



Authentication and Authorisation for Research and Collaboration

Sirtfi

Addressing Federated Security Incident Response

Hannah Short

CERN, Computer Security
hannah.short@cern.ch



GDB ISGC Taipei
March 8th 2017

Agenda



Federated Security Incident Response

- The problem
- The solution

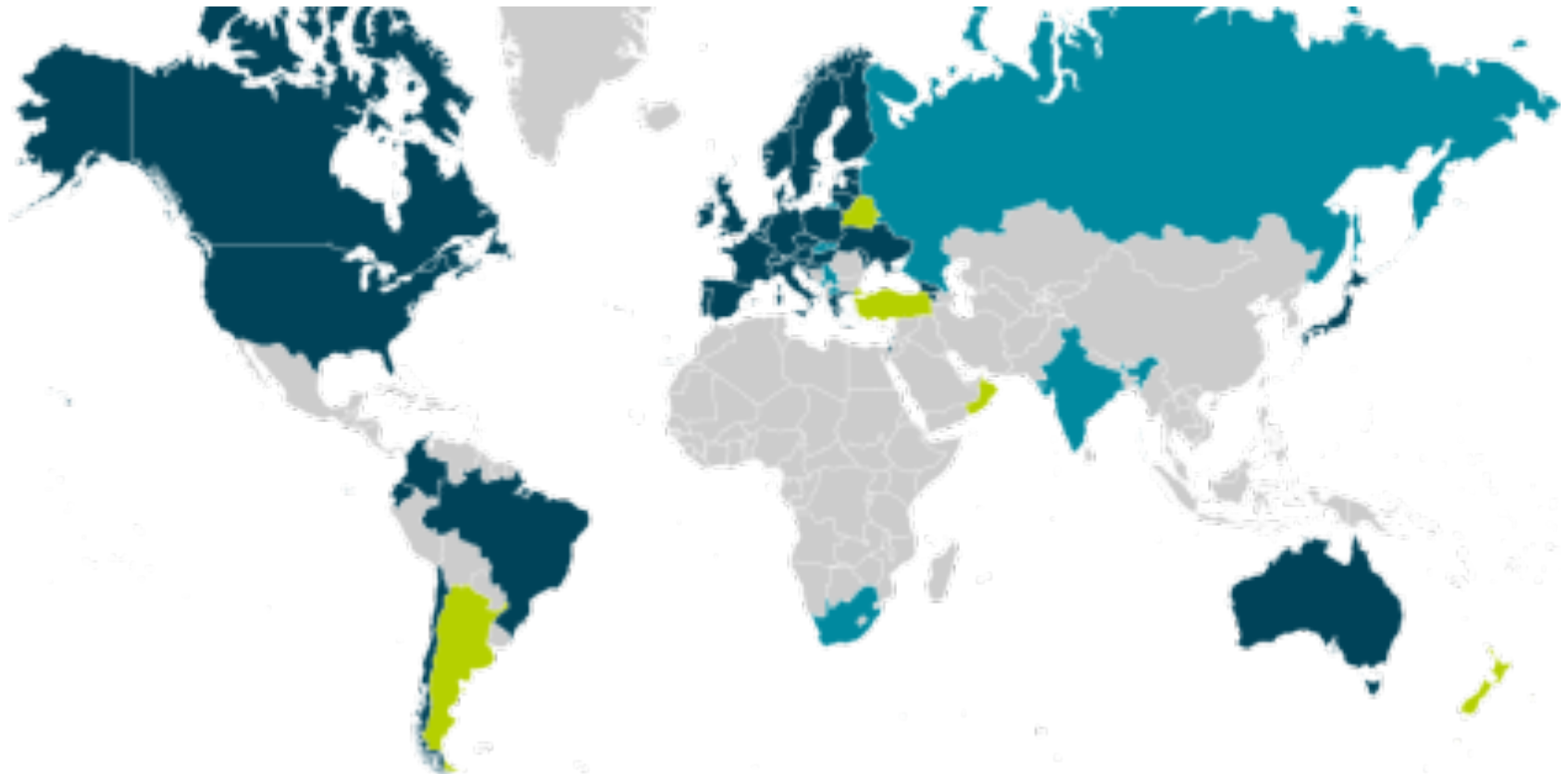
A Security Incident Response Trust Framework for Federated Identity

- A history
- Trust Framework Requirements

Why does this affect WLCG?

