Trust & Identity Workshop

Trust & Identity Team
trid@switch.ch

Bern, 14.3.2018
Agenda: Morning

• 10:15 – 11:25
  • Welcome to the Trust & Identity WG
  • The new SWITCH edu-ID Service Description
  • An Organization adopts SWITCH edu-ID
  • Single digital identity and multiple affiliations

• 11:25 – 11:45 Coffee break

• 11:45 – 12:35
  • What happens when a current affiliation ends?
  • SWITCH edu-ID behind the scenes

• 12:35 – 13:20 Buffet lunch & Coffee
Agenda: Afternoon

• 13:20 – 14:30
  • Custom-tailor the SWITCH edu-ID service for your SP
  • Think about data protection
  • Secrets of the SWITCH edu-ID password
  • Interfederation Update
  • Single logout
• 14:30 – 14:50 Coffee break
• 14:50 – 15:45
  • SWITCHpki News
  • SWITCH edu-ID Liaisons
  • SWITCH edu-ID Roadmap
  • What’s new @SWITCH
  • Wrap-up & Goodbye
• 15:45 – 16:30
  • Individual discussions with SWITCH
Business fields

• Network
• Security
• Trust & Identity
• Infrastructure and Data Services
• Registry and Procurement
Added value for customers

Community work

Foundation

Integrated offer
Trust & Identity: Projects and Services

- Swiss edu-ID (project)

- SWITCH edu-ID (service)

- SWITCHaai

- SWITCHpki
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
...nobody want’s to jump as the first one

- No experience or guidance
- Unknown pitfalls
- Waste of resources
- ....
However several showed interest

- EPFL
- FHNW
- UNIFR
- UNIGE
- UNIL
- UNISG
- ZHAW

Goal:
elaborate migration plans
once the first one jumped successfully…

1.11.2017: SWITCH
...others will follow!

2018
- UNILU
- PHSchwyz

2019
- UNIL
- UNISG
- ZHAW
- FHNW
- UNIFR
- ....
“Step 1 Jumpers” 2017+ (just planning!) are

- EPFL (Pierre Mellier)
- FHNW (Michael Hausherr)
- UNIFR (Jacques Tissot)
- UNIGE (Pierre-Yves Burgi)
- UNIL (Alexandre Roy/Christopher Greiner)
- UNISG (Armin Schibli)
- ZHAW (Nisanth Muthukirushnasamy)
“Step 2 Jumpers” 2018/2019 are

Implementation:
- UNIL
- UNISG
- ZHAW
- UniLU (u)
- PHSZ

Planning:
- BFH
- FernUni
- FHSG
- HES-SO
- HSLU
- HTW Chur
- HWZ
- NTB (u)
- PHBern
- PHSZ
- PH Zug (u)
- UniBE (u)
- UniLU (u)
- UniNE
- ZHdK

(u) = unfunded
SWITCH edu-ID
Service Description

Andres Aeschlimann

aai@switch.ch

Berne, 14. March 2018
Characteristics (1/2)

- 30 pages long (!)
- Available in D, F, E, and I:
  → https://www.switch.ch/edu-id/terms/
- Describes the service
  → follows the SWITCH template for service descriptions
- Defines relationships to end users and organisations
  → incorporates the Terms of Use (ToU)
  → incorporates the Governance of the SWITCHaai Federation
Characteristics (2/2)

• Is based on SWITCH Service Regulations and GTC
  → SWITCH Service Regulations for the SWITCH Community
    https://www.switch.ch/about/disclaimer/service-regulations/
  → SWITCH General Terms and Conditions for the Extended SWITCH Community: https://www.switch.ch/about/disclaimer/gtc/

• Follows the REFEDS policy template as recommended by GÉANT:
    https://wiki.refeds.org/display/FBP/Federation-Best-Practice+Home
Should I read it?

• Do I use it?
• Do I want to know what the SWITCH edu-ID is?
History of this Service Description

- The SWITCH edu-ID Service Description replaces the SWITCHaai Service Description from 2011
  - SWITCHaai federation policy is in Chapter 5
  - SWITCHaai federation name does not change
Federation Partners

Two flavours

• **Basic:** Such federation partners are contributing **services** to the Federation.
  → are having a sponsorship support by an **organization** from the SWITCH Community, or
  → are having an established, contracts-based relationship with SWITCH Community members

• **Plus:** Such federation partners are **introducing End Users** (and services) into the Federation
  → Currently limited to organizations in the extended SWITCH Community
As the Federation Operator, SWITCH operates the SWITCHaai Federation and consults both the SWITCH edu-ID Advisory Board and the Trust & Identity WG.

https://www.switch.ch/edu-id/governance/
As the Federation Operator, SWITCH operates the SWITCHaai Federation and consults both the SWITCH edu-ID Advisory Board and the Trust & Identity WG.

SWITCH edu-ID Advisory Board

- Acts as an advisory organ concerning the long-term strategy of the SWITCH edu-ID service.
- SWITCH decides on the composition of the SWITCH edu-ID Advisory Boards.
- The SWITCH edu-ID Advisory Board has no decision-making authority.
How an Organization Integrates edu-ID
Using the example of SWITCH

Rolf Brugger
rolf.brugger@switch.ch
Bern, 14.03.2018
An organization adopts SWITCH edu-ID
Organization Operating its own AAI-IdP
Organization with edu-ID Integration

Organization

Directory
AP

IdP
Attribute aggregator
Directory

Org
Service

UZH Org

SWITCH

© 2018 SWITCH | 4
The organization SWITCH has adopted edu-ID last year.
The User’s Perspective
Communication to Users

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

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

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

**Further Checks**

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

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

### Attributes Table

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistent-id</td>
<td><a href="https://aai-logon.switch.ch/idp/shibboleth1">https://aai-logon.switch.ch/idp/shibboleth1</a> [<a href="https://attribute-viewer.aai.switch.ch/shibboleth187fO9XcJs1uVAw9Cq">https://attribute-viewer.aai.switch.ch/shibboleth187fO9XcJs1uVAw9Cq</a>][MIQ][RaH4=]</td>
</tr>
<tr>
<td>uniqueID</td>
<td><a href="mailto:642448@switch.ch">642448@switch.ch</a></td>
</tr>
<tr>
<td>givenName</td>
<td>Rolf</td>
</tr>
<tr>
<td>surname</td>
<td>Brugger</td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:rolf.brugger@switch.ch">rolf.brugger@switch.ch</a></td>
</tr>
<tr>
<td>homeOrganization</td>
<td>switch.ch</td>
</tr>
</tbody>
</table>
AIA Attribute Viewer

