MIMI Discovery

IETF 119

MIMI WG

Brisbane – Mar 2024

J Peterson
Consensus Points (from October)

• We assume there are multiple Messaging Service Providers (MSPs)
• MSPs want to assert mappings for the Service Independent Identifiers (SII) registered at their platform
  – E.g. telephone numbers whose users are reachable at the MSP
• Message senders want to discover which SIIs map to which MSPs
• The ecosystem does not generally trust MSPs not to assert false SII-SSI mappings

• The discovery problem is thus twofold
  – Authentication: MSPs need to trust someone to authentication SII-SSI mappings
  – Distribution: MSPs need a way to query SII-SSI mappings across multiple platforms
First Principles

• A Discovery Provider (DP) operates a query service
  – Query key is an SSI
  – The base query response value could be:
    • A. Reachability information for one or more MSPs
      – A protocol interface to which messages can be sent for that SII
    • B. One or more SSIs
      – These would be a URI or similar globally-routable locators
    • Some SSIs will be composed of an SII and a domain, basically, so
      the distinction between A and B is inexact
      – If you already have or can make an SSI, you don’t need discovery
  – There are use cases for additional data in the response
    • Keying information, for example – or similar metadata
Second Principles

• Which SIDs are in scope?
  – Telephone numbers seem like the most pressing case
    • Mobile numbers the most pressing of those
    • There are use cases where landline (e.g. triple-play) telephone numbers can receive/send messages
  – Should email addresses also be in scope?
  – Do we gain anything by restricting the scope to mobile numbers?
    • One potential gain is the difficulty of ascertaining the geopolitical location of email addresses
Fundamentals of DPs

• Is the DP a logical singleton?
  – Or will there, for various geopolitical and policy reasons, be sharding?

• Will a discovery query involve more than one DP?
  – Do we expect DPs should act something like recursive resolvers?
  – Or do we expect queriers (MSPs) will fork queries to multiple DPs?

• Do we expect some Message Service Providers (MSPs) will run their own DP?
  – A world where basically you go to each MSP to get info about their users
    • May be equivalent to just sending an SII in a message to each MSP
  – If an MSP is the default DP for a client, is there potential bias in the discovery result?

• Should users have to be aware of DPs at all?
  – What sorts of policies shape which DPs would be queried, and how are those policies expressed, and by whom?
Query/Response Fundamentals

• When do we think discovery happens?
  – Right as a message to an SII about to be sent?
  – When a user establishes some sort of contact book or social graph?

• What happens when discovery yields multiple mappings for an SII?
  – Is the originator of a message given a choice between them?
  – Does a message fan out to all of them?
  – Is it the job of the originating MSP to narrow it down to one?
    • Maybe with the aid of preferences, see next slide
User and Social Graph Privacy

• Are the mappings aggregated at DPs private?
  – Is the information that a given MSP is a route to an SII itself sensitive?
  – Is there a requirement to prevent enumeration attacks?
    • Or do we think MSP mappings are basically public?

• How important is spam prevention for SIIs in particular?
  – SIIs kind of have a built-in spam problem – you can still receive unsolicited SMSs, for example

• How can we protect discovery from data collection threats?
  – Correlation threat in particular between discovery queries and messages
  – Currently thinking is that we want to either:
    • Hide the IP address of the querier from the MSP/DP (with IP blinding)
    • Hide the data an MSP is requesting from a DP (with PIR)
Sender and Receiver Preferences

• Again, how aware do users want/need to be of the discovery process?

• Sending User
  – Should a sending user’s preferences determine which MSP a message will go to?
  – Should capability be a factor (e.g., already having an account on MSP A, B, and C but not D or E)?

• Receiving User
  – Should a receiving user be able to express prefs about the MSP(s) on which they receive communications?
    • How rich should those prefs be? Should concepts like context (work/home) be a part of them?
    • Is enforcing a default potentially unfair to non-gatekeeper MSPs?

• Who or what reconciles these capabilities and preferences?
  – Are we setting ourselves up for another OFFER/ANSWER?
Discovery and MIMI identity

• Why should MSPs trust the mappings held by a DP?
  – Concern is that a rogue MSP/user will illegitimately advertise itself as a route to an SII to a DP

• This has some interaction with how identity works in MIMI
  – See draft-mahy-mimi-identity
  – Who should be able to claim an SII as an identifier in communications?

• Is there a need for neutral services to prove mappings/identities for SIIs?
  – An example is sketched in draft-peterson-mimi-idprover
  – Some MSPs (likely “gatekeepers”) are likely to act as their own idprovers, just as they might act as DPs
    • There may be for legacy user bases, but should MIMI require stronger proofs for new SII enrollments?