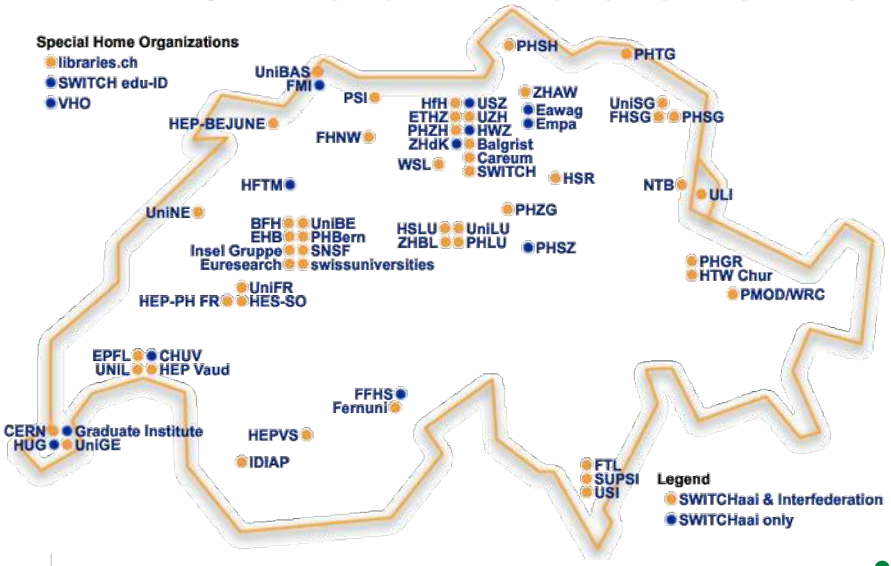
SWITCH edu-ID

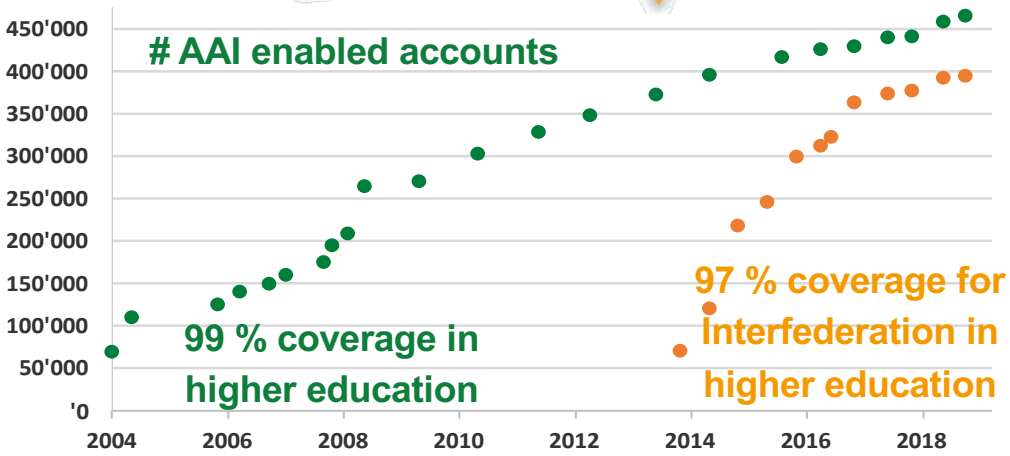
The project and beyond

