More Instant Messaging Interoperability (MIMI) Working Group

IETF 118 - Prague
November 10, 2023

Image courtesy of Stable Diffusion

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Mask policy

Note taker?

Agenda

- Chair slides (3 minutes)
- MIMI Protocol open issues (Travis Ralston and Konrad Kohbrok, 30 minutes)
- Discovery
  - Consensus points thus far (chairs, 10 minutes)
  - Interoperable Private Identity Discovery for E2EE Messaging (Femi Olumofin, 35 minutes)
  - Discovery of MIMI Service-Specific Identifiers via DNS (Vittorio Bertola, 15 minutes)

Framing of the user discovery problem

- **Service-specific identifier (SSI)**: identifies a unique user within a single service provider's service and encodes the service provider in the identifier
- **Service-independent identifier (SII)**: identifies a unique user independent of any specific service
- **Messaging providers** want to assert mappings from SIIs to their SSIs.
- A large number of messaging providers may exist.
- **Clients (or providers acting on their behalf)** want to discover which SSIs map to a given SII.
- In general, clients (or providers acting on their behalf) do not trust messaging providers' assertions of SII-SSI mappings (they may trust some, but not all). They assume some messaging providers will assert false SII-SSI mappings.

User discovery consensus points

“Discovery” involves two separable problems:

- **Authentication** of SII-SSI mappings
  - Clients (or their providers acting on their behalf) need to trust the mappings
  - Similar shape as a PKI, where **mapping authorities** doing authentication have similar properties, threat models, and constraints as CAs
    - Implies option for messaging providers to be their own mapping authorities or use third-party mapping authorities
- **Distribution** of SII-SSI mappings
  - Clients (or providers acting on their behalf) need an efficient way to query mappings from **distributions points**
  - Since mappings are authenticated, distribution points need not be trusted
  - Distribution points can be designed according to scaling and privacy goals
    - May imply that messaging providers serve as distribution points