Entity Categories

GÉANT Data Protection CoCo and REFEDS Research & Scholarship R&S

SWITCH

SWITCHaai Team
aai@switch.ch

Outline

- Entity category
- GÉANT Data Protection Code of Conduct (CoCo)
- REFEDS Research & Scholarship (R&S)

Entity categories

A generic method to enrich metadata

- Tag an entity (SP or IdP) as being part of a category
- Requires a specification for international coherent use
  - Criteria
    - Purpose
    - Policies
    - Or other

In interfederation context:

- Filling the gap of missing common policies
- Support or increase scalable trust

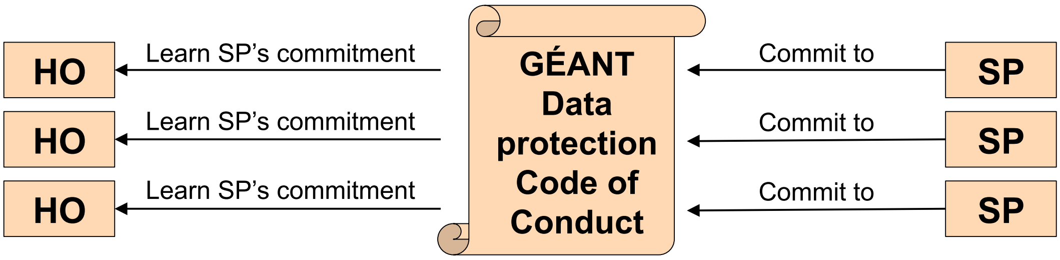
Metadaten

```
<!--  AAI Viewer Interfederation Test  -->
<EntityDescriptor entityID="https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth">
  <Extensions>
    <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>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        FriendlyName="swissEduPersonHomeOrganization" Name="urn:oid:2.16.756.1.2.5.1.1.4"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>switch.ch</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        FriendlyName="swissEduPersonHomeOrganizationType" Name="urn:oid:2.16.756.1.2.5.1.1.5"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>others</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  ...
</EntityDescriptor>
```

GÉANT Data Protection Code of Conduct

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



HO ← Learn SP's commitment ← GÉANT Data protection Code of Conduct ← Commit to ← SP

HO ← Learn SP's commitment ← GÉANT Data protection Code of Conduct ← Commit to ← SP

HO ← Learn SP's commitment ← GÉANT Data protection Code of Conduct ← Commit to ← SP

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

GÉANT Data Protection Code of Conduct

- Principles:
  - Legal compliance
  - Purpose limitation
  - Data minimisation
  - Deviating purposes
  - Data retention
  - Third parties
  - Security measures
  - Information duty towards end user
  - Information duty towards home organization
  - Security breaches
  - Liability
  - Transfer to third countries
  - Governing law and jurisdiction
  - Eligibility to execute
  - Termination of the Code of Conduct
  - Survival of the clauses
  - Precedence

Data Protection Code of Conduct (DP CoCo)

Normative documents

- Data Protection Code of Conduct for SPs in EU/EEA
- Entity category specification 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
- Managing DP risks using CoCo
- Privacy policy guidelines for SPs
- What attributes can an SP request
- DP good practice for Home Organisations
- Federation operator guidelines
- Handling non-compliance
- IdP inform/consent GUI guidelines

https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

Cookbook for DP CoCo

https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook

Privacy policy template

- Name of the service
- Description of the service
- Data controller and a contact person
- Jurisdiction
- Personal data processed
- Purpose of the processing of personal data
- Third parties to whom personal data is disclosed
- How to access, rectify and delete the personal data
- Data retention
- Data Protection Code of Conduct

REFEDS Research & Scholarship

- R&S SPs support
  - Research & scholarship interaction
  - Collaboration
  - Management
- No SPs from publishers!
- Attributes:
  - Personal identifiers: email, person name, eduPersonPrincipalName
  - Pseudonymous identifier: eduPersonTargetedID
  - Affiliation: eduPersonScopedAffiliation
  - Minimal subset: eduPersonPrincipalName, mail, person name

(person name = given name + surname OR displayName)

Comparison

REFEDS R&S	GÉANT DP CoCo
Global	Mainly Europe
Common purpose of the SPs	Common data protection standards
Fixed set of attributes	SP can require any attributes