eduGAIN – An Opportunity for Research Collaborations

SWITCHaai Team
aai@switch.ch

Agenda

- Why eduGAIN?
- Status
- GÉANT Data Protection Code of Conduct
- Scalable Attribute Release

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

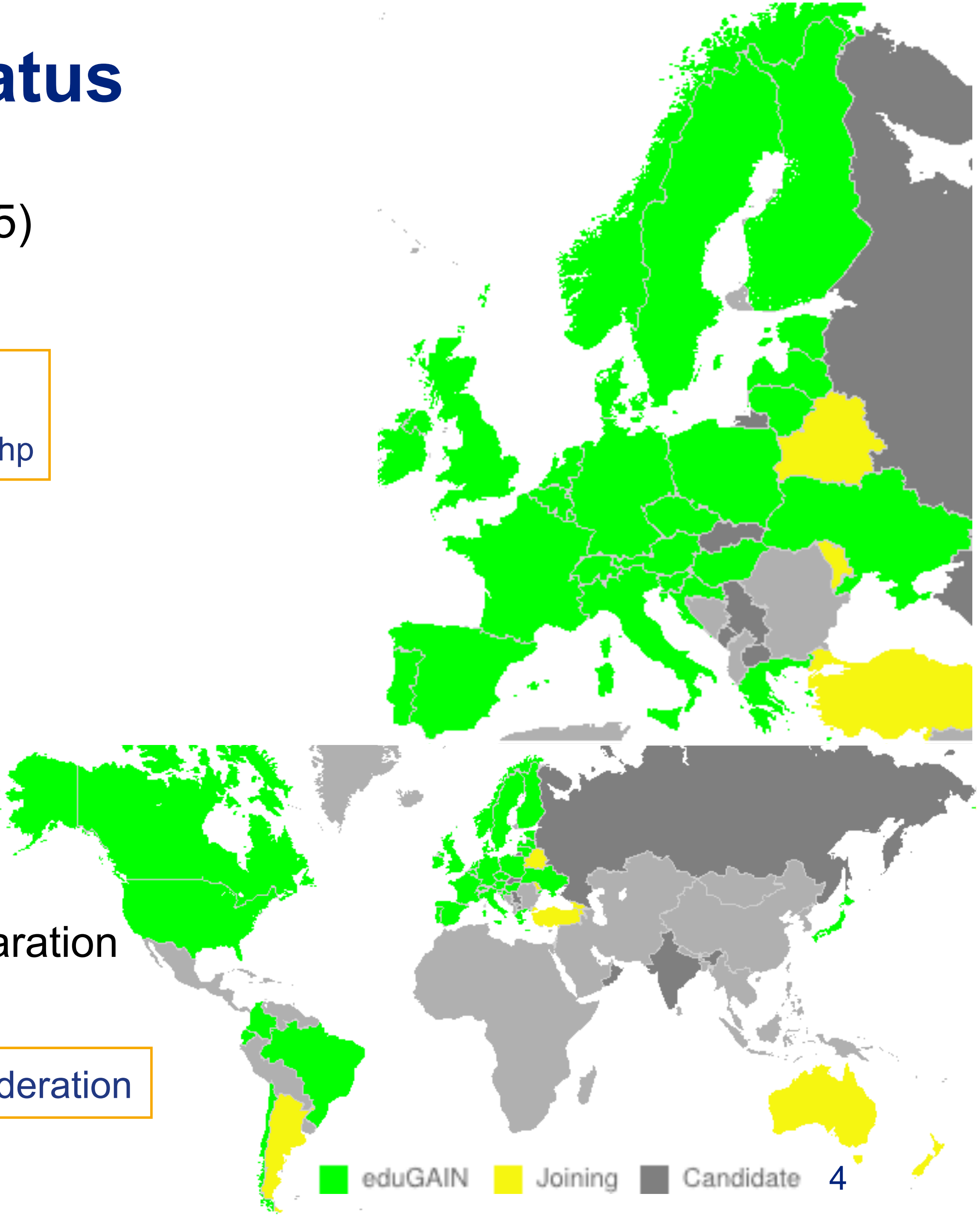
Interfederation Status

