Our core beliefs

Together for greater capability, convenience and security in the digital world.
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
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
Trust & Identity

Thomas Bärecke
Thomas.Baerecke@switch.ch

Swiss edu-ID update event
27.06.2018 Bern
Trust & Identity

- Your Added Value
- Our Customers
- Our Offer
Your added value

The universal and secure key

• Lifelong universal and safe access to services in the academic community

• Universal identity for everyone related to the academic world

• Uniform solution for all users and services

• High security

• Internationally compatible through cooperation with GÉANT

• Governance ensured through universities

• Expandable architecture
Our customers

Higher education
• Cantonal universities
• ETH/EPF domain with research institutions
• Universities of applied sciences
• Universities of teacher education

University-related organizations
• University hospitals
• Private educational institutions
• Coordination offices

Federation Partner
• Publishing houses
• Training opportunities
• Alumni organizations
Our offer

Universal and secure identity

- SWITCH edu-ID / SWITCHaai
- SWITCHpki
- AP-Hosting / IdP-Hosting
- Federation Partner
- Interfederation (GÉANT eduGAIN)
- PKI-Certificate with selectable quality level
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
- 1330 service provider, 113 federation partners

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
Customer tailored SSL-certificates

SWITCHpki delivers customer tailored SSL-certificates for servers and users

Customers

• Universities
• University related organizations

Services

• OV-/EV certificates
• Purchase options retail or bulk (500+)

Your benefits

• Rapid ordering process
• Customer tailored certificates
SWITCH edu-ID for Beginners

Thomas Bärecke
Thomas.baerecke@switch.ch

Swiss edu-ID update event
27.06.2018 Bern
Identity management

Identity management

users

organisations

services
The foundation: SWITCHaai

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

Special Home Organizations

# Resources

# Home Organizations

99.9 % coverage in higher education

© 2018 SWITCH | 4
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
- Post-graduate
- Employment
- Further education
- Self-Employment

© 2018 SWITCH | 7
Tidying up

Swiss edu-ID

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

© 2018 SWITCH
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

SWITCH edu-ID

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
- 2018
- 2017
- 2016

- Mobile/non-web
- National licenses
- WITCH drive
- CH/EU eID
- SwissID
- Educa.ch

- MFA
- LoA

- SLSP/Libraries
- SWITCH engines
- Federal consultation 2017
- Regular contacts

- Regular contacts
- Edu-ID university
- Edu-ID university
- Edu-ID university
**“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

- **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
  - study branch
  - 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>
</table>
| linked              | • “nothing”!  
                      • Communication measures                                            | naked Swiss edu-ID                                                                          |
|                     |                                                                      | edu-ID with affiliations and assurance levels                                               |
| integrated          | • Migrate all users to edu-ID  
                      • Manage Swiss edu-ID identifier in internal directory  
                      • Operate attribute provider                                                | • No local SAML-IdP required anymore  
                      • More efficient user identity initialization  
                      • Access to SPs with new Protocols  
                      • New Auth methods                                                      |
| deeper integration  | • Receive and process IdM updates from Swiss edu-ID  
                      • Notify Swiss edu-ID of IdM updates                                       | • Streamlined IdM processes  
                      • up-to-date identities  
                      - locally  
                      - in entire community                                                   |
Swiss edu-ID, SWITCH edu-ID and the eID landscape
What’s new @ SWITCH Q2/18

- **Community Service Hub**
  POC was completed end of February
  swit.ch/csh, sebastian.sigloch@switch.ch

- **FUTURE UNIVERSITY**
  Think Tank SWITCH in partnership with W.I.R.E
  christine.lanner@switch.ch

- **Coordination office on scientific information**
  Conceptional work together with swissuniversities
  andreas.dudler@switch.ch

- **Procurement**
  Adobe Framework Agreement and Microsoft Data Processing Amendment (DPA) signed
  procurement@switch.ch

- **SLSP @ SWITCH**
  Subtenants from 1 March 2018 at SWITCH premises
  christine.lanner@switch.ch
What's new @ SWITCH Q2/18

Security
- **SWITCH-CERT**
  - Mattermost, a secure chat for NREN
cert@switch.ch

- **Malware / Phishing**
  - New contact
  spamreport@post.switch.ch
  spamanalysis@post.switch.ch

Network
- **Big Data Transfer Community**
  - Interdisciplinary network and security workshop
together with higher education
daniel.bertolo@switch.ch
  silvio.oertli@switch.ch
  martin.leuthold@switch.ch

- **IoT Working Group**
  - Interdisciplinary (researchers, network, security)
  community together with higher education
  kurt.baumann@switch.ch, daniel.bertolo@switch.ch

Trust & Identity
- **SWITCH edu-ID**
  - Deployment step 2
  christoph.graf@switch.ch
  
  - Swiss edu-ID Update Event 2018, 27 June, Berne
  switch.ch/edu-id/events/update-event-2018/
  
  - Read our Blog
  identityblog.switch.ch

Infrastructure & Data Services
- **SWITCHengines**
  - are now qualified for SNF and Innosuisse funding
  
  - storage and data solutions started with universities

  - P-5 long term storage project submitted
  konrad.jaggi@switch.ch, switch.ch/engines
Targets of the project stream Swiss edu-ID

1. Modernising identity management at Swiss universities
   - For lifelong learners, designed for long-term use
   - Open to all relevant stakeholder groups
   - Interoperable with national and international initiatives and services

2. Implementing the identity hub SWITCH edu-ID
   - Operated by SWITCH for the research and education sector under the governance of the Swiss universities
   - Evolutionary extending the well-established SWITCHaai

3. Accompanied implementation at universities
Targets of the project stream Swiss edu-ID

1. Modernising identity management at Swiss universities
   • For lifelong learners, designed for long-term use
   • Open to all relevant stakeholder groups
   • Interoperable with national and international initiatives and services

2. Implementing the identity hub SWITCH edu-ID
   • Operated by SWITCH for the research and education sector under the governance of the Swiss universities
   • Evolutionary extending the well-established SWITCHaai

3. Accompanied implementation at universities

4. Block 1: edu-ID in the eID landscape
   Block 4: Microsoft integration concept & demo

5. Block 2: features and technical roadmap

6. Block 3: project roadmap and status
Supporting global research collaboration

Cross-sectoral collaboration (evtl. also e-ID functions)

Project FIDES of EDK/CDIP

Supporting the design and implementation of the identity federation of the Swiss schools
AAI-enabling only «half-way» done:
- often implemented for *shared* Web-Resources
- usually not implemented for LDAP/AD-integrated *local* resources

Why does this matter?...
Block 4: Microsoft integration concept & demo

AD/LDAP connected services:
→ edu-ID ready?
  We’ll look into this…

AAI/edu-ID enabled service:
Ready for external authentication
→ edu-ID ready
SWITCH edu-ID's contribution to the future of Swiss universities

Future University
The Future University Think Thank is an initiative of SWITCH in partnership with WIRE to proactively monitor long-term developments in the Swiss education and research landscape and to provide strategic support for decision-makers. The first published study gave rise to 10 theses.

Three of these approaches are particularly relevant for identity management. SWITCH edu-ID offers solutions for the following driving forces…
<table>
<thead>
<tr>
<th>Future drivers for the universities</th>
<th>Role of SWITCH edu-ID</th>
</tr>
</thead>
</table>
| **THE END OF THE MASS LECTURE HALL** | • SWITCH edu-ID connects the analogue with the digital identity  
   • Based on the existing trust relationship  
   • Interworking with SwissSign/SwissID |
| **LIFE LONG LEARNING** | • SWITCH edu-ID is the user-centric, long-lived identity of Switzerland's education and research landscape  
   • Networked with the future identity solution of schools in Switzerland (FIDES project) |
| **UNIVERSITIES AS ECOSYSTEMS** | • SWITCH edu-ID is the cross-university identity of all players in Swiss higher education  
   • Internationally networked via GÉANT (EU project) |

See handout «Future University»
edu-ID Technical Upgrades

Lukas Hämmerle
lukas.haemmerle@switch.ch

Bern, 27. June 2018
Overview

New technical features:
1. Affiliation Chooser
2. Single Logout
3. User-Driven Deduplication

Also new, but covered in this presentation:
• REST/JSON APIs
• Usability improvements
• Custom Views
• Password Checking
• …
1. Affiliation Chooser

- **Goal**: Backwards compatible attributes for edu-ID users with multiple affiliations
- User chooses his affiliation/role in which he connects to SP
  - I.e. private identity or organizational identity
- Step between login and attribute release consent
  - Shown only when needed. Depends on SP and available affiliations
- Available only to users of migrated organisations
Affiliation Chooser Screenshot

