The challenges of (non-)openness: Trust and Identity in Research and Education.

DEI 2018, Zagreb, April 2018
Ann Harding, SWITCH/GEANT
@hardingar

www.geant.org
Who am I? Why am I here?

Ann Harding, SWITCH
@hardingar

Medieval History,
Computer Science
Sociology

Activity Leader, Trust & Identity
Development
GÉANT
About GÉANT

GÉANT Association supports and represents over 40 NRENs across Europe.
Together they support over 10,000 institutions and 50 million academic users.
Trust, Identity & Security

Supporting users and enabling secure access to services

**eduroam** - secure global roaming access service **250+ million authentications per month** in 89 territories

**eduGAIN** - interconnects identity federations around the world, simplifying access to content, services and resources ~ 3500 identity providers accessing services

**AARC project** – collaborating with e-infrastructures, research collaborations, libraries & federations to share policies, architectures, training materials & pilots that avoid re-inventing the authentication & authorisation wheel

**REFEDs** – supporting identity federations worldwide

**Trusted Introducer** – services for security and incident response teams

**Certificate Service** – delivering cost-effective digital certificates.

In partnership with [digicert](https://www.digicert.com)
AAI as seen from “Realising the European Open Science Cloud“

“Build on existing capacity and expertise where possible”.

“The major technical challenge is the complexity of the data and analytics procedures across disciplines rather than the size of the data per se.”

“Generic protocols ... ICT standards of e-infrastructure communities....”

“Combine single sign-on issues with the connection of social and professional people oriented web applications resulting in a federated identity and credentials for all people in the EOSC “
eduGAIN - existing capacity for EOSC

Enabling secure Single Sign On services to global research and educational resources

Federated identities enable users to access a wide range of services using a single account sign-on managed by their 'home' institution

- Improves access
- Improves security
- Reduces management overhead and costs.

April 2018:
50 Federations active
5 Federations with voting rights in process of joining
4572 entities
eduGAIN – building on existing capacity
eduGAIN - an open ecosystem of existing resources

- Federations, both national and community
- Home organisations ranging from schools to specialist research organisations and even some public/private initiatives
- Service providers ranging from for-profit journals, open source e-learning platforms, parking & expenses management systems, commercial clouds, research community services
- Common link – to serve research and education
Open does not mean the same for everyone
Yet everyone has to care about data access policies

Social Sciences, Arts and Humanities
Life Sciences
High-Energy Physics and Astronomy
Earth Sciences and Observations

How do we build an infrastructure open for everyone’s needs?
Openness leads to Complexity

More Machines (Moore's Law)

More People (Scholars, citizens)

e-infrastructure

HTC
Big
Compute
Big Data

Technology
Crowd Intelligence
Digital Research
Big Data Acquisition
Crowd Sourcing
Crowd Funding, open Innovation
Collaborative Design

Social Networks

Conventional Computing

Science 2.0

The Future

www.geant.org
Complexity of requirements – generic infrastructure

eduGAIN Services 2016 and Services 2018

- Campus Infrastructure
- Library & Journals
- Teaching & Learning
- Cloud Service
- Collaboration Platform
- Research Service
- Other
- Uncategorised

Complexity

www.geant.org
Network Design Pattern

- Design pattern 1: Protect your elephant flows
- Design pattern 2: Unclog your data taps
- Design pattern 3: Build a well tuned end to end infrastructure

Trust and Identity Design Pattern

- Design pattern 1: Enable your collaboration flows
- Design pattern 2: Unclog your policy taps
- Design pattern 3: Build a well trusted end to end infrastructure

Science DMZ, the Trust and Identity View

Design pattern 1: Enable your **collaboration** flows
- Export IdPs to eduGAIN
- Export eResearch SPs to eduGAIN
- Make sure you can provide human support

Design pattern 2: Unclog your **policy** taps
- For hub and spoke – do you need the same policies for all your users? Can you be more flexible?
- For full mesh – do you need to leave everything to the edges? Can you use your resource registry/central tools to apply policy for e-Research more scalably?

Design pattern 3: Build a **well trusted end to end infrastructure**
- Use Research and Scholarship and GÉANT Code of Conduct Entity Categories to make trust scale beyond your federation
- Adopt SIRTFI incident response framework to build trust
Openness – Learning to speak each other’s language

Public comments due by 12 December 2017: OASIS SAML V2.0 Subject Identifier Attributes Profile Version 1.0 docs.oasis-open.org/security/saml-... < "best practice" user identifiers for #SAML subjects (cf. #OIDC 'sub' claim)

still a lot of work to do but: ' In our ChIP-seq experiments, 46/305 mAbs (15%) against 36/176 (20.5%) targets passed as per ENCODE standards (Supplementary Table 7)'

6:40 PM - 13 Nov 2017

10:08 AM - 20 Mar 2018
AARC and eduGAIN – responding to complexity

eduGAIN has helped many collaboration communities to interconnect and access / share resources. Policies, best practices and support have all been enhanced in the last 5 years.

To go above the baseline of eduGAIN, AARC is creating a common AAI framework for research and collaboration communities that should work for everyone:

• One blueprint architecture
• One set of policies
• One set of training resources
• Working with research collaborations to pilot and improve technical and policy aspects

Relationship between the AARC blueprint architecture, eduGAIN and the GÉANT network.
Generic Protocols & Standards: AARC Blueprint Architecture for Interoperability of AAIs

- **User Identity**: Social, eGov
- **Identity Access Management**: IdP
- **Proxy**: Token Translation
- **End Services**: SP
- **Authorisation**

https://aarc-project.eu/blueprint-architecture/
Infrastructure to support research -

Collaboration platform to enable use of federated identity in research communities

Supports AARC architecture

Neutral partner for any e-Infra or Research Infra inc. “long tail”, informal groups
The Lego Approach

- **User Identity: eduTEAMS Identity Hub**
  - One persistent (SAML) IdP for many ‘Guest’ Identity Providers
  - Provides Account recovery if users change main a/c
  - Available and accessible through eduGAIN
  - Supports Research and Scholarship Entity Category

- **User Attributes: eduTEAMS Membership Management service**
  - VO specific workflows for onboarding members
  - Accessible through eduGAIN

- **End Services: Discovery Service**
When Privacy Meets Openness
InAcademia is a service being developed that simply validates to other services that the user is a student or staff member of the academic community. Helps service providers offer academic discounts online and in real time.

A lightweight federated identity process with minimal attribute release (essentially a simple yes/no).

Easy for Service Providers to implement.

Removes need for scans of ID cards or primitive e-mail address-based 'authentication'.
Openness in Summary

- Open Services
- Open Architectures
- Open Policies
- Open to New Technologies
- Open to New Use Cases
- Open to Service Models
- Open to Flexibility
- Open to Privacy
- Open for Science