



Authentication and Authorisation for Research and Collaboration

AARC Assurance Profiles

Addressing Federated Security Incident Response

Hannah Short

CERN

hannah.short@cern.ch



Kantara

April 7th, 2016

Agenda

The AARC Project

Policy & Best Practice Harmonisation Work Package

Assurance Gaps

- Minimum LoA
- Sirtfi

Recording Adoption

- Self Assessment

-
- Authorisation and Authentication for Research and Collaboration
 - European Commission funded project
 - 2 years, 2015/17
 - 20 partners from NRENs, E-Infrastructures & Libraries
 - Builds on existing AAls and on production federated infrastructures.

The AARC vision is to create a future in which e-Infrastructures and new research collaborations cooperate seamlessly on top of a scalable and interoperable AAI.

<https://aarc-project.eu>

- Global scope, though Europe-focused
- Many moving parts...
- Must ensure any policy adoption/technical changes are:
 - Easy to adopt
 - Legally acceptable
 - Financially beneficial/neutral
- AARC2 proposal submitted
 - 2017/19
 - 27 partners (so growing!)
 - Focus on users





Policy and best practices harmonisation

- Tasks chosen around perceived policy gaps
- Areas identified jointly by e-infrastructures, research infrastructures and NRENs

Delivery of an assurance baseline and differentiated assurance framework;

Enable consistent handling of security incidents when federated access is enabled;

Develop support models for (inter)federated access to commercial services;

Develop translation guidelines to enable exchange of accounting and usage data.

Identify a minimal set of policies to explore policy and security aspects to enable attribute aggregation;

enable the integration of attribute providers and of credential

Develop translation guidelines to enable exchange of accounting and usage data.

Policy and best practices harmonisation

Assurance Gaps

Common
Baseline
Level of
Assurance



Security
Incident
Response

- Can we

Minimum LoA

Research community interviews

- Interviewed 6 research infrastructures
 - CLARIN (language research)
 - DARIAH (arts and humanities)
 - ELIXIR (life science)
 - LIGO (physics)
 - photon/neutron facilities (physics)
 - WLCG (physics)
- Interviewed 2 e-infrastructure
 - EGI
 - PRACE
- Interview results: <https://wiki.geant.org/x/nQHbAg>

Minimum LoA

Interview results



1. The accounts in the Home Organisations must each belong to a known individual
2. Persistent user identifiers (i.e., no reassign of user identifiers)
3. Documented identity vetting procedures (not necessarily face-to-face)
4. Password authentication (with some good practices)
5. Departing user's eduPersonAffiliation must change promptly
6. Self-assessment (supported with specific guidelines)

