Authentication and Authorisation for Research and Collaboration

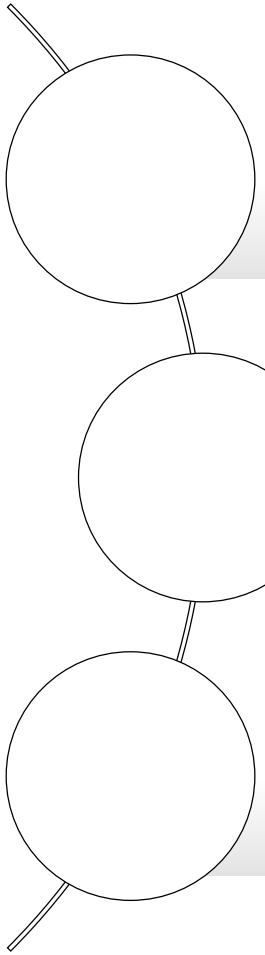
Incident Response

Sirtfi and Beyond

Hannah Short
CERN Computer Security
AARC NA3

WISE
March 27th 2017

Agenda



Incident Response in Distributed Infrastructures

Impact of Identity Federations

Filing the gaps

Incident Response in Distributed Infrastructures

Security Incident Response in Distributed Infrastructures

Shared Policies

- Written rules, and obligations
- Clear basis for exclusion from infrastructure if not followed
- Reasonable likelihood that sites follow best practices in security

Operational Support

- Incident preparation and prevention - cascade advisories, IOCs, patches etc
- Coordinate incident response across multiple Sites
- Power to block problematic Sites & users

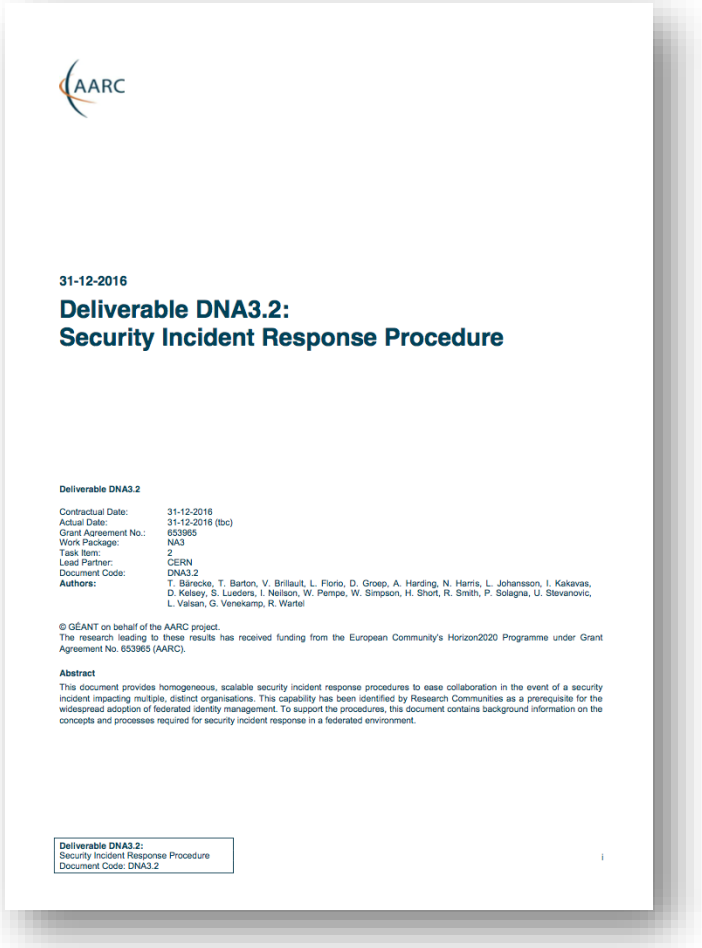
Trust

- Fundamentally, incident response is more successful when the individuals know and trust each other
- Online trust
  - Consistent, trustworthy behaviour
  - Voluntary collaboration
- Offline trust
  - Key exchange
  - Verification that you are a real person ☺

Security Incident Response Models

AARC Project Deliverable DNA3.2 provided opportunity to:

- Analyse existing models
- Consider Security Incident Response Procedures in the context of eduGAIN (stay tuned for the second part of this talk!)



31-12-2016

Deliverable DNA3.2:
Security Incident Response Procedure

Deliverable DNA3.2

Contractual Date:	31-12-2016
Actual Date:	31-12-2016 (tbc)
Grant Agreement No.:	653965
Work Package:	NA3
Task Item:	2
Lead Partner:	CERN
Document Code:	DNA3.2
Authors:	T. Bärecke, T. Barton, V. Brillault, L. Florio, D. Groep, A. Harding, N. Harris, L. Johansson, I. Kakavas, D. Kelsey, S. Lueders, I. Neilson, W. Pempe, W. Simpson, H. Short, R. Smith, P. Solagna, U. Stevanovic, L. Valsan, G. Venekamp, R. Wartel

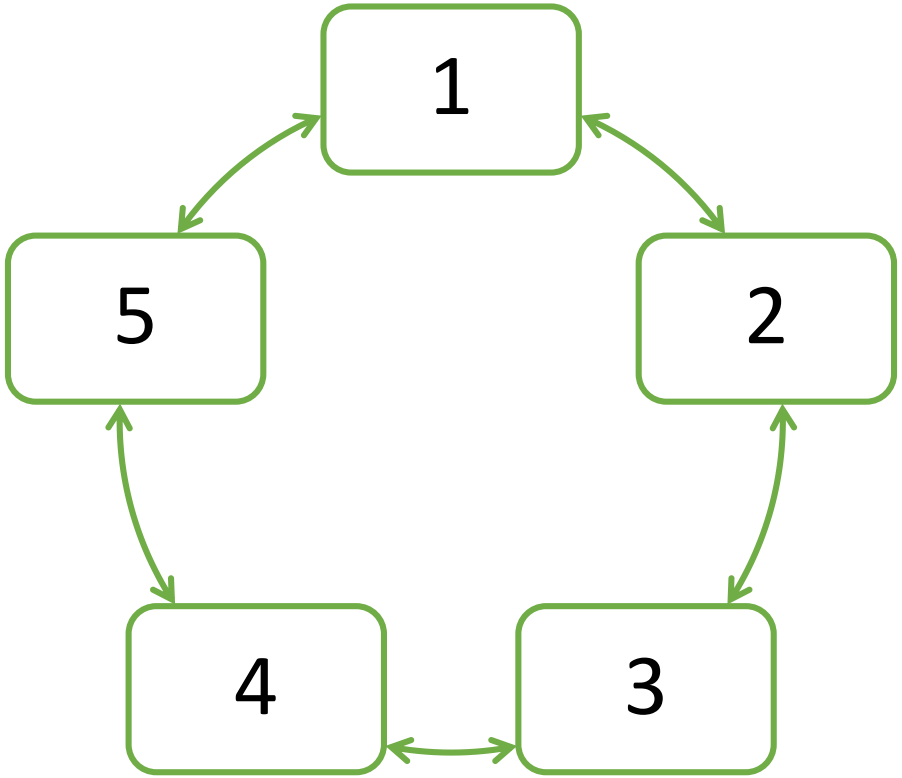
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

This document provides homogeneous, scalable security incident response procedures to ease collaboration in the event of a security incident impacting multiple, distinct organisations. This capability has been identified by Research Communities as a prerequisite for the widespread adoption of federated identity management. To support the procedures, this document contains background information on the concepts and processes required for security incident response in a federated environment.

