

A view of the MIMI discovery problem

as described in draft-bertola-mimi-discovery-dns-00, sections 2-3

MIMI Interim, 30.07.2023

Vittorio Bertola <vittorio.bertola@open-xchange.com>

Defining the discovery problem



multiple 1-to-many non-exclusive unidirectional relations

Use cases

1. User A wants user B to contact them, and gives them a MIMI-specific identifier
2. User A wants user B to contact them, and gives them an «external» identifier from another service (email address, telephone number)
3. User B already knows user A's «external» identifier in another service (email address, telephone number) and wants to try contacting them

Requirements on user identifiers

- Being reachable on MIMI by an external identifier is optional and subject to the identified user's active consent
 - This implies that we also need MIMI-specific user identifiers
- MIMI-specific identifiers should be simple and human-friendly (writeable, speakable, transmittable)
- Both users and providers (and anyone else) could create, own and manage MIMI-specific identifiers
- The MIMI-specific identifier does not change when the user changes MIMI service, unless it is owned by the old service provider
- Identifiers cannot be easily guessed if the user wants so

Requirements on the solution

- Supports any number of 1-to-many non-exclusive unidirectional relations; can easily scale
- As decentralised as possible, to prevent points of surveillance
- Offers security and privacy; it is not easy to learn other people's identifiers in transit or acquire batches of identifiers and connections
- Allows for any number of discovery providers; anyone should be able to (self-)host a MIMI service, including discovery at least of their MIMI-specific identifiers
- Uses open standards, with as many implementations as possible; barriers to entry should be as low as possible

Requirements on the solution (non-tech)

- Does not create intellectual property issues (e.g. ownership of identifiers)
- Does not pose significant legal and regulatory issues, or require significant regulatory work; in particular, it is compatible with the main data protection regimes
- Is cost-effective
- Has a business model