There are more than 30 attributes defined for SWITCHaai. Most participating organisations release a subset of these attributes only, and not all attributes are available to every AAI user. What you should see below is:

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

Further Checks

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

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

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistent-id</td>
<td><a href="https://aai-logon.switch.ch/idp/shibboleth1https://attribute-viewer.aai.switch.ch/shibboleth1877F09XCljuVAsw9CqIMQ79raH4=">https://aai-logon.switch.ch/idp/shibboleth1https://attribute-viewer.aai.switch.ch/shibboleth1877F09XCljuVAsw9CqIMQ79raH4=</a></td>
</tr>
<tr>
<td>SAML2 Attribute Name:</td>
<td></td>
</tr>
<tr>
<td>urn:oasis:names:c2:SAML:2.0:nameid-format:persistent</td>
<td></td>
</tr>
<tr>
<td>uniqueID</td>
<td><a href="mailto:642448@switch.ch">642448@switch.ch</a></td>
</tr>
<tr>
<td>SAML2 Attribute Name:</td>
<td></td>
</tr>
<tr>
<td>urn:oid:2.16.756.1.2.5.1.1.1</td>
<td></td>
</tr>
<tr>
<td>givenName</td>
<td>Rolf</td>
</tr>
<tr>
<td>SAML2 Attribute Name:</td>
<td></td>
</tr>
<tr>
<td>urn:oid:2.5.4.42</td>
<td></td>
</tr>
<tr>
<td>surname</td>
<td>Brugger</td>
</tr>
<tr>
<td>SAML2 Attribute Name:</td>
<td></td>
</tr>
<tr>
<td>urn:oid:2.5.4.4</td>
<td></td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:rolf.brugger@switch.ch">rolf.brugger@switch.ch</a></td>
</tr>
<tr>
<td>SAML2 Attribute Name:</td>
<td></td>
</tr>
<tr>
<td>urn:oid:0.9.2342.19200300.100.1.3</td>
<td></td>
</tr>
<tr>
<td>homeOrganization</td>
<td>switch.ch</td>
</tr>
</tbody>
</table>
The Perspective of the Service Providers
Communication to Service Providers

\[ x - 10 \text{ days} \]

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

Woah! We need more time for testing!

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

Integrated Linkage

edu-ID

WAYF

Entity-ID: edu-ID.ch

Uni-X

Entity-ID: uni-x.ch

Attribute Provider

© 2018 SWITCH | 17
Adoption Approaches

Linking at Registration

Linking at Admission

Linking after Admission

https://projects.switch.ch/eduid
SWITCH IdM before Day X

Employee mgt system registration (web-form)

LDAP Directory

IdP (Shibb)

edu-ID
API, attribute aggregator, IdP

| id | Name | Email | Addr | ...
|----|------|-------|------|---
|    |      |       |      |   
|    |      |       |      |   
|    |      |       |      |   

send registration form to employee (paper)

Fill in registration form and send it back

Fill in internal web form

Send data to directory

Activate account on first working day

© 2018 SWITCH | 19
SWITCH IdM after Day X

1. **Employee mgt system registration (web-form)**
   - Send registration form to employee (paper) with edu-ID instruction
   - Fill in registration form and send it back
   - Fill in internal web form
   - Send data to directory
   - Activate account on first working day

2. **LDAP Directory**
   - Create affiliation

3. **edu-ID**
   - Link edu-ID, sends Identifier by email
   - Fill in internal web form
   - Send data to directory
   - Activate account on first working day

4. **Link edu-ID**
   - Employee mgt system
   - Edu-ID

5. **AP (Shibb)**
   - Edu-ID API, attribute aggregator, IdP

© 2018 SWITCH | 20
Registration of a new Member

Link edu-ID

Employee mgt system registration (web-form)

LDAP Directory
Die Seite dient der Anmeldung neuer SWITCH Mitarbeitender. Dazu werden der SWITCH edu-ID Identifikator und die unten angezeigten Daten an das Human Resources Team von SWITCH übermittelt, welches diese Angaben dann in die relevanten Benutzerverzeichnisse einträgt.

Folgende Informationen an das SWITCH Human Resource Team übermitteln:

- **Swiss edu-ID Identifier**: 674f1668-6299-
- **Vorname**: Rolf
- **Familienname**: Brugger

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

Eine neue Registrierung für einen SWITCH Mitarbeiter ist eingegangen:

Swiss edu-ID Identifier:
674f1668-6299-

Vorname: Rolf
Familienname: Brugger
Geburtsdatum: 19
E-Mail-Adresse:
Geschlecht: Männlich
Wohn-Adresse: Zürich, Suisse
Mobil-Nummer: +41 79
ORCID Identifikator: http://orcid.org/0000-0001-9351-8252
Bevorzugte Sprache: Englisch

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

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

Vielen Dank & Freundliche Grüße
SWITCH edu-ID Team

--

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

- Involved parties at the Organization
  - Human resources 1d
  - IdM/Account management 3-4d
  - Support 1d
  - Communication 1d
- Everything went smoothly
Individual Roadmaps

Account linking of current members

Link users before day X

Link users after day X

Link users at day X

Onboarding of future members

Linking after admission

Linking at registration

Linking at admission

AP-Interface

Attribute push

Attribute pull
## Adopting the edu-ID at Organizational Level

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

IdP Authentication | SP Attributes
---|---
UZH
---
ZHAW
---

Private Identity
Affiliation
Affiliations

edu-ID
---
UZH
---
ZHAW
---
User Chooses Affiliation

- edu-ID
- UZH
- ZHAW

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

Choose an Identity to Proceed

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

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

- **Student @ switch.ch**
  - rolf.brugger@switch.ch

- **Private Person**
  - mail@rolfb.ch

Manage your identities
Services Define Accepted Affiliations

• SWITCH edu-ID can represent
  • A private identity
  • And multiple affiliations
• Many SPs will not accept all kinds of affiliations
  • Access to Student Dashboard → university members only
  • Student registration → private users only

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

edu-ID

UZH

ZHAW

Affiliation Chooser

© 2018 SWITCH | 36
No Affiliation - Service limited to students
Service limited to private users only:
Service accepts all kinds of users:
Extended Service:
### Default Intended Audience

<table>
<thead>
<tr>
<th>Audience</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>University users</td>
<td>excluded</td>
</tr>
<tr>
<td>University of Applied Sciences users</td>
<td>excluded</td>
</tr>
<tr>
<td>Hospital users</td>
<td>excluded</td>
</tr>
<tr>
<td>Library users</td>
<td>excluded</td>
</tr>
<tr>
<td>Professional education and training college</td>
<td>excluded</td>
</tr>
<tr>
<td>Institution on the upper secondary level</td>
<td>excluded</td>
</tr>
<tr>
<td>Virtual Home Organization</td>
<td>excluded</td>
</tr>
<tr>
<td>Other users</td>
<td>excluded</td>
</tr>
</tbody>
</table>

### Specific Intended Audience

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

- **Add a new specific intended audience**
  - **SWITCH edu-ID** users

### SWITCH edu-ID Private Identity

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

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

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

• Affiliation chooser is relevant for organizations with integrated edu-ID
• Long-term perspective: It will replace the WAYF
• With properly configured intended audience
  ➞ improved user experience
What happens...
...when a current affiliation ends?

Etienne Dysli-Metref
etienne.dysli-metref@switch.ch

Bern, 14.03.2018
What is an affiliation?

• Role held by an end user associated with an organisation in the SWITCHaai Federation.

• Created by linking a base identity with the organisation-related identity of the user.

• A base identity can be linked with none, one or multiple affiliations.

• An existing affiliation is described as a current affiliation; a previous, no longer active, affiliation is described as a former affiliation.
Attribute aggregator

The attribute aggregator is a *cron job*

- Queries all attribute providers (your IdPs) for current affiliations.
- Uses the edu-ID SP as intermediary to query IdPs.
- For this, it needs an identifier, obtained when the account was linked (persistent ID).
Attribute aggregator

The attribute aggregator is a cache

- Affiliations are stored in the SWITCH edu-ID system.
- Allows the edu-ID IdP to take over the role of the institutional IdP and present the user, at login time, with a choice of affiliations.
Current and former affiliations

An affiliation ceases to be current when either:

- the attribute aggregator no longer receives attributes for a given user, or
- a migrated organisation notifies the edu-ID system (not implemented yet).

What does the SWITCH edu-ID system do with the affiliation data when it ceases to be current?

- Today: nothing happens
- Tag it as *former affiliation* (not implemented yet)
Attribute aggregator, under the hood

- Makes a SAML attribute query for all persistent IDs linked with each edu-ID account, ~40k queries in 4 hours.
- Going through the SP saves a lot in SAML implementation and processing but hides errors happening between SP and IdP.
- If attributes are received, then the affiliation is updated with new values. The affiliation stays current.
- If no attributes are received several times (days) in a row, the affiliation expires (not implemented yet).
Expiration of an affiliation

1. The affiliation is removed from the edu-ID account and stored in the former affiliations space. The edu-ID IdP will no longer send attributes related to this affiliation to SPs, nor offer it as a choice upon login.

2. SPs which have subscribed to affiliation changes are notified (not implemented yet). For example: SWITCHdrive, SWITCHengines, SPs in SWITCHaai.

3. SPs which have not subscribed will notice the affiliation change when the set of attributes they receive changes (upon next login or with an attribute query).
Preparation and next steps

For IdP Administrators

• After the SWITCH edu-ID adoption your IdP might remain and will in that case be called an *Attribute Provider* and you will be called *AP Administrator*.

• Make sure the SAML2 attribute query endpoint of your IdP is correctly published in the Resource Registry.

• Make sure your firewall and/or ACLs allow access to this endpoint from the edu-ID SP.

• Make sure your IdP’s attribute filter allows releasing attributes to the edu-ID SP.

• [optional but recommended] Configure HomeOrganisation and HomeOrganisationType attributes with a Static DataConnector so that they are always released.
SWITCH edu-ID...
...behind the Scenes

Daniel Lutz
daniel.lutz@switch.ch

Berne, 14. March 2018
Overview

- Infrastructure and Software Components
- Service Quality and Availability
- IdP Extension developed by SWITCH
Infrastructure and Software Components

Data Center Zürich

Data Center Lausanne
Environments for Production and Testing

**Production**  Federation: SWITCHaai  **Testing**  Federation: AAI Test

- **Production**
  - Zürich
  - Lausanne

- **Testing**
  - Zürich
  - Lausanne
Software Components (1/2)

“My edu-ID” Account Management
• Account management tool for users (account owners)
• Software: Web application developed by SWITCH (PHP)

Administration
• Administration tool for support staff
• Software: Web application developed by SWITCH (PHP)

SP
• Authentication service for applications above (“AAI”)
• Software: Shibboleth Service Provider

Attribute Aggregator
• Collects identities (attributes) from organizations and stores them to the edu-ID accounts they are linked with.
• Software: Server application developed by SWITCH (Java)
Software Components (2/2)

LDAP Master / Slave
• Main data store
• Software: OpenLDAP

IdP
• IdP of the SWITCH edu-ID
• Software: Shibboleth Identity Provider
  • with extension for "Affiliation Chooser", developed by SWITCH

Databases
• Databases for "SCIM Groups" and local IdP data
• Software: MariaDB and PostgreSQL

SCIM Groups
• Simple group management based on the eduPersonEntitlement attribute
Service Quality and Availability

General

• Fully operated by SWITCH
• Availability:
  • In general 24x7
  • SWITCH aims to achieve availability of at least 99.99%. Disruptions that compromise the service remain reserved.
  • SWITCH always conducts planned maintenance work outside normal business hours and announces such work at least one week in advance on the login page of SWITCH edu-ID.
  • SWITCH undertakes to initiate or complete measures to remedy disruptions and malfunctions of the service within normal business hours.
Web applications, LDAP master

- Running on single instance
- No HA (yet)
- Single LDAP master server (read-write access)
- Data continuously synchronized to two LDAP slave servers
- More LDAP slave servers could easily be added if required
Identity Provider, LDAP slaves

- Two instances
- Based on IdP Hosting Platform
- Active-Standby setup with manual handover
- Connected to two LDAP slave servers
- Setup is somewhat redundant, but we will need to improve performance and availability.
Monitoring

