

Interfederation



SWITCH

SWITCHaai Team
aai@switch.ch

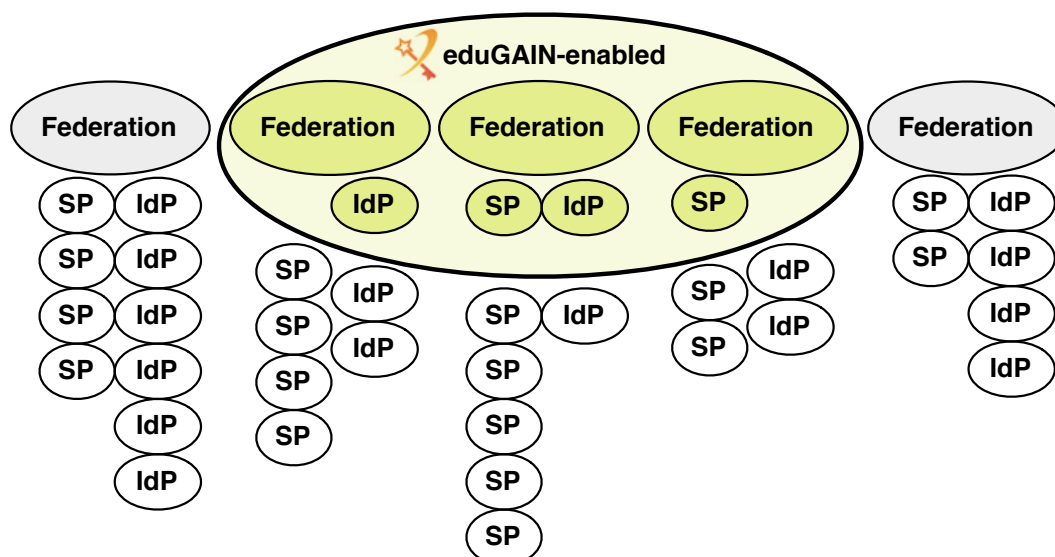
Agenda

- 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 22 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 Adoption Width vs. Depth



- Good federation adoption (Width)
- Entity Adoptions (Depth) is growing
- Not every SP has requirements to interfederate

Interfederation Status

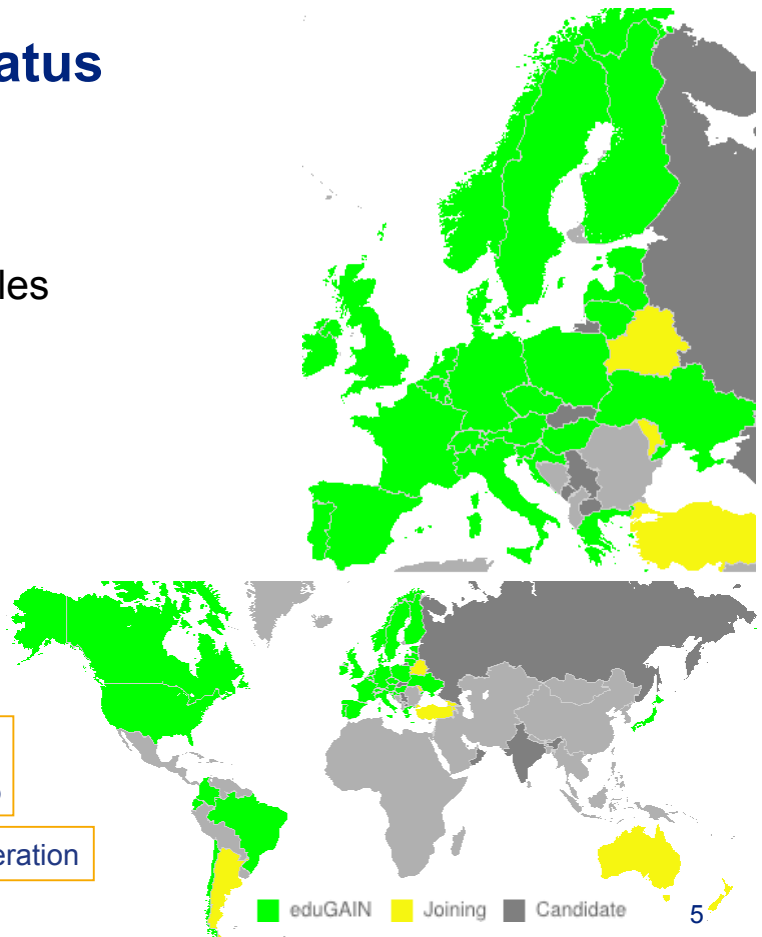
- eduGAIN is the GÉANT Interfederation Service
- eduGAIN design principles
 - Low barrier to entry
 - No requirements to change local standards/procedures
 - Minimal central infrastructure
- Status August 2015
 - Total: 1412 IdPs, 965 SPs
 - From SWITCHaai: 20 IdPs, 8 SPs

