Guide for Federation Participants

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 v2 compliance. NB: Sirtfi v2 compliance implies compliance with the original Sirtfi (v1).

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 entity metadata in the federation.

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

```
<ContactPerson xmlns:remd="http://refeds.org/metadata"
        contactType="other"
        remd:contactType="http://refeds.org/metadata/contactType/security">
<GivenName>Security Response Team</GivenName>
<EmailAddress>mailto:security@xxxxxxxxxxxxxxx</EmailAddress>
</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 values “https://refeds.org/sirtfi” and “https://refeds.org/sirtfi2” following the established process of your local federation on updating metadata.

An example Sirtfi Entity Attribute is shown below:

Sirtfi entity attribute

```
<EntityDescriptor ...>
<Extensions>
<attr:EntityAttributes>
...
<saml:Attribute 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/sirtfi2
</saml:AttributeValue>
<saml:AttributeValue>https://refeds.org/sirtfi
</saml:AttributeValue>
</saml:Attribute>
...
</attr:EntityAttributes>
</Extensions>
...
</EntityDescriptor>
```

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

Step 4: Use Sirtfi

Now that you're Sirtfi v2 compliant, what does it mean?

- If you are contacted for help with an external incident, you are obliged to respond and actively collaborate with other Sirtfi compliant entities on a best effort basis
- You must notify other parties impacted by an incident as you become aware of it and also follow any applicable procedures of any federations to which your organisation belongs
- In the event of an incident involving a federated entity or user, contact the relevant security contact listed in metadata (see How To Look Up Security Contacts for details on how to do this)
- The eduGAIN Security Incident Response Handbook is available to supplement your established incident response procedures