• 24x7 monitoring via Nagios
• Specific probes and overall probes (some of them are simulating a whole login process)
• Notifications through e-mail and SMS
Technical Roadmap Options

- Moving to Docker Containers
- OpenShift technology on SWITCHengines
- High Availability, Load Balancing and Clustering wherever possible
IdP Extension "Affiliation Chooser"

- Allows user to select private or linked identity, including associated attributes, to use to access the service, while preserving SSO functionality (i.e. authenticate once).
- Can automatically choose appropriate identity if SP correctly declares intended audience.
- Edu-ID IdP can mimic your IdP, so that SPs take it for your IdP:
  - Edu-ID IdP can issue exactly the same SAML assertions
  - SPs can be left untouched at adoption of edu-ID
  - Except when an organization uses local attributes (open issue)
- Is implemented in Java as an extension to the Shibboleth IdP
- Includes Java code and an own, specific configuration
Challenges experienced

• Shibboleth IdP software doesn't support multiple assertion issuers out-of-the-box.
  • This functionality was not part of the initial design.
  • But the software provides means to do it. Although with some restrictions, which we placed as issues to the Shibboleth development team.

• Attribute resolution configuration gets quite complex. (Different attribute resolution steps required at different places during the login flow.)
Custom-tailor the edu-ID service for your SP

Lukas Hämmerle
lukas.haemmerle@switch.ch

Trust & Identity WG Meeting
14. March 2018, Bern
Overview

• How to tailor the edu-ID look & feel per SP
  • Custom Views in a nutshell

• How can a SP trigger a user to complete his user profile?
  • edu-ID Login Link Composer quick tour
Custom Views in a Nutshell

• **Use-Case:**
  Organisations started to use edu-ID for student registration

• **Problem:**
  Students start at organisation X with look & feel Y but then get to edu-ID service with look & feel Z

• **Solution:**
  Allow organisation-specific logo and texts to make registration process more consistent
Find the 10 Differences

Registration Page:

Create a SWITCH edu-ID account

Please complete the following form to create a new SWITCH edu-ID account.

Personal Data

First Name: John
Last Name: Doe

E-mail Address: john.doe@example.org
Password:
Confirm Password:

How much is:

I fully understand and accept the Terms of Use for creating and using a SWITCH edu-ID account. The Terms of Use will also be sent to you by e-mail when your account has been successfully created.

Create account
Also for Login Page
Data to Provide for Custom View

entityID=
returnURL.[en|it|fr|de]=
login-logo-url.[en|it|fr|de]=
login-logo-link-url.[en|it|fr|de]=
login-name.[en|it|fr|de]=
login-outro.[en|it|fr|de]=
reg-logo-url.[en|it|fr|de]=
reg-logo-link-url.[en|it|fr|de]=
reg-name.[en|it|fr|de]=
reg-tou-amendment.[en|it|fr|de]=
reg-intro.[en|it|fr|de]=
reg-outro.[en|it|fr|de]=
edu-ID Custom Views Summary

• Custom Views per Service Provider
  • Not only for student registration SPs
  • Currently custom views for 16 SPs configured

• Multiple languages supported
  • Currently: Italian, French, German, English

• Return URL to send user to after registration
  • User is sent authenticated or unauthenticated to given URL after registration

• More information:
  https://switch.ch/edu-id/support/howto/customization/
edu-ID Login Link Composer

Some SPs want to:

- Send user to **particular URL** after
  - Registration
  - Login
  - Both

- Ensure the user has a **particular attribute**
  - E.g. mobile, home address (unverified/verified)

- Force **particular language** to be used on edu-ID pages
  - Regardless of user’s browser language
No problem…. or is it?

Previous use-cases can be achieved by just sending the user to a particular URL:


The Easy Way

• Composing URLs manually is not trivial
• edu-ID Login Link composer makes it trivial
  https://switch.ch/edu-id/support/howto/link-composer/
Summary

SPs can customize appearance and flows of edu-ID

• Logo can be added
• Text can be added
• Web Flow can be triggered

In spite of customizations it still should be sufficiently clear to user that he has an edu-ID account.
Think about Data Protection
Goal

We are compliant with the different applicable data protection laws
But …

Data Protection Law compliant
3 Actors

Cantonal Universities

Federal Institutes of Technology

Federal Data Protection Law

Cantonal Data Protection Laws

SWITCH
2 Purposes

University Administration

SWITCH edu-ID

User Purposes
How to get & deliver answers …

• Legal questions collected (regulations WG, 2014)

• Questions sent to different Data Protection Officers (2015)

• Several queries on federal data protection officer because of expected written answer (2015 - … )

• Legal developments in CH and EU observed (2014 - … )

• Participation in E-ID consultation (May 2017)

• Situation about social security number AHVN13 analysed with FHNW (2017)

• SWITCH edu-ID database declared (2017)

• Service Description elaborated (federation policies adopted; 2018)
Statements by Data Protection Officers

- Positive: „Lifelong use“ of SWITCH edu-ID
- Negative: Storing data after leaving Higher Education Institution

→ solution found

Allow to delete account (if no active affiliation)

Former affiliation & user consent
AHVN13

- Use of AHVN13 as attribute within SWITCH edu-ID?
- Legal assessment by SWITCH
- Legal advise:
  - Use of AHVN13 deemed as too delicate
  - Observe political development about usage of AHVN13
- Legislative project for wider applicability

*Risk analysis (in German): https://projects.switch.ch/eduid/documents/*
Legal aspects of the Service Description

• Data protection provisions (chapter 6.3)

• Provisions regarding warranty, liability, applicable law, place of jurisdiction etc.

https://www.switch.ch/edu-id/terms/
7 Privacy Principles

1. Lawfulness, fairness and transparency

2. Purpose limitations

3. Data minimisation

4. Accuracy

5. Storage limitations

6. Integrity and confidentiality

7. Accountability

Use of data described

Data economy in federation

Updates

Deletion of accounts

Data security

Demonstrate compliance with principles
7 Privacy Principles

1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality
7. Accountability

Privacy by

- **Design**: technical integration
- **Default**: data protection friendly settings

Demonstrate compliance with principles
How to protect data in general

1. **Apply law(s) and principles for processes & services**
   E.g., store & release only data necessary for the declared and current purpose

2. **Consult (local) Data Protection Officer**
   (knows local regulations as well as law)

3. **Apply specific policies**
   - Resource Registry ➔ Data Release Policy (fill role of administrator)
   - Local (university) policies

4. **Inform & instruct staff and end users**
   - Clear user guides, Help, ToU, courses for IT and other staff
   - User awareness campaigns (security, data protection)
How to protect data in SWITCH edu-ID?

