Attribute Release in SWITCHaai

CoCo and R&S in a full-mesh federation

SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Porto, 15. June 2015

Overview

- Motiviation
- Facts about SWITCHaai
- How we organize attribute release
- Supporting CoCo and R&S
  - For IdPs
  - For SPs
- Experiences and Recommendations

Motivation for CoCo and R&S

- eduGAIN's three major problems
  - ~~Too small federation coverage~~ Federation coverage quite good
  - ~~Too~~ small IdP coverage Getting better thanks to opt-out change
  - Attribute release does not work We still suck here... ☹

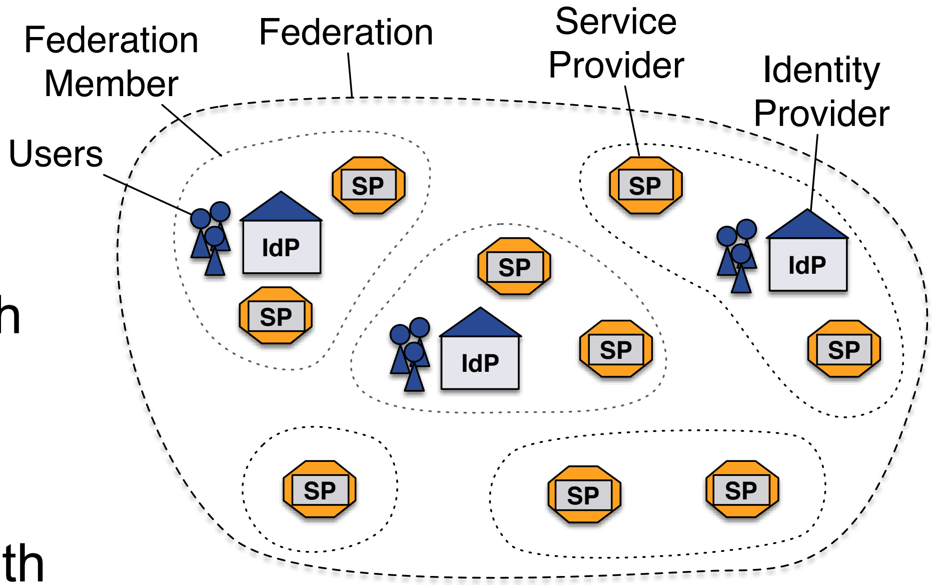
- Research communities (rightly) **complain that their services don't get even the most basic attributes**!

- What's eduGAIN/federation good for without attributes?

- CoCo and R&S can solve attribute release problem!
  - But your support as federation operator is required!

SWITCHaai Facts

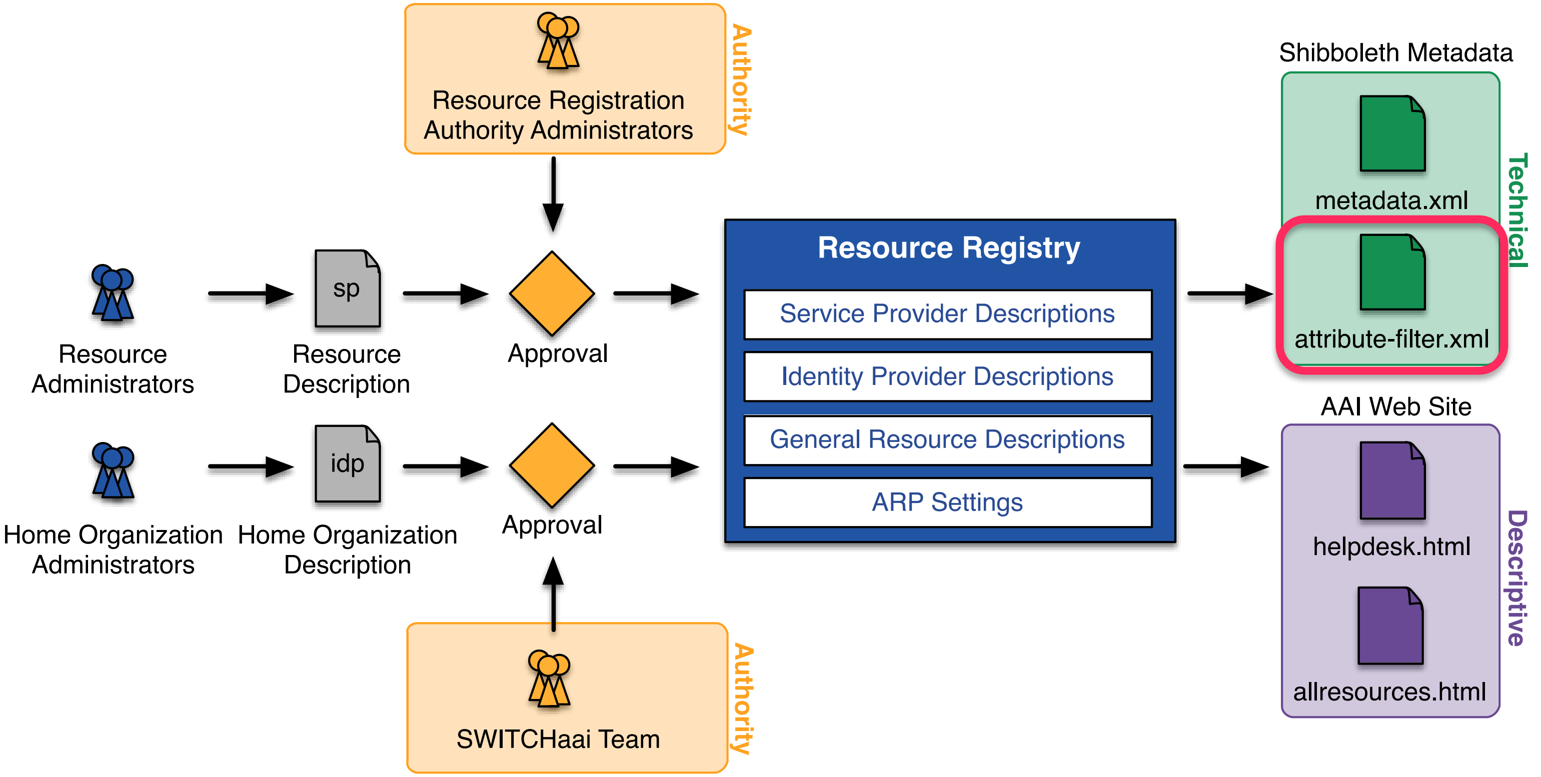
- Full-mesh federation!



