Introduction to Sirtfi

Tom Barton, Chair, Sirtfi Working Group
Hannah Short, former Chair, Sirtfi Working Group

April 2022

REFEDS

Overview

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.

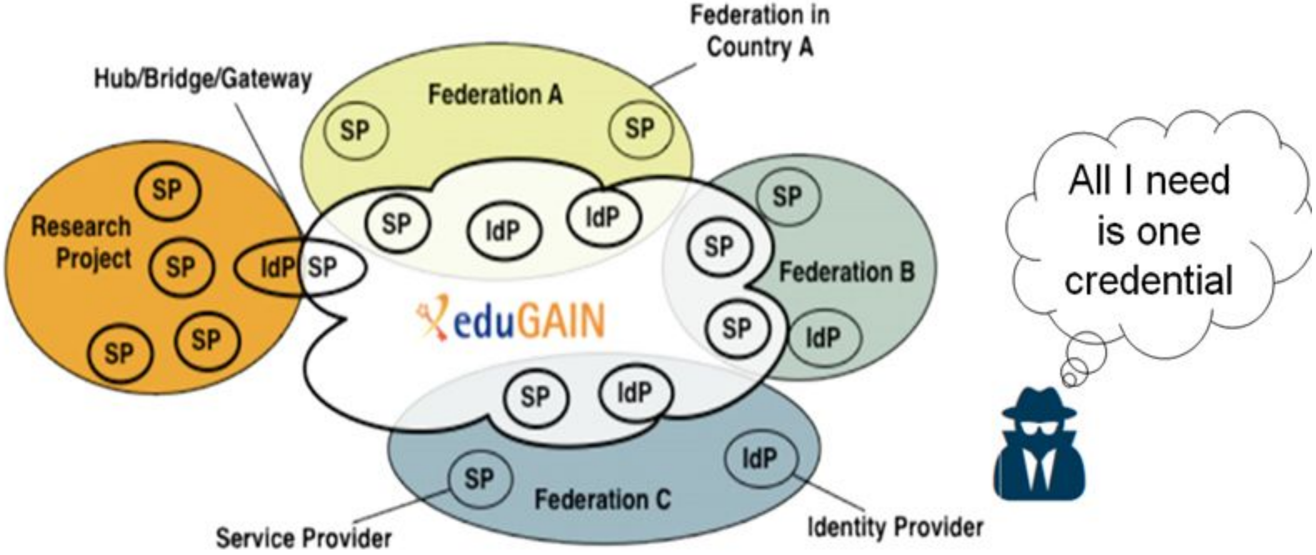
It defines a modest set of security protections for federated entities and a standard means of publishing security contact information for them.

A party participates in Sirtfi by first ensuring that they implement those security protections, then coordinating with their Federation Operator to publish this self-attestation together with their security contact information.

Why is this needed? Read on.

What if …?

… an incident spread throughout the federated Research & Education community via a single compromised identity?

