Sirtfi

Incident Response for Federations

Hannah Short (AARC & CERN)
Co-Author: Irina Mikhailava

IAMOnline EU Webinar Series
March 15th 2017 15:30 CET

Agenda

- Introduction to Sirtfi (10min)
- Added value for SPs (10min)
- Added value for IdPs (15min)
- The role of federations (15min)
- Q&A (15min)

Why?

Security is important for Researchers!

We must protect:

- Their identities
- Their research data

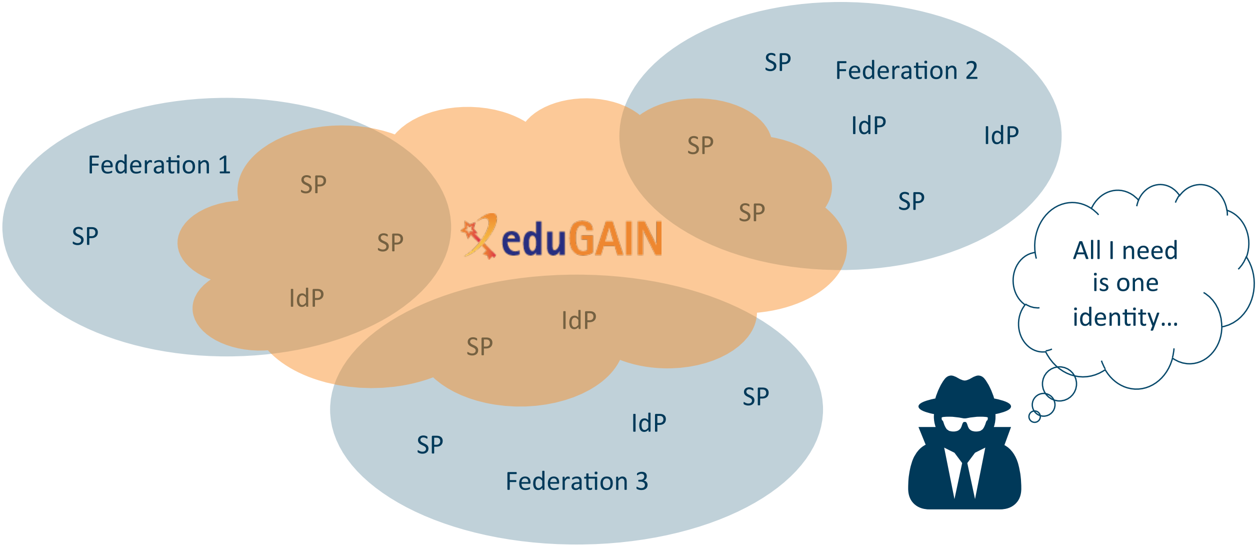
Image credit GEANT

Historically, researchers have been protected by security policies and operations within their closed communities

