DMA, MIMI, (D)MLS, Linearized Matrix and more…

Matrix Conference - September 20, 2024

Travis Ralston
Director of Standards Development - matrix.org
@travis:t2l.io | travisr@matrix.org

Digital Markets Act

matrix

- DMA requires “gatekeepers” to open their platforms up for interoperability with other similar providers.
- For messaging, only WhatsApp and Facebook Messenger are gatekeepers so far.
- The same encryption, if any, needs to be maintained between providers.
- Gatekeepers are starting to publish their Reference Offers (terms of interop), and they so far look like opening up existing APIs.
- APIs can always change though. A common (open) standard can help.
- Matrix is an existing open standard, but is quite large for the scope of interop. Linearized Matrix is smaller, and similar to MIMI in model.

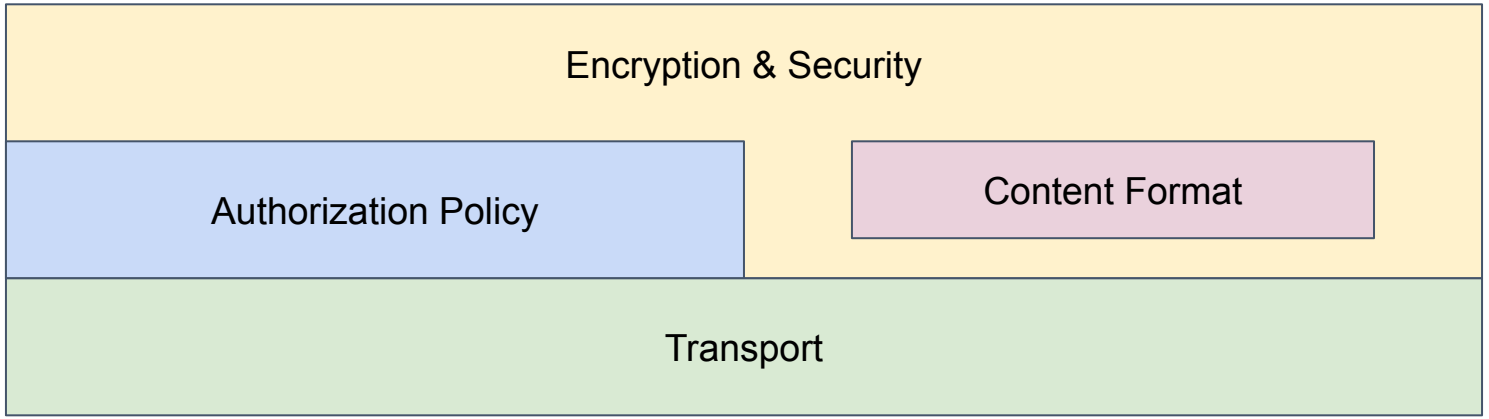
Projects

- “More Instant Messaging Interoperability” (MIMI) working group at the IETF is aiming to specify a standard for modern interoperable communication.
- Linearized Matrix created as a simplified version of Matrix for use in interoperability/MLS settings.
- Matrix itself, as a fully-featured and existing open standard for interoperable communications, including messaging.
- “Messaging Layer Security” (MLS) provides security and group membership guarantees. Now RFC 9420.
- “Decentralized MLS” (DMLS) aims to make something like MLS work in environments like Matrix.

Problem domains

DMA-style protocol interoperability requires 4 major pieces:

1. **Encryption** - how are we securing messages?
2. **Content format** - What does a message *actually* look like?
3. **Authorization policy** - who is allowed to do things?
4. **Transport** - surely we need to ship the messages somewhere.



More Instant Messaging Interoperability (MIMI)