- eduGAIN in Total (Aug. 2015)
  - 1406 IdPs, 959 SPs

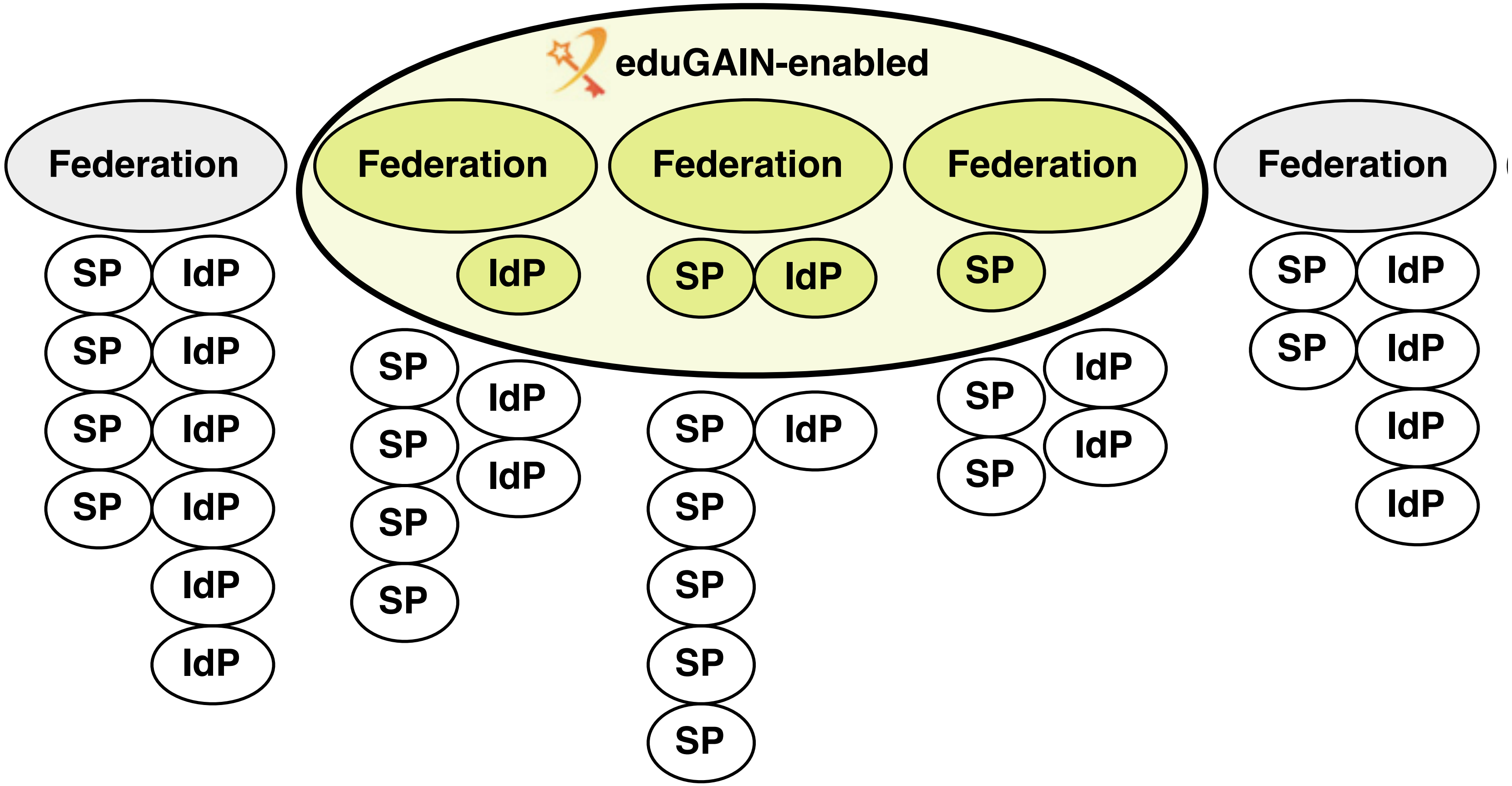
http://www.edugain.org
https://technical.edugain.org/status.php

- Status in CH
  - 20 IdPs enabled
    ~ 52% of the accounts
  - 8 SPs enabled
  - 31 institutions signed the
    Interfederation Access Declaration