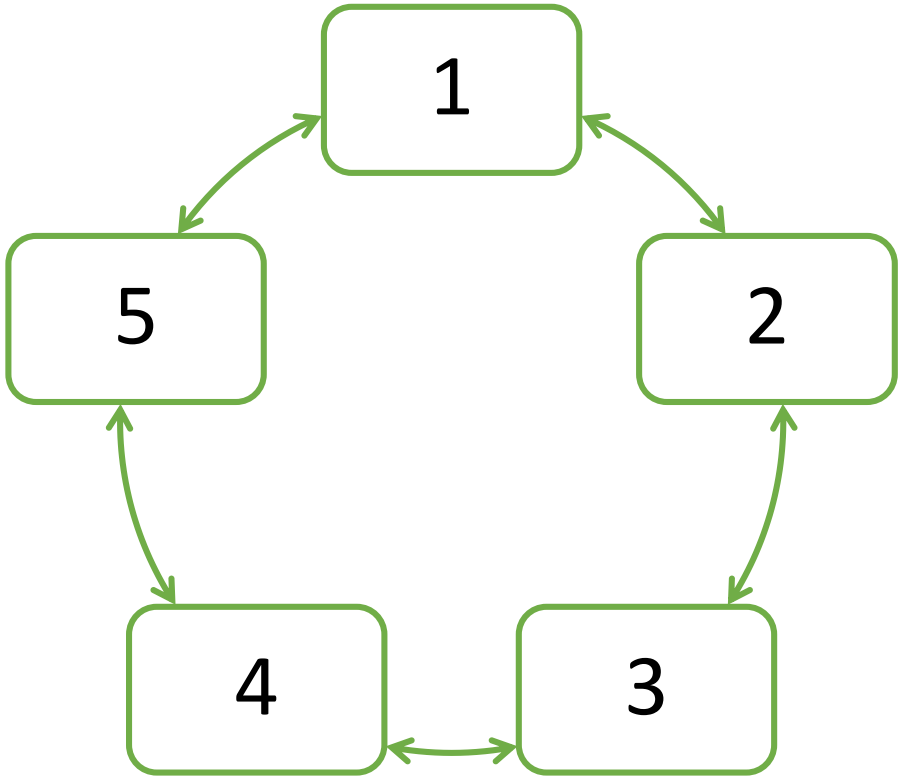
https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf

Fully Distributed Model



During Incident Response

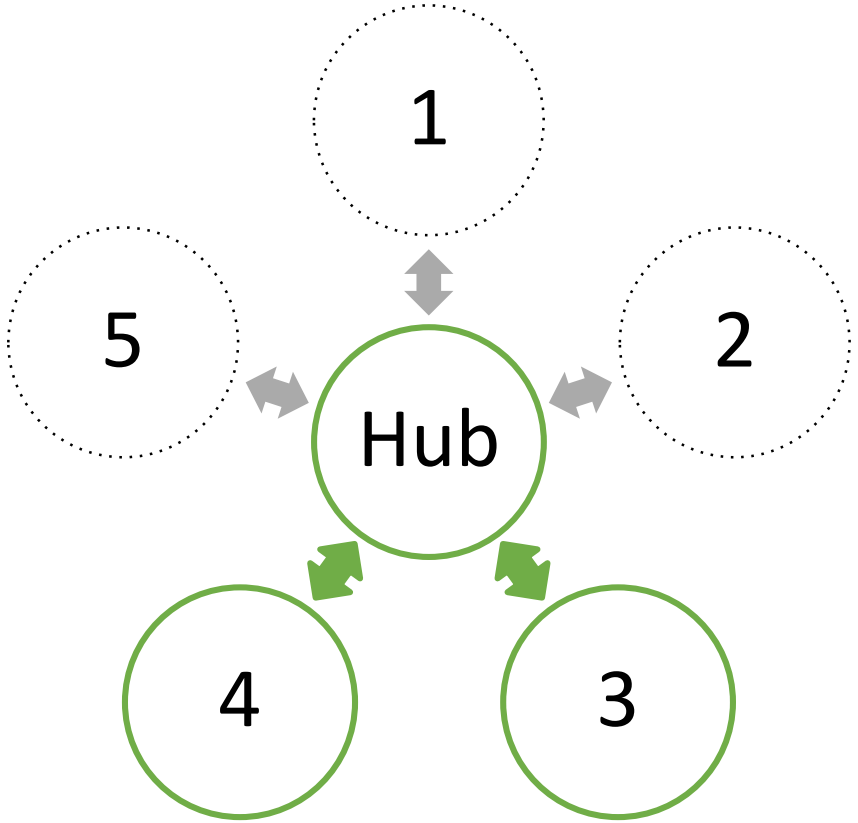
Information shared between all participants



Post-Incident-Report Sharing

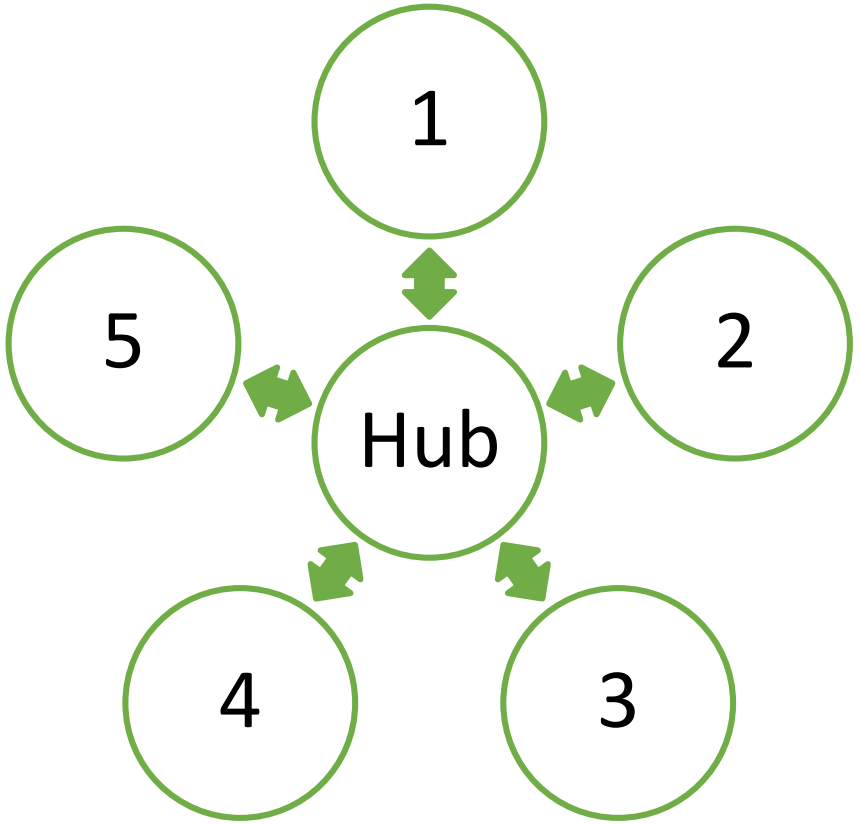
Information shared between all participants

