DRAFT

A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

Version 2

Abstract

This document identifies practises and attributes of organisations that may facilitate their participation in a trust framework called Sirtfi whose purpose is to enable coordination of security incident response across federated organisations.

Audience

This document is intended for use by the personnel responsible for operational security of federated entities such as Identity Providers, Service Providers and Attribute Authorities, and by Federation Operators who may facilitate its adoption by their member organisations.

Other Sources / Attribution / Acknowledgements: An earlier version of this work, “A Security Incident Response Trust Framework for Federated Identity (Sirtfi)”, is a derivative of “A Trust Framework for Security Collaboration Among Infrastructures” by D. Kelsey, K. Chadwick, I. Gaines, D. Groep, U. Kaila, C. Kanellopoulos, J. Marsteller, R. Niederberger, V. Ribaillier, R. Wartel, W. Weisz and J. Wolfrat, used under CC BY-NC-SA 4.0.

Introduction

This section is informative.

Trust federations, which provide foundation services that enable authentication and authorisation systems to extend across organisational boundaries, are operated within many nations in support of their Research and Education (R&E) sectors and others. This capability allows Service Provider (SP) organisations to extend access rights to their resources to users whose credentials are managed by Identity Provider (IdP) organisations. Thousands of organisations around the world trust R&E federations with the operation of these foundation services, and their number continues to grow.

While extremely valuable for large scale collaboration that is a characteristic of R&E activities, this approach also exposes a new vector of attack on SP resources. Since one user credential may have access to SPs at multiple organisations, federation presents a way to leverage a compromise at one organisation into an attack on others. The global scale of the overall federated access management system also poses a new challenge to the ability to respond to security incidents. How can one organisation know how, or even whether, to contact another to coordinate response to a security incident, and why should they trust each other in doing so?

Sirtfi is a means to enable a coordinated response to a security incident in a federated context that does not depend on a centralised authority or governance structure to assign roles and responsibilities for doing so. Its intent is threefold:

1. Enable communication and coordination in managing federated security incidents.
2. A reasonable collection of pertinent event data is available to help collaborating incident responders.
3. At least minimal security protections are applied to information systems that directly handle federated transactions.

The Normative Assertions for Federated Entity Operators section below defines a set of criteria that support these objectives to which an organisation operating a federated entity self-attests their conformance. This self-attestation is recorded in the federation metadata of associated entities, as specified below in the section entitled Sirtfi v2 Identity Assurance Certification Description for Federation Operators, enabling other parties to make contact in connection with a federated security incident, and to signal that basic security of those federated entities is attended to by their operators.

Members of the R&E community have a long-standing tradition of strong international collaboration, and R&E federations embody trust as their main value. Federated entities trust each other based on the policies and procedures of R&E federations and of their member organisations. Sirtfi defines a way to extend that fabric of trust to the management of federated security incidents. It does not require any form of external audit or review to support a self-attestation of conformance.

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

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].

Normative Assertions for Federated Entity Operators

This section is normative.

In this section we define a set of assertions that each organisation shall self-attest to so that they may participate in Sirtfi. These are divided into four areas: operational security, incident response, traceability and user rules and conditions.

An attestation to the assertions in this document refers specifically and only to the statements in this section that are identified by labels within square brackets "[", "]".

How thoroughly each asserted capability should be implemented across the organisation's information system assets, either directly by the organisation or by third parties responsible for their operation, is not specified. Care should be focused on information system elements that directly handle federated transactions; however, the investment in mitigating a risk should be commensurate with the degree of its potential impact and the likelihood of its occurrence, and this determination can only be made within each organisation.

Operational Security [OS]

Managing access to information resources, maintaining their availability and integrity, and maintaining confidentiality of sensitive information is the goal of operational security.

- [OS1] Security patches in operating system and application software are applied in a timely manner.
- [OS2] A process is used to manage vulnerabilities–in software operated by the organisation.
- [OS3] Means are implemented to detect and act on possible intrusions using threat intelligence information in a timely manner.
- [OS4] A user's access rights can be suspended, modified or terminated in a timely manner.
- [OS5] Users and Service Owners (as defined by ITIL) within the organisation can be contacted.
- [OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

Incident Response [IR]

Assertion [OS6] above posits that a security incident response capability exists within the organisation. This section's assertions describe its interactions with other organisations participating in Sirtfi. They are intended to augment but not supersede local procedures when an incident may extend beyond the organisation.

Communications with other federation members may be conducted in English or may be conducted in another language as appropriate to those members.

- [IR1] Provide security incident response contact information as may be requested by any federation to which your organisation belongs.
- [IR2] Respond to requests for assistance with a security incident from other organisations participating in Sirtfi in a timely manner.
- [IR3] Notify security contacts of entities participating in Sirtfi when a security incident investigation suggests that those entities are involved in the incident. Notification should also follow the security procedures of any federations to which your organisation belongs.

- [IR4] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in Sirtfi.
- [IR5] Respect user privacy as determined by the organisation's policies or legal counsel.
- [IR6] Respect the Traffic Light Protocol [TLP] information disclosure policy and use it during incident response communications with federation participants.

Traceability [TR]

To be able to answer the basic questions "who, what, where, and when" concerning a security incident requires retaining relevant system generated information, including accurate timestamps and identifiers of system components and actors, for a period of time.