The document: <https://wiki.geant.org/x/wIEVAw>

Minimum LoA

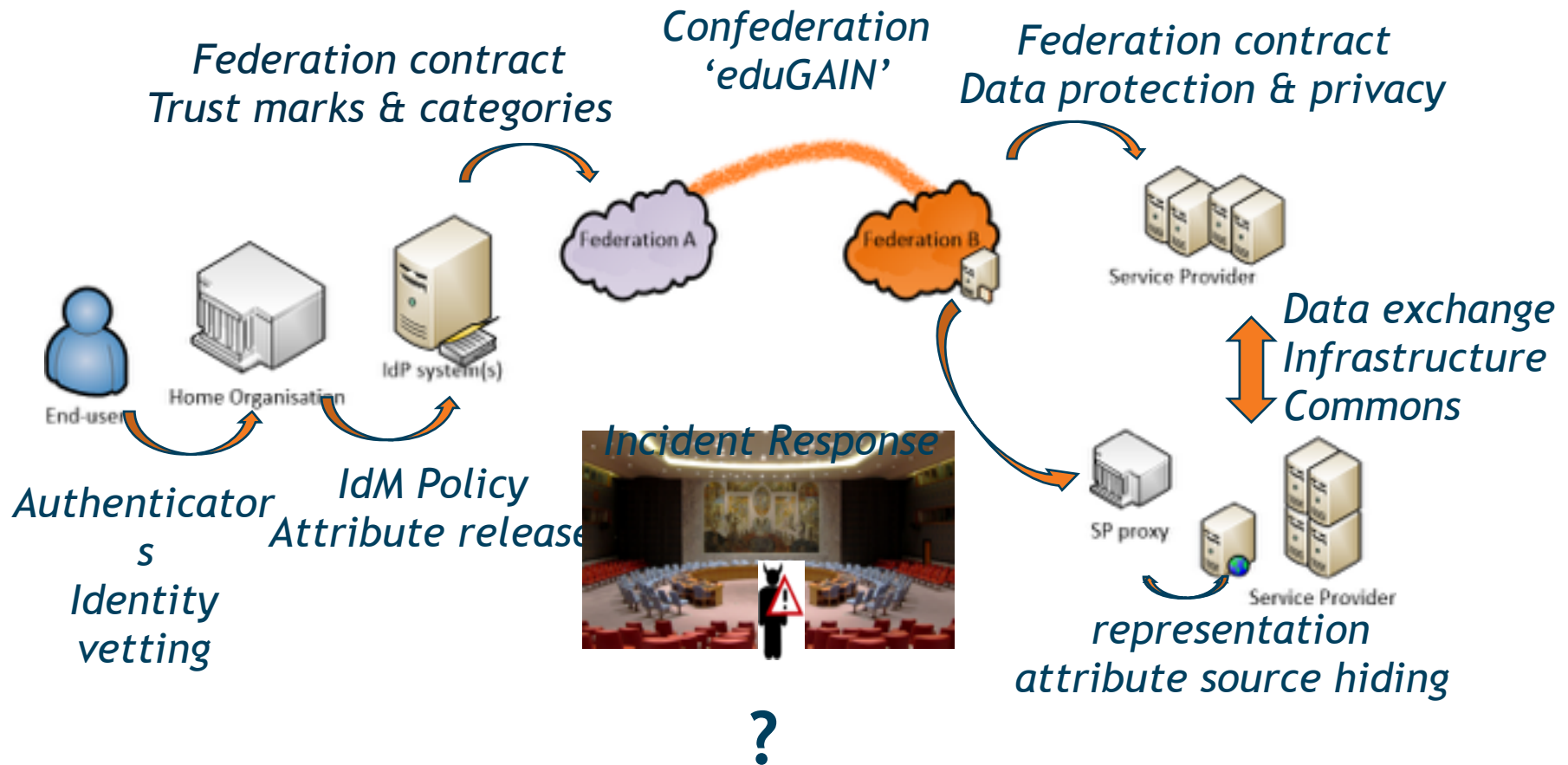
Next steps

- REFEDS working group
- Likely that each minimum LoA requirement will be a separate Entity Category



