SWITCH edu-ID for Beginners

Thomas Bärecke
Thomas.baerecke@switch.ch

Swiss edu-ID update event
27.06.2018 Bern
The foundation: SWITCHaai

Enter higher education, get one key, access many resources
SWITCHaai Federation Spring 2018

- 99.9% coverage in higher education

# AAI enabled accounts

# Resources

# Home Organizations

Interfederation enabled
eduGAIN: Current Status

eduGAIN in Total
• 2'716 IdPs
• 1'972 SPs

Status in CH
• 52 IdPs enabled
  ~ 85% of all AAI accounts
  ~ 97% of all Higher Ed accounts
• 18 SPs enabled

https://technical.edugain.org/status
https://www.switch.ch/aai/interfederation
But what happens over time?

School, University education, Side Job, Community Work, Side Job, Post-graduate, Employment, Further education, Further education, Self-Employment.
Tidying up

Swiss edu-ID

- School
- University education
- Side Job
- Side Job
- Community Work
- Employment
- Post-graduate
- Further education
- Employment
- Self-Employment
- Further education

© 2018 SWITCH | 8
With SWITCHaai

- students
- employees
- externals, guests
- collaborations, project teams

SWITCHaai

e.g. service specific secondary logins
With SWITCH edu-ID

- students
- employees
- externals, guests
- collaborations, project teams

If needed: richer attribute set available
SWITCH edu-ID concept corner stones

• Persistency:
  – Built to survive organisational affiliations

• User-centrism:
  – User issues his/her identity in a light-weight self-registration process
  – User brings his/her identity to the university/employer (if pre-existing)
  – User decides whether to pass on data (but usually not on its contents!)
SWITCH edu-ID concept corner stones (cont.)

• Organisational backing:
  – Organisations add or validate attributes of identities

• Openness:
  – Open to members of Swiss academia and people with relation to it

• Scalable quality:
  – Allow for low quality: Yes, this is a feature!
  – Foresee validation processes to increase the quality level
  – Offer quality transparency: relying parties can base decisions on quality level

• Support mobile environments and non-web use cases
Affiliations, Roles

Alice
- UniA - current
  Affiliation: staff
- UniA - former
  Affiliation: student
  AA UniA

Bob
- UniB - current
  Affiliation: student
- UniB - former
  Affiliation: student
  AA UniB
IdM Trends: with SWITCH edu-ID

- 2019: SLSP/Libraries
- 2017: SWITCH engines
- 2016: National licenses, WITCH drive
- 2018: Mobile/non-web, LoA, MFA

SWITCH edu-ID:
- SwissID
- Educa.ch
- Regular contacts
- Federal consultation 2017

Edu-ID university:
- Regular contacts
- Regular contacts

© 2018 SWITCH
“Swiss edu-ID” vs. “SWITCH edu-ID”

• The concept “Swiss edu-ID”
  – Reflected in the architecture document and in the service description

• The identifier “Swiss edu-ID”
  – A 32 digit hexadecimal encoded number following RFC4122. Well hidden.

• The project “Swiss edu-ID”
  – SWITCH initiated the CUS P-2 projects “Swiss edu-ID” and “Swiss edu-ID phase II” to implement the roadmap of the substrategy

• The service “SWITCH edu-ID”
  – The services “SWITCH edu-ID V1.0” and “SWITCH edu-ID V2.0” are milestones on that roadmap
Broader Use Cases

- **SWITCH edu-ID**
  - e.g. LMS for students, staff, external people
  - Serving a wider user base

- **SWITCH edu-ID**
  - e.g. National Licenses

- **SWITCH haai**
  - e.g. LMS for students and staff

- **SWITCH edu-ID**
  - e.g. Academic File Sharing

Multiple affiliations and (meta-) quality information
Data Model

Private Identity
- Unique/pers-edu-ID
- HomeOrg eduid.ch
- First/last name
- Email
- Home postal address
- Mobile phone
- Date of birth
- ORCID

Managed and controlled by individual

Current Affiliations
- HomeOrg: UniA
  - Unique/persistent-ID
  - First/last name
  - Date of birth
  - Email
  - Phone
  - Postal address
  - Affiliation
  - study branch
  - “local attributes”

Former Affiliations
- HomeOrg: UniB
  - Unique/persistent-ID
  - First/last name
  - Date of birth
  - Email
  - Phone
  - Postal address
  - Affiliation
  - study branch
  - “local attributes”

- HomeOrg: UniC
  - Affiliation
  - study branch
  - affiliation period

- HomeOrg: UniD
  - Affiliation
  - affiliation period

Managed and controlled by universities
## SP Opportunities

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extend user group (alumni, guests, …)</td>
<td></td>
</tr>
<tr>
<td>New attributes (edu-ID unique ID, ORCID)</td>
<td></td>
</tr>
<tr>
<td>Get extensive affiliation information</td>
<td></td>
</tr>
<tr>
<td>Get attribute quality information</td>
<td></td>
</tr>
<tr>
<td>Attribute verification processes</td>
<td></td>
</tr>
<tr>
<td>Get user profile change notifications</td>
<td>(  )</td>
</tr>
<tr>
<td>Share attribute/group information with other SPs</td>
<td>(  )</td>
</tr>
<tr>
<td>AM protocols for national services (OIDC, AD, LDAP)</td>
<td>(  )</td>
</tr>
<tr>
<td>Access to former affiliations</td>
<td></td>
</tr>
</tbody>
</table>
Benefits for Organizations

More efficient identity management
• More efficient enrollment processes for students (and staff)
• More up-to-date user information, less duplicates
• Finally a solution for all the “nasty” cases
  • Temporary or short term members like guests,
  • Research groups with university members and private partners
• Stay in contact with former members
• Long-term perspective: more quality for less money
  ➔ Cooperative identity management with universities
Cooperative Identity Management

University IdM-processes:
- Registration
- Name change
- Address change
- Incidents

SWITCH edu-ID IdM-Processes:

IdM Uni 2

IdM Uni 3

IdM Uni 4

IdM Uni 5

Name change
Address change
On/Offboarding
## Organisation Integration Depth

<table>
<thead>
<tr>
<th>Level</th>
<th>Tasks</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>linked</td>
<td>• “nothing”!</td>
<td>naked Swiss edu-ID</td>
</tr>
<tr>
<td></td>
<td>• Communication measures</td>
<td>edu-ID with affiliations and assurance levels</td>
</tr>
<tr>
<td>integrated</td>
<td>• Migrate all users to edu-ID</td>
<td>• No local SAML-IdP required anymore</td>
</tr>
<tr>
<td></td>
<td>• Manage Swiss edu-ID identifier in internal directory</td>
<td>• More efficient user identity initialization</td>
</tr>
<tr>
<td></td>
<td>• Operate attribute provider</td>
<td>• Access to SPs with new Protocols</td>
</tr>
<tr>
<td>deeper integration</td>
<td>• Receive and process IdM updates from Swiss edu-ID</td>
<td>• New Auth methods</td>
</tr>
<tr>
<td></td>
<td>• Notify Swiss edu-ID of IdM updates</td>
<td>• Streamlined IdM processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• up-to-date identities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- locally</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- in entire community</td>
</tr>
</tbody>
</table>
Lunch

until 13:15

Main course:
Buffet

Dessert:
Coffee, Sweets etc.: Cafeteria kiosk
(please show your badge)