SWITCH edu-ID for Beginners

Christoph Graf
christoph.graf@switch.ch

Berne, 29.6.2017
Topics for the next 60 minutes

- Introduction and numbers (Christoph Graf)
- Why SWITCH edu-ID (Andres Aeschlimann)
- News for Services (Rolf Brugger)
- News for Organisations (Rolf Brugger)
Our core beliefs

Together for greater capability, convenience and security in the digital world.
SWITCH is an integral part of the Swiss academic community.

Based on our core competencies

- Network
- Security
- Identity Management

SWITCH offers collaboratively developed ICT solutions that empower users in and beyond the academic world to achieve leading edge results in a globally competitive environment.
Added value for customers

Community work

Foundation

Integrated offer
Foundation purpose

Excerpt from the deed of foundation
Berne, 22 October 1987

"The foundation has as its objective to create, promote and offer the necessary basis for the effective use of modern methods of telecomputing in teaching and research in Switzerland, to be involved in and to support such methods.

It is a non-profit foundation that does not pursue commercial targets."
Our customers

SWITCH community
- Swiss universities on tertiary level (academic sector) and their research institutions

Extended community
- Other organizations involved in research or education

Commercial customers
- Registrars of .ch- and .li-Domain-Names, Swiss financial institutions, research-related industry and government
Integrated offer

- Video Management
- Collaboration
- Procurement
- Network
- Trust & Identity
- Security
- Infrastructure & Data Services
- Registry
The universal and secure key

SWITCH edu-ID is the universal and safe identity for access to services in the academic community.

Customers
• Universities
• University related organizations
• Third-party providers

Services
• IdP/AP-hosting
• 800 service provider, 70 federation partner

Your benefits
• One identity for all services in the federation
• Legal bases of Switzerland
• Governance defined by the universities
• SWITCH as a partner for your investment in the future
The foundation: SWITCHaai

Enter higher education, get one key, access many resources
But what happens over time?
Tidying up

Swiss edu-ID

School

University education

Employment

Self-Employment

Side Job

Post-graduate

Employment

Further education

Side Job

Community Work

Further education

School
Why SWITCH edu-ID

Andres Aeschlimann
andres.aeschlimann@switch.ch

Berne, 29.6.2017
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
People without SWITCHaai accounts?

SWITCHaai: ☒
SWITCH edu-ID: ✓

Services and tools
Openness: “Not anyone should have a SWITCH edu-ID”

because

Getting access is done by a
- explicit (identify person)
- implicit (personal attribute)
registration procedure

misconception

User-centrism: “Make sure SWITCH edu-ID has sufficient quality”

because

SPs can rely on high quality attributes

but

Not all SPs need high quality attributes

attribute

tradeoff

quality

low entrance barrier

Counterexample: ID / Passport

Counterexample: Github-ID
Affiliations, Roles

Alice

UniA - current  
Affiliation: staff

UniA - former  
Affiliation: student

AA UniA

Bob

UniB - current  
Affiliation: student

UniB - former  
Affiliation: student

AA UniB
What’s in for the Universities?

- Migrated university
- Mobile/ non-web
- National licenses
- SWITCH drive
- CH/EU eID?
- SuisseID /SwissID
- educa.ch
- MFA
- LoA/QL
- SLSP/ Libraries ?
- SDSC ??

© 2017 SWITCH | 7
“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
Basic Components of the SWITCH edu-ID

SWITCH edu-ID Operator

- Affiliation Archive
- Affiliation Index
- Attribute Aggregator
- Attribute Filter
- Federation Registry
- Attribute Authority
- User Profile Panel
- User Authentication
- Audit Log
- SP Notification
- IdM Provisioning Service
- User Directory
- User Provisioning Service
- IdM Admin Panels
- Affiliation Archive
- Federation Registry

SWITCHedu-ID Participant

- Organisational IdM
- Attribute Provider
- Organisational Directory

Participants and Federation Partners

Participants
# Decision Matrix for Services

<table>
<thead>
<tr>
<th>ID for university members only</th>
<th>One affiliation at a time ➔ classic model</th>
<th>Multiple affiliations at a time or quality info ➔ extended model</th>
</tr>
</thead>
<tbody>
<tr>
<td>• LMS for students and staff</td>
<td>• Academic file sharing system (SWITCHdrive)</td>
<td>• Private people accessing to research publications (National Licenses) edu-ID</td>
</tr>
<tr>
<td>AAI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Broader Use Cases

- **SWITCH edu-ID**
  - e.g. LMS for students, staff, external people

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

- **SWITCHaai**
  - e.g. LMS for students and staff

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

Serving a wider user base

Multiple affiliations and (meta-) quality information
Questions?
Services and SWITCH edu-ID

Rolf Brugger
rolf.brugger@switch.ch

Berne, 29.6.2017
Data Model

Base Identity

<table>
<thead>
<tr>
<th>Unique/pers-edu-ID</th>
<th>HomeOrg eduid.ch</th>
<th>First/last name</th>
<th>Email</th>
<th>Home postal address</th>
<th>Mobile phone</th>
<th>Date of birth</th>
<th>ORCID</th>
</tr>
</thead>
</table>