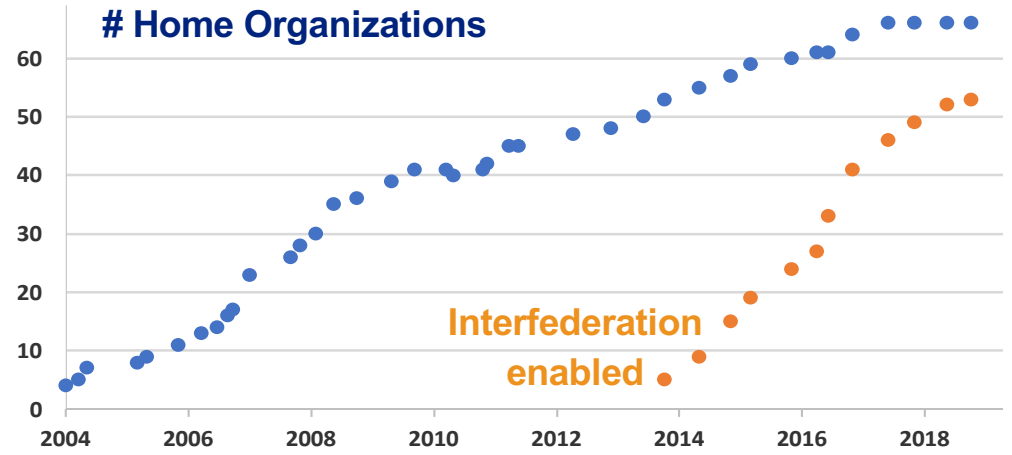
Christoph Graf
christoph.graf@switch.ch

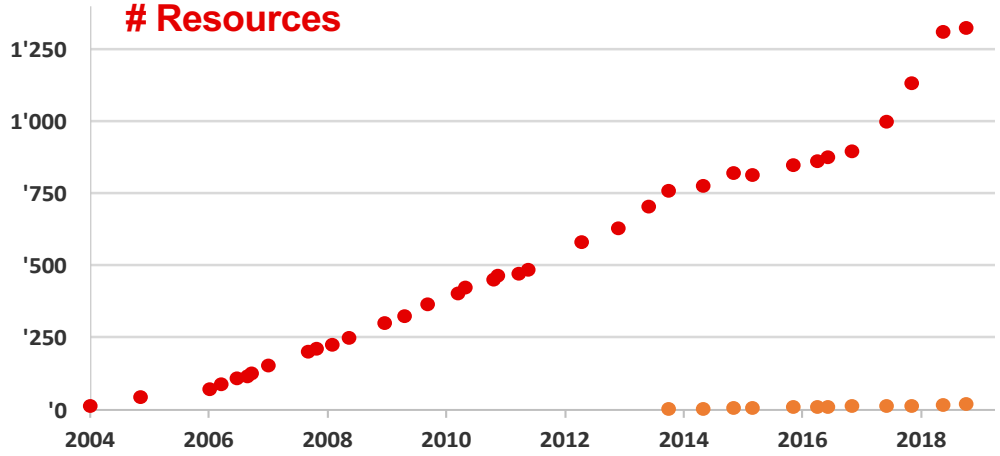
