

Resource Registry Interfederation Options

Interfederation via eduGAIN and Entity Categories



SWITCH

SWITCHaai Team
aai@switch.ch

Goals

- Get an idea of the benefits when participating in interfederation
- Know what it takes to enable an IdP for Interfederation
- Understand the concept of Entity Categories
- Recognize how Entity Categories can help in a data protection conformant attribute release that scales

Interfederation Option

What to consider before enabling an IdP for Interfederation



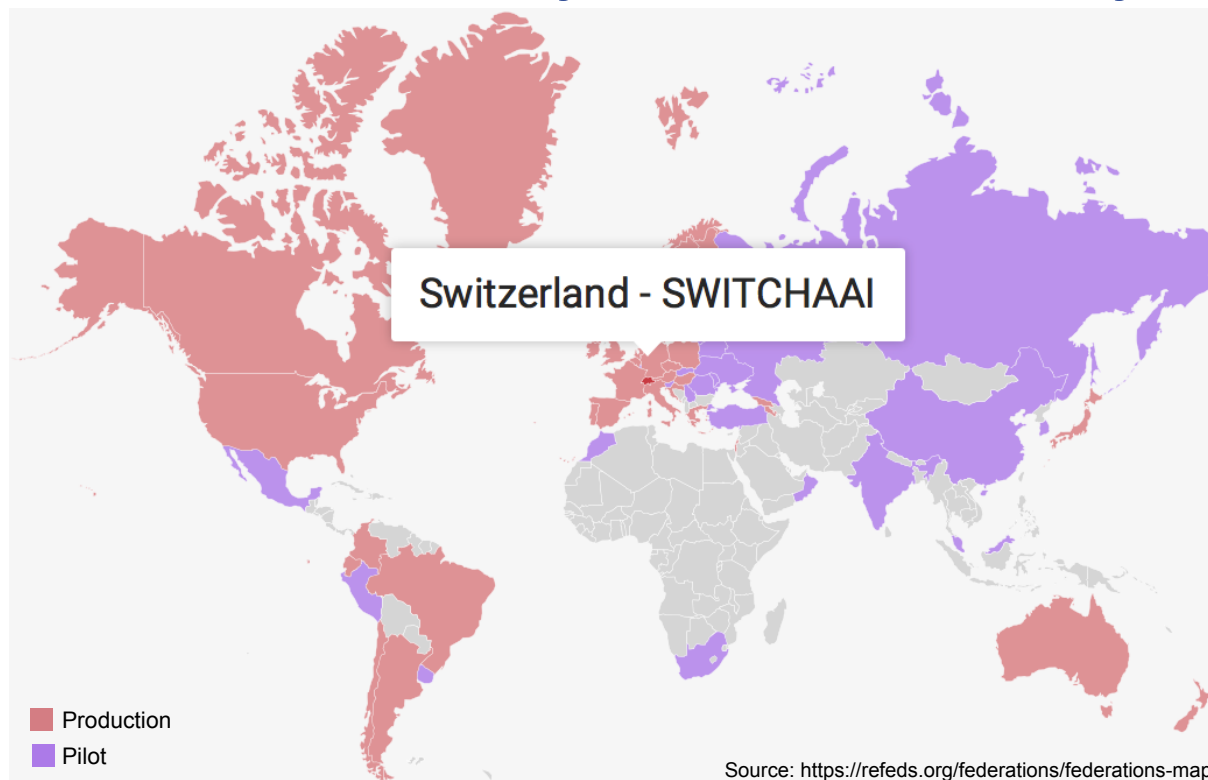
SWITCH

SWITCHaai Team
aai@switch.ch

Why Interfederation?

- Most Federations are 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. EBSCOhost 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 to **access services from other federations**
 - Enable the SP for interfederation
 - The service can **serve users from other federations**

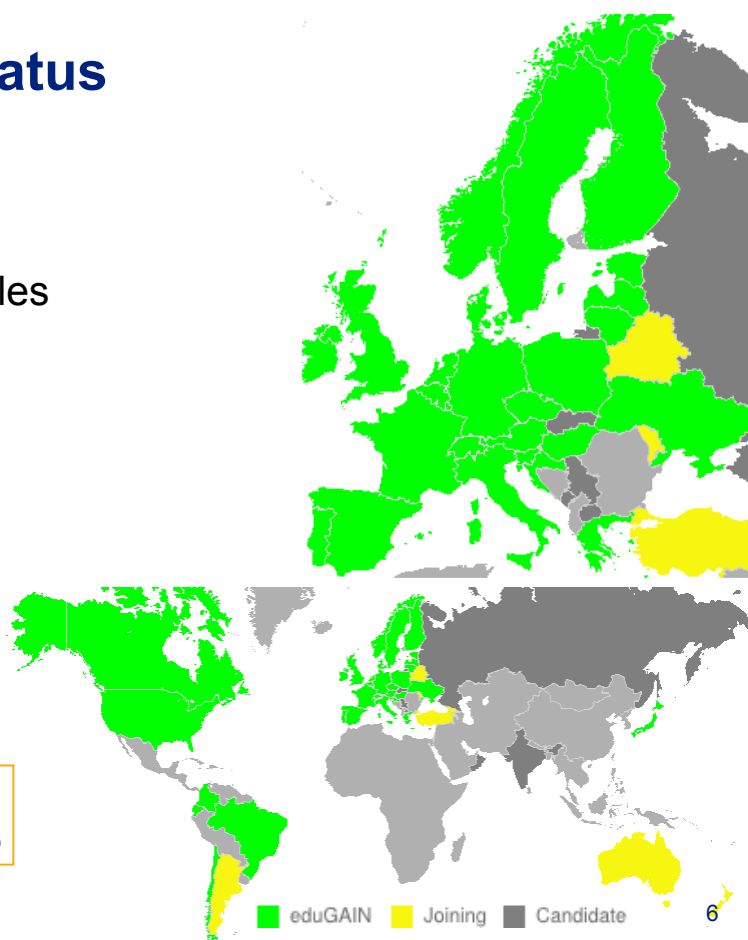
All Academic Identity Federations Globally



