Sirtfi

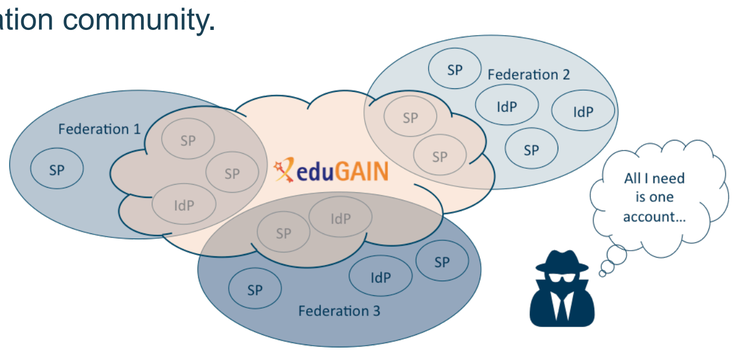
A Security Incident Response Trust Framework for Federated Identity

The **S**ecurity **I**ncident **R**esponse **T**rust Framework for **F**ederated **I**dentity (Sirtfi) provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration. Sirtfi has been developed with input from Identity Federation communities worldwide and aims to provide a scalable safeguard against inevitable future attacks.

Is your organization part of an identity federation?
Make security a priority by adopting Sirtfi.

The problem

The growth and inter-connection of federations has created a new vector of attack. One compromised account can provide access to a multitude of services across the inter-federation community.



The quality of operational security at organizations is variable and often unknown to other participants. There is typically no minimum level of security to join a federation. Consequently, there is no guarantee of effective collaboration between organizations in the event of an inevitable federated incident.

The Problem: organizations are choosing to opt out of eduGAIN, or block authentication, due to lack of trust.

The solution

Since a centrally coordinated incident response capability within the community does not exist, participants must collaborate to mitigate the risk of incidents.

Sirtfi describes practices and attributes that identify an organization as being capable of participating effectively in incident response. The framework stipulates preventative measures to protect an organization from attack, and behaviour to adopt in the event of an incident. By adopting Sirtfi, an organization asserts that it can meet the following points:

Operational Security
- Provide security incident response capability with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.

Incident Response
- Assure confidentiality of information exchanged
- Identify trusted security contacts
- Guarantee a response during collaboration

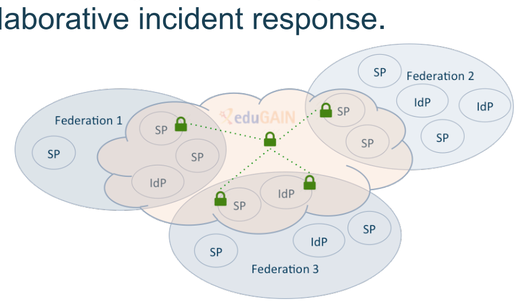
Traceability
- Record and share relevant system generated information
- Ensure such information is kept in accordance with policy

Participant Responsibilities
- Confirm that end users are aware of an appropriate AUP

The Solution: a Trust Framework for Federated Security

Why should I join?

Sirtfi is used as an identifier to mark trusted partners within eduGAIN. Compliance is expressed in metadata and gives a transparent view of those organizations willing to engage in collaborative incident response.



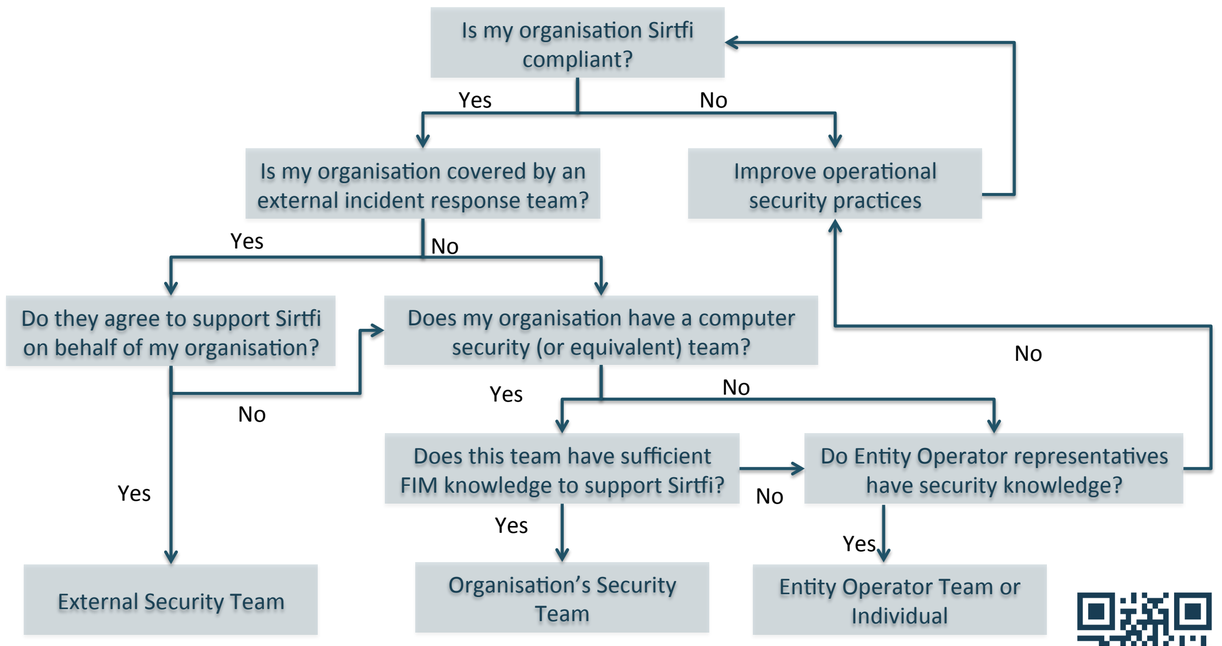
The credibility gained by asserting Sirtfi compliance opens doors within eduGAIN as organizations choose to enable authentication based on this enhanced trust.

IdPs	SPs
Gain **access** to useful services that only allow authentication from Sirtfi compliant IdPs	Gain **users** whose home organizations only allow authentication at Sirtfi compliant SPs
Guarantee an efficient and effective **response** from partner organizations during incident response	
Raise the bar in operational **security** across eduGAIN	

How can I join?

Are you part of an identity federation? Just follow these simple steps

- ❑ Test your organization
  Ensure that your organization satisfies every Sirtfi requirement
- ❑ Choose a Sirtfi Contact
  Use the flowchart below to help!
- ❑ Assert your compliance
  Work with your Federation Operator to add Sirtfi Extensions to your metadata



Get started at https://refeds.org/sirtfi

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965, **AARC** (Authentication and Authorisation for Research and Collaboration)