Hub and Spoke



During Incident Response

Information shared between affected participants



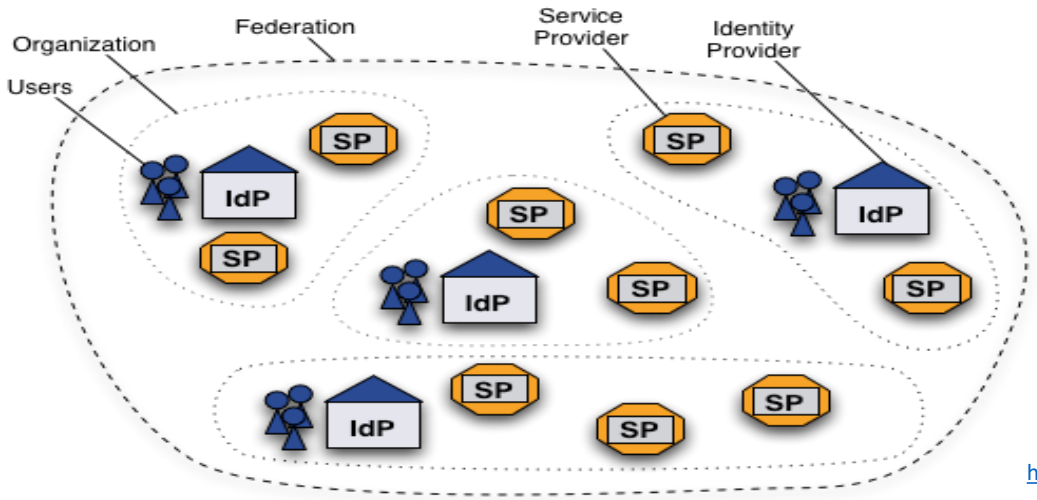
Post-Incident-Report Sharing

Information shared between all participants

Impact of Identity Federations

Federated Identity Management Worldwide
What is a Federation?

- Federated Identity Mangement (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 SAML2 protocol for information exchange
- Each entity within the federation is described by metadata