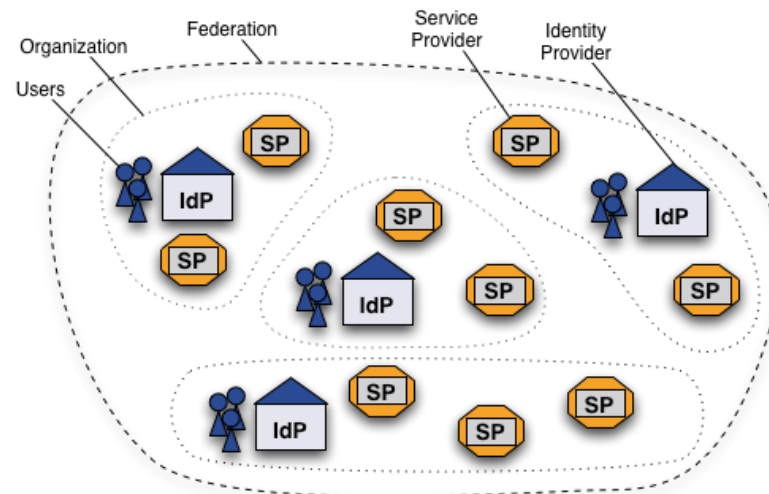
What if...?

... an incident spread throughout the federated R&E community via a single compromised identity?



What is a Federation?

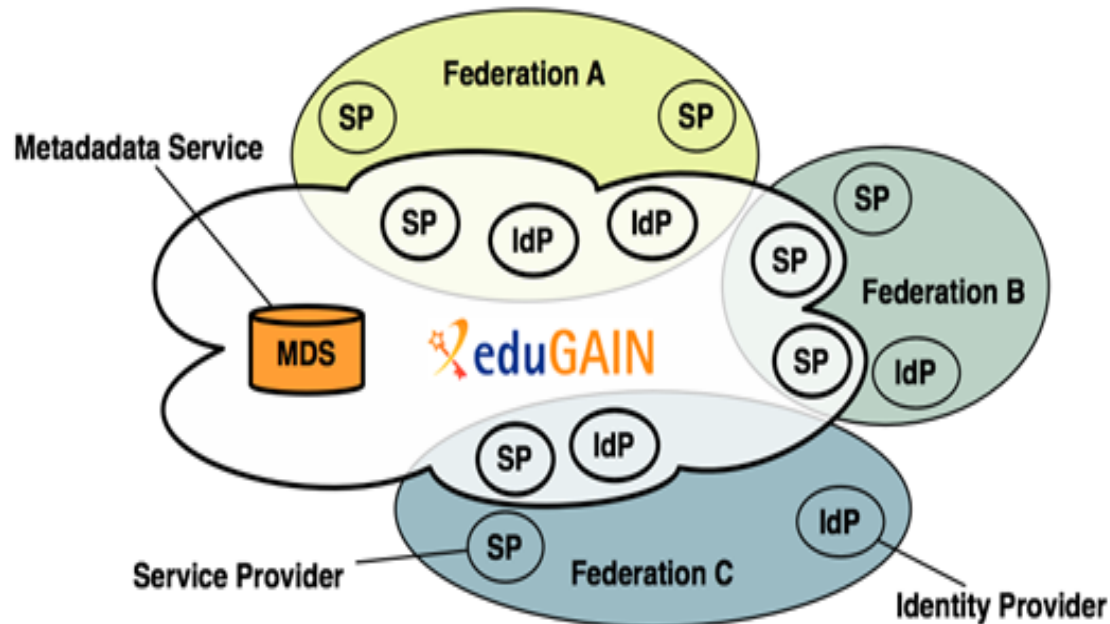
- Federated Identity Management (**FIM**) is the concept of groups of Service Providers (**SPs**) and Identity Providers (**IdPs**) agreeing to interoperate under a set of policies
- Federations are typically established nationally and use the SAML 2.0 protocol for information exchange
- Each entity within the federation is described by metadata



<https://www.switch.ch/aai/about/federation/>

What is eduGAIN?

