SIRTFI WG Update
REFEDS, June 2021

Dave Kelsey
UKRI STFC Rutherford Appleton Laboratory
(on behalf of Tom Barton, University of Chicago and Internet2)

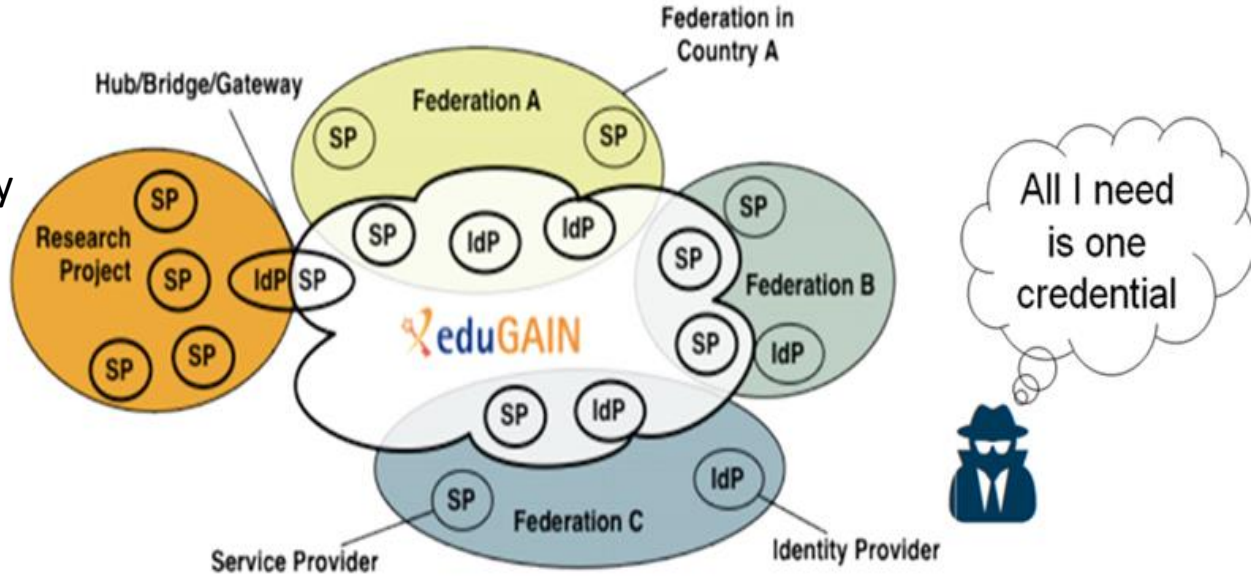
SIRTFI - security incident response trust framework for federated identity

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.



Overall arc of work[1]

Phase 1	Sirtfi v1 and related	Done
Phase 2	Define roles and responsibilities of the various parties in managing federated security incidents, information sharing guidelines, tools, procedures, and templates	Done
Phase 3	• Sirtfi v2 (add proactive notification, improve based on field experience) • Promote responsiveness testing by federation operators or other parties • Analyse suitability of existing identity event notification solutions such as IETF's Security Events to R&E federations	In Progress

[1] https://wiki.refeds.org/display/GROUPS/SIRTFI

eduGAIN Security Incident Response Handbook

- Roles, responsibilities, and procedures for
  - Federation Participants
  - Federation Operators
  - eduGAIN Security team
- Adopted by the eduGAIN Security Team, recommended for all parties
- Respects incident response coordination roles where they are already established
- Federation Operators are default coordinators within their federations
- eduGAIN Security team coordinates across federations
- Augments, does not supersede, established local policies and procedures

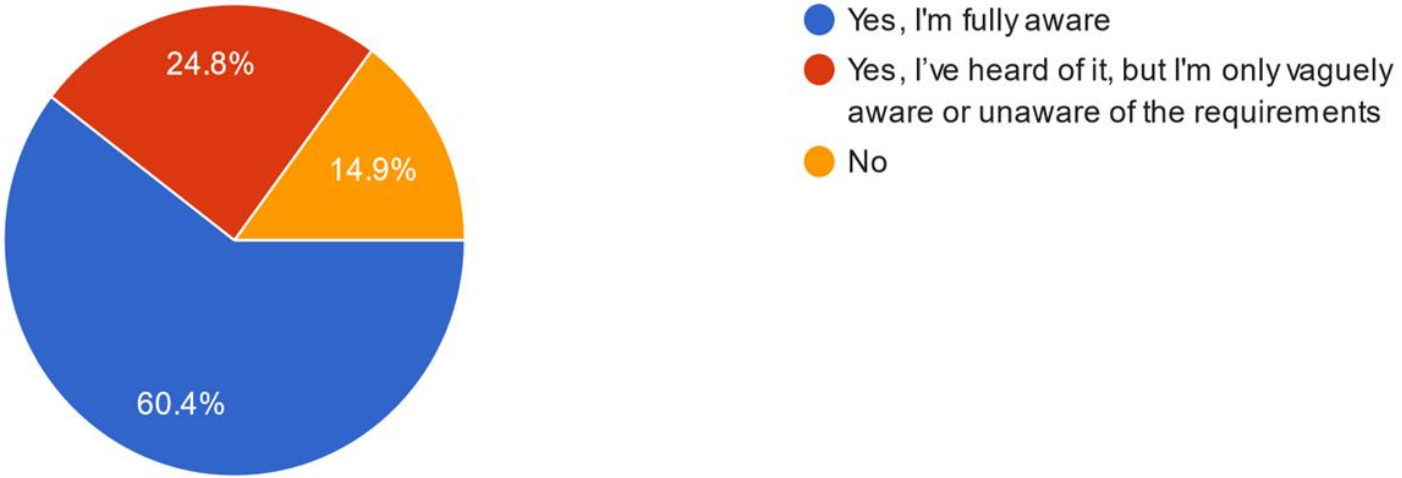
Update on open tasks

Sirtfi v2	Survey to inform of field experience was given to identified contacts of all eduGAIN entities
Suitability of IETF Security Events to R&E Feds	Upon review, interim conclusion is that if the Working Group should undertake some action, it should be to reinforce uptake of MISP
Responsiveness testing	Not started

SIRTFI survey summary

Are you aware of Sirtfi and its requirements?

101 responses

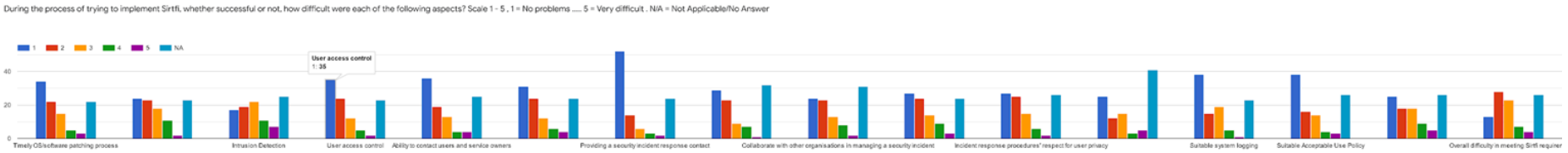


SIRTFI survey summary

Has your organisation considered implementation of the requirements for Sirtfi for some or all of its federated entities?

101 responses

SIRTFI survey summary



In case that isn't clear … 😕

Weaker responses in connection with Sirtfi specifications about …

- IR procedures, especially whether they suitably respect user privacy
- Ability to collaborate with other organisations in managing an incident
- Use of Traffic Light Protocol
- Ensuring acceptance of AUP by users
- Adequacy of intrusion detection and vulnerability management

SIRTFI survey summary

Would you support an addition to Sirtfi that would require your organisation to proactively notify other organisations of a security incident you've detected that is believed may impact them?

101 responses