Policy and best practices harmonisation

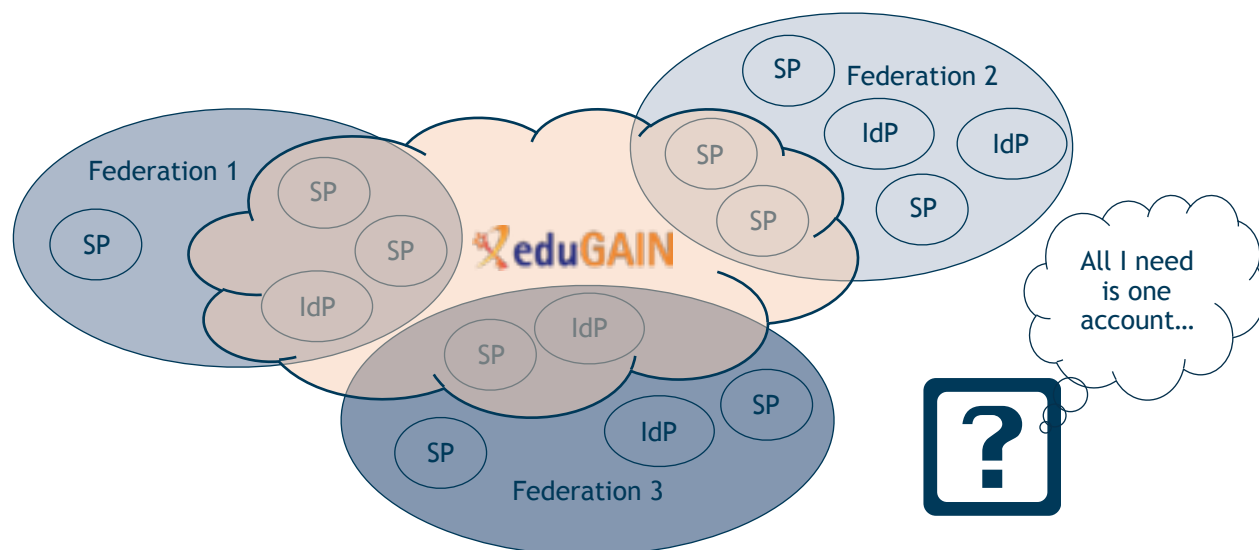
The chain of assurance



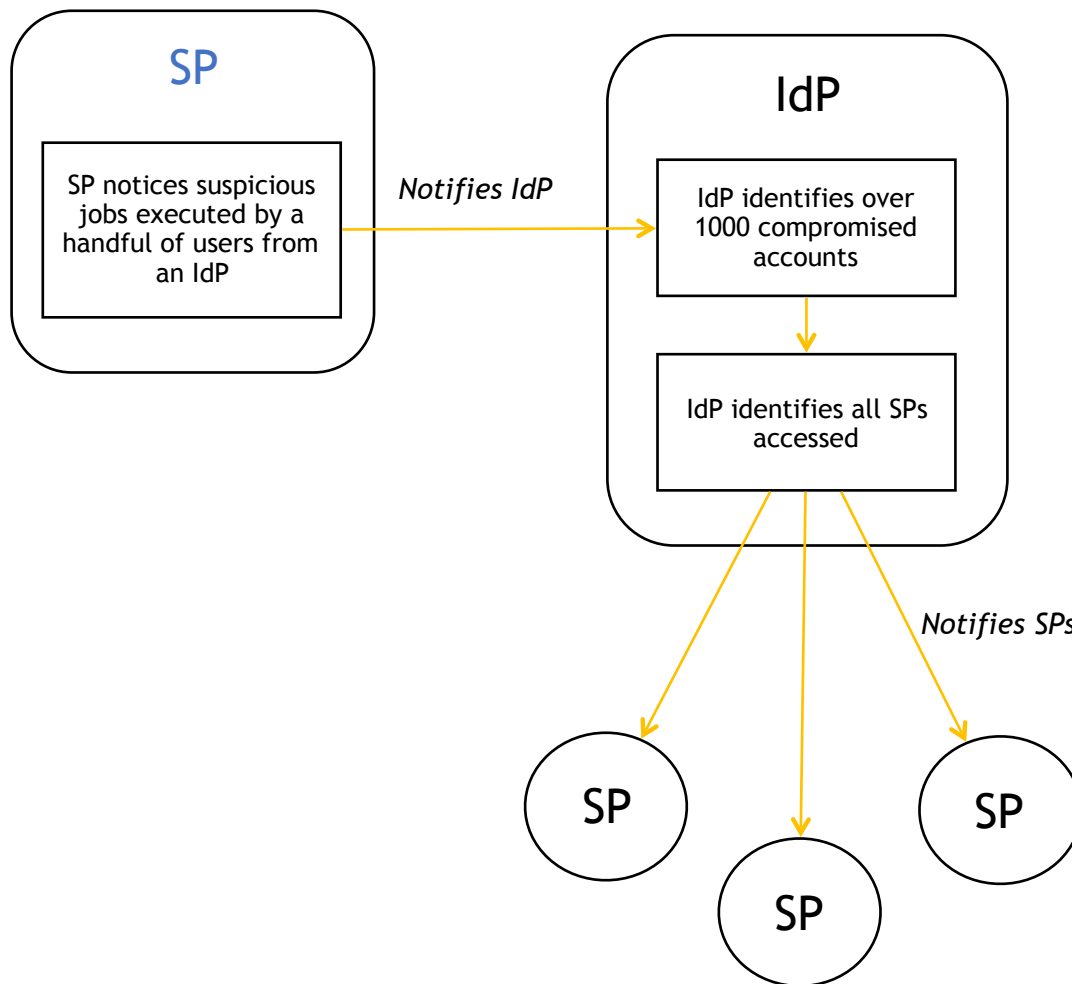
Security Incident Response

The problem

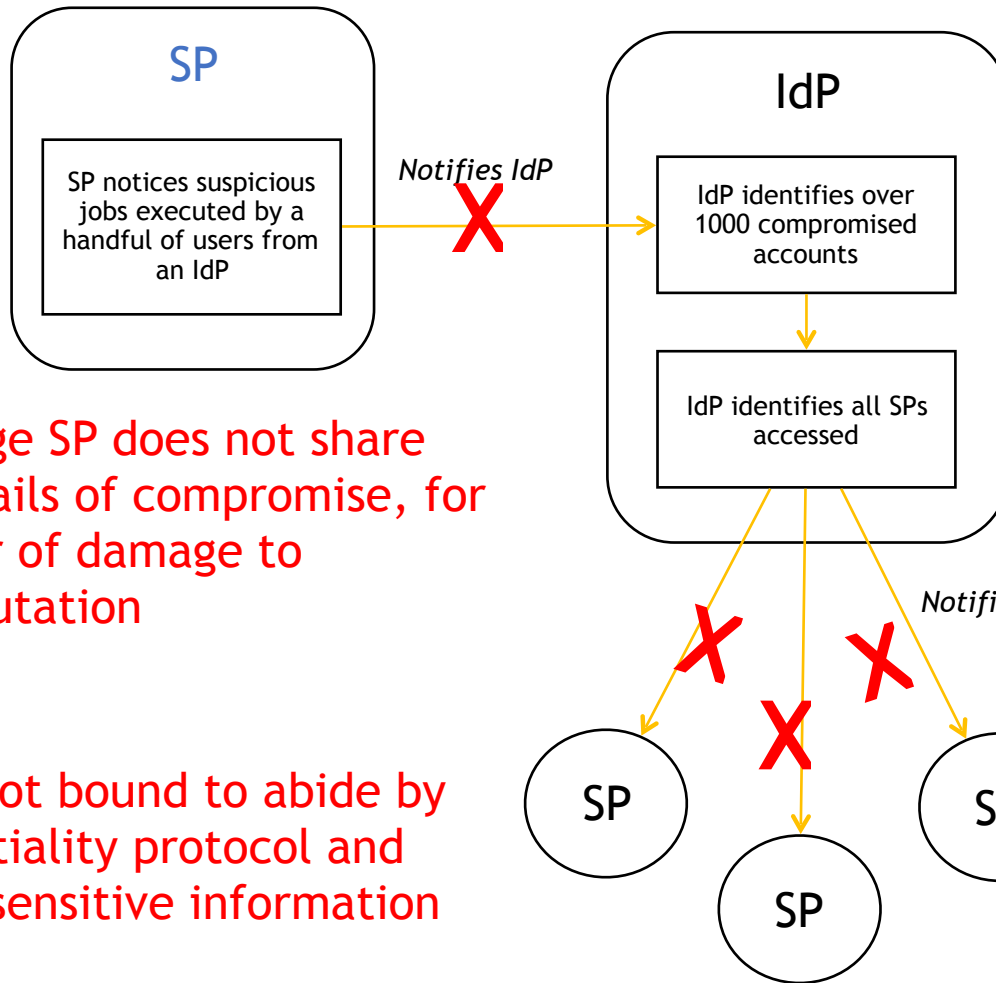
- Clearly an inviting vector of attack
- The lack of a centralised support system for security incident response is an identified risk to the success of eduGAIN
- We will need participants to collaborate during incident response - this may be outside their remit



It all seems like common sense...



... but in reality



Small IdP may not have capability to block users, or trace their usage



Large SP does not share details of compromise, for fear of damage to reputation



SPs are not bound to abide by confidentiality protocol and disclose sensitive information

No security contact details!