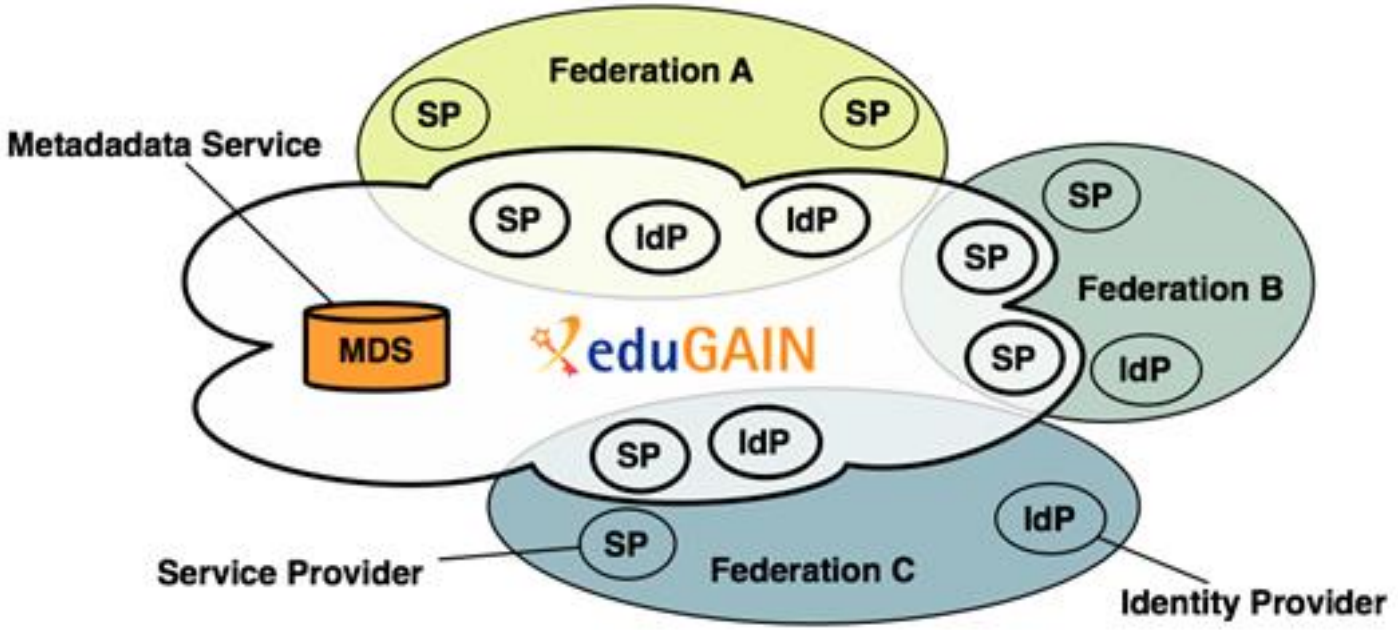


https://www.switch.ch/aai/about/federation/

Credit to Alessandra Scicchitano – GEANT for this slide

Federated Identity Management Worldwide
eduGAIN

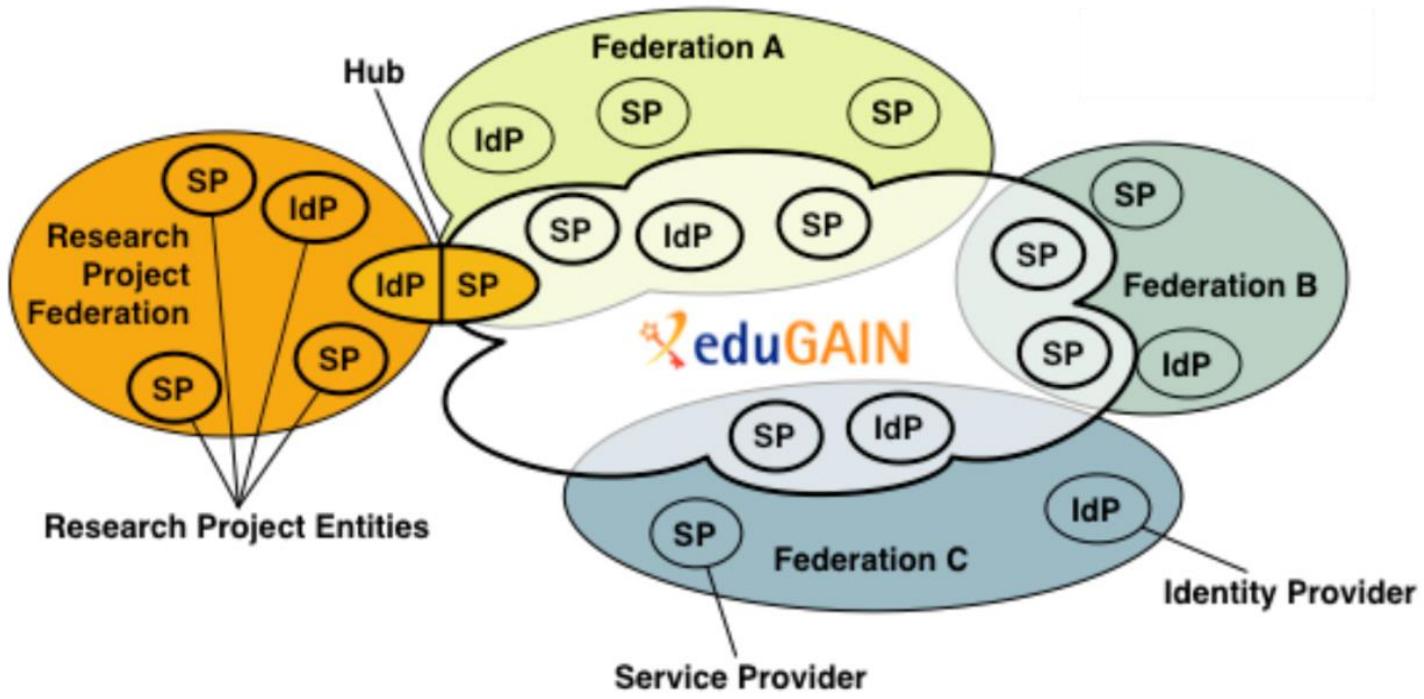
- eduGAIN is a form of interfederation
- Participating federations share information (metadata) about entities from their own federation with eduGAIN
- eduGAIN bundles this metadata and publishes it in a central location.



Credit to Alessandra Scicchitano – GEANT for this slide

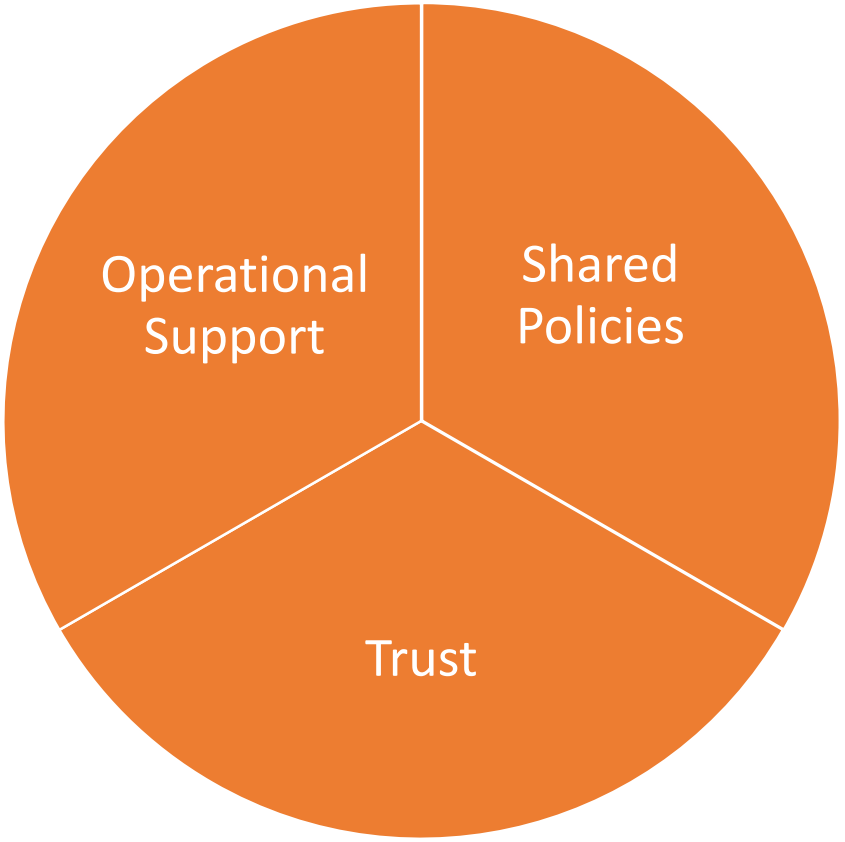
Our Interaction with Identity Federations

- Research Communities typically join through an SP-IdP proxy
  - From the outside (eduGAIN) it looks like an SP
  - From the inside it looks like an IdP
- We depend on the stability of eduGAIN as an authentication infrastructure!



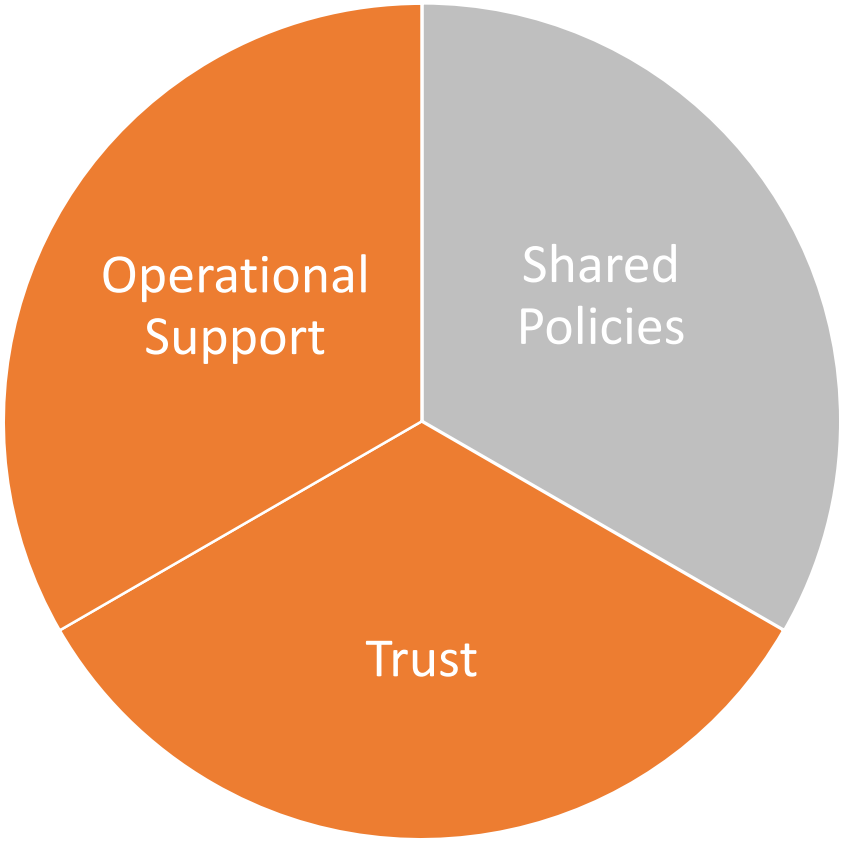
The SP-IdP Proxy Model. Source: GEANT, GN3PLUS13-642-23