Managed and controlled by individual

Current Affiliations

<table>
<thead>
<tr>
<th>HomeOrg: UniA</th>
<th>Unique/persistent-ID</th>
<th>First/last name</th>
<th>Date of birth</th>
<th>Email</th>
<th>Phone</th>
<th>Postal address</th>
<th>Affiliation</th>
<th>study branch</th>
<th>“local attributes”</th>
</tr>
</thead>
</table>

Former Affiliations

<table>
<thead>
<tr>
<th>HomeOrg: UniB</th>
<th>Unique/persistent-ID</th>
<th>First/last name</th>
<th>Date of birth</th>
<th>Email</th>
<th>Phone</th>
<th>Postal address</th>
<th>Affiliation</th>
<th>study branch</th>
<th>“local attributes”</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>HomeOrg: UniC</th>
<th>Affiliation</th>
<th>study branch</th>
<th>affiliation period</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>HomeOrg: UniD</th>
<th>Affiliation</th>
<th>study branch</th>
<th>affiliation period</th>
</tr>
</thead>
</table>
SWITCH edu-ID quality model

- Authentication quality: NIST SP 800-63-2
  - Level 1: no id proving
  - Level 2: single factor auth
  - Level 3: multi factor auth
  - Level 4: multi factor auth with hard cryptographic tokens

- Attribute validation quality: eCH-0171 quality model
  - Level 1 “low”:
    Minimal trust in asserted value
  - Level 2 “medium”:
    Basic processes and control mechanisms. Verification with non-official ID or certificate
  - Level 3 “high”:
    Processes and control mechanisms are supervised by external entity. Verification with more than one non-official ID or certificate
  - Level 4 “very high”:
    Processes backed by legal standards. Supervision by accredited entity. Verification with official ID or certificate
## Quality in Both Models

### “Extended Model”

<table>
<thead>
<tr>
<th>Unique/pers-edu-ID</th>
<th>HomeOrg eduid.ch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>quality 1..4</td>
</tr>
<tr>
<td>Email (user-managed)</td>
<td>quality 1..4</td>
</tr>
<tr>
<td>Home postal address</td>
<td>quality 1..4</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>quality 1..4</td>
</tr>
<tr>
<td>Date of birth</td>
<td>quality 1..4</td>
</tr>
<tr>
<td>ORCID</td>
<td>quality 1..4</td>
</tr>
<tr>
<td>Affiliation</td>
<td>student</td>
</tr>
<tr>
<td>study branch</td>
<td></td>
</tr>
<tr>
<td>Email (affil)</td>
<td><a href="mailto:johnd@uniA.ch">johnd@uniA.ch</a></td>
</tr>
<tr>
<td>Affiliation</td>
<td>staff@UniB</td>
</tr>
<tr>
<td>Email (affil)</td>
<td><a href="mailto:johnd@UniB.ch">johnd@UniB.ch</a></td>
</tr>
</tbody>
</table>

### “Classic Model”

<table>
<thead>
<tr>
<th>Unique/pers-ID</th>
<th>id@UniA</th>
</tr>
</thead>
<tbody>
<tr>
<td>HomeOrg</td>
<td>UniA</td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Home postal address</td>
<td></td>
</tr>
<tr>
<td>Mobile phone</td>
<td></td>
</tr>
<tr>
<td>Date of birth</td>
<td></td>
</tr>
<tr>
<td>ORCID</td>
<td></td>
</tr>
<tr>
<td>Affiliation</td>
<td>student@UniA</td>
</tr>
<tr>
<td>study branch</td>
<td></td>
</tr>
<tr>
<td>Email (affil)</td>
<td><a href="mailto:johnd@uniA.ch">johnd@uniA.ch</a></td>
</tr>
</tbody>
</table>

AAL-quality
### 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
Duplicates

“A person has at most one account”

• Intentional or unintentional duplicates?
• Technical measures
  – Register personal attributes and check for uniqueness:
    email, mobile phone number, Orcid-ID, passport number…
  – Heuristics with groups of attributes:
    first name + last name + birth date
  – Costs of attribute verification?
  – Data protection! (Social security number AHVN13)
• Service-Design
  – In the long run a person has no advantage with a double identity
    ➔ can be achieved if identity is intensively used
## 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></td>
<td></td>
<td>• New Auth methods</td>
</tr>
<tr>
<td>deeper integration</td>
<td>• Receive and process IdM updates from Swiss edu-ID</td>
<td>• Streamlined IdM processes</td>
</tr>
<tr>
<td></td>
<td>• Notify Swiss edu-ID of IdM updates</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

Salads, Curry & Beverages: Buffet

Dessert: Coffee, Sweeties etc.: Cafeteria kiosk

(please show your badge)
SWITCH – an integral part of the Swiss academic community since 1987.

www.switch.ch/30years
Agenda

Welcome & introduction

Pilot projects
- National licenses service
- Student registration pilots
- Cloud-ID migration
- Swiss edu-ID mobile app

Coffee break (14:30 – 14:55)

First results from migration strategy planning
- Most promising integration scenarios
- Status & statements from participating universities

Roadmap and next steps

Conclusions (until 16:15)
Mission

SWITCH is an integral part of the Swiss academic community.

