

# User Discovery Requirements

[draft-interop-mimi-discovery-requirements](#)

Giles Hogben, Femi Olumofin, Jon Peterson, & Jonathan Rosenberg  
IETF 120 Vancouver  
18 September 2024



# Overview

- MIMI user discovery enables a message sender to locate messaging service providers on which a particular recipient can be reached
  - Eliminating the need for prior knowledge of the recipient's specific service
- The draft defines requirements for user discovery using globally unique identifiers, such as email addresses, and phone numbers

# Terminology

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

# The Discovery Problem

- Asserting verifiable mappings between CSIs and MSPs
  - Assertible by a single DP, yet distributable by any DP
- Looking up mappings to determine MSPs for which a CSI can be reached
  - Authenticity is verifiable using the included metadata
- Additionally:
  - Prioritize user privacy
  - Allow users to control their discoverability
  - Integrate well with E2EE and other MIMI protocols

# Requirements

Authenticating Mappings



Preferences



Discovery Protocol



Operational

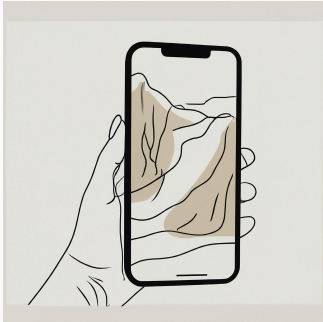


Security & Abuse Prevention



# Authenticating Mappings

Client



MSP



- Jointly computed
- Client proof of possession
- MSP confirms reachability
- Prevent independent DP assertions
- Publicly verifiable

DP



+14081231234 ⇨ {Wire, metadata, signature}

# 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 collaborate to generate a verifiable representation of the CSI-to-MSP mapping. This can then be shared with any DP and verifiable by clients
- 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

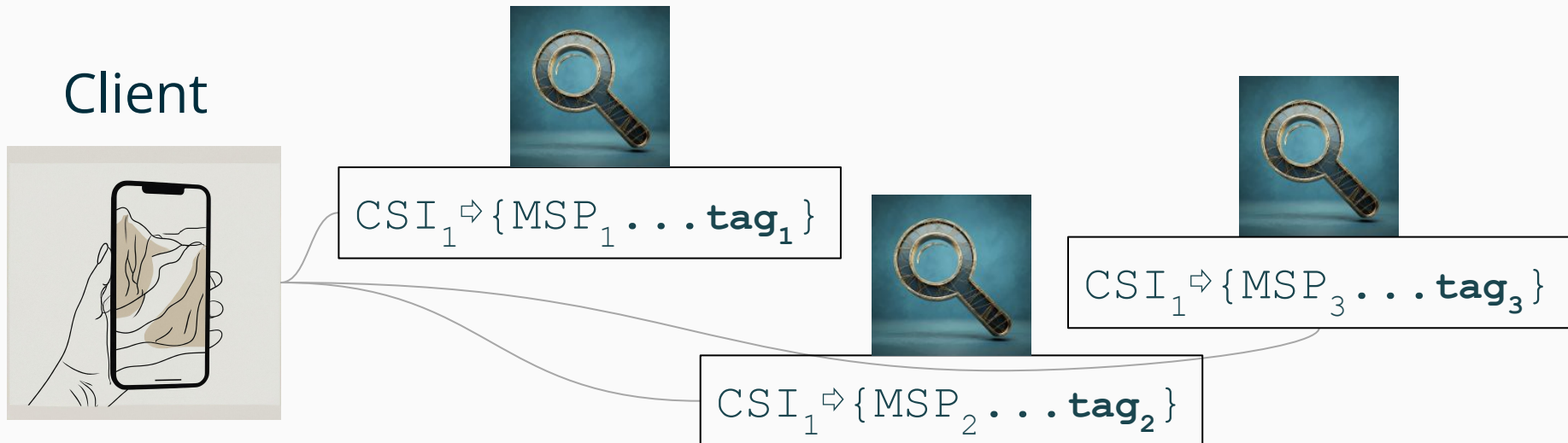


# Preferences

- Preferences of multiple stakeholders:
  - Sender seeking reachability information
  - Recipient with the mapped identity
  - DPs (and collaborating MSPs)
- Requirements considered **recipient preferences** only (CUJs):
  - Sender mapping preferences
  - Same-app preferences
  - No-random mapping preferences
  - No-duplication preferences
  - Per-sender preferences
  - Closed/Open-ended group preferences
- Decisions:
  - Deferred detailed preferences/capabilities to implementations
  - Includes a basic requirement

