Interfederation

SWITCHaai Team
aai@switch.ch

Agenda

- Why Interfederation?
- Status
- Scalable Attribute Release
- GÉANT Data Protection Code of Conduct & Privacy Policy
- How to Interfederate in SWITCHaai?

Why Interfederation?

- Federations are mostly of national scope
  - Services may need to register in multiple federations to serve all their users. That's time consuming and becomes a huge overhead.
    e.g. EBSCO Publishing is registered in 21 federations!
- Research projects are mostly multi-national

- **Interconnecting national federations ➔ Interfederation**

➔ Register the IdP or SP in only one federation and enable it for interfederation
  - Enable the IdP for interfederation
    ➔ Its users will be able access services from other federations
  - Enable the SP for interfederation
    ➔ The service can serve users from other federations

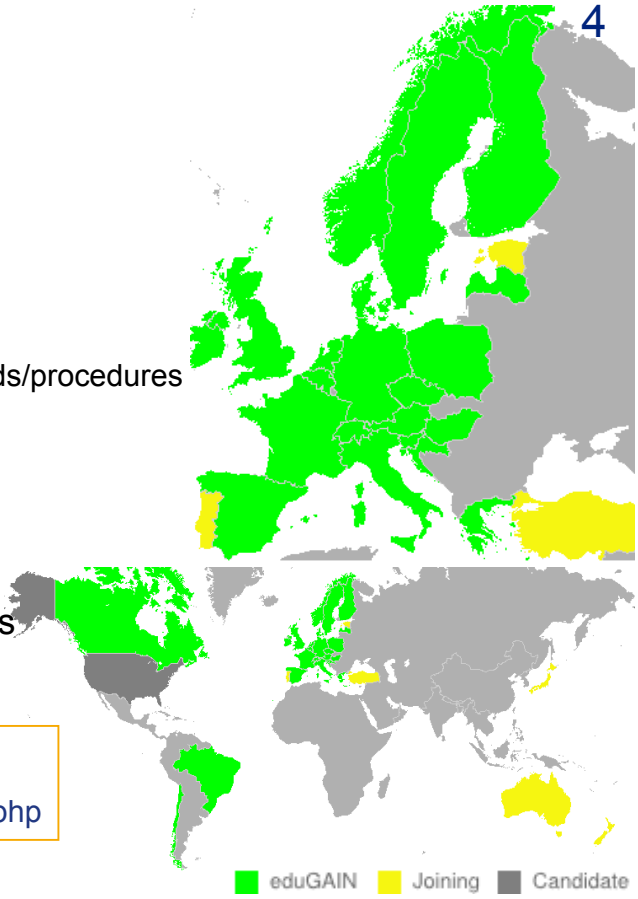
eduGAIN Status

- eduGAIN is the GÉANT Interfederation Service

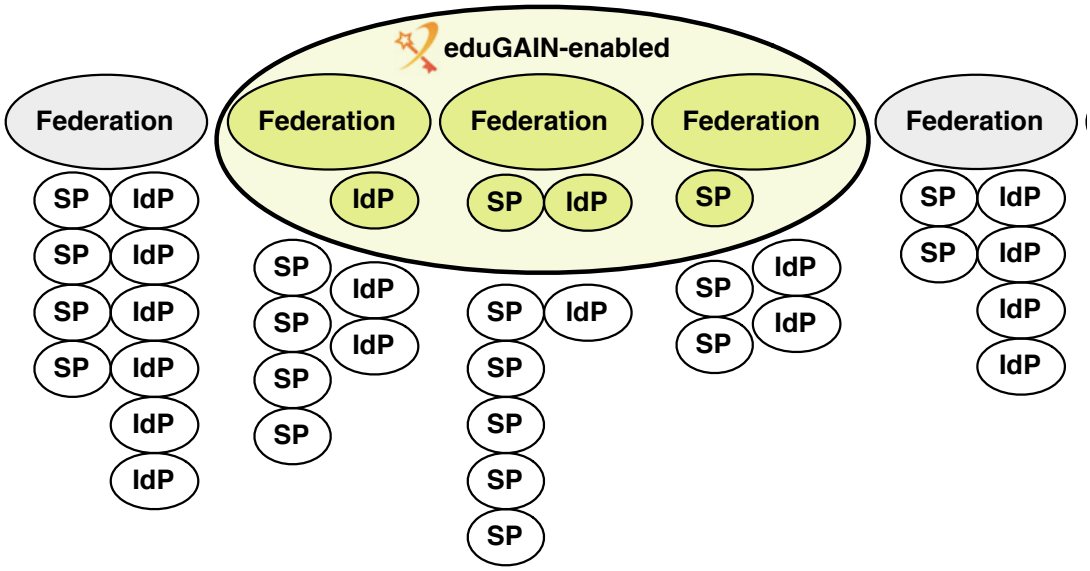
- eduGAIN design principles
  - Low barrier to entry
  - No mandate to change local standards/procedures
  - Minimal central infrastructure