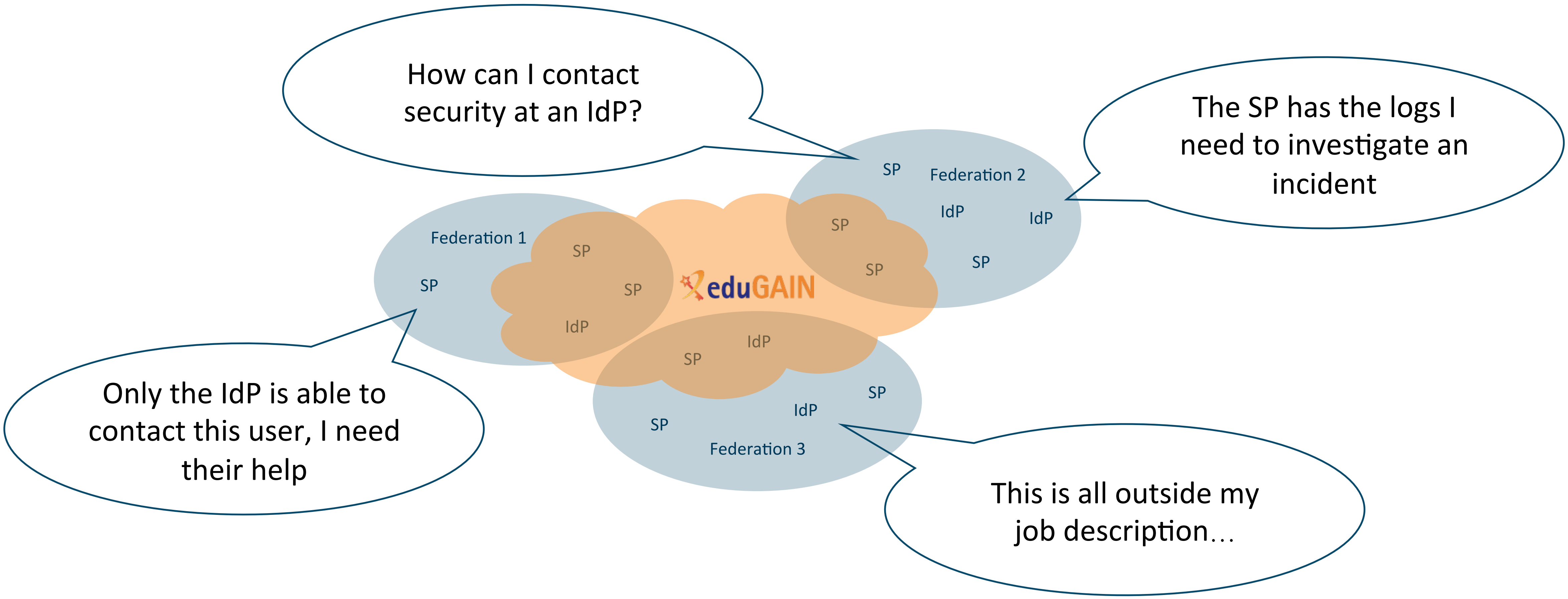
EduGAIN allows researchers to access services beyond their closed community, and enables external identities to access community owned resources

*Sirtfi is a framework to provide **security** within identity federations and interfederation, so that researchers remain **protected** outside their closed community*

Why is incident response difficult in identity federations?



Why is incident response difficult in identity federations?



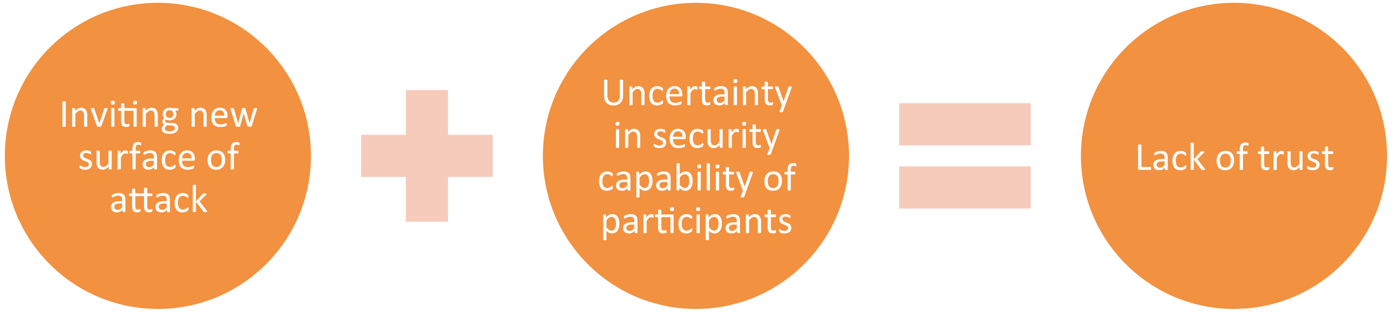
How can I contact security at an IdP?

