Hackathon outcomes

On the morning of March 1st, Judith Bush posted to the eduGAIN@fedcm slack channel:

Hi there, reporting from Hotel Zico. Yesterday’s meeting concluded with a glow of satisfaction for all parties. Cameron (Mozilla) and Sam (Chrome) grew to appreciate the security aspects of federation controlled metadata, in particular

* the oversight and policy, and
* the security of inclusion of both the IdP & SP’s endpoints

By providing a way browsers can confidently classify transactions as federation vetted authentication patterns instead of possible tracking over time (that is, they can trust that participants are continually being reviewed for compliance), federations that can participate in an as yet defined conglomeration of federations will be able to use their protocols as currently implemented, and new protocols can evolve. The user will communicate to the browser through a Seamless Access like pattern that they are choosing a particular IdP for a RP. The user will be able to continue to add different IdPs to their choices. The browser storage will persist the choices to help speed selection. Once that choice is made, the browser identifies the chosen IdP to the RP, and the protocol exchange begins. There’s a proposal that the chosen federation provides the selection UX. This allows for a federation appropriate user experience, such as eIDAS presenting a map. As an additional efficiency and privacy protection is that the RP can specify which of the possible federation IdPs are acceptable. This filter will prevent a user from leaking an affiliation that is not appropriate for the RP.

By the end of March 1 we had two proposals, that could be considered one staged proposal of an evolution in trust:

idp-sp-storage-api: [https://github.com/fedidcg/proposals/issues/4](https://github.com/fedidcg/proposals/issues/4)

In this proposal, the SP tells the browser the user’s IdP choice (that can be mediated by a SeamlessAccess discovery UI) plus provides the IdP and SP endpoints (as in metadata) so that the browser will classify those endpoints as authentication if the user permits the linking between IdP and SP.

Offloading Trust: [https://github.com/fedidcg/proposals/issues/5](https://github.com/fedidcg/proposals/issues/5)

In this proposal, the discovery pattern is intermediated by the Browser – this melds the UX of discovery with the browser registration of an approved IdP and SP link and prevents the SP from knowing the user’s IdP choice until it is approved BUT the UI is a much heavier lift for the browsers. A further step of publicizing the federation allows browsers to not merely trust the SP that the endpoints are not tracking but have a fourth party – the federation – ensure trust.

We admit that both these proposals elevate authentication NASCAR issues from the IdP to the federation if an SP needs to participate in multiple federations.

One significant amount of work: showing up to polish and defend our proposals at the FedCM W3C CG

More work: middle things! do proxies just iterate using the same approval flows? What sort of federation extensions are needed? Can Browsers use [https://www.iqtf.net/sinctfi/](https://www.iqtf.net/sinctfi/)? How do we prepare for OAuth federations? Are our communities ready to work on the changes to “log on” and “sign on” buttons everywhere?