- Status March 2014
  - Total: 200 IdPs, 103 SPs
  - From SWITCHaai: 8 IdPs, 8 SPs

http://www.edugain.org
http://www.edugain.org/technical/status.php

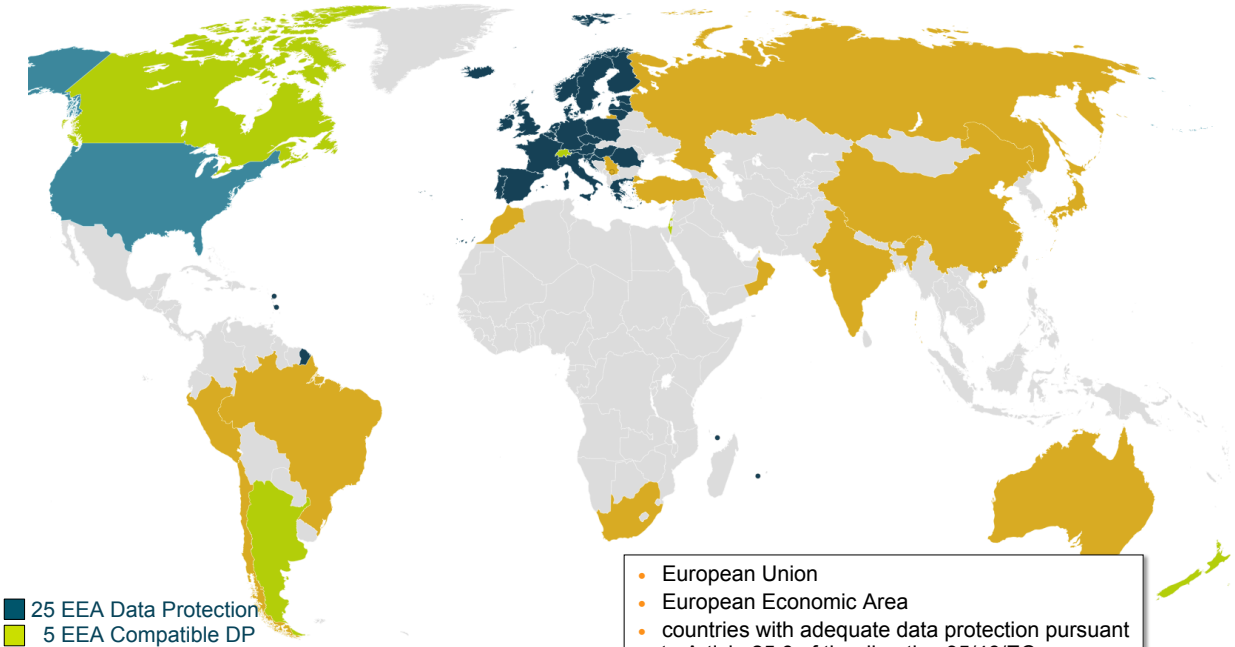


eduGAIN Adoption Width vs. Depth



- Good federation adoption (Width)
- Entity Adoptions (Depth) is growing (110% increase in 2013, 129% for SPs)
- Not every SP and IdP has requirements to interfederate

