

How to bake CoCo and R&S

GÉANT Code of Conduct (CoCo) and R&S for SP and IdP



SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Berne, 13. August 2014

Recipe Book



Table of Contents

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

More detailed Recipe on:

https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook

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

Main Ingredients for CoCo Recipes

- **1 unit of will power:**
To deal with „boring“ but important data protection issues
- **15 minutes of precious Time:**
To read and understand the Code of Conduct:
<http://www.geant.net/uri/dataprotection-code-of-conduct/v1>
Don't worry, it's only 4 pages (103 lines) long
- **A few minutes more**
To implement the necessary steps (time depends on SP/
IdP and already available ingredients)

CoCo for Home Organisations/IdP

- Full CoCo Recipe for Identity Providers:
https://wiki.edugain.org/Recipe_for_a_Home_Organisation
 - Not all of the 5 steps apply for SWITCHaai organisations
- Additional Ingredient for this Recipe: uApprove
 - Attribute Release Consent module
<https://www.switch.ch/aai/support/tools/uApprove.html>
 - uApprove plugin is strongly recommended to deploy for Home Organisations that enabled Interfederation-support.
 - Can be disabled when users access Swiss Resources

Attribute Consent with uApprove

SWITCHaai SWITCH

[About AAI](#) | [FAQ](#) | [Help](#) | [Privacy](#)

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 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?

Adapt Attribute Release Policies

- Identity Providers that want to support the CoCo, „only“ need to adapt Attribute Release Policies (e.g. attribute-filter.xml)
- For SWITCHaai Identity Providers using Shibboleth, this can be conveniently done via the Resource Registry
 - Shibboleth IdPs by default are configured to download attribute-filter.xml file from Resource Registry.
 - For ADFS-based Identity Providers this is not possible

CoCo Default Settings

- For SWITCHaai Home Organisations the default setting is to release required attributes to services that committed to the CoCo
 - EU data protection laws are adequate to Swiss laws
 - uApprove asks user for consent before data is released to non-SWITCHaai services
 - Use the CoCo within Switzerland only is also possible but should generally not be necessary
- Home Organisations will be able to change their settings (opt-out) in section „7. Attribute Release Settings“

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 than 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.

available end of August 2014

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**. If the attribute release for this entity category is 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**

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

Default settings for Home Organisations. Will be available in RR end August 2014.

CoCo for Resources/SP

- Full Coco Recipe for Service Providers:
https://wiki.edugain.org/Recipe_for_a_Service_Provider
– No extra work needed for steps 2, 4 and 5 for SWITCHaai Resources
- **Quick Start**
To (technically) commit to 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

1. Create Privacy Statement

- Template available on:
https://refeds.terena.org/index.php/Privacy_policy_guidelines_for_Service_Providers
Format of the template is not strict but a recommendation
- Important is a reference to the CoCo, e.g.:
„Personal data will be protected according to the Code of Conduct for Service Providers, a common standard for the research and higher education sector to protect the user's privacy.“
The link must point to:
<http://www.geant.net/uri/dataprotection-code-of-conduct/v1>

Example Privacy Policy for AAI Interfederation Attribute Test.

Interfederation Attribute Test Privacy Statement

Name of the service	Interfederation Attribute Test
Description of the service	Allows to check if an organisation/Identity Provider releases the attributes recommended by eduGAIN .
Data controller and a contact person	SWITCH , the Swiss education & research network.
Jurisdiction	CH Switzerland Zurich.
Personal data processed	<p>1. For all users</p> <ul style="list-style-type: none"> • IP address • Referrer address (the web page a user is coming from) <p>2. Only for authenticated users The following attributes are only processed/displayed if they are released by the organisation of the user that is accessing the Interfederation Attribute Test</p> <ul style="list-style-type: none"> • E-mail • Home organization • Home organization type • Affiliation • Targeted ID/Persistent ID • Principal name • Scoped affiliation • Display Name • Common Name • SCHAC Home Organisation • SCHAC Home Organisation Type <p>All of the above attributes are declared as required to check if they really are released by an organisations.</p>
Purpose of the processing of personal data	The IP and referrer addresses of all web page visitors are stored in the web server log file for debugging purposes. For authenticated users, the Interfederation Service may receive all personal data mentioned-above. This personal data is only used to check if a Home Organisation is able to release all the attributes that the eduGAIN attribute profile recommends to support.
Third parties to whom personal data is disclosed	No data will be released to third parties. Personal data is only shown to the user himself. Data might also be used by SWITCH staff members for debugging purposes.
How to access, rectify and delete the personal data	Contact via aai@switch.ch . To rectify the data released by an organisation about you, contact that Home Organisation's IT helpdesk.
Data retention	Personal data, IP address and referrer are only stored in log files created by the web server and the SAML software. Log files are kept only for 30 days and are deleted automatically after this time.
Data Protection Code of Conduct	Personal data will be protected according to the Code of Conduct for Service Providers , a common standard for the research and higher education sector to protect the user's privacy.

Created with standard CoCo template.

