Interfederation

Introduction, update & current status

SWITCH

Thomas Lenggenhager
thomas.lenggenhager@switch.ch

Berne, 13 August 2014

Agenda

- Why Interfederation?
- Status
- Scalable Attribute Release
- GÉANT Data Protection Code of Conduct & Privacy Policy
- Entity Category Attributes
- How to Interfederate in SWITCHaai?
- Tools to explore Interfederated Entities

Why Interfederation?

- Federations are mostly of national scope
  - Services may need to register in many 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

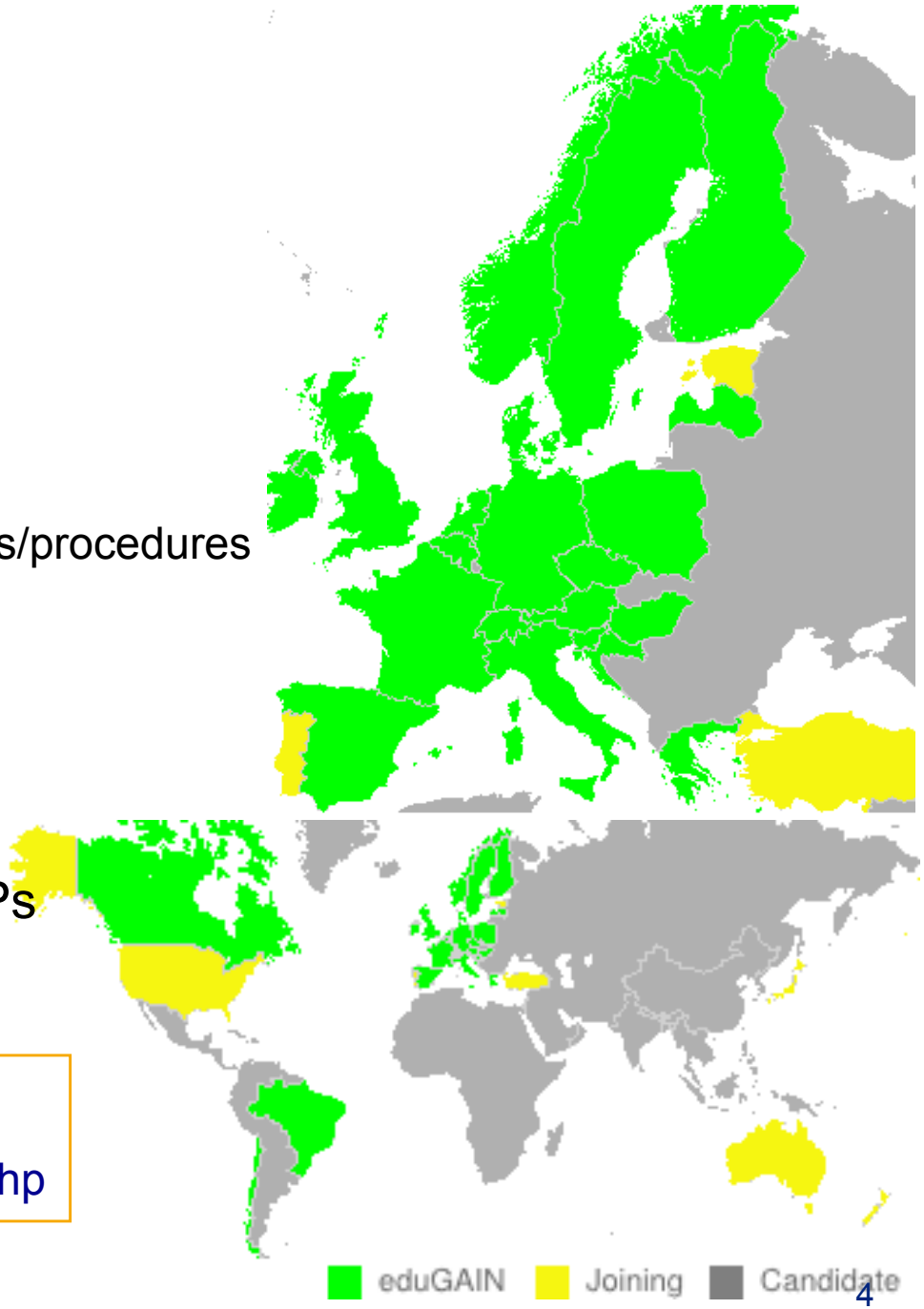
- Enable the IdP for interfederation
  - ➔ Its users will be able access services from other federations
- Enable the SP for interfederation
  - ➔ The service can serve users from other federations