- eduGAIN is a form of interfederation
- Participating federations share information (metadata) about entities from their own federation with eduGAIN
- eduGAIN bundles this metadata and publishes it in a central location.



-
- As WLCG adopts federated access, it becomes a just small player in eduGAIN
 - Hidden behind the CERN SP proxy
 - From the eduGAIN perspective, the CERN SP Proxy appears like any other SP, complexity and maturity of resources are not broadcast
 - We are susceptible to eduGAIN's weaknesses
 - We have less control over credential management than IGTF
 - No central blocking mechanism
 - No influence over federation governance
 - We are exposed to a new attack surface

Federated Security Incident Response

What if...?



- How could we determine the scale of the incident?
 - Do useful logs exist?
 - Could logs be shared?
- Who should take responsibility for resolving the incident?
- How could we alert the identity providers and service providers involved?
- Could we ensure that information is shared confidentially, and reputations protected?

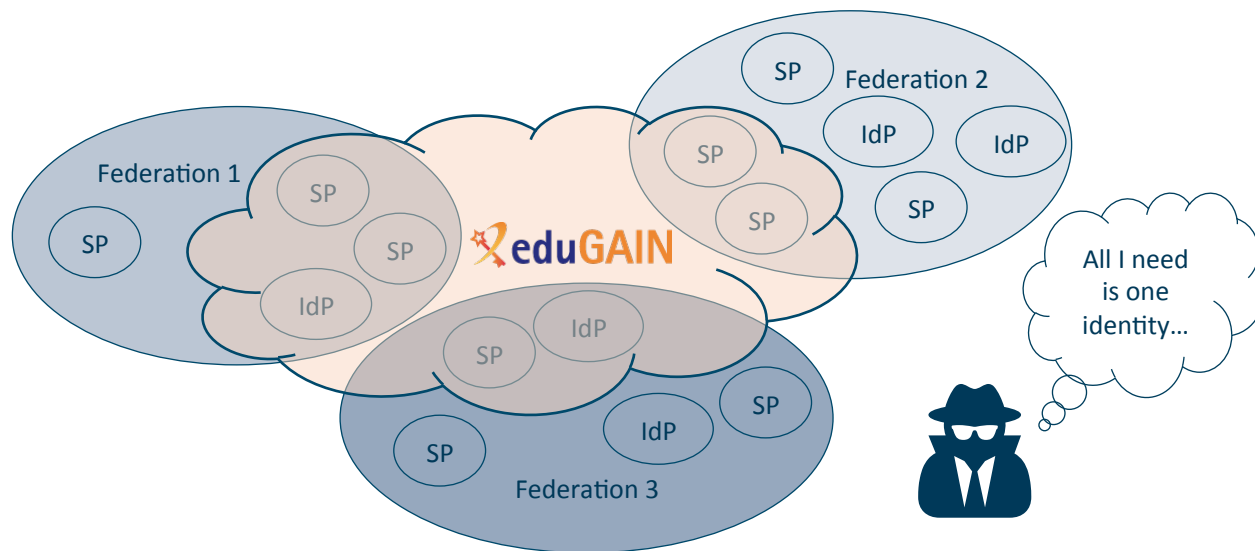
eduGAIN numbers	
Federations:	41
All entities:	3797
IdPs:	2341
SPs:	1461
Standalone AAs:	3