Security Incident Response in Distributed Infrastructures



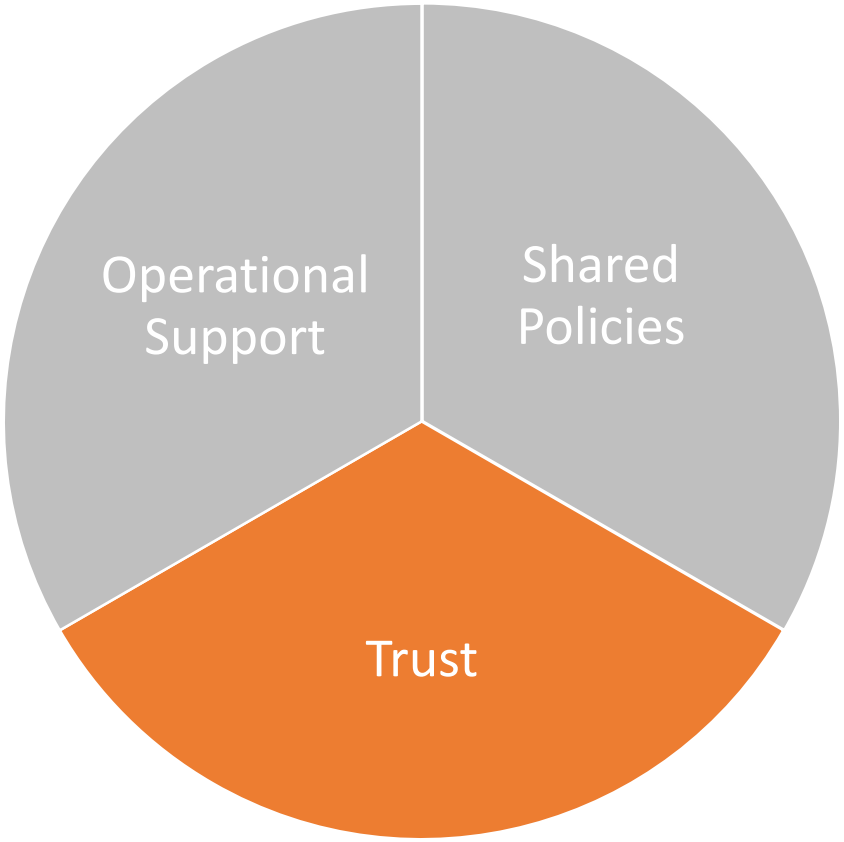
The challenge of Federated Identity Management

- EduGAIN membership includes 4 policies… Security Incident Response is not one
- We have no insight into security practices of each participant
- Collaboration between IdPs and SPs is essential to build full incident timeline – they have no obligation to collaborate



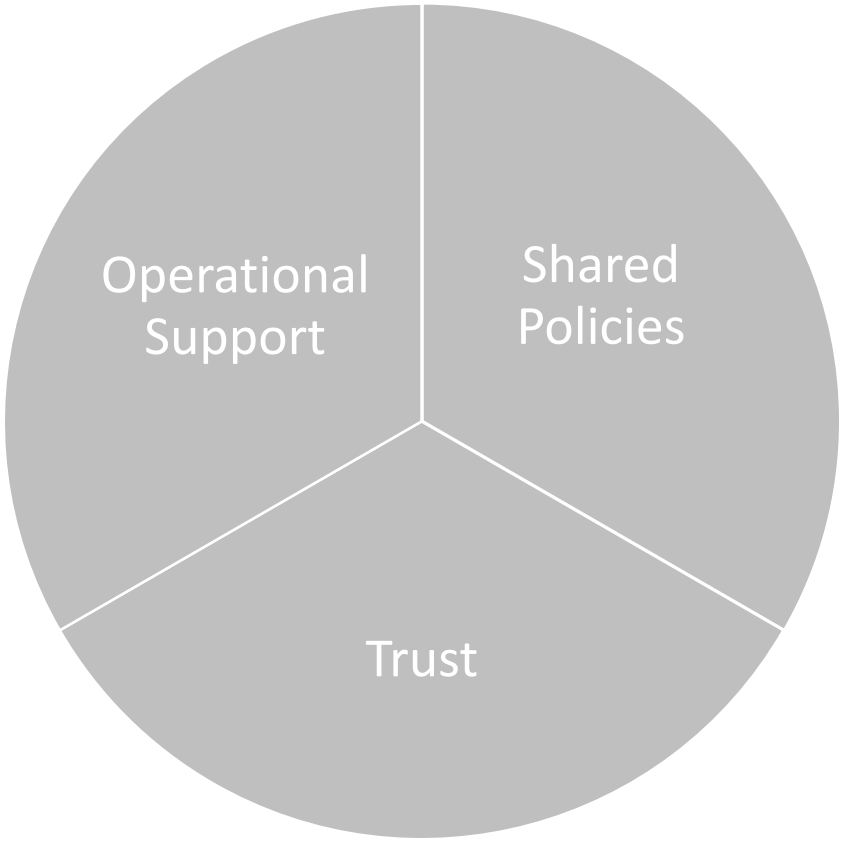
The challenge of Federated Identity Management

- EduGAIN has no central help desk
- Few national federations offer central security support
- No way to block an identity, IdP, or federation <u>everywhere</u> and <u>immediately</u>



The challenge of Federated Identity Management

- Security is often not priority (or even in skillset) of engaged FIM participants
- Simply too big…