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

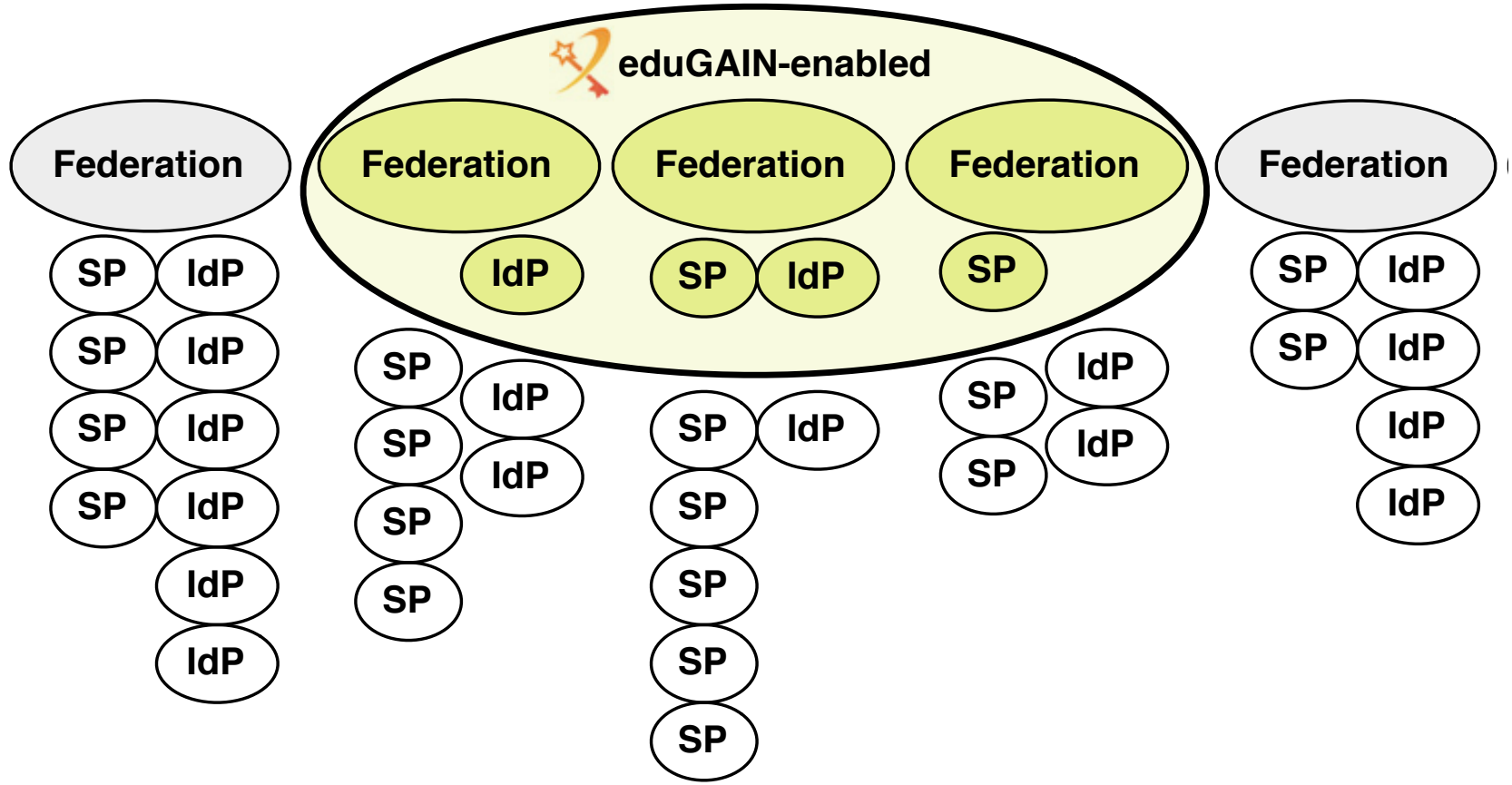
- Status July 2014
  - Total: 513 IdPs, 138 SPs
  - From SWITCHaai: 12 IdPs, 8 SPs



