MIMIMI: MIMI Metadata Minimization

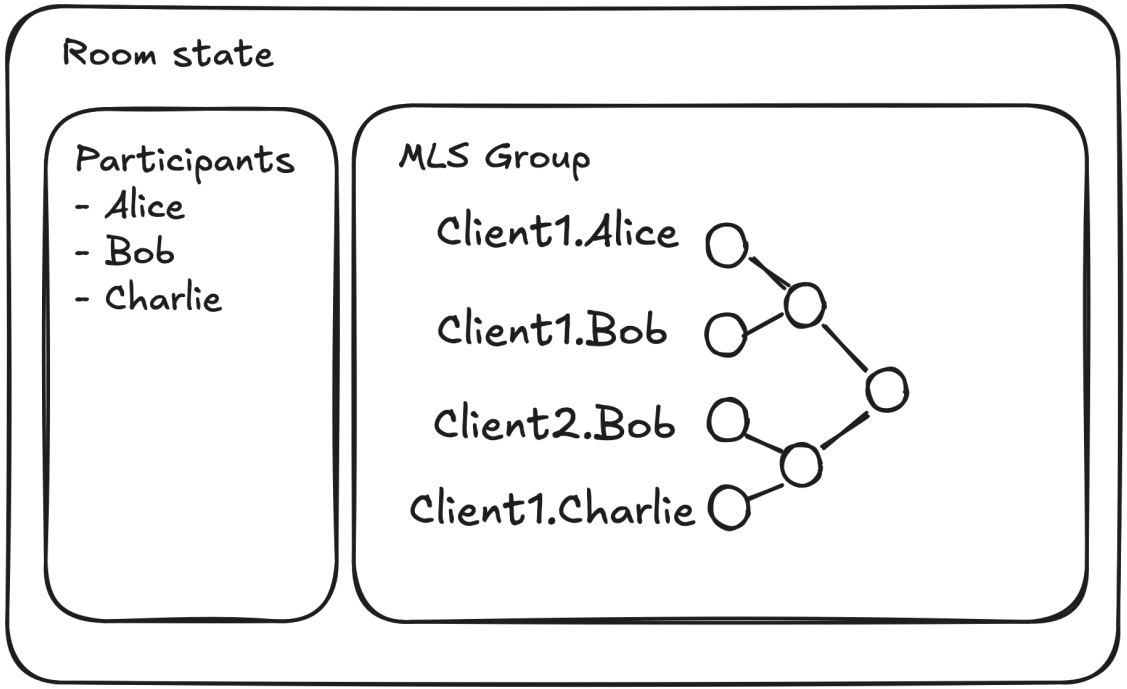
Konrad Kohbrok, Raphael Robert

2024-11-07 - IETF 121 Dublin

Metadata visible to MIMI Hubs

- List of room participants
- Room's MLS group contains a list of clients
- Hub can associate operations with individual users and clients
- Can we hide some of this metadata?

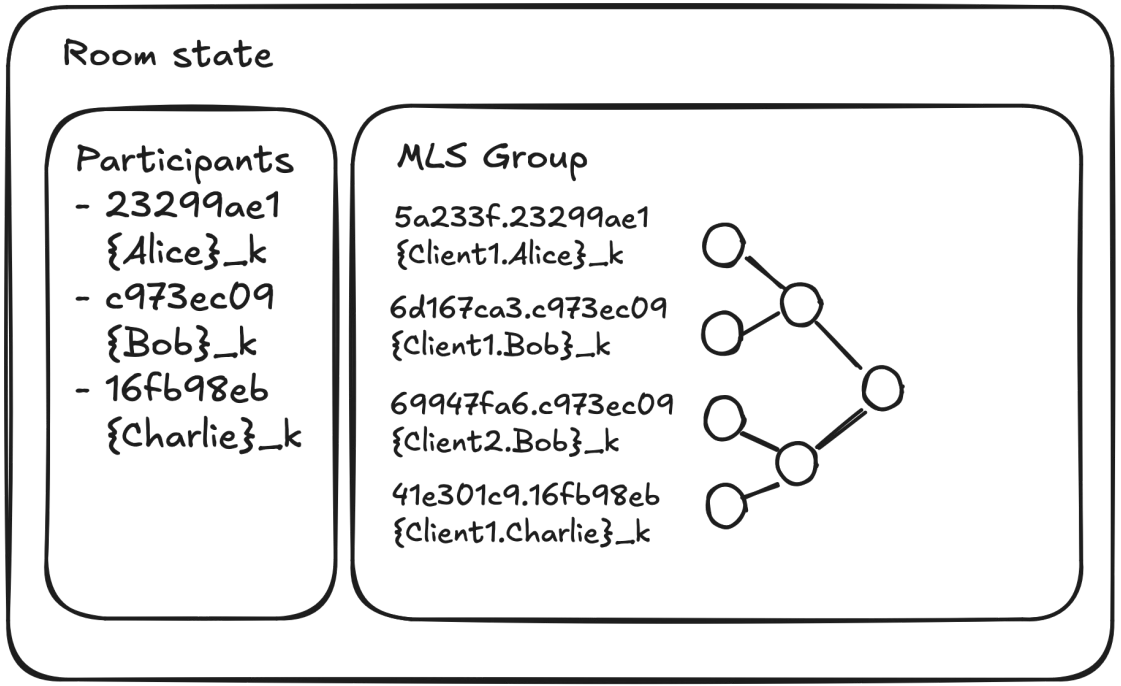
Metadata visible to MIMI Hubs



Optional minimal metadata mode

- Replace user and client identifiers on the Hub with per-room pseudonyms
- Credentials hold encrypted user and client identifiers
- Room participants need key material to learn identifiers of other users and clients

Minimal metadata mode



Less metadata, more key management

- Users need to share key material to add one-another to groups (“connections”)
- Adders need to provide keys to allow new participants to learn identities
- New members joining via “join flow” need to learn key, e.g., from a join link
- Negligible impact on performance

WIP

- Original MIMIMI protocol design has just gone through an audit
- Pseudonymization of the participant list depends on what MIMI credentials look like
- Currently working on PR against main MIMI protocol doc