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



eduGAIN Adoption Width vs. Depth

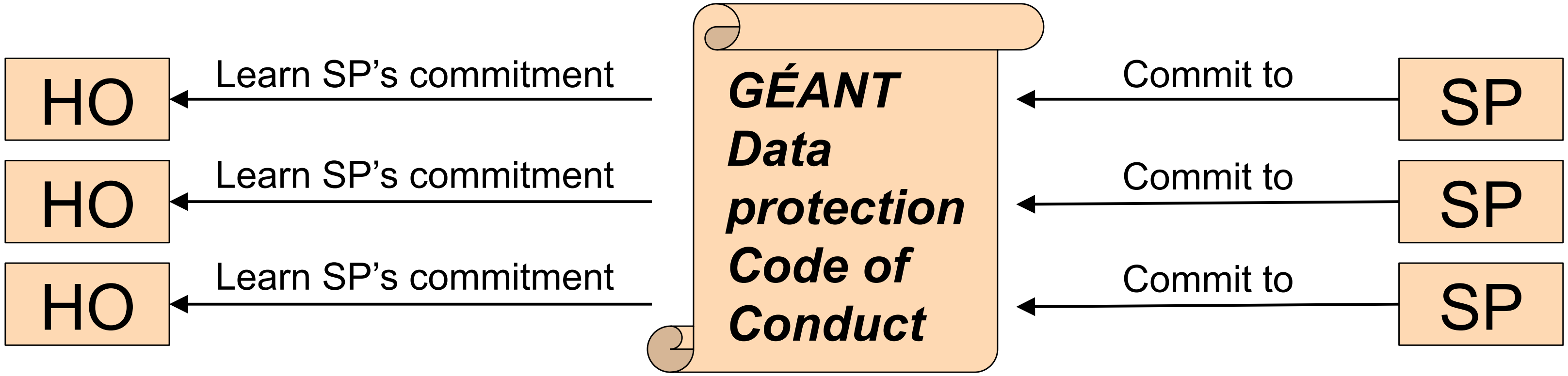


- Good federation adoption (Width)
- Entity Adoptions (Depth) is growing for IdPs (150% increase from 2014 to 2015)
- Not every SP and IdP has requirements to interfederate

GÉANT Code of Conduct – Data Protection within eduGAIN

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

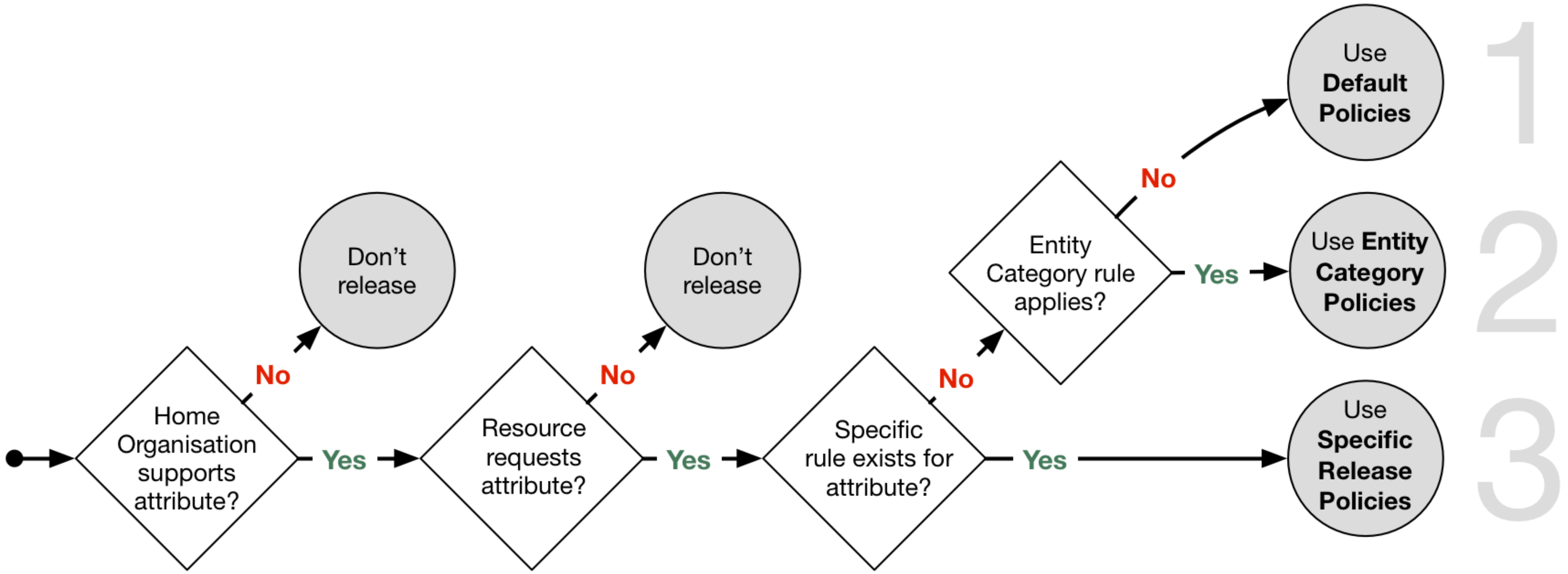
- The method is based on the EU Data Protection directives
- That will encourage the Home Organisation IdP to release attributes