- 61 Identity Providers
  - 59 IdPs (97%) use Shibboleth
- 834 Service Providers
  - More than 95% use Shibboleth
  - SP/IdP ration: **13.6**
- **Attribute release rules** have been **centrally generated** by federation registry since 10 years production operation

SWITCHaai Resource Registry

- Our federation management tool
- Predecessor of Jagger (*jagger.heanet.ie*)



Attribute Release in SWITCHaai

- **Resource Registry generates attribute filters per IdP**
  - SWITCHaai IdPs download attribute-filter.xml hourly from Federation Registry (via https)
  - Each file is custom-tailored to IdP based on attribute release settings: https://rr.aai.switch.ch/switchaai/example.org/attribute-filter.xml
  - Local attribute filter to override generated rules

- Resource Registry knows which attributes that:
  - IdPs support
  - SPs (including eduGAIN SPs) request

- IdP Admins configure release policies on Resource Registry

IdP Attribute Release Settings

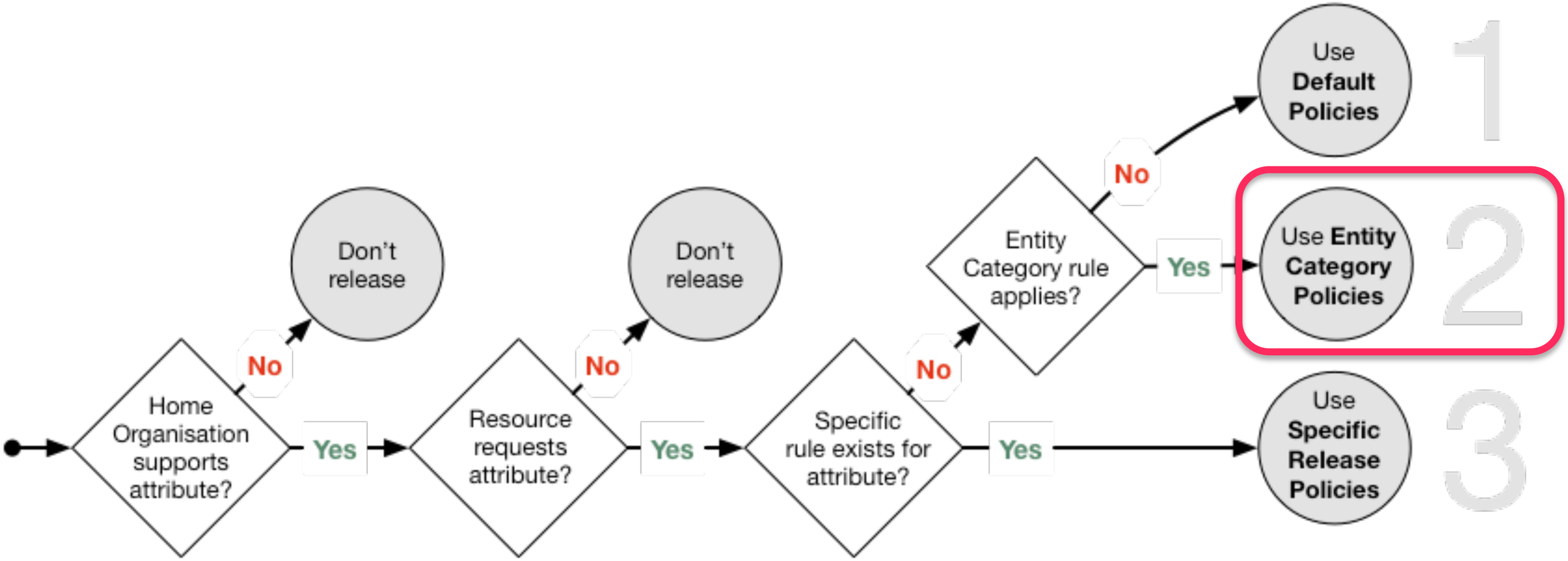
- Attribute release depends on three kind of policy types:
  1. **Default** Release Policies
  2. **Entity Category** Release Policies (CoCo, R&S)
  3. **Specific** Release Policies

- IdP **admins configure** their policies on Resource Registry

- **"Diff" email** to admins when attribute release file changes
  – Due to policy changes or because SPs were added/removed/changed

Attribute Release Decision Flow

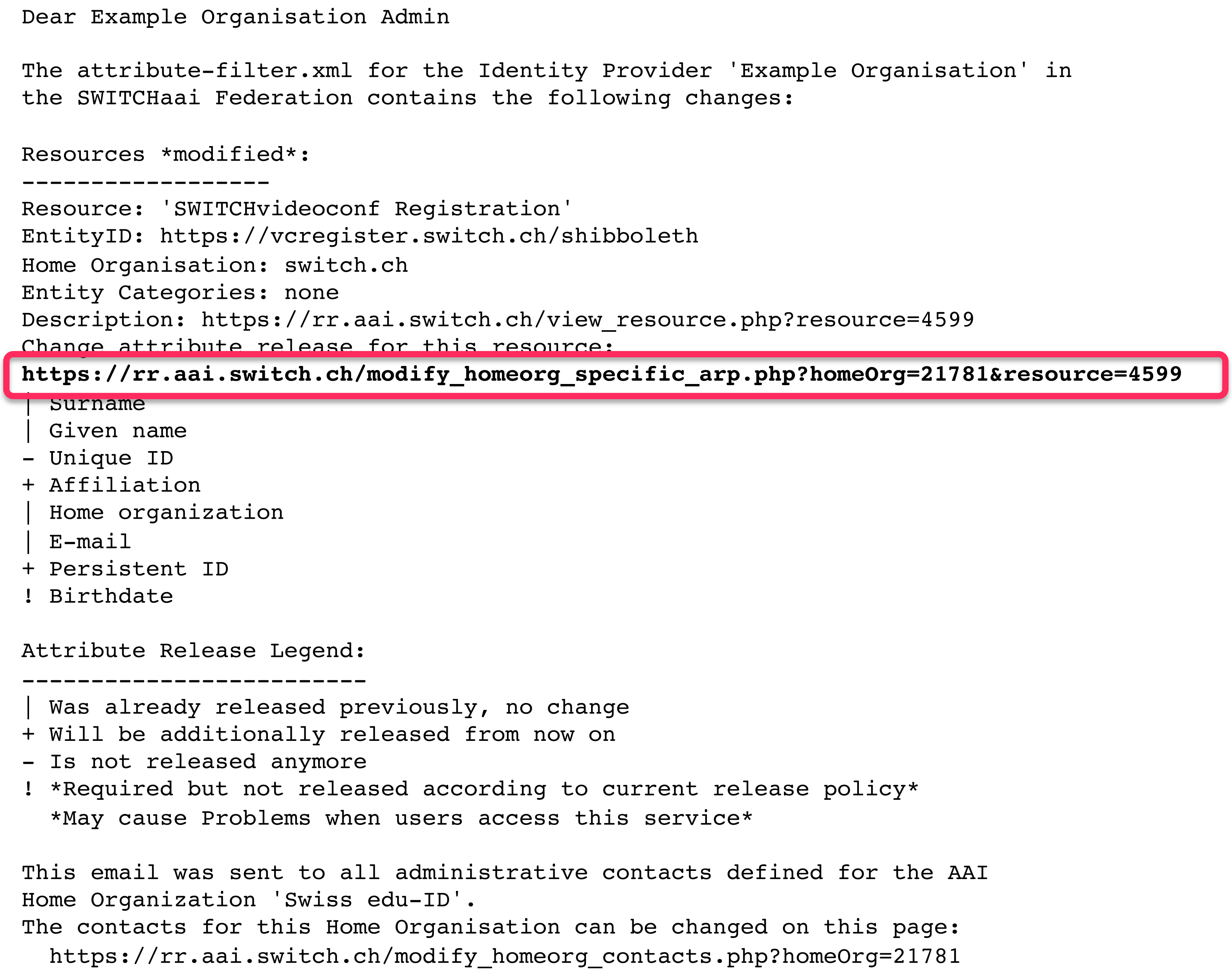
How is it decided if an attribute (e.g. email) is release by the IdP of a Home Organisation to a particular Resource/SP?



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

Notification emails

- **Acceptance** of default web-based attribute release policy management **is better if IdP admins are in control**
- They have to be **notified of changes** affecting their IdP
- Therefore Resource Registry sends **notification mails with "diff"** of attribute filter to technical contact of IdP whenever IdP downloads changed attribute-filter.xml



```
Dear Example Organisation Admin

The attribute-filter.xml for the Identity Provider 'Example Organisation' in
the SWITCHaai Federation contains the following changes:

Resources *modified*:
------------------
Resource: 'SWITCHvideoconf Registration'
EntityID: https://vcregister.switch.ch/shibboleth
Home Organisation: switch.ch
Entity Categories: none
Description: https://rr.aai.switch.ch/view_resource.php?resource=4599
Change attribute release for this resource:
https://rr.aai.switch.ch/modify_homeorg_specific_arp.php?homeOrg=21781&resource=4599
| Surname
| Given name
- Unique ID
+ Affiliation
| Home organization
| E-mail
+ Persistent ID
! Birthdate

Attribute Release Legend:
-------------------------
| Was already released previously, no change
+ Will be additionally released from now on
- Is not released anymore
! *Required but not released according to current release policy*
  *May cause Problems when users access this service*

This email was sent to all administrative contacts defined for the AAI
Home Organization 'Swiss edu-ID'.
The contacts for this Home Organisation can be changed on this page:
  https://rr.aai.switch.ch/modify_homeorg_contacts.php?homeOrg=21781
```

What is Needed to Technically "Support" Entity Categories like CoCo and R&S?

- Very **easy if entity is eligible** to get entity category

- **For IdPs:**
  - Add attribute **release policy rules** to attribute-filter.xml file, which is downloaded by Shibboleth IdPs hourly
  - Add **EntityCategory support attribute** to federation/interfederation metadata

- **For SPs:**
  - Add **EntityCategory attribute** to federation/interfederation metadata

Considerations to Introduce CoCo/R&S

- Making **IdPs** support entity categories is more important!
  - SP support should be less of a problem
- Reasonable to **support both categories**
- Making IdPs support them is technically easy for us (we just have to add rules to attribute filter files)
- Main **discussions about defaults values** and how to announce and introduce changes
- Decision to:
  - Make IdPs release R&S minimal attribute set and required CoCo attributes by default
  - Allow IdP admins to opt-out any time and even before changes are introduced

Introducing CoCo and R&S for IdPs

- **13. Aug. 2014:** Announcement of upcoming changes at AAI Tech Update event (targeting mostly IdP admins)
- **21. Aug. 2014:** Announcement on AAI mailing list
- **28. Aug. 2014:** IdP admins could start Opting-Out
- **2. Oct. 2014:** Activation of Entity Category Based attribute release with default to support CoCo and R&S

0 Opt-Outs so far. All interfederation-enabled IdPs support R&S and CoCo
(CoCo support not yet published for CERN)

How We Implemtened ECs*

1. CoCo for Home Organisations/IdP CoCo/IDP
2. R&S for Home Organisations/IdP R&S/IdP
3. CoCo for Resources/SP CoCo/SP
4. R&S for Resources/SP R&S/SP

* No guarantee that recipe works for all federations

Introduction of CoCo and R&S

CoCo and R&S were introduced at the same time

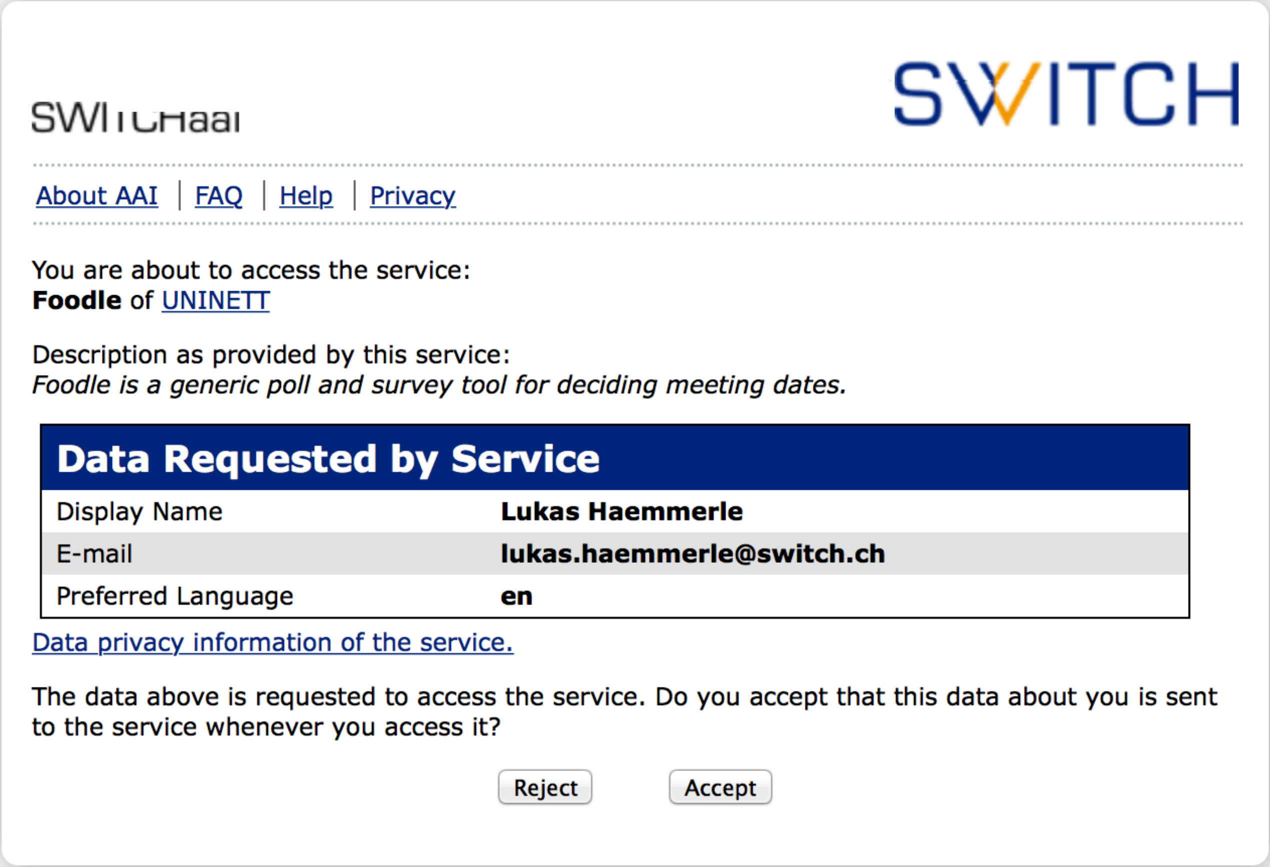
Goals:

- **High coverage** from the beginning
  - But only for Interfederation-enabled IdPs
- **Minimize work** for IdP admins
  - Opt-out approach and reasonable defaults
  - Release rules **automatically added to attribute-filter.xml**
- **Good acceptance**
  - Reasonable defaults and legal advice
  - User consent!

R&S/IdP CoCo/IDP

Key Ingredient: User Consent

IdPs required to implement user consent for attributes



You are about to access the service:
Foodle of UNINETT

Description as provided by this service:
Foodle is a generic poll and survey tool for deciding meeting dates.

Data Requested by Service	
Display Name	**Lukas Haemmerle**
E-mail	**lukas.haemmerle@switch.ch**
Preferred Language	**en**

Data privacy information of the service.

