2023-03-23

Attending: Heather Flanagan, Judith Bush, Mary McKee, **Gary Windham**, Chris Phillips, Scott Cantor, Zacharias Törnblom, Philip Smart, Gabor Eszes, Kellen Murphy, Mark Rank (joined at the half)

1. Agenda bash and ask for scribes
2. Why we’re doing this - recap
3. Mondays meeting (**FedID CG**) - key takeaways (Heather’s list)
   a. Scale (number of IdPs)
   b. Origin (browser) vs endpoints (SAML/OIDC)
      i. It is, and isn’t an issue
   c. Proxy services
   d. Interferes with at least the SAML protocol on a level outside of 3pc
   e. Session timing (i.e., sessions may be very short-lived)
      i. CP: FedCM talks about ‘accounts’ when in reality this is about ‘sessions’
   f. SAML and OIDC have similar but not the same behavior, esp. when it comes to circles of trust
4. What is missing from the proposals
   a. How can we be more precise in our use cases
      i. The basics?
      ii. Showcasing what the expected FedCM implementation should look like?
   b. How can we make sure the responses from browsers are more precise

**Livescribe Minutes**

Why we’re doing this - recap

Shared discussion - Communication about the changes coming to our community; there’s the communication/advocacy up to the browsers

- How do we harness interest from the community as we delve into technical proposals and the sense of urgency diminishes?
  - Upcoming Presentation at TNC (Albania) - Philip Smart
  - Upcoming Presentation at I2 Community Exchange (Atlanta) - Judith Bush
  - Mary McKee: instead of saying “here’s why FedCM is bad for us”, focus on how [paste recap from below]
  - We need to keep up-to-date on the latest info, people want to know how it affects them, how it breaks. “Daylight on the topic:”
  - Mary: I do think communication back to the R&E community needs to frame the problem in the way we need to communicate to the FedCM development community - if we don’t reframe the problem statement somewhat (and peg communications around that), we’ll continue having to follow up with reframing, which seems to be eating a lot of time.
  - Scott: I can try to get a joint stance from the people who worked on SAML, that may help

- FedSSO is not just an R&E story but a globally accepted practice story – case in point:
  - Part of the usGov framework

- Now, for technical stuff:
  - Tempo/cadence of which/how to handle the scale problem (our item 1, issue 4 in tracker)
    - Phil: suggestion on breaking out the FedCM API to some of the results from March 20th call which seemed to have a different direction after the demo (scaling issues were highlighted)
  - If

- If not clear already in the proposals, add pre-requisite that SAML is required to work in order for the two proposals to work
- Could this be pushed out in a staged process - where our proposal is an interim step

The “six takeaways” i.e. six key current barriers affecting the current FedCM proposal from our point-of-view from the previous FedID CG meeting:

1. Scale (number of IdPs) – FedCM UX proposals cannot accommodate the 1000s of IdPs that could potentially be used; the protocol cannot accommodate concepts like SAML federations, WAYF
2. Different trust domains: Origin (browser) vs endpoints (SAML/OIDC)
3. Proxy services
4. Interferes with at least the SAML protocol on a level outside of 3rd party cookies
5. Session timing (i.e., sessions may be very short-lived)
6. SAML and OIDC have similar but not the same behavior, esp. when it comes to circles of trust

“Interferes with at least the SAML protocol on a level outside of 3pc”

- Also, FedCM is designed with the assumption that the SP enumerates all possible IdPs it’s willing to accept, which doesn’t fit the federated trust model we’re used to
  - Also the IdP needs to enumerate all SPs it’s willing to talk to also.
- How do we find out whether this is a genuine intent of FedCM or a misfeature?
Z: Q: how do we offer constructive ways to handle these things
   • Adjust the issue?
   • Submit the smaller items chopped up into the things?
   • <no clear answer offered yet?>

Discussion on the nuances of what consumes what, and then how that is protected (SECFETCH?)

After 'yes',

CP: <not discussed>: Q: if a new RP is coming online and needs to decide what technology to use for SSO, why would they choose this new tech?

Actions undertaken: Phil to touch base with Sam to check in on things to be taken.

Group outlook:
   • Possibility to submit issues but structurally first

Comment: Interrogate idp to get consent and then get out of the way