Based on our core competencies

- Network
- Security
- Identity Management

SWITCH offers collaboratively developed ICT solutions that empower users in and beyond the academic world to achieve leading edge results in a globally competitive environment.
Added value for customers

- Community work
- Foundation
- Integrated offer
Our customers

SWITCH community
- Swiss universities on tertiary level (academic sector) and their research institutions

Extended community
- Other organizations involved in research or education

Commercial customers
- Registrars of .ch- and .li-Domain-Names, Swiss financial institutions, research-related industry and government
SWITCH edu-ID / SWITCHaai

The universal and secure key
SWITCH edu-ID is the universal and safe identity for access to services in the academic community.

Customers
- Universities
- University related organizations
- Third-party providers

Services
- IdP/AP-hosting
- 800 service provider, 70 federation partner

Your benefits
- One identity for all services in the federation
- Legal bases of Switzerland
- Governance defined by the universities
- SWITCH as a partner for your investment in the future
SWITCHaai Federation Summer 2017

99% coverage in higher education

# AAI enabled accounts

# Resources

# Home Organizations

Interfederation enabled
Strategy work of CRUS-P2

- Use cases collected in spring 2013
- Findings and conclusions published:
  - "Foundations for the strategy", aka "Identity Management"
  - Prominent role of identity management for all "national services"
- Groups set up by CRUS-P2 to work on specific fields of action
  - Kick-off end of August 2013
  - Results delivered by 11 October 2013
- Strategy group "Identity Management":
  - Matteo Corti, ETH Zürich
  - Omar Benkacem, Université de Genève
  - Roberto Mazzoni, UZH
  - Wolfgang Lierz, ETH Bibliothek
  - Christoph Graf, SWITCH
  - Dieter Glatz, Universität Basel
  - Kai Blanke, Universität St. Gallen
  - Mario Gay, Università della Svizzera italiana
SWITCH edu-ID identity corner stones

**Persistency**: identities to survive organisational affiliations

**User-centrism**: the only stable element is the user

**Organisational backing**: the primary trust anchor

**Openness**: for all users with relation to Swiss academia

**Scalable quality**: transparency & validation processes

Support **mobile** environments & **non-web** use cases
Project roadmap 2014-2020

Swissuniversities’ funding uncertainty:
• No submission opportunity mid Aug 2017
• Future submission process under review

Position of SWITCH: We follow this roadmap
What are National Licences?

- Purchase of eJournals backfiles (up to 2015)
- For the scientific community in Switzerland
- Funded by SUC-P2 (swissuniversities)
- 7.6 Mio. CHF for products, 2.57 Mio CHF for long-term archiving and infrastructure

Project of the Consortium of Swiss Academic Libraries

- University members
- Private individuals
In order to guarantee a relevant and varied portfolio for the national licences, established academic publishers were selected for the project. These national licences form a journal portfolio that is used comprehensively and frequently. Access until the recent past (2015) is possible.
National Licenses Requirements

• Needs to work for the whole Switzerland
• Meet the contractual agreements: (citizenship, active user, terms of use)
• Access should be granted immediately to authorized persons (no need to go to a library, to wait for a letter, ...)
• Authentication should be possible directly on publisher's platform (no proxy) using SAML/Shibboleth
• The process should as automated as possible
Division of Responsibilities

SWITCH edu-ID

• Manage identities for private individuals
• Verification procedures for home address and mobile phone number
• Implement entitlement attribute `common-lib-terms`
• IdP / SAML
• Technical support

National Licenses

• Contact to publishers
• End-user interface
  – Search engine for scientific articles
  – User registration platform
  – Manage rules for user entitlements
• End-user support
National Licenses

www.nationallicences.ch
www.swissbib.ch

Access for private users available since December 2016 via swissbib

- 6.2 Mio Articles
- 1’000 private users
Registration Pilots of ZHAW, ZHdK and FHNW

Petra Kauer-Ott
petra.kauer@switch.ch
Berne, 29.6.2017
Student Registration Pilots

Goals:
1. Improve/redesign registration process  
   (as part of IdM/IAM redesign)
2. Replace “throw away identities” for student candidates
3. Equip new members with an edu-ID (facilitate transition)

Pilots:
• ZHAW: Go live 31.5.17 (operational)
• ZHdK: Go live decision end of July 2017
• FHNW: Go live 30.6./1.8.17

Adaptations of Evento are included in the latest release.
Project Online-Registration (ONLA)

Registration Portal with Evento and SWITCH edu-ID
Project Online-Registration (ONLA)

Contents:

• Project development process
• Current situation
• Outlook
• Technical integration
Project Online-Registration (ONLA)

Project development process

- April 2015: Start project "Online Anmeldung" (online registration)
  - No suitable tool available on the market.
- October 2015: Discussion with FHNW colleagues.
  - FHNW on the way to create tender documents.
  - Already decided to cooperate with SWITCH.
Project Online-Registration (ONLA)

Project development process

• November 2015: Solution with Evento
  ▪ new technology “WebModules”
  ▪ EFHG = 11 universities form a panel to develop 'their' Evento
  ▪ 11 universities shared the costs – and can use the new online registration
  ▪ ZHAW and FHNW run the project together
Project Online-Registration (ONLA)

ONLA is ONLINE

Degree: Master of Science in Life Science
Semester start: Spring Semester 2018
Since: 31.05.2017

Website Department N
Anmeldung Master of Science in Life Sciences

Im Anmeldeportal melden Sie sich online für einen Studienplatz an der ZHAW an. Sie werden dabei durch den Anmelde-, Zulassungs- und Immatrikulationsprozess begleitet.