<table>
<thead>
<tr>
<th>Secure storage of data</th>
<th>ISMS</th>
<th>ISMS/other</th>
<th>credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of data</td>
<td>SLA</td>
<td>SLA</td>
<td>(updates)</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>access/policy</td>
<td>access/policy</td>
<td>credentials</td>
</tr>
<tr>
<td>Transparency</td>
<td>user consent, ToU, SLA</td>
<td>local ToU</td>
<td>My account</td>
</tr>
<tr>
<td>Accuracy (correctness of data)</td>
<td>verified email, mobile number, postal address</td>
<td>all transmitted attributes (verification)</td>
<td>ToU, updates</td>
</tr>
<tr>
<td>Data Economy (minimisation)</td>
<td>define minimal requirements</td>
<td>apply minimal requirements</td>
<td>user consent</td>
</tr>
<tr>
<td>Audits</td>
<td>ISMS</td>
<td>(right reserved)</td>
<td>inspection</td>
</tr>
<tr>
<td>Attribute Release Policy (ARP) in RR</td>
<td>approval process</td>
<td>approval by RRA admin</td>
<td>user consent</td>
</tr>
<tr>
<td>Federation trust layer</td>
<td>governance</td>
<td>community rules</td>
<td>membership</td>
</tr>
</tbody>
</table>
Current Law Situation

EU General Data Protection Regulation (GDPR) (Datenschutzgrundverordnung DSGVO):
- enforcement 25.5.2018
- important also for Switzerland
→ no immediate adaptations necessary (for SWITCH)

Revision of CH Federal Data Protection Act (Bundesgesetz über den Datenschutz DSG):
- includes adaptations for EU law
- delayed, expected earliest for end of 2018
- “compatibility” with GDPR
→ SWITCH will avoid double adjustments and apply CH law

New E-ID law
- simultaneously with data protection act or later
- impact possible if used as basic identity (but not directly on edu-ID)

https://www.eugdpr.org/
https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung.html
Tasks for the future

• Fill seat for legal representative in Advisory Board (mandate by SWITCH; hints welcome!)

• Analyse & compare legal statements of Data Protection Officers

• Analyse draft and final version of FDPA; prepare changes (if necessary)

• More detailed description of data processing

• Prepare process for inspection of record by users

• Prepare paper with reasoning for universities
Result:

We are compliant with the different applicable data protection laws
Secrets of the edu-ID Password

Lukas Hämmerle
lukas.haemmerle@switch.ch

Trust & Identity WG Meeting
14. March 2018, Bern
Setting a Good Password

- **System:** "Sorry, your password is too old and has expired – choose a new one."
  - **User types:** roses

- **System:** "Sorry, too few characters."
  - **User types:** pretty roses

- **System:** "Sorry, you must use at least one numerical character."
  - **User types:** 1 pretty rose

- **System:** "Sorry, you cannot use blank spaces."
  - **User types:** 1prettyrose

- **System:** "Sorry, you must use at least one upper case character."
  - **User types:** 1FUCKINGprettyrose

- **System:** "Sorry, you cannot use more than one upper case character consecutively."
  - **User types:** 1FuckingPrettyRose

- **System:** "Sorry, you must use no fewer than 20 total characters."
  - **User types:** 1FuckingPrettyRoseShovedUpYourAssIfYouDon'tGiveMeAccessRightNow!

- **System:** "Sorry, you cannot use punctuation."
  - **User types:** 1FuckingPrettyRoseShovedUpYourAssIfYouDon'tGiveMeAccessRightNow

- **System:** "Sorry, that password is already in use."
Design Goals (back in 2014)

- Pragmatic password selection process
  - No enforced renewal of passwords
  - Reasonable protection against brute-force cracking
  - Ease-of-use for user (e.g. no autocomplete="off")

- State of the art password hashing algorithm
  - When passwords hashes stolen, it should be hard to crack them
  - Hashing algorithm widely accepted and standard
  - Pragmatic balance between security and compatibility

- Today: >50’000 accounts and no user complaints since 2014 regarding difficulty to choose a password
Coming Up

1. Password Hashing

2. Choosing a Password

3. NIST Password Recommendations
Password Hashing

Passwords are stored as Salted SHA 512 with 5’000 rounds.

SHA-512("None0fYourBusine55" + "c004b603fecbb45b")^{5000}

<table>
<thead>
<tr>
<th>LDAP Password type</th>
<th>Random Salt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password type</td>
<td>Rounds</td>
</tr>
<tr>
<td>{CRYPT}$6$rounds=5000$c004b603fecbb45b$oO7tlG04nkDIUTQ0BPTZSF.UpGjjAoh0ZnsmMuO4K4XMW6n48TfqHyHE0YbhImfBGrfDcYzO9a.34jHaC78ZF.</td>
<td></td>
</tr>
</tbody>
</table>
Choosing a Password

• Users choose their passwords, edu-ID provides guidelines

Password

• Not all passwords are accepted. Depends on password score:
  • Length, Uppercase, Lowercase, Numbers, Symbols
  • Score must exceed a certain threshold

• Must not be in database with leaked passwords
  • **Since July 2016**: Local check (search as you type) against list of 10 million “most used“ password (only 41’000 of them exceed threshold)
  • **Since Feb. 2018**: When submitted, check against Troy Hunt’s 501M leaked password hashes (password/full hash are not sent to service)
Accepted and Rejected Passwords

424242424242 - √ ok
Thisisalongpassword - √ ok
this is also long - √ ok
This1$Shrt - √ ok

jesuis1pilote - X not accepted
Weihnachtsbaum - X not accepted
123456789qwertyuiop - X not accepted
Q1w2e3r4t5y6u7i8o9p0 - X not accepted

Most Used and Leaked passwords
NIST Password Recommendations

- NIST = National Institute of Standards and Technology
- NIST Special Publication 800-63B: Digital Identity Guidelines
  - Released June 2017
  - Chapter about Memorized Secrets (”Passwords”)

Interesting Changes:
- Removed periodic password change requirements
- Dropped password composition requirements
- Introduced check of passwords against lists of commonly used or compromised passwords
NIST Password Rules: **SHALL**

