Sirtfi

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.

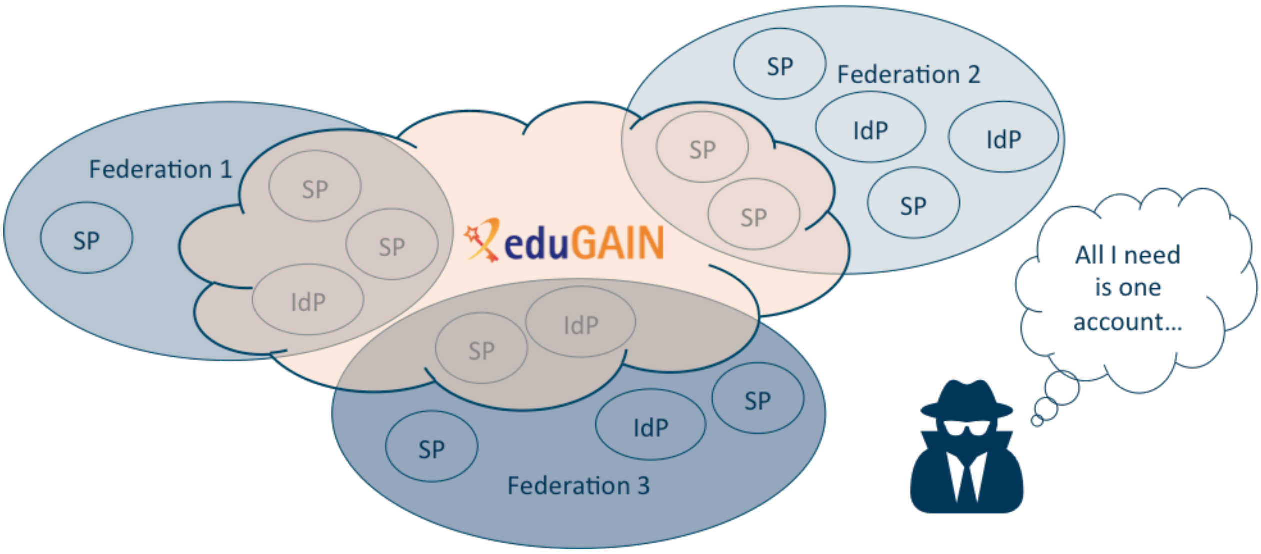
Why is Sirtfi needed?
What will Sirtfi change?
What are the benefits of Sirtfi?

The Sirtfi framework has been written by the **REFEDS** (the Research and Education FEDerations group) Sirtfi Working Group.

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)

The Problem: Lack of Trust

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 organisations 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 organisations in the event of an inevitable federated incident.

Inviting new vector of attack + Uncertainty in security capability of participants = Lack of trust

Organisations are choosing to opt out of eduGAIN, or block authentication, due to lack of trust.

The Solution: a Trust Framework for Incident Response

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

Sirtfi describes practices and attributes that identify an organisation as being capable of effectively participating in incident response. The framework stipulates preventative measures to protect an organization from attack, and behaviour to adopt in the event of an incident.

Operational Security

- Require that a security incident response capability exists 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 contacts
- Guarantee a response during collaboration

Traceability

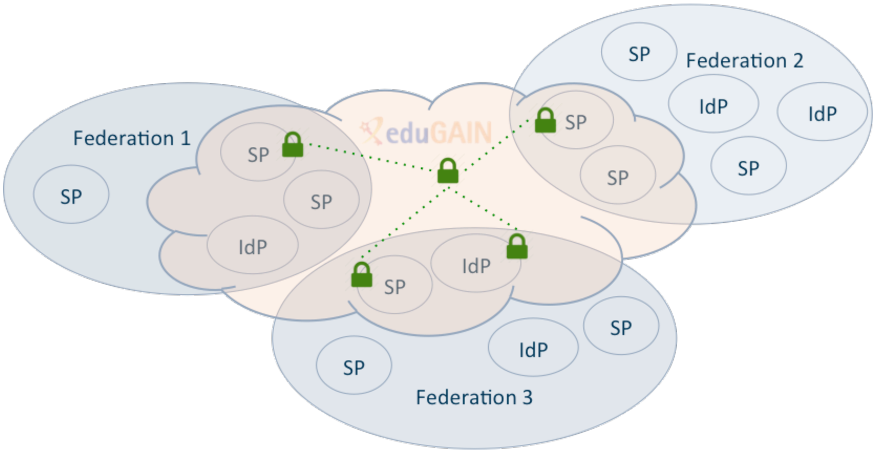
- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

The Benefits

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



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

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