Interfederation through eduGAIN - steps and challenges

eduGAIN interfederation service

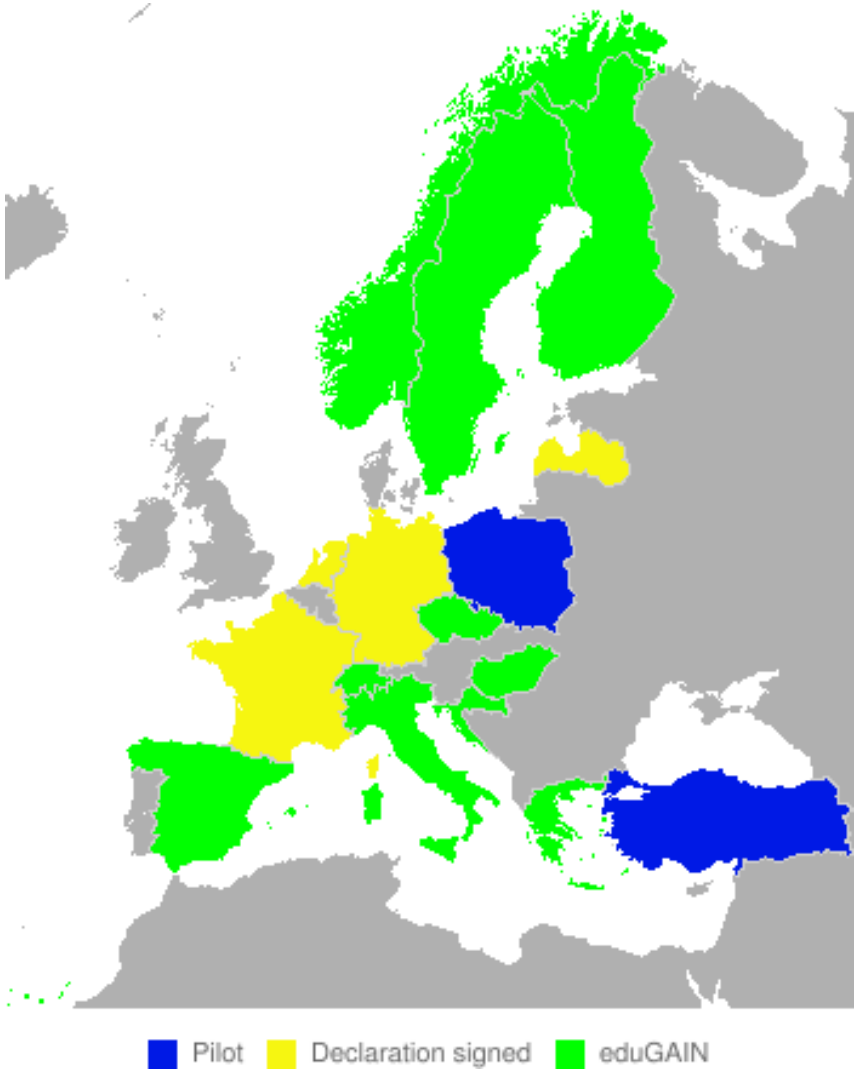
2012-02-27 Federated Identity Systems for Scientific Collaborations workshops: Taipei

