Snctfi

SP/IdP Proxies and a new Policy Trust Framework
AARC NA3 Task 4 – Scalable Policy Negotiation

David Kelsey
STFC-RAL

FIM4R meeting - Montreal
19 Sep 2017
A research community wants to use R&E federation 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

see AARC Blueprint Architecture

But still have to establish trust between the eduGAIN IdPs and the research community
  - Or between Infrastructures

SP/IdP Proxy wishes to assert:
  - REFEDS Research and Scholarship
  - GÉANT data protection code of conduct
  - REFEDS Sirtfi

How can we build such scalable trust?

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

Picture from GEANT – eduGAIN
“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
- Version 1
SCI Version 2 – now published by WISE

• Aims
  • Involve wider range of stakeholders
    • GEANT, NRENS, Identity federations, ...
  • Address conflicts in version 1 for new stakeholders
  • Add new topics/areas if needed (or indeed remove topics)
  • Revise all requirements
  • Simplify!

• SCI Version 2 was published on 31 May 2017

• https://wise-community.org/sci/

• Endorsement of SCI Version 2 at TNC17 (Linz) – 1 June 2017
  • has been received from the following infrastructures; EGI, EUDAT, GEANT, GridPP, MYREN, PRACE, SURF, WLCG, XSEDE

• https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx

• Worked more on Guidelines/FAQ for SCI version 2 – NSF Cybersecurity Summit (15 Aug)
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”
• **Abstract:** identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy

• **The target audience:** intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness

• **Snctfi version 1**
  - An output of the EU H2020 AARC project
  - Published on 26 April 2017
  - [https://aarc-project.eu/policies/snctfi/](https://aarc-project.eu/policies/snctfi/)

• **Peer-review and assessments – future work**
  - Interoperable Global Trust Federation (IGTF)
  - [https://www.igtf.net/snctfi/](https://www.igtf.net/snctfi/)

• **EGI Security Policy Group – together with AARC2**
  - Working on two “Community” security policies – to implement requirements of Snctfi
Structure of the Snctfi document

• Background and Introduction
• Operational security [OS]
  • Aiming to prevent security incidents, or
  • Minimise the impact of those that occur
• User responsibilities [UR, RU, RC]
  • To establish trust between the Infrastructure and the R&E federations, and between Infrastructures, the Infrastructure relies on appropriate behaviour by its users and user communities.
  • Addresses issues related to user management, AUPs, security incident response, ...
• Protection and processing of personal data [DP]
  • Bind the Infrastructure Constituents and Collections of users to either
    • A common Infrastructure Data Protection policy (framework)
    • Or GEANT Data Protection Code of Conduct
Next steps

- **AARC2 with EGI (and WLCG)**
  - Finalise the two example “Community” security policies to implement Snctfi
    - First: govern the relationship between Community and Infrastructure(s)
    - Second: govern how the Community manages itself and its Users

- **AARC2 with IGTF (not yet discussed and agreed)**
  - Work on guidance, FAQ and assessment criteria

- **FIM4R?**
  - Try using Snctfi for your Research Infrastructure/Community
  - Provide feedback
    - Problems deploying?
    - Requirements not clearly specified?
    - Issues missing from Snctfi?
Thank you

Any Questions?

david.kelsey@stfc.ac.uk

https://aarc-project.eu