The SP has the logs I need to investigate an incident

Only the IdP is able to contact this user, I need their help

This is all outside my job description…

Federated Security Incident Response
A Solution



Inviting new surface of attack + Uncertainty in security capability of participants = Lack of trust

- 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."*

Credit to David Kelsey (STFC) for this content

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

PoS PROCEEDINGS OF SCIENCE

A Trust Framework for Security Collaboration among Infrastructures

PoS(ISGC 2013)011

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

© Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike Licence. http://pos.sissa.it

Credit to David Kelsey (STFC) for this content

A Security Incident Response Trust Framework

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

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

What is 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

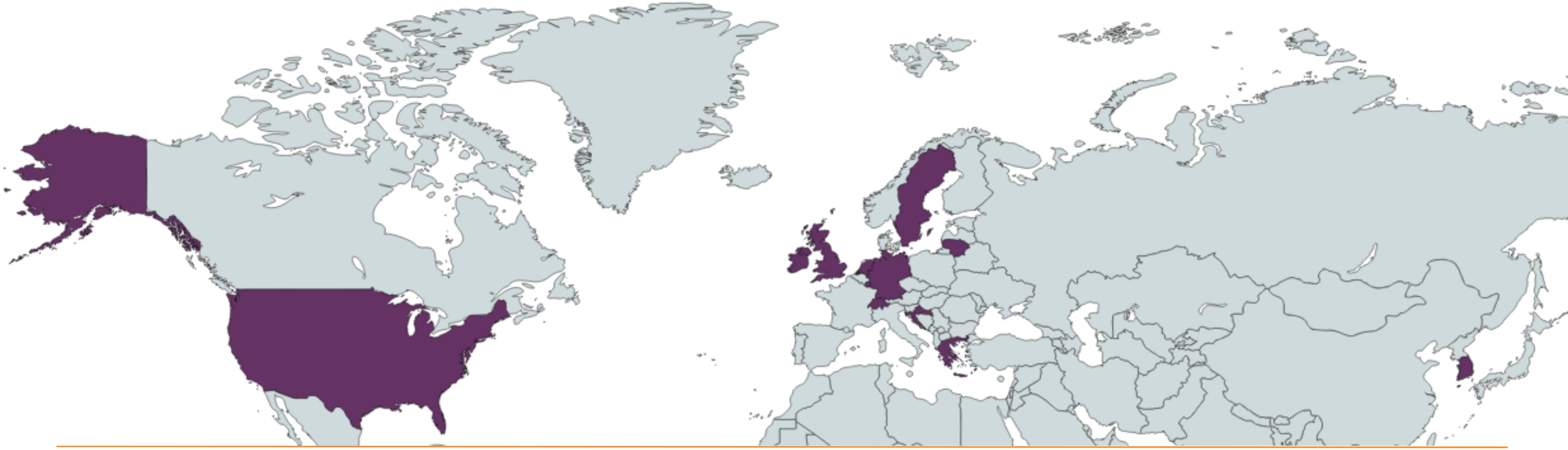
Traceability

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

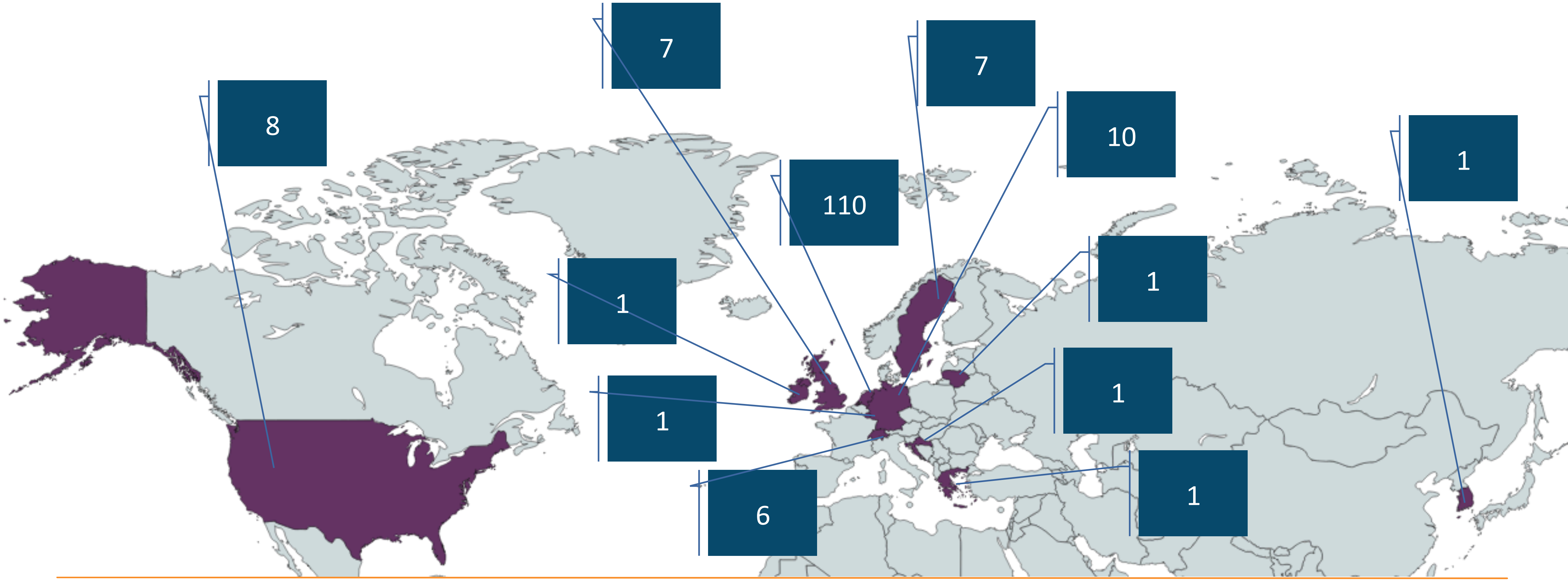
Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