- Minimum 8 characters long ✓ (min. 10 chars)
- No hint/reset questions stored ✓
- Compare password against list of commonly-used password ✓ (Leaked passwords won’t be accepted)
- Rate limiting ✗ (failed logins are monitored/alerted though)
- Encrypted/authenticated channel to check password ✓
- Salted Password hashes ✓
- Salt length min. 32 bit ✓ (128 bit)
- Approved random number generator ? (unclear, but used openssl is considered cryptographically secure ✓)
- No truncation ✓
NIST Password Rules: SHOULD

- No character type composition rules (√) (see previous slides)
- Password up to 64 characters √ (tested with 256 chars)
- All printing ASCII and space characters accepted √
- Warning when unicode characters are used X (not needed)
- Password-strength meter √
- Allow pasting password √
- A memory-hard hash function √ (Salted SHA-512)
- Hash iteration as large as verification server performance will allow, typically at least 10,000 iterations √/ X (“only” 5000)
- Additional hashing operation with secret stored in hardware module X (would break interoperability with SWITCHdrive/SWITCHengine, considerable effort needed)
Conclusion

• We care about good passwords!

• SHA-512 with 5’000 rounds probably still sufficient
  • Protection good enough unless NSA/FSB/MOSA/ want our passwords

• Most NIST recommendations are followed
  • Rate limiting is yet to be implemented
  • Hardware module for securing password hashes to be considered
    (is this in use at any university for storing password hashes?)

• Two-Factor authentication to be introduced late 2018
  • First: SMS One Time Password
  • Then: Time-based One Time Password
Interfederation Update

Thomas Lenggenhager
aai@switch.ch

Bern, 14.03.2018
Outline

• Interfederation Status

• Entity categories
  • In general
  • REFEDS Research & Scholarship (R&S)
  • GÉANT Data Protection Code of Conduct (CoCo)
  • Security Incident Response Trust Framework for Federated Identity (SIRTFI)
eduGAIN: Current Status

eduGAIN in Total
• 2655 IdPs, 1888 SPs

https://technical.edugain.org/status

Status in CH
• 51 IdPs enabled
  ~ 88% of all AAI accounts
  ~ 97% of all Higher Ed accounts
• 15 SPs enabled

https://www.switch.ch/aai/interfederation
SWITCHaai Interfederation Status

Special Home Organizations
- libraries.ch
- SWITCH edu-ID
- VHO

Legend
- SWITCHaai & Interfederation
- SWITCHaai only
Entity categories

• A generic method to enrich metadata
  • Tag an entity (SP or IdP) as being part of a category
  • Requires a specification for international coherent use
    • Criteria, Purpose, Policies, etc.

• In interfederation context:
  • Filling the gap of missing common policies
  • Further scalable attribute release (R&S and CoCo)
  • Support or increase scalable trust (SIRTFI)
How does it look like in SAML Metadata

<!-- AAI Viewer Interfederation Test -->
<entityDescriptor entityID="https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth">
  <Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:OASIS:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      </saml:Attribute>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      FriendlyName="swissEduPersonHomeOrganization" Name="urn:oid:2.16.756.1.2.5.1.1.4" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>switch.ch</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                      FriendlyName="swissEduPersonHomeOrganizationType" Name="urn:oid:2.16.756.1.2.5.1.1.5" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>others</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
</entityDescriptor>
REFEDS R&S

• REFEDS Research & Scholarship category
  • Federations can "tag" research and education SPs
    • Research & scholarship interaction
    • Collaboration
    • Management
    • Not for SPs from publishers
  • Allows easier/safer attribute release

• Restricted Attribute set:
  • Personal identifiers: email, person name, eduPersonPrincipalName
  • Pseudonymous identifier: eduPersonTargetedID
  • Affiliation: eduPersonScopedAffiliation
GÉANT Data Protection Code of Conduct

Increase the trust in Service Providers (SPs)

- The method is based on the EU Data Protection directives
- The SP has to provide a Privacy Policy (in English, according to the guideline)
- That will encourage the Home Organisation IdP to release attributes
  ➔ attribute release will scale

Code of Conduct Toolkit

- Data Protection Code of Conduct for SPs in EU/EEA
- Entity category attribute definition for the Code of Conduct
- SAML2 profile for the Data Protection Code of Conduct
## Comparison between R&S and CoCo

<table>
<thead>
<tr>
<th>REFEDS R&amp;S</th>
<th>GÉANT DP CoCo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Mainly Europe</td>
</tr>
<tr>
<td>Common purpose of the SPs</td>
<td>Common data protection standards</td>
</tr>
<tr>
<td>Fixed set of attributes</td>
<td>SP can require any attributes</td>
</tr>
</tbody>
</table>

GÉANT DP CoCo v2 in preparation:
- Based on GDPR
- Targets worldwide scope

http://refeds.org/category/research-and-scholarship
SIRTFI - coordinated incident response

• A Security Incident Response Trust Framework for Federated Identity
  • Operational Security
  • Incident Response
  • Traceability
  • Participant Responsibilities

• Initiated and driven by CERN and other big science infrastructures

https://refeds.org/sirtfi
Entity Category Adoption Internationally

- **CoCo**: 330
- **R&S**: 524
- **SIRTFI**: 250

Total: 1104
### SIRTFI adoption in SWITCHaai IdPs

<table>
<thead>
<tr>
<th>CERN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universities</td>
</tr>
<tr>
<td>Universität Basel</td>
</tr>
<tr>
<td>Université de Genève</td>
</tr>
<tr>
<td>Universities of applied sciences</td>
</tr>
<tr>
<td>HES-SO</td>
</tr>
<tr>
<td>HSR</td>
</tr>
<tr>
<td>ETH-Rat</td>
</tr>
<tr>
<td>EPFL</td>
</tr>
<tr>
<td>ETH Zürich</td>
</tr>
<tr>
<td>PSI</td>
</tr>
<tr>
<td>SWITCH</td>
</tr>
<tr>
<td>SWITCH edu-ID</td>
</tr>
<tr>
<td>SWITCH</td>
</tr>
<tr>
<td>VHO</td>
</tr>
</tbody>
</table>
Single Logout with the SWITCH edu-ID IdP

Daniel Lutz & Thomas Lenggenhager
aai@switch.ch

Berne, 14. March 2018
Overview

- SLO with the SWITCH edu-ID IdP
  - The scenarios with Screenshots

- Open issues with SLO and Shibboleth IdP v3.3

- How to make an SP SLO compliant

- What you should know about SP SLO
Single Logout Scenarios

The scenarios

a) Logged in at a single SP

b) Logged in at multiple SPs
   b1) All support SLO
   b2) Not all support SLO

Logout initiated at the SWITCH edu-ID My Account web application for all scenarios:
Case a) Logged in at a single SP

You have been logged out successfully.