Valter Nordh, NORDUnet / GU

Introduction to the eduGAIN service

- 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



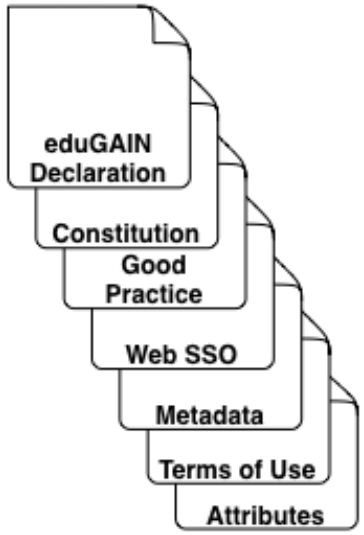
Introduction to the eduGAIN service

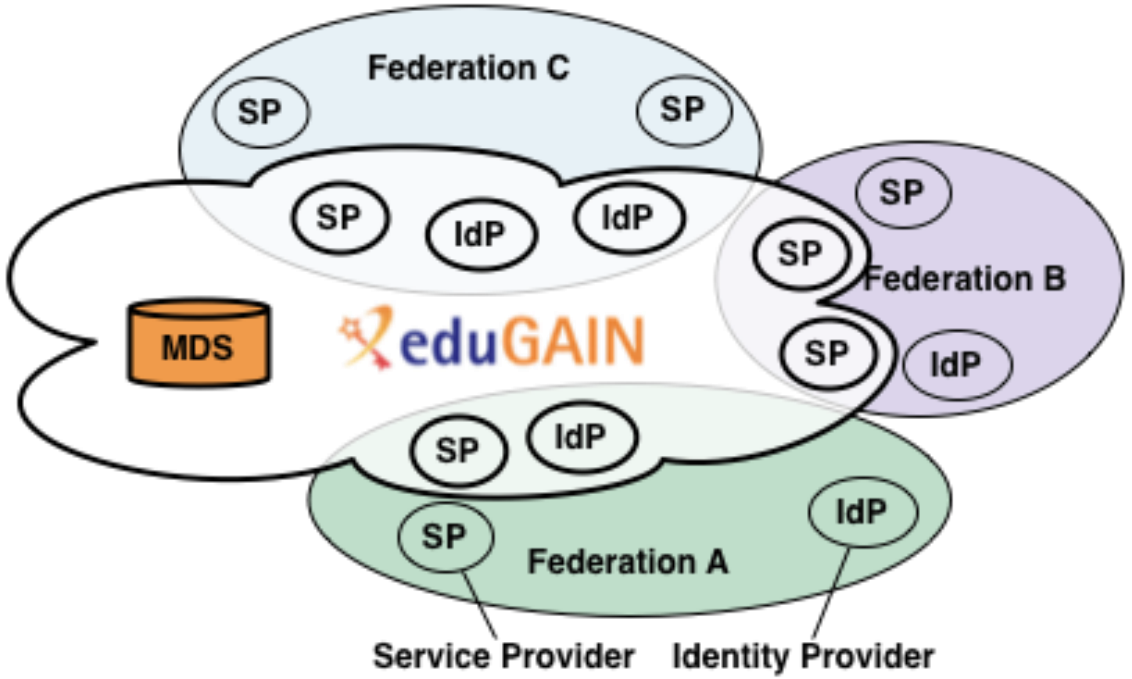
- The eduGAIN interfederation service – created and built within the GÉANT project
- Funding of the GÉANT project comes from EU NRENs and the EC
- During the development of the eduGAIN service mostly federation operators has been represented (from participant NRENs)

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

Innovation through participation

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)

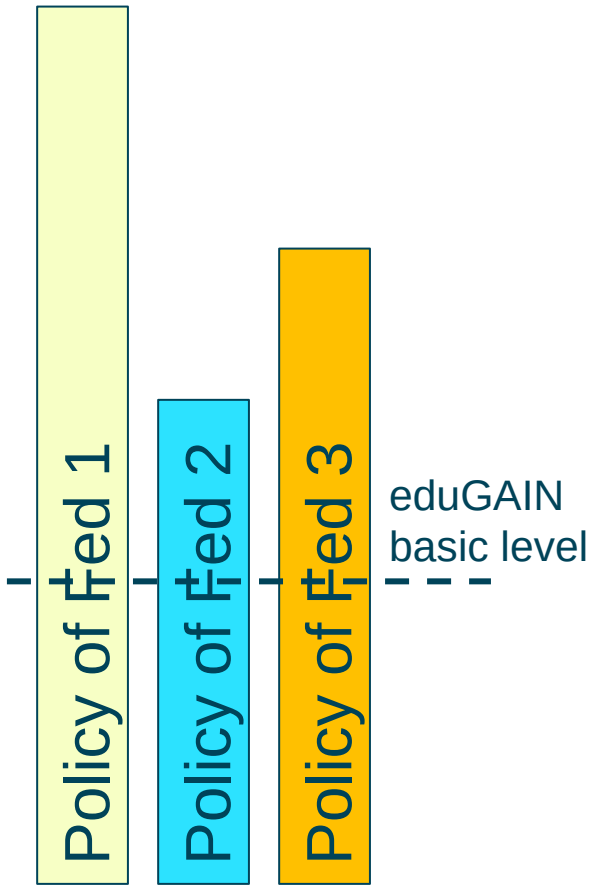
- No federation policy => no federation
  - c.f. PEER, a pure SAML metadata delivery service

