Guide for Federation Operators

This page aims to guide Federation Operators in supporting the adoption of the Sirtfi Framework.

Coordinating Adoption

During the process of Sirtfi adoption, federation operators should anticipate providing support to entities. An FAQ maintained by the Sirtfi working group is available to help you.

The Sirtfi Framework does not itself entitle federation operators to limit which of their entities may self-attest to Sirtfi compliance, although Sirtfi also does not place any constraint on policies that each federation chooses to adopt.

Please reach out to your REFEDS contacts should you, as a federation operator, require assistance. If you have no active members within REFEDS, contact us via contact@refeds.org and ask for the Sirtfi Working Group.

Sirtfi Contact Choice

Your federation may wish to provide specific guidance on the choice of Sirtfi Contact. For more information, visit Choosing a Sirtfi Contact.

Should your federation already provide centralised federated security incident response, you may choose to leverage this existing capability.

Metadata Extensions

How should your federation participants add the two required extensions to their metadata? The Guide for Federation Participants describes the two extensions in further detail.

Be sure to communicate how an entity should assert their compliance and add their Sirtfi contact. Usually, federations choose to manage such metadata extensions centrally and act as the registrar. They would simply request the Sirtfi contact details from an entity via email.

Sirtfi and Sirtfi v2

Both original Sirtfi (v1) and Sirtfi v2 will remain supported for the indefinite future. There is no plan to deprecate v1 with the introduction of v2. See Coexistence of Sirtfi v1 and v2 for details. Best practice is to encourage adoption of Sirtfi v2 by your members but to support those members who wish to remain at v1. For reference: Sirtfi v1 specification and Sirtfi v2 specification

Sample Outreach Letter for Federation Participants

Sample outreach letters have been provided below to assist with communication to your federation. Many thanks to Incommon and REN-ISAAC for their input.

Sample Outreach Letter 1

Dear Federation Members,

<THIS FEDERATION>, alongside international partners, strongly urge federation participants to be ready to manage federation-related security incidents. Here's how.

Sirtfi [1] is an international framework for federated security incident response. It specifies a means to publish your readiness for incident response in federation metadata. This framework asks that each federation entity, ie, Identity and Service Providers, contain security contact information in its federation metadata; that normal security incident response procedures associated with it reasonably address the statements in the Sirtfi specification; and if so, that a Sirtfi tag is attached to the entity.

<THIS FEDERATION> recently made self-management of the security contact and Sirtfi flag available. Participant Site Administrators can now manage Sirtfi status for all systems that are part of the Federation. Please ask them to ensure that your security contact information is correctly expressed in federation metadata and to set the Sirtfi flag if you believe that your security incident response procedures reasonably meet the statements in the Sirtfi specification.

Academic collaborations, cloud services, and other uses depend on sensitive resources, such as unique instruments, software, high performance data processing environments, and corpi of data, being accessible through global federation. Most <THIS FEDERATION> participants are home to faculty, students, and staff that need to use these services to be successful in their endeavours. Please help them to succeed by being prepared to manage a federated security incident that could otherwise threaten valuable resources.

[1] https://refeds.org/sirtfi

Sample Outreach Letter 2

We invite you to join the Security Incident Response Trust Framework for Federated Identity, Sirtfi.

To improve security within <THIS FEDERATION>, and across eduGAIN, a trust framework has been defined that addresses concerns over operational security and incident response. By becoming Sirtfi compliant, your organisation will raise its level of assurance; Sirtfi creates an improved level of trust between federation participants resulting in increased collaboration between federated entities.

To find out more about Sirtfi, visit the homepage at https://refeds.org/sirtfi

To become Sirtfi compliant, refer to the Sirtfi Technical Wiki at https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home

We recommend choosing <guidance on Sirtfi contact choice> as your Sirtfi contact.

Two metadata extensions are required to become Sirtfi compliant, <we will manage these changes centrally||these should be added to your organisation's metadata directly>

<ANY OTHER INFORMATION>

Regards,

Entity Attributes Filtering

The assertion of Sirtfi compliance for a Relying Party is expressed in metadata with the use of an Entity Attribute [1] as described in the OASIS documentation for asserting compliance with assurance profiles [2]. The validation strategy for local federation entity metadata might need to be reconsidered in order to allow local Entities to assert Sirtfi compliance. Additionally, if a federation has a filtering procedure in place while republishing eduGAIN metadata, federator operators need to ensure that their filtering strategy is adapted in order to facilitate the use of Sirtfi.

Two additions are necessary in the metadata of an entity asserting Sirtfi compliance so federation operators should focus on whitelisting/allowing the following :

Assurance-certification Entity Attribute

Sirtfi compliance is expressed with the use of the Entity Attribute "urn:oasis:names:tc:SAML:attribute:assurance-certification" holding the values of https://refeds.org/sirtfi and https://refeds.org/sirtfi2 (if SirtfiV2 is met) in an entity's metadata as seen below:

Sirtfi entity attribute

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...>
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
        <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
        <saml:AttributeValue>https://refeds.org/sirtfi2</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
</md:EntityDescriptor>
```

Security Contact

A security contact element is added in every Entity that asserts Sirtfi compliance as seen below:

REFEDS security contact

REFEDS security contact

```
<md:ContactPerson xmlns:remd="http://refeds.org/metadata"
    contactType="other"
        remd:contactType="http://refeds.org/metadata/contactType/security">
  <md:GivenName>Security Response Team</md:GivenName>
  <md:EmailAddress>mailto:security@xxxxxxxxxxxxxxx</md:EmailAddress>
</md:ContactPerson>
```

Multiple EmailAddress tags may be defined should an organisation wish to add both a generic email address and an individual.

This contactType has been defined within the REFEDS XSD Metadata Extension Schema.

[1] http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html

[2] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf