Interfederation Update

Thomas Lenggenhager
aai@switch.ch

Bern, 14.03.2018
Outline

- Interfederation Status
- Entity categories
  - In general
  - REFEDS Research & Scholarship (R&S)
  - GÉANT Data Protection Code of Conduct (CoCo)
  - Security Incident Response Trust Framework for Federated Identity (SIRTFI)
eduGAIN: Current Status

eduGAIN in Total
• 2655 IdPs, 1888 SPs

[Link: https://technical.edugain.org/status]

Status in CH
• 51 IdPs enabled
  ~ 88% of all AAI accounts
  ~ 97% of all Higher Ed accounts
• 15 SPs enabled

[Link: https://www.switch.ch/aai/interfederation]
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, etc.

• In interfederation context:
  • Filling the gap of missing common policies
  • Further scalable attribute release (R&S and CoCo)
  • Support or increase scalable trust (SIRTFI)
How does it look like in SAML Metadata

```xml
<!-- 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: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>
...
REFEDS R&S

• REFEDS Research & Scholarship category
  • Federations can "tag" research and education SPs
    • Research & scholarship interaction
    • Collaboration
    • Management
    • **Not** for SPs from publishers
  • Allows easier/safer attribute release

• Restricted Attribute set:
  • Personal identifiers: email, person name, eduPersonPrincipalName
  • Pseudonymous identifier: eduPersonTargetedID
  • Affiliation: eduPersonScopedAffiliation
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

GÉANT Data protection Code of Conduct

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
# Comparison between R&S and CoCo

<table>
<thead>
<tr>
<th>REFEDS R&amp;S</th>
<th>GÉANT DP CoCo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Mainly Europe</td>
</tr>
<tr>
<td>Common purpose of the SPs</td>
<td>Common data protection standards</td>
</tr>
<tr>
<td>Fixed set of attributes</td>
<td>SP can require any attributes</td>
</tr>
</tbody>
</table>

**GÉANT DP CoCo v2 in preparation:**
- Based on GDPR
- Targets worldwide scope

---

http://refeds.org/category/research-and-scholarship

© 2018 SWITCH | 9
SIRTFI - coordinated incident response

- A Security Incident Response Trust Framework for Federated Identity
  - Operational Security
  - Incident Response
  - Traceability
  - Participant Responsibilities

- Initiated and driven by CERN and other big science infrastructures

https://refeds.org/sirtfi
Entity Category Adoption Internationally

CoCo: 330
R&S: 524
SIRTFI: 250
SIRTFI adoption in SWITCHaai IdPs

- CERN
- Universities
  - Universität Basel
  - Université de Genève
- Universities of applied sciences
  - HES-SO
  - HSR
- ETH-Rat
  - EPFL
  - ETH Zürich
  - PSI
- SWITCH
  - SWITCH edu-ID
  - SWITCH
  - VHO