Sirtfi Call

August 7th 16:00 CEST

Attendees: Hannah, Nicole, Scott K, Doug P., Uros, Alan, Tom, Tangui

GDPR

- Impact of GDPR means data leaks must be reported
- CoCov2 recommends Sirtfi as means to provide contacts and confidential communication
- Anyone being compliant with CoCo version 2 will have to include Sirtfi
- Mutually beneficial as creates requirement

Communication Channels

- Need to avoid that personal information gathers at the eduGAIN support platform level
    - Must enable point to point communication
- Slack channels have been seen to be effective, ongoing maintenance
- How do you define the people who have access to the channel? How do you vet them?
- Need to be able to pull in people, no automatic access
- 2 kinds of information sharing tasks
    - Managing the incident (small, relevant parties pulled in)
    - Bystanders (broadcasting appropriate details and reporting) -> potentially out of scope?
- KPI = shorter time to get a response going
- https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf
- Suggestion of a wider paper on how to improve the response time of an incident AND (possibly) roles and responsibilities
    - Response time of mailbox can be tested fairly easily
    - Roles and Responsibilities are more difficult to define and approve
- We need to be able to count on who will do the vetting
- What about sanctions if communication is not responded to?
- How does this relate to out-of-bands mechanism
- Whether or not (and how) contact should be contacted could be Sirtfiv2

Registration Tool/out of bounds Sirtfi assertion

- What should it do? Static DB? Queriable?
- Not all federations are the same in terms of uptake of new standards or certifications, we want individuals to be able to take these things up regardless
    - Option 1 = wait… a bit long
    - Option 2 = InAcademia style tool to query

    - Option 3 = inject to eduGAIN
- Want to not upset federations that are actually doing things quickly
- Could fulfil the need for multiple frameworks but better to be specific at this stage perhaps
- Perhaps could inject at eduGAIN level (but not a long term solution), but maybe want to decouple from eduGAIN for sustainability purposes
    - May result in over dependency on eduGAIN and “lazy” federation operators
    - Could do for X time, business model
- Perhaps separate data from (federation) metadata
- Ways to expose assertions by elements behind a proxy?
- Could tie in with Roland’s methodology
- Can we tie trust in to this data store of Sirtfi assertions? Reputation based (could define the “Guild”)
    - Votes based?
    - Base trust on incident communication?
    - Role play extended, determines trust?
- Have a “Guild of Mature IdPs”/Communities of interest
    - Good timing, scientific research communities are becoming frustrated and have energy to put in here

Actions:

- Nicole to talk with GEANT
- Hannah add to discussions for FIM4R
- All, think about what we want to communicate at REFEDS@TechEx & AARC