Code of Conduct Toolkit

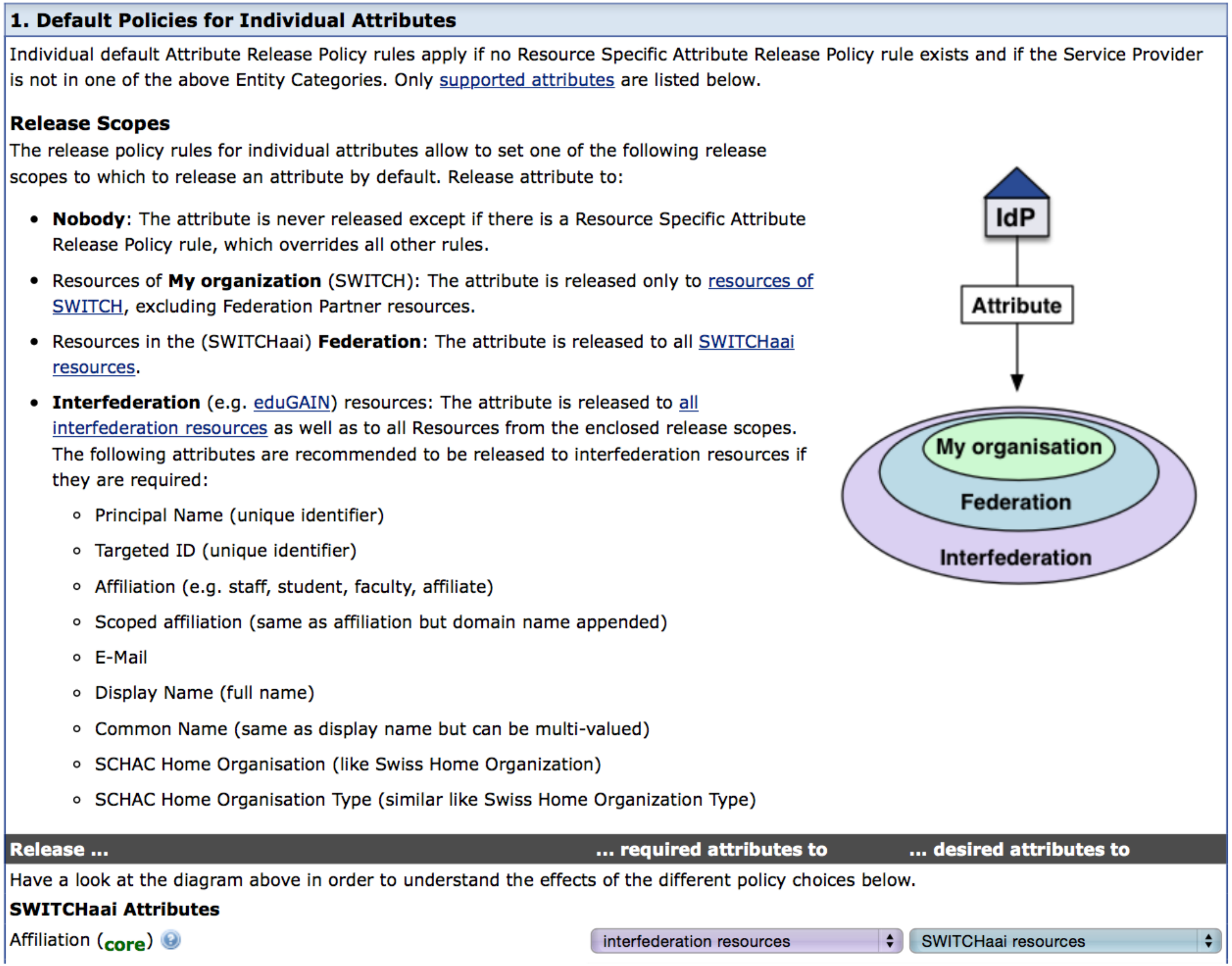
- Data Protection Code of Conduct for SPs in EU/EEA
- SAML2 profile for the Data Protection Code of Conduct
- Entity category attribute definition for the Code of Conduct

