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

AARC

- 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 AAIs and on production federated infrastructures.

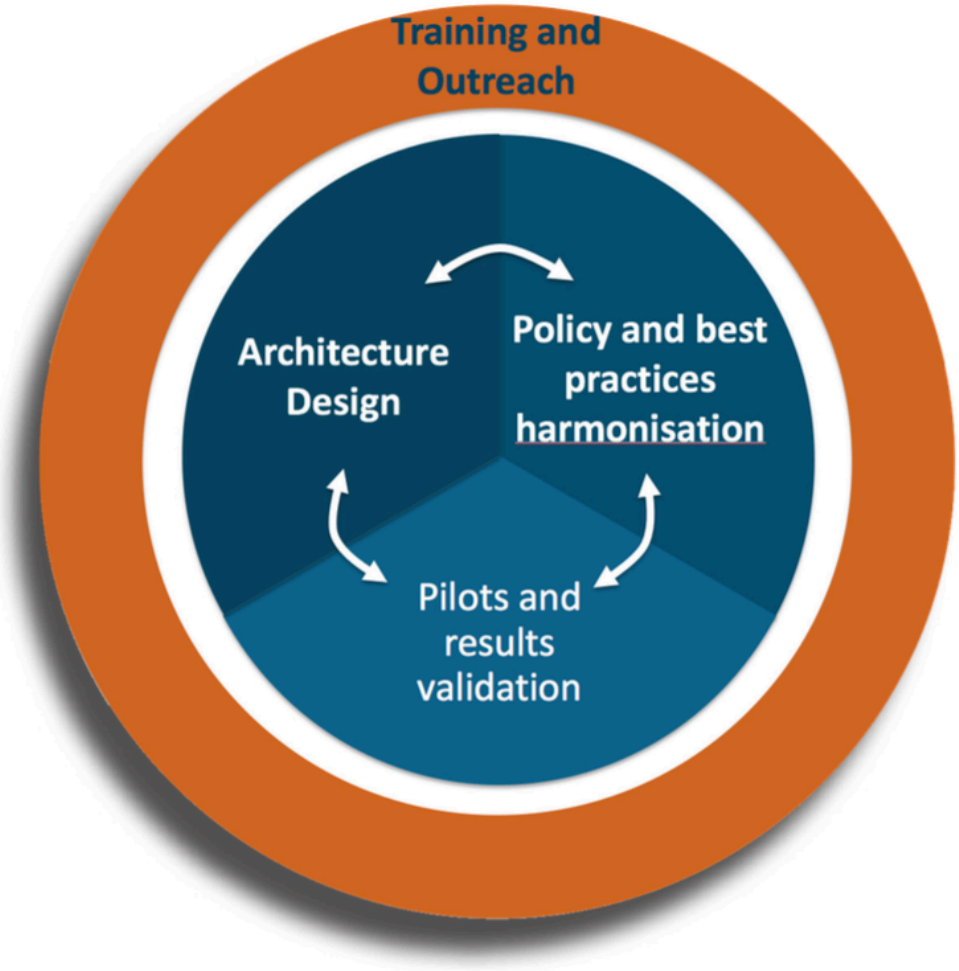
The AARC vision is to create a future in which e-Infrastructures and new research collaborations cooperate seamlessly on top of a scalable and interoperable AAI.

https://aarc-project.eu

AARC

- 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

AARC


Training and Outreach
Architecture Design
Policy and best practices harmonisation
Pilots and results validation

Policy and best practices harmonisation

What does assurance mean? And to whom?
How much differentiation of LoA can people handle?

How can we address incidents that propagate through the federated space?

Can we get policy coordination to scale?

What is the place of third-party commercial and eGov providers?
How does that help guest identity?

How can we share necessary accounting?

What's a sustainable distribution of responsibilities amongst AAI participants?

Credit to David Groep (Nikhef) for this slide

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;

Identify a minimal set of policies to enable attribute aggregation;

Explore policy and security aspects to enable the integration of attribute providers and of credential translation services;

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

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

Develop guidelines to enable exchange of accounting and usage data.

Policy and best practices harmonisation
Assurance Gaps

Common Baseline Level of Assurance

- Multiple LoA profiles exist but tend to be localised & require considerable negotiation to adopt
- Based on empirical studies, what is a reasonable baseline of assurance to expect from R&E IdPs?

Security Incident Response

- Can we facilitate collaborative incident response?
- Is there a way to make this attractive to participants?