# Basic Recipient's Preference Requirement

- 7 Authenticated mappings MUST include a preference **tag** to enable recipients to control their preferred contact mapping



$CSI_1 \mapsto \{MSP_1 \dots, \text{"Default"}\}$

$CSI_1 \mapsto \{MSP_2 \dots, \text{"WhatsApp"}\}$

$CSI_1 \mapsto \{MSP_3 \dots, \text{"HoopsFriend, Personal"}\}$



# Discovery Protocol: requests

- Define message format for requests
- CSI: telephone number or email address
  - Globally unique, backing source of truth, user ownership proof, and cross-service usability
- Parameters:
  - Federation: Control whether the DP queries other DPs
  - MSP filter: Scope responses to specific MSPs of interest
  - DP list: Guide query federation decisions with sub-options for:
    - DP-preferred federation
    - Client-selected federation
    - All DPs

# Discovery Protocol: processing

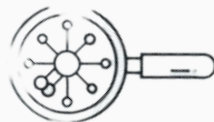
- Protect user discovery social graph either by making the querier anonymous or the CSI and mapping confidential
- Disclose default behavior (e.g., do not federate for performance, privacy or regulatory reasons) and comply with federation defaults
- Allow client rate-limiting for non-default queries
- Allow other DPs rate-limiting if they have low-throughput
- Define sub-protocols to facilitate communication and data exchange between between DPs and MSPs

# Discovery Protocol: responses

- Accommodate scenarios with varying numbers of MSPs or mappings in the discovery results
- Support verbose and compact response formats:
  - Verbose: includes unique list of mappings discovered with metadata for mappings verification
  - Compact: such as a bit string, where each set bit indicates the CSI is reachable at the MSP assigned to that bit position

# Discovery Protocol Requirements

- |    |   |
|----|---|
| 8  | Discovery requests <b>MUST</b> support any globally unique CSI with backing source of truth (CISP for telephone), ownership proof, and cross-service usability  |
| 9  | DP <b>MUST</b> protect at least the querier's identity or the target CSI in requests  |
| 10 | Discovery requests <b>MUST</b> support federation, MSP filter, and DP list query parameters   |
| 11 | DP <b>MUST</b> disclose default behavior and follow the agreed-upon federation default  |
| 12 | DP <b>MAY</b> rate-limit non-default queries given their higher processing costs  |
| 13 | DP <b>MAY</b> rate-limit requests sent to low-throughput DP endpoints   |
| 14 | Discovery responses <b>MUST</b> accommodate zero, one, or multiple MSPs in results  |
| 15 | <b>MUST</b> 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 |

