# Incident Response in R&E Federation

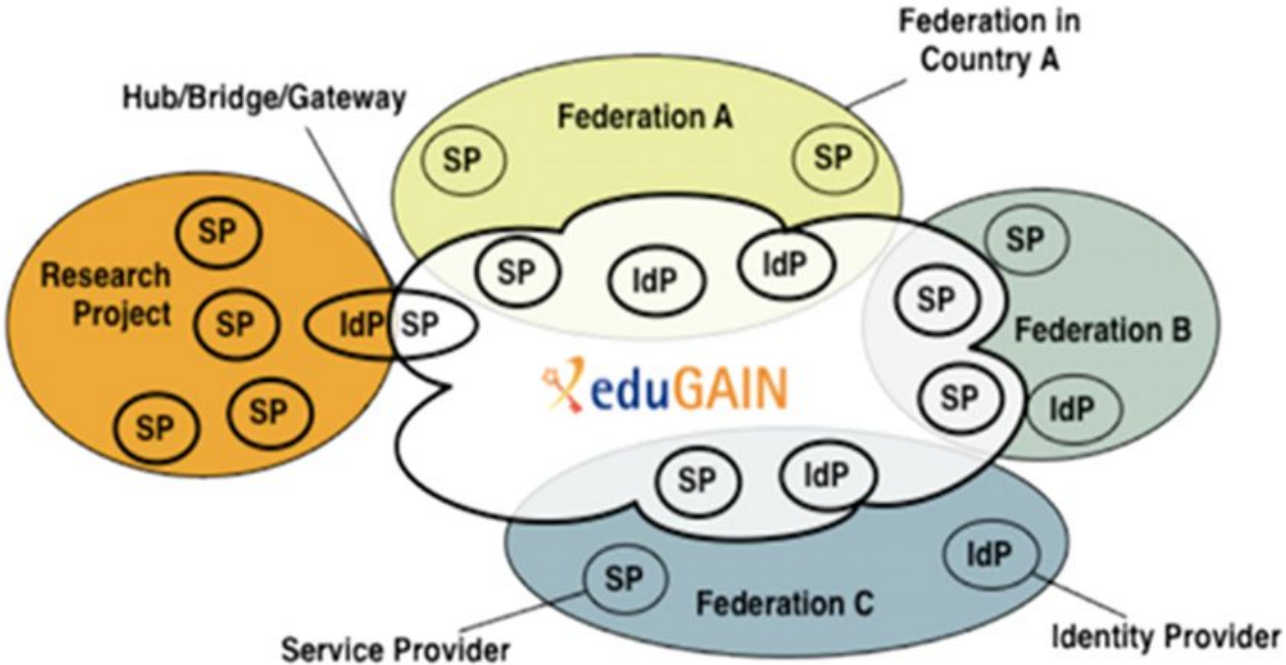

**HOW19**

Romain Wartel
CERN, SIRTFI WG member

Tuesday, March 19, 2019

slides prepared by Tom Barton

# Academic collaboration and R&E federation




faculty, students, staff

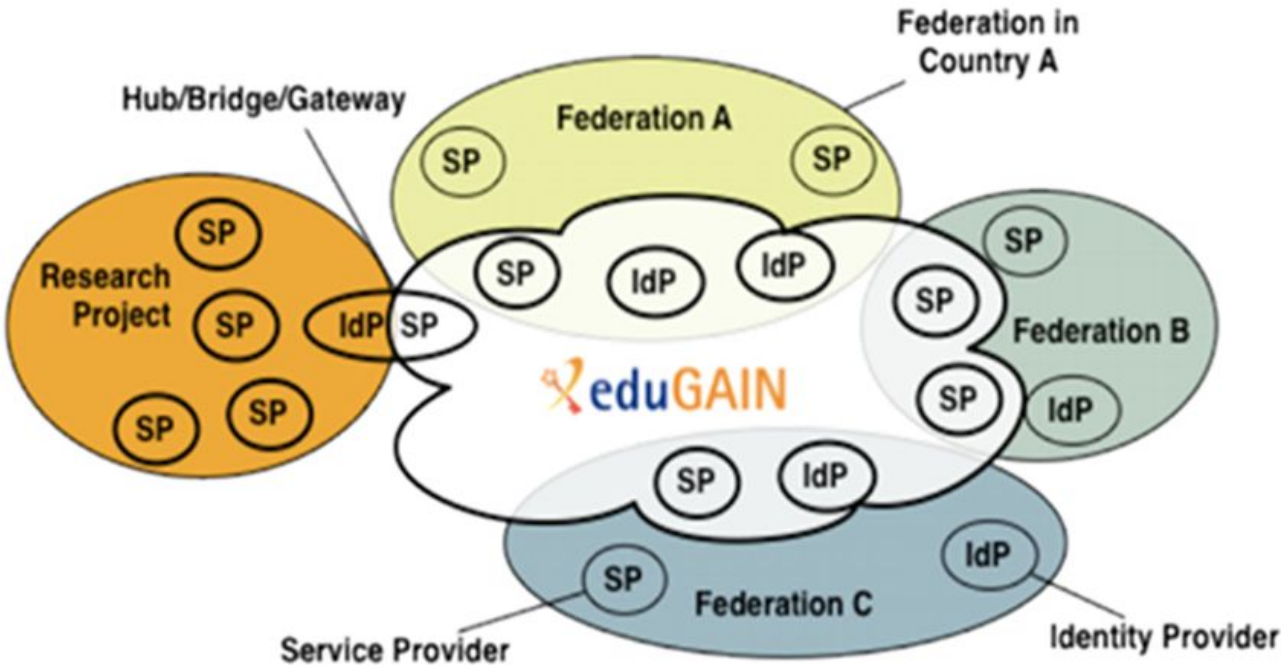
data sets
intellectual property
specialized instruments
specialized computing