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

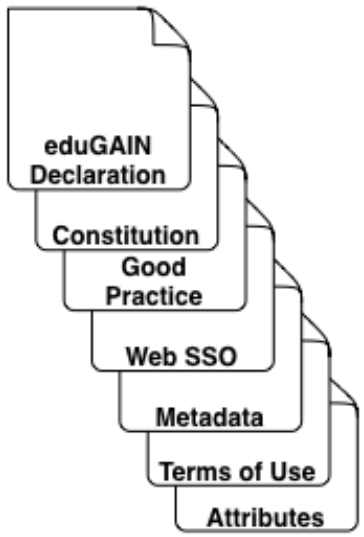


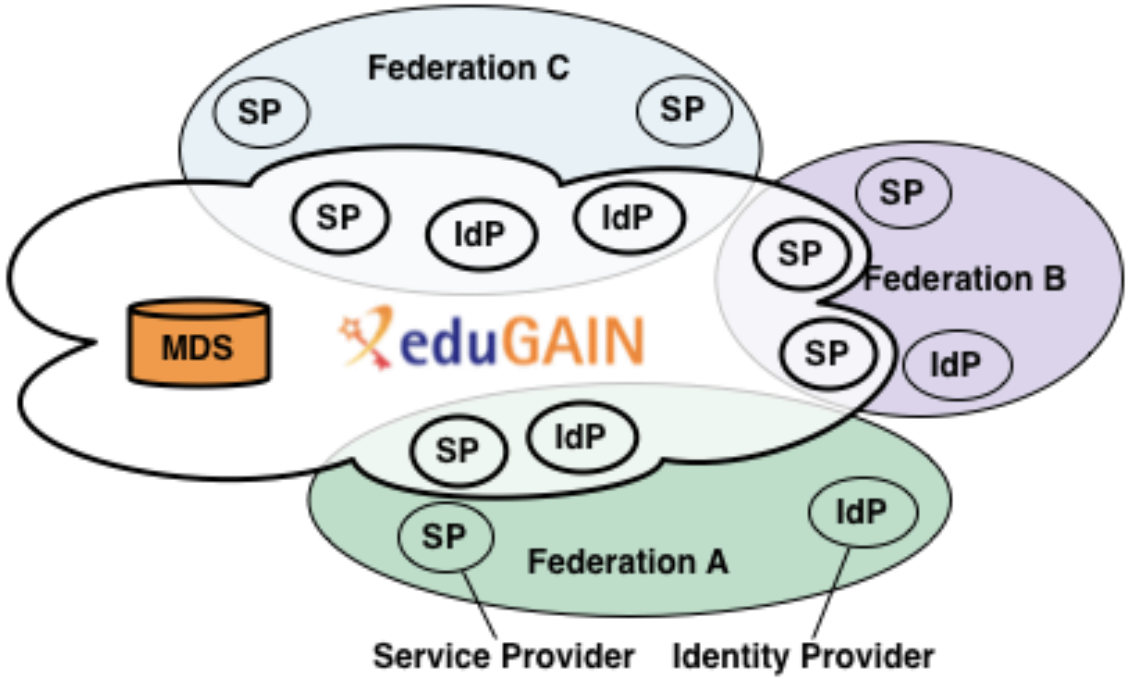
- Keep the bar low for federations to join
- Don't exclude anyone
- Keep the basic level of trust low
- Introduce optional profiles for higher levels of trust
  - Data protection
  - Level of Assurance