Attributes:
homeOrg: switch.ch
affiliation: staff
uniqueID: 2348u32@switch.ch

Attributes:
homeOrg: eduid.ch
Affiliation: affiliate
uniqueID: 23489cdh4e@eduid.ch
2. Single Logout

- Single Login is relatively easy, single logout (SLO) is hard
- Web applications might need to be adapted for SLO
SLO at edu-ID IdP

- edu-ID IdP supports Single Logout
  - Has been enabled for several months
- Logout initiated at the SWITCH edu-ID My Account web application for all scenarios:

  ... or on a Service Provider that supports logout
If SLO is supported on SPs
Requirements to support SL

- SP needs to add SLO URLs in Resource Registry
- Web application might need to be adapted to clear its session
- Requires SP session ID to be stored in application session
Affiliation Chooser and SLO Demo

1. Login on Resource Registry
   • Choosing SWITCH staff as IdP
2. Login on AAI Attribute Viewer
   • Choosing edu-ID IdP and edu-ID private affiliation
   • Notice the Single Sign On
3. Login on edu-ID ”My Account”
4. Logout from ”My Account” and other two SPs
   • Sends logout request to AAI Attribute Viewer and Resource Registry
5. Check if still logged in in AAI Viewer
   • Should not be the case

This works only for users of migrated organisations!
3. User-Drive Deduplication

Situation

- Duplicate account = same user has > 1 edu-ID accounts
- Duplicate accounts are bad
- Duplicate accounts cannot be 100% prevented
  More on https://identityblog.switch.ch/2018/06/15/clone-wars/
- Duplicate accounts are sometimes useful for developers
Account Creation Recapitulation

Minimum data to create edu-ID account:

- First name - Not unique
- Last name - Not unique
- Verified E-mail address - Unique, but user often has many

Name is not unique and e-mails addresses are cheap!
Counter-Duplicate Strategy

1. **Try to prevent** as many duplicates as possible
   - I.e. based on cookie and unique data

2. **Identify** duplicate accounts and allow users to **merge** them
   - Based on unique data (AAI, ORCID, e-mail, mobile number, …)
   - Automated account merge process

3. **Introduce** ”official” system/test/technical accounts
   - Organisations will be able to create their own technical accounts

4. **Merge accounts on our own in compliance with Terms of Use**
   - Currently not done regularly
Identifying Duplicates

- Adding or linking already associated unique values
- User also receives information on duplicates by email
Reminder to Deduplicate Accounts

• Reminder sent 2 weeks later if accounts were not merged
Account Merge by User: Step 1

You can merge multiple duplicate SWITCH edu-ID accounts on the following pages. When merging two accounts, information from the duplicate account to be removed will be added to the remaining account where this is possible and reasonable. The duplicate account will then be removed.

To start the process, please first provide e-mail address and password of your other account.

**This account**

- **E-mail Address**: elisabeth.muster@hepl.ch

**Other account**

- **E-mail Address**: elisabeth.muster@unige.ch
- **Password**: *******

Forgot password?

How much is: 15 + 16 + 5 =

- **Result**: 36

Cancel Reset Proceed
Account Merge by User: Step 2

Please select which account you would like to keep. Identity data from the other account will then be merged into the remaining account where possible.

First Name Elisabeth
Last Name Muster
E-mail Address elisabeth.muster@hepl.ch
Account creation date 3. 5. 2017 15:58:19
Last login date 5. 6. 2018 08:59:37
Accessed services 10
Linked active identities 2

Choose account to keep

First Name Elisabeth
Last Name Muster
E-mail Address Elisabeth.Muster@unil.ch
Account creation date 19. 11. 2014 11:48:31
Last login date 26. 3. 2018 15:11:25
Accessed services 0
Linked active identities 1

Keep this account
(This is the recommended choice)

Cancel
Proceed
Account Merge by User: Step 3

Please select which account you would like to keep. Identity data from the other account will then be merged into the remaining account where possible.

First Name Elisabeth
Last Name Muster
E-mail Address elisabeth.muster@hepl.ch
Account creation date 3. 5. 2017 15:58:19
Last login date 5. 6. 2018 08:59:37
Accessed services 10
Linked active identities 2

This account will remain

First Name Elisabeth
Last Name Muster
E-mail Address Elisabeth.Muster@unil.ch
Account creation date 19. 11. 2014 11:48:31
Last login date 26. 3. 2018 15:11:25
Accessed services 0
Linked active identities 1

This account will be removed.