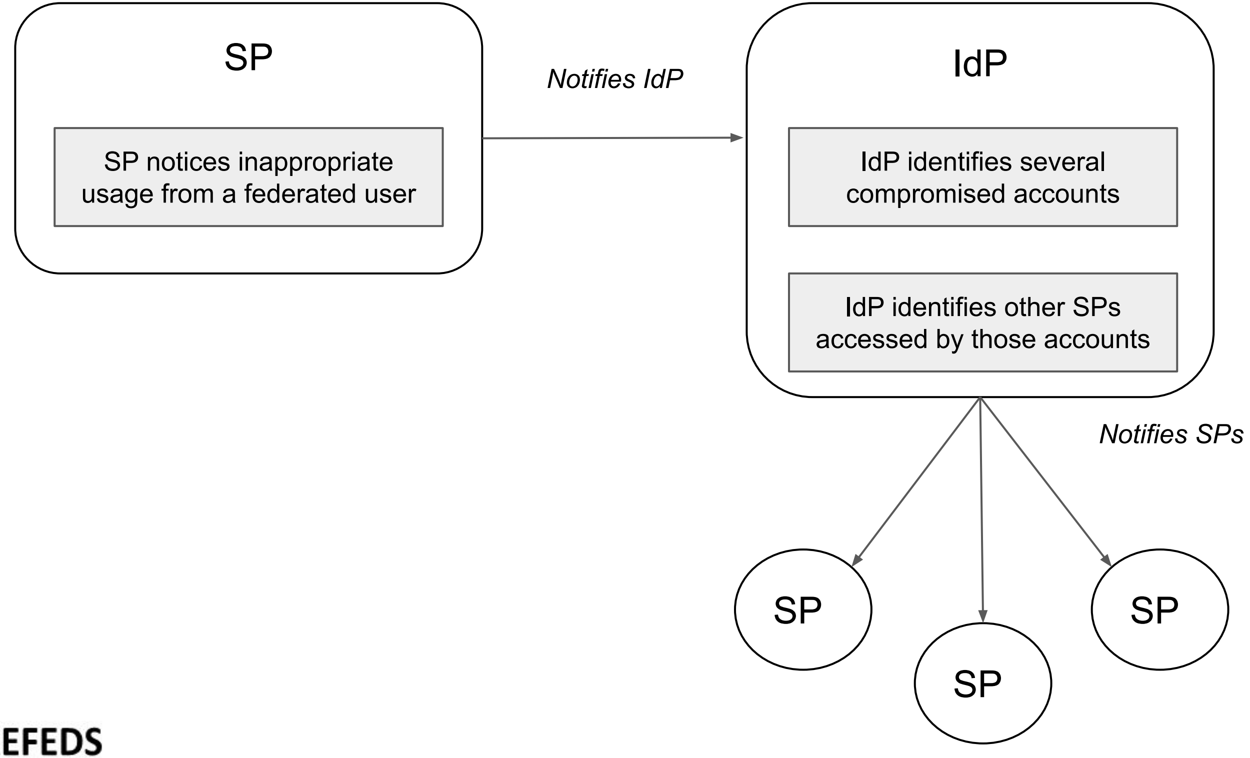


REFEDS

What if … ?

- Could we determine the extent of the incident?
- Could we ensure that incident related information is shared confidentially?
- Could we alert the federation members involved?
- Who would take charge of the incident investigation?