Data valid as of March 2017

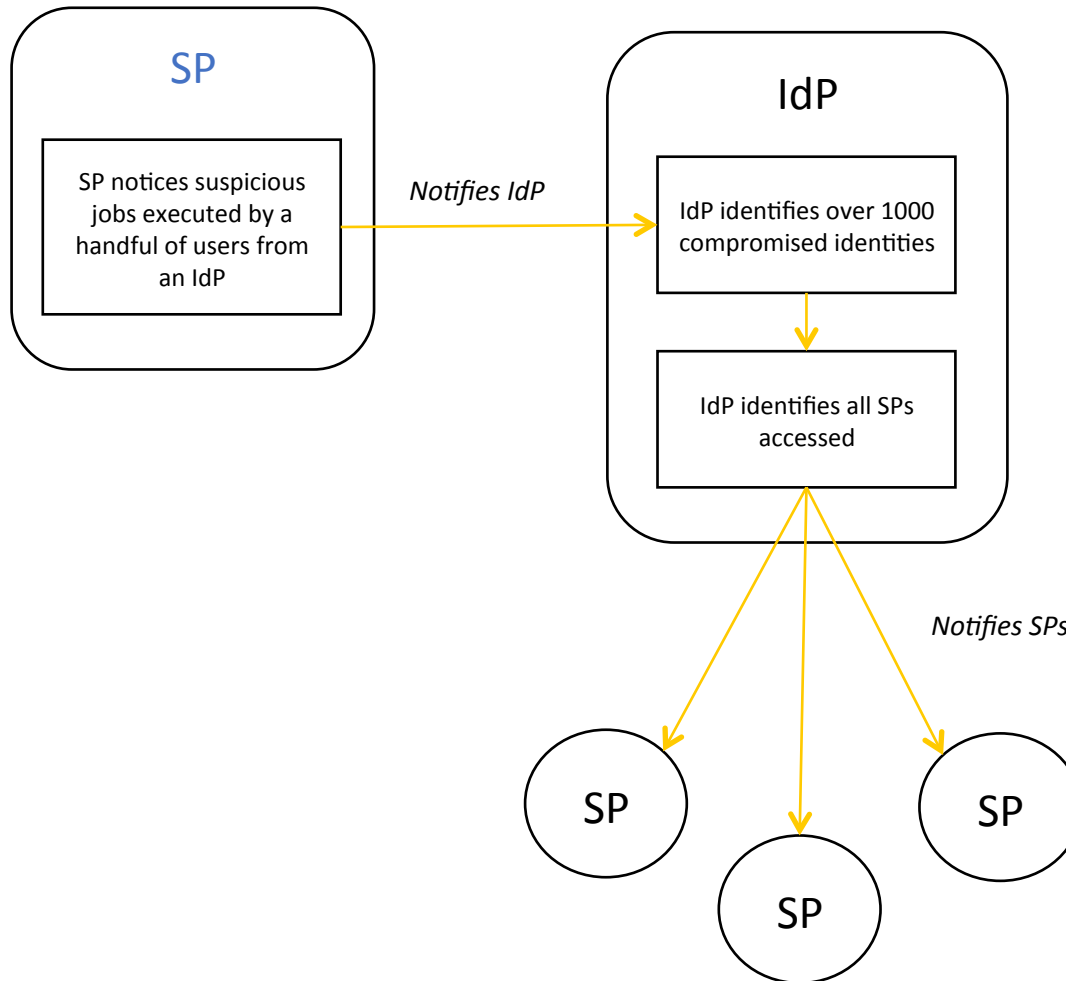
Federated Security Incident Response

The problem

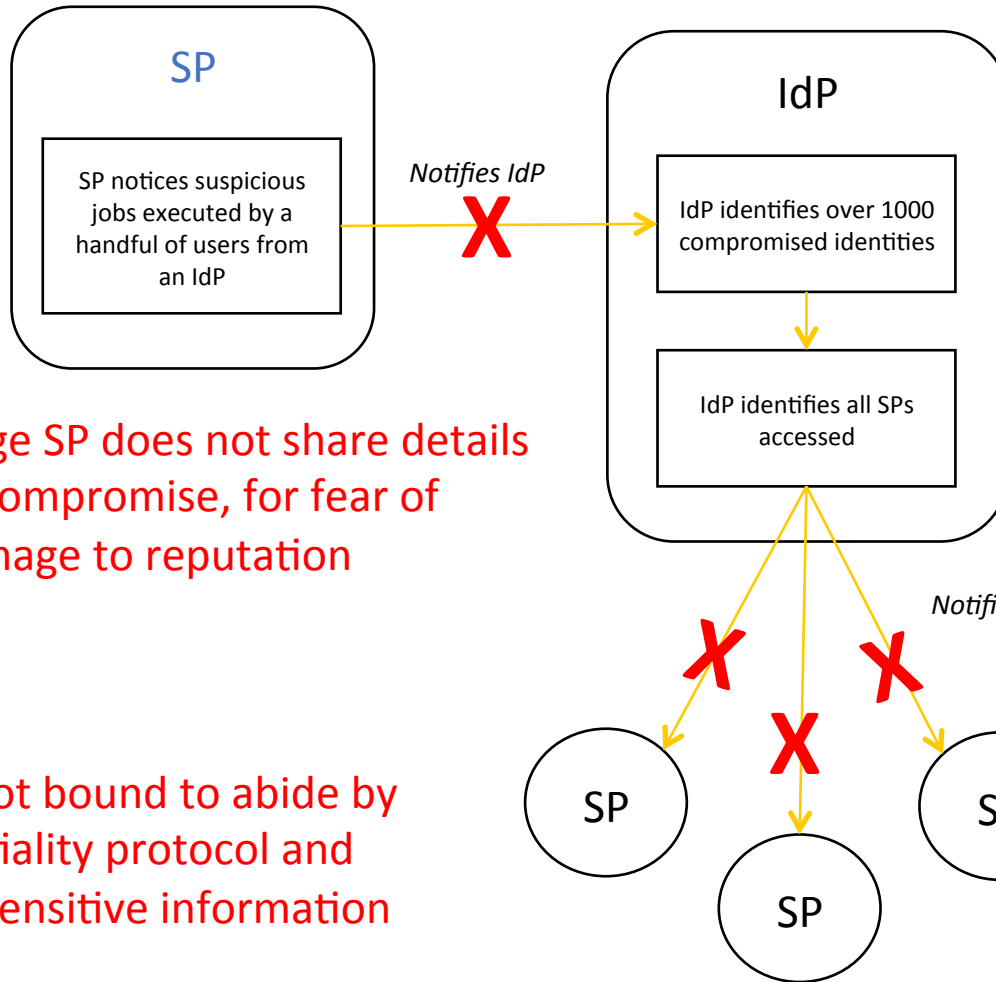
- An inviting possibility for malicious actors
- We will need participants to collaborate during incident response – this may be outside their remit



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!



Federated 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!

A Security Incident Response Trust Framework

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.”*

A Security Incident Response Trust Framework 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



A Security Incident Response Trust Framework

Sirtfi status



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

This framework has been approved by the REFEDS Community and registered as an assurance profile by the Internet Assigned Numbers Authority (IANA)

<https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml>

A Security Incident Response Trust Framework

Sirtfi summary



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

Who is in?