Please read before you continue

Merging duplicate accounts is generally recommended to avoid access problems in the future. Merging accounts has the following consequences that you should be aware of before continuing:

- The password of the account to be removed will not be transferred to the remaining account. The password for the remaining account that stays the same.
- User settings and content of some services (e.g. SWITCHdrive) that were accessed with the account to be removed might not be available for some time directly after the account is merged. This is because the operators of the respective services might first need to transfer user settings and content to the account that remains. When the account is merged, SWITCH will inform the operators of the affected services and ask them to apply the necessary changes in a timely manner.

Cancel  Merge accounts
Account Merge by User: Result

Successful Account Merge

The account merging operation was successful. The details were also sent to your primary e-Mail address elisabeth.muster@hepl.ch. Please review your account data to see if your identity data still is correct and up-to-date after the account merging.

View Account Details
Merging Information to User

Mail to user includes:

- Merge code as reference
- Main data changes
- Hint that access to some services might not work till service admins apply some changes (update identifier values of merged account)

```
Chère/Cher Elisabeth Muster

Nous vous informons que deux de vos comptes utilisateurs SWITCH edu-ID viennent d’être fusionnés.

Pour votre compte encore existant, vous avez utilisé l’adresse e-mail:
  elisabeth.muster@epfl.ch
Le mot de passe pour ce compte reste le même, il n’a pas été affecté par la fusion.

Pour votre compte maintenant supprimé, vous avez utilisé l’adresse e-mail:
  Elisabeth.Muster@unil.ch

Le cas échéant, les informations d’identité du compte maintenant supprimé ont été transférées sur votre compte encore existant. En particulier:

* Adresse e-mail supplémentaire:
  elisabeth.muster@gmail.com
  Elisabeth.Muster@unil.ch

Les comptes utilisateurs ont été fusionnés par l’équipe de support SWITCH edu-ID avec le commentaire suivant:
“Account merge performed by end-user”

Vous pouvez consulter toutes les données de votre compte utilisateur SWITCH edu-ID sous ‘Mon compte’ à l’adresse: https://macib.switch.ch
Veuillez mentionner le code #180605D3F9 pour toute communication avec SWITCH edu-ID ou les fournisseurs de services dans le cadre de cette fusion de compte.

Si vous avez des questions ou si vous avez besoin d’aide, veuillez contacter l’équipe de support SWITCH edu-ID via swizeduID@switch.ch ou +41 44 268 15 89.

Bien cordialement,
Équipe SWITCH edu-ID

___

SWITCH edu-ID is a service of SWITCH
SWITCH, Weredstrasse 2, P.O. Box, 8021 Zurich, Switzerland
https://projects.switch.ch/eduID/ swizeduID@switch.ch
```
Merging Information to SP admins

Mail to SP admins of those SPs that are affected by merge contains:

• Merge code as reference
• Link to a receipt including the values that changed for user
• Technical contact(s) of SP is informed when merge happens
Account Merge Receipt

Merge Receipt for SP:

• Merge code as reference
• Link is valid 3 months
• Includes actual changes that should be applied
• Only attributes shown which are relevant for this SP (identifier attributes, i.e. uniqueID, mail, Swiss edu-ID, …)
• Instructions shown for SP admin what is recommended to do

Receipt Content

Receipt created on: 25. 5. 2018 13:05:15.

The SWITCH edu-ID user described below had two duplicate accounts. These two accounts were merged into one account and the duplicate account was removed. The removed duplicate account was used on the Service Provider "LH demo and development service" with entityID https://maclh.switch.ch/shibboleth.

There may be steps required on the SP’s side to reflect this account merge. Please review the following changes that results from the account merge.

Merging Code

------------
#180525624A

User Details

* Name: Elisabeth Muster
* Email: Elisabeth.Muster@unil.ch

Identifier Attribute Changes

The following attributes requested by the SP https://maclh.switch.ch/shibboleth are affected by this account merge:

* swissSeduPersonUniqueID:
  Now archived: 557191071261@test.eduid.ch
  Still existing: 72600657562@test.eduid.ch

* mail:
  Now archived: Elisabeth.Muster@unil.ch
  Still existing: elisabeth.muster@hep1.ch

* edupersonPrincipalName:
  Now archived: 557191071261@test.eduid.ch
  Still existing: 72600657562@test.eduid.ch

* swissSeduID:
  Now archived: 00000000-21d8-4bab-8fee-242ac92c3de8
  Still existing: 00000000-4ed8-4391-849c-0f5625597174
Summary