Vorbereitung Unterlagen und Informationen

Halten Sie für die Anmeldung alle Unterlagen in elektronischer Form bereit beziehungsweise legen Sie sich die notwendigen
Project Online-Registration (ONLA)

Student Registration

Enter your e-mail address and password below, then click on the Login button to continue.

**SWITCH edu-ID**

E-mail: [john.doe@example.org](mailto:john.doe@example.org)

Password: [Hint your password](#)

Login

Forgot password?

Options for personal data protection:

For registration at ZHAW you need an Swiss edu-ID account.
If you don't have one already, please create it now.
Project Online-Registration (ONLA)

Outlook:

- Students can register to all degrees online for study starts from Autumn Semester 2018 onwards.

- A subsequent project which has been initiated to implement ONLA professionally and technically shall be finalised in October 2017.
Project Online-Registration (ONLA)

Why SWITCH edu-ID?

• Challenge of identity:
  ▪ We need to be able to identify each individual login.
  ▪ We should not create any student account before matriculation.

➤ SWITCH edu-ID offers a solution for exactly this problem!
Project Online-Registration (ONLA)

Key integration requirements:

• User Interface:
  ▪ Good and clear information about the process
  ▪ Customizable registration/login screens (logo, text, links)

• Technical:
  ▪ Swiss edu-ID internal identifier available for SP
  ▪ Integration with CLX.EventoNG
Project Online-Registration (ONLA)

Customizable:

redesigned registration process with less single steps
Project Online-Registration (ONLA)

Technical realization:

- Create a SWITCH edu-ID and login to the registration portal:
  - Person is created in Evento and its UID is stored in the Evento-Database.
  - CLX.Evento OAuth Server supports SAML2.0.
  - Logout on Evento and SWITCH is possible.
Next steps I:

- Duplicate detection
  - Currently only few fields are used in registration process (firstname, surname, e-mail)
  - Primary identifier missing (e.g. social security number, birthdate)

- For candidates who already have an internal account (employees, current students):
  - In planning: Login with existing AD account (via ADFS)
  - Maybe: automatic detection on single Loginpage: SWITCH <> ADFS
Project Online-Registration (ONLA)

Next steps II:

• Synchronization between SWITCH edu-ID and Active Directory…
ZHdK ONLA Pilot

Claudia Monstein, project leader IAM

Ongoing IAM redesign project

→

Occasion to implement online registration
Online Registration Pilot

for master studies music and design

Planning: Go Live in summer 2017

Decision: end of July 2017

Precondition: tested, reliable and approved pilot solution
Implementation of ONLA with SWITCH edu-ID

but …

additional requirement is feature for multiple login options:
• developed by Crealogix
• not ready yet
• must be tested before go live
Best & Worst Case

涼:
- multiple login options: AD login AND edu-ID login
  - student with local account uses AD account
  - new student uses edu-ID account

運:
- only login option with edu-ID for all students
  - risk of duplicates
Change Process

- Complexity of IAM project
- Staff ready for new process?
- Legal questions answered?
- Requirements of different study fields implemented? (standardization vs. individualized solutions)
edu-ID Pilot Projects
@fhnw
edu-ID Pilot Projects

3 pilot projects

- EVER
- ONLA
- Groups Inside Guest
EVER

- Evento Event Registration
- Continuing Education courses (CAS, MAS, seminars, etc.)
- Login with edu-ID and AAI FHNW
- Single Page Angular Application with .NET Backend Services
- OIDC Authentication
- Go-Live: 30.06.2017
ONLA

- Online Registration for degree studies (bachelor and master)
- Part of Evento school administration suite (developed by CREALOGIX)
- Login only via IdP edu-ID
- Go-Live: 01.08.2017
Groups Inside Guest

- SharePoint Collaboration Platform
- Working with external partners, researchers, suppliers etc.
- Migration project (replacing an existing solution with dedicated AD)
- Consistent user experience for FHNW resources
- Go-Live: 01.11.2017
Key aspect 1 – High level process

Same generic process in all cases:

1. Onboarding application (initiate)
2. Manage edu-ID affiliation @fhnw in IAM System
3. Access FHNW resources (based on Affiliation attributes)
Key aspect 2 – seamless user experience

- 2 registration flows
  - Registration with Login
  - Login (with Registration if needed)
- Only possible with a edu-ID Registration Form Customization (return url)
- Flows can be controlled with special parameters (target URL)
  - Security restriction: same host as Service Provider
- Target URL is consistent through the whole registration flow
Login mit eduID
→ login
→ register

www.fhnw.ch/eduid

FAQ Seite

Aufruf mit URL Parameter
- ?entityID=sts.fhnw.ch
- ?target=appName (neu)
(target ist ein optionaler Parameter welcher über gesamter
Registration Request bestehen bleiben soll)

Token bei email Verification (tokenID)
→ da muss der Parameter target auch wieder enthalten sein

Return URL *
Auswerten von target
- target = appA
- target = appB

Applikation A

Applikation A

Applikation B

Applikation B

eduid Registration

email address Verifikation

Demo

Links

- https://www.switch.ch/aai/guides/sp/edu-id-link-composer/
Questions?