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 the up to the exchangers
- Legal issues when transferring PII between entities in an international context

Introduction to the eduGAIN service





- 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 SP Code of Conduct

Innovation through participation

The problem

Data controller

Data controller

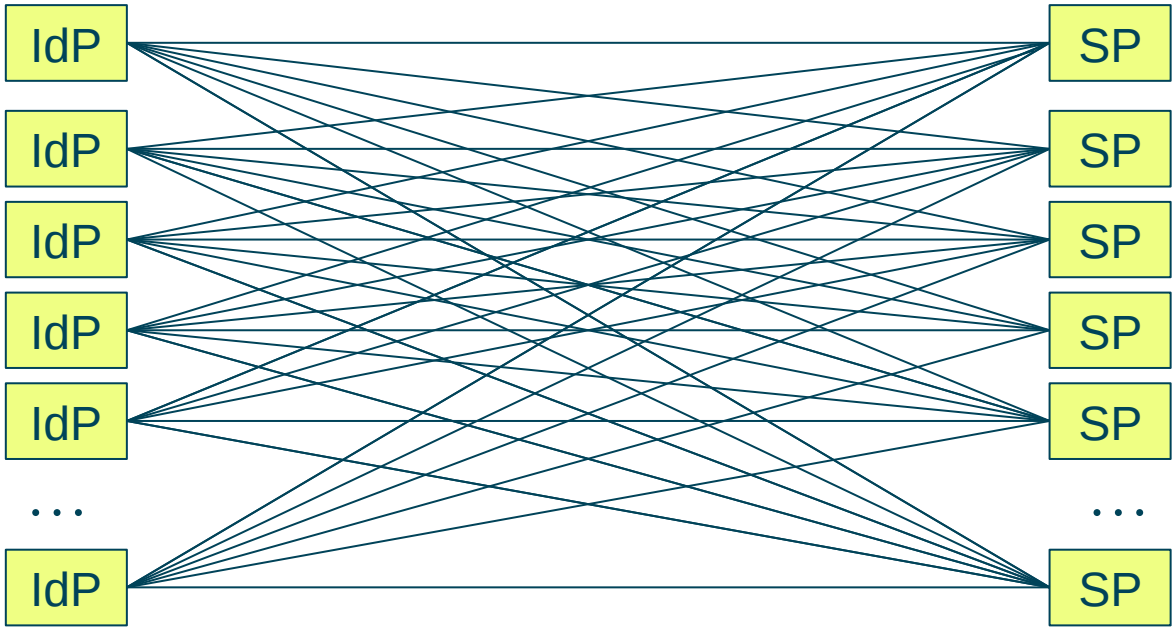
- IdP takes privacy risks when it releases personal data to an SP
- What if the SP gets hacked and personal data leaks to the Internet?
  - The regulator fines or end user sues the SP?
  - The regulator fines or end user sues the IdP??

