Sirtfi Version 2

ISGC2024, Security Workshop, 25 March 2024

David Kelsey

UKRI STFC Rutherford Appleton Laboratory

(with many thanks to Tom Barton, Internet2 and other members of the REFEDS Sirtfi Working Group)

REFEDS

A Security Incident Response Trust Framework for Federated Identity

Sirtfi v2 has been published

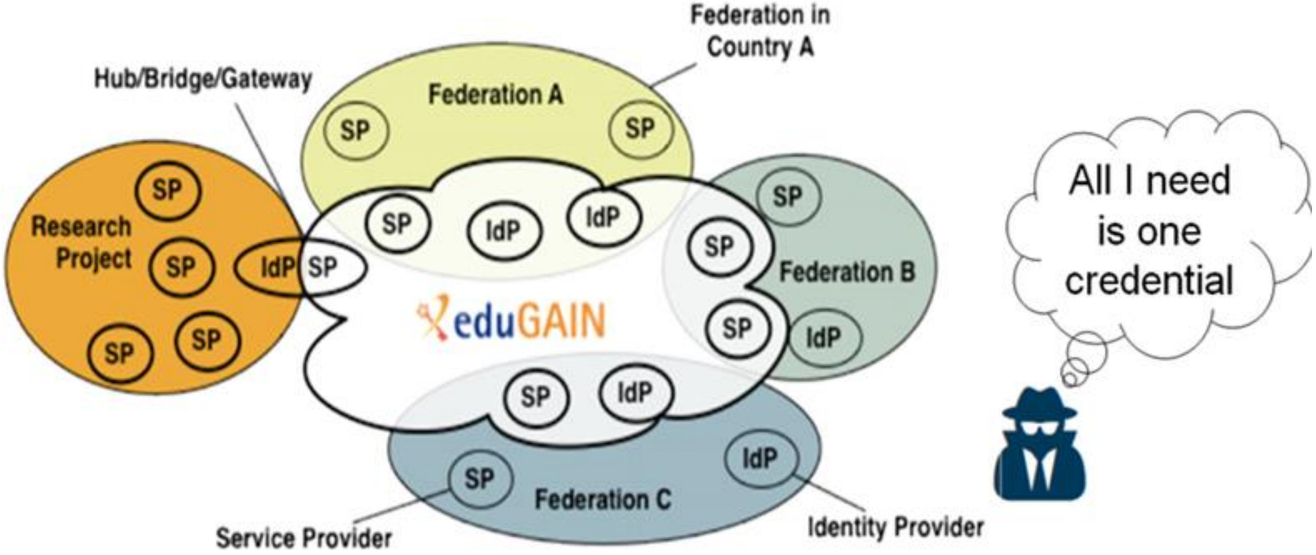
Original Sirtfi (v1) will NOT be deprecated

They will coexist (nicely!)

Sirtfi v2 implies Sirtfi (v1)

What is Sirtfi version 1?

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

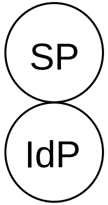


Sirtfi Version 1

- https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf
- A derivative of “Trust Framework for Security Collaboration among Infrastructures” - SCI version 1
  - ISGC2013
  - https://pos.sissa.it/179/011/pdf
- “The Security Incident Response Trust Framework for Federated Identity (Sirtfi) provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration”
- FIM4R requirements paper (version 1) – required “Operational Security”

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



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

Be willing to collaborate in responding to a federated security incident *and notify 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

Changes of v2 Over v1

- Added a new assertion that expresses an obligation to notify, in addition to v1's obligation to respond
- Clarified wording of several assertions based on survey responses and other feedback
- Clarified role of 3rd parties
- Revamped the v1 Participant Responsibilities section into v2's User Rules and Conditions to better reflect practises in the field
- Incorporated "Sirtfi Identity Assurance Certification Description for Federation Operators" into the v2 spec
- Amended Syntax, Registration Criteria, and Removal Criteria sections to reflect co-existence of Sirtfi (v1) and Sirtfi v2

Publication

- Sirtfi Version 2 was published in July 2022
  - https://refeds.org/wp-content/uploads/2022/08/Sirtfi-v2.pdf
- Substantial revisions and additions to associated guidance documents
- REFEDS Sirtfi web site updated to reflect coexistence of both versions
  - https://refeds.org/sirtfi
- Federation Operators and others promoting Sirtfi adoption are encouraged to promote v2 for new adopters