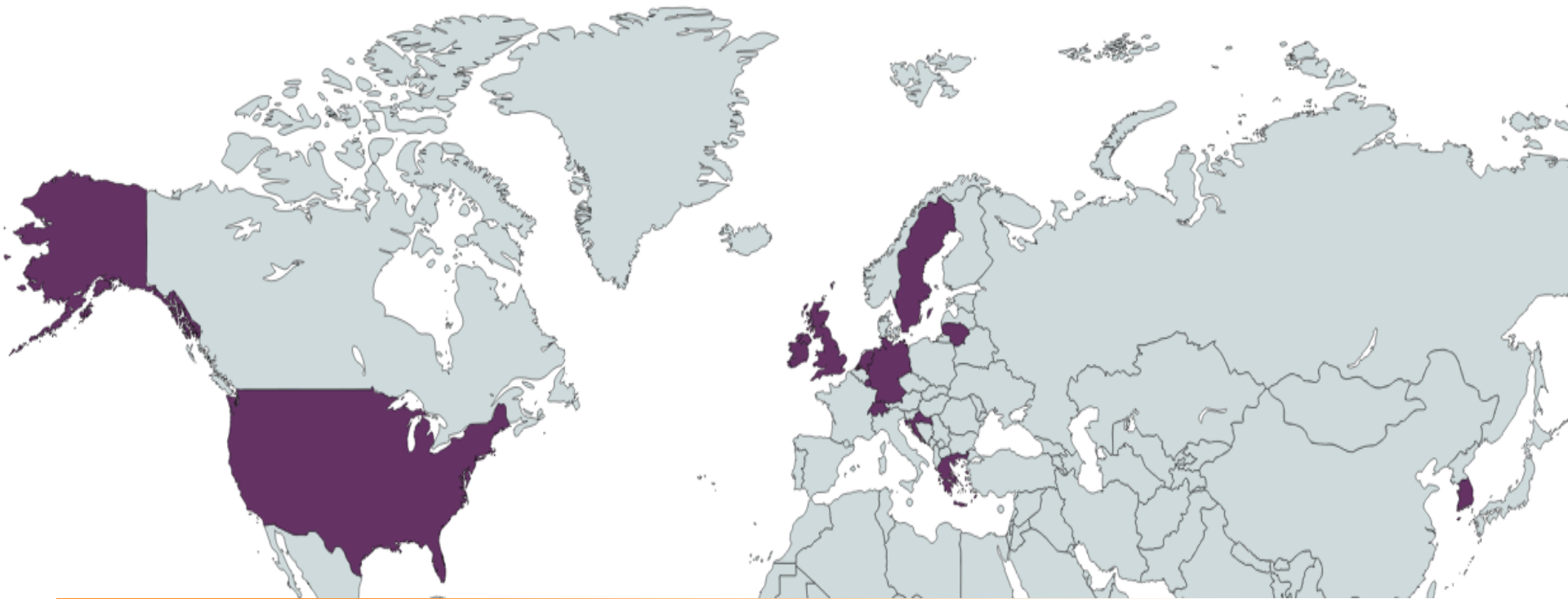
Who?	SP	IdP	Federation
Role	I provide services to researchers, with identities historically controlled by providers I know and trust	I give my researchers an identity to grant access to remote services	Allows SPs and IdPs to interoperate
Impact of eduGAIN	eduGAIN provides a pool of identities from providers that I may not know, and over whom I have no authority	EduGAIN lets my researchers access services that I may not know or trust	EduGAIN allows my SPs/IdPs to interact with entities outside my control
Why Sirtfi?	I can use Sirtfi to identify trustworthy identities, and establish a channel of communication with their providers in case of a security incident	I can use Sirtfi to know that my users are accessing secure services, and establish a channel of communication with those services in case of a security incident	I can use Sirtfi to protect my members, ensure that they are operating good security practices and are able to participate in incident response

Disclaimer: this is written at a time when there is only one global interfederation, eduGAIN