Security Incident Response

The solution

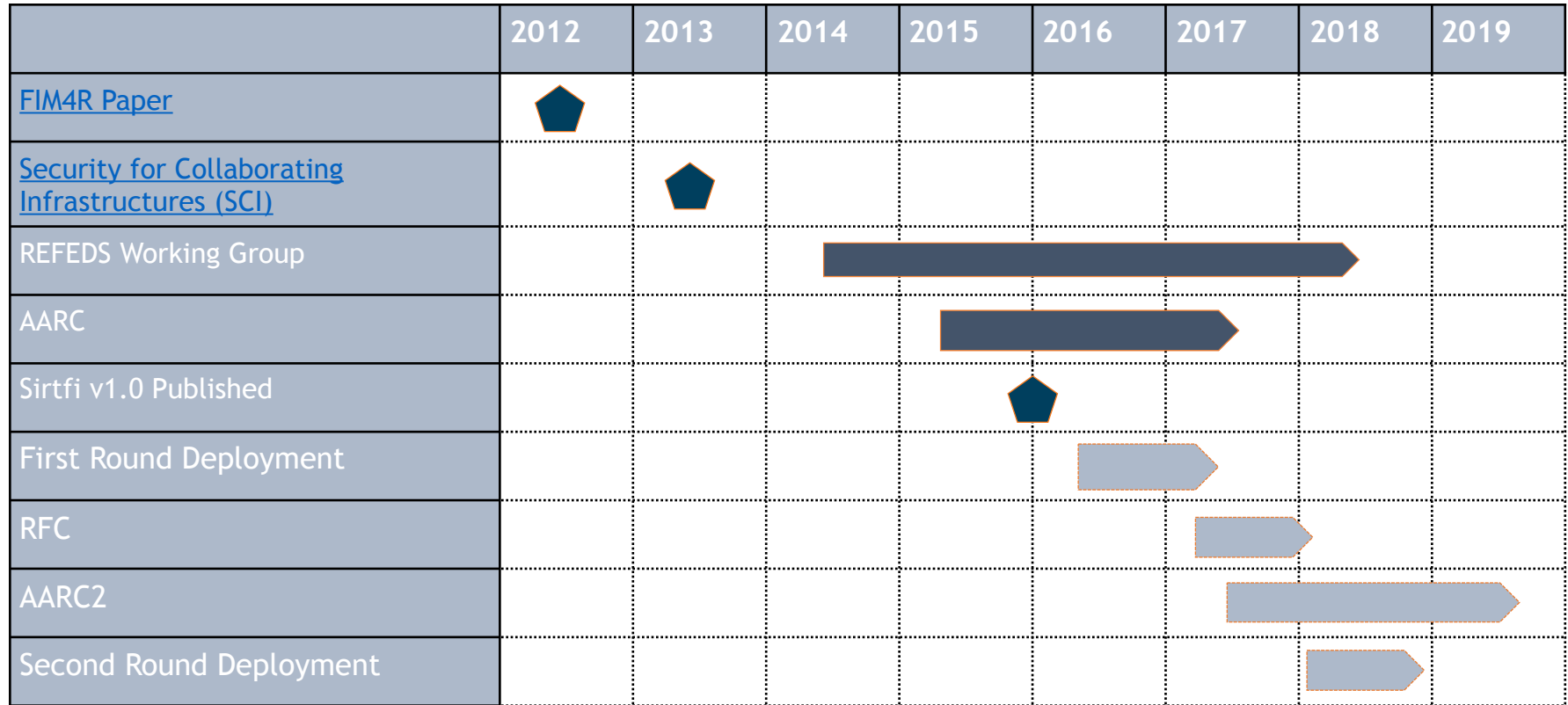


- Attacks inevitable 😞
- But we can make security capability transparent and build relationships between organisations and people 😊

...We need a trust framework!

Security Incident Response

A history and the future



Security Incident Response

FIM4R



- Issue of IdM raised by IT leaders from EIROforum labs (Jan 2011)
 - CERN, EFDA-JET, EMBL, ESA, ESO, ESRF, European XFEL and ILL
- These laboratories, as well as national and regional research organizations, face similar challenges
- Prepared a paper that documents common requirements
<https://cdsweb.cern.ch/record/1442597>

“Security procedures and incident response would need to be reviewed. Today, each resource provider is for example responsible for terminating access by known compromised identities. With identity federation, this responsibility will be shifted to the IdP though resource providers will insist on the ability to revoke access.”

“Such an identity federation in the High Energy Physics (HEP) community would rely on:

- *A well-defined framework to ensure sufficient trust and security among the different IdPs and relying parties.”*

Security Incident Response

Security for Collaborating Infrastructures (SCI)

- A collaborative activity of information security officers from large-scale infrastructures
 - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, ...
- Laid the foundations for a *Trust framework*
 - Enable interoperation (security teams)
 - Manage cross-infrastructure security risks
 - Develop policy standards
 - Especially where not able to share identical security policies
- Proceedings of the ISGC 2013 conference http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf



- The SCI document formed the basis for the Security Incident Response Trust Framework for Federated Intity

