June 21, 2018

Attending: Tom, Alan, Hannah, Romain, Uros, Nicole, Shannon,

Proposed agenda:

1. Agenda bash
2. Discuss Sirtfi+ Registry requirements in light of Niels' presentation last time and subsequent list traffic. Do we have consensus on a path forward?
    a. Reference: Sirtfi+ Registry requirements
3. WG plan of action: first settle Sirtfi+ registry path forward, then focus on "Federated Security Incident Response Procedure" paper.
4. Else?

The WG appeared to reach consensus on the general outline of the Sirtfi+ Registry. It is operated to address issues with site operators being able to express Sirtfi metadata elements in their federation metadata by means of their parent R&E federation. The general idea follows Niels' "pixie dust" model and borrows from that term.

Sketch of the Sirtfi+ Registry

1. It is an SP in eduGain.
2. It ingests and validates the eduGain aggregate. Only entities in this aggregate will be operated upon by the Sirtfi+ Registry.
3. A governance mechanism maintains a group of "trustees" who can "endorse" a "duster" for a given entity.
4. Trustees interact with the Sirtfi+ Registry to maintain a list of (federated user, entity) pairs that express who is endorsed as a "duster" to supply authoritative Sirtfi attestation for which entities.
5. A federated user who is endorsed as a duster for a given entity may supply attestations of Sirtfi compliance and security contact for that entity. They can attest either to Sirtfi compliance (including security contact) or to lack of Sirtfi compliance for the entity. Each attestation replaces any previous one for that entity.
6. Periodically (once or several times per day?) eduGain entities referenced in endorsed attestations that assert Sirtfi compliance are reviewed to determine which have Sirtfi metadata elements. For those that do not, the endorsed attested Sirtfi metadata is added to the original entity metadata and the result is added to a Sirtfi+ Registry entity aggregate. The aggregate is signed using a well-known key.
7. Relying parties download the Sirtfi+ Registry metadata aggregate and ingest it along with eduGain or other metadata, with the purpose of using the Sirtfi+ Registry form of an entity's metadata over any others, or otherwise as local policy may determine.

There were a few other points of discussion:

- The Sirtfi+ Registry signing key could be established at a signing ceremony, e.g. at a TNC meeting, or it could be supplied by eduGAIN, constituting another form of endorsement.
- The governance mechanism in #3 and the policy that it implements need to be carefully thought through. Should trustees be considered solely as individuals, or should some organizations or projects be entitled to identify one or more trustees? Exactly how this bootstrapping of trust in the registry should be maintained is interesting.
- Once there is a Sirtfi+ Registry, the WG may wish to layer on additional operations, e.g. to assign points to entities based on some assessment or endorsement scheme. We decided to postpone thinking through supporting details until after we get the basic platform specified.
- The Registry will only operate on entities from federations that do not (yet) support Sirtfi self-attestation. When an entity begins to get its Sirtfi stuff through its native federation, the Sirtfi+ Registry will no longer touch it.