at organizations everywhere

connected by global federation

SIRTFI
Security Incident Response Trust Framework for Federated Identity

# Dimensions of R&E federation




68 countries

>5,400 eduGAIN entities

>16,700 total entities (28% InCommon)

>10,000,000 users

SIRTFI
Security Incident Response Trust Framework for Federated Identity

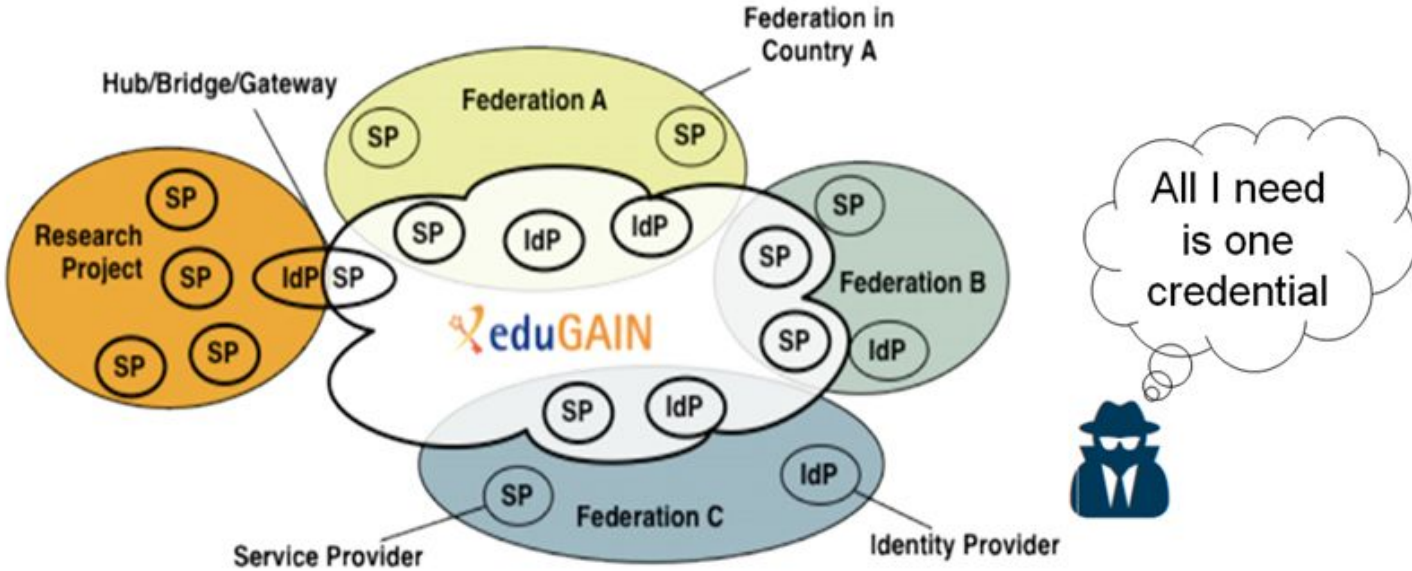
# SIRTFI - security incident response trust framework

Be willing to collaborate in responding to a federated security incident.

Apply basic operational security protections to your federated entities

in line with your organization's priorities.

Self-assert SIRTFI "tag" so that others will know to trust this about you.