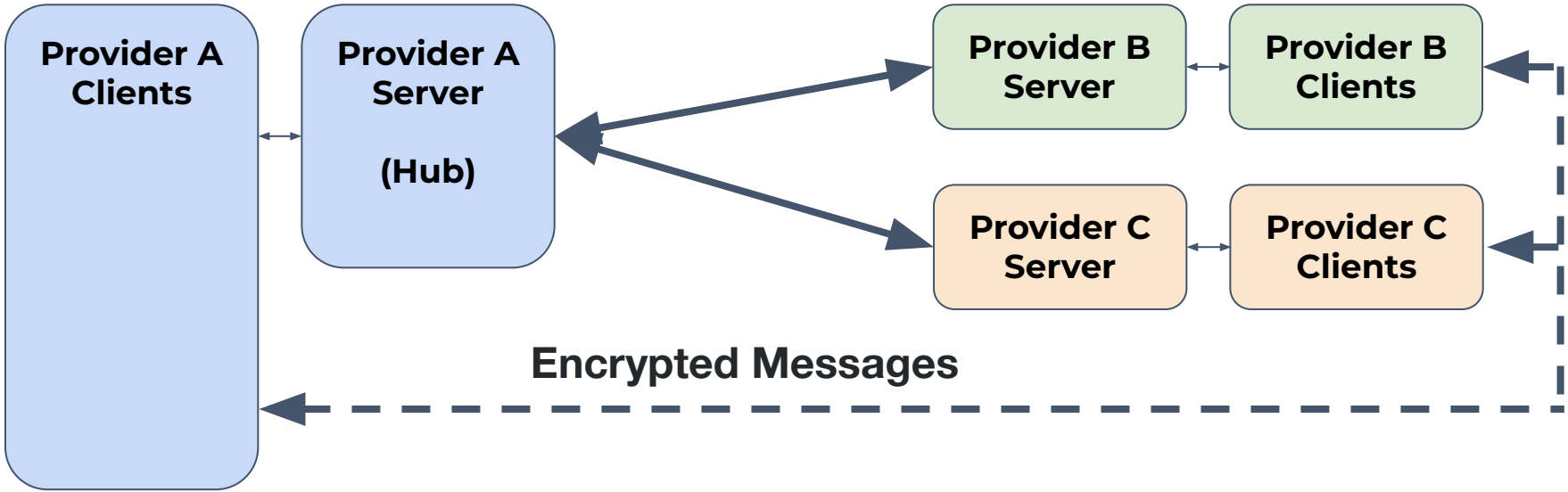
MIMI

matrix

- At last FOSDEM, the WG was putting the last finishing touches on protocol.
- I-D.mimi-arch and I-D.mimi-protocol exist, following extensive feedback from working group.
- Atomic membership operations via MLS AppSync
  - User participation and client membership updated at the same time.
- Started theorizing about a “reduced metadata” mode.
- Working on identity/discovery, and abuse reporting mechanisms.
- We continue to participate, bringing ideas back to Matrix where we can.

MIMI: Room model

- Uses a ‘hub and spoke’ fanout.
- Hub server enforces policy and distributes messages.
- Follower servers communicate through hub server whenever possible.



MLS & Matrix

MLS off the shelf

matrix

- Bring your own Delivery Service (DS; transport/fanout).
- Bring your own policy.
- Bring your own identity/concept of users.
- Bring your own content format (Application Messages).
- Cryptographic group membership for devices.
- Replaces device lists in Matrix.
- Requires a sequencing server for Commits.
- Application Messages can be out of order (up to a point).
- Key-shared history isn't really a thing: just re-send/encrypt.

Linearized Matrix off the shelf

- Hub & spoke room model, like MIMI.
- Linked list data structure internally, rather than a DAG.
- Encryption agnostic, though more aware of MLS than Double Ratchet.
- Deals with events, like normal Matrix does.
- Maintains a concept of user membership.
- Interoperates with Matrix (theoretically).

MLS+Linearized Matrix?

matrix

- User membership is a superset of MLS group membership.
- Users can be added to rooms with zero devices. Another *client* must bring that user's clients into the group.
- We would now have cryptographic room membership! 🎉
- We need a sequencing server for MLS Commits though, which would be the Linearized Matrix hub server.
- Largely unmodified Client-Server API from Matrix.
- Different federation semantics and therefore API.

MLS+Matrix?

- Room splits are a concern, when servers go offline.
- One option is to only allow the conversation to continue on the side with the hub server.
- Better option would be to support partitions and let both sides communicate.
- Consensus mechanisms may help elect hub servers on for each side of a partition.
- Consensus can also be used to (maybe) “fix” the room upon reconnection.
- MLS Re-Init may also help heal group conflicts.

Thanks

Travis Ralston
Director of Standards Development - matrix.org
@travis:t2l.io | travisr@matrix.org