Federations & GÉANT Data protection Code of Conduct



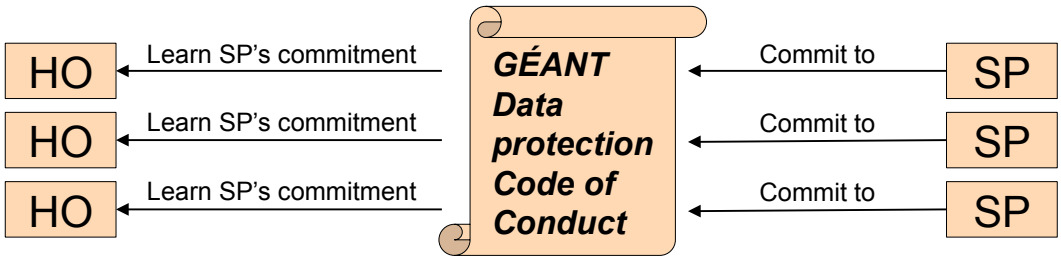
25 EEA Data Protection
5 EEA Compatible DP
1 Safe Harbor (USA)
13 Federations outside GÉANT CoCo (4 in or joining)

- European Union
- European Economic Area
- countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC
  - e.g. Switzerland
  - e.g. the US safe harbour

GÉANT Code of Conduct – Data Protection within eduGAIN

We need to increase the trust in Service Providers (SPs)

- The method is based on the EU Data Protection directives
- That will encourage the Home Organisation IdP to release attributes



Code of Conduct Toolkit

- Data Protection Code of Conduct for SPs in EU/EEA
- SAML2 profile for the Data Protection Code of Conduct
- Entity category attribute definition for the Code of Conduct

Data Protection Code of Conduct (DP CoCo)

Normative documents:

- Data Protection Code of Conduct for SPs in EU/EEA
- SAML2 profile for the DP CoCo
- Entity category attribute definition for the DP CoCo

Non-normative, informational documents:

- Introduction
- Introduction to the DP directive
- Risk management
- Privacy policy guidelines
- What attributes can an SP request
- Good practice for Home Organisations
- Federation operator guidelines
- Handling non-compliance
- IdP GUI guidelines

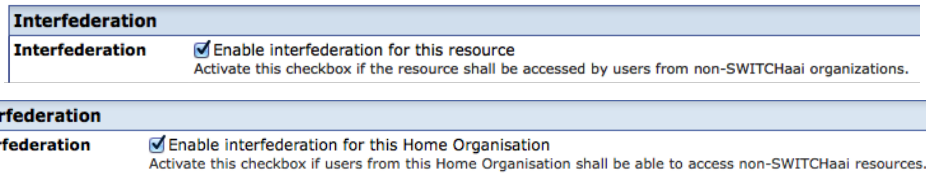
https://refeds.terena.org/index.php/Data_protection_coc
https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook

The Steps to Interfederate in SWITCHaai

1) Once per SWITCHaai Participant from the SWITCH Community a signature is required (see next slide)

2) SWITCH will set the 'flag' in the Resource Registry

3) Now, SP and IdP administrators can opt-in for interfederation;
   - they first adapt their SP and IdP configurations according to the "Enabling Interfederation Support" guides
     the IdP administrator installs and configures uApprove to support user consent
   - Finally the administrator can click the checkbox in the Resource Registry!



https://www.switch.ch/aai/interfederation
https://www.switch.ch/aai/docs/interfederation/sp-deployment.html
https://www.switch.ch/aai/docs/interfederation/idp-deployment.html

SWITCHaai Interfederation Access Declaration

Signing the Interfederation Access Declaration asserts:

1) the institution is aware of the additional data protection requirements when releasing personal data beyond SWITCHaai participants.

2) the institution acknowledges that it is liable for the actions of its End Users according to the "Service Regulations for Services by SWITCH" and the "SWITCHaai Service Description"

3) that the IdP supports user consent (uApprove module)

4) the SPs will adhere to the "Data Protection Code of Conduct" (CoCo) and implement a privacy policy along the CoCo-criterias

https://www.switch.ch/aai/interfederation
https://wiki.edugain.org/How_to_write_the_privacy_policy