You can now close your browser or the current tab.
Case b1)   Logged in at multiple SPs   (1/3)
Case b1) Logged in at multiple SPs (2/3)

user picked: Stay logged in

You have been logged out successfully.

You're still logged in to the following services:

- AAI Attributes Viewer
- AAI Attributes Viewer Test

You can now close your browser or the current tab.
Case b1) Logged in at multiple SPs (3/3)

user picked: Log out of all services

You have been logged out successfully of all SWITCH edu-ID services.

You can now close your browser or the current tab.
Case b2) Logged in at multiple SPs (1/3)

You have been logged out successfully.

You're still logged in to the following services:

- AAI Attributes Viewer
- SWITCH WWW

Log out of all services  Stay logged in
Case b2) Logged in at multiple SPs (2/3)

You have been logged out successfully.

You're still logged in to the following services:

- AAI Attributes Viewer
- SWITCH WWW

You can now close your browser or the current tab.
Case b2) Logged in at multiple SPs (3/3)

user picked: Log out of all services

Logout

Logout failed for some services:

- SWITCH WWW

For security reasons, we recommend to close your browser. This is all the more important when working at a public computer (e.g. in computer pools or Internet cafés).
Open issues with SLO and Shib IdP v3.3 (1/3)

Default user experience has some deficiencies

Case a):

Our Identity Provider
(replace this placeholder with your organizational logo / label)

This page is displayed when a logout operation at the Identity Provider completes. This page is an example and should be customized. It is not fully internationalized because the presentation will be a highly localized decision, and we don’t have a good suggestion for a default.

The logout operation is complete, and no other services appear to have been accessed during this session.

Case b):

Our Identity Provider
(replace this placeholder with your organizational logo / label)

This page is displayed when a logout operation at the Identity Provider completes. This page is an example and should be customized. It is not fully internationalized because the presentation will be a highly localized decision, and we don’t have a good suggestion for a default.

Would you like to attempt to log out of all services accessed during your session? Please select Yes or No to ensure the logout operation completes, or wait a few seconds for Yes.

Yes  No

If you proceed, the system will attempt to contact the following services:
Demo SP2
Demo SP1

or wait a few seconds for Yes
Open issues with SLO and Shib IdP v3.3 (2/3)

Case b2) text stays on screen, even after completion
Open issues with SLO and Shib IdP v3.3 (3/3)

• The modifications applied on the SWITCH edu-ID IdP are not forward compatible with future versions.

• No deployment instructions we could recommend for SLO with a Shibboleth IdP 3.3.
How to make an SP SLO compliant (1/4)

- Prepare your SPs for SLO
  - The SP will profit of local logout immediately and of SLO once the IdP is SLO capable

![AAI Resource Registry](image)

**AAI Resource Registry Federation Login**

You were successfully logged out from the Resource Registry. To completely log out from all applications that you are still logged in, please quit your web browser.

**Login**

Please select your organization in one of the drop down lists below. Then authenticate in order to get access to the Resource Registry.

<table>
<thead>
<tr>
<th>SWITCHaai Federation</th>
<th>AAI Test Federation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login with: SWITCHaai</td>
<td></td>
</tr>
<tr>
<td>VHO - Virtual Home Organization</td>
<td></td>
</tr>
</tbody>
</table>

The above drop-down list contains all organizations currently participating in the production SWITCHaai infrastructure.
How to make an SP SLO compliant (2/4)

• User initiates Logout from a page without frames

• Replace in shibboleth2.xml the <Logout>Local</Logout> element with <Logout>SAML2 Local</Logout>

• Terminate the web application session
  • Case a) web application has no session management
    → sufficient to terminate the SP session
  • Case b) web application has own session management
    • Application session timeout ≤ SP session timeout.
    • Application has a mapping: internal session ID ↔ SP session ID.
    • SP needs to be able to end the web application session.
      → Add a <Notify> element to shibboleth2.xml
      This points to the web application’s logout link. At the end, the application must redirect to the return link provided as query parameter.
How to make an SP SLO compliant (3/4)

• **Additional requirements for non-Shibboleth SPs**
  
  • SP must support HTTP-Redirect binding.
  
  • SLO requests MUST be signed.
  
  • The `<saml:NameID>` element in `<samlp:LogoutRequest>` messages MUST NOT be encrypted.
  
  • SLO responses MUST be signed.

These requirements were derived from the draft
**SAML V2.0 Interoperability Deployment Profile V1.0:**
https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
How to make an SP SLO compliant (4/4)

• Behavioral requirements
  • SPs MUST terminate a subject’s local session before issuing a `<samlp:LogoutRequest>` message to the IdP.
  • SPs MUST NOT issue a `<samlp:LogoutRequest>` message as the result of an idle activity timeout.
  • Only publish a SLO service location in the Resource Registry once all the requirements are met. → This avoids bad user experience.

• Virtual Hosting Limitations
  • An SP that maintains distinct sessions across multiple virtual hosts SHOULD identify itself by means of a distinct entityID (with associated metadata) for each virtual host.
    → A single entity can have only one `<SingleLogoutService>` endpoint per binding.
What you should know about SP SLO

Five independent sessions at IdP, SP1, app1, SP2 & app2

• End of SP session does not necessarily imply end of Application session.
• Each session has its own timeout. Ensure: $SP_{\text{timeout}} \geq App_{\text{timeout}}$
• **User has to initiate SLO.** A timeout should **never** trigger SLO.
SP Single Logout in action (1/12)

1) User clicks Logout within **Application 1**
SP Single Logout in action  (2/12)

2) **Application 1** ends its session
3) **Application 1** redirects to **SP1 Logout**
4) **SP1** ends its session
5) **SP1** redirects to **IdP Logout**
6) **IdP** ends its session
7) **IdP** offers choice for **Logout all** or **Stay logged in**
SP Single Logout in action  (8/12)

8) **IdP** calls **SP2 Logout** in a frame

User clicked on:

Log out of all services
9) **SP2** redirects within the frame to **Application 2** logout

[Diagram showing SP Single Logout in action]
10) **Application 2** ends its session and redirects to **SP2 Logout**
11) **SP2** ends its session and redirects back to **IdP**
12) IdP reports success
Single Logout Guide

• Initially it will be for SP only, based on the content of these slides.