http://www.edugain.org

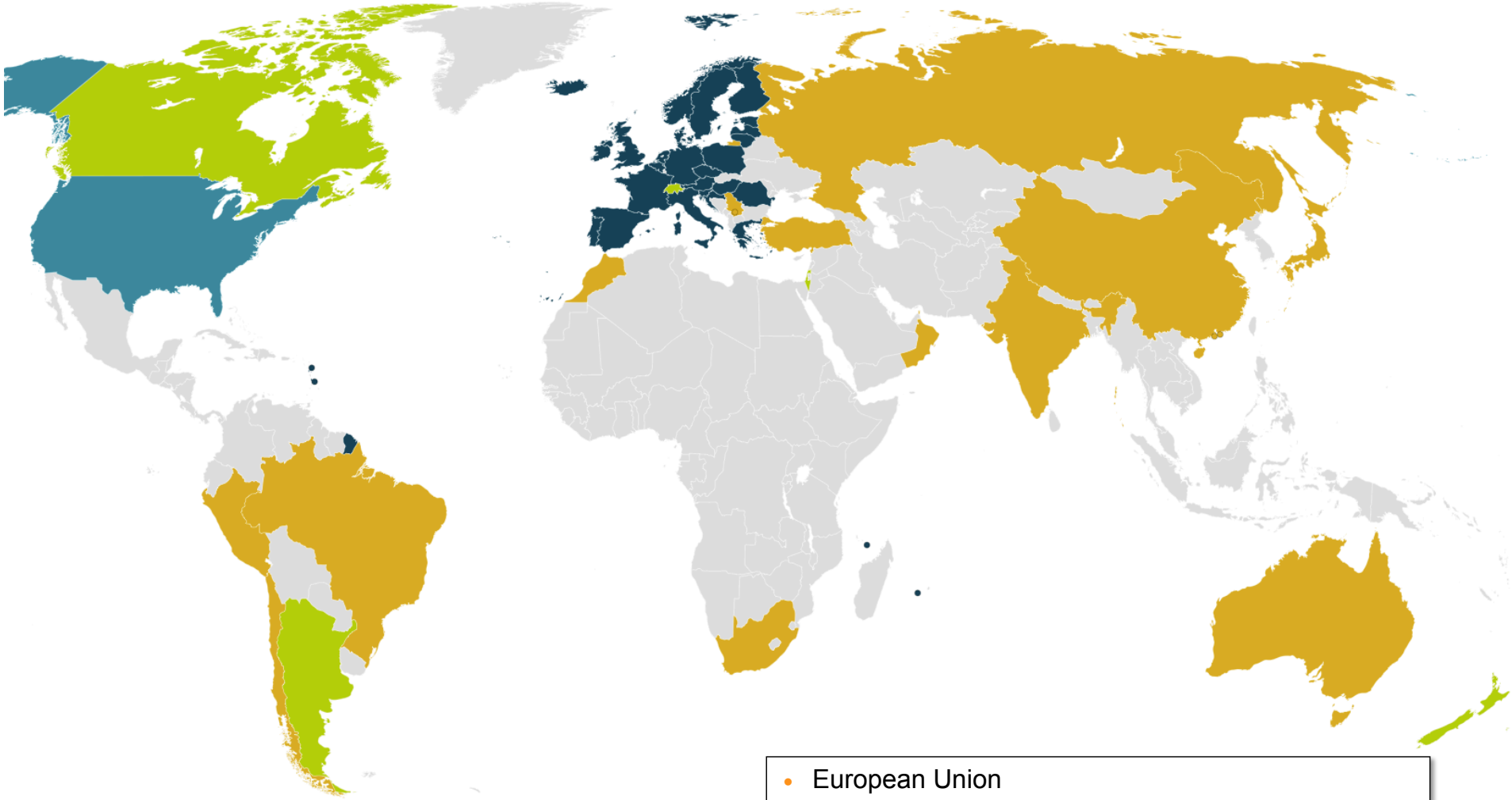
http://www.edugain.org/technical/status.php