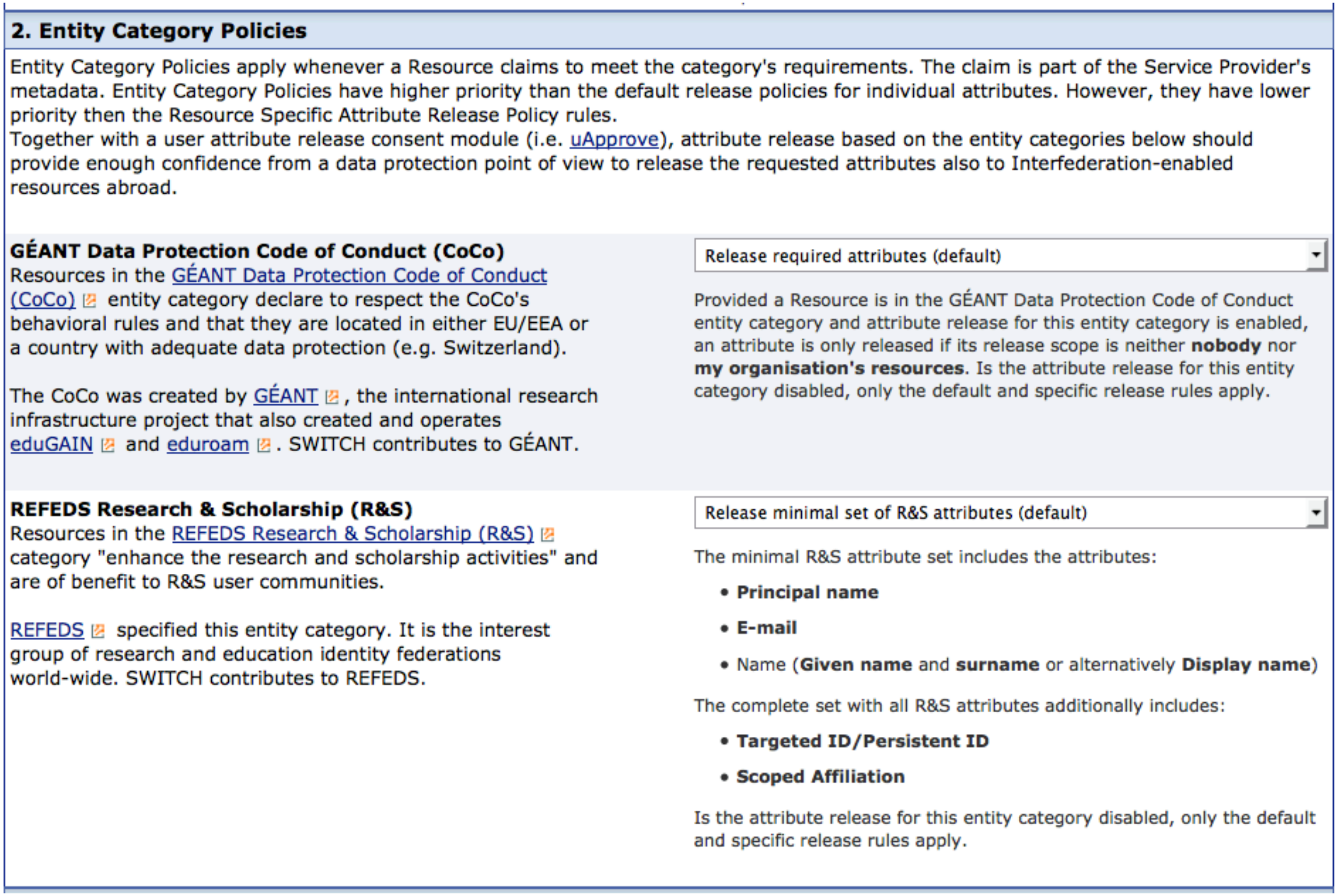
The data above is requested to access the service. Do you accept that this data about you is sent to the service whenever you access it?

CoCo/R&S Default Settings

- Release **required attributes to CoCo SPs**
  - EU data protection laws are adequate to Swiss laws
- Release **minimum attribute set to R&S SPs**
  - Services enhance research and scholarship
- IdP admins can **change settings any time** on Resource Registry (= opt-out)

R&S/IdP CoCo/IDP

Default Settings on Resource Registry



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**

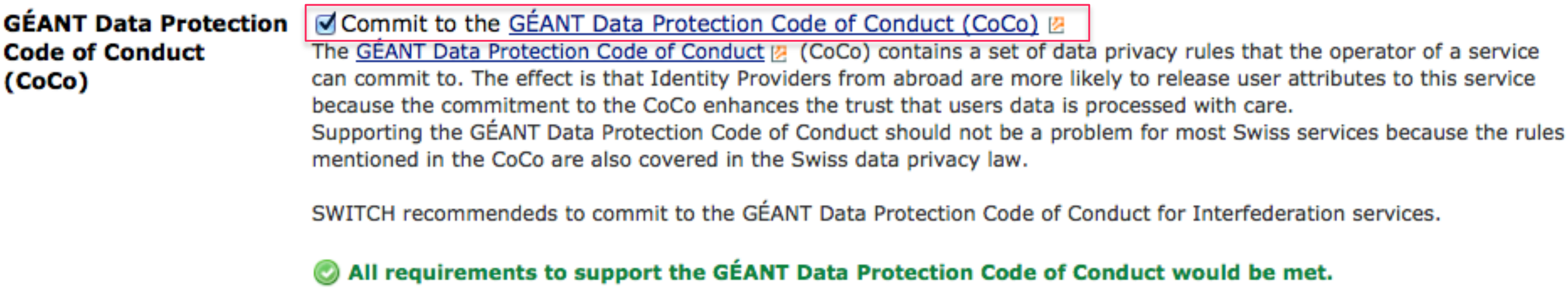
Is the attribute release for this entity category disabled, only the default and specific release rules apply.

CoCo for Resources/SP

- **Steps for SP admin to get CoCo**:
  1. Create/extend Privacy Statement web page
  2. Add URL to privacy statement web page in Resource Registry
  3. Enable CoCo support in Resource Registry
     (tick a checkbox, see next slide)

- **Resource Registry automatically checks:**
  - Privacy URL is defined
  - Privacy statement contains name and link to CoCo
  - Other CoCo requirements are already met by default in SWITCHaai
  - No re-checks (CoCo monitor does that already)

Ticking the CoCo Checkbox



GÉANT Data Protection Code of Conduct (CoCo)

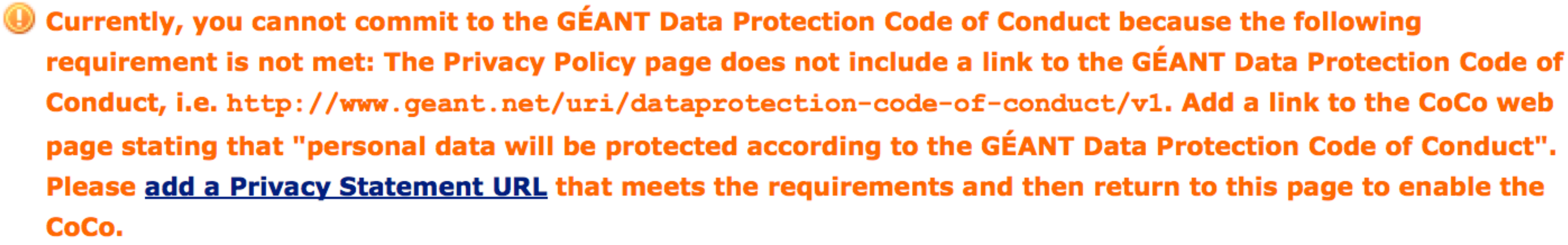
☑ Commit to the GÉANT Data Protection Code of Conduct (CoCo)

The GÉANT Data Protection Code of Conduct (CoCo) contains a set of data privacy rules that the operator of a service can commit to. The effect is that Identity Providers from abroad are more likely to release user attributes to this service because the commitment to the CoCo enhances the trust that users data is processed with care.
Supporting the GÉANT Data Protection Code of Conduct should not be a problem for most Swiss services because the rules mentioned in the CoCo are also covered in the Swiss data privacy law.