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-infrastructures
  - EGI
  - PRACE
- Interview results: https://wiki.geant.org/x/nQHbAg

Credit to Mikael Linden for this slide

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)

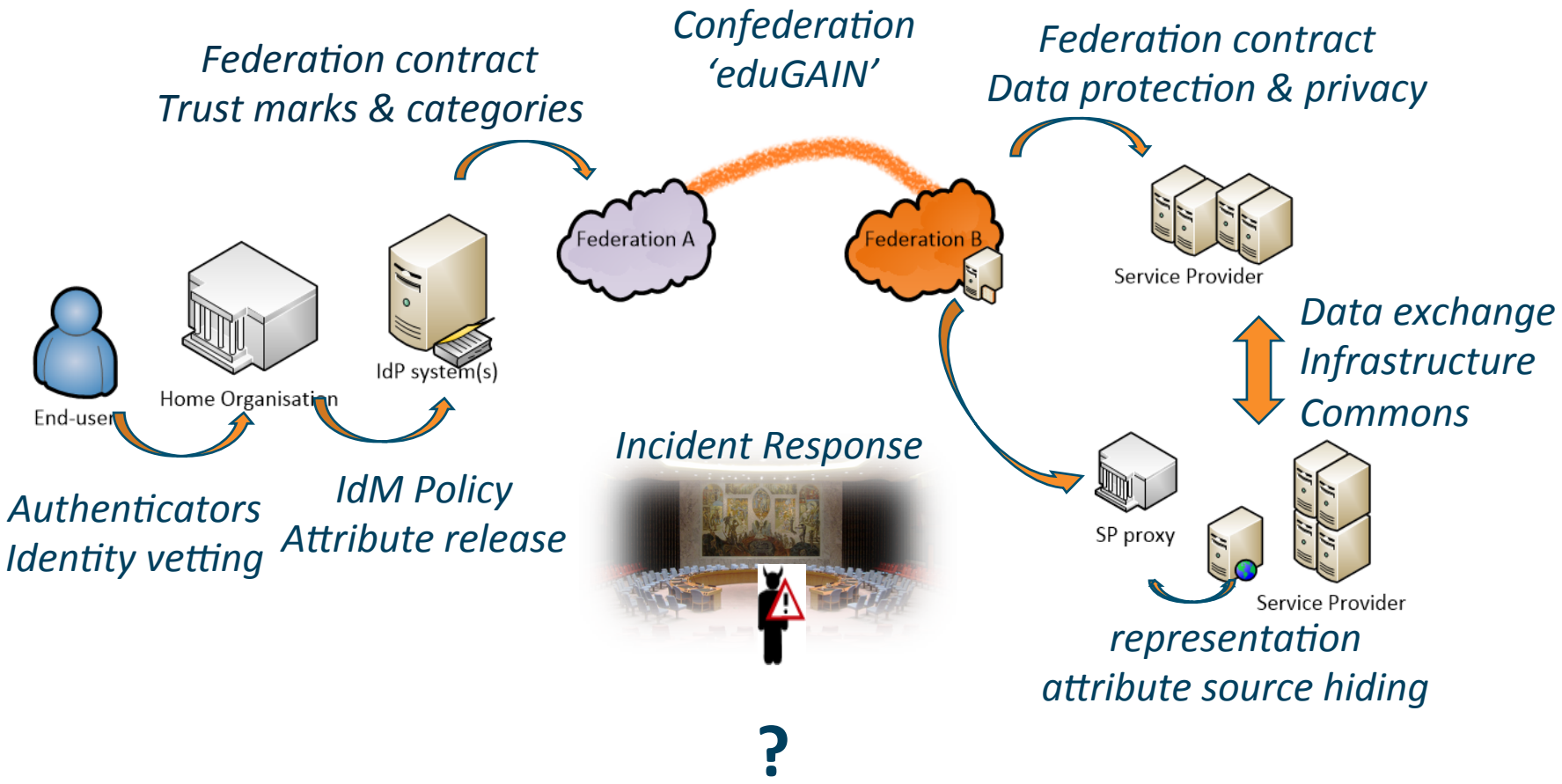
The document: https://wiki.geant.org/x/wIEVAw