<http://www.edugain.org>

<https://technical.edugain.org/status.php>

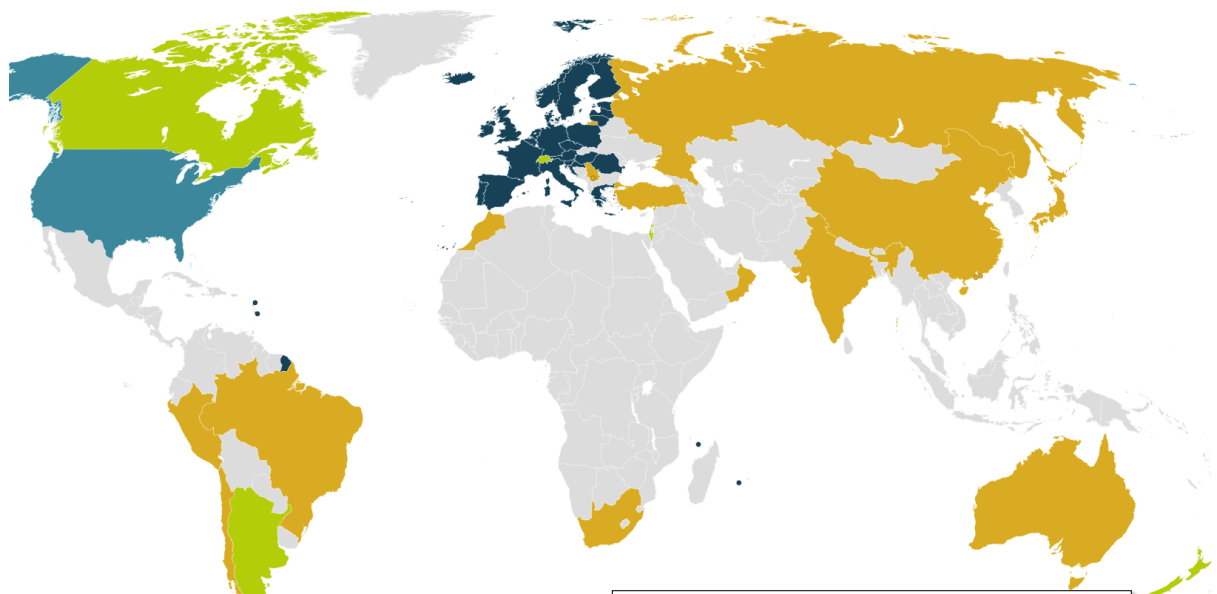
<https://www.switch.ch/aai/interfederation>

© 2015 SWITCH



5

Federations & GÉANT Data protection Code of Conduct



- 25 EEA Data Protection
- 5 EEA Compatible DP
- 1 Safe Harbor (USA)
- 13 Federations outside GÉANT CoCo

- 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

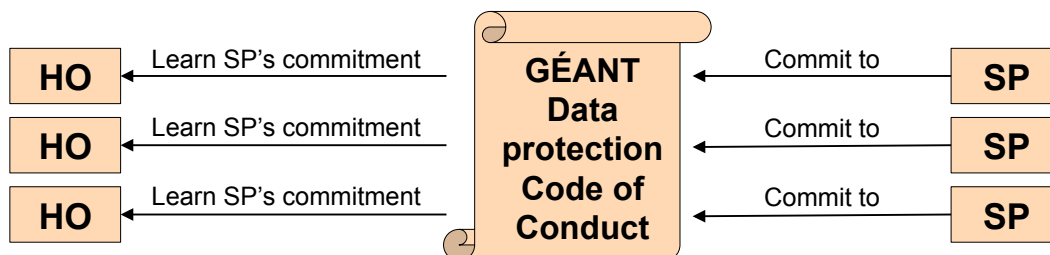
© 2015 SWITCH

6

GÉANT Data Protection Code of Conduct

Increase the trust in Service Providers (SPs)

- The method is based on the EU Data Protection directives
- The SP has to provide a Privacy Policy (in English, according to the guideline)
- That will encourage the Home Organisation IdP to release attributes
 - ➔ attribute release will scale



Code of Conduct Toolkit

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

Data Protection Code of Conduct (DP CoCo)

Normative documents

- [Data Protection Code of Conduct for SPs in EU/EEA](#)
- Entity category specification for the DP CoCo
- SAML2 profile for the DP CoCo

<http://www.geant.net/uri/dataprotection-code-of-conduct/v1/>

Non-normative, informational documents

- Introduction
- Introduction to the DP directive
- Managing DP risks using CoCo
- [Privacy policy guidelines for SPs](#)
- What attributes can an SP request
- [DP good practice for Home Organisations](#)
- Federation operator guidelines
- Handling non-compliance
- [IdP inform/consent GUI guidelines](#)

<https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>

Cookbook for DP CoCo

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;
 - First adapt the SP or IdP configuration according to the "Enabling Interfederation Support" guides
 - The IdP administrator configures user consent
 - Finally the administrator can click the checkbox in the Resource Registry!

Interfederation	
Interfederation	<input checked="" type="checkbox"/> Enable interfederation for this resource Activate this checkbox if the resource shall be accessed by users from non-SWITCHaai organizations.

Interfederation	
Interfederation	<input checked="" type="checkbox"/> Enable interfederation for this Home Organisation Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources.

<https://www.switch.ch/aai/interfederation>

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 (for IdPv2 install uApprove)
- 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