Sirtfi Identity Assurance Certification Description

Sirtfi WG Comments Welcome August 16th - August 23rd
REFEDS-wide Comments Welcome August 24th - September 14th
Consultation ~ September 16th

Overview

Research and Education Federations are invited to use Sirtfi (the Security Incident Response Trust Framework for Federated Identity) with their members to facilitate incident response collaboration.

Sirtfi adherence is registered in an entity's metadata as a SAML Identity Assurance Certification Entity Attribute and a REFEDS Security Contact. An implementation guide has been made available [GUIDE].

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]. This definition is written in compliance with the REFEDS Security Contact Metadata Schema Extension [CONTACT] and OASIS Identity Assurance Certification [OASIS].

An FAQ for Sirtfi has been made available to support deployment [FAQ].

Definition

Any federated entity, including, but not limited to, Identity Providers, Service Providers, and Attribute Authorities, is a potential candidate for Sirtfi membership. To be declared Sirtfi compliant, an entity MUST support every assertion in the published framework, Sirtfi v1.0 [SIRTFI]. A registrar SHOULD add the assurance entity attribute to the relevant entity descriptor when the party that operates the entity declares compliance with the assertions of the Sirtfi framework. A registrar MAY also do this on behalf of the party that operates the entity without their explicit request, but only when the registrar has specific knowledge that the party is already subject to policy that encompasses the Sirtfi framework.

To support federated incident response, a security contact MUST be added to an entity's metadata in conjunction with the entity attribute declaration. A security contact from outside the entity's organisation MAY be used.

Syntax

The following URI is used as the attribute value for the Identity Assurance Certification Entity Attribute: https://refeds.org/sirtfi

The presence of the Sirtfi Identity Assurance Certification Entity Attribute (herein the Sirtfi Attribute) indicates that an entity claims to support the assertions of Sirtfi v1.0 [SIRTFI]. The Sirtfi Assurance Entity Attribute value is the sole indicator of Sirtfi support. The Sirtfi Attribute MUST NOT be applied to an entity unless that entity is known to conform to the Sirtfi framework, via self-assertion or adherence to an equally or more restrictive policy. Other semantics SHOULD NOT be inferred from the absence or presence of the Sirtfi Attribute. This constitutes an extension of the OASIS SAML V2.0 Identity Assurance Profiles, Version 1.0 [OASIS], which was scoped to describe use of the attribute by Identity Providers only.

Registration Criteria

Before an entity's registrar adds the Sirtfi Attribute to that entity's metadata, the registrar MUST perform the following checks:

- The entity claims to have passed a self-assessment of Sirtfi v1.0 [SIRTFI] or is known to be subject to a policy that encompasses all the requirements of the Sirtfi framework.
- A security contact has been provided for the entity, and this contact is published in the entity's metadata in accordance with the REFEDS Security Contact Metadata Schema Extension [CONTACT]

Self-Assessment

To complete a self-assessment, entities MUST assess their own systems and processes to determine whether they can support every assertion of the normative document, Sirtfi v1.0 [SIRTFI]. If so, they MAY approach their registrar for membership. No external peer review is required.

Removal Criteria

If an entity can no longer comply with the assertions listed in the normative Sirtfi document v1.0 [SIRTFI], the entity MUST remove the Sirtfi entity attribute from its entity descriptor, or request its registrar do so on its behalf. The registrar SHOULD consider the Sirtfi Attribute in scope of any of their policies that regulate the validity of published metadata.

Periodic Renewal

Sirtfi v1.0 describes a baseline of best practices in security. It is expected that once an entity is Sirtfi compliant, they will remain so. As such, registrars are not required to implement periodic renewal from their participants.

Security Contact

The entity, or party providing Incident Response support on behalf of the entity, MUST:

- Provide a security contact [CONTACT] containing:
  - Name, included as a GivenName element (this MAY be the name of a service function, such as “Security Operations”)
  - Email, included as an EmailAddress element
  - OPTIONAL additional fields from the SAML Standard for contactPerson [SCHEMA]
- Ensure that communication sent to the security contact is not publicly archived.

The registrar MAY:

- Perform, or facilitate, an annual check for responsiveness of the security contact

The security contact MUST:

- Abide by the Sirtfi normative assertions IR2 to IR6 of the normative Sirtfi document v1.0 [SIRTFI], on behalf of the entity

All parties involved in Federated Incident Response MAY use the security contact to:

- Initiate security incident response collaboration as outlined in the Sirtfi framework [SIRTFI]
- Investigate failure to comply with assertions listed in the normative Sirtfi document v1.0 [SIRTFI]

Examples

Example Security Contact

```
<ContactPerson xmlns:remd="http://refeds.org/metadata"
              contactType="other"

remd:contactType="http://refeds.org/metadata/contactTyp
e/security">
  <GivenName>Security Response Team</GivenName>

<EmailAddress>mailto:security@xxxxxxxxxxxxxxx</EmailAdd
ress>
</ContactPerson>
```

Example Assurance Certification

```
<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/sirtfi
               </saml:AttributeValue>
            </saml:Attribute>
            ...
      </attr:EntityAttributes>
   </Extensions>
...
</EntityDescriptor>
```

References

[EntityCatTypes] Young, I, Johansson, L, and Cantor, S Ed., “The Entity Category SAML Attribute Types”, July 2014.

[GUIDE] “Sirtfi Home”, March 2016 https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home

[SIRTFI] T. Barton et al, December 2015 https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf.

[FAQ] “Sirtfi FAQs”, March 2016, https://refeds.org/sirtfi/sirtfi-faqs

[CONTACT] "Security Contact Metadata Extension Schema, https://wiki.refeds.org/display/STAN/Security+Contact+Metadata+Extension+Schema

[OASIS] SAML V2.0 Identity Assurance Profiles Version 1.0, https://wiki.oasis-open.org/security/SAML2IDAssuranceProfile

[EDUGAIN] http://services.geant.net/edugain/Pages/Home.aspx

[SCHEMA] http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf