Privacy Framework for Attribute Release in an (Inter)Federation

Valter Nordh, NORDUnet / GU
Mikael Linden, CSC
Steven Carmody, Brown University
The eduGAIN interfederation service is intended to enable the trustworthy exchange of information related to identity, authentication and authorisation between the GÉANT (GN3) Partners' federations. The eduGAIN service will deliver this through co-ordinating elements of the federations' technical infrastructure and a policy framework controlling the exchange of this information.

www.edugain.org
Introduction to the eduGAIN service
Introduction to the eduGAIN service

- 7th generation of the pan-European Research and Education Network infrastructure – continuation of a success story
- Connects 40 European countries through 32 NREN Project Partners & 4 NREN Associates
- 50,000km of network infrastructure and 12,000km of lit fibre
- 40 million users
- Outstanding service availability
Introduction to the eduGAIN service

- The eduGAIN interfederation service – created and built within the GÉANT project

- Funding of the GÉANT project comes from EU NRENs and the EC

- During the development of the eduGAIN service mostly federation operators has been represented (from participant NRENs)
Introduction to the eduGAIN service

- eduGAIN in GN3 is built as a full mesh-model, where all entities talk to each other.

- Lightweight central components, both technically and process-wise, designed so that it’s easy to join.

- Low bar for joining – more complex to manage all possible interactions.

- Normally a federation exposes a part of it’s services / identity providers to interfederation, so called opt in.
Introduction to the eduGAIN service

- eduGAIN entities are (normally) a subset of a federation
- Profiles and policies to harmonize environment
eduGAIN policy (and trust) framework
Federation is all about trust

- **SP needs to trust the IdP**
  - **LoA**: quality of identities and authentication are as agreed
  - **Schema**: attributes and their semantics are as agreed
- **IdP needs to trust the SP**
  - **Privacy**: That the SP does not infringe the privacy laws
- Everyone needs to trust the federation operator
  - **Security**: Operations are done securely
  - **Rules**: Operations follow the federation rules
- These issues are covered in the federation policy (agreement)

- No federation policy => no federation
  - c.f. PEER, a pure SAML metadata delivery service
Starting point for the eduGAIN service

- **Heterogeneous** national federations
  - Sectors covered: universities, research institutions, schools...
  - Level of Assurance (LoA): reliability of identities/authentication
  - Attributes. Recommended attributes. Semantics (ePAffiliation)
  - Privacy mechanisms: attribute release policies, consent modules
  - Incident handling mechanisms
  - Liability, indemnification, other typical contractual issues

- eduGAIN didn’t want to make the national federations to change policies
  - Would have caused too much trouble/hassle for the federations
eduGAIN’s approach

- Keep the bar low for federations to join
- Don’t exclude anyone
- Keep the basic level of trust low
- Introduce optional profiles for higher levels of trust
  - Data protection
  - Level of Assurance
Introduction to the eduGAIN service

- The eduGAIN interfederation service is targeting federations

- Federations target IdPs and SPs!

- eduGAIN provides the means for entities to exchange information – but what gets exchanged is up to the exchangers

- Legal issues when transferring PII between entities in an international context
In this environment, what solutions are there to assist a SP in getting the “rights” attributes needed from IdPs in an international environment?

eduGAIN SP Code of Conduct…
eduGAIN resources

- www.edugain.org
- eduGAIN service definition and policy
- Presentation from TNC2011 on how SWITCH AAI and eduGAIN by Lukas Hämmerle (well worth reading/watching!)
  “Trimming your AAI federation fit for eduGAIN… technically”
  Slides available [here](#)
  Online presentation [here](#) (starting at around 58 min)
- eduGAIN policy
  Recommended reading with regards to the policy:
  Introduction to the eduGAIN Policy Framework
  eduGAIN Constitution
  eduGAIN Declaration (the document a federation sign and publish)
- Contact the eduGAIN OT at edugain-ot@geant.net