1. Affiliation Chooser
   • For now only relevant for migrated organisations

2. Single Logout
   • Requires SP to publish SLO URLs and maybe changes in web app

3. User-Driven Deduplication
   • Users can deduplicate accounts on their own with as few side effects as possible
Swiss edu-ID Deployment Step 1: Short project review
«Swiss edu-ID Step 1» work packages

• Migration strategy work packages for:
  – UniFR, UniGE, Unil, UniSG, EPFL, FHNW, ZHAW

• Functional upgrade work packages in a nutshell:
  – Support for use of AHVN13
  – Privacy and data security
  – Uniqueness
  – Credential management
  – Group management

• Project management, communication and outreach
  – Liaisons, pilots and usability tests
Functional upgrade work packages in a nutshell

• Support for use of AHVN13
  – Limited benefit due to the lack of corresponding interfaces at BFS/OFS
  – No «AHVN13» attribute at this time, developments to be observed

• Privacy and data security
  – Analysis of edu-ID adoption scenario carried out, no show-stoppers identified
  – awaiting final feedback from federal data protection officer (pending for 3 years, with lots of nagging)

• Uniqueness
  – User-driven de-duplication process implemented and in production now

• Credential management

• Group management
  – A light version of group management ("complementary attributes") could be implemented by generalising a custom solution for the "National licenses" service; now in use at multiple libraries
  – Many contacts to research teams (CSCS, SIB, SDSC, SPHN, etc.), but no convincing use cases for a more generic group management service identified yet
Liaisons

• FIDES / Identity federation of Swiss schools
  – EDK/CDIP project mandated to educa.ch
  – Participation of SWITCH under discussion with EDK/CDIP

• SwissID
  – Informal contact established with SwissSign, several workshops held
  – Promising use cases identified: “easy onboarding”, services sharing, E-ID functions

• «Swiss edu-ID Mobile APP» project of HTW Chur
  – Three mobile use cases identified, demonstrator implemented
  – Integration of OIDC provider on SWITCH edu-ID on roadmap
Pilots and usability tests

• Student registration with evento
  – Implemented by crealogix, piloted by FHNW and ZHdK
  – Now a standard extension (ONLA) to the evento distribution in use by a growing number of sites

• MFA (multifactor authentication)
  – MFA pilot implementation supported by SWITCH, in production at UniGE
  – Adapting to SWITCH edu-ID environment planned autumn 2018

• Usability tests mandated by swissuniversities
  – Heuristic evaluation (HTW Chur) & test scenarios with users (HESGE)
  – Feedback was quite positive, many recommendations were given
  – Most could be implemented to optimise the overall experience
Technical Roadmap

Thomas Lenggenhager
thomas.lenggenhager@switch.ch
edu-ID Update Event, 27.6.2018, Berne
Overview

• Principles for feature prioritisation

• Technical Features planned for the next quarters
  • Microsoft Integration
  • Group Management
Principles for Feature Prioritisation

• List of functional upgrades according to the *Deployment Step 2.2* application
• Requirements of SWITCH Community members adopting edu-ID
• Use case driven
• ‘Minimum viable product’ first
  • followed by stepwise refinements
Technical Features planned (1/3)

• Technical Accounts 3Q2018
• Attribute Aggregation 3Q2018
  • via LDAP or PostgreSQL 3Q2018
• Offboarding and Former Affiliations 4Q2018
• Two-Factor Authentication 4Q2018
• OpenID Connect (OIDC) Provider 1Q2019
Technical Features planned (2/3)

Microsoft-Integration

- Solution Concept 3Q2018
- Proof of Concept (PoC) 4Q2018
- PoC Analysis 1Q2019
- Specification, Implementation 1Q2019
- Step-wise deployment starts 3Q2019
Technical Features planned (3/3)

Group Management

• Use Case Analysis & Pilot Recommendations 3Q2018
  • integration of group management for SWITCH services in edu-ID
  • generic group management
  • integration of external group management

• Solution Concept for the three use cases 4Q2018
• Definition of Service Environment 4Q2018
SWITCH edu-ID
Project Roadmap

Petra Kauer-Ott
petra.kauer@switch.ch
edu-ID Update Event
27.6.2018, Berne
Project roadmap 2014-2020