SWITCH recommendeds to commit to the GÉANT Data Protection Code of Conduct for Interfederation services.

✓ **All requirements to support the GÉANT Data Protection Code of Conduct would be met.**

– Warning is shown if any CoCo requirements are not met



Currently, you cannot commit to the GÉANT Data Protection Code of Conduct because the following requirement is not met: The Privacy Policy page does not include a link to the GÉANT Data Protection Code of Conduct, i.e. `http://www.geant.net/uri/dataprotection-code-of-conduct/v1`. Add a link to the CoCo web page stating that "personal data will be protected according to the GÉANT Data Protection Code of Conduct". Please add a Privacy Statement URL that meets the requirements and then return to this page to enable the CoCo.

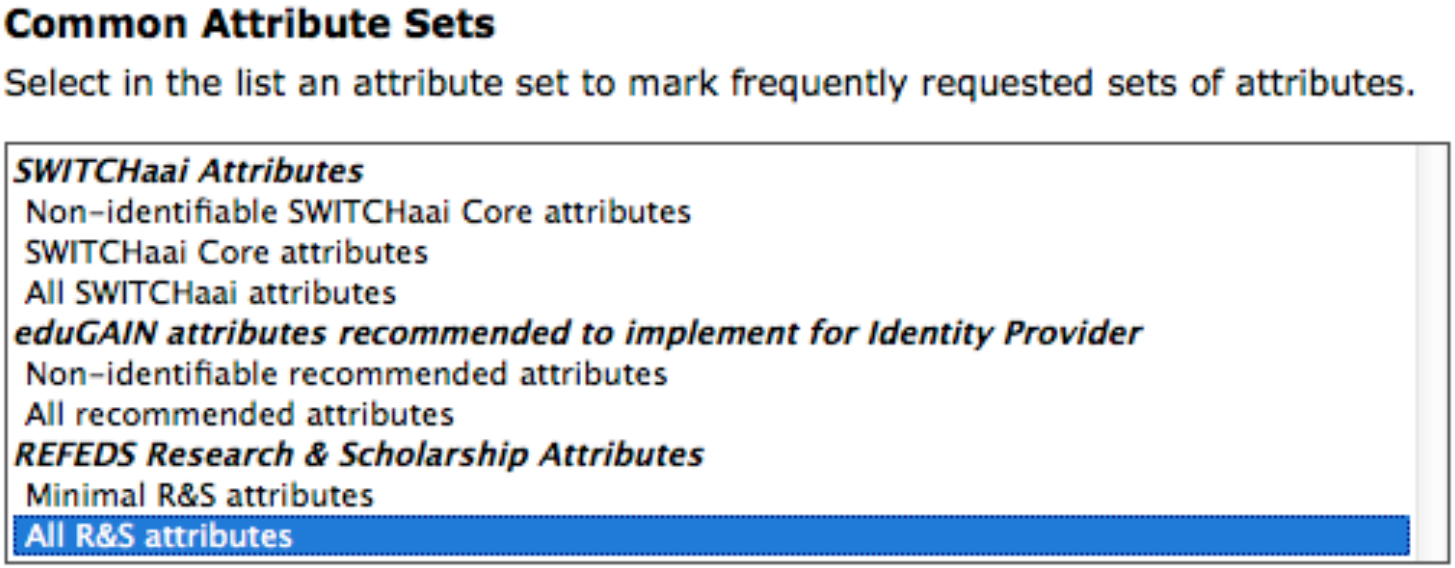
R&S for Resources/SP

- **Steps for SP admin to get R&S**:
  In Resource Registry:
  1. Add Information URL
  2. Ensure only R&S attributes are requested
  3. Request R&S support in Resource Registry
     (tick a checkbox, see next slide)
  4. Wait until request is approved by federation operator
     (check if service "enhances research and scholarship")

- **Resource Registry automatically checks:**
  - Information URL defined
  - Other R&S requirements are already met by default in SWITCHaai

R&S Attribute Set

- SP admins declare their attribute settings in Resource Registry
- Resource Registry offers different recommendations



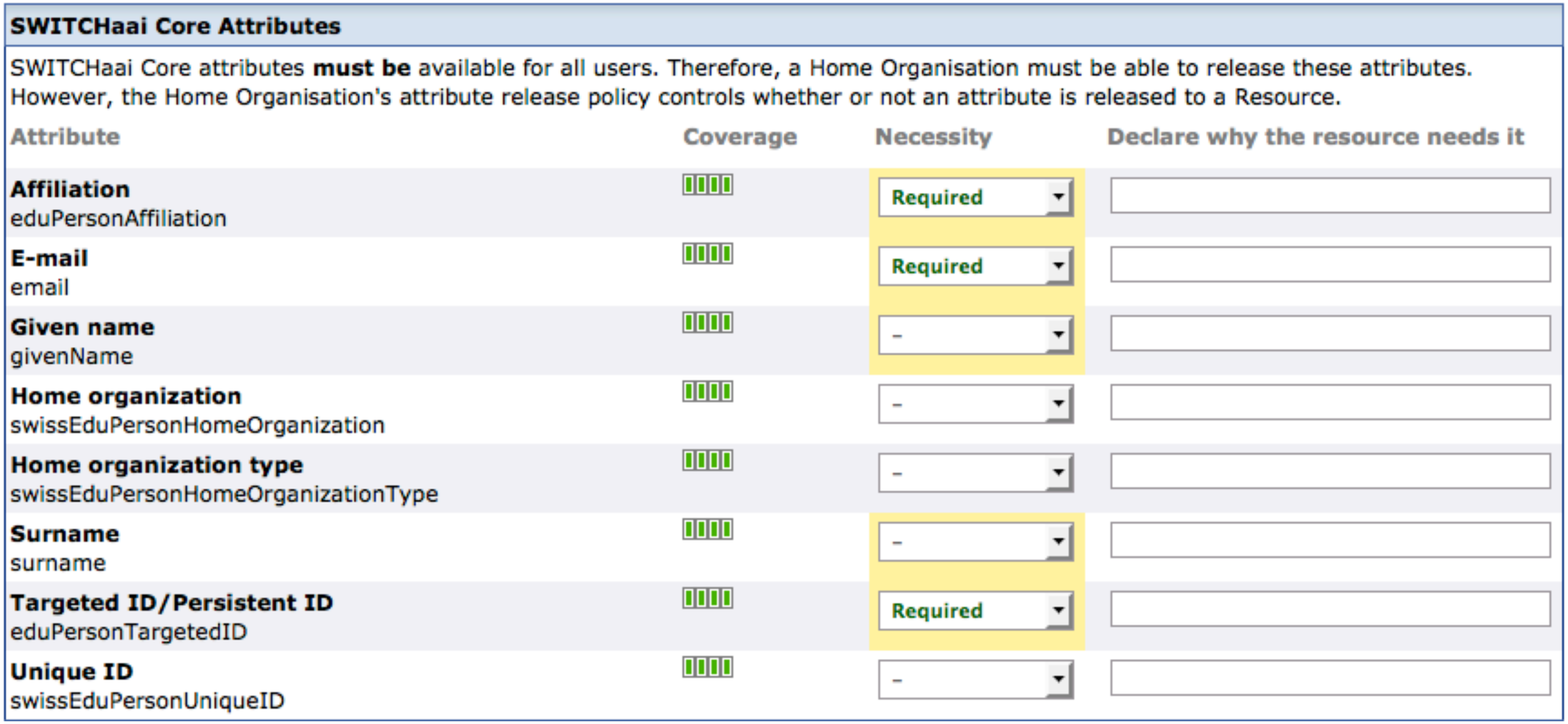
Common Attribute Sets

Select in the list an attribute set to mark frequently requested sets of attributes.