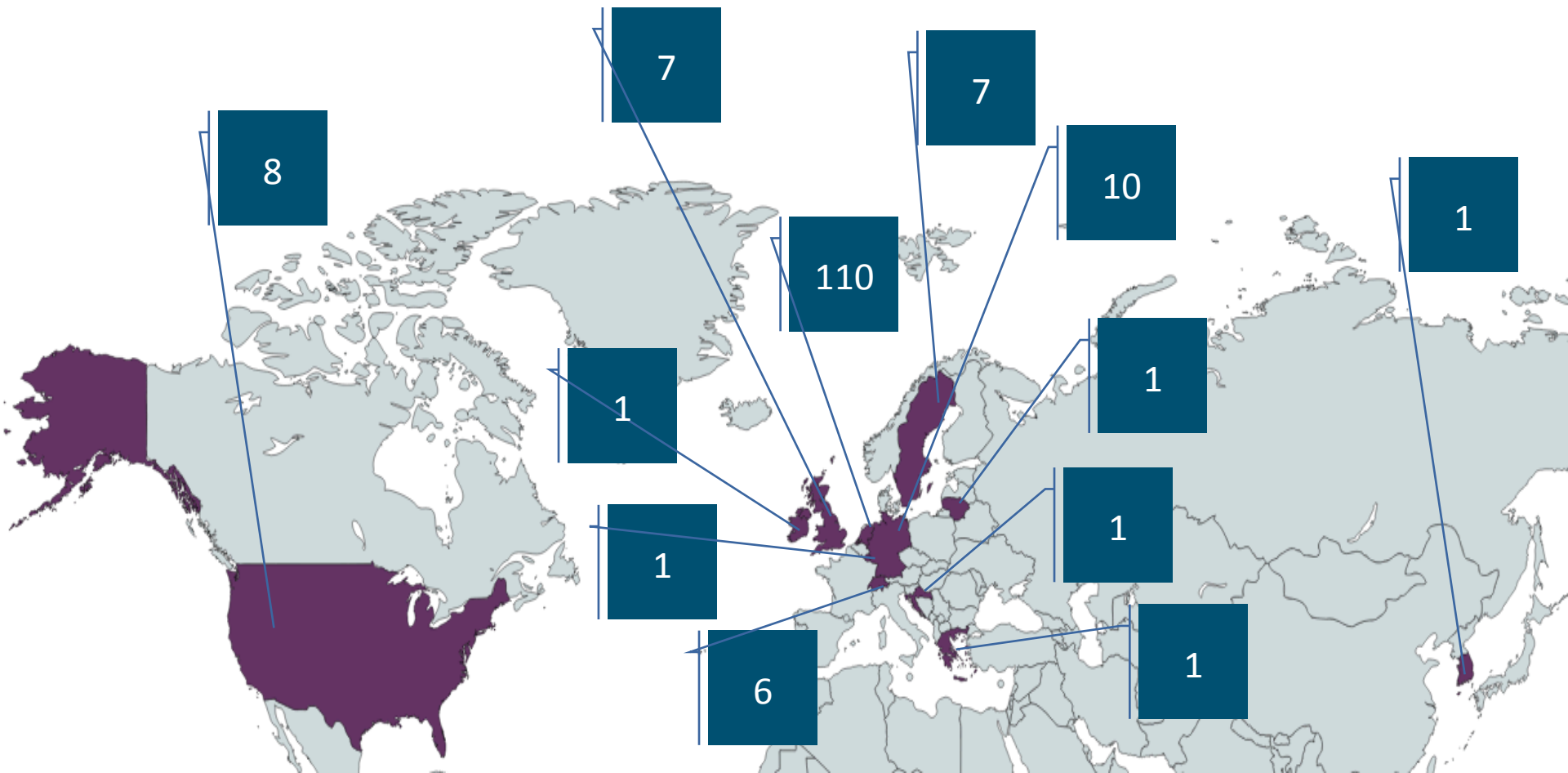
Why are we in?

Who?	Sp	IdP	Federation	EduGAIN
SP	I should adopt Sirtfi to advertise that I am a secure service (encourage IdPs to trust me), and to broadcast my security contact information	I would like SPs to adopt Sirtfi so that I know my users are accessing secure sites, and to provide a contact point for incident handling	I would like IdPs & SPs in my federation to adopt Sirtfi to reflect the level of security provided by my constituents and to enable me to handle security incidents efficiently and effectively.	We want security incident response to work, to maintain the trust that eduGAIN participants have in eduGAIN
IdP	I would like IdPs to adopt Sirtfi so that I can identify trustworthy sources of identity to grant access to my critical infrastructure, and to provide a contact point for incident handling	I should adopt Sirtfi to advertise that I am a source of identities covered by good security practices, and to provide a contact point for incident handling		

Adoption since April 2016



Adoption since April 2016



How to adopt Sirtfi

A simple recipe

- Up to date instructions can be found on the Sirtfi Wiki <https://wiki.refeds.org/display/SIRTFI/Guide+for+Federation+Participants>
- All Federation Entities, including but not limited to IdPs and SPs, can adopt Sirtfi by following this simple recipe
 1. Complete a self assessment of your entity following the Sirtfi Framework (all requirements included in the appendix of this presentation)
 2. Choose a security contact and include this in federation metadata
 3. Assert Sirtfi compliance by adding a Sirtfi Entity Attribute to your metadata

Liaise closely with your Federation Operator as they will have specific processes for updating federation metadata

How to adopt Sirtfi

Find out more – Home Page



The screenshot shows the REFEDS website's Sirtfi page. At the top, there is a navigation bar with the REFEDS logo and links for Home, Blog, Wiki, Meetings, Sponsor, Federations, Our Work, and About. A search icon is also present. Below the navigation bar is a red banner with the word 'SIRTFI' in white on the left and 'REFEDS > SIRTFI' in white on the right. The main content area has a white background and contains the following text:

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](#).