Contact:
- Michael Hausherr, Enterprise Architect
  T: +41 56 202 71 56, E: michael.hausherr@fhnw.ch
- Joël Hasler, System Specialist SharePoint
  T: +41 56 202 70 79, E: joel.hasler@fhnw.ch
Project Liaison with „Swiss edu-ID Mobile APP“

Christoph Graf
christoph.graf@switch.ch

Berne, 29.6.2017
SWITCH edu-ID identity corner stones

**Persistency**: identities to survive organisational affiliations

**User-centrism**: the only stable element is the user

**Organisational backing**: the primary trust anchor

**Openness**: for all users with relation to Swiss academia

**Scalable quality**: transparency & validation processes

Support **mobile environments** & **non-web** use cases
Liaison with project “Swiss edu-ID Mobile”

Goal: Sustainable integration of the Swiss edu-ID Mobile App deliverables with the SWITCH edu-ID services and infrastructure

Conditions: strategic fit and positive cost-benefit assessment (next milestone autumn 2017)

Lead: Christian Glahn, HTW Chur
Partners: USI, FHNW
Coffee Break

until 14:55

Take something to drink (coffee, tea etc.) & to eat (fruit, sugary treat etc.)

at the Cafeteria kiosk
(please show your badge)

After the break: Please fill in the feedback form!
Integration Scenarios
Integrating the SWITCH edu-ID at a University

Rolf Brugger
eduid@switch.ch

Bern, 28.6.2017
Adoption Path for an Organization

- API: Organization notifies edu-ID about new affiliations
- API: edu-ID knows current attributes for a person
  - edu-ID requests current attributes when they are needed (polling)
  - Organization notifies edu-ID about attribute changes (pushing)
- Make sure all organization members …
  - Have an edu-ID
  - Linked to organizational identity
    ➔ Current and future members
- Shut down local Shib-IdP
Onboarding of new (future) Users, Offboarding and Attribute Updates
On-/off-boarding in the “Leading System” approach

- Employee mgmt system
- Student mgmt system
- Cont. educ. mgmt system

Member enrolment (online form with edu-ID Login)

Email, Name, ID, …

Member un-enrollment

Email, Name, ID

don-/off-boarding, updates (notification)

ID, affiliation

edu-ID IdP

edu-ID IdM

User data flow

edu-ID protected web site
Decentral On-/off-boarding in the “Meta Directory” approach

**Member enrolment**
- Employee mgt system
- Student mgt system
- Cont. educ. mgt system
- Member un-enrolment

**Email, Name, ID**
- Meta DB: Full edu-ID coverage

**edu-ID**
- IdP
- IdM

**User data flow**
- edu-ID protected web site

© 2017 SWITCH | 5
Centralized On-/off-boarding in the “Meta Directory” approach (synchronous)

Member enrolment → Employee mgt system → Member enrolment
Member enrolment → Student mgt system → Member enrolment
Member enrolment → Cont. educ. mgt system → Member enrolment

Member un-enrolment

edu-ID Linking (i.e. mail invitation)

Account Creation

Onboarding (notification)

Meta DB
Full edu-ID coverage

edu-ID Linking

edu-ID unlinked

Member ID

Email ID

Affiliation ID

Offboarding, updates (by periodical polling)

edu-ID protected web site

User data flow
Centralized On-/off-boarding in the “Meta Directory” approach (asynchronous)

- Member enrolment
- Employee mgt system
- Student mgt system
- Cont. educ. mgt system
- Member un-enrolment
- “Meta” DB
- Partial edu-ID coverage
- edu-ID Linking
  - edu-ID protected web site
  - User data flow
  - edu-ID protected web site

- Member enrolment
- Member enrolment
- Member enrolment

- edu-ID IdP
- edu-ID IdM

- onboarding (notification)
- affiliation ID
- ID, affiliation
- offboarding, updates (by periodical polling)

© 2017 SWITCH | 7
edu-ID Linking Page

University: user profile

https://eduid.ch/link
?code=123XYZ
&ret=uni.ch/uprofile

edu-ID linked

https://uni.ch/uprofile
?code=123XYZ
&id=f7b83c42-9f3d-45de-8146-1e00e15938a9

SWITCH edu-ID

edu-ID login

create edu-ID

Onboarding “add affiliation”

edu-ID IdP
API to Update Affiliation Status (SCIM)

- Organization informs edu-ID IdP about affiliation changes
  - Add/remove affiliation
  - Update affiliation (attribute push as alternative to attribute polling)

- SCIM REST API (Draft)