Development

Swiss edu-ID Phase 1
Swiss edu-ID Phase 2

Functional Upgrades

Adoption

Depl. Step 1  Depl. Step 2  Depl. Step 3  Depl. Step 4
Entry Points - Planning

Swiss edu-ID Phase 1
Swiss edu-ID Phase 2

Development

Functional Upgrades

Depl. Step 1
Depl. Step 2
Depl. Step 3
Depl. Step 4

Adoption
Entry Points - Reality

Development

Swiss edu-ID Phase 1  Swiss edu-ID Phase 2

Functional Upgrades

Adoption

Depl. Step 1
without funding
Depl. Step 2.1
Depl. Step 2.2
Depl. Step 3 & 4

© 2018 SWITCH | 4
Idea: Entry Points for Sub-Projects

**Development**

- Swiss edu-ID Phase 1
- Swiss edu-ID Phase 2
- Functional Upgrades

**Adoption**

- Depl. Step 1
- No funding
- Depl. Step 2.1
- Depl. Step 2.2
- Depl. Step 3 & 4

with sub-projects
Project & Sub-Project Submissions

• Last project entry for SWITCH 19.8.2018 *, including generalized effort for
  – planning & adoption
  – functional upgrades

• SWITCH manages sub-projects* for 2019 and 2020. Foreseen submission dates:
  – 30.11.18 (start January 2019) (subject to approval)
  – 31.5.2019 (start July 2019)
  – 30.11.2019 (start January 2020)
  – 31.3.2020 (if there is still funding available; start May 2020)

→ Declaration of participants and planned functional upgrades towards swissuniversities
→ Reporting end of 2019 and end of 2020 (status information every 6 months)

* not yet confirmed by swissuniversities
Advantages

• less administrative work
• different entry points with short forerun
• overall budget and planning horizon for 2 years

Possibility to submit
a) one sub-project (planning & adoption in one step)
b) two sub-projects (planning, adoption later)

Funding per organisation ca.
• 1 PM planning
• 3 PM adoption
  Total 3 - 4 PM for planning & adoption
Next Steps

• July
  – Approval for Depl. Step 2.2 (we hope so)
  – Outline by swissuniversities for project submission

• 19. August
  – Submission of project Depl. Steps 3/4

• 30. November
  – Submission of sub-projects

• August until end of year
  – Workshops with planning organisations (Depl. 2.2)
  – First university adoptions
  – Elaborate detailed specifications for further adopting organisations
  – Preparatory meetings with organisations without plans so far

Use the form we will provide on our web page
No need for funding?

GO!

Start planning at any time (in agreement with SWITCH)
SWITCH edu-ID
Status at Organisations & Adoption Scenarios

Petra Kauer-Ott
petra.kauer@switch.ch
edu-ID Update Event
27.6.2018, Berne
The 7 early birds

• contributed to define **requirements** and to elaborate **scenarios**

• triggered development of **components** useful for all organisations (APIs, administrative interface, technical accounts etc.)

• could plan with a long lead time (influence on IdM redesign, relation to student portal etc.)
First “jumpers” integrating SWITCH edu-ID

2017: SWITCH

2018: UNILU, PHZUG, FernUni

2018/19: UNIL, UNISG, ZHAW, .. HSLU, PHSZ, …

2019: UNIFR, FHNW, …

(to be confirmed)
Adopting edu-ID at SWITCH

- Involved parties at the Organization
  - Human resources 1d
  - IdM/Account management 3-4d
  - Support 1d
  - Communication 1d
- Everything went smoothly
Who is on the way?

2017
Planning: 7
Adoption: 1

2018
Planning: 12
Adoption: 3-4

2019
Planning: ?
Adoption: 3-6

2020
Planning: ?
Adoption: ?
Project Deployment Steps

- **Depl. 1 (2017/18)**
  - Planning: early birds EPFL, UNIFR, UNIGE, UNIL, UNISG, FHNW, ZHAW

- **Depl. 2.1 (2018)**
  - Planning & Adoption: UNILU, FernUni, PHZG

- **Depl. 2.2 (2018/19)**
  - Planning: UNIBE, UNINE, BFH, FHSOG, HES-SO, HSLU, HTWChur, HWZ, NTB, ZHdK, PHBern, PHSchwyz
  - Adoption: UNIL, UNISG, ZHAW

- **Depl. 3/4 (2019/20)** (not confirmed yet)
  - Planning: FFHS, HSR, PHZH, your organisation?
  - Adoption: UNIFR, FHNW, your organisation?

