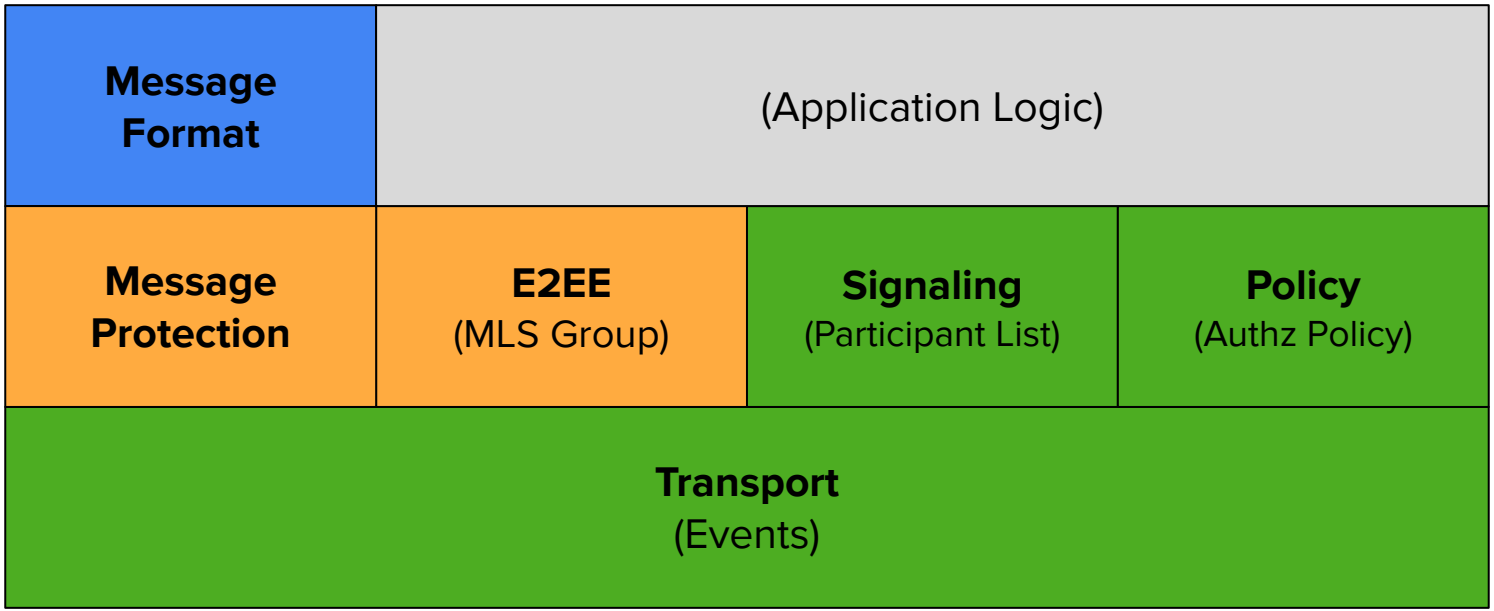
Preemption + Confirmation require some coupling between control protocols

- 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.

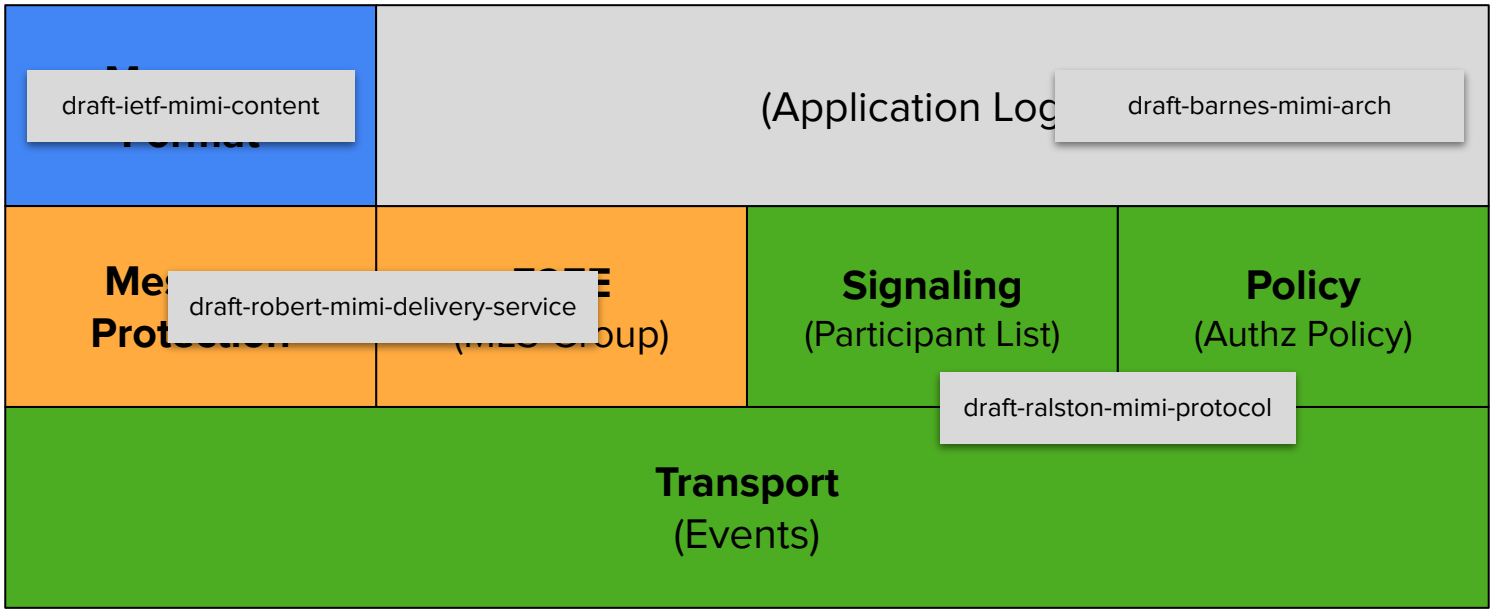


Lego* Bricks



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

Lego* Bricks



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