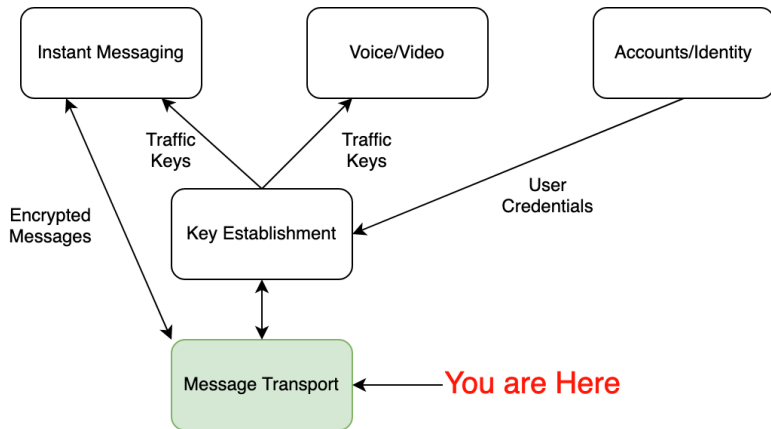


# MIMI Transport Requirements

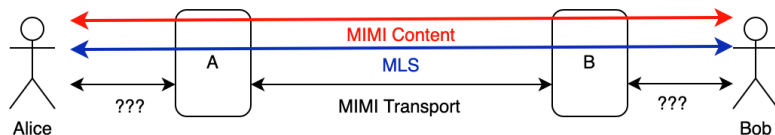
Eric Rescorla  
ekr@rtfm.com

2022-11-10

# Abstract Architecture



# Protocol Breakdown



# Question 1: How much are we defining?

- A full system obviously needs a client to-server protocol
  - Message protection and content need to be E2E
  - ... but message transport is not
- Most existing systems (XMPP, SIMPLE, etc. do it all)
- Is client  $\longleftrightarrow$  server in scope?

# Naming and discovery

- Two main kinds of existing identifiers
  - *System Specific (SSI)*. e.g., “1.650.555.1000 on WhatsApp” (or maybe `mimi:16505551000@whatsapp.com`)
  - *System Independent (SII)*: e.g., 1.650.555.1000 or `ekr`
- In general, an SII isn't enough to automatically contact someone
  - You don't know what system they are on
  - The same SII may appear on multiple systems (e.g., phone numbers on WhatsApp + iMessage)
- *Discovery* is the process of determining which system(s) an SII appears on

## Question 2: Do we need to support discovery?

- ① Only solve for SSIs
- ② Solve for SSIs now and build discovery separately
- ③ Integrate discovery and consent (SPIN, draft-rosenberg)
  - These designs assume that the SII is actually an SSI in some other system
  - What about systems that just use handles?

# Consent



- No modern system allows Alice to just start messaging Bob
- She needs to get consent first
- Typically this consists of sending an *invite*
  - Bob has to accept before seeing Alice's messages

# Question 3: What can happen before consent?

- ① Alice can't do anything until Bob consents
- ② Alice can get KeyPackages beforehand
  - Do we have to worry about exhaustion?
- ③ Alice can send messages to Bob but they're quarantined until Bob accepts
  - Potential concerns about excess data on Bob's side



# Messages and Channels

- (At least) three modalities
  - 1-1 messages
  - Group messages
  - Channels/rooms
- Some overlap between group messages and channels
- What about multiple group messages (or 1-1 messages) with the same membership?
  - This is handled inconsistently

## Question 4: What models do we support?

- ① Everything's a group (this is what MLS thinks)
  - Is this rich enough? What about moderation, etc.?
- ② Channels are fundamentally different (XMPP, Slack, etc.)
  - And maybe we don't need group messages?