eduroam.ch

Christian Rohrer
What is eduroam?

• Wireless roaming service for higher education

• From local campus to locations across the globe

• Based on 802.1X standard and a hierarchy of RADIUS proxy servers
eduroam @ TRID WG Meeting?

Sign-in once
Authentication/Authorisation
Authentication Server (IdP)
@Home Organisation

Access wherever you are
Network Access
Authenticator (SP)
@Current Position

RADIUS
EAP

Access Point
Ethernet Switch

© 2020 SWITCH | 78
• Web application providing users with eduroam profiles using their edu-ID accounts
• Device-specific profiles using eduroam CAT tool
• Secure technology: X.509 user certificates, not username/password
eduroam.ch | Authentication & Authorisation

- Regular process: Supplicant > Authenticator > RADIUS

- RADIUS server
  - Checks for an edu-ID account (Authentication)
  - Gets current affiliation from the edu-ID IdP (Authorisation)

- Access decision ultimately granted by the Authenticator
eduroam.ch | Wait, there is more

• End-User Support
• Monitoring and metrics

• VLAN Assignment (Guest network) on road map
  – Server side: RADIUS server sends VLAN group along
  – Client side: Authenticator gets the edu-ID attributes needed for VLAN group decision
eduroam.ch | Current Status & Outlook

• Running as a pilot, somewhat limited feedback

• Survey among heads of IT about interest in the service

• Let your boss know if you see potential for eduroam.ch at your organisation
Thanks! Questions?
Migration Roadmap: Who’s next?

Rolf Brugger
Project Plan to Integrate edu-ID at a University

Kickoff → Concept, Planning → Implementation
• Linking Service
• Affiliation sync → Changeover → Cleanup, debriefing

Communication

Day X
Coordination of Time Slots for Migration

• Most intensive collaboration between SWITCH and migrating organization
  – Testing of linking app
  – Testing of affiliation synchronization
  – Testing of most important services

• Coordination of time slots for testing and changeover

https://switch.ch/edu-id/organisations/adoption/upcoming/
Status P-5 Project

Christoph Graf
Swiss edu-ID project roadmap 2014-2020

Development

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

Deployment / Adoption

- Depl. Step 1
- Depl. Step 2
- Depl. Step 3
- Depl. Step 4
Additional call for participation due to COVID-19:
- Last chance to secure project funding
- Project runtime July-Dec 2020
- Contact: eduid@switch.ch
The World around us

Christoph Graf
The identity neighbourhood

Supporting global research collaboration

SwissID

National E-ID

Swiss schools’ identity federation

© 2020 SWITCH
E-ID status and outlook

• The E-ID law
  – Loi sur les services d’identification électronique / Bundesgesetz über elektronische
    Identifizierungsdienste
  – Passed Sept 2019 in parliament
  – Referendum against the law succeeded 16 Jan 2020

• Next steps
  – E-ID directive (ordonnance / Verordnung) expected summer/autumn
  – Vote on E-ID-Law Nov 2020 at the earliest

• Working group of potential E-ID-IdPs of Federal Office of Justice
  – Potential IdP-operators as per the E-ID law were invited
  – SWITCH is participating (helps us to assess our role as IdP or RP)
E-ID: what’s in for SWITCH?

• Elements of the Swiss E-ID
  – **User attributes**: the core function of any E-ID; useful for signup processes, age verification, attribute validation, etc.
  – **Login function**: to e-Gov and other services; promising to reduce credential sets (e.g. “less passwords to remember”)

• Relevance to SWITCH
  – **User attributes**: interesting for SWITCH edu-ID to increase quality level of self-provided attributes (as IdP or relying party)
  – **Login function**: unlikely to attract interest
Edulog status and outlook

• Edulog: The identity federation of the primary and secondary schools, run by educa.ch
  – Governed by the cantons
  – Built on similar standards and principles as AAI and edu-ID
  – Federating IdPs of cantons, municipalities or schools with the help of a central SAML proxy

• Technical operator selected in January 2020: ELCA
• Federation production services to start Aug 2020 (schoolyear 20/21) with 5 cantons participating (BS, BL, FR, GL, VS)
• Growth will take time, not all cantons and schools are ready
Edulog: what’s in for SWITCH?

• Cross-federation use cases between schools and tertiary education
  – Pupils eventually become students
  – PH-students return to schools for practical training
  – PHs offer continued education to school teachers

• Interoperation scenario
  – Integration level rather low between Edulog and SWITCH edu-ID (limited to some form of identity linking)
  – Simple to implement for SWITCH and Edulog, but user-friendliness somewhat limited
Supporting life long learning, research and collaboration

Maarten Kremers
SURF
Trust & Identity WG Meeting and
SWITCH edu-ID Update Event 2020
Virtual – 20th May 2020
Why eduID?