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



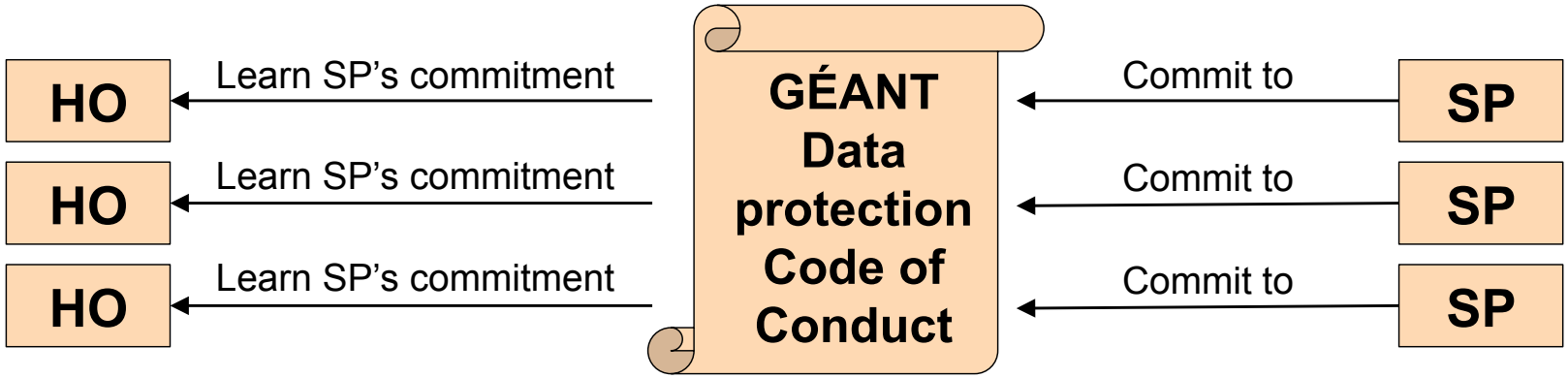
25 EEA Data Protection
5 EEA Compatible DP
1 Safe Harbor (USA)
13 Federations outside GÉANT CoCo (4 in or joining)

- 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

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 attribute definition 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
- 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

Data Protection Code of Conduct Cookbook

https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook

Entity Category Attributes

- A means to express 'conformance' to a definition in SAML, in a machine readable way
  - An Entity Category requires a proper definition and a process
  - According to the process, the Federation Operator includes the 'SAML-snippet' into the entity description in metadata

- Motivation to introduce Entity Categories for interfederation?
  - Better scalable attribute release for interfederation due to (hopefully) wide deployment of these definitions

- The first two internationally accepted entity category definitions
  - GÉANT Data Protection Code of Conduct (CoCo)
    http://www.geant.net/uri/dataprotection-code-of-conduct/v1/
  - REFEDS Research & Scholarship
    https://refeds.org/category/research-and-scholarship/