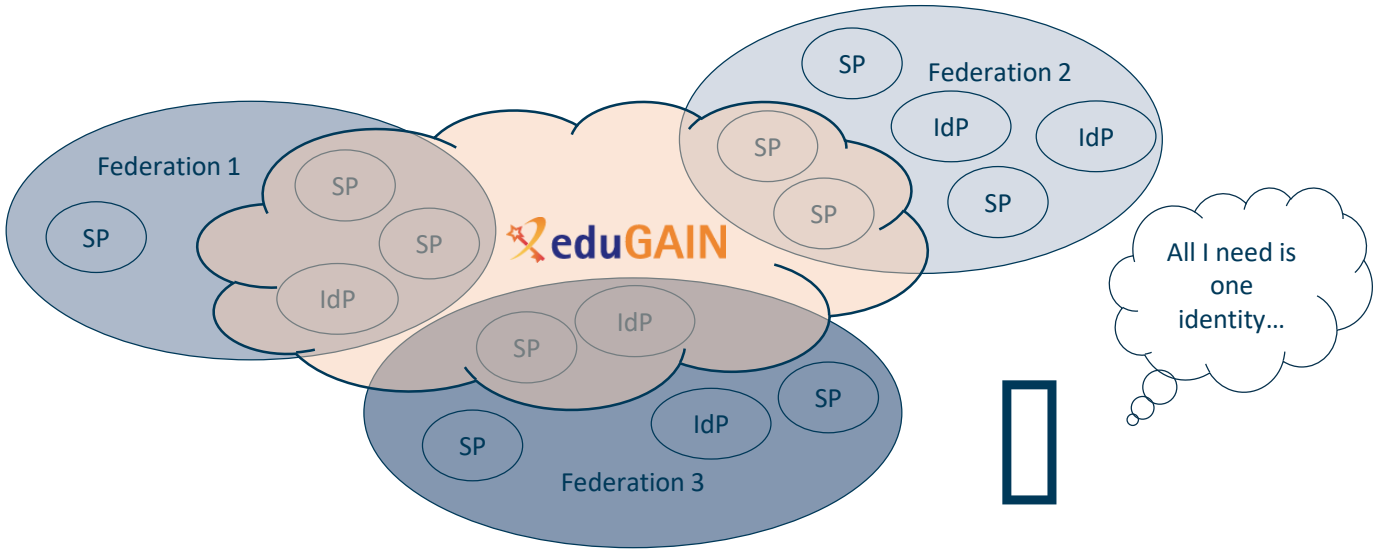
2360 IdPs

Potential sources of compromised identities

1493 SPs

Potential targets

What can we do?



Clearly an inviting attack surface… luckily, this was noticed several years ago!

Beginnings

- Issues 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

Evolution

Several years later, 2016

Security
Incident
Response
Trust Framework for
Federated
Identity

✓Approved by the REFEDS (Research & Education FEDerations) Community

✓Registered Internet Assigned Numbers Authority (IANA) Assurance Profile https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml

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

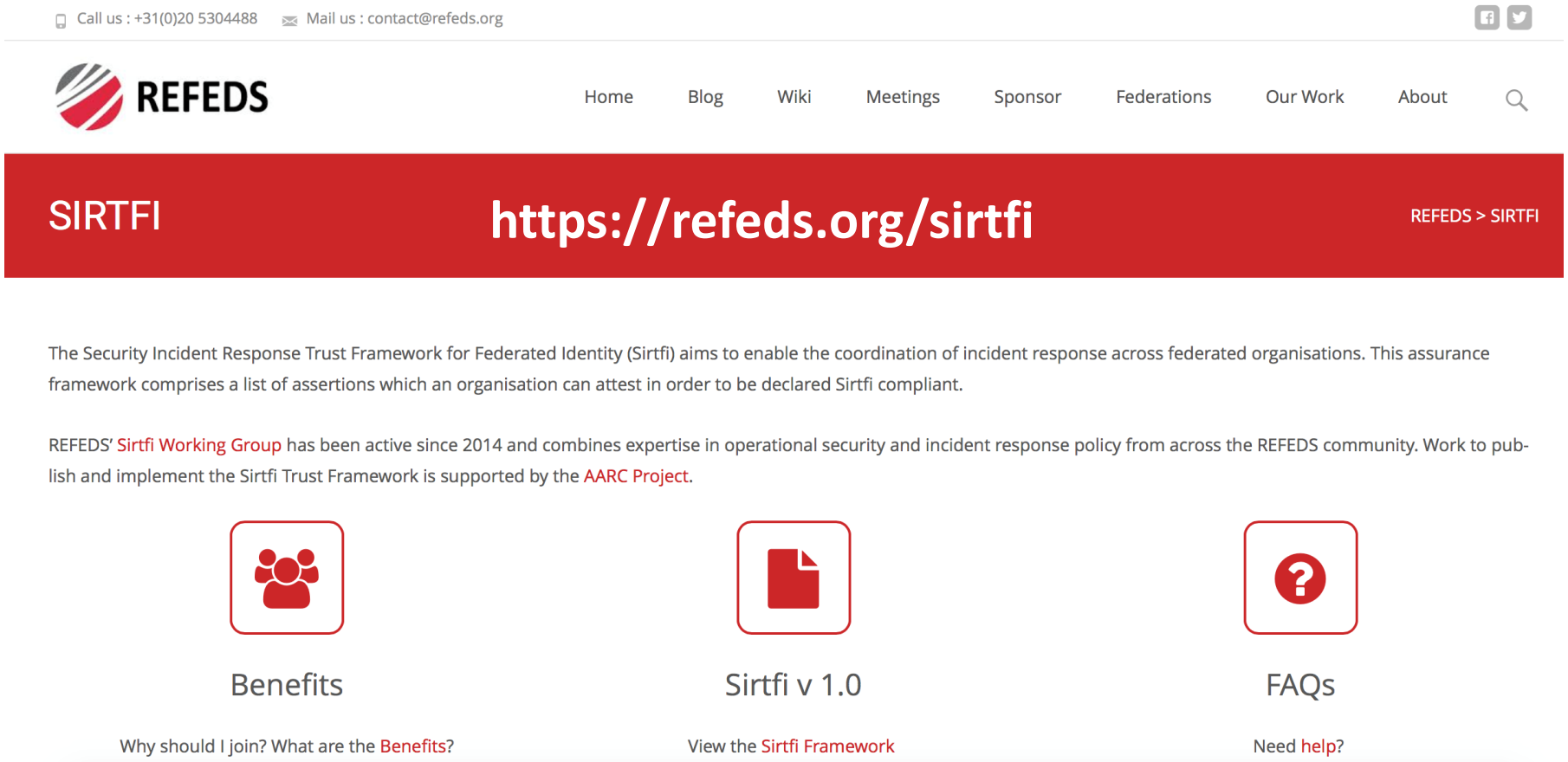
Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

