Consensus Points: The Basics

• Discovery Provider (DP)
  – May be operated by MSPs, or may be independent

• Messaging Service Provider (MSP)
  – There are many of these, who may be federated (or not)

• Authenticated Mappings
  – Are aggregated at DPs, and map between identifiers and MSPs
  – Relying parties trust the signers of mappings, which are not necessarily a DP or MSP

• Discovery queries use identifiers as a key
  – Gone around on terminology a few times now
    • Proposal: Instead of Service Independent Identifier (SII), let’s use Cross-Platform Identifier (CPI)
    • Keep Service-Specific Identifier (SII) as is.
  – Anyone object?

• Discovery is not required by the DMA – this is extra credit work
Consensus Points

• The discovery problem is twofold
  – Authentication: MSPs need to trust someone to authenticate mappings
  – Distribution: MSPs need a way to query for mappings across multiple platforms

• Discovery acts on CPIs
  – If you already have an SSI, you don’t need discovery

• Preference expressed for a “singleton” DP – probably operated by an MSP
  – But let’s design protocol in as architecture-neutral a way as possible
    • Works whether users or MSPs query DPs
  – Discovery should be able to work at various stages of messaging
    • From contact books, at the time messages are sent, upon consent, etc.
  – People generally unconcerned about enforcing “fairness” in discovery
    • Or rather, that it seems too hard to enforce

• We agree that discovery is not about finding a common capability between platforms
  – Still a bit murky about what user preferences are...
Receiver Preferences

• At the end of the last interim, we were focusing on receiver preferences
  – Not so much interest in sender preferences
  – General sentiment was we should keep things simple
    • As Alissa noted, it's not like we got this right for email, etc.
  – We frequently appealed to being able to sort incoming requests into contexts
    • Work, home, hobby, etc.

• So what would this look like?
  – How does a receiving user be able to express prefs about the MSP(s) on which they receive communications?
    • Is this like a document that users will create (Rohan's “card”?)
    • How rich should those prefs be?
    • Is enforcing a default potentially unfair to non-gatekeeper MSPs?

• Who or what enforces receiver preferences?
  – Is this the job of the DP? Of the MSP? Or of users somehow?
User and Social Graph Privacy

• Are the mappings aggregated at DPs private?
  – Is the information that a given MSP is a route to a CPI itself sensitive?
  – Is there a requirement to prevent enumeration attacks?
    • Or do we think MSP mappings are basically public?
• User consent and involvement in mappings creation
  – Must users consent to create CPI-to-MSP mappings?
  – Must users participate to create mappings?
    • Mitigates MSP-DP collusion scenario
• How important is spam prevention for CPIs in particular?
  – CPIs 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)
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 CPI
• This has some interaction with how identity works in MIMI
  – See draft-mahy-mimi-identity
  – Who should be able to claim a CPI as an identifier in communications?
    • Also I understand there has been some recent discussion about pseudonyms etc at other MIMI interims
• Is there a need for neutral services to prove mappings/identities for CPIs?
  – 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 CPI enrollments?
Open Concerns

• How to provide a “consistent user experience” of discovery
  – Authenticated mappings are a key part of that
    • Not all mappings will be available at all DPs, though
  – When multiple MSPs have authenticated mappings for a CPI, who chooses and how?
    • Random is not consistent
    • Drop down menus are not necessarily what users want

• Realistically, the best we can do is provide tools that MSPs will use to realize MIMI

• Any other issues people want to raise?
  – We’ve covered a lot since Brisbane
Path Forward

• Hopefully we don’t need to block out chunks of time this big for high-level discussion anymore
• The Plan: issue a new discovery requirements document
• Enumerate what the requirements are we’ve captured so far
  – Get this in shape for Vancouver