User Discovery Requirements

draft-interop-mimi-discovery-requirements

Giles Hogben, Femi Olumofin, Jon Peterson, & Jonathan Rosenberg
IETF 121 Dublin
November 7, 2024

Overview

- MIMI user discovery enables a message sender to locate messaging service providers on which a particular recipient can be reached
  - requires no prior knowledge of the recipient's provider

- The draft defines requirements for user discovery using globally unique identifiers
  - phone numbers
  - email addresses

Terminology

- **Cross-Service Identifier (CSI):** A globally unique identifier for a user across services (e.g., phone number, email address)
- **Cross-Service Identifier Provider (CSIP)**: An entity that issues and manages CSIs (e.g., telco companies, email providers)
- **Messaging Service Provider (MSP)**: An entity that provides messaging services (e.g., WhatsApp)
- **Service Specific Identifier (SSI)**: A unique identifier for a user within a single messaging service (e.g., an X handle)
- **Discovery Provider (DP)**: An entity that collects, stores, and facilitates the discovery of CSI to MSP mappings

The Discovery Problem

- Asserting verifiable mappings between CSIs and MSPs
- Looking up mappings to determine MSPs for which a CSI can be reached
- Additionally:
  - Prioritize user privacy
  - Allow users to control their discoverability
  - Integrate well with E2EE and other MIMI protocols

Requirements in -01

Authenticating Mappings

Discovery Protocol

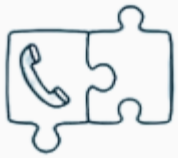
Preferences

Operational

Security & Abuse Prevention

Authenticating Mapping Requirements

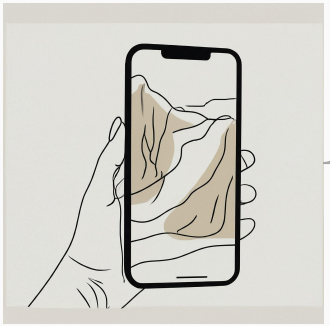
1	DP MUST verify user's CSI possession through proof-of-possession challenges through a CSIP, certificate authority or designated parties
2	MSP MUST confirm CSI reachability on its service
3	Client, MSP, and DP MUST jointly compute a verifiable mapping representation of CSI-to-MSP
4	DP MUST NOT be able to create a verifiable mapping without CSI holder and MSP involvement
5	DP MUST NOT be able to falsely claim user completed proof-of-possession
6	Other users MUST be able to verify CSI holder's participation in mapping creation



Basic Recipient's Preference Requirement

7	Authenticated mappings MUST include a preference index or string to allow recipients to control their preferred contact method

Client



$CSI_1 \Rightarrow \{MSP_1, \ldots, \mathbf{0}\}$

$CSI_1 \Rightarrow \{MSP_2, \ldots, \mathbf{2}\}$

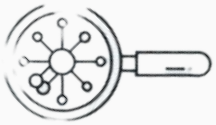
$CSI_1 \Rightarrow \{MSP_3, \ldots, \mathbf{3}\}$

$CSI_1 \Rightarrow \{MSP_1, \ldots, \text{"business"}\}$
$CSI_1 \Rightarrow \{MSP_2, \ldots, \text{"basketball"}\}$

IETF

Discovery Protocol Requirements

8	Discovery requests MUST support any globally unique CSI with backing source of truth (CISP for telephone), ownership proof, and cross-service usability
10	Discovery requests MUST support federation, MSP filter, and DP list query parameters
11	DP MUST disclose default behavior and follow the agreed-upon federation default
12	DP MAY rate-limit non-default queries given their higher processing costs
13	DP MAY rate-limit requests sent to low-throughput DP endpoints
14	DP MUST protect at least the querier's identity or the target CSI in requests
9	Discovery responses MUST accommodate zero, one, or multiple MSPs in results
15	MUST define both verbose and compact response formats, where verbose responses include detailed mapping information and metadata, while compact responses provide a simple indication of CSI reachability on returned MSPs



Operational Requirements

16	Discovery service MUST remove mappings made outdated by CSI re-assignment to a new user within a reasonable time
17	Older mappings generally take precedence over newer ones for the same CSI unless explicitly invalidated by the original CSI holder or superseded by a stricter proof of possession verification
18	DP MUST verify if a mapping is the first mapping for a given CSI and, if so, broadcast invalidation requests to other DPs to invalidate any existing mappings for that CSI
19	Users SHOULD be provided with mechanisms to invalidate existing mappings or create replacement mappings for their CSIs
20	New CSI mappings SHOULD be discoverable within some standardized maximum time limit (e.g., 24 hours)

IETF

Security & Abuse Prevention Requirements

21	Discovery service MUST leverage contractual and technical means to prevent malicious MSPs from falsely claiming CSI association
22	Discovery service MUST incorporate anti-DDoS, anti-enumeration, and anti-spam mechanisms
23	All communication between clients, DPs, and MSPs MUST be encrypted in transit and authenticated

IETF

Refined Requirements

Simplified the **initial 23** detailed requirements
into
10 broader, high-level requirements

Requirement roles

Recipient	Sender	Discovery Provider
		
• Possesses a CSI assigned by a CSIP • Authorizes verifiable mapping of CSI to an MSP set • Recipient of communications	• Knows of a CSI • Discover mappings of CSI to MSP sets • Sender of communications	• Aggregates verifiable mappings by recipients • Retrieves mappings for CSIs of interest to senders

Recipient Requirements Preconditions

- The user possesses a valid CSI issued by a CSIP.
- The user has an active account with the MSP.
- The user associates the CSI with the account.

—

Reference:
CSI (Cross-Service Identifier): Your globally unique ID across multiple services like your email addresses and mobile phone numbers

CSIP (Cross-Service Identifier Provider): The issuer of your globally unique ID, like your email provider and telecoms

MSP (Messaging Service Provider): The platforms we use to chat e.g., WhatsApp

Recipient Requirements

1	Any mapping of a CSI to an MSP set MUST only be verifiably authorized by the recipient
2	A mapping MUST allow for the inclusion of tags or similar constructs to indicate the recipient's preferences for using each included MSP
3	Authorization to remove existing mappings for a given CSI MUST be limited to either the recipient or the CSIP managing that CSI (in cases of reassignment)

Sender Requirements

4	During discovery, a sender MUST be able to retrieve all of the verifiable mappings that exist for a given CSI
5	Mappings MUST include means for senders to verify their authenticity

Discovery Provider Requirements

6	Mappings discovery for a given CSI MUST support results with zero, one, or multiple mappings
7	The privacy of the sender's social graph MUST be protected using appropriate mechanisms. At a minimum, the privacy of one or both of the following MUST be preserved: ● Source IP address, username, and other identifying attributes ● Queried CSI and response mappings
8	If data is exchanged between two or more servers as part of processing discovery requests, it MUST NOT include any identifying information about the request source • • •

IETF

Discovery Provider Requirements

9	All data exchanged between clients and servers in the processing of a discovery request MUST be encrypted in transit
10	Any database with verifiable mappings MUST be protected against enumeration attacks aimed at extracting all or a substantial portion of its records

IETF

Summary

- Reframed the initial requirements to be both comprehensive and high-level, ensuring flexibility for future design work
- **The authors express gratitude to the Working Group for their valuable feedback, with particular appreciation for the insightful feedback from Ekr on this iteration of the requirements**