Zürich, November 13th 2018

SWITCHaai Federation Autumn 2018

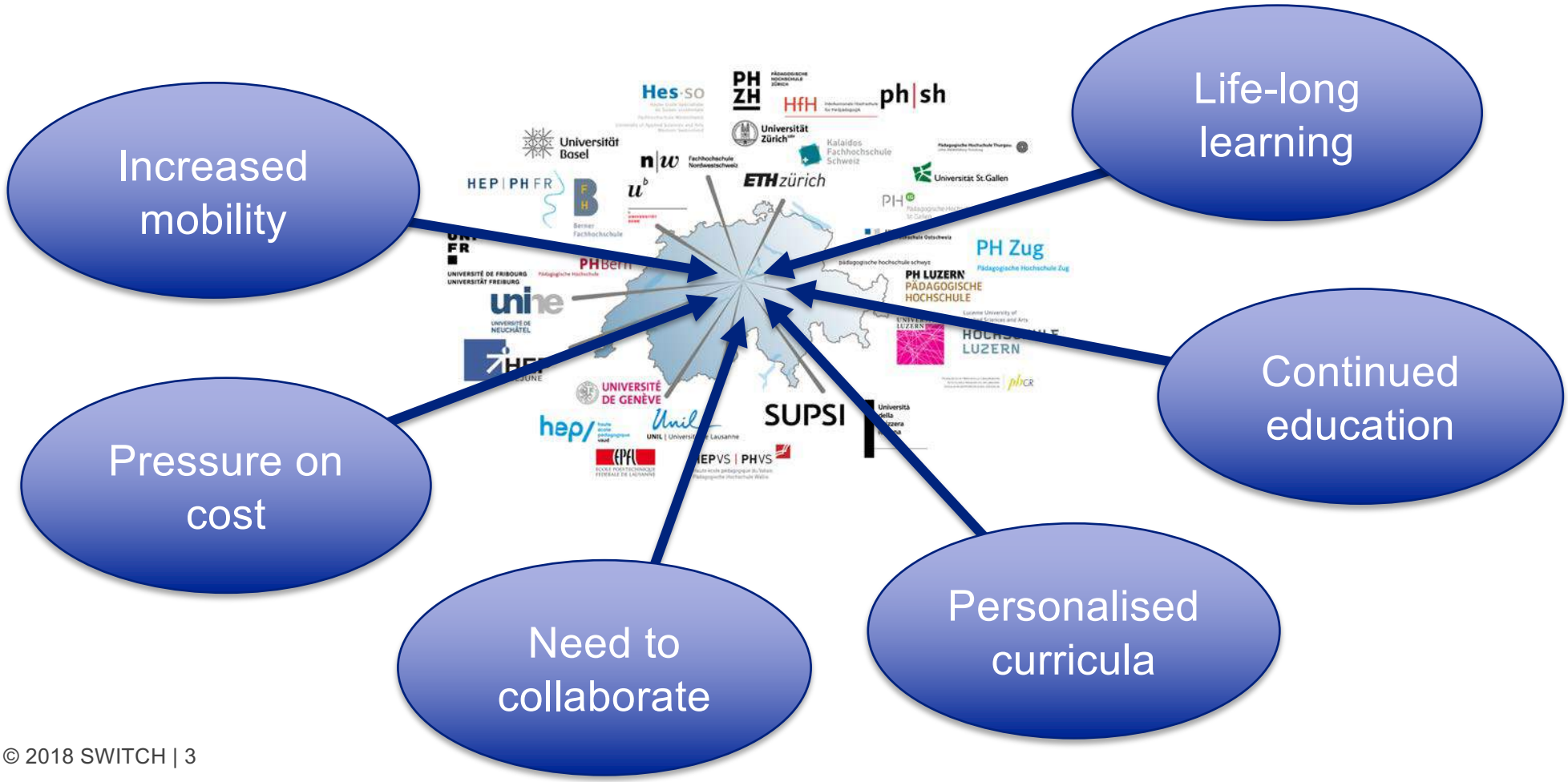