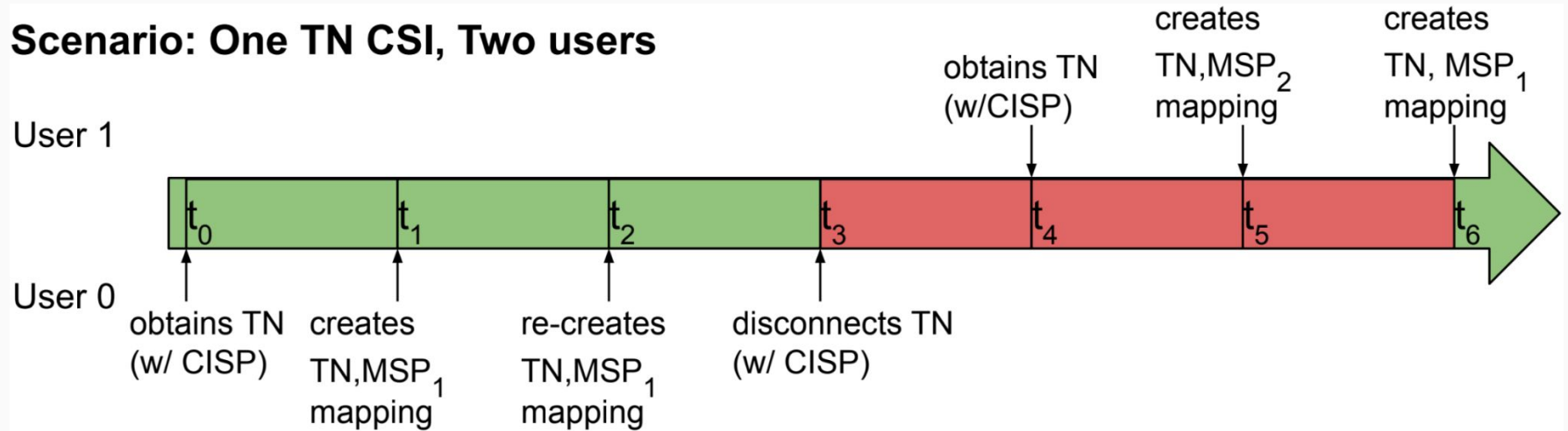


# Operational

- Making changes
  - Obtain new CSI (retire mappings with old CSI)
  - Update existing mappings (e.g., key rotation)
  - Invalidate/delete existing mappings
- Timeliness
  - Remove outdated mappings promptly, considering legacy system limitations (telephone number routing/assignment)
  - Enable discoverability of new CSI mappings within a specified timeframe

# Operational

## Scenario: One TN CSI, Two users



Time	Discovery results	Possible mitigations
$t_3$	Incorrect TN,MSP <sub>1</sub> mapping because TN is now inactive	(1) DP should subscribe to inactive TN pool channel (challenging) (2) MSP should broadcast new TN updates by users (with consent) to enable old TN mappings deletion
$t_4$	Incorrect TN,MSP <sub>1</sub> mapping for new TN user	DP should subscribe to TN reassignment channel
$t_5$	Correct and incorrect mappings (TN,MSP <sub>2</sub> and TN,MSP <sub>1</sub> )	DP should confirm if mapping is first and broadcast invalidation requests to other DPs to void existing mappings

# Operational Requirements

- |    |   |
|----|---|
| 16 | Discovery service <b>MUST</b> 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 <b>MUST</b> 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 <b>SHOULD</b> be provided with mechanisms to invalidate existing mappings or create replacement mappings for their CSIs   |
| 20 | New CSI mappings <b>SHOULD</b> be discoverable within some standardized maximum time limit (e.g., 24 hours)   |



# Security and Abuse Prevention

- Blackhole prevention
  - Prevent malicious MSPs from falsely claiming CSI association to hijack discovery of legitimate mappings
- DDoS, enumeration, and spam prevention
  - Implement robust mechanisms to thwart attacks and abuse (e.g., rate limiting, obfuscation, and differential access based on reputation)
- Encryption and authentication
  - Ensure all communication between clients, DPs, and MSPs is encrypted and authenticated

# 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                                 |



# Additional areas critical for user discovery/implementation

- Federation mechanisms
  - Define protocols for communication and data exchange between DPs
- Data sovereignty
  - Respect data locality and jurisdictional laws (e.g., GDPR)
- Registry
  - Service Host for DP metadata and service configurations in a federated DP scenario

# Summary

- These requirements are for a secure, privacy-friendly, and efficient user discovery service for MIMI
- By specifying/implementing these requirements, we can empower users with greater control over their discoverability and create a more interoperable messaging landscape
- **The authors extend their sincere gratitude to the working group for their invaluable feedback and insightful discussions during the WG meetings**

# Next Steps

- Call for adoption