**Add an affiliation:**

```text
PUT https://eduid.ch/api/v1/Users/04111fb2-5e82-4b20-81bf-fa0f4f86aa07
{
  swissEduIDLinkedAffiliation:"student@organization.org",
  swissEduIDAffiliationPeriodBegin:"2017-12-01"
}
```

**Remove an affiliation:**

```text
PUT https://eduid.ch/api/v1/Users/04111fb2-5e82-4b20-81bf-fa0f4f86aa07
{
  swissEduIDAffiliationPeriodEnd:"2017-12-01"
}
```
Equip all Current Organization Members with an edu-ID
Adoption Path

Linked

Integrated

© 2017 SWITCH | 12
Scenario 1: Involve all Users before Day X

Preparation: invite users to create and link edu-ID account

At day X: Merge linked accounts

Before day X: linked accounts have limited functionality. Users can’t access to classic SPs as Org-members.
Scenario 2: Involve Users after Day X

At day X: Users lose federation account

At day X: Merge linked accounts

After day X: invite users to create and link account
Scenario 3: create edu-ID for Users

At day X:
- Create edu-ID accounts
- Merge linked accounts

Duplicate resolution
Migration Strategy Planning

= preparatory work for adoption of SWITCH edu-ID
= project planning

1. Have/develop a clear vision (now → future)
2. Define goals, tasks and outline
3. Involve the right people
4. Identify risks
5. Describe work/steps
6. Define roadmap
Reach the finish line together

SWITCH edu-ID

University (IAM project)

Integration
The early birds are

- EPFL
- FHNW
- UNIFR
- UNIGE
- UNIL
- UNISG
- ZHAW
The early birds do

1. Work on their migration strategy

2. Show other birds how to “catch the worm”
Migration strategy project
@fhnw
Motivation

- Timing is everything
  - Identity and Access Management (IAM) Project
  - Benefit from each other
  - Good starting point for IAM project
- AAI very important for FHNW, high number of AAI enabled resources
  - SWITCH edu-ID is the evolution of AAI
  - Strategic topic
- Guidance from head of IT (initiated by enterprise architecture team)
Benefits

- Gives the possibility to re-engineer and automate various processes (e.g. ONLA – onboarding of students)
- Ability to eliminate media disruption and make the processes more consistent
- Bring your own account
  - Account management and Self-service functionalities can be outsourced for external and guest Accounts
- One Account for everything
  - Medium-term: specific target groups no longer need a local account (e.g.. ONLA → moodle → inside → eduroam …)
  - Long-term: one account for all services
Putting all pieces together

- Small project team (4-6 people from central IT)
- Focus on fundamental work, get the necessary technical expertise
- Work out the relevant parameters together with SWITCH
- When the «big picture» is all there we expand the project scope
  - Plan and initialize Communication
  - Start with the decision making process
Communication

- The question is when, how much to whom?
  - Communication is one of the key steps in this project

- What we did until now:
  - Specific selective communication in the pilot project scope
  - Respective product owner defined the communication strategy

- What we do in the future:
  - After «big picture» is assembled
  - Brood communication inside and outside of IT (different stakeholder)
    Ideas: raffle aligned with project marketing
          notice on the AAI Login Page
Technical challenges

- Integration of SWITCH edu-ID as federated identity into IAM system
- «Hybrid» edu-ID adoption scenario
- Custom attribute synchronization
- Kerberos integration for login
- Technical edu-ID Accounts
Ressource

- 3 Workshops (→ 1.5 day per person)
- Note:
  - a big part of the groundwork was done in the IAM project
  - preparation time for the workshops was therefore not excessive
- Pilot projects handled outside of the migration project
Next Steps

- 3 pilots go live within the next months
- One more workshop with SWITCH to finalize the big picture
- Decision making across all departments
- Setup the communication strategy
- Initialize the implementation project in coordination with the IAM project
Questions?

Contact:
- Michael Hausherr, Enterprise Architect
  T: +41 56 202 71 56, E: michael.hausherr@fhnw.ch
- Joël Hasler, System Specialist SharePoint
  T: +41 56 202 70 79, E: joel.hasler@fhnw.ch
Status & Statements

EPFL
Risks

• Strict regulations about exchange of private user data
• Acceptance of first movers’ risks is very low
• Integration of SWITCH edu-ID at minimal cost
Strict regulations about exchange of private user data

- No answers from the Federal Data Protection and Information Commissioner (FDPIC)
- Technical alternatives without attribute cache seem possible
Acceptance of first movers’ risks is very low

- Mostly all current EPFL WEB use cases are well managed by SWITCHaai
- Main stakeholders are not against SWITCH edu-ID. It may be a solution for the future. They are waiting
- Scientists have a strong need for Non-WEB Authentication at a Federation level
Integration of SWITCH edu-ID at minimal cost
FIRST WORKSHOPS – SWITCH EDU-ID
CONTEXT

- Full redesign of the Information System (Campus Management)
WHY PILOTING?