Current adoption

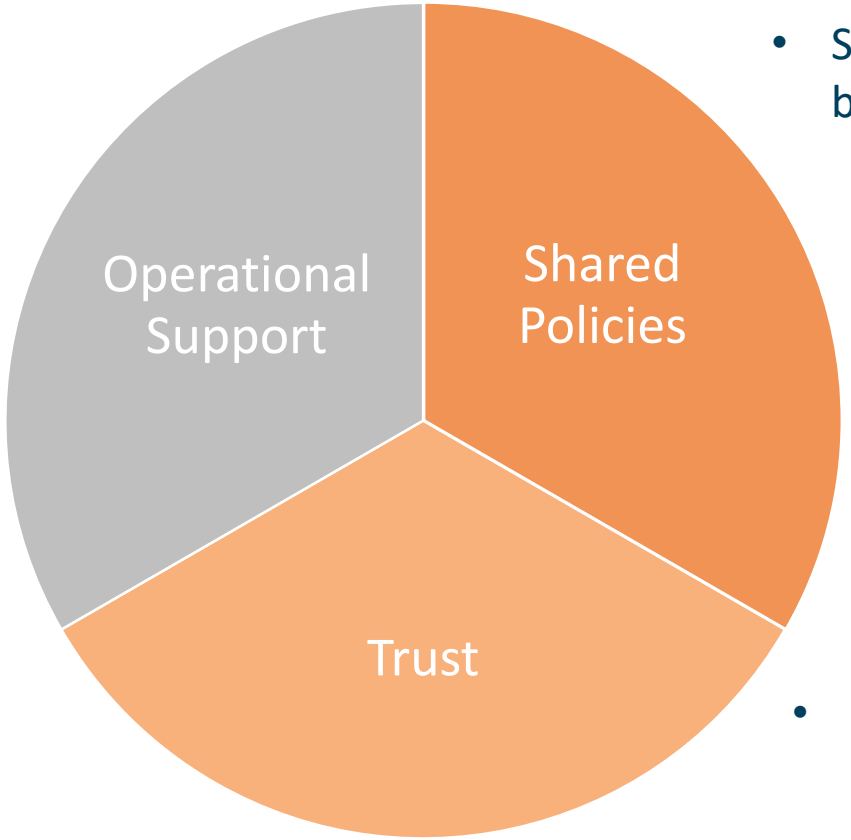
Who?	AA	IDP	SP	(blank)	Grand Total
Greece		3	1		**4**
Austria		1			**1**
Luxembourg		1			**1**
Corea		1			**1**
Switzerland	4	5	1		**10**
UK	2	3	2		**7**
Ireland		6			**6**
Italy	1	2			**3**
Netherlands		103	2	3	**108**
Sweden	4	5			**9**
Lithuania		1			**1**
USA	4	8			**12**
Total	**15**	**139**	**6**	**3**	**163**

Find out more



How does Sirtfi help?

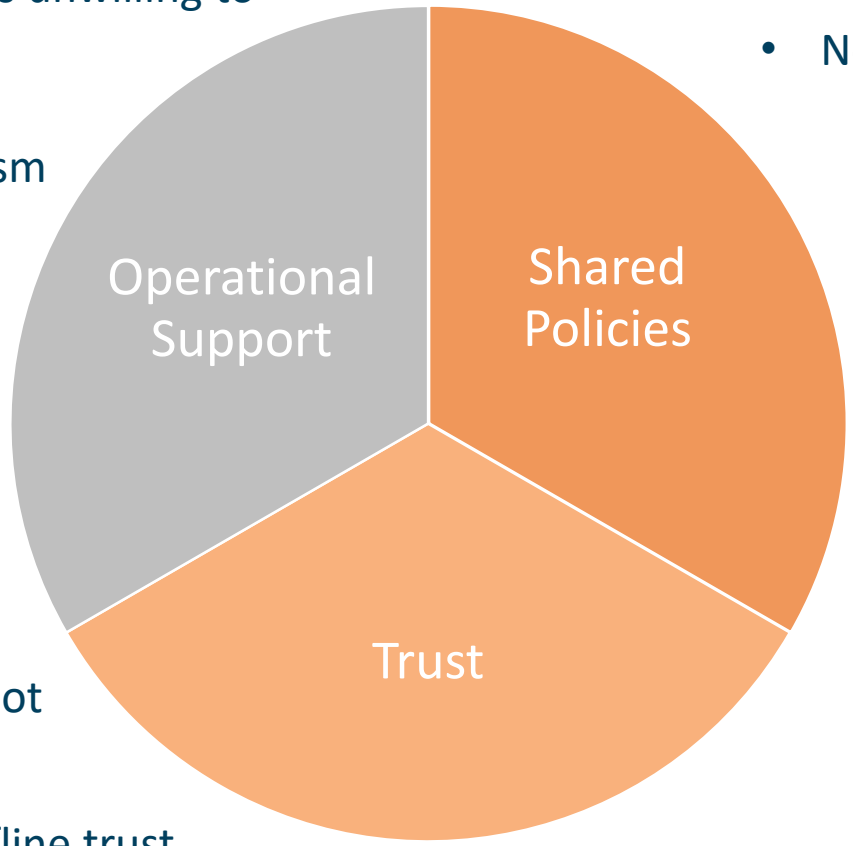
How does Sirtfi help?



- Shared framework fulfills purpose of basic policy
  - Obliged to collaborate
  - Basic operational security best practices
- Allows us to identify security conscious bodies

How does Sirtfi not help?

- Some Federation Operators unwilling to act as gatekeepers
- No large-scale blocking mechanism
- No shared procedures



- Trust tied to organisation/entity, not individual
- Difficult to build offline trust

Filling the gaps

How can we build the necessary security capability for eduGAIN?

Operational Support

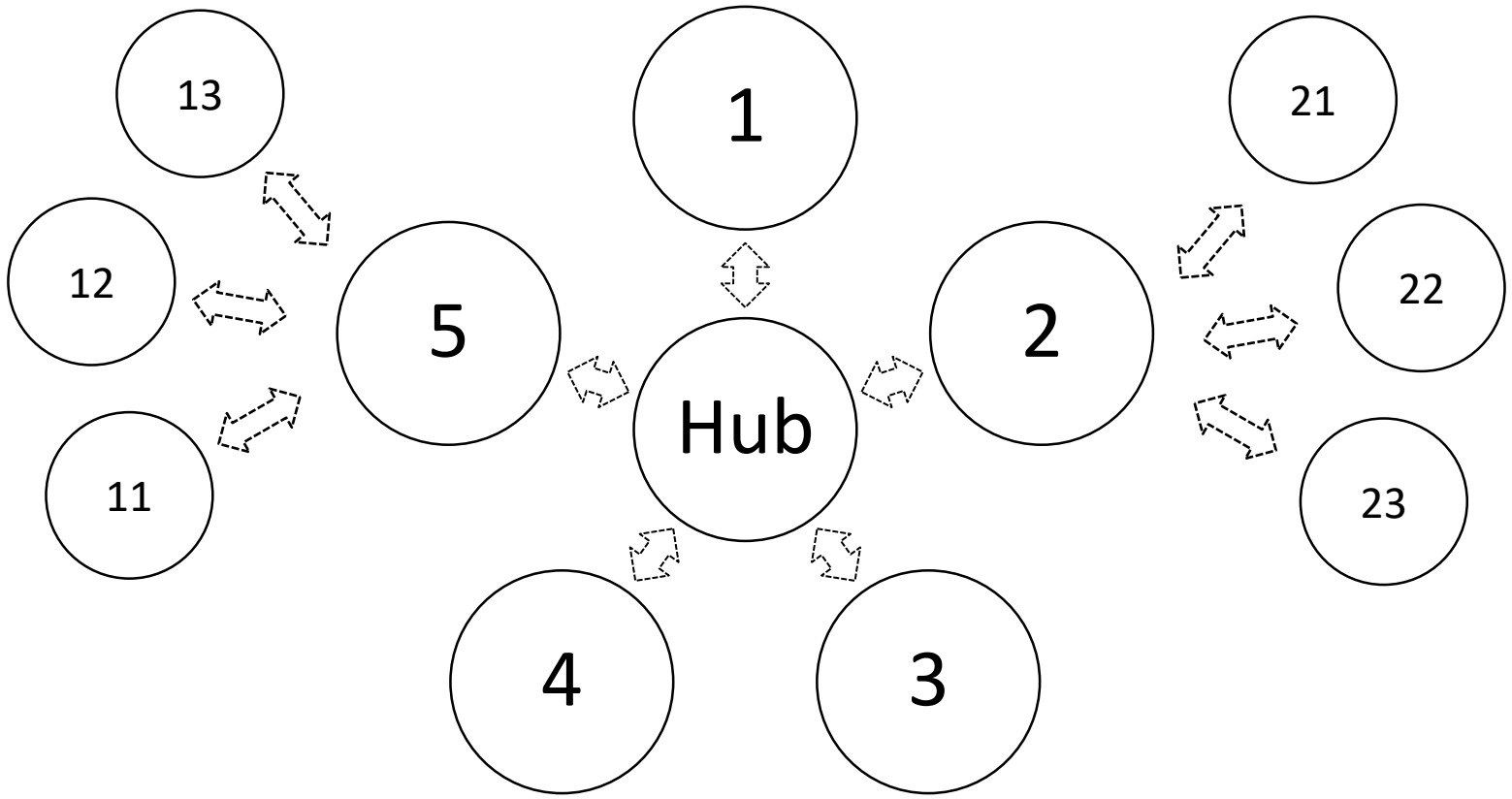
- eduGAIN itself announced early this year that they will provide a support platform capable of coping with roughly 200 tickets per year
- Security Incidents will be in scope of this team by Autumn

