Swiss 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!)

• 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
Questions from the Community

- Persistency?
- Centralisation of IdM?
- Will the investment pay off?
- Role of organisations?
- Openness?
- User centrisim?
- One digital ID for everything?
Persistency

• One academic ID for a lifetime?
• Will people remember / re-use / maintain their ID?

➔ Yes, if the ID is useful
➔ It will depend on
  • Services offered by universities their alumni and non-academic users
  • Regularity of the usage of the SWITCH edu-ID
  • Services offered for academic community
Centralization of the IdM

- Data protection issues?
- Single point of failure? Reliability?
- Loss of control for universities?

➔ It is only a partial centralization
➔ SWITCH has experience in running critical infrastructure
➔ Universities keep a major role in the federation
The Role of Organizations

• Data protection issues?
• Single point of failure? Reliability?
• Loss of control for universities?

➔ It is only a partial centralization
➔ SWITCH has experience in running critical infrastructure
➔ Universities keep a major role in the federation
## Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Registration Administrator at Participant</td>
<td>Confirms/rejects Service Providers from own organisation</td>
</tr>
<tr>
<td>Service Registration Administrator at Operator</td>
<td>Confirms/rejects Service Providers from Federation Partners without Attribute Provider</td>
</tr>
<tr>
<td>Service Administrator</td>
<td>Registers and updates Service Provider descriptions in Federation Registry</td>
</tr>
<tr>
<td>Attribute Release Administrator</td>
<td>Defines attribute release policy for all Service Providers</td>
</tr>
<tr>
<td>IdM Administrator</td>
<td>Handles IdM updates</td>
</tr>
<tr>
<td>Participant IdM Administrator</td>
<td>Signs federation partner agreement</td>
</tr>
</tbody>
</table>
Openness and User Centrism

- Really? Anyone can have an SWITCH edu-ID?
- Doe we know the users?
- Can we trust the users?
Openness: “Not anyone should have a Swiss edu-ID”

- because

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

- because

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

misconception

Sharing attributes makes SPs more efficient

but

Not all SPs need high quality attributes

attribute

quality

tradeoff

low entrance barrier

Counterexample: ID / Passport

Counterexample: Github-ID

because

because
Swiss 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
Will the Investment pay off?

• Is SWITCHaai not sufficient?
One Digital ID for Everything

• Local accounts will not go away
• Personal master data is managed in multiple locations

➔ How can edu-ID help simplifying master data management?
➔ SWITCH edu-ID can serve as ID provisioning hub
Basic Components of Swiss edu-ID

Swiss edu-ID Participant
- Organisational IdM
- Attribute Provider
- Organisational Directory

Swiss edu-ID Operator
- Affiliation Archive
- Affiliation Index
- Attribute Aggregator
- Attribute Provider
- User Directory
- User Profile Panel
- User Authentication
- IdM Admin Panels
- SP Notification
- Audit Log
- Federation Registry
- Attribute Filter
- User Directory

Service Provider

Participants and Federation Partners

Participants

Operator

SWITCH
Synchronize IdM of Universities and Swiss edu-ID

- one common password
- synchronise name changes
Identity Management Processes

• Account…
  – Creation
  – Blocking / unblocking
  – Deletion
• Death of a user

• Attribute…
  – Editing
  – Verification

• Duplicate account…
  – Detection
  – Resolution

• Current affiliations…
  – Person enters an organisation (add affiliation)
  – Person leaves an organisation (transform affiliation “current -> former”)

• Former affiliations…
  – Add
  – Edit
  – Delete
Dependencies

Four partially dependent deployment dimensions

1. User Adoption
2. Adapting / extending services (AM)
3. Deployment at organisations (IdM)
4. Developing the Swiss edu-ID (central IdP, directory, UI, …)
User Adoption

SWITCHaai linking Swiss edu-ID

SP Opportunities

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Jul '15</th>
<th>Dec '16</th>
<th>2017-20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extend user group (alumni, guests, …)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>New attributes (edu-ID unique ID, ORCID)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Get more attribute information (extended model)</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Get user profile change notifications</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Share attribute/group information with other SPs</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>AM protocols for national services (OIDC, AD, LDAP)</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Support migrating users AAI-&gt;edu-ID</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrently serve AAI and Swiss edu-ID Users</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full coverage (all org members have an edu-ID)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️*</td>
</tr>
<tr>
<td>Access to former affiliations</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️*</td>
</tr>
</tbody>
</table>

* Only for users of ‘migrated’ organisations
### Organisation Integration Depth

<table>
<thead>
<tr>
<th>Level</th>
<th>Tasks</th>
<th>Benefits</th>
<th>Jul ’15</th>
<th>Dec ’16</th>
<th>2017-20</th>
</tr>
</thead>
</table>
| 1 linked | • “nothing”!  
• Communication measures | naked Swiss edu-ID  
edu-ID with affiliations and assurance levels | ✔ | ✔ | ✔ |
| 2 deployed | • 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 | ✔ |
| 3 integrated | • 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 | ✔ |

### Basic Components of Swiss edu-ID

![Diagram of Swiss edu-ID components](image_url)
Minimal Deployment Levels Compared

Deployment Level

Level 1
linked
2016

Level 2
deployed
2017…

Minimal Deployment

- Replace Shibboleth IdP with attribute provider
- Extend local directory with edu-ID Identifier
- Implement user onboarding: get ID into directory
- Implement user offboarding: remove affiliation
Advanced Deployment Levels Compared

Deployment Level

Level 2
deployed
2017…

Level 3
integrated
2018…

Advanced Deployment

• Integrate advanced identity management processes
  – Deal with user attribute changes (name, email, phone number, …)
    • Propagate to identity federation
    • Accept from identity federation
  – Duplicate account resolution
  – Account blocking and unblocking
  – Manage former affiliations
### Swiss edu-ID Development Phases

