Authentication and Authorisation for Research and Collaboration

Snctfi and scalable policies

AARC NA3 Task 3.4 – scalable policy negotiation

David Kelsey (STFC-RAL)
Task leader NA3.4

AARC All Hands meeting, Athens
20 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?

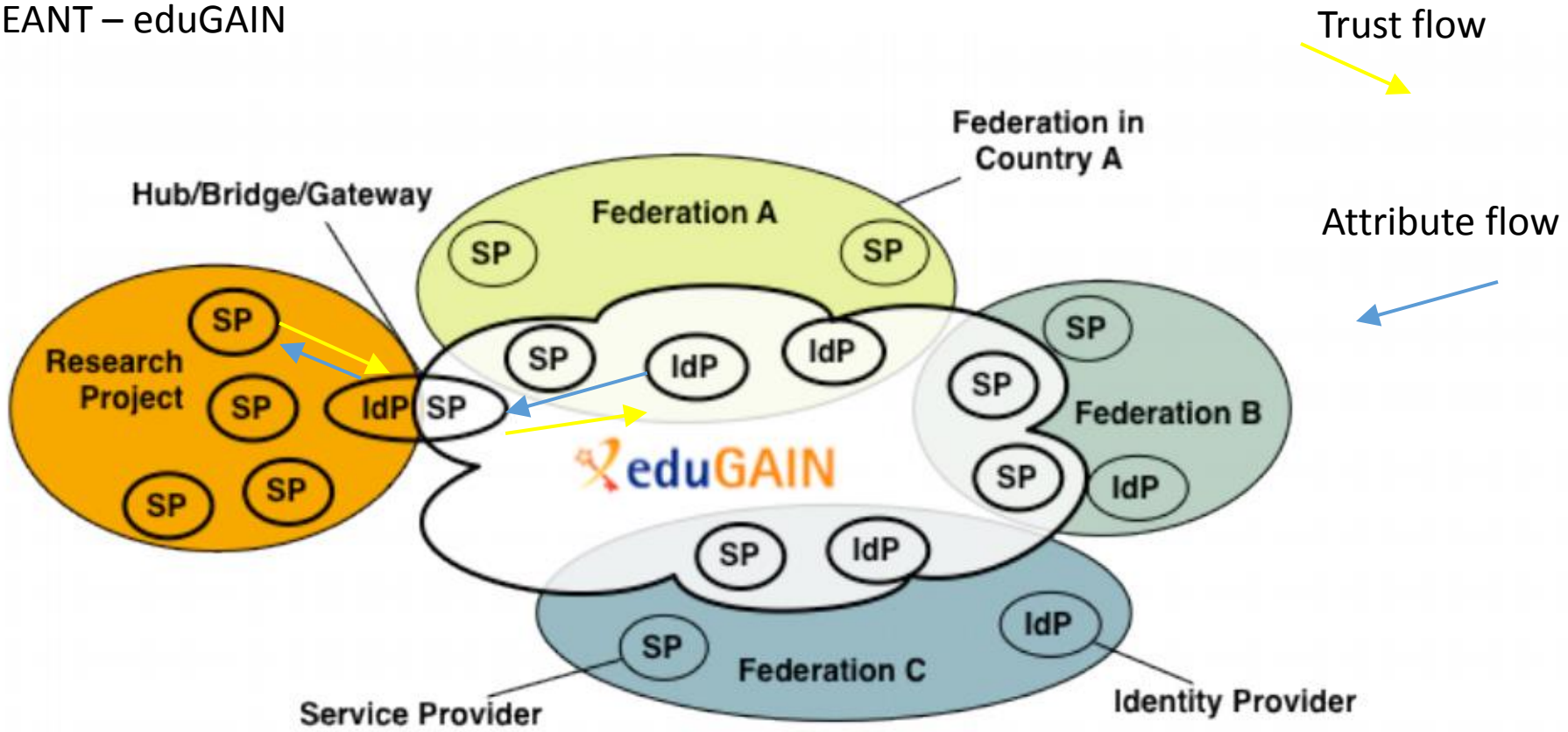
- > Snctfi

Outline (this talk)

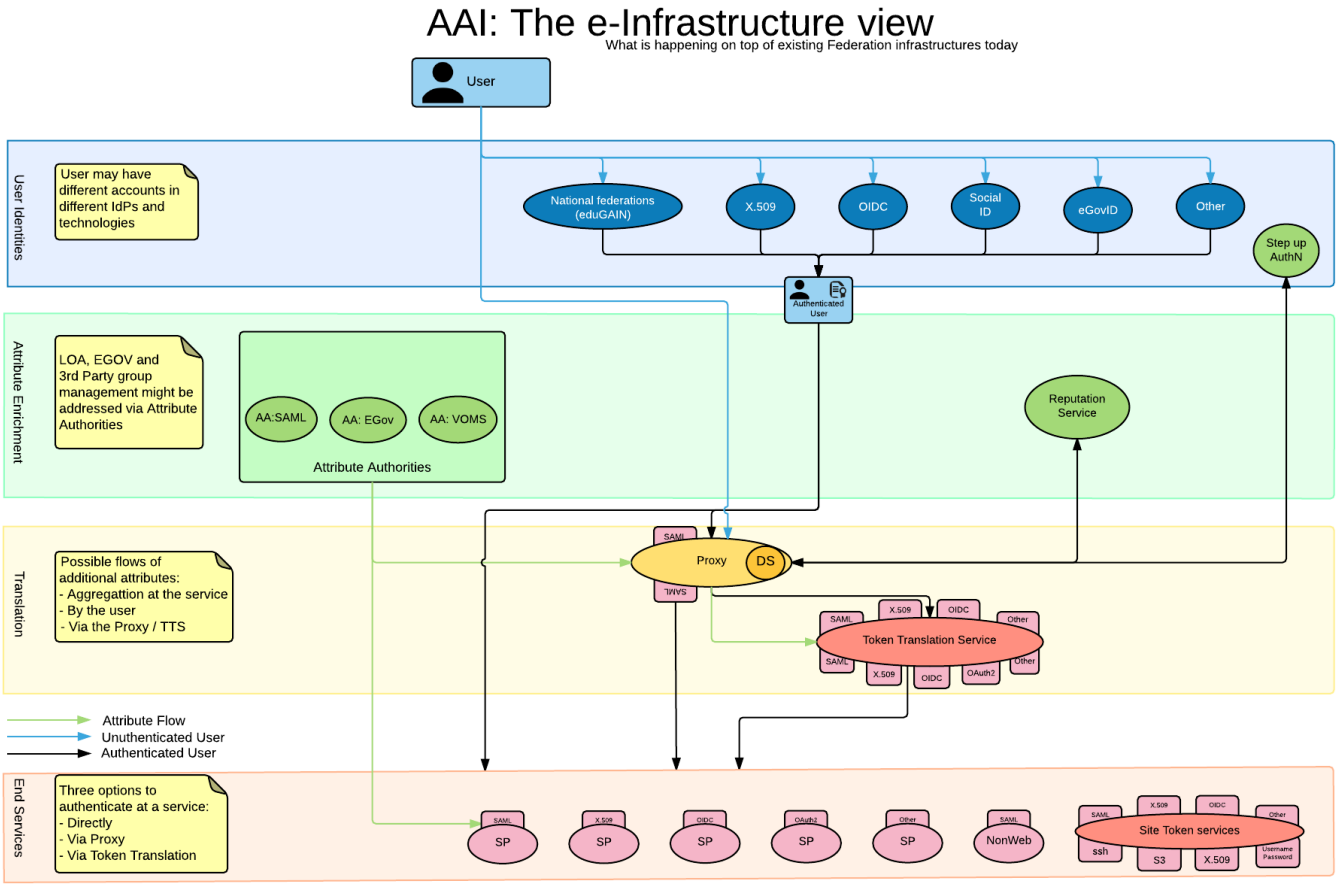
- Snctfi – a reminder
- Work on documents
  - AARC Deliverable DNA3.4
  - The Snctfi version 1 document
  - Publish in the ISGC2017 conference proceedings?

Flow of attributes and trust – via SP/IdP Proxy

Picture from GEANT – eduGAIN



AARC Blueprint Architecture (2016 draft)



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”

Structure of the Snctfi document

- Introduction
- Operational Security
  - Infrastructure must ensure that all members:
    - [OS1] Abide by the *Infrastructure* defined security requirements
    - [OS2] Meet the requirements of Sirtfi
    - Continues on …
- Assigning responsibilities
  - Addresses issues related to user management, AUPs, security incident response, …
    - Users, Collections of users, SPs, AAs, SP-Proxy
- 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 (new) GEANT DP CoCo

Deliverable DNA3.4

Deliverable DNA3.4

- Work in progress
- “Recommendations on the grouping of entities and their deployment mechanisms in scalable policy negotiation”
  - A month 24 deliverable
- Draft Document in Google docs
  - See AARC NA3 private wiki for link
- Structure defined (details next slide)
  - Entities, groupings & scalable policies
  - Snctfi
  - Other policy work
  - Conclusions and future plans
  - Appendix 1: The Snctfi document
  - Appendix 2: Considerations for designing an infrastructure

DNA3.4 (cont'd – more details)

- Entities, groupings & scalable policies
  - REFEDS R&S, Geant DP CoCo, Sirtfi, links to tools
  - Report and earlier work done by RENATER
- Snctfi
  - Describe the problem we are addressing; AARC BPA; GEANT use case
  - How was the document produced? Input from FIM4R, IGTF, REFEDS, Vienna TIIME meeting, etc.
- Other policy work
  - Policy/best practices on AA, Best practices on credential stores, Policy work behind RCauth CA
  - Examples: ELIXIR & EGI
- Conclusions and future plans
  - Address EU GDPR, AARC deliverable on DP and accounting, new GEANT DP CoCo version 2
  - Take Snctfi forward in wider community including IGTF, FIM4R, REFEDS, WISE, …
  - Deployment to be tackled as part of AARC2
  - How is the Snctfi document maintained in future? – IGTF? FIM4R? (& AARC2)
  - Assessment of Snctfi compliance (self audit, peer review, IGTF, …)

The Snctfi document

Snctfi document

- Snctfi working group
  - Had meetings by Vidyo
- Draft document in Google docs (getting close – good draft by end of this week)
  - URL on NA3 private wiki
- Definition
  - The *Infrastructure*
    - SPs, SP-Proxy, IdPs, AAs, operations/management
    - Either a Research Infrastructure or an e-Infrastructure
- Target audience (of the document)
  - The Infrastructure operations/management team (they are responsible for the SP-Proxy)
- Aims (of the document)
  - Help build a trustworthy *Infrastructure*
  - For trust with eduGAIN federations, for trust between *Infrastructures*
  - To enable SP-Proxy metadata to assert Sirtfi, Geant DP CoCo (and R&S)

Snctfi document (2)

- Allow for different binding mechanisms, including contracts, MoUs, SLAs, or policies
  - Binds SPs to the Snctfi requirements
  - Allows the Infrastructure to assert Snctfi compliance
- This is not a REFEDS entity category
  - Rather an assurance mark

ISGC2017 paper

ISGC2017 paper

- I talked at ISGC2017 on Snctfi
  - Taipei (7 Mar 2017)
  - *http://indico4.twgrid.org/indico/event/2/session/14/contribution/41*
  - “Can R&E federations trust Research Infrastructures?”
- We have the option to submit a written paper to the conference proceedings
  - My view is “yes”
  - SCI version 1 was published in ISGC 2013
  - Good to have “papers”
- Structure would be
  - The version 1 of Snctfi (as is)
  - But make it into a paper with more background and introduction and a summary
  - Much of the same material as in DNA3.4
  - We own the copyright everywhere (or inherit it under CC)

Thank you

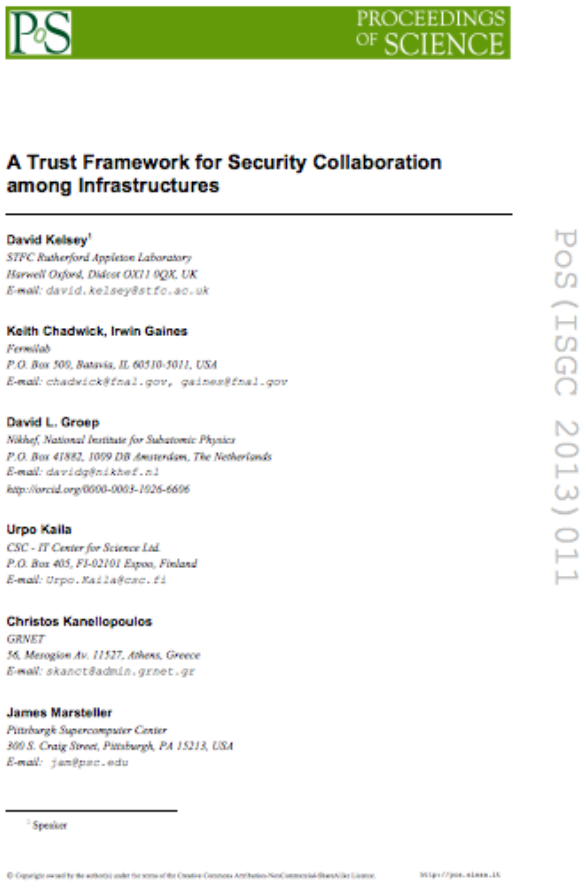
Any Questions?

david.kelsey@stfc.ac.uk

https://aarc-project.eu

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).

"Security Collaboration among Infrastructures" (SCI) – our starting point



PROCEEDINGS OF SCIENCE

A Trust Framework for Security Collaboration among Infrastructures

David Kelsey[1]
STFC Rutherford Appleton Laboratory
Harwell Oxford, Didcot OX11 0QX, UK
E-mail: david.kelsey@stfc.ac.uk

Keith Chadwick, Irwin Gaines
Fermilab
P.O. Box 500, Batavia, IL 60510-5011, USA
E-mail: chadwick@fnal.gov, gaines@fnal.gov

David L. Groep
Nikhef, National Institute for Subatomic Physics
P.O. Box 41882, 1009 DB Amsterdam, The Netherlands
E-mail: davidg@nikhef.nl
http://orcid.org/0000-0003-1026-6606

Urpo Kaila
CSC - IT Center for Science Ltd.
P.O. Box 405, FI-02101 Espoo, Finland
E-mail: Urpo.Kaila@csc.fi

Christos Kanellopoulos
GRNET
56, Mesogion Av. 11527, Athens, Greece
E-mail: skanct@admin.grnet.gr

James Marsteller
Pittsburgh Supercomputer Center
300 S. Craig Street, Pittsburgh, PA 15213, USA
E-mail: jam@psc.edu

[1] Speaker

http://pos.sissa.it

PoS(ISGC 2013)011

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