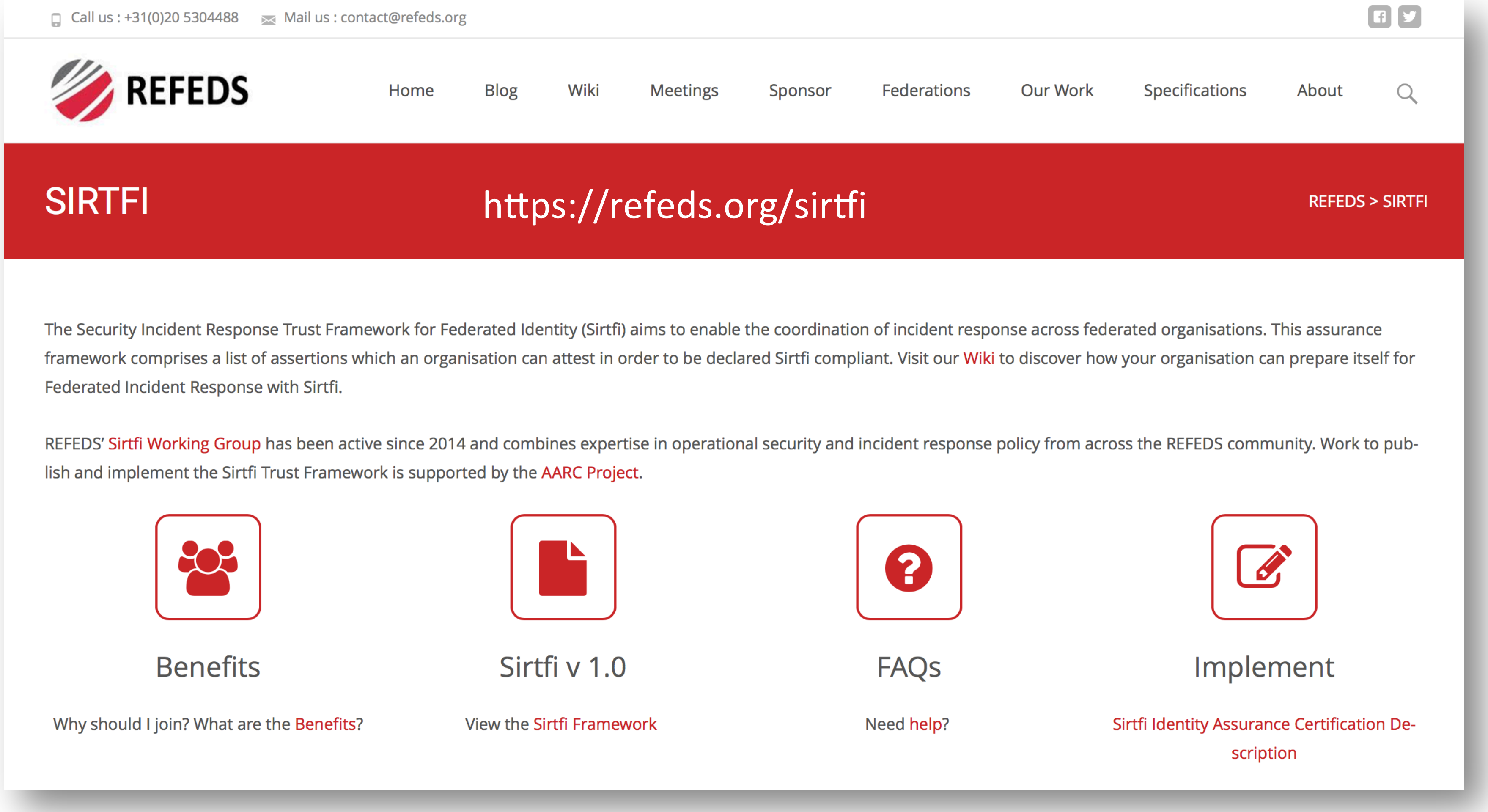
Adoption



Adoption



Find out more



SIRTFI

https://refeds.org/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. Visit our Wiki to discover how your organisation can prepare itself for Federated Incident Response with Sirtfi.

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?

Implement

Sirtfi Identity Assurance Certification Description

Added Value for SPs

Added value for SPs

Why should I adopt Sirtfi?

I should adopt Sirtfi to advertise that I am a secure service (to encourage IdPs to trust me), and to broadcast my security contact information

Added value for SPs

Why should IdPs adopt Sirtfi?

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

Use case, CERN

- Certificate based federation -> transitioning to identity federation
- We have authority over all sites (SPs) in the federation, and established channels of incident response
- We are able to suspend credentials centrally, without going to the certificate authority (IdP)

Use case, CERN

- Certificate based federation -> transitioning to identity federation
- We have authority over all sites (SPs) in the federation, and established channels of incident response
- We are able to suspend credentials centrally, without going to the certificate authority (IdP)