SWITCHaai Attributes
Non-identifiable SWITCHaai Core attributes
SWITCHaai Core attributes
All SWITCHaai attributes
eduGAIN attributes recommended to implement for Identity Provider
Non-identifiable recommended attributes
All recommended attributes
REFEDS Research & Scholarship Attributes
Minimal R&S attributes
All R&S attributes

Request Subset of R&S Attributes

Attribute sets are highlighted (yellow), but SP admin still has to declare necessity (required or desired)

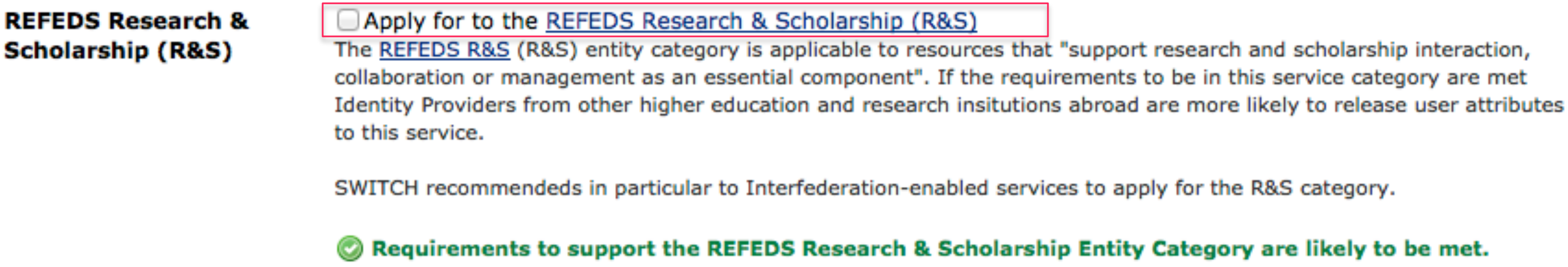


SWITCHaai Core Attributes

SWITCHaai Core attributes **must be** available for all users. Therefore, a Home Organisation must be able to release these attributes. However, the Home Organisation's attribute release policy controls whether or not an attribute is released to a Resource.

Attribute	Coverage	Necessity	Declare why the resource needs it
Affiliation eduPersonAffiliation	▮▮▮▮	Required	
E-mail email	▮▮▮▮	Required	
Given name givenName	▮▮▮▮	-	
Home organization swissEduPersonHomeOrganization	▮▮▮▮	-	
Home organization type swissEduPersonHomeOrganizationType	▮▮▮▮	-	
Surname surname	▮▮▮▮	-	
Targeted ID/Persistent ID eduPersonTargetedID	▮▮▮▮	Required	
Unique ID swissEduPersonUniqueID	▮▮▮▮	-	

Requesting R&S Entity Category



REFEDS Research & Scholarship (R&S)

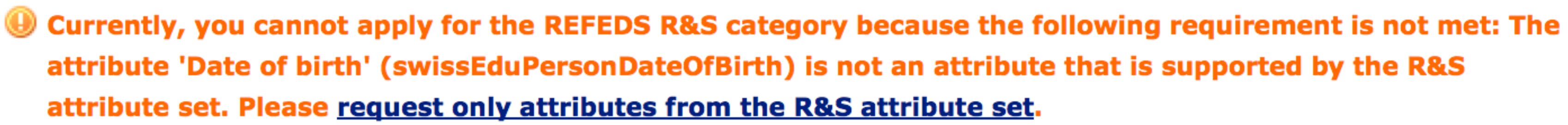
□ Apply for to the REFEDS Research & Scholarship (R&S)

The REFEDS R&S (R&S) entity category is applicable to resources that "support research and scholarship interaction, collaboration or management as an essential component". If the requirements to be in this service category are met Identity Providers from other higher education and research insitutions abroad are more likely to release user attributes to this service.

SWITCH recommendeds in particular to Interfederation-enabled services to apply for the R&S category.

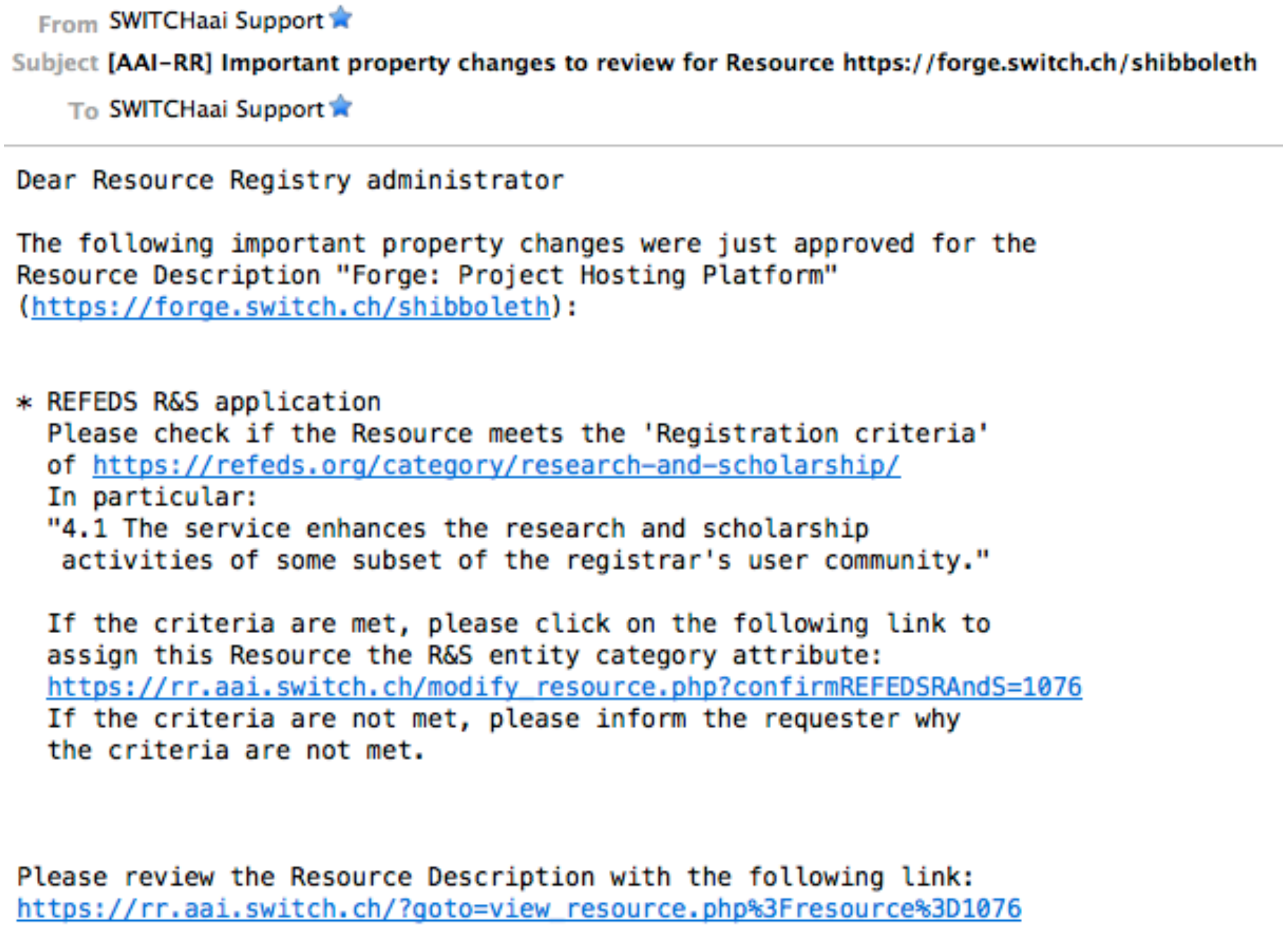
✓ **Requirements to support the REFEDS Research & Scholarship Entity Category are likely to be met.**