=> To avoid risks, IdPs hesitate to release attributes to SPs

- Unless we manage to develop a framework which reduces the IdP risks

=> Privacy Code of Conduct

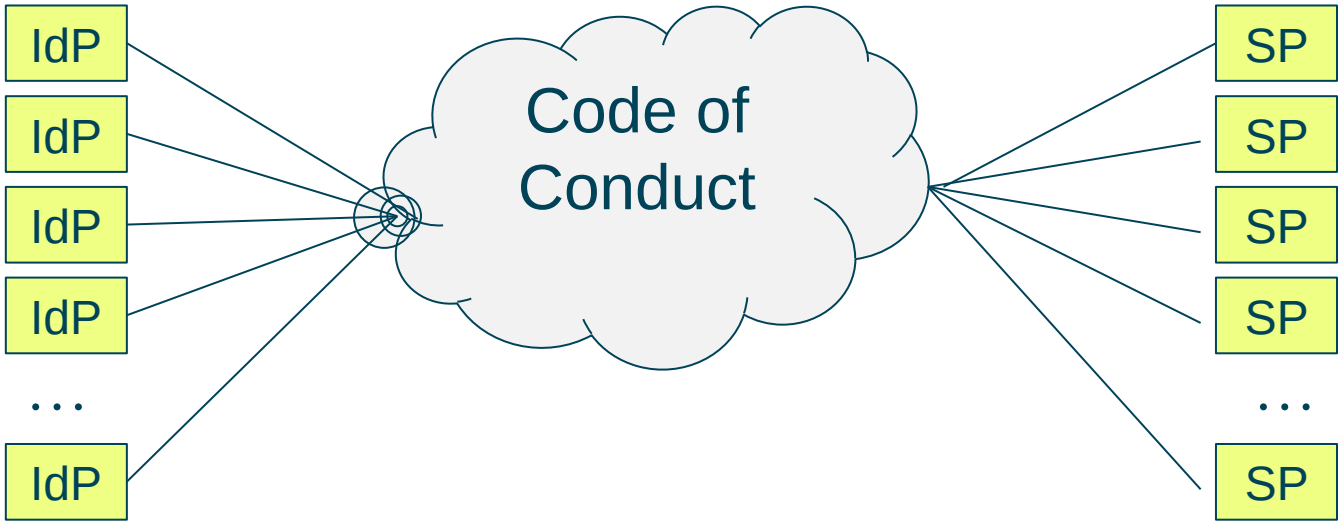
Abandoned solution: bilateral contracts between IdPs and SPs



- There are potentially hundreds or thousands of IdPs and SPs

=> bilaterals do not scale

The proposed approach



1. SPs commit to the Privacy Code of Conduct
   - Derived from the EU Data protection directive
   - Federation's SAML metadata is used to mediate the commitment
2. IdPs can see that SPs have committed to the CoC
   - We hope that this eases the release of attributes needed by SPs

Requirements and limitations

Requirements

- **Balance the risks and the easiness of collaboration** for research and higher education
- Try to **avoid big changes** to current architecture (such as, existing federation agreements)
  - Would slow down adoption

Scope limitations

- Only **non-sensitive personal data** is released
- Limit to transfer **to EU/EEA countries** in the beginning
  - The General data protection regulation may ease release out of EU

Process

- SP declares it abides by the CoC
- IdP may feel more comfortable
  - And release attributes to that SP
- Job done ☺

SP Code of Conduct

- Data minimisation
  - Only strictly necessary attributes
  - Choose least intrusive option
- Grounds for processing
  - That necessary to deliver the service
  - Don’t offer the users extras
- Privacy statement available to the user
- Use of attributes
  - Only for access control and personalisation
- Security of information
  - Organisational and technical measures
  - Deleted when no longer needed

Requirements for SPs

- Publish a signed (digitally/ink) CoC for SPs
  - Include a link to the document in the SAML metadata
- List the attributes required by the SP
  - Using RequestedAttribute elements in the SAML metadata
- Write and publish a Privacy Policy document
  - Link it from the SPs landing page
  - Reference it in the SP metadata (mdui:PrivacyStatementURL)
- Add other required SAML metadata elements
  - Mdui:DisplayName
  - Mdui:description
  - Mdui:logo
- Take care of your SPs security issues

Requirements for SPs

- Development of eduGAIN CoC
- In February we held an initial workshop in Brussels, see:
  https://www.terena.org/events/details.php?event_id=2211
  Here is the actual text for the CoC hosted.
- We are now gathering opinions from involved stakeholders, and plan to go for a review process in April.
- Please send us your comments, ideas etc for inclusion!
  Mikael Linden, CSC, is responsible for developing the Code CoC:

  Mikael.Linden@csc.fi

Questions and Answers

- Q a A

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