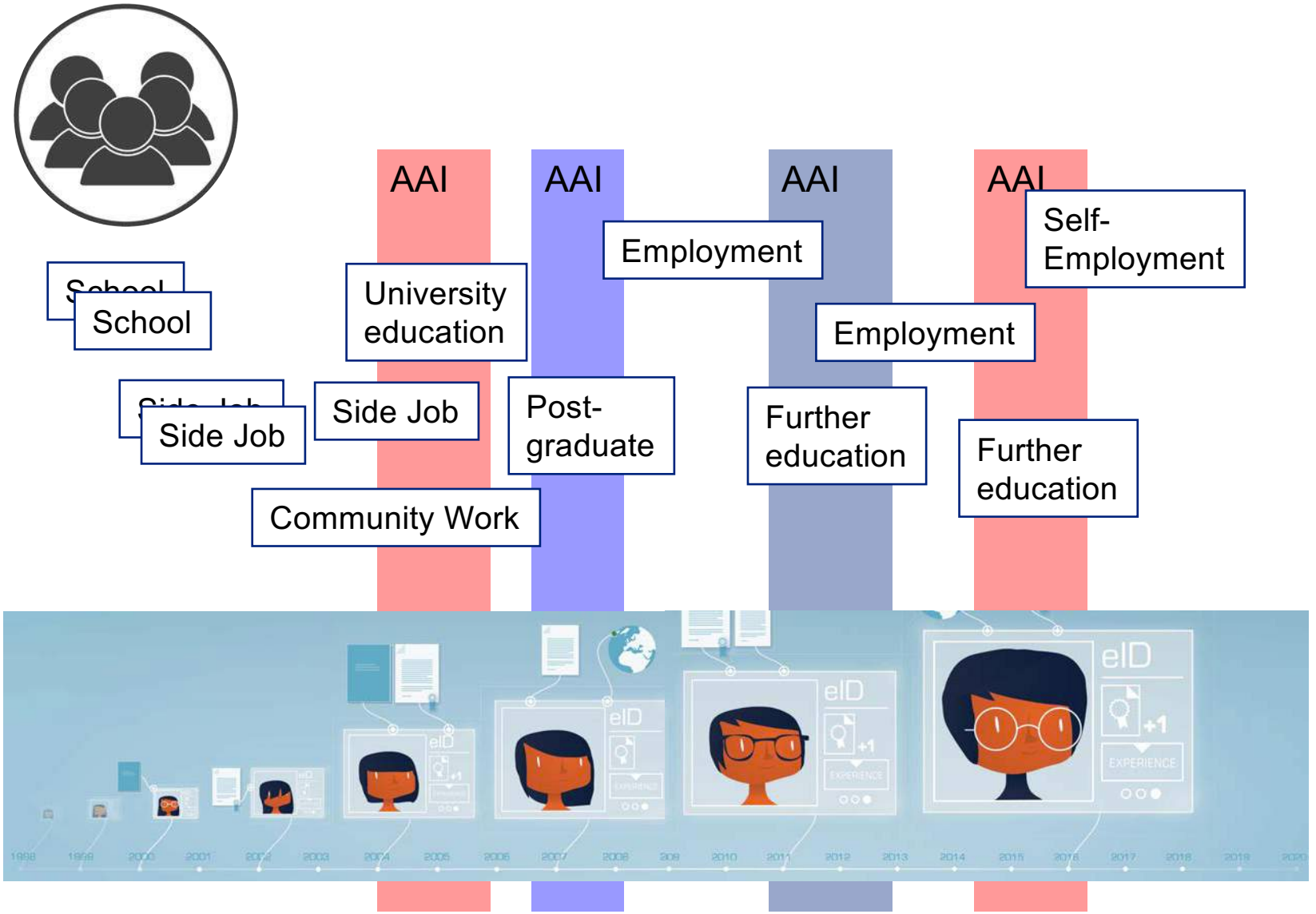




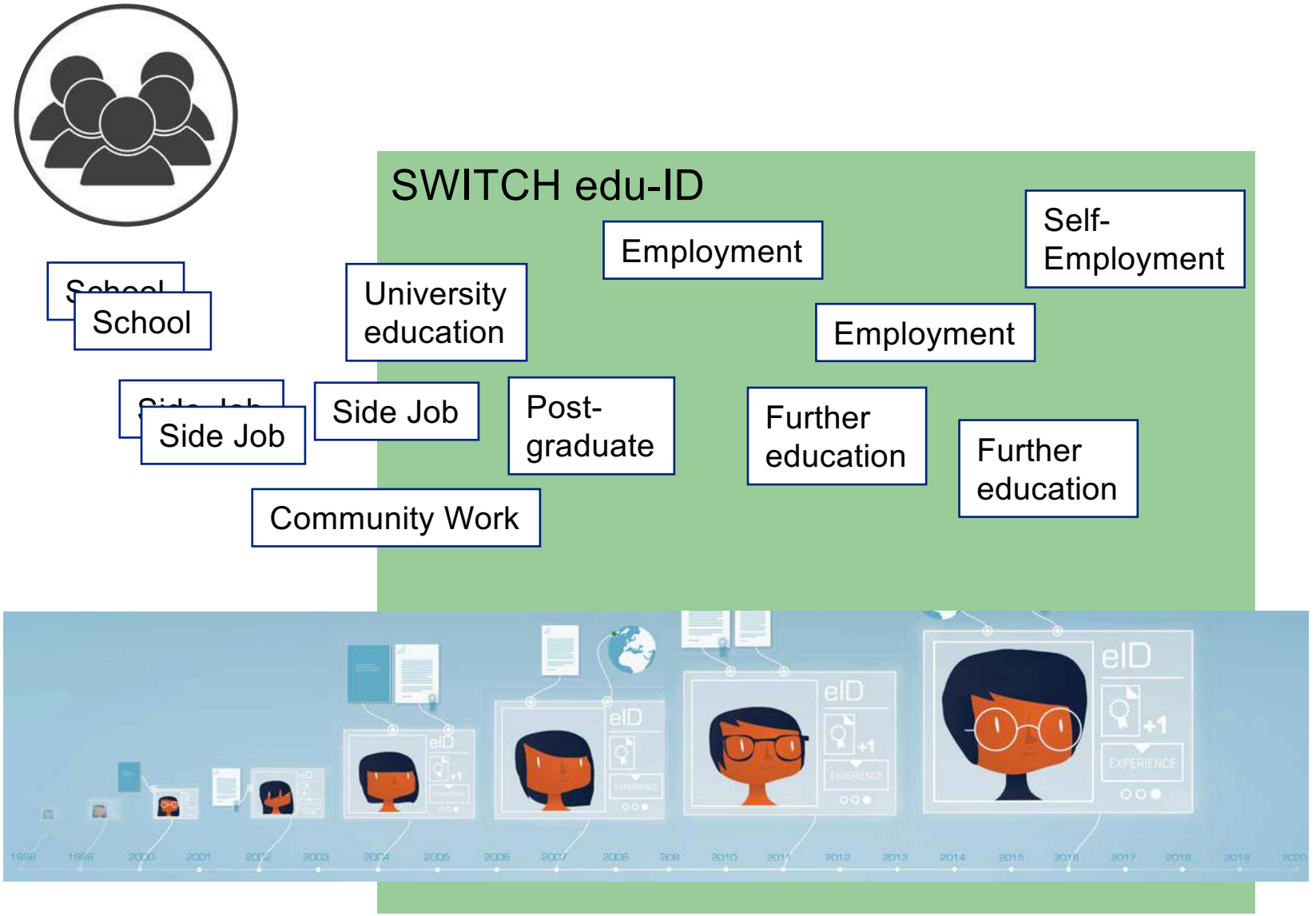
… new trends, new challenges & requirements



