MIMI Security and Privacy Requirements

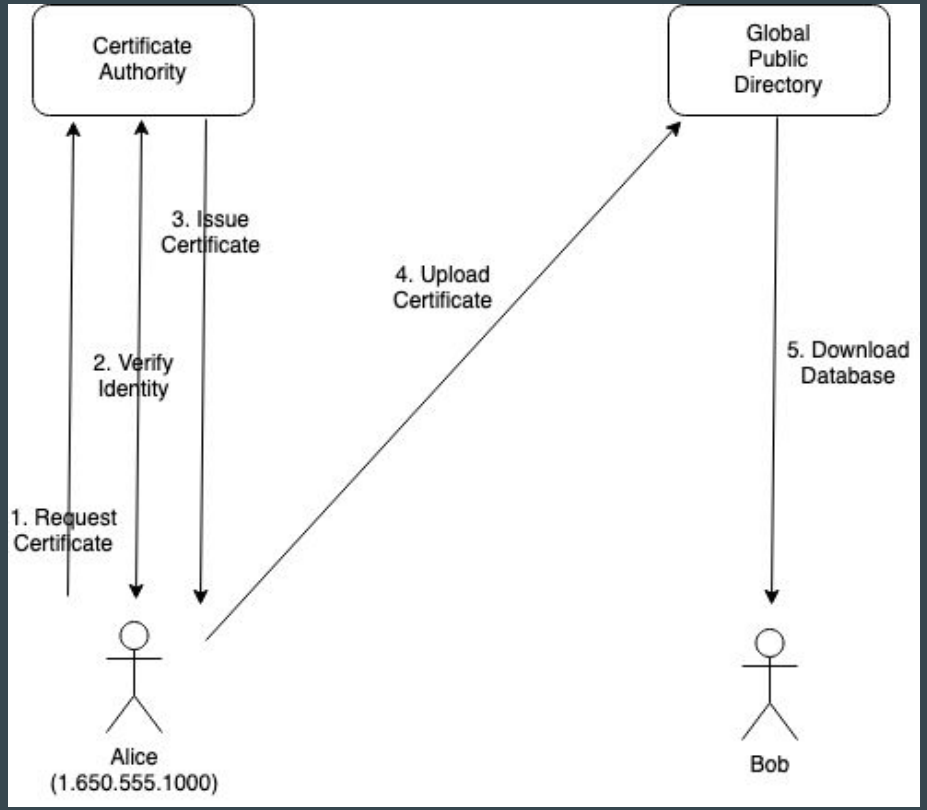
Interim 2023-09-13

Eric Rescorla

Overall Context

- Alice has one or more SIIs (let's just assume one for now)
- Alice signs up for some set of applications **A**
  - Each application has an SSI
- Bob has Alice's SII and wants to contact Alice
- Needs to look up the mapping of Alice's SII to her SSIs and associated metadata
  - e.g., Keying material
- Probably via some kind of discovery service

Intuition Pump: What's wrong with this picture?



Security of SII → SSI Mapping (I)

- Who is allowed to record a mapping for a given SII?
- The discovery service (if any)
- The application provider?
  - If so, what prevents claiming to serve an SII you do not?
- Only the end user?
  - If so, how is this authenticated?

Privacy of SII → SSI Mapping: Big picture

- Is this information secret at all?
- It's possible now to probe services individually for accounts "does this person have an account on WhatsApp"
- But maybe not at scale

- Are we trying to solve this problem at all?*

*If "no" we can skip the next three slides.

Privacy of SII → SSI Mapping: Other Users

- Option 1: Alice can't find Bob's SSIs without his consent?
  - If not, is this interactive (as in spin) or static (as in the contact list)?
  - Where is this enforced?
- Option 2: She can find them without his consent, but we are trying to prevent mass disclosure
  - Some kind of rate limiting?

Privacy of SII → SSI Mapping: APs

- Should APs be able to get other APs mappings?
- Should this be restricted?
  - For instance by permission or by contact lists
- Rate limited?

Privacy of SII → SSI Mapping: Discovery Service*

- Are we trying to conceal this information from the discovery service
- This seems challenging

*Whatever that is

Privacy of Social Graph

- Are people's contact lists secret? Assume the answer is "yes"
- Should the discovery service be able to see the pair of requester/target?
- Should APs be able to see the pair of requester/target?

Tradeoffs

- It’s tempting to answer “yes” to all of this stuff
  - Privacy is good
- But there are tradeoffs
  - Design complexity
  - Some types of privacy may be at the expense of others