• Once the issues are solved on the IdP side, an SLO guide for IdP will follow.

• Ensure a good user experience: Register a SLO Service Location only once you are sure that the entity is capable to handle SLO properly.
SWITCHpki News

Andres Aeschlimann
andres.Aeschlimann@switch.ch

Bern, 14.3.2018
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
Situation in 2016

- Symantec: 31%
- Comodo: 20%
- GoDaddy: 20%
- GlobalSign: 7%
- DigiCert: 6%
- GoDaddy: 4%
- Entrust: 4%
- StartCom: 2%
- Let's Encrypt: 1%
- NetSeal: 5%
- Others: 3%

We are grateful for the information in this presentation provided by our partner WiseKey/QuoVadis
Situation in 2017

- Comodo: 28%
- GoDaddy: 18%
- GlobalSign: 13%
- DigiCert: 6%
- Let's Encrypt: 5%
- Entrust: 2%
- Others: 0%
Let’s Encrypt

• Increase in market share from 4 to 28% in one year
• DevOps minded: Automation and scalability in everything they do
• DV means: Keep encryption, while leaving identity
• Certificates have a lifetime of 90 days
• Everything newly developed
## More statistics

<table>
<thead>
<tr>
<th></th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Certs</td>
<td>5.2 Mio</td>
<td>5.7 Mio</td>
</tr>
<tr>
<td>ECC Certs</td>
<td>24’000</td>
<td>370’000</td>
</tr>
<tr>
<td>Short lived (&lt;2 months)</td>
<td>480’000</td>
<td>1.2 Mio</td>
</tr>
<tr>
<td>EV Certs</td>
<td>~ 5%</td>
<td>shrinking</td>
</tr>
</tbody>
</table>
Shorter validity of certificates

• Once upon a time you could have certificates that were valid for 5 years
• Validity has now been cut down to 825 days (approx. 2 years and 3 months) by the CA Browser Forum (*pushed by the browser companies*)
• Validity of only one year is foreseeable
• Let’s Encrypt is already at 90 days
More facts and trends

- Automatic Certificate Management Environment (ACME) becomes an IETF Specification:
- Certificate Transparency has now an RFC:
- Next step: all new trusted SSL certificates must be logged by CA’s by April 2018.
  https://casecurity.org/2017/05/03/certificate-transparency-deadline-moved-to-april-2018/
- DevOps (Let’s Encrypt) predominant
- Squeeze on small providers
- Google is setting up their own trust services
- So does Amazon
The role of SWITCH

1. Closely watch the market
2. Share information and report back to the Community
3. Listen to you
4. Find appropriate solutions for the Academic Community
5. Go to step 1
Links

https://www.ct-observatory.org/
Consequence of CT

https://crt.sh/?zlint=1+week&dir=^&sort=7
Links

https://cabforum.org/baseline-requirements-documents/
SWITCH edu-ID Liaisons

Christoph Graf
christoph.graf@switch.ch

Bern, 14.03.2018
Academic community Switzerland
Academic identity
Federations worldwide

Third party services
e.g. publishing houses

national

international

academic sector

other sectors

© 2018 SWITCH | 4
The existing SWITCH identity federation

The potential future identity federation of the schools

• Mandate of EDK/CDIP to educa.ch under review
• Contact EDK/CDIP-SWITCH established
Liaison with **SwissID**

Existing customer base: 450'000

expected customer base 2019: 4'000'000

Potential collaboration benefits:
- «easy onboarding» in both directions
- Simplified cross-resource access
- E-ID functions?
- Member benefits (e.g. «studentness»)?

Informal, regular information exchange established
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
Supporting Organization Integration

Functionality required for UniL, UniSG, ZHAW

• **Organizational administration interface:**
  to maintain security, support, identity management and other administrative processes at organizations.

• **Support for local and bilateral attributes**

• **Affiliation push-API**

• **Support for technical accounts:**
  Non-personal accounts for monitoring, testing, and other special purposes.

• **Account linking after admission:**
customizable linking service
Functional extensions

• Integration with Microsoft Products:
  – SPNEGO/Kerberos authentication
  – Authn with edu-ID for on premise services like Exchange
  – Authn with edu-ID for cloud services like Office 365

• Group Management (GM)
  – VHO replacement
  – Evaluate and test generic GM system run by SWITCH
  – Develop concept and test integration of externally operated GM

• Strong authentication

• OpenID connect provider:
  for mobile and web applications

• eduroam integration
What’s new @ SWITCH Q1/18

• **Community Service Hub**
  POC will be completed end of February
  [swit.ch/csh](http://swit.ch/csh), sebastian.sigloch@switch.ch

• **Community Think Tank**
  First steps: surveys and interviews
  christine.lanner@switch.ch

• **Coordination office on scientific information**
  Conceptional work together with swissuniversities

• **Check service availability**
  [status.switch.ch](http://status.switch.ch)

• **SLSP @ SWITCH**
  Subtenants from 1 March 2018 at SWITCH premises
What’s new @ SWITCH Q1/18

Security
• SWITCH-CERT
  - Mattermost for NREN
cert@switch.ch

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

Network
• Service Platform Higher Education Science DMZ
  - Interdisciplinary network and security workshop
together with higher education
daniel.bertolo@switch.ch
silvio.oertli@switch.ch
martin.leuthold@switch.ch

Trust & Identity
• SWITCH edu-ID
  - Deployment step 2
christoph.graf@switch.ch

  - First T&I WG-Meeting, 14 March 2018
switch.ch/edu-id/events/register-trid-wg/

  - Read our Blog
identityblog.switch.ch

Infrastructure & Data Services
• SWITCHengines
  - are now qualified for SNF funding
  - storage and data solutions started with universities
konrad.jaggi@switch.ch, switch.ch/engines

© 2018 SWITCH | 2
Save the date!

The next edu-ID update will take place on

Wed, 27.6.2018

https://help.switch.ch/eduid/
Working for a better digital world