Below the text are three red-bordered icons in a row: a group of three people, a document with a folded corner, and a question mark. Under each icon is a text label and a link:

- Benefits**: Why should I join? What are the [Benefits?](#)
- Sirtfi v 1.0**: View the [Sirtfi Framework](#)
- FAQs**: Need [help?](#)

<https://refeds.org/sirtfi>

How to adopt Sirtfi

Find out more – Technical Wiki



A screenshot of a web browser displaying the Sirtfi Technical Wiki homepage. The browser's address bar shows 'REFEDS Spaces'. The page header includes a search bar, a help icon, and a 'Log in' link. The left sidebar contains the Sirtfi logo, a 'Pages' section with a 'Blog' link, and a 'PAGE TREE' with links to 'Guide for Federation Participants', 'Guide for Federation Operators', 'Choosing a Sirtfi Contact', 'Sirtfi Metadata Aggregates', and 'FAQs'. The main content area is titled 'Sirtfi Home' and includes a creation date: 'Created by Nicole Harris, last modified by Hannah Short on Sep 23, 2016'. The main text reads: 'Welcome to the Sirtfi Technical Wiki. Sirtfi is the Security Incident Response Trust Framework for Federated Identity. For background information on Sirtfi please visit the Sirtfi Homepage. Where to start? • Guide for Federation Participants • Guide for Federation Operators • Choosing a Sirtfi Contact • Sirtfi Metadata Aggregates • FAQs. Looking for a quick overview? This presentation introduces the motivation for and implementation of Sirtfi.' Below the text is a thumbnail for a presentation titled 'An introduction to Sirtfi' with the AARC logo and text 'Authentication and Authorisation for Research and Collaboration'.

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

Why does this affect me?

- CERN has implemented a requirement that eduGAIN IdPs must be Sirtfi compliant to have access
- This includes everything behind CERN's Single-Sign-On
 - WLCG web services
 - Security MISP instance <https://misp.cern.ch>

CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

Sign in with your CERN account


Reminder: you have agreed to comply with the CERN computing rules


Use credentials

Username or Email address Password

Remember Username or Email Address [Need password help ?](#)


Use one-click authentication

 [Sign in using your current Windows/Kerberos credentials \[autologon\]](#)
Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC (Firefox help here).


 [Sign in using your Certificate \[autologon\]](#)
Use a EuGridPMA trusted certificate. Don't forget to first map your Certificate to your CERN Account.

Use strong two factor authentication [show]

Sign in with a public service account

 [Facebook, Google, Live, etc.](#)
Authenticate using an external account provider such as Facebook, Google, Live, Yahoo, Orange.

Sign in with your organization or institution account



Why is my organisation not listed?

Related sites

- ◆ [Need password help ?](#)
- ◆ [Create/Check your account](#)
- ◆ [EduGain disclaimer settings](#)
- ◆ [Service Desk +41 22 76 77777](#)
- ◆ [Computing Status Board](#)
- ◆ [Connection using IPv6](#)



Thanks to those IdPs who have already asserted compliance, e.g. University of Glasgow!

Conclusions

- The Security Incident Response Trust Framework for Federated Identity (Sirtfi) has been developed to address the gap in security response capability within federated computing.
- By creating a sub-network of security conscious entities, and providing contact information for each member, the group raises its mutual trust and is able to establish contact with each other should the need arise.
- This is important for WLCG to be able to maintain the current level of security offered by the existing certificate-based federation



REFEDS

Thank you

Any Questions?

hannah.short@cern.ch



<https://aarc-project.eu>



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.