- ✓ Articulate framework requirements
- ✓ Complete Community Consultation
- ✓ Publish Sirtfi framework
- ✓ Create Training material
- Confirm metadata extensions
- Begin adoption
- Support filtering based on Sirtfi

Operational Security

- Require that a security incident response capability exists with sufficient authority to

Incident Response

- Assure confidentiality of information exchanged

Traceability

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

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

Security Incident Response

Sirtfi, security contact details

- Based on the InCommon security contactType
- What to include?
 - Individual or group email contact? Recommend generic
 - Telephone number in case critical infrastructure down? Would that really help?
 - PGP Key?
- The specification is flexible, section 2.3.2.2 of <https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>

```
<ContactPerson contactType="other"
  xmlns:icmd="http://refeds.org/metadata"
icmd:contactType="http://refeds.org/metadata/contactType/security">
<GivenName>Security Response Team</GivenName>
  <EmailAddress>security@institution.edu</EmailAddress>
</ContactPerson>
```

Security Incident Response

Sirtfi, expressing compliance



- Asserting compliance via standard [OASIS](#) specification
- Applied to register with [IANA](#)

```
<attr:EntityAttributes>
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
    <saml:AttributeValue>https://refeds.org/sirtfi</
saml:AttributeValue>
  </saml:Attribute>
</attr:EntityAttributes>
```

Security Incident Response

Benefits of Sirtfi



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

Security Incident Response

Find out more - Home Page



Call us : +31(0)20 5304488 | Mail us : contact@refeds.org



Home | Blog | Wiki | Meetings | Sponsor | Federations | Our Work | About |

SIRTFI

REFEDS > SIRTFI

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant.

REFEDS' [Sirtfi Working Group](#) has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the [AARC Project](#).



Benefits

Why should I join? What are the [Benefits](#)?



Sirtfi v 1.0

View the [Sirtfi Framework](#)



FAQs

Need [help](#)?

<https://refeds.org/sirtfi>

Security Incident Response

Find out more - Technical Wiki

A screenshot of a web browser showing the SIRTFI Home page on the REFEDS wiki. The page has a light grey header with the REFEDS logo and 'Spaces' dropdown, a search bar, and a 'Log in' link. The main content area is divided into a left sidebar and a main content area. The sidebar contains the SIRTFI logo, 'Pages' and 'Blog' links, a 'PAGE TREE' section with links to 'Guide for Federation Participants', 'Guide for Federation Operators', and 'FAQs', and 'Space tools' at the bottom. The main content area has a 'Pages' header, the title 'SIRTFI Home', and a sub-header 'SIRTFI Home'. Below this, it states 'Created by Nicole Harris, last modified by Hannah Short on Mar 31, 2018'. The main text reads 'Welcome to the Sirtfi Technical Wiki' and 'Sirtfi is the Security Incident Response Trust Framework for Federated Identity. For further background on Sirtfi please visit the [Sirtfi Homepage](#).' There is also a 'Where to start?' section with a bulleted list of links to 'Guide for Federation Participants', 'Guide for Federation Operators', and 'FAQs'. The AARC logo is visible at the bottom of the main content area.

<https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home>

Recording Adoption

Self Assessment

- Communities are happy with self assessment as long as the group is relatively small
- The eduGAIN world is not small!
- Some use cases require peer review
- At a larger scale automation will be necessary
- How do we ensure the correct people complete the assessment?