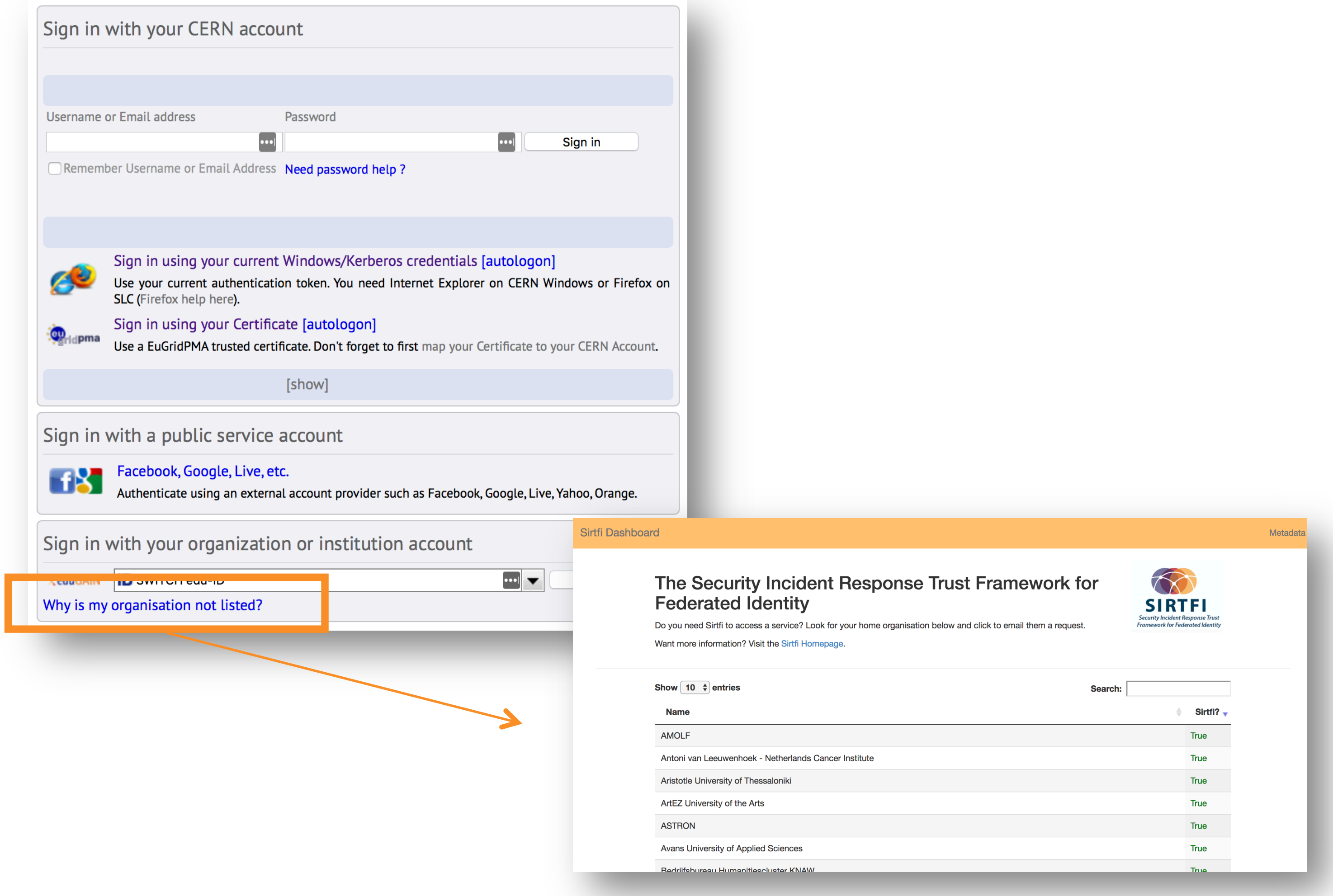
- Using eduGAIN significantly impacts the level of security we are able to offer our researchers
- There is no central blocking mechanism
- There are no established incident response channels or procedures

Use case, CERN

To ensure that we are able to offer our users and services a consistent level of security, we require that **all IdPs** accessing CERN (and our computing infrastructure, WLCG) **are Sirtfi compliant.**

Use case, CERN

- How do we benefit from Sirtfi?
  - In the event of a security incident, we are able to look up the security contacts of affected identities’ IdPs
  - We can start the incident response process
- Our obligations
  - We will respond to requests for assistance from other organisations



Sign in with your CERN account

Username or Email address

Password

□ Remember Username or Email Address

Need password help ?

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.

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

SWITCH edu-ID

Why is my organisation not listed?

The Security Incident Response Trust Framework for Federated Identity

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Do you need Sirtfi to access a service? Look for your home organisation below and click to email them a request.

Want more information? Visit the Sirtfi Homepage.

Show 10 entries

Search:

Name	Sirtfi?
AMOLF	True
Antoni van Leeuwenhoek - Netherlands Cancer Institute	True
Aristotle University of Thessaloniki	True
ArtEZ University of the Arts	True
ASTRON	True
Avans University of Applied Sciences	True
Bedrijfsbureau Humanitiescluster KNAW	True

Thank you

Any Questions?

hannah.short@cern.ch

AARC

http://aarc-project.eu/

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

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 sexrvices	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, although content should be applicable for all interfederations

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		