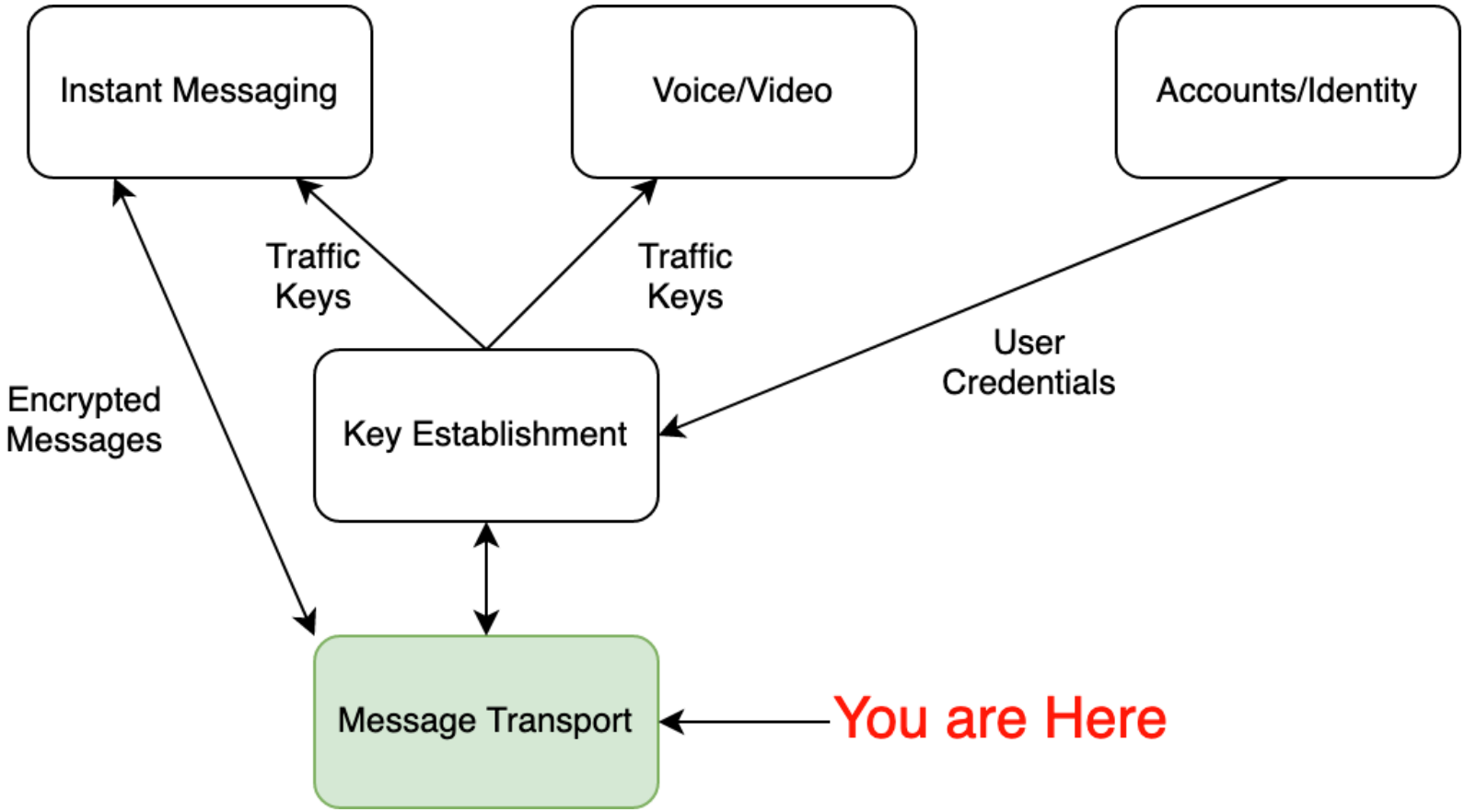
# MIMI Transport Requirements

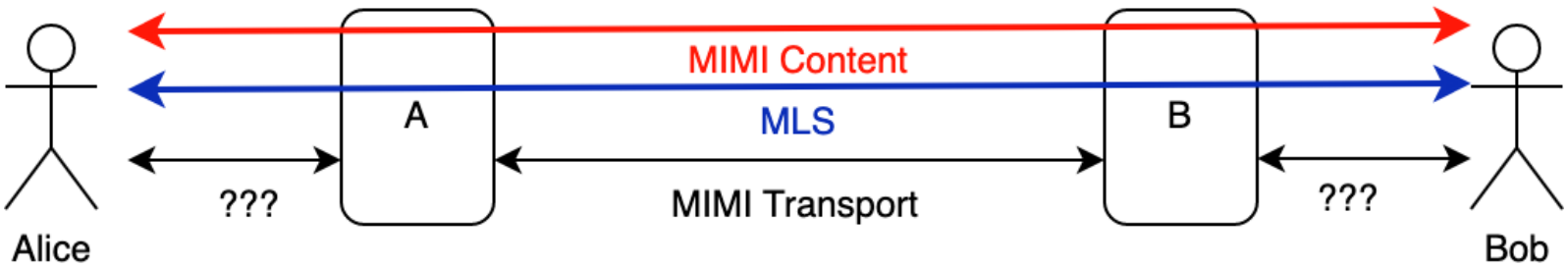
Eric Rescorla
ekr@rtfm.com

2022-11-10

# Abstract Architecture



# Protocol Breakdown



# Question: 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: 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?


- Alice just send messages to Bob if she has his identifier
  - This is a spam vector
- Or does she need to get consent first?
  - Typically this consists of sending an *invite*
  - ... Bob has to accept before seeing Alice's messages

# KeyPackage Availability

- Sending encrypted messages requires the KeyPackage
- This leaks whether the recipient exists
  - Some ideas around fake KeyPackages but I don't think they work
- Potential risk of KeyPackage exhaustion

# Question: which modes do we support?

1. Alice can send messages to Bob immediately
2. Alice can send messages to Bob but they're quarantined until Bob accepts
   - Potential concerns about excess data on Bob's side
3. Alice can't do anything until Bob consents

# 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: 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?

# Question: How much channel/room Management do we need?

- XMPP (MUC) and Matrix have fairly complicated room management
  - Ownership
  - Moderation
  - Kick/ban etc
  - Ask to join chats
- A lot of systems don't
- Is this stuff we need?

# Question: What's the basic data transfer model?

- Message delivery
  - Individual messages (SMTP)
  - Streaming (XMPP)
  - Open question: recovery from failure
- State synchronization
  - Channel/room oriented (MTP, ActivityPub)
  - Overall state (Matrix?)
  - Open question: notification of new actions
- Also some questions around transport binding 9e.g., to HTTP)

# Question: room/channel portability?

- General assumption seems to be a room/channel lives on one system
  - Except for Matrix
- Is it possible to move channels between owners?
  - For instance, if the last member from the owner leaves
  - Linearized matrix allows this
  - XMPP, MTP, etc. don't seem to

# Question: MLS-layer authentication for transport-layer transitions?

- Suppose `alice@atlanta.com` and `bob@biloxi.com` are in a channel
- Can `atlanta.com` add `adam@atlanta.com` to the channel at the transport layer?
  - This still wouldn't work at the MLS layer
  - But the roster would be confused
  - And in some systems, this might eventually end up adding `adam@atlanta.com` to the channel
- Do all transitions need to be MLS-signed and *verified* by each server

# Question: Privacy for metadata?

- `draft-robert` talks about protecting the group roster
- Is this necessary? Desirable? Undesirable?
- What about concealing the identity of the sender and the recipient(s)?