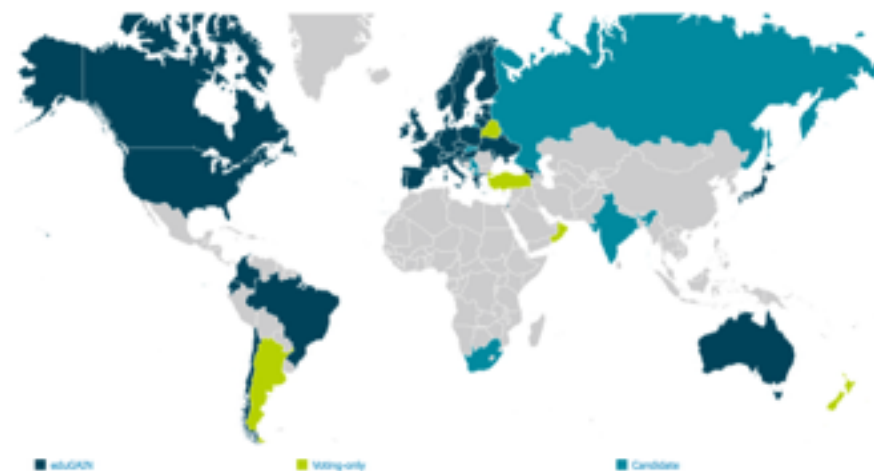
eduGAIN Stats

Federations: 38

All entities: 3157

IdPs: 2007

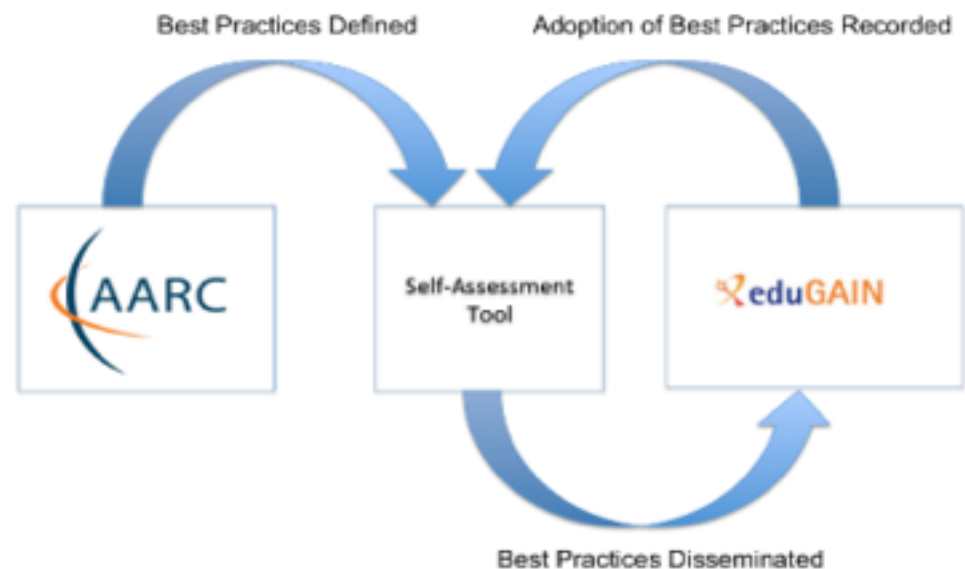
SPs: 1151



Recording Adoption

Self Assessment

- Spinoff project from LoA/Sirtfi activities to develop a self assessment tool*
 - Optional Peer Review
 - Integration with SAML Metadata
 - Adoption Monitoring
- Feedback has been positive, but must ensure design scale
- Unclear how this tool will be developed, looking to the next round of AARC and GEANT Projects



* https://docs.google.com/document/d/10kguCdxWn38z_EGRnrjCl4GSeO44zFGGeXWHGmzz27o

Conclusions

- The AARC Project aims to ensure that identity federation succeeds, both in technologies and policies
- Measures to address perceived assurance gaps were included in the Policies and Best Practices Harmonisation Work Package
- Community based interviews have defined a minimum acceptable LoA, this will be the basis for an assurance profile
- There is a clear assurance gap in federated security, which is being addressed by a trust framework
- A Self-Assessment tool would prove valuable for multiple use cases to scale adoption

Appendix, Sirtfi Assertions

Operational security

- [OS1] Security patches in operating system and application software are applied in a timely manner.
- [OS2] A process is used to manage vulnerabilities in software operated by the organisation.
- [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats
- [OS4] A user's access rights can be suspended, modified or terminated in a timely manner.
- [OS5] Users and Service Owners (as defined by [ITIL](#) [ITIL]) within the organisation can be contacted.
- [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.

Incident response

- [IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs.
- [IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.
- [IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust framework.
- [IR4] Follow security incident response procedures established for the organisation.
- [IR5] Respect user privacy as determined by the organisations policies or legal counsel.
- [IR6] Respect and use the [Traffic Light Protocol \[TLP\]](#) information disclosure policy.

Traceability

- [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.
- [TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices.

Participant responsibilities

- [PR1] The participant has an Acceptable Use Policy (AUP).
- [PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.

Thank you Any Questions?

hannah.short@cern.ch



<https://aarc-project.eu>

