How an Organization Integrates edu-ID
Using the example of SWITCH

Rolf Brugger
rolf.brugger@switch.ch
Bern, 14.03.2018
An organization adopts SWITCH edu-ID
Organization Operating its own AAI-IdP
Organization with edu-ID Integration
The organization SWITCH has adopted edu-ID last year
identity management

users

organisations

services
The User’s Perspective
Communication to Users

x - 6 months
"Get an edu-ID and link it to your AAI – account"

x - 10 days
“SWITCH will integrate edu-ID. You will see a new login window.
• Use your email address as user name
• Use your SWITCHdrive password or set a new one.”
There are more than 30 attributes defined for SWITCHaai. Most participating organisations release a subset of these attributes only, and not all attributes are available to every AAI user. What you should see below is:

- **8 SWITCHaai core attributes**, released by the user’s home organisation and must be available for all users
- 0 or more **other SWITCHaai attributes**, released by the user’s home organisation and are optional to implement for users
- 0 or more **local/bilateral attributes**, released by the user’s home organisation and are used only by one or a few organisations
- 5 or more **Metadata attributes**, set by the Shibboleth Service Provider from the user organisation’s metadata. Find out more...
- 8 or more Shibboleth attributes, set by the Shibboleth Service Provider if a user has a valid session.

**Further Checks**

It is also recommended to check if SWITCH is passing the:

- **Interfederation Attribute Check** to allow its users access to research and education services world-wide available via eduGAIN
- **Attribute Query Check** to allow Service Providers to query user attributes from the SWITCH Identity Provider using a user’s eduPersonTargetedID/persistentID attribute. This is allows services find out if a user account still exists and to update user records out of band. It also is a requirement for the migration to the Swiss edu-ID.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistent-id</td>
<td><a href="https://attribute-viewer.aai.switch.ch">https://attribute-viewer.aai.switch.ch</a></td>
</tr>
<tr>
<td>SAML2 Attribute Name: um:oid:2.16.756.1.2.5.1.1.1</td>
<td><a href="mailto:642448@switch.ch">642448@switch.ch</a></td>
</tr>
<tr>
<td>uniqueID</td>
<td></td>
</tr>
<tr>
<td>SAML2 Attribute Name: um:oid:2.16.756.1.2.5.1.1.1</td>
<td></td>
</tr>
<tr>
<td>givenName</td>
<td>Rolf</td>
</tr>
<tr>
<td>SAML2 Attribute Name: um:oid:2.5.4.4</td>
<td></td>
</tr>
<tr>
<td>surname</td>
<td>Brugger</td>
</tr>
<tr>
<td>SAML2 Attribute Name: um:oid:2.5.4.4</td>
<td></td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:rolf.brugger@switch.ch">rolf.brugger@switch.ch</a></td>
</tr>
<tr>
<td>SAML2 Attribute Name: um:oid:0.9.2342.19200300.100.1.3</td>
<td></td>
</tr>
<tr>
<td>homeOrganization</td>
<td>switch.ch</td>
</tr>
</tbody>
</table>
There are more than 30 attributes defined for SWITCHaai. Most participating organisations release a subset of these attributes only, and not all attributes are available to every AAI user. What you should see below is:

- 8 SWITCHaai core attributes, released by the user’s home organisation and must be available for all users
- 0 or more other SWITCHaai attributes, released by the user’s home organisation and are optional to implement for users
- 0 or more local/bilateral attributes, released by the user’s home organisation and are used only by one or a few organizations
- 5 or more Metadata attributes, set by the Shibboleth Service Provider from the user organisation’s metadata. Find out more...
- 8 or more Shibboleth attributes, set by the Shibboleth Service Provider if a user has a valid session.

Further Checks
It is also recommended to check if SWITCH is passing the:

- Interfederation Attribute Check to allow its users access to research and education services world-wide available via eduGAIN
- Attribute Query Check to allow Service Providers to query user attributes from the SWITCH Identity Provider using a user’s eduPersonTargetedID/persistentID attribute. This is allows services find out if a user account still exists and to update user records out of band. It also is a requirement for the migration to the Swiss edu-ID

