Guide for Federation Participants

Step by Step Guide for asserting Sirtfi compliance

The following section contains a simple recipe that can be used by Identity Providers and Service Providers to assert Sirtfi compliance.

Step 1: Self Assessment

Complete a self assessment of your organisation following the Sirtfi Framework

If you are able to agree with each and every statement included in the framework, your organisation is Sirtfi compliant. To assert this compliance, two extensions must be added to your SP/IdP's federation metadata.

Your local federation may manage all metadata extensions centrally. In this case, ask your federation operator to perform the following steps.

> ⚠ If your federation operator is not aware of Sirtfi, refer them to the Sirtfi Homepage

Step 2: Add Security Contact Details

Add relevant security contact details to your entity metadata, following the established process of your local federation on updating metadata. Consult the guide on Choosing a Sirtfi Contact for recommendations on the most appropriate contact point for your entity.

An example of a ContactPerson element can be seen below:

REFEDS security contact

```
<md:ContactPerson xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
      contactType="other"
      remd:contactType="http://refeds.org/metadata/contactType/security"
      xmlns:remd="http://refeds.org/metadata">
  <md:GivenName>Security Response Team</md:GivenName>
  <md:EmailAddress>mailto:security@xxxxxxxxxxxxxxx</md:EmailAddress>
</md:ContactPerson>
```

Refer to the REFEDS Standards and Specification Wiki for full details: Security Contact Metadata Extension Schema

Step 3: Assert Sirtfi Compliance

Express the Sirtfi compliance assertion in your metadata by adding the EntityAttribute “urn:oasis:names:tc:SAML:attribute:assurance-certification” with the value https://refeds.org/sirtfi, following the established process of your local federation on updating metadata.

An example Sirtfi Entity Attribute is shown 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:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
</md:EntityDescriptor>
```

Refer to the OASIS Identity Assurance Profiles Specification for full details: OASIS Specification

Step 4: Use Sirtfi

Now that you're Sirtfi compliant, what does it mean?

- If you're an SP, you may wish to restrict authentication to only those IdPs who are also trusted. See this page Sirtfi Metadata Aggregates to get started
- In the event of an incident involving a federated entity or user, contact the relevant security contact listed in metadata

- If you are contacted for help in an external incident, you are obliged to respond and actively collaborate with other Sirtfi compliant entities