FAQs

Frequently Asked Questions

This list of Frequently Asked Questions is provided to complement the information contained in the Sirtfi Trust Framework Document.

General Questions

Q: What are the benefits of the Sirtfi trust framework?

A: By expressing compliance with Sirtfi, your organisation can increase the level of trust it holds within the community. By improving this trust, other organisations will be more likely to grant access or permit authentication. The key benefit of becoming Sirtfi compliant is the ability to collaborate effectively with other Sirtfi compliant organisations, in the event of a federated security incident. See Why Sirtfi for additional benefits.

1. How do I participate?

A: Details can be found in the Guide for Federation Participants in the Sirtfi Technical Wiki.

Q: Which types of federated entities are encouraged to join?

A: All types. Sirtfi compliance signals that an entity supports a baseline of operational security and is able and willing to collaborate in incident response. Any participant within the framework may initiate incident response, or respond to a call for assistance with responding to an incident. For incident response to be successful in a federated environment, all entities should participate.

1. What changes must I make to our existing security practises to comply with Sirtfi?

Sirtfi sets a low bar for the level of operational security needed to comply; it primarily serves to develop the trust relationships needed for inter-organisational incident response rather than to strengthen an organisation's existing cyber security practices. It is expected that most organisations are able to comply with Sirtfi quickly and easily. The precise measures and changes required at an organisation to become Sirtfi compliant, if any, are left to the determination of the organisation itself.

1. I currently comply with Sirtfi v1. What more must I do for Sirtfi v2?
2. This question is answered in the Coexistence of Sirtfi v1 and Sirtfi v2 document.

Q: Must all of my systems satisfy the Sirtfi requirements in order for my organisation to assert Sirtfi compliance?

A: No. As discussed in the Sirtfi trust framework: "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".

Q: Can one organisation assert Sirtfi compliance for another organisation's entity?

A: Yes, providing certain conditions are met. An organisation may assert Sirtfi on behalf of a separate entity, such as the hub of a hub-and-spoke federation on behalf of its members, providing that existing policies between the parties are equal to or more restrictive than Sirtfi. Similarly, a security contact for an entity may be provided at a separate organisation, provided that they will abide by Sirtfi requirements on behalf of the entity.

Q: Who can I ask for help?

A: Your Federation Operator will be able to guide you or, if required, redirect you to appropriate individuals within REFEDS.

1. What can I do if my incident response message, sent to a Sirtfi compliant entity's security contact and properly marked using the Traffic Light Protocol, is not responded to in a timely manner?

A: You can send a message to other contacts listed for the entity to ask their help to elicit a response, although you should not send the original message to them if its TLP level precludes sharing the information outside of the intended security contact. Also, you can ask their Federation Operator to try to elicit a response using their contacts with the organisation. This will also help them to be aware of behaviour of one of their members that is potentially non-compliant. If an organisation can no longer comply, they must stop asserting their compliance with the Sirtfi trust framework.

Q: Are there any requirements for data protection?

A: No data protection requirements are stipulated within the Sirtfi trust framework beyond use of the Traffic Light Protocol. Each organisation should analyse their own regulatory obligations and risk profile in terms of personal data and take corresponding precautions.

Q: Are there any requirements for the assurance of users' identities? For example, is there a security requirement for all accounts to be linked to identifiable individuals?

A: No. Sirtfi is a trust framework for security incident response. Other trust frameworks, such as the REFEDS Assurance Framework, address identity and authentication assurance, attributes, or other aspects of achieving overall trust in federated transactions.

Q: I am a federation operator, where can I find further information to support Sirtfi adoption within my federation?

A: Details can be found in the Guide for Federation Operators in the Sirtfi Technical Wiki.

Q: Who should I choose as my Sirtfi security contact?

A: See Choosing a Sirtfi Contact in the Sirtfi Technical Wiki.

Q: How is Sirtfi compliance assessed?

A: Entities are encouraged to complete a self-assessment of their organisation against the requirements of the Sirtfi trust framework. There is no requirement for external review. A successful self-assessment is sufficient for an organisation to be able to assert the Sirtfi assurance entity attribute in their entity's metadata.

1. I'm a Federation Operator. Can I limit which of my registered entities are permitted to assert Sirtfi?
2. Sirtfi does not specify how a federation operator may choose to operate, apart from specifying the syntactical requirements of expressing Sirtfi in entity metadata.

Q: Can I assert Sirtfi if I am running a proxy?

A: Yes, although each assertion in the trust framework must be considered in the specific context of your proxy. For example, a group of Service Providers may be accessed through a single Service Provider Proxy that is registered in an identity federation. [TR1] requires logs to be kept to enable traceability, so a Service Provider Proxy should ensure that downstream services are recording such logs. Similarly, an IdP Proxy may issue authentication and attribute assertions that have originated from multiple other Identity Providers. [OS5] requires that users can be contacted, so if an Identity Provider Proxy implements some means to do so then it is able to satisfy the requirement.

Some research infrastructures have adopted Snctfi, which defines a policy framework that allows determination of the "interoperable trust" between an SP Proxy and the community of services behind the Proxy. Snctfi was designed to enable the Proxy to assert Sirtfi compliance on behalf of the research infrastructure it proxies.