**PROs**
- «baby-sitting» by SWITCH

**CONs / RISK**
- Low maturity on both sides
OUR JOURNEY WITH SWITCH (…SO FAR)

- Objectives set upfront:
  - Architecture & migration strategy defined by end 2017

- 3x 2h workshop
  - Unifr participants: security officer, AAI admin, AD admin, software architect

- 3x 1h technical discussion (1-to-1)

- Preparation work (AAI admin): ~10h
TARGET ARCHITECTURE

- Meta Directory approach
- Centralised Provisioning approach
- Leading System approach
MIGRATION / ONBOARDING APPROACHES (TBC)

- **Onboarding (new students & new staff)**
  - Edu-ID account required on 1st access to AAI ressources, after cut-off day

- **Migration (existing students & staff)**
  - *Same as above*

- **Current discussions**
  - *Moodle users migration*
  - *Ok from Direction*
  - *Technical design and development*
THANK YOU FOR YOUR ATTENTION

Contact:
- aai@unifr.ch
Swiss edu-ID – UNISG Status Update
29. June 2017

Simon Frigg
# Project Information

## Project Goal

Base for SWITCH edu-ID is provided at UNISG

## Tasks

- Define onboarding processes for students & staff
- Create tool for mapping of SWITCH edu-ID and UNISG accounts
- Store SWITCH edu-ID Identifier
- Integrate login mechanism via ADFS

## Benefit

- Replacement of SWITCHaai
- Access for library users (Swiss Library Service Platform (SLSP))
- Redesign of future registration process: Use of SWITCH edu-ID
- Joint Medical Master HSG & Uni ZH – possible collaboration
Integration Scenario(s)

Best Chances:
Mix between «Meta-Directory» and «Centralised Provisioning»

Reasons:
• Many independent Business Units administer their own applications with own data sets
• Within project Swiss edu-ID only base is elaborated
• Swiss edu-ID project depends on other identity management projects ongoing at UNISG (CRM, account management)
ICT – F&S

SWITCH EDU-ID
SWITCH edu-ID

GOALS & EXPECTATIONS

• **benefit** for ZHAW: usability, performance, management of overlapping roles etc.
• **impact** on users & processes, e.g., change of user id
• **coverage of the overall life-cycle** with the changing roles (e.g., applicant, staff, student, alumni)
• **efficiency** in relation to business processes and IT-infrastructure
• **realistic roadmap** for transition to SWITCH edu-ID
SWITCH edu-ID

PEOPLE

- IDM project leader
- IT head & team leader
- security officer
- business applications
- access management
- online registration project

Others: ZHAW responsible for communication inside of ZHAW and (if necessary) involvement of additional stakeholders

Nisanth
Muthukirushnasamy
SWITCH edu-ID

WORK & CHALLENGES

Work:
• Analyse current use of SWITCHaai
• Identify impact on existing processes/systems

Effort (so far):
preparation for workshops: 1 day
+ analysis of impact: 3 days
+ 2 workshops (6 people): 6 days

Challenges:
• Deeper understanding of internal IAM processes
• Identification of stakeholders
• Few adaptations on existing systems and processes
SWITCH edu-ID

BEST POSSIBLE INTEGRATION SCENARIO: MIXED

Onboarding
1. existing users (students & staff):
   Provisioning of edu-ID account by ZHAW for all people with SWITCHaai account
2. new students:
   via online registration (ONLA)
3. staff:
   via internal IdM with notification to edu-ID
   (→ new affiliation)

Offboarding (students & staff):
• Notifications (→ loss of affiliation)

Communication strategy
to grant deposit of private (primary) email address before leaving ZHAW
SWITCH edu-iD

1. Evaluate scenarios in detail
2. Elaborate planning for integration of SWITCH edu-ID
Show how to catch the worm (1)

Ask & answer questions:
- What can/should be improved?
- What are the requirements?
- How does the current system look like?
- What interfaces are provided?
- How should notifications be used?
- Which services need the extended model?
- How do on- and offboarding processes work?
- Which scenario(s) would fit best?
- Who has to be informed and how?
- What has to be developed?
- Is a contract necessary?
- Who will decide?
- ....
- ....
Show how to catch the worm (2)

Generic Documentation for next planning phases:

Guide with Checklists

A) …
B) ...
C) ...
D) ...
Roadmap & Next Steps

Petra Kauer-Ott
petra.kauer@switch.ch

Berne, 29.6.2017
Swiss edu-ID Deployment Step 1 in 2017

**Swissuniversities’ funding uncertainty:**
- No submission opportunity mid Aug 2017
- Future submission process under review
Swiss edu-ID Deployment 2017 - 2020

Phase II

Extension

Deployment Step 1

Functional Upgrade 1

Strategy Series A

Deployment Step 2

Functional Upgrade 2

Migration Series A

Strategy Series B

Deployment Step 3

Functional Upgrade 3

Migration Series B

Strategy Series C

Deployment Step 4

Functional Upgrade 4

Migration Series C

Strategy Series D

Swiss edu-ID Operation & Supporting Measures

2016 2017 2018 2019 2020
<table>
<thead>
<tr>
<th>Phase II</th>
<th>Extension</th>
<th>Deployment Step 1</th>
<th>Deployment Step 2</th>
<th>Deployment Step 3</th>
<th>Deployment Step 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Functional Upgrade 1</td>
<td>Strategy Series A</td>
<td>Functional Upgrade 2</td>
<td>Strategy Series B</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Migration Series A</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>Functional Upgrade 3</td>
<td>Strategy Series C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Migration Series B</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>Functional Upgrade 4</td>
<td>Strategy Series D</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Migration Series C</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Swiss edu-ID Operation &amp; Supporting Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
</tr>
</tbody>
</table>

Swiss edu-ID Deployment 2017 - 2020
How to continue?