<table>
<thead>
<tr>
<th>Swiss edu-ID functionality</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>• User centric identity, self-serviced</td>
<td>- Jul 2015</td>
</tr>
<tr>
<td>• Support for current affiliations</td>
<td></td>
</tr>
<tr>
<td>• Get affiliation information through SAML attribute query</td>
<td></td>
</tr>
<tr>
<td>• Swiss edu-ID IdP provides extended attribute model to services</td>
<td></td>
</tr>
<tr>
<td>• Shared attribute management</td>
<td></td>
</tr>
<tr>
<td>• SP notifications</td>
<td></td>
</tr>
<tr>
<td>• Swiss edu-ID IdP provides classic model with affiliation chooser</td>
<td>- Dec 2016</td>
</tr>
<tr>
<td>• Organisational Shib-IdP is replaced by attribute provider</td>
<td></td>
</tr>
<tr>
<td>• &quot;direct&quot; access to affiliation information in org-directory</td>
<td></td>
</tr>
<tr>
<td>• all organisation members are migrated to Swiss edu-ID</td>
<td></td>
</tr>
<tr>
<td>• Org-IdM and edu-ID-IdM processes are connected</td>
<td>2017-2020</td>
</tr>
<tr>
<td>• Support for former affiliations</td>
<td></td>
</tr>
<tr>
<td>• New AM protocols (OIDC)</td>
<td></td>
</tr>
</tbody>
</table>

---

### Swiss edu-ID Deployment 2017 - 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></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **2016**
- **2017**
- **2018**
- **2019**
- **2020**
# Swiss edu-ID Deployment Step 1 in 2017

<table>
<thead>
<tr>
<th>Preparation</th>
<th>Migration Strategy</th>
<th>Project Management / Communication / Outreach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workshops stage 1</td>
<td>Workshops stage 2</td>
<td>Jan Feb Mar April May June July Aug Sept Oct Nov Dec</td>
</tr>
<tr>
<td>Individual Analysis 1</td>
<td>Individual Analysis 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Functional Upgrade

- Uniqueness
- Credential Management
- 3rd Party Vetting
- Group Management

## Project Application

- Consolidation
- Individual Migration Plans
- Generic Migration Strategies

### Workshops stage 1

- Individual Analysis 2

### Workshops stage 2

- Individual Analysis 2

### Individual Migration Plans

- Coordination

### Generic Migration Strategies

### Project Application

---

**Blog:** [identityblog.switch.ch](http://identityblog.switch.ch)

**Website:** [eduid.ch](http://eduid.ch)

**World café tomorrow:**

- National Active Directory server
- How to inform stakeholders
- Quality and Assurance

© 2016 SWITCH
OpenID Connect in the context of SWITCHaai and SWITCH edu-ID

ICT Focus, Lausanne, November 2016

Etienne Dysli Metref
etienne.dysli-metref@switch.ch
What is OpenID Connect?

OpenID Connect allows for clients of all types, including browser-based JavaScript and native mobile apps, to launch sign-in flows and receive verifiable assertions about the identity of signed-in users. openid.net (https://openid.net/connect/faq/)

- Adds “simple identity layer” on top of OAuth 2.0 framework
- Easy solution for delegating access to protected resources
- OpenID Connect 1.0 (OIDC) finalised early 2014
- Popular with web and mobile developers
SAML vs. OAuth vs. OIDC

Simply put

- SAML: single sign-on + user attributes
- OAuth: API authorization between applications
- OIDC: single sign-on + user attributes + API access

Token format

- SAML: XML
- OIDC: JSON web token (JWT)

Will OIDC replace SAML?

Not so soon, OIDC is still missing essential features:

- No federation support (yet), only bilateral trust agreements
- Every client must register itself with every IdP
  ⇒ Manual client registration does not scale
- Automatic client registration then?
  Would open your user directory to anyone on the Internet!
- Fewer standardised user attributes
Operating SAML and OIDC in parallel

What you can do if you want OIDC internally now

- Choose and install an OIDC IdP
- Register internal clients with it

Integration possibilities

1. Separate: standalone IdP for OIDC
2. Gateway: protect an OIDC IdP with a SAML SP
Operating SAML and OIDC in parallel

1. Separate: just run a standalone IdP for OIDC

- SAML Service Providers
- SAML Identity Provider
- LDAP / AD user directory
- OIDC Identity Provider
- OIDC clients
Operating SAML and OIDC in parallel

2. Gateway: protect an OIDC IdP with a SAML SP

- OIDC Identity Provider
- SAML Identity Provider
- LDAP / AD user directory
- SAML SP
- OIDC clients
How could we deploy OIDC to the entire SWITCHaai federation?

- Ask each institution to operate an OIDC service?
  ⇒ rollout too slow

- One IdP with OIDC for the whole federation
  ⇒ the SWITCH edu-ID IdP!

- Solves part of the scalability problem, but would still use manual client registration...
SWITCH edu-ID OIDC deployment

Today

- Proof of concept Shibboleth IdP with OpenID Connect
- Shibboleth IdPv3 addon (https://github.com/uchicago/shibboleth-oidc) developed by the University of Chicago and Unicon
- Open to testers from the community, contact us (mailto:aai@switch.ch) if you want to try

Next year

- Real OIDC IdP (with manual client registration)
Projects bridging the SAML–OIDC gap

- Mapping eduPerson attributes to OIDC claims REFEDS OIDCre WG (https://wiki.refeds.org/display/GROUPS/OIDCre)
- OpenID Connect Federation draft (https://openid.net/specs/openid-connect-federation-1_0.html)