Compare [https://projects.switch.ch/eduid/adoption/](https://projects.switch.ch/eduid/adoption/)
Planning Activities (Workshops)

1. Involve stakeholders
   (decide who to involve for input, acceptance, planning & support)
2. Define user base (students, staff, continuing education, guests, etc.)
3. Formulate institutional goals and expected benefit
4. Analyse relevant IdM processes (as on- and offboarding)
5. Describe migration scenarios for different user groups
6. Write project plan for adoption
   (duration, resources, development tasks, communication etc.)

→ Result: usually internal project application

https://projects.switch.ch/eduid/adoption/step1-concept/
Stakeholders (Planning)

Leading “actors”
- Central IT
- Service Providers
- Management
- Students
- Teachers
- Researchers

Additionally involved
- Registration Office
- Certification Office
- HR
- Continuing Education
- Library
- Career Services
- Alumni
- Support
- Administration
- Communication Dept.
- Legal Office
- Security Office
- Facility Management

External Parties
- Headhunters
- Job Markets
- Companies (HR)
- Content (Platform) Providers
- Publishers
- Social Networks
Stakeholders (Implementation)

Leading “actors”
- Central IT
- Service Providers
- Management
- Students
- Teachers
- Researchers
- Registration Office
- Certification Office
- HR
- Continuing Education
- Library
- Career Services
- Alumni
- Support
- Administration
- Communication Dept.
- Legal Office
- Security Office
- Facility Management

Additionally involved

External Parties
- Headhunters
- Job Markets
- Companies (HR)
- Content (Platform) Providers
- Publishers
- Social Networks
Prepare Communication

• part of planning
• work during adoption phase

Currently communication guide under revision by UNILU
Evaluate Linking Options

Understand options and choose appropriate for different user groups as students and staff:

<table>
<thead>
<tr>
<th>New members</th>
<th>Current members</th>
</tr>
</thead>
<tbody>
<tr>
<td>at Registration</td>
<td>before Day X</td>
</tr>
<tr>
<td>at Admission</td>
<td>at Day X</td>
</tr>
<tr>
<td>after Admission</td>
<td>after Day X</td>
</tr>
</tbody>
</table>

(Possible combinations like start with "before Day X" and continue with “at Day X” for tardy users)

https://projects.switch.ch/eduid/adoption/linking-methods/
## Different Linking Options

<table>
<thead>
<tr>
<th>New members</th>
<th>Current members</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>at Registration</strong>&lt;br&gt;adapt registration application; organisation knows identifier and releases affiliation later</td>
<td><strong>before Day X</strong>&lt;br&gt;linking by users (with AAI or organisational account)</td>
</tr>
<tr>
<td><strong>at Admission</strong>&lt;br&gt;registration not touched; when organisational account is created</td>
<td><strong>at Day X</strong>&lt;br&gt;edu-ID created for users not having already one (→ risk of duplicates)</td>
</tr>
<tr>
<td><strong>after Admission</strong>&lt;br&gt;on demand</td>
<td><strong>after Day X</strong>&lt;br&gt;users without linked edu-ID loose access&lt;br&gt;→ linking by users with organisational account</td>
</tr>
</tbody>
</table>

(Possible combinations like start with "before Day X" and continue with “at Day X” for tardy users)

[https://projects.switch.ch/eduid/adoption/linking-methods/](https://projects.switch.ch/eduid/adoption/linking-methods/)
## Define your Scenario

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UNILU</td>
<td>at Admission, before day X, Org-Push</td>
<td>after Admission, edu-ID Linking service, Org-Push</td>
<td></td>
<td></td>
<td>Admin interface</td>
</tr>
<tr>
<td>UNIL</td>
<td>at Admission, before day X, Org-Push</td>
<td>at Admission, before day X, Org-Push</td>
<td></td>
<td></td>
<td>API</td>
</tr>
<tr>
<td>UNISG</td>
<td>after Admission, before day X</td>
<td>after Admission</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZHAW</td>
<td>at Admission, at day X, Org-Push</td>
<td>at Admission, at day X, Org-Push</td>
<td>via ONLA or IdM triggering, at day X, Org-Push</td>
<td>current members: new registration; new members: no linking, entitlement attribute</td>
<td></td>
</tr>
</tbody>
</table>
Experiences from Workshops

Planning effort
• ca. 10-20 days
• decreasing
• depending on university size and complexity of IdM processes

Complexity higher when
• IdM redesign in progress
• No central system in place
• Large organisation
• Deeper integration

→ There’s a suitable way for each organisation!
Recommendations

• Start **planning early**
  → more time for implementation

• Start **registration not too early** & not without prior planning
  → ensure linking is done

• Inform & **involve the right people**
  → ensure backing & contribution
Technical Questions

- Some information available on https://www.switch.ch/edu-id/support/

- As description of APIs
  Features: handling of affiliations, entitlements and memberships, check if email is associated with an edu-ID; update fields (like last login time), trigger attribute queries etc.