Questions on Sirtfi Assertions

The following refer to the Sirtfi v2 wordings and numberings. If your question relates to a v1 criterion, please refer to the answer located in the corresponding v2 area below.

Operational Security [OS]

[OS1] Security patches in operating systems and application software are applied in a timely manner.

Q: *Does this imply that only supported software, for which patches are actively supplied, should be used?*

A: *Yes, though the support may come from any qualified source, such as an open source community, a software vendor, or your own organisation. [OS1] does not imply that only commercial software be used; however, [OS2] implies that any software deployed by an organisation, custom or otherwise, must be actively maintained in the event that a vulnerability is identified.*

[OS2] A process is used to manage vulnerabilities in software operated by the organisation.

Q: *What does [OS2] add to [OS1]? How can you manage security patches in a timely manner if you don't have a process for it?*

A: *[OS1] and [OS2] are specified separately to cover the case where vulnerabilities are not necessarily addressed by patches. It also addresses scenarios where software is maintained by the organisation rather than by a third party.*

[OS3] Means are implemented to detect and act on possible intrusions using threat intelligence information in a timely manner.

Q: *Does this requirement apply to all systems run by an organisation, or just IdP/SP related services?*

A: *As discussed in the Sirtfi trust framework: "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*". This is applicable to all Sirtfi assertions.

[OS4] A user's access rights can be suspended, modified or terminated in a timely manner.

Q: *What is a "timely manner"?*

A: *The definition of appropriate timescales will vary by organisation based on maturity of the services and resource availability; Sirtfi does not specify a time limit. Response time should be commensurate with the impact of the incident.*

[OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.

Q: *What is ITIL?*

A: *ITIL is a standardised glossary of definitions used within the IT community. Please refer to https://www.axelos.com/resource-hub/glossary/ITIL-4-glossaries-of-terms.*

[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.

Q: *Does this security incident response capability need to be documented?*

A: *Sirtfi does not specify documentation requirements. Ideally the organisation's incident response capability will be documented in the form of policies and procedures.*

Q: *Should organisations have equivalent agreements with their subcontractors to ensure an incident response capability exists?*

A: *Since normative assertions “should be focused on information system elements that directly handle federated transactions”, if a subcontractor’s cooperation is needed in connection with responding to an incident involving such system elements then you should be confident that they will. Best practice indicates that contracts with subcontractors should cover incident response. The Sirtfi trust framework could be used as a starting point for such contractual agreements.*

Incident Response [IR]

[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.

Q: *Are the security incident interactions covered intended to be limited to SAML interactions?*

A: *Using the Sirtfi security contact outside the scope of SAML is undefined. However, Sirtfi and its required security contact information can be and have been implemented in non-SAML contexts.*

[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.

Q: *What does [IR4] add to [IR2]? If you are able and willing to collaborate for incident response (as per [IR4]) doesn't that imply that you respond to related requests (as per [IR2]) in a timely manner?*

A: *This is to highlight the importance of active collaboration, beyond a simple acknowledgment, whether or not your organisation is directly impacted by the incident.*

Q: *Can Sirtfi compliant entities request contact information in order to directly interact with our end-users?*

A: *Basically, no. Sirtfi only mandates that communication conducted in the course of managing a security incident must be acknowledged. [OS5] and [IR4] imply that if a User must be contacted in the course of managing a security incident, the User’s organisation can and will take that step.*

[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.

Q: *Will I need to use the TLP for all communication once I have agreed to Sirtfi?*

A: *No, not for all communications. However, the TLP should be used to identify the sensitivity of information shared with federated incident responders but there is no stipulation for other communication. All communication regarding federated incidents, i.e. incidents affecting the entity in the metadata, must have a traffic light colour assigned, and any information you receive should be handled in accord with any TLP level it is marked with.*

Traceability [TR]

[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.

Q: *How can I make sure that my logs are sufficient?*

A: *Check your logging configuration to make sure that you are storing timestamps and identifiers. It is important that these logs are available (or can easily be made available) to (and only to) relevant personnel during incident response. The following example is an appender to a logback.xml file as used at a typical Shibboleth IdP that employs central logging to yoursysloghost.foo.edu. This example ensures that the IP address of the remote client is recorded and may be used as inspiration for IdPs looking to improve the usability of their logs.*

logback.xml appender

```
<appender name="IDP_SYSLOG" class="ch.qos.logback.classic.net.SyslogAppender">

    <syslogHost>yoursysloghost.foo.edu</syslogHost>

    <facility>AUTH</facility>

    <port>514</port>

    <suffixPattern>[%thread] [%logger:%line] - [%mdc{idp.remote_addr}] %msg</suffixPattern>

</appender>
```

The following extract shows the modified root element of logback.xml to include IDP_SYSLOG.

logback.xml <root> element

```
<root>
```

```
    <level value="INFO" />
    <appender-ref ref="IDP_PROCESS" />
    <appender-ref ref="IDP_WARN" />
    <appender-ref ref="IDP_SYSLOG" />
</root>
```

[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]

[UR1] The participant has defined rules and conditions of use.

Q: *Do these rules and conditions need to be specific for identity federation?*

A: *No, as long as all activity conducted at entities within the federation are covered.*

[UR2] There is a process to notify all users of these rules and conditions of use.