Can R&E federations trust Research Infrastructures?
The Snctfi policy/trust framework

David Kelsey (STFC-RAL)
Co-author: David Groep (Nikhef)

ISGC2017 - Taipei
7 Mar 2017
A classic FIM4R use case – “Research Communities and eduGAIN”

• A research community wants to use federated IdPs (eduGAIN)
• But they have many distributed research community SPs
  • And they do not all want to (or cannot) join a national identity federation
• A popular way of joining the two worlds together is via an SP/IdP Proxy
  • Acts as an SP in the eduGAIN world
  • Acts as an IdP for the research community
• But still have to establish trust between the eduGAIN IdPs and the research community
  • To allow attributes to flow
• How can we build scalable trust?

- > Snctfi
Flow of attributes and trust – via SP/IdP Proxy

Picture from GEANT – eduGAIN
Infrastructure Policy and Trust Framework – requirements

• To establish trust between eduGAIN and the Infrastructure (research or e-Inf)
• A framework which binds all IdPs, SPs and AAs together (within the Infrastructure)
• Enable eduGAIN & the R&E federations to trust the SP-Proxy (and hence its community behind)
  • To allow/encourage the release of R&S attributes
• The federations only see the SP-Proxy
• Q: Why should the R&E federations trust that SP-Proxy?
  • A: Because the SP-Proxy asserts categories and assurance marks
    • R&S
    • Sirtfi
    • Data Protection (CoCo)
• The new policy and trust framework
  • Constrains the behaviour of the Infrastructure
  • To allow the SP-Proxy to assert R&S, Sirtfi and DP CoCo on behalf of the Infrastructure
“Security Collaboration among Infrastructures” (SCI) – our starting point

Http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

- EGI, HBP, PRACE, EUDAT, CHAIN, WLCG, OSG and XSEDE
- Defined a policy trust framework
  - build trust and develop policy standards for collaboration on operational security
- SCI was used as the basis for Sirtfi
  - A Security Incident Response Trust Framework for Federated Identity
  - to enable coordination of security incident response across federated organizations
Why “Snctfi”? 

Scalable Negotiator for a Community Trust framework in Federated Infrastructures

Snctfi

• As for “Sirtfi”
  • A meaningful acronym which is pronounceable
  • With no pre-existing hits in search engines

• “Sanctify” - meaning: make legitimate or binding

• Synonyms for “sanctify”:
  Approve, endorse, permit, allow, authorise, legitimise, “free from sin”
Snctfi - the new Trust and Policy Framework

- The target audience is the *Infrastructure* as a whole
- Scope: The SP-Proxy, the SPs, any AAs, token translators, credential stores, ...
- Allow for different binding mechanisms, including contracts, MoUs, SLAs, or policies
- Build Trust between the *Infrastructure* and eduGAIN
  - And between *Infrastructures*
- This is not a REFEDS entity category
  - Rather an assurance mark
- Started from SCI document V1
- Added new policy requirements
  - E.g. behaviour of the SP-Proxy and Attribute Authorities
- Removed topics not needed
  - Detailed security requirements (as covered by Sirtfi)
  - Legal and management issues
- Reworded existing topics as necessary
Structure of the Sirtfi document

• Background and Introduction

• Operational Security
  • [OS1] Abide by the *Infrastructure* defined security requirements, e.g. a CSIRT
  • [OS2] Meet the requirements of Sirtfi

• Participant responsibilities
  • Addresses issues related to user management, AUPs, security incident response, ...
    • Users
    • Collections of users
    • SPs

• Data Protection
  • Bind those SPs that consume eduGAIN attributes (and some collections of users) to either
    • A common *Infrastructure* Data Protection policy (framework)
    • Or the GEANT DP CoCo
Future plans

- **Timelines**
  - Aiming for a complete draft by end of March 2017
  - Then wider discussion with FIM4R and REFEDs
- “Publish” a version of Snctfi (as a proposed trust framework)
  - An AARC NA3 deliverable – to be completed before end of April 2017
- Then Snctfi can still be modified during formal adoption
  - In AARC2
  - by FIM4R/IGTF (and REFEDS)

- As an aside:
- SCIV2-WG busy in “WISE”
  - Can we merge SCI version 2, Sirtfi and this new framework?
  - [https://wiki.geant.org/display/WISE/SCIV2-WG](https://wiki.geant.org/display/WISE/SCIV2-WG)
- Decided to tackle this re-merge for SCI version 3
Thank you

Any Questions?

david.kelsey@stfc.ac.uk

https://aarc-project.eu

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