June 7, 2018

Attending: Tom, Hannah, Pål, Uros, Romain, Brett, Niels, Alan, Shannon, Niels

Proposed agenda:

1. Agenda bash
2. Niels' presentation

Stimulating presentation engendered much back and forth discussion. Niels sketched a technical process and also ideas on operationalizing it. The technical sketch is that a system, for example based on pyff, can take in eduGain entity metadata and enhance it according to defined policies. It would do so by also hosting a service for community-sourced "pixie dust", ie, entity metadata decorations whose semantics need only be shared by a given community. Data added by means of the service, eg, Sirtfi self-attestation and security contact info, would be added only to those eduGain entities lacking same. SPs would consume the dusted entities by pulling entities from the service as a secondary authoritative source, after their home federation.

Niels envisioned locating this capability on research community proxies. This would address needs for Sirtfi and any other community-local pixie dust they may need and also solves the problem of those relying on dusted metadata knowing whether to trust its source. Everything is local: trust, operations, pixie dust semantics.

WG members had some questions and concerns about that community-local model. It would require interaction between each research community's proxy operator and each IdP that's home to a user in the research community, with implication that it might end up only partially addressing the problem of working around R&E Feds that don't yet enable their members to add Sirtfi stuff to their entity metadata, even when that problem is constrained to research community use cases. It also does not address the problem of SPs lacking Sirtfi stuff in their R&E Fed metadata and IdPs that need to know it, or fed operators that need to know it to enable mounting a response to a security incident.

But Niels' ideas suggest another operational model that might better fit the Sirtfi requirements. Have a single, global, instance of a "Sirtfi pixie dust metadata oracle". Operated by Geant or IGTF, for example (big ask, but just imagine for a moment). Pyff creates dusted metadata as sketched above, all signed by a key allocated to this operation to signify adherence to its committed operating policies, which themselves must carefully express that all eduGain sourced metadata details are untouched, that only Sirtfi dust has been sprinkled, that it's the bona fide REFEDS Sirtfi and no other, that only the right types of people have been authorized to submit Sirtfi attestation and security contact info, that sort of thing. In other words, we'd have to face the hard problems that Niels' community-local approach side-steps.

3. With that fresh in mind, review Sirtfi+ Registry requirements doc

   No time.

4. Else?