Attribute Release Rules


Home Organisation supports attribute?
No
Don't release
Yes
Resource requests attribute?
No
Don't release
Yes
Specific rule exists for attribute?
No
Entity Category rule applies?
No
Use **Default Policies**
1
Yes
Use **Entity Category Policies**
2
Yes
Use **Specific Release Policies**
3

Attribute Release Settings (1)

Resource Registry –
Edit Home Organization Description –
Attribute Release Settings



1. Default Policies for Individual Attributes

Individual default Attribute Release Policy rules apply if no Resource Specific Attribute Release Policy rule exists and if the Service Provider is not in one of the above Entity Categories. Only supported attributes are listed below.

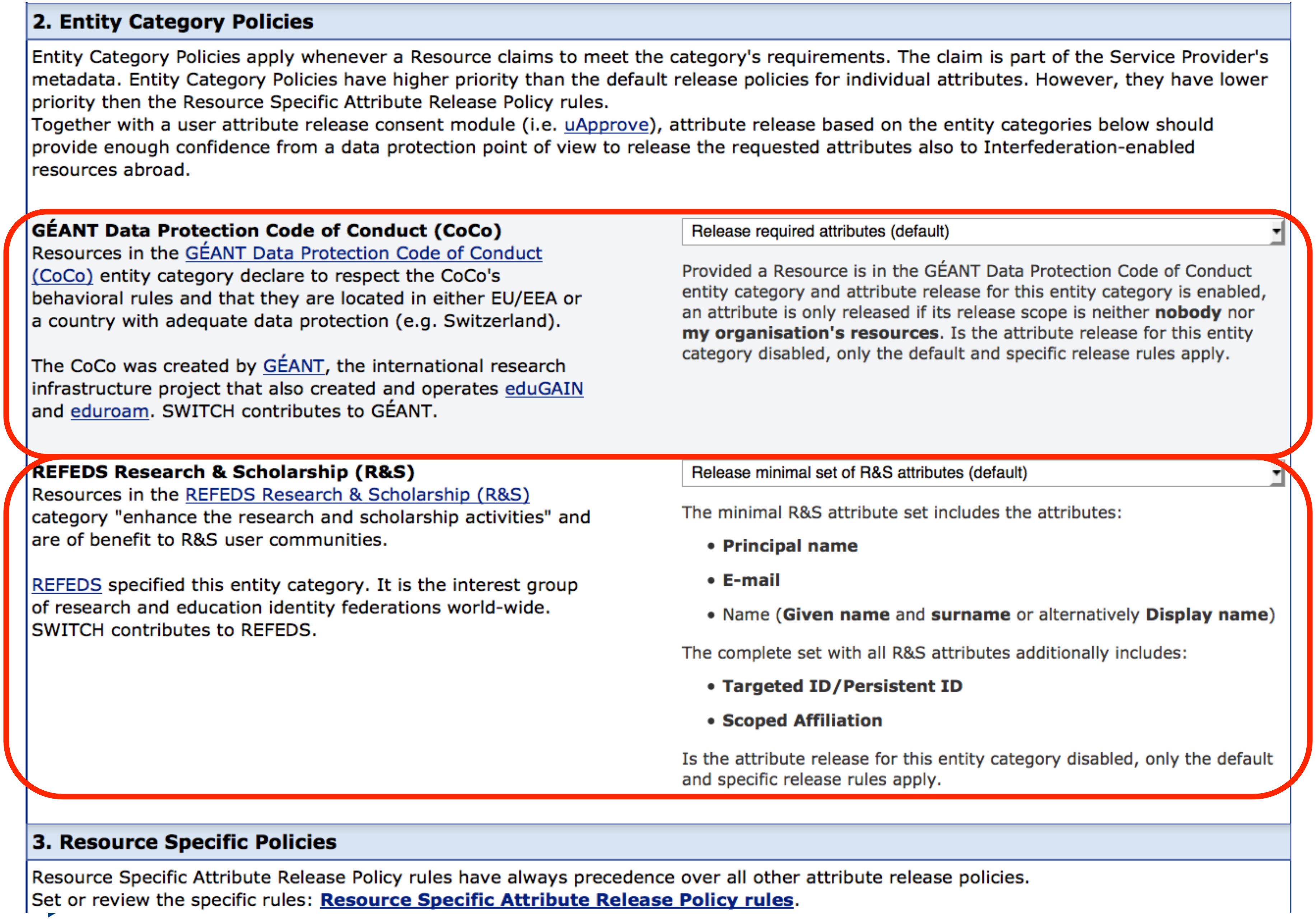
Release Scopes

The release policy rules for individual attributes allow to set one of the following release scopes to which to release an attribute by default. Release attribute to:

- **Nobody**: The attribute is never released except if there is a Resource Specific Attribute Release Policy rule, which overrides all other rules.
- Resources of **My organization** (SWITCH): The attribute is released only to resources of SWITCH, excluding Federation Partner resources.
- Resources in the (SWITCHaai) **Federation**: The attribute is released to all SWITCHaai resources.
- **Interfederation** (e.g. eduGAIN) resources: The attribute is released to all interfederation resources as well as to all Resources from the enclosed release scopes. The following attributes are recommended to be released to interfederation resources if they are required:
    - Principal Name (unique identifier)
    - Targeted ID (unique identifier)
    - Affiliation (e.g. staff, student, faculty, affiliate)
    - Scoped affiliation (same as affiliation but domain name appended)
    - E-Mail
    - Display Name (full name)
    - Common Name (same as display name but can be multi-valued)
    - SCHAC Home Organisation (like Swiss Home Organization)
    - SCHAC Home Organisation Type (similar like Swiss Home Organization Type)

Release ...	... required attributes to	... desired attributes to
Have a look at the diagram above in order to understand the effects of the different policy choices below.		
SWITCHaai Attributes		
Affiliation (core)	interfederation resources	SWITCHaai resources

Attribute Release Settings (2)



2. Entity Category Policies

Entity Category Policies apply whenever a Resource claims to meet the category's requirements. The claim is part of the Service Provider's metadata. Entity Category Policies have higher priority than the default release policies for individual attributes. However, they have lower priority then the Resource Specific Attribute Release Policy rules.
Together with a user attribute release consent module (i.e. uApprove), attribute release based on the entity categories below should provide enough confidence from a data protection point of view to release the requested attributes also to Interfederation-enabled resources abroad.

GÉANT Data Protection Code of Conduct (CoCo)
Resources in the GÉANT Data Protection Code of Conduct (CoCo) entity category declare to respect the CoCo's behavioral rules and that they are located in either EU/EEA or a country with adequate data protection (e.g. Switzerland).

The CoCo was created by GÉANT, the international research infrastructure project that also created and operates eduGAIN and eduroam. SWITCH contributes to GÉANT.

Release required attributes (default)

Provided a Resource is in the GÉANT Data Protection Code of Conduct entity category and attribute release for this entity category is enabled, an attribute is only released if its release scope is neither **nobody** nor **my organisation's resources**. Is the attribute release for this entity category disabled, only the default and specific release rules apply.

REFEDS Research & Scholarship (R&S)
Resources in the REFEDS Research & Scholarship (R&S) category "enhance the research and scholarship activities" and are of benefit to R&S user communities.

REFEDS specified this entity category. It is the interest group of research and education identity federations world-wide. SWITCH contributes to REFEDS.

Release minimal set of R&S attributes (default)

The minimal R&S attribute set includes the attributes:

- **Principal name**
- **E-mail**
- Name (**Given name** and **surname** or alternatively **Display name**)

The complete set with all R&S attributes additionally includes:

- **Targeted ID/Persistent ID**
- **Scoped Affiliation**

Is the attribute release for this entity category disabled, only the default and specific release rules apply.

3. Resource Specific Policies

Resource Specific Attribute Release Policy rules have always precedence over all other attribute release policies.
Set or review the specific rules: **Resource Specific Attribute Release Policy rules**.

Why should you care?

There are 8176 international projects with participants from Switzerland in the CORDIS [1] database of the European Commission

Probably some researchers from your institution are participating in one of them

[1] Community Research and Development Information Service

One example

DARIAH

- Digital Research Infrastructure for the Arts and Humanities

Cooperating Swiss partners

- University of Basel
- University of Bern
- University of Geneva
- University of Lausanne
- University of Zurich
- Swiss Academy of Humanities and Social Sciences