Trust

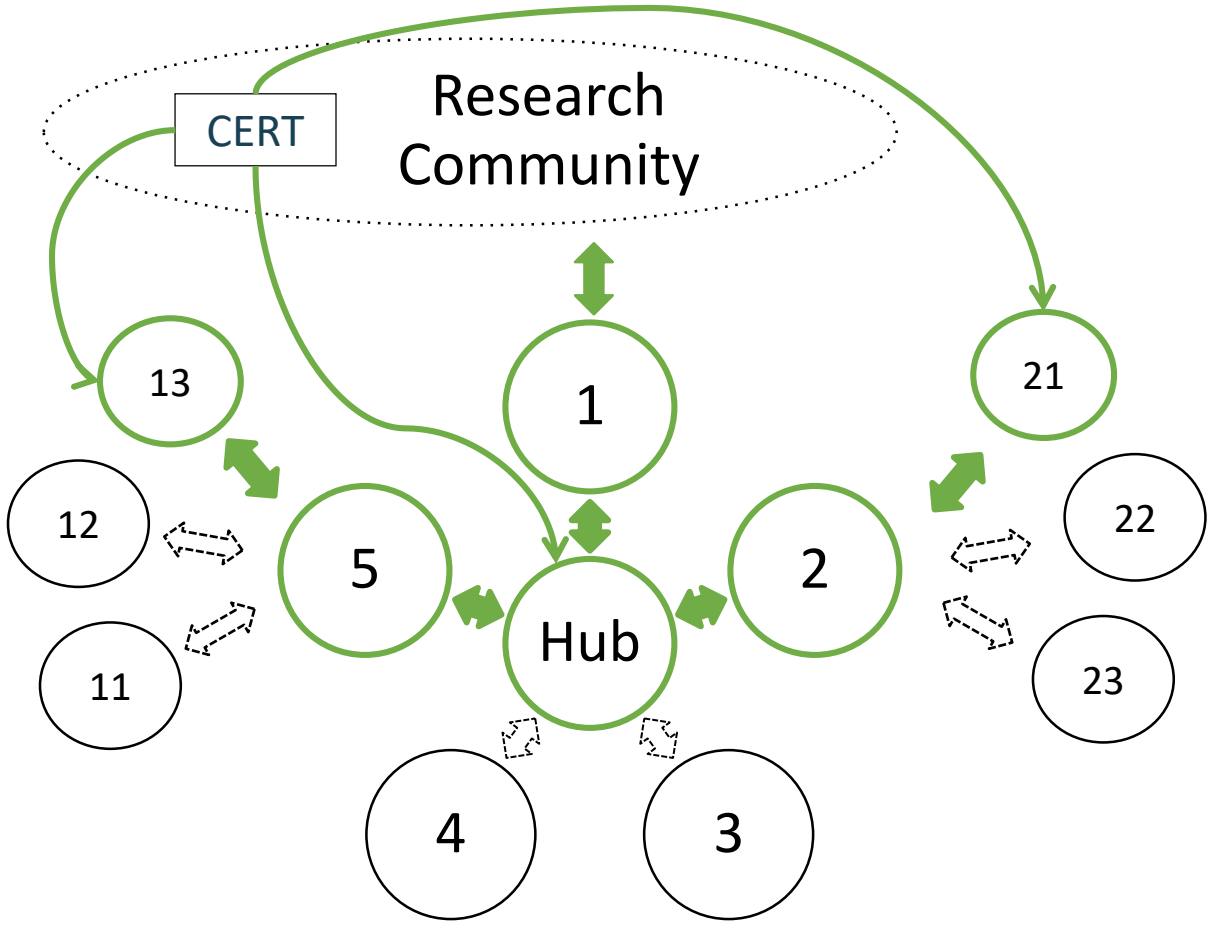
- Identified need for Trust Portal
- Crowd source trust and provide method for identifying confidence in an entity outside metadata

Incident Response Procedure for Interfederation

- DNA3.2 provides template procedures based on EGI/WLCG and inspired by common practices
- Leverages existing trusted relationships in Identity Federations
  - Sort of “nested hub” →
- Research Communities (RCs) need procedures for two purposes:
  - eduGAIN to secure itself
  - eduGAIN to cooperate with us during an incident



Role of Research Communities



- Typical SPs do not have a mature security capability
- Many RCs have expertise and motivation to lead incident response and should be allowed to do so
- Procedures are flexible to allow the most appropriate entity to be the Incident Response Coordinator

Next Steps

Document has already had input from many sources

- Identity Federations (Germany, US, UK, Sweden, Switzerland)
- SPs (ORCID)
- Research Community Reps (CERN, EGI, KIT)
- Review by Scott Koranda (LIGO) and Leif Nixon

Next steps

- Circulate ***more*** widely
- Encourage National Identity Federations to adopt similar policies
- Ensure that the eduGAIN support platform is able to effectively play the central role we need

Thank you

Any Questions?

hannah.short@cern.ch

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).