- Student mobility
- Flexibilisation
- Life long learning
- Identity across institutions
- Central approach, not an approach per organization
- Tailored to educational domain
Characteristics of the eduID

• Identity for students
• Life long usable
• Under the control of the user
• Respects privacy
• Increase level of assurance
• Enrich with attributes from external sources
Possible interpretations of the eduID

- A number, the "ID"
- An identity based on attributes
- An account based on identities
- A login service unlocking accounts

Set of rules & regulations
Examples usage eduID

- Micro-credentials
- Register to education
- Courses at second institution
- Collaborative curriculum
- End of study
- After study
- Using Own eID

Pilot 2020
What does eduID offer for educational institutions?

- Lowering administrative burden of student mobility and increased collaboration between institutions
- Better GDPR position as the student is in its own control his data
- More certainty with regards to the digital identity of students in data exchange between institutions
- Better support for identification of target groups who normally are not or no more in the student information system: Prospects, guests, ‘external’ students, alumni
- Harmonization in recognizing “internal” and “external” students
- In the long run as a replacement for the current institutional identity
What does eduID offer for students

• Better and simpler administrative process for taking courses at other institutions
• The student is in control of its own information
• Supporting life long learning, student is recognizable over the course of his whole learning carrier
• A solid and simple solution to access educational systems, an eID systems for education
Current status eduID

- Proof-of-Concepts
- pilot eduBadges
- pilot student mobility
- In production: Guest IdP (IdP of last resort)
Guest IdP

edulD: 1 account for education and research

An edulD is an account for users within education and research in the Netherlands. It is yours and exists independent of an educational institution.

You can use edulD to login to several services connected to SURFconext. edulD is meant for users who do not have an account with an institution or for services where an institution-independent account is useful.

edulD is still under development. In the future, you will be able to use edulD for many more things. For example, you can use edulD after your studies, as an alumnus, or during your studies, if you wish to follow classes at several institutions simultaneously.

Guest IdP
In production per Q2 2020
What will we do in 2020?

1. Follow-up pilot edubadges and support service development edubadges

2. Start-up student mobility pilot:
   Goal: registering for an educational course with '1 click'.

3. Making eduID core functionalities available for use via SURFconext
Student Mobility Pilot

It should become easier for students to follow educational courses outside their own educational institutions.

• Website with educational courses that can be followed
• Registering for a unit of study at another institution is done with '1 click'.
• Personal data is exchanged with the student's consent.
• At all times, the student has at least insight into, but preferably control over, the exchange of data from and about him/her.
• The infrastructure is applicable at other institutions and can be scaled up both inside the alliance as outside.
• Start for academic year 2021-2022.
What will we do in 2020?

Core Development:

1. Pass eduID number at login via SURFconext
2. Digital identity to login
3. Security and privacy for data exchange
Let’s have a break… …until 11:00
Consequences and future developments

Andres Aeschlimann
Overview

• Future of the IdP Hosting Service in the light of the SWITCH edu-ID

• Shibboleth IdP Roadmap
Future of the IdP Hosting Service

• Organisations are adopting the SWITCH edu-ID one by one
• They don’t need an own IdP any more
• Question yourself (as an organisation):

  *Do we still need an own IdP?*
Future of the IdP Hosting Service

- The number of IdP Hosting instances has already started to decrease
- IdPv4, IdPv5: More work for less customers

*Phase-out will be an option!*
(No) Future of the IdP Hosting Service:

*IdP Hosting won’t remain a SWITCH service in the medium term*
Shibboleth IdP Roadmap

• Shibboleth IdPv4 was released on 11. March 2020
  • Many old configuration elements dropped. Eliminate first all deprecation warnings in IdPv3.4
  • Thereafter, in place upgrade from IdPv3.4 strongly recommended
  • See the Wiki for more details: https://wiki.shibboleth.net/confluence/display/DEV/Project+Roadmap#space-menu-link-content

• No more detailed IdPv4 Installation Guide planned, the guide for IdPv3.4 is the final one.

• SWITCHaai will provide relevant configuration files suitable for IdPv4+, like
  • attribute-resolver-*.xml, metadata-provider-*.xml, services.xml
  • attribute-filter_v4.xml (dynamically provided by the Resource Registry)
SWITCHaai News

Thomas Lenggenhager
SWITCHaai News Overview

• Phasing out TLS 1.0 & TLS 1.1

• Not forgotten: Metadata Query (MDQ)

• Shibboleth IdPv4: New default XML encryption algorithm

• The Attribute Release Inspector in the Resource Registry
  It’s your friend!
Phasing out TLS 1.0 & TLS 1.1