→ Use planning project or contact directly our team in case of questions

Some parts under development – further functions might be implemented (depending on needs of universities)
Legal Questions

• Feedback from cantonal officers (ZH, LU, FR)
• No answer by federal data protection officer

**Body of arguments** currently under progress
→ publication in July
See you soon!

→ 30.11.18 next possibility to start planning with funding
SWITCH edu-ID / Microsoft integration concept & demo

Christoph Graf
Christoph.graf@switch.ch
edu-ID Update Event, 27.6.2018, Berne
AAI-enabling only «half-way» done:
- often implemented for *shared* Web-Resources
- usually not implemented for LDAP/AD-integrated *local* resources

Why does this matter?...
University

AD/LDAP connected services: 
→ edu-ID ready?
Now, we look into this…
With AD connected services in focus

AAI/edu-ID enabled service: 
Ready for external authentication 
→ edu-ID ready
Typical service types

Microsoft cloud services
- O365 (web, fat client)
- Azure

«modern» on-prem services
- With federated login (AAI, ADFS)

«legacy» on-prem services
- Basic
- NTLM
- Kerberos
- Own userstore

AAD = Azure AD

© 2018 SWITCH | 4
Scenario A: Cloud only

• SWITCH (productive environment):
  – Already adopted edu-ID
  – Own tenant with O365 licenced
  – No local AD, only AAD (Azure AD)

• Demo use case
  – SWITCH employee logs into O365 with edu-ID (Demo 1)
Scenario B: Hybrid case

• Uni Demo (demo set-up):
  – Already adopted edu-ID
  – Own tenant with O365 licenced
  – Populated local AD, synced with AAD Connect (no credentials in AAD)

• Demo use cases:
  – Uni Demo staff or student log into O365 with edu-ID
    (Web & Fat Client: Demo 2)
  – Uni Demo staff or student access on-prem «legacy» service (Demo 3)
Demo 1: O365 for SWITCH employees

0. User provisioning with scripts to AAD

1. Access attempt (unauthenticated)

2. Home realm discovery (WAYF)

3. Authentication

4. Service access (authenticated)

User

Admin

Office 365

Azure AD

SWITCH edu-ID (production federation)

Organisation SWITCH (edu-ID adopted)

Microsoft Cloud
Demo 2: O365 for Uni Demo

1. Access attempt (unauthenticated)
2. Home realm discovery (WAYF)
3. Authentication
4. Service access (authenticated)

Azure AD

Microsoft Cloud

Office 365

Organisation Uni Demo (edu-ID adopted)

User

Admin

© 2018 SWITCH | 8
Demo 3: «legacy» on-prem service (Kerberos)

Office 365

SWITCH edu-ID

SWITCH edu-ID (test federation)

Azure AD

Microsoft Cloud

Organisation Uni Demo (edu-ID adopted)

User

Service access

Local authentication

«legacy» on-prem service
SWITCH edu-ID/MS integration concept

Your service login
• Longlived, cross-organisational, user-centric, SSO…
• Use it, whenever this window appears (and only then)
• Requirements:
  – Organisation performed edu-ID-adoption
  – AAD: Custom-domain with edu-ID authentication configuration

When relevant:

Your local machine login
• Issued by your organisation (typ. together with machine)
• SWITCH edu-ID will offer windows integrated authentication (SPNEGO provided by edu-ID) for domain-joined clients
Summary

• Access to Microsoft cloud services (O365, Azure) for your organisation (tenant) with SWITCH edu-ID
• Harmonized login experience (AAI, Azure and Azure-connected services)
• Integrating the SAML and Azure «worlds» into the SWITCH edu-ID ecosystem
• Seamless SSO (with windows integrated login)
• SWITCH has built expertise (workshops, consultant, trainings)
Next steps

• Validation of integration concept with specialists from our community
  – If interested to contribute, please contact eduid@switch.ch

• Integration of AD-connected service will be added to future edu-id planning projects
  – and reassessed, where needed