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>



Enabling Interfederation in the Resource Registry

Prerequisite

Due to **data protection** considerations, each institution needs to sign the *SWITCHaai Interfederation Access Declaration*

→ SWITCH will enable the checkbox in the Resource Registry

Interfederation

Interfederation Enable interfederation for this Home Organisation
Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources.

Enabling interfederation means that metadata about this resource is published in non-SWITCHaai organization and can be used by other Identity Providers which are not part of SWITCHaai. The metadata will also include contact information about this resource. Before enabling a service for interfederation, make sure that:

- All internationally standardized core attributes are declared as supported
- The default attribute release policy is adapted such that internationally used attributes are released to interfederation resources
- The specific attribute release rules are accurate and up-to-date

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

Recommended Interfederation Attributes

Friendly name	Defined in	Example
displayName	eduPerson	Peter Sample
common name (cn)	eduPerson	Peter Sample
mail	eduPerson	peter.sample@example.org
eduPersonAffiliation eduPersonScopedAffiliation	eduPerson	staff staff@example.org
eduPersonPrincipalName	eduPerson	234cd8z239@example.org
schacHomeOrganization	SCHAC	example.org
schacHomeOrganizationType	SCHAC	urn:schac:homeOrganizationType:ch:university urn:schac:homeOrganizationType:eu:higherEducationInstitution
eduPersonTargetedID / Persistent Name ID	eduPerson	https://idp.example.org/idp/shibboleth! https://sp.example.org/shibboleth! 2389cdhu3e-sda7323

eduPerson <http://www.internet2.edu/products-services/trust-identity-middleware/eduperson-eduorg/>
 SCHAC <https://wiki.refeds.org/display/STAN/SCHAC+Releases>

Enabling Interfederation (2)

Interfederation

Interfederation

Enable interfederation for this Home Organisation

Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources.

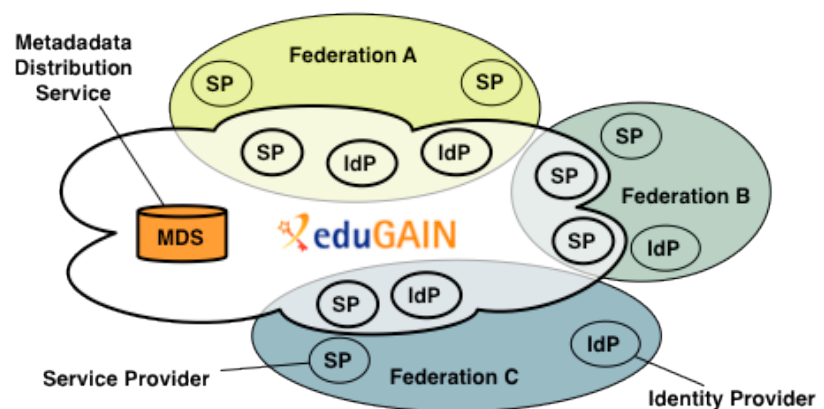
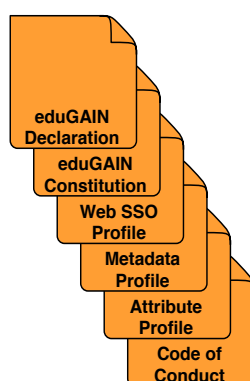
Enabling interfederation means that metadata about this resource is published in non-SWITCHaai organization and can be used by other Identity Providers which are not part of SWITCHaai. The metadata will also include contact information about this resource.

Before enabling a service for interfederation, make sure that:

- All internationally standardized core attributes are [declared as supported](#)
- The default [attribute release policy is adapted](#) such that internationally used attributes are released to interfederation resources
- The [specific attribute release](#) rules are accurate and up-to-date

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

eduGAIN: What is it and how does it work? ¹⁰



- eduGAIN provides policy framework and standards to build trust
- SPs and IdPs of participating federations should opt-in for eduGAIN.
 - Some federations decided for opt-out instead
- MDS fetches, aggregates and republishes metadata