- SWITCHaai team then will check and approve the application.
- Warning is shown if any R&S requirements are not met



! Currently, you cannot apply for the REFEDS R&S category because the following requirement is not met: The attribute 'Date of birth' (swissEduPersonDateOfBirth) is not an attribute that is supported by the R&S attribute set. Please request only attributes from the R&S attribute set.

R&S Request Email



From SWITCHaai Support ★
Subject **[AAI-RR] Important property changes to review for Resource https://forge.switch.ch/shibboleth**
To SWITCHaai Support ★

```
Dear Resource Registry administrator

The following important property changes were just approved for the
Resource Description "Forge: Project Hosting Platform"
(https://forge.switch.ch/shibboleth):


* REFEDS R&S application
  Please check if the Resource meets the 'Registration criteria'
  of https://refeds.org/category/research-and-scholarship/
  In particular:
  "4.1 The service enhances the research and scholarship
   activities of some subset of the registrar's user community."

  If the criteria are met, please click on the following link to
  assign this Resource the R&S entity category attribute:
  https://rr.aai.switch.ch/modify_resource.php?confirmREFEDSRAndS=1076
  If the criteria are not met, please inform the requester why
  the criteria are not met.


Please review the Resource Description with the following link:
https://rr.aai.switch.ch/?goto=view_resource.php%3Fresource%3D1076
```

Experience of Introducing CoCo/R&S

- Very little to no feedback from IdP admins
- All has been going smooth
- Introducing R&S, CoCo support had only small effect on actual attribute filters
  - Default rules set for international attributes (attributes recommended for eduGAIN) already were releasing most attributes

Recommendation on Introducing CoCo and R&S Support

- Plan to **support both**: CoCo and R&S!
- Set **reasonable defaults** (i.e. opt-out)
- Discuss defaults with company legal advisor
- Leave IdP admins sufficient time (weeks) to opt-out
- Be brave ☺
  - Remember: eduGAIN will die without fixing attribute release problem!

Thank you

Any questions?

Experiences with centrally managed attribute release

- **Centrally managed attribute release is great!**

- **Very few attribute release problems** in 10 years operation
  - SP not getting attributes it needs
  - No problems with attribute release with eduGAIN so far (probably due to low usage).

- **Scalability becomes an issue**
  - 830 SWITCHaai SPs plus almost 1000 eduGAIN SPs
  - Instead of explicit rules, usage of dynamic rules (e.g. "release all required attributes to SPs supporting CoCo"), but will require up-to-date IdPs

- **Not aware of any lawsuit or major complaints** for the past 10 years due to the way attribute release is handled.

General Recommendations on Attribute Release

- Offer an **easy to configure** and use attribute release rule generation!

- Set **reasonable defaults (opt-out)**

- **Inform about changes** in advance

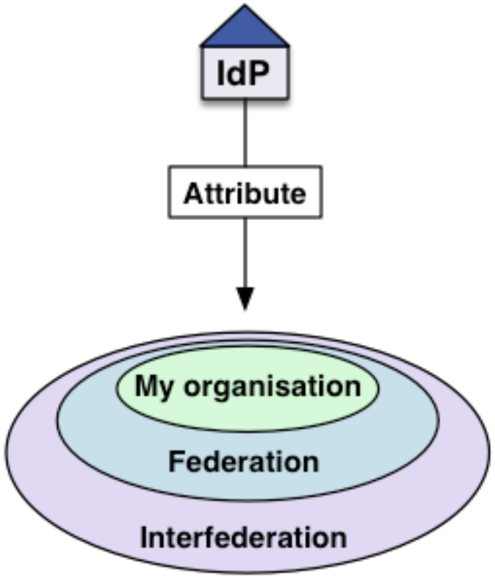
- **Automatically notify** IdP admins about changes in their release files

- Provide easy **method to adapt attribute release rules**

1. Default Release Policies

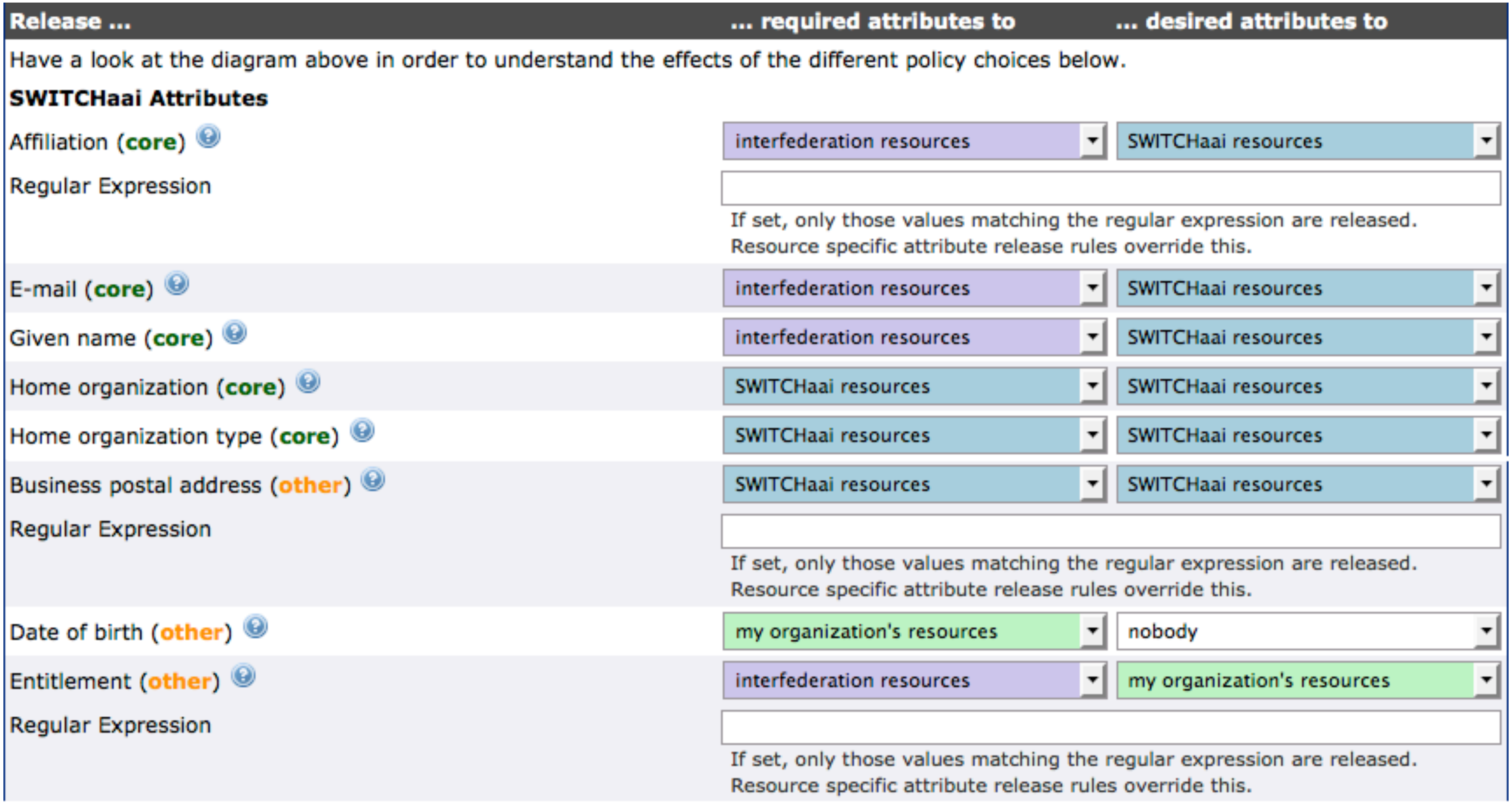
IdP Admin decides for each **required** and **desired** attribute* to which release scope it is released:

- **Nobody** (useful with 3. Specific Rules)
  - Useful for specific attribute policies
- SPs of same **organisation**
- SPs for same **federation**
- SPs in eduGAIN/**Interfederation**



* We are considering to remove distinction between required and desired attributes.

1. Example Default Release Policy



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
Regular Expression	If set, only those values matching the regular expression are released. Resource specific attribute release rules override this.	
E-mail (core)	interfederation resources	SWITCHaai resources
Given name (core)	interfederation resources	SWITCHaai resources
Home organization (core)	SWITCHaai resources	SWITCHaai resources
Home organization type (core)	SWITCHaai resources	SWITCHaai resources
Business postal address (other)	SWITCHaai resources	SWITCHaai resources
Regular Expression	If set, only those values matching the regular expression are released. Resource specific attribute release rules override this.	
Date of birth (other)	my organization's resources	nobody
Entitlement (other)	interfederation resources	my organization's resources
Regular Expression	If set, only those values matching the regular expression are released. Resource specific attribute release rules override this.	

2. Entity Category Policies

Release attributes based on fact whether SP is in CoCo or R&S category

See slides on CoCo and R&S

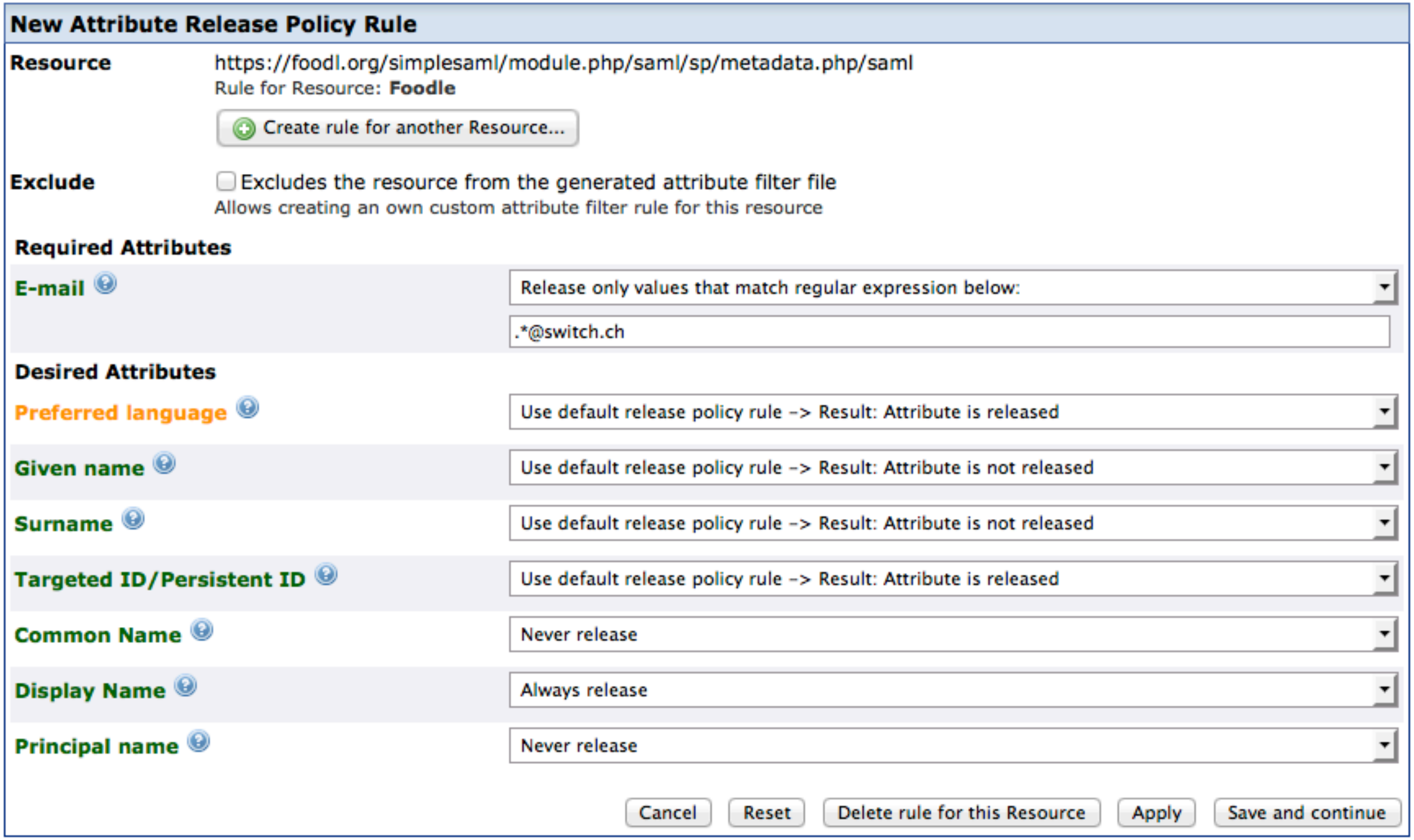
3. Specific Release Policies

- Always have precedence over previous two policies

- Used to create "exceptions from the (default) rules"

- Total 88 specific attribute release rules
  - For a total of 59 Shibboleth IdPs in federation
  - Only one university has more specific rules than SWITCH
  - 25 Home Organisation have no specific rules at all

3. Example Specific Release Policy



New Attribute Release Policy Rule

Resource https://foodl.org/simplesaml/module.php/saml/sp/metadata.php/saml
Rule for Resource: **Foodle**

Exclude □ Excludes the resource from the generated attribute filter file
Allows creating an own custom attribute filter rule for this resource

Required Attributes

E-mail	Release only values that match regular expression below: .*@switch.ch

Desired Attributes

Preferred language	Use default release policy rule -> Result: Attribute is released
Given name	Use default release policy rule -> Result: Attribute is not released
Surname	Use default release policy rule -> Result: Attribute is not released
Targeted ID/Persistent ID	Use default release policy rule -> Result: Attribute is released
Common Name	Never release
Display Name	Always release
Principal name	Never release