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistent-id</td>
<td><a href="https://aai-logon.switch.ch/idp/shibboleth/https://attribute-viewer.aai.switch.ch/shibboleth187F09XCjisuVAsw9Cq1M0Q19raH4=">https://aai-logon.switch.ch/idp/shibboleth/https://attribute-viewer.aai.switch.ch/shibboleth187F09XCjisuVAsw9Cq1M0Q19raH4=</a></td>
</tr>
<tr>
<td>SAML2 Attribute Name: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</td>
<td><a href="mailto:642448@switch.ch">642448@switch.ch</a></td>
</tr>
<tr>
<td>uniqueID</td>
<td></td>
</tr>
<tr>
<td>SAML2 Attribute Name: urn:oid:2.16.756.1.2.5.1.1.1</td>
<td>Rolf</td>
</tr>
<tr>
<td>givenName</td>
<td></td>
</tr>
<tr>
<td>SAML2 Attribute Name: urn:oid:2.5.4.42</td>
<td>Brugger</td>
</tr>
<tr>
<td>surname</td>
<td></td>
</tr>
<tr>
<td>SAML2 Attribute Name: urn:oid:2.5.4.4</td>
<td></td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:rolf.brugger@switch.ch">rolf.brugger@switch.ch</a></td>
</tr>
<tr>
<td>homeOrganization</td>
<td>switch.ch</td>
</tr>
</tbody>
</table>
The Perspective of the Service Providers
Communication to Service Providers

"SWITCH will integrate edu-ID. Users will see another login window. Technically, nothing changes for the SP."

x - 10 days

Woah! We need more time for testing!

Our metadata is hardwired!
The Perspective of the Organization
Setup with an Integrated Organization

Linked Integrated

Educ-ID

Aai: Uni-X

WAYF

Uni-X IdP
Entity-ID: uni-x.ch

Attribute Provider

edu-ID

Affiliation chooser

edu-ID Login

edu-ID IdP
Entity-ID: edu-ID.ch

Entity-ID: edu-ID.ch

Entity-ID: uni-x.ch

© 2018 SWITCH | 17
Adoption Approaches

Linking at Registration

Member enrolment → Employee mgt system → Meta DB (Full edu-ID coverage) → Email, Name, ID

Member enrolment → Student mgt system → Meta DB (Partial edu-ID coverage)

Member enrolment → Cont. educ. mgt system → Member un-enrolment

Linking at Admission

Member enrolment → Employee mgt system → Meta DB (Full edu-ID coverage) → edu-ID Linking (i.e. email invitation)

Member enrolment → Student mgt system → Account Creation

Member enrolment → Cont. educ. mgt system → Member un-enrolment

Linking after Admission

Member enrolment → Employee mgt system

Member enrolment → Student mgt system

Member enrolment → Cont. educ. mgt system

Member un-enrolment

https://projects.switch.ch/eduid

© 2018 SWITCH | 18
SWITCH IdM before Day X

Employee mgt system registration (web-form)

LDAP Directory

IdP (Shibb)

edu-ID API, attribute aggregator, IdP

<table>
<thead>
<tr>
<th>id</th>
<th>Name</th>
<th>Email</th>
<th>Addr</th>
<th>…</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Send registration form to employee (paper)

Fill in registration form and send it back

Fill in internal web form

Send data to directory

Activate account on first working day
SWITCH IdM after Day X

1. Link edu-ID
2. Employee mgt system registration (web-form)
3. Fill in internal web form
4. Send data to directory
5. Activate account on first working day
6. Create affiliation

<table>
<thead>
<tr>
<th>id</th>
<th>Name</th>
<th>Email</th>
<th>Addr</th>
<th>…</th>
<th>eduID-Iden</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HR sends registration form to employee (paper) with edu-ID instruction
Fill in registration form and send it back
Link edu-ID, sends Identifier by email
Fill in internal web form
Send data to directory
Activate account on first working day
Create affiliation

© 2018 SWITCH | 20
Registration of a new Member

1. Link edu-ID
2. Employee mgt system registration (web-form)
3. LDAP Directory
Diese Seite dient der Anmeldung neuer SWITCH Mitarbeitender. Dazu werden der SWITCH edu-ID Identifikator und die unten angezeigten Daten an das Human Resources Team von SWITCH übermittelt, welches diese Angaben dann in die relevanten Benutzerverzeichnisse einträgt. 

Folgende Informationen an das SWITCH Human Resource Team übermitteln:

**Swiss edu-ID Identifier**

674f1668-6299-

**Vorname**

Rolf

**Familienname**

Brugger

Klicken sie auf 'Weiter' um mit der Anmeldung fortzufahren und die obigen Daten zu übermitteln.
Liebes HR Team,

Eine neue Registrierung für einen SWITCH Mitarbeiter ist eingegangen:

<table>
<thead>
<tr>
<th>Swiss edu-ID Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td>674f1668-6299-</td>
</tr>
<tr>
<td>Vorname: Rolf</td>
</tr>
<tr>
<td>Familienname: Brugger</td>
</tr>
<tr>
<td>Geburtsdatum: 19</td>
</tr>
<tr>
<td>E-Mail-Adresse:</td>
</tr>
<tr>
<td>Geschlecht: Männlich</td>
</tr>
<tr>
<td>Wohn-Adresse:</td>
</tr>
<tr>
<td>Mobil-Nummer: +41 79</td>
</tr>
<tr>
<td>ORCID Identifikator:</td>
</tr>
<tr>
<td><a href="http://orcid.org/0000-0001-9351-8252">http://orcid.org/0000-0001-9351-8252</a></td>
</tr>
<tr>
<td>Bevorzugte Sprache: Englisch</td>
</tr>
</tbody>
</table>