Position of SWITCH:

• SWITCH is committed to continue along this roadmap (backed by strategy)
• SWITCH will recruit candidates for “Depl. Step 2” until end of Aug 2017
  – Kick-Off for recruitment today at the edu-ID Update Event

BFH ?
UNIBE ?
PHBern ?
ETHZ ?
UZH ?
UNILU ?
HSLU ?
USI ?
UNIBAS ?
Functional Upgrades – 2018 wishlist

• Migration support (account linking etc.)
• Notification handling (SCIM, processes etc.)
• OIDC – Provider (result of exchange with mobile app project)
• Eduroam integration (planned piloting)
• Interfederation
• De-duplication process for end-users (user-interface)
• Monitoring for end-users
• ….
Next Steps

- Continue migration planning with universities
- Migrate first organisation: SWITCH
- Recruit candidates for Deployment Step 2
- Plan Deployment Step 2 in detail
- Provide generic documentation and assist universities with their individual integration plans
- Add technical components for preferred integration scenarios
- Implement additional functionalities
  a) as planned &
  b) new customer requirements
Everything that’s necessary to reach the finish line together!
Deployment Step 1 –
Intermediate Conclusions
SWITCH edu-ID Info Day 2017

Christoph Graf
christoph.graf@switch.ch

29 June 2017, Berne
The early birds …

1. Work on their migration strategy

2. Show other birds how to “catch the worm”

EPFL, FHNW, UniFR, UniGE, Unil, UniSG, ZHAW
The “Meta-Directory” approach

Business Units

HR
- Employee mgt system

Student admin
- Student mgt system

Cont. Educ.
- Cont. educ. mgt system

??
- “All others” mgt systems

IT Services

“Meta” DB

User data flow

AAI IdP

edu-ID IdM

edu-ID IdP

SWITCH

© 2017 SWITCH | 3
The “Centralised provisioning” approach

Business Units

HR
- Employee mgt system

Student admin
- Student mgt system

Cont. Educ.
- Cont. educ. mgt system

??
- “All others” mgt systems

IT Services

“Meta” DB

Provisioning engine

AAI IdP

SWITCH

edu-ID IdM

edu-ID IdP

User data flow
The “Leading System” approach

Business Units

- HR
  - Employee mgt system

- Student admin
  - Student mgt system

- Cont. Educ.
  - Cont. educ. mgt system

IT Services

- Leading system
  - Provisioning engine
  - AAI IdP

SWITCH

- edu-ID IdM
- edu-ID IdP

User data flow
Supporting processes: “Meta-Directory”

Business Units

HR
Employee mgt system

Student admin
Student mgt system

Cont. Educ.
Cont. educ. mgt system

??
“All others” mgt systems

IT Services

“Meta” DB

SWITCH

edu-ID
IdM

Supporting processes
Challenges

Business Apps (e.g. finance, communication)
Supporting processes: “Centralised provisioning”

- **Business Units**
  - Employee mgt system
  - Student mgt system
  - Cont. educ. mgt system
  - “All others” mgt systems

- **IT Services**
  - “Meta” DB
  - Provisioning engine
  - Business Apps (e.g. finance, communication)

- **Switch**
  - edu-ID IdM

---

Supporting processes:

Challenges
Supporting processes: “Leading system”

IT Services

- Provisioning engine
- Leading system

Business Units

- HR
  - Employee mgt system
- Student admin
  - Student mgt system
- Cont. Educ.
  - Cont. educ. mgt system

SWITCH

- edu-ID IdM

Business Apps

- Business Apps (e.g. finance, communication)

Supporting processes:

Challenges
Generic adoption scenarios

- Proposed adoption scenarios adapted to identity management ripeness
- Does not replace individual adaptation and planning efforts
### Identity Management Evolution

#### Meta-Directory
- Decentralised user management
- Basic support to business applications
- Crisscross processes between business applications and leading systems
- Role-scoped user management
- Limited benefit of new SWITCH edu-ID features

#### Provisioning System
- Decentralised user management
- Single point of contact to business applications
- Streamlined processes between business applications and provisioning system
- Role-scoped user management
- Limited benefit of new SWITCH edu-ID features

#### Leading System
- Centralised core user management
- Single point of contact to business applications
- Streamlined processes between business applications and provisioning system
- User-centric user management
- Full benefit of new SWITCH edu-ID features

- Improved agility and support for business applications
- Stronger role of the IT department as integration orchestrator
And an element of future-proof-ness

More: https://www.switch.ch/edu-id/
Blog: identityblog.switch.ch
Service: eduid.ch
Website: switch.ch/edu-id
Stories: switch.ch/stories/
Event: Workshops 2017
      ICT Focus 27./28.11.
SWITCH – an integral part of the Swiss academic community since 1987.

www.switch.ch/30years