2. Add Privacy URL


- Go to Resource Registry, <https://rr.aai.switch.ch>
- Click on „Edit Resource Description“ of Resource
- Add Privacy URL in section „2. Descriptive Information“


English Resource Information	
Name	<input type="text" value="AAI Viewer Interfederation Test"/> <p>Display name to show for this Resource. Ideally no longer than 33 characters. May be displayed to the user during login.</p>
Description	<input type="text" value="This service is used to test the interfederation readiness of SWITCHaai Identity Providers."/> <p>In the description you should briefly describe the purpose of this Resource. For example "The purpose of this service is to ...". Ideally no longer than 100 characters. May be displayed to the user during login.</p>
Information URL	<input type="text" value="https://aai-viewer.switch.ch/interfederation-test/"/> <p>URL to a web page that provides more comprehensive description than the one above. In order to request to be included in the REFEDS Research & Scholarship (R&S) entity category, provide a URL to a general information page about this service. This information page must be in English. After providing the URL, enable the R&S support in section '7. Intended Audience'.</p>
Privacy URL	<input type="text" value="https://aai-viewer.switch.ch/interfederation-test/privacy-statement.html"/> <p>URL to a web page contains a privacy statement that describes how identity information will be used and managed. This URL must be publicly accessible. In order to commit to the GÉANT Data Protection Code of Conduct (CoCo), provide a URL to a privacy statement page that contains a link to http://www.geant.net/uri/dataprotection-code-of-conduct/v1. The privacy statement must be in English and ideally follows this privacy policy template. After providing a privacy statement URL, enable the CoCo support in section '7. Intended Audience'.</p>
Keywords	<input type="text"/> <p>Space-separated keywords (locations, tags, categories, labels) related to this Resource. Multiple connected words can be separated by the + character. The keywords are primarily used to search for this entity.</p>

3. Commit to CoCo

- Go to section „Intended Audience and Interfederation“
 - Check „Commit to GÉANT Data Protection Code of Conduct (CoCo)“

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 recommends 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.

available end of August 2014

– Warning is shown if any CoCo requirements are not met

- Finally, submit Resource Description for approval

R&S for Home Organisations/IdP

- Similar to CoCo: Attribute release
- For SWITCHaai Home Organisations the default setting is to release the minimal set of R&S attribute to services in the Research & Scholarship entity category
 - Services enhance research and scholarship
 - uApprove asks user for consent before data is released to non-SWITCHaai services
 - Use of R&S within Switzerland only is also possible but should generally not be necessary
- Home Organisations will be able to change their settings in section „7. Attribute Release Settings“

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 than 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**. If the attribute release for this entity category is disabled, only the default and specific release rules apply.

available end of August 2014

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**

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

Default settings for Home Organisations. Will be available in RR end August 2014.

R&S for Resources/SP

- Full R&S specification:
<https://refeds.org/category/research-and-scholarship/>
- **Quick Start**
To (technically) commit to CoCo.
In Resource Registry:
 1. Add InformationURL in section "2. Descriptive Information"
 2. Ensure only R&S attributes are requested
 3. Request inclusion in R&S Entity Category in section "7. Intended Audience and Interfederation"

1. Add Information URL

- Go to Resource Registry, <https://rr.aai.switch.ch>
- Click on „Edit Resource Description“ of Resource
- Add Information URL in section „2. Descriptive Information“

English Resource Information	
Name	<input type="text" value="AAI Viewer Interfederation Test"/> Display name to show for this Resource. Ideally no longer than 33 characters. May be displayed to the user during login.
Description	<input type="text" value="This service is used to test the interfederation readiness of SWITCHaai Identity Providers."/> In the description you should briefly describe the purpose of this Resource. For example "The purpose of this service is to ...". Ideally no longer than 100 characters. May be displayed to the user during login.
Information URL	<input type="text" value="https://aai-viewer.switch.ch/interfederation-test/"/> URL to a web page that provides more comprehensive description than the one above. In order to request to be included in the REFEDS Research & Scholarship (R&S) entity category , provide a URL to a general information page about this service. This information page must be in English. After providing the URL, enable the R&S support in section '7. Intended Audience'.
Privacy URL	<input type="text" value="https://aai-viewer.switch.ch/interfederation-test/privacy-statement.html"/> URL to a web page contains a privacy statement that describes how identity information will be used and managed. This URL must be publicly accessible. In order to commit to the GÉANT Data Protection Code of Conduct (CoCo) , provide a URL to a privacy statement page that contains a link to http://www.geant.net/uri/dataprotection-code-of-conduct/v1 . The privacy statement must be in English and ideally follows this privacy policy template . After providing a privacy statement URL, enable the CoCo support in section '7. Intended Audience'.
Keywords	<input type="text"/> Space-separated keywords (locations, tags, categories, labels) related to this Resource. Multiple connected words can be separated by the + character. The keywords are primarily used to search for this entity.

2. Limit Attribute to R&S Set

- In section "6. Requested Attributes" select one of the R&S attribute sets to mark the attributes in that set
- Then request from the marked attributes those as required that are needed by the service

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

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	<input type="text"/>
E-mail email		Required	<input type="text"/>
Given name givenName		-	<input type="text"/>
Home organization swissEduPersonHomeOrganization		-	<input type="text"/>
Home organization type swissEduPersonHomeOrganizationType		-	<input type="text"/>
Surname surname		-	<input type="text"/>
Targeted ID/Persistent ID eduPersonTargetedID		Required	<input type="text"/>
Unique ID swissEduPersonUniqueID		-	<input type="text"/>

3. Apply for R&S Entity Category

- Go to section „Intended Audience and Interfederation“
 - Check „Apply for to the REFEDS Research & Scholarship (R&S)“

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 recommends 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.**

available end of August 2014

– Warning is shown if any R&S requirements are not met

- Finally, submit Resource Description for approval. SWITCH then will check and approve the application.

Baking can be fun 😊