It seems like common sense …



SP

SP notices inappropriate usage from a federated user

Notifies IdP

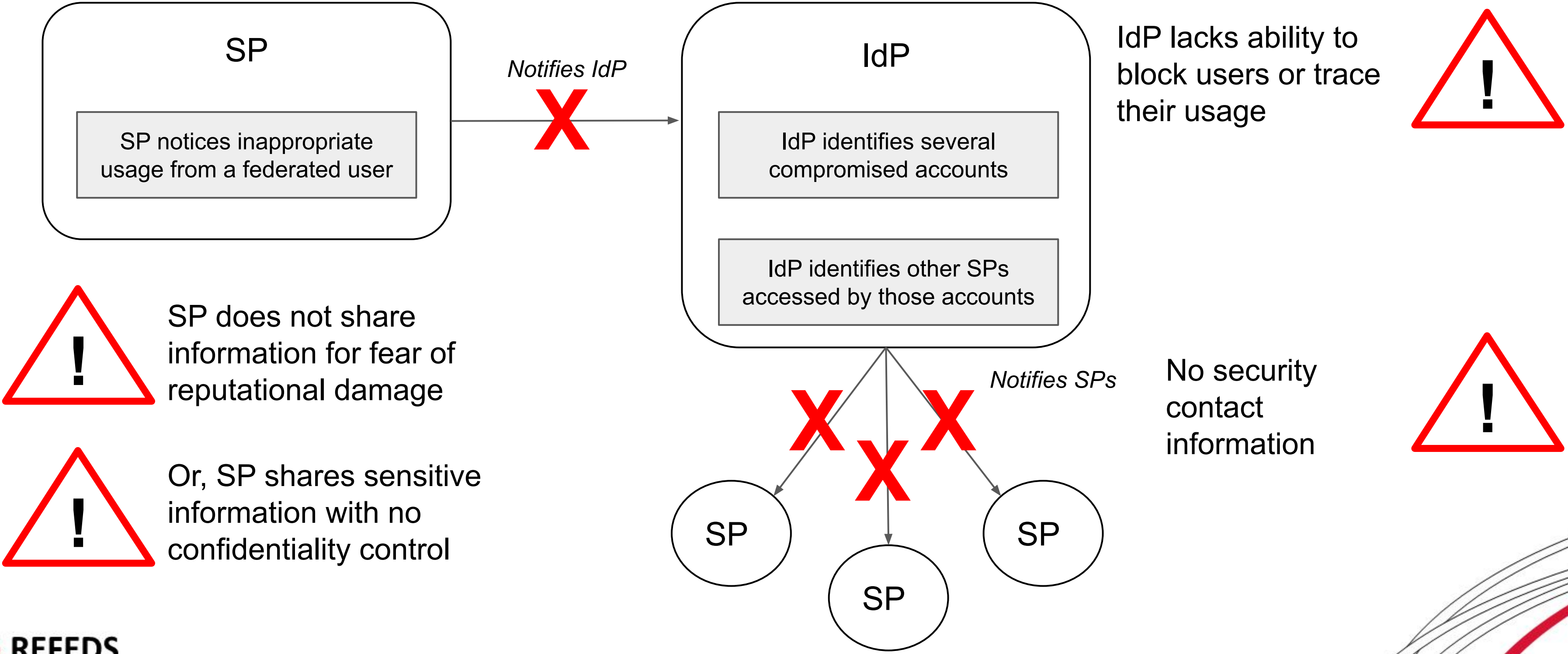
IdP

IdP identifies several compromised accounts

IdP identifies other SPs accessed by those accounts

Notifies SPs

… but in reality



SP

SP notices inappropriate usage from a federated user

Notifies IdP

IdP

IdP identifies several compromised accounts

IdP identifies other SPs accessed by those accounts

IdP lacks ability to block users or trace their usage

SP does not share information for fear of reputational damage

Or, SP shares sensitive information with no confidentiality control

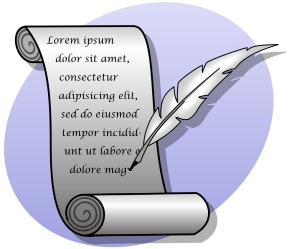
Notifies SPs

No security contact information

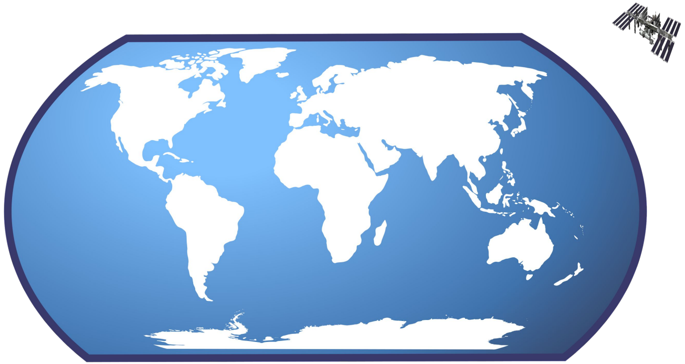
The solution

We agree to abide by

a common framework



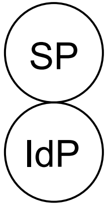
wherever we are



That’s a Trust Framework, a defined aspect of the trust already built on and placed in our collaborative efforts, like federations and research e-infrastructures

Sirtfi - Security Incident Response Trust Framework for Federated Identity

Apply basic operational security protections to your federated entities in line with your organisation’s policies and priorities



SP

IdP

Patch, manage vulnerabilities, detect intrusions, manage access, log events

Be willing to collaborate in responding to a federated security incident and notify[1] others when you realise that an incident impacts them

Respect user privacy and use the Traffic Light Protocol with other Sirtfi participants

Publish security contact and self-assert a Sirtfi “tag” so that others will know to trust this about you

```
<EntityDescriptor
…
Sirtfi tag
…
security contact
…
</EntityDescriptor>
```

Coordinate with your Federation Operator to publish in federation metadata

[1] This is the only substantive difference between Sirtfi (v1) and Sirtfi v2.

When a security incident happens …

- Conduct your incident investigation using your usual procedures
- If you notice that a federated entity outside of your organisation is impacted by the incident, notify them about it and begin to collaborate with them to manage the incident
- When you are notified by another Sirtfi partner of your involvement in an incident they are investigating, respond to their request in a timely manner
- The eduGAIN Security Incident Response Handbook can be used to supplement your normal incident response procedures

The REFEDS Sirtfi wiki space has guidance materials that go into more detail.

REFEDS

eduGAIN Security Incident Response Handbook

- Roles, responsibilities, and procedures for
  - Federation Participants
  - Federation Operators
  - eduGAIN Security team
- Adopted by the eduGAIN Security Team, recommended for all parties
- Respects incident response coordination roles where they are already established
- Federation Operators are default coordinators within their federations
- eduGAIN Security team coordinates across federations
- Augments, does not supersede, established local policies and procedures