A CoCo Entity Attribute Example

```
<EntityDescriptor entityID="https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth">
  <Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="http://rr.aai.switch.ch/"
                            registrationInstant="2014-08-06T14:17:48Z">
      <mdrpi:RegistrationPolicy xml:lang="en">
        https://www.switch.ch/aai/federation/switchaai/
        metadata-registration-practice-statement-20110711.txt
      </mdrpi:RegistrationPolicy>
    </mdrpi:RegistrationInfo>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      Name="http://macedir.org/entity-category"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>
          http://www.geant.net/uri/dataprotection-code-of-conduct/v1
        </saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  ...
</EntityDescriptor>
```

REFEDS Research & Scholarship (R&S) (1)

- Suitable for
  - *"Service Providers that support research and scholarship interaction, collaboration or management as an essential component"*
  - *"The service enhances the research and scholarship activities of some subset of the registrar's user community"*
- However
  - ***"Not to be used** for licensed content such as e-journals"*

- R&S Category Attributes Bundles
  - **personal identifiers:** email address, person name, eduPersonPrincipalName
  - **pseudonymous identifier:** eduPersonTargetedID
  - **affiliation:** eduPersonScopedAffiliation
- Minimal Subset of the R&S Attribute Bundle
  - eduPersonPrincipalName
  - mail
  - displayName OR (givenName AND sn)

mostly less than what is in a mail-footer but enough for most R&S services

REFEDS Research & Scholarship (R&S) (2)

- How will it work?
  - SP administrator applies for inclusion into this category
  - Federation operator (e.g. SWITCH, DFN, RENATER, GARR) checks application, approves it and adds snippet to metadata
  - SP requests a subset of R&S Category Attributes
  - IdP knows from metadata that SP is in the R&S Category
  - IdP that supports R&S Category is ready to release attributes
  - User consents the release

- An SP that is in the R&S Entity Category should increase confidence of IdP administrators

  → more likely to receive more attributes than without

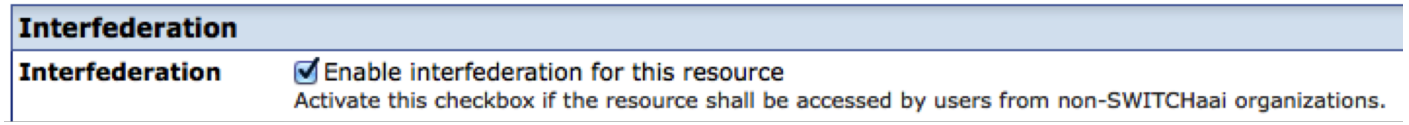
https://refeds.org/category/research-and-scholarship/

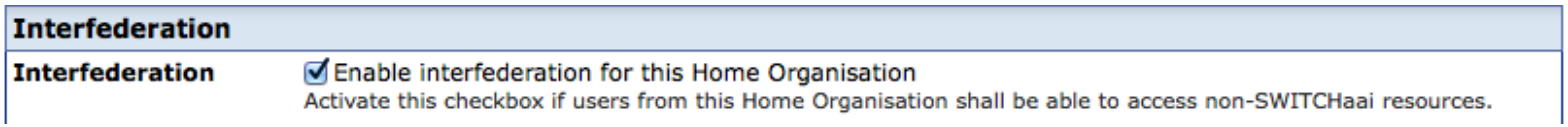
The Steps to Interfederate in SWITCHaai

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 enable 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 deploys a user consent module (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

Tools to explore interfederated entities

- Is a university IdP or an SP already interfederated?
  - go to: http://www.edugain.org/technical/status.php
  - pick the country where the entity might be registered
  - under 'Metadata URL' click on 'validate this metadata set', then on 'show entities list'
- or try the **Is Federated Checker** (beta)
  - go to: https://wiki.edugain.org/isFederatedCheck/
  - provide email addresses or domain names

- Which interfederated SPs are committed to the GEANT Data Protection Code of Conduct (CoCo)?
  - go to: http://monitor.edugain.org/coco

- **Federation Service Catalog** (proof of concept, best effort)
  - go to: http://www.terena.org/~schofield/servicecatalogue/
- Upcoming **REFEDS Metadata Explorer Tool** (MET) (beta)
  - go to: http://met.refeds.org/met/