Sirtfi+ Registry

High Level Requirements Specification for Prospective Operators and Developers

Motivation

Not all federations have the same resources and capabilities, and that is not expected to change on time scales needed by certain SP communities.The R&E Federation community needs to move away from the notion that there can only be one source of truth, and one path to trust, for all assertions embodied in federation metadata. Communities of Practice or other Sources of Authority for specific assertions should not necessarily have that operational constraint imposed on their ability to use global federation infrastructure for their own benefit.

One step in that movement is to provide members of a Federation that is not yet ready to support Sirtfi with an alternative means to manage their Sirtfi attestations, until such time as the Federation is prepared to do so natively. The Sirtfi+ Registry described here provides that function.

~~A "Sirtfi attestation" signals a commitment by one organisation to collaborate with others in a joint activity in a manner that adheres to certain minimal standards. Since such joint activities can be put at risk if one collaborator fails to uphold those standards, the Sirtfi+ Registry also provides a means for certain trusted parties to override the Sirtfi attestation asserted by an organisation about its own entities.~~

~~Thus, eduGAIN metadata as enhanced by the Sirtfi+ Registry provides federated entities with the most comprehensive source of Sirtfi information.~~

Glossary

Term	**Description**
Sirtfi	The Security Incident Response Trust Framework for Federated Identity https://refeds.org/sirtfi .
Entity	A federated entity, such as an SP or an IdP, whose metadata is authoritatively managed via an eduGAIN-connected Federation.
Sirtfi+ Registry	The proposed tool for making Sirtfi attestations about entities unable

	to do so through their own Federation.
Duster	A user of the Sirtfi+ Registry who is authorised to make or remove a Sirtfi attestation about an entity. A Duster for an entity can only be someone who is reached through that entity's registered contacts.

Functional Requirements

1. The Sirtfi+ Registry is an SP in eduGAIN.
2. It ingests and validates the eduGAIN aggregate. Only entities in this aggregate may be operated upon by the Sirtfi+ Registry.
3. An out of band mechanism is used to identify those federations whose members are to be permitted to use the Sirtfi+ Registry for purpose of managing their Sirtfi self-attestations. We'll refer to those as "Sirtfi+ federations" below.
4. A federated user who has authority over a given entity in a Sirtfi+ federation can be self-authorised as a Duster for that entity by requesting the Sirtfi+ Registry to send a validation email to one of the entity's contact addresses in its eduGAIN metadata and successfully completing the email verification loop.
5. A Duster for a given entity in a Sirtfi+ federation 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 positive or negative attestation replaces any previous one in the Sirtfi+ Registry for that entity.
6. Periodically (once or several times per day?) eduGAIN entities in Sirtfi+ federations referenced in positive attestations of Sirtfi compliance are reviewed to determine whether their Sirtfi metadata elements correctly reflect their standing in the Sirtfi+ Registry. For those that do not, the attested Sirtfi metadata is added to the original entity metadata and the result is added to a Sirtfi+ Registry metadata aggregate. eduGAIN entities that include the Sirtfi tag and security contact info are also copied untouched to the Sirtfi+ Registry metadata aggregate, so that this aggregate contains all Sirtfi-compliant entities regardless of origin. The aggregate is signed using a well-known key minted specifically for the Sirtfi+ Registry.
    a. Authenticated entity metadata is provided in accordance with common federation practices, e.g. publish a signed metadata aggregate and/or support MDQ.
    b. The SAML mdrpi:PublicationInfo, mdrpi:PublicationPath, and mdrpi:Publication extension elements should be updated for entities having Sirtfi material added to them.
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.
8. A publically accessible view of Duster attestations is maintained as a transparency measure.
9. All logins to the Sirtfi+ Registry are via federation, relying on users' home organisations or other IdPs in eduGAIN. There are no local accounts for users.

Note that as a consequence of #3 and #7, when an entity begins to get its Sirtfi metadata elements through its home federation, the Sirtfi+ Registry will no longer touch its metadata.

Other Considerations

- The Sirtfi+ Registry operator must be approved by the REFEDS Sirtfi Working Group.
- 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.
- Once there is a Sirtfi+ Registry, the Sirtfi WG may wish to layer on additional operations following further requirements gathering activities. Potential features include:
    - Suspension of entities or tags in the published metadata feed due to security concerns
    - Extension to other frameworks, including peer-assessed frameworks
    - Community cross-vetting of tags

User perspective

This use case illustrates how a Duster interacts with the Sirtfi+ Registry.

Use Case 1: An administrator for entity X, which may be either an IdP or an SP, self-asserts Sirtfi compliance through the Sirtfi+ Registry.

1. The administrator logs into the Sirtfi+ Registry using any IdP in eduGAIN at which which they have an account.
2. The administrator requests an email loop authorisation to act as a Duster for entity X.
3. The Sirtfi+ Registry determines whether entity X belongs to a Sirtfi+ federation. If so, it sends an email loop verification message to the Technical Contact for entity X as shown in eduGAIN metadata. If not, it gives a suitable error message to the administrator.

4. The administrator receives the email loop verification message at the Technical Contact address and follows its instructions to complete the verification.
5. The Sirtfi+ Registry creates an authorisation record showing self-authorisation of the administrator as Duster for entity X and sends a confirmation message to the Technical Contact.
6. The administrator receives the confirmation message and so knows that the Sirtfi+ Registry will now let them act as a Duster for entity X.
7. The administrator logs into the Sirtfi+ Registry using their home organisation credential and submits a positive Sirtfi attestation and security contact for entity X.
8. The Sirtfi+ Registry includes the Sirtfi assurance profile and security contact for entity X the next time eduGAIN metadata is reviewed, and publishes the information.
9. Interested parties who subscribe to the Sirtfi+ Registry metadata feed are able to see the Sirtfi assurance profile and security contact for entity X.