- These protocols are obsolete: Grade capped to B
- Attribute Viewer, RR & WAYF-Test require TLS 1.2: Grade A+
- Most IdP Hosting IdPs warn users on login page referral to http://browsertest.aai.switch.ch
- Require TLS 1.2, block TLS 1.0 & TLS 1.1:
  - On **Thu 2. July 2020** for these IdPs: SWITCH eduID, adopted organizations & IdP Hosting customers
  - On **Wed 5. August 2020** for WAYF
- Check your own web server configurations, consult the Mozilla SSL Configuration Generator: https://ssl-config.mozilla.org
Not forgotten: Metadata Query (MDQ)

• Growing number of SAML entities ➔ Metadata file size increases

• This mainly affects the interfederation enabled IdPs & SPs
  • Consider to increase the RAM and Tomcat’s heap allocation!
  • Not affected are the vast majority of SPs registered in SWITCHaai

• If the SWITCHaai federation would support the Metadata Query Protocol, IdPs and SPs could load metadata only on request, when needed.
  • Some international federations started to support it.
  • We see no urgent need yet, it’s on our watch list.
Shibboleth IdPv4: New default XML encryption algorithm

• Be careful in case you plan to update to IdPv4 or install a new IdPv4 IdP:
  • The default XML encryption algorithm changed
    Now it is AES128-GCM, up-to-now it was AES128-CBC
  • Old Shibboleth SPs and most other SP implementations will not interoperate with the new default.
  • Check out the details in the IdPv4 Release Notes: https://wiki.shibboleth.net/confluence/display/IDP4/ReleaseNotes
  • We intend to enhance the Resource Registry, so that SPs will be able declare the encryption algorithms supported. Modern IdPs will know when to apply the safer XML encryption algorithm.
eduGAIN Enabled Services and their Attribute Requirements
- The Attribute Release Inspector in the Resource Registry is your friend

Lukas Hämmerle
Problem

• Sometimes users end up at eduGAIN service like this:

![Error Message]

• IdP did not release all required attributes to SP
What is the Attribute Release Inspector?

• Tool to show **which attributes are released** by a specific Identity Provider (IdP) to a specific Service Provider (SP)

• Works for SWITCHaai and Interfederation/eduGAIN SPs
For whom is it useful?

- **Service Provider admins:**
  - Check if a SWITCHaai Identity Provider releases attributes to services

- **Identity Provider admins:**
  - Check if default/specific attribute release rules allow release of a particular attribute to an SP

Helps debugging attribute release problems!
How does it look like? – Selection form

Attribute Release Inspector for 'GÉANT Service Provider Proxy'

<table>
<thead>
<tr>
<th>Relying Parties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Select Federation</td>
<td>Interfederation</td>
</tr>
</tbody>
</table>
## How does it look like? – Result

**Attribute Release Rule of Home Organization 'SWITCH' for Resource 'GÉANT Service Provider Proxy'**

Create Specific Attribute Release Policy Rule for 'GÉANT Service Provider Proxy'

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Comment</th>
<th>Released by ldP</th>
<th>Regex</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required Attributes</strong></td>
<td><strong>All required attributes are provided.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td>Required according to eduGAIN metadata</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>Scoped affiliation</td>
<td>Required according to REFEDS Research &amp; Scholarship (R&amp;S)</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>Targeted ID/Persistent ID</td>
<td>Required according to eduGAIN metadata</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>Principal name</td>
<td>Required according to eduGAIN metadata</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td><strong>Desired Attributes</strong></td>
<td><strong>Some desired attributes are not provided.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Given name</td>
<td>Desired according to eduGAIN metadata</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>Surname</td>
<td>Desired according to eduGAIN metadata</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>Display name</td>
<td>Desired according to eduGAIN metadata</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>Affiliation</td>
<td>Desired according to eduGAIN metadata</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Where can I find the Release Inspector?

• Part of the AAI Resource Registry
  – Click on link shown for each Resource Descriptions in Resources tab
  – Or via “Home Organizations” tab for each Home Organisation
  – Or access “Attribute Release and Filtering Inspector” via “Home”
    https://rr.aai.switch.ch/view_attribute_release.php
Wrap-Up

Andres Aeschlimann
& Petra Kauer-Ott
No more 2-year-certificates

- TLS server certificates issued on or after September 1, 2020 00:00 GMT/UTC must not have a validity period greater than 398 days¹.

SWITCHpki News

Andres
Aeschlimann
Questions for the plenum?

- Success of the SWITCH edu-ID: Adoptions (UniFR)
- News flash
- P5 program
- SWITCH edu-ID and other initiatives (eduID @ SURFnet)
- Break
- Roadmaps (IdP Hosting, Documentation on IdP deployment)
- SWITCHaai News
- SWITCHpki News
Feedback (Petra)
Slides will be available

... at the usual place:
https://www.switch.ch/edu-id/events/trid-wg-2020/
Mark the date in your calendar

Next Trust & Identity WG meeting and SWITCH edu-ID Update event will take place

Wednesday, 19.5.2021