Falls euch dieser zukünftige Mitarbeiter bekannt ist, veranlasst bitte die nötigen Schritte um diesen Mitarbeiter zu erfassen und ihn in die relevanten Benutzerverzeichnisse einzutragen. Am Besten mit folgendem Link:

https://ldaptool.switch.ch/Request_User?swisseduid=674f1668-6299-

Vielen Dank & Freundliche Grüße
SWITCH edu-ID Team

--

SWITCH edu-ID is a service of SWITCH
SWITCH, Werdstrasse 2, P.O. Box, 8021 Zurich, Switzerland
https://projects.switch.ch/eduid/ eduid-support@switch.ch
Conclusions
Adopting the edu-ID at SWITCH

- Involved parties at the Organization
  - Human resources 1d
  - IdM/Account management 3-4d
  - Support 1d
  - Communication 1d

- Everything went smoothly

Main effort at edu-ID project team
Individual Roadmaps

Account linking of current members

Link users before day X

Link users at day X

Link users after day X

Onboarding of future members

Linking after admission

Linking at registration

Linking at admission

AP-Interface

Attribute push

Attribute pull
Adopting the edu-ID at Organizational Level

<table>
<thead>
<tr>
<th>Users</th>
<th>Service Providers</th>
<th>Organizational Identity Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Get an edu-ID</td>
<td>• (no changes)</td>
<td>• Provide mechanism to link edu-ID of new users to organizational ID</td>
</tr>
<tr>
<td>• Link your organizational ID to your edu-ID</td>
<td></td>
<td>• Extend directory with edu-ID identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Replace IdP by attribute provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inform edu-ID about new members (REST API call)</td>
</tr>
</tbody>
</table>
One Single Digital Identity
with
Multiple Affiliations
Identities and Affiliations

IdP Authentication

SP Attributes

UZH

ZHAW

edu-ID

UZH

ZHAW

Private Identity

Affiliation

Affiliations
User Chooses Affiliation

edu-ID

UZH

ZHAW

Affiliation Chooser

www.switch.ch
This is the test instance of the SWITCH edu-ID service. It contains test accounts that can be deleted or changed any time. The service can also be restarted any time!

Choose an Identity to Proceed

You are about to access the service 'AAI Attribute Viewer' with one of your identities. Choose one to proceed.

When you return to the service it will recognize you with the identity you choose now.

Student @ switch.ch
rolf.brugger@switch.ch

Private Person
mail@rolfb.ch

Manage your identities
Services Define Accepted Affiliations

• SWITCH edu-ID can represent
  • A private identity
  • And multiple affiliations

• Many SPs will not accept all kinds of affiliations
  • Access to Student Dashboard ➞ university members only
  • Student registration ➞ private users only

→ Intended Audience setting in resource registry
One Affiliation - Service limited to students
Two Affiliations - Service limited to students

Affiliation Chooser

edu-ID

UZH

ZHAW
No Affiliation - Service limited to students
Service limited to private users only:
Service accepts all kinds of users:
Extended Service:

edu-ID
___
___
___

UZH
___
___
___
___

ZHAW
___
___
___

edu-ID
___
___
___

UZH
___
___
___

ZHAW
___
___
___

© 2018 SWITCH | 40
### Default Intended Audience

- **University** users are ... *excluded*
- **University of Applied Sciences** users are ... *excluded*
- **Hospital** users are ... *excluded*
- **Library** users are ... *excluded*
- **Professional education and training college** users are ... *excluded*
- **Institution on the upper secondary level** users are ... *excluded*
- **Virtual Home Organization** users are ... *excluded*
- **Other** users are ... *excluded*

### Specific Intended Audience

This section allows defining exceptions to the above default intended audience. The settings below always have precedence over the default audience settings.

- **Add a new specific intended audience**

  - ** SWITCH edu-ID** users are... *included*

### SWITCH edu-ID Private Identity

Users with a **SWITCH edu-ID Private Identity** are...

- If **included**, your resource may receive SAML assertions for SWITCH edu-ID users who might not have an active affiliation with an organisation and self-registered their account with only their **private identity**.

- If **excluded**, the SWITCH edu-ID IdP will **not issue** SAML assertions for SWITCH edu-ID private identities.

Pick **include** if your resource offers its services to a broad user base and does not intend to restrict user access based on organisational affiliations only. Your resource can identify a SWITCH edu-ID private identity by its eduPersonScopedAffiliation value 'affiliate@eduid.ch'.
Conclusions

- Affiliation chooser is relevant for organizations with integrated edu-ID
- Long-term perspective: It will replace the WAYF
- With properly configured intended audience

→ improved user experience