- [TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.
- [TR2] Information attested to in [TR1] is retained in conformance with the organisation’s security incident response policy or practices.

User Rules and Conditions [UR]

Identity Providers and Service Providers (participants) have a responsibility to notify users that their access may be controlled following unauthorised use, such as during a security incident. The definition of authorised use may be communicated to the user via an Acceptable Usage policy, terms and conditions, contract or other agreement. This may be done directly between the participant and the user, or between a third party and the user in the case that operation of a system has been delegated.

- [UR1] The participant has defined rules and conditions of use.
- [UR2] There is a process to notify all users of these rules and conditions of use.

Sirtfi Identity Assurance Certification Description for Federation Operators

This section is informative.

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].

This definition is written in compliance with the REFEDS Security Contact Metadata Schema Extension [CONTACT] and OASIS Identity Assurance Certification [OASIS].

Definition

This section is normative.

Any federated entity is a potential candidate for Sirtfi certification. To be declared Sirtfi compliant, an entity MUST support every assertion in the Normative Assertions for Federated Entity Operators section above (herein the Sirtfi v2 Assertions). A registrar SHOULD add the assurance entity attribute defined below to the relevant entity descriptor when the party that operates the entity declares compliance with the Sirtfi v2 Assertions. 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 v2 Assertions.

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

This section is normative.

The following URI is used as the attribute value for the Sirtfi (v2) Identity Assurance Certification Entity Attribute (herein the Sirtfi v2 Attribute): https://refeds.org/sirtfi2

The following URI continues to be used as the attribute value for the original Sirtfi (v1) Identity Assurance Certification Entity Attribute (herein the Sirtfi v1 Attribute): https://refeds.org/sirtfi

The presence of the Sirtfi v2 Attribute indicates that an entity claims to support the Sirtfi v2 Assertions. The Sirtfi v2 Attribute MUST NOT be applied to an entity unless that entity is known to conform to the Sirtfi v2 Assertions, via self-assertion or adherence to an equally or more restrictive policy. 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.

Because compliance with Sirtfi v2 Assertions implies compliance with the assertions of Sirtfi v1 [SIRTFIv1], an entity's registrar SHALL ensure that the Sirtfi v1 Attribute is also included in the entity's metadata when the Sirtfi v2 Attribute is present.

The presence of the Sirtfi v1 Attribute indicates that an entity claims to support the Sirtfi v1 assertions. The Sirtfi v1 Attribute MUST NOT be applied to an entity unless that entity is known

to conform to the Sirtfi v1 assertions, 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 v1 Attribute.

Registration Criteria

This section is normative.

Before an entity's registrar adds the Sirtfi v2 Attribute to that entity's metadata, the registrar MUST perform the following checks:

- The entity claims to have passed a self-assessment of the Sirtfi v2 Assertions or is known to be subject to a policy that encompasses all the requirements of the Sirtfi v2 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]

Before an entity's registrar adds the Sirtfi v1 Attribute to that entity's metadata, the registrar MUST perform the following checks:

- The entity claims to have passed a self-assessment of the Sirtfi v1 Assertions or is known to be subject to a policy that encompasses all the requirements of the Sirtfi v1 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]

Removal Criteria

This section is normative.

If an entity can no longer comply with the Sirtfi v2 Assertions, the Sirtfi v2 Attribute MUST be removed from its entity descriptor. The registrar SHOULD consider the Sirtfi v2 Attribute in scope of any of their policies that regulate the validity of published metadata.

If an entity can no longer comply with the Sirtfi v1 Assertions, the Sirtfi v1 Attribute MUST be removed from its entity descriptor. In this case, the Sirtfi v2 Attribute, if present in the entity descriptor, MUST also be removed. The registrar SHOULD consider the Sirtfi v1 Attribute in scope of any of their policies that regulate the validity of published metadata.

Periodic Renewal

This section is normative.

Sirtfi 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

This section is normative.

The entity operator, 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.
- If the entity removes the security contact [CONTACT] from metadata, it MUST also remove the corresponding Sirtfi Attribute

The registrar MAY perform, or facilitate, a periodic check for responsiveness of the security contact.

Examples

This section is informative.

Example Security Contact (as per [CONTACT]):

```
<ContactPerson xmlns:remd="https://refeds.org/metadata"
   contactType="other"
   remd:contactType="http://refeds.org/metadata/contactType/security">
<GivenName>Security Response Team</GivenName>
<EmailAddress>mailto:security@xxxxxxxxxxxxxxx</EmailAddress>
</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/sirtfi2
      </saml:AttributeValue>
      <saml:AttributeValue>https://refeds.org/sirtfi
      </saml:AttributeValue>
   </saml:Attribute>
   …
   </attr:EntityAttributes>
</Extensions>
...
</EntityDescriptor>
```

References

[RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, https://datatracker.ietf.org/doc/html/rfc2119

[CONTACT] "Security Contact Metadata Extension Schema”, https://refeds.org/metadata/contactType/security.

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

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

[ITIL] Axelos ITIL Glossary of Terms, https://www.axelos.com/glossaries-of-terms

[OASIS] SAML V2.0 Identity Assurance Profiles Version 1.0: https://wiki.oasisopen.org/security/SAML2IDAssuranceProfile.

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

[SIRTFIv1] “A Security Incident Response Trust Framework for Federated Identity (Sirtfi)”, https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

[TLP] Traffic Light Protocol, https://www.first.org/tlp/