# SIRTFI progress

| | | |
|---|---|---|
| Done | SIRTFI v1 | • REFEDS (international) standard<br>• Federation member organizations adopt<br>• 16 normative statements - intentionally low bar<br>• Security contact in entity metadata<br>• Guidelines for Federation Operators<br>• 938 IdPs and SPs have adopted so far |
| In process | Incident Response for R&E Federation | • Roles, responsibilities, tools, procedures, guidelines, templates for various parties involved in federated incident response - extend prior AARC work<br>• Federation operators, eduGAIN operator, associated CSIRTs, federation member organizations |
| LIGO PoC | SIRTFI+ Registry | • Manage SIRTFI tagging for entities in federations not yet supporting SIRTFI (and maybe more…) |

# Aligned work

- Security contact checking tool (GÉANT)
  - SIRTFI WG to provide guidance on how it should be deployed across R&E federation

- Adding incident response to eduGAIN support (GÉANT)

# SIRTFI in InCommon

| | SIRTFI tag | security contact | total |
|---|---|---|---|
| IdPs | 88 | 515* | 530 |
| SPs | 411 | 4022 | 4138 |

- Member orgs can self-attest in the Federation Manager UI
- Security contacts are required by Baseline Expectations
  - Entities that don't meet will soon be removed
- Proposal to add SIRTFI to Baseline Expectations appears to be moving forward
  - Would require all InCommon entities to become SIRTFI compliant

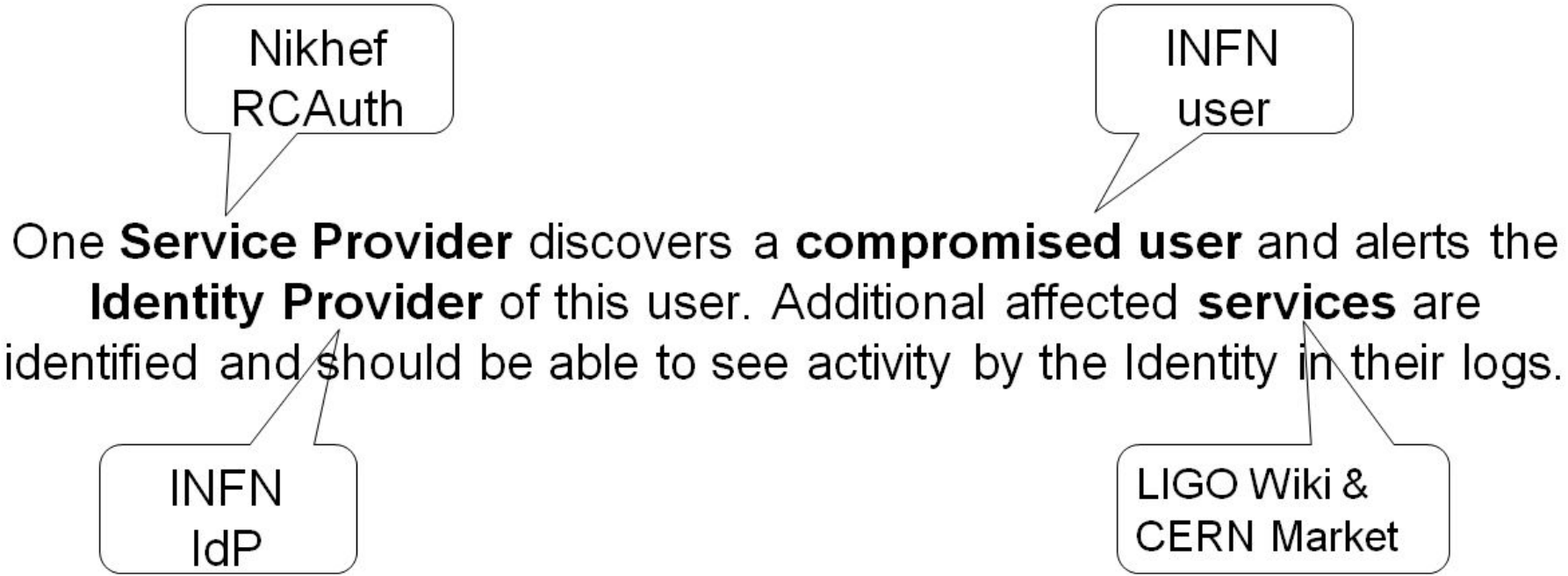
SIRTFI
Security Incident Response Trust Framework for Federated Identity

*Most of the 15 IdPs that don't have a security contact are test IdPs that will be removed

# SIRTFI and SNCTFI

- Both are derivative of Security for Collaboration among Infrastructures (SCI)
- SNCTFI contains normative statements about security and privacy practices among a collection of resource providers
  - Egs, CERN, WLCG, Nikhef, …
- An e-infrastructure's federation proxy presents their SNCTFI attestation to their federation operator to demonstrate SIRTFI and R&S Entity Category compliance

# Table tops, to occur annually



# Questions?

sirtfi@lists.refeds.org

Also:
Tom Barton <tbarton@uchicago.edu>, SIRTFI WG chair
Romain Wartel <Romain.Wartel@cern.ch>