Credit to Mikael Linden for this slide

Minimum LoA
Next steps

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

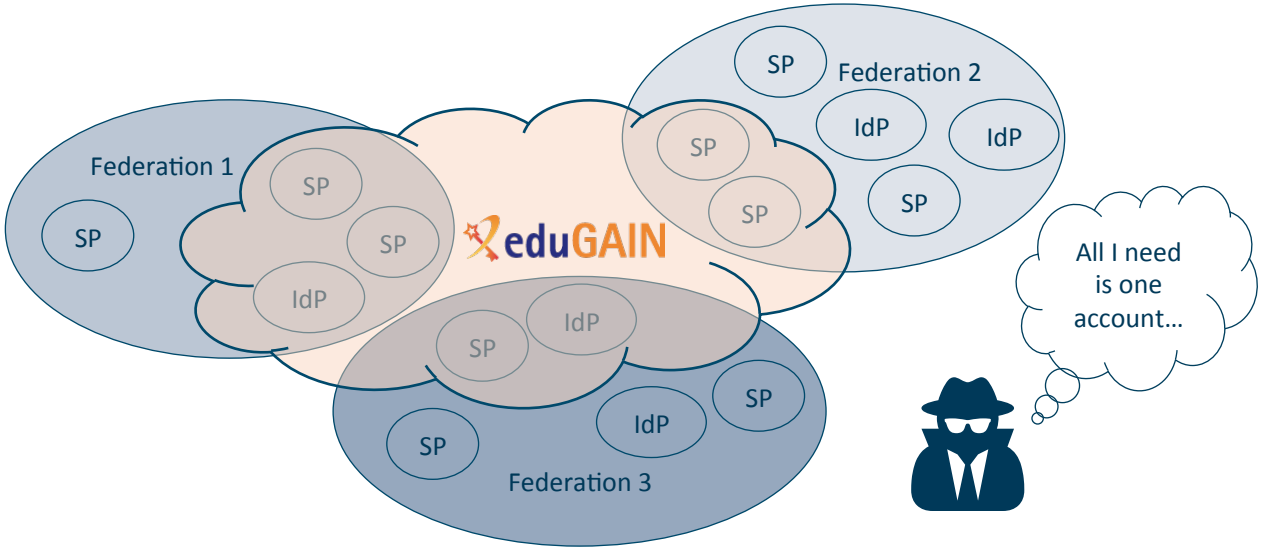
Policy and best practices harmonisation
The chain of assurance



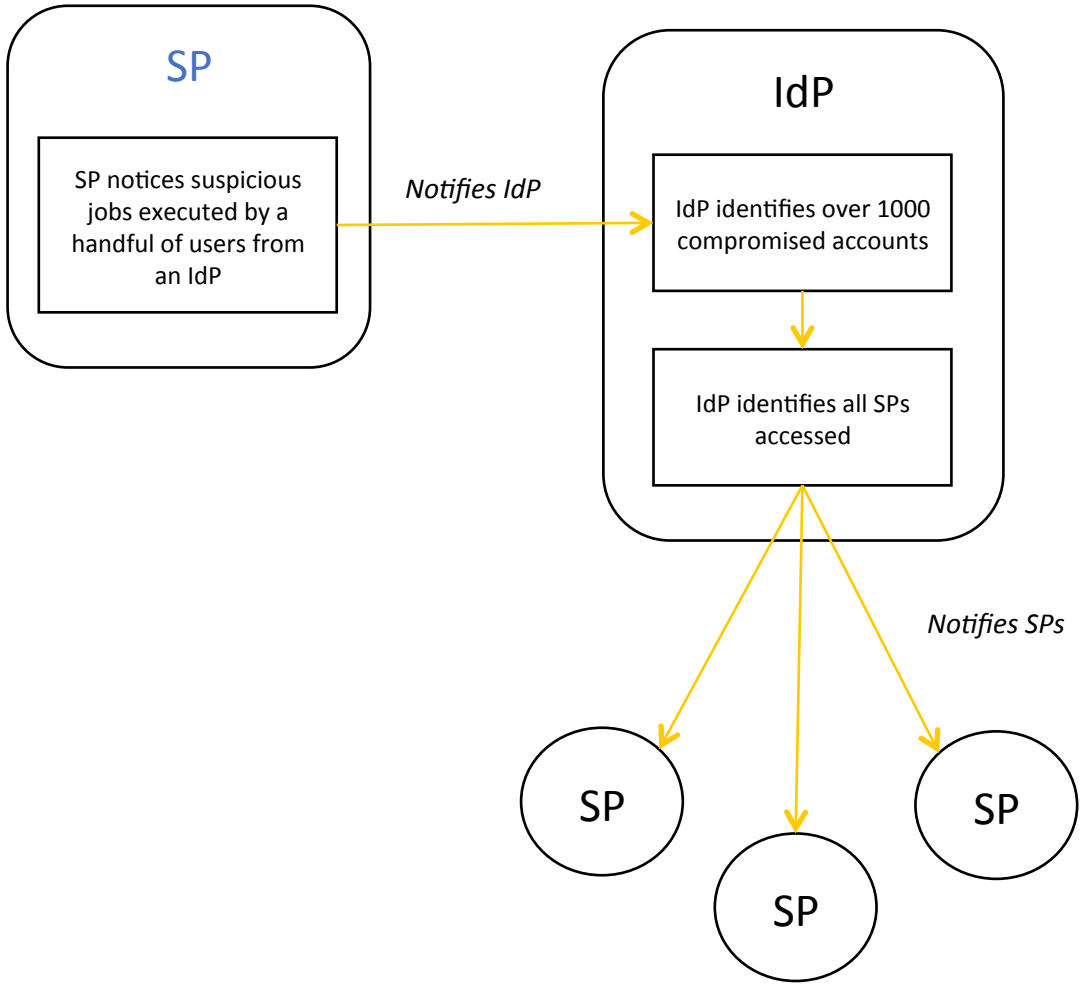
Credit to David Groep (Nikhef) for this slide

Security Incident Response
The problem

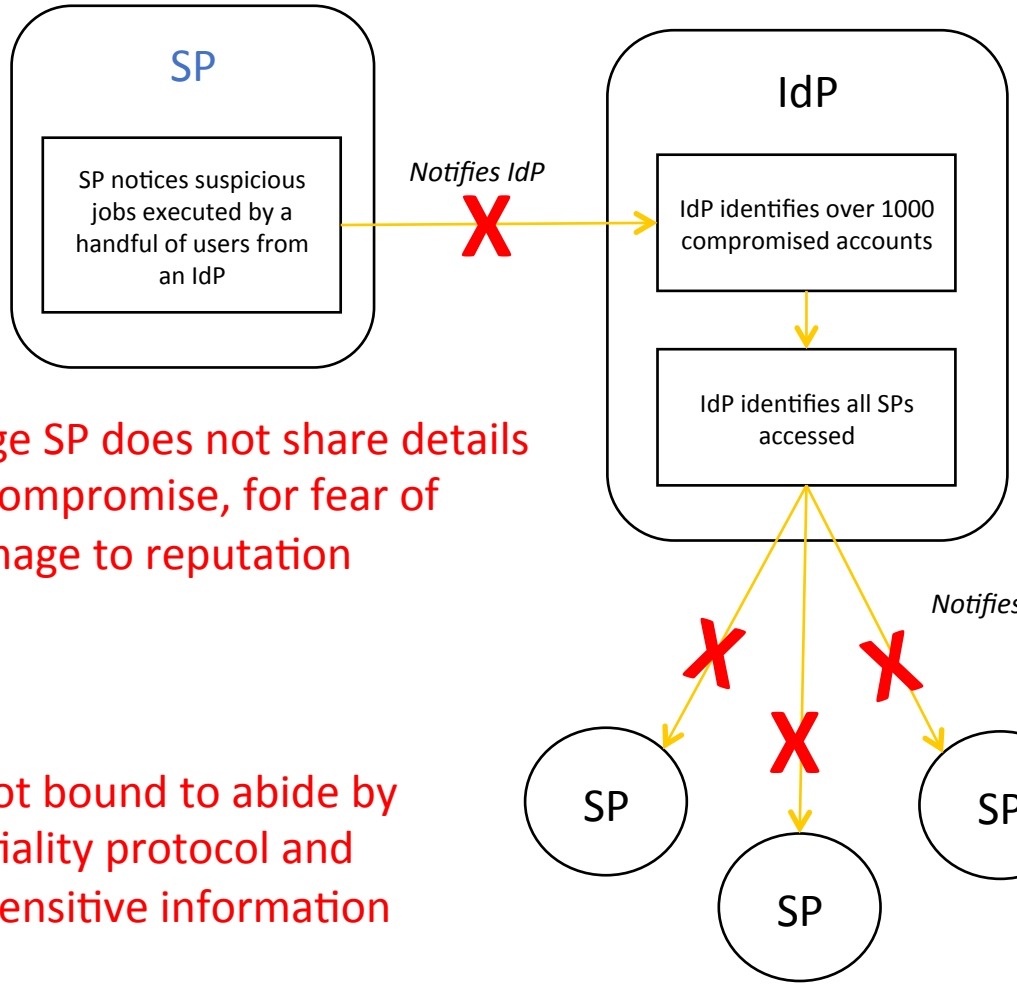
- Clearly an inviting vector of attack
- The lack of a centralised support system for security incident response is an identified risk to the success of eduGAIN
- We will need participants to collaborate during incident response – this may be outside their remit



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

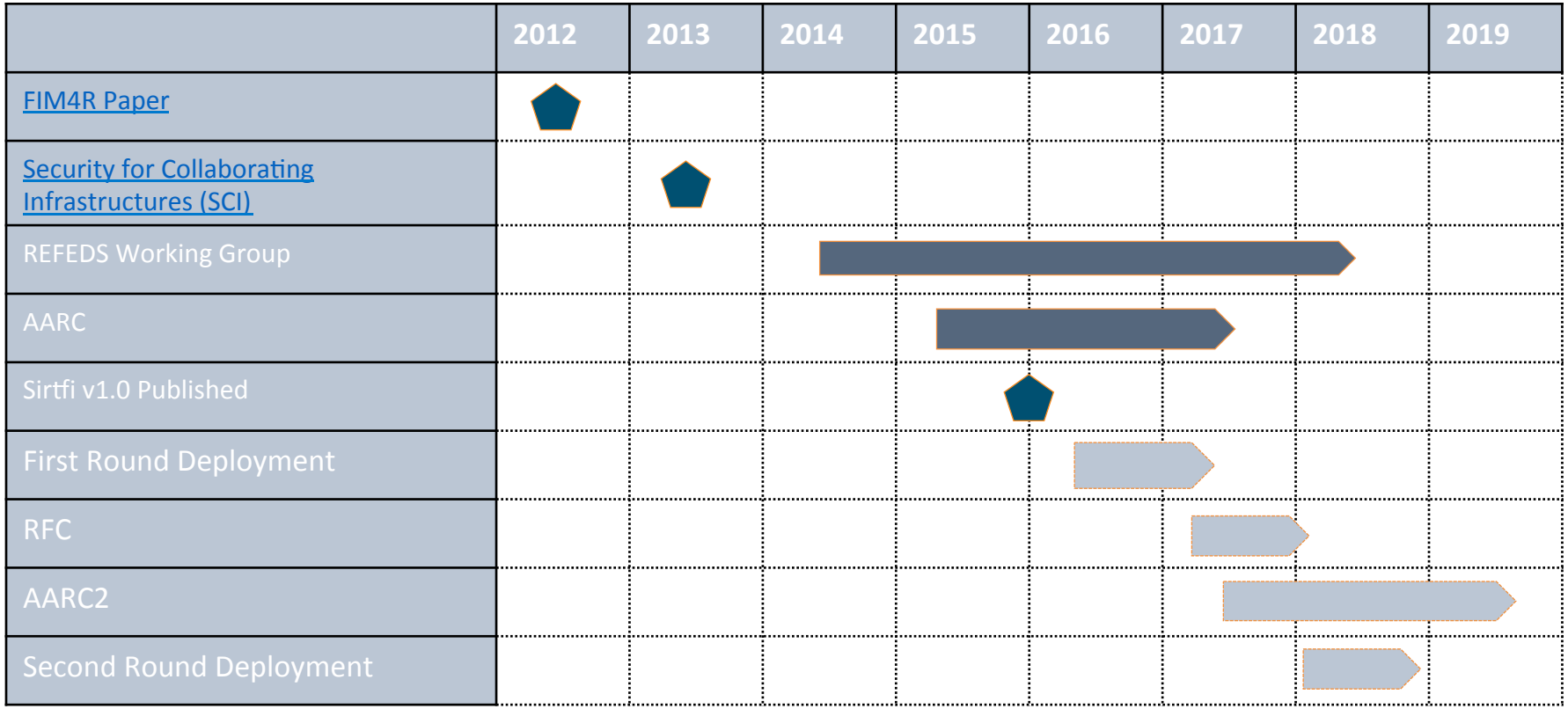
No security contact details!

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."

Credit to David Kelsey (STFC) for this content

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 SCIENCE

A Trust Framework for Security Collaboration among Infrastructures

David Kelsey[1]
STFC Rutherford Appleton Laboratory
Harwell Oxford, Didcot OX11 0QX, UK
E-mail: david.kelsey@stfc.ac.uk

Keith Chadwick, Irwin Gaines
Fermilab
P.O. Box 500, Batavia, IL 60510-5011, USA
E-mail: chadwick@fnal.gov, gaines@fnal.gov

David L. Groep
Nikhef, National Institute for Subatomic Physics
P.O. Box 41882, 1009 DB Amsterdam, The Netherlands
E-mail: davidg@nikhef.nl
http://orcid.org/0000-0003-1026-6606

Urpo Kaila
CSC - IT Center for Science Ltd.
P.O. Box 405, FI-02101 Espoo, Finland
E-mail: Urpo.Kaila@csc.fi

Christos Kanellopoulos
GRNET
56, Mesogion Av. 11527, Athens, Greece
E-mail: skanct@admin.grnet.gr

James Marsteller
Pittsburgh Supercomputer Center
300 S. Craig Street, Pittsburgh, PA 15213, USA
E-mail: jam@psc.edu

[1] Speaker

PoS(ISGC 2013)011

- Proceedings of the ISGC 2013 conference http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

Credit to David Kelsey (STFC) for this slide

Security Incident Response
Sirtfi

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

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

Security Incident Response
Sirtfi

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

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>
```


Credit to David Groep (Nikhef) for this slide

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

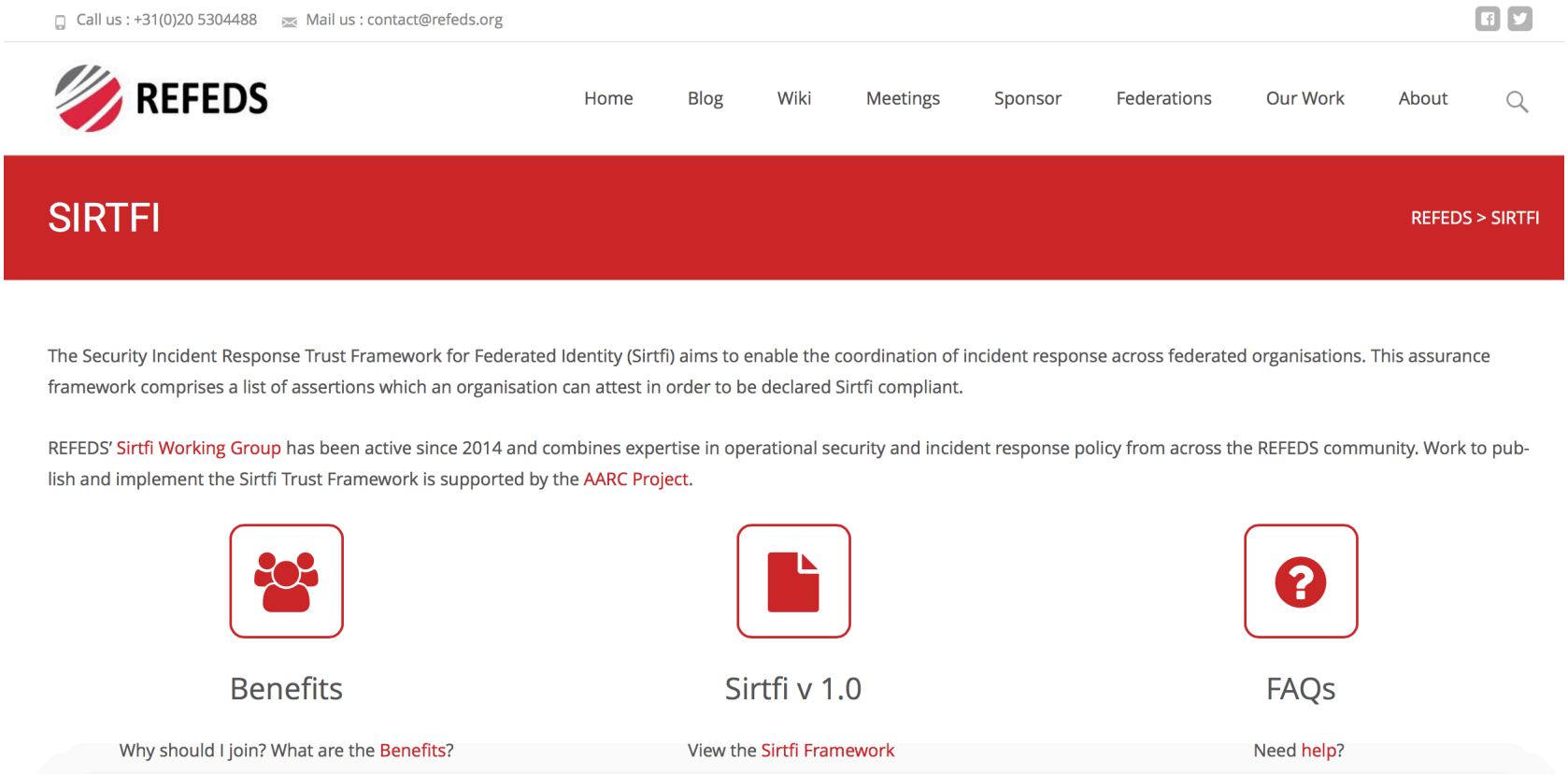
IdPs
Gain **access** to useful services that only allow authentication from Sirtfi compliant IdPs

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

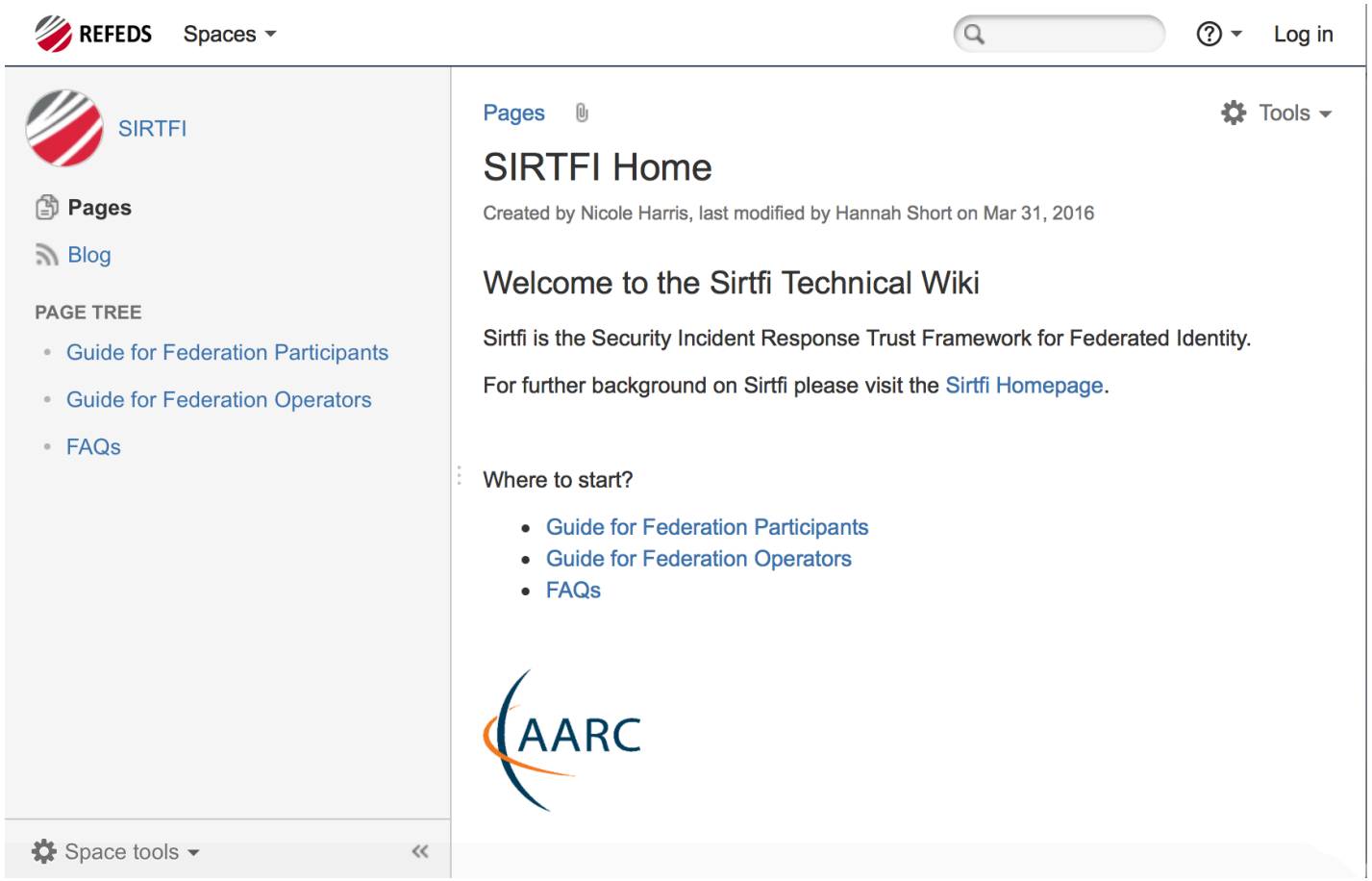
Raise the bar in operational **security** across eduGAIN

Security Incident Response
Find out more – Home Page



https://refeds.org/sirtfi

Security Incident Response
Find out more – Technical Wiki

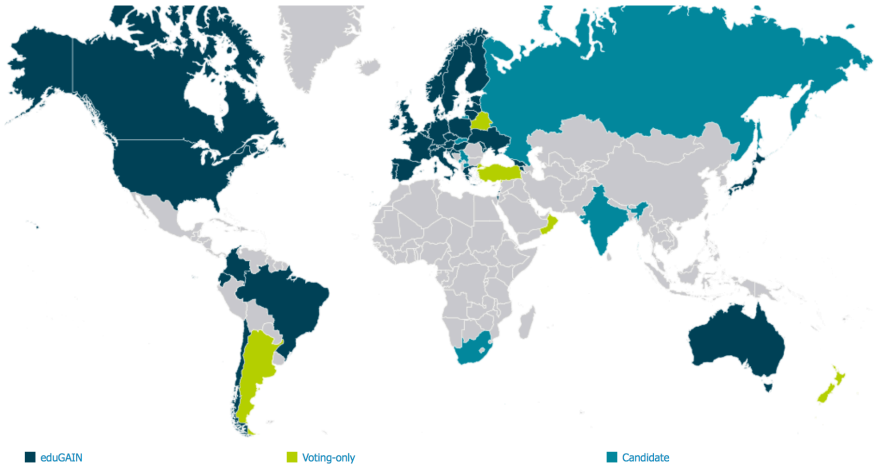


https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home

Recording Adoption
Self Assessment

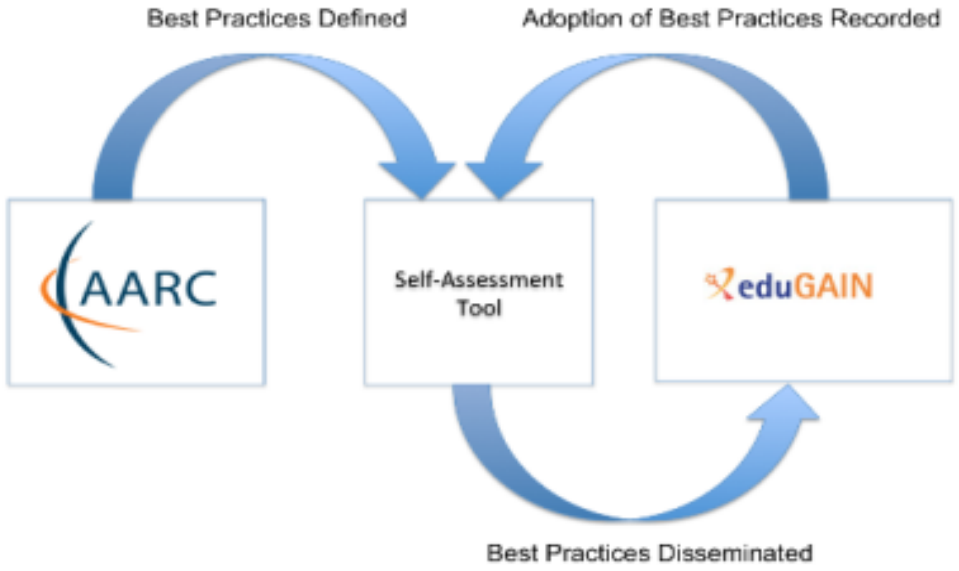
- Communities are happy with self assessment as long as the group is relatively small
- The eduGAIN world is not small!
- Some use cases require peer review
- At a larger scale automation will be necessary
- How do we ensure the correct people complete the assessment?

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 scales
- Unclear how this tool will be developed, looking to the next round of AARC and GEANT Projects



* https://docs.google.com/document/d/10kguCdxWn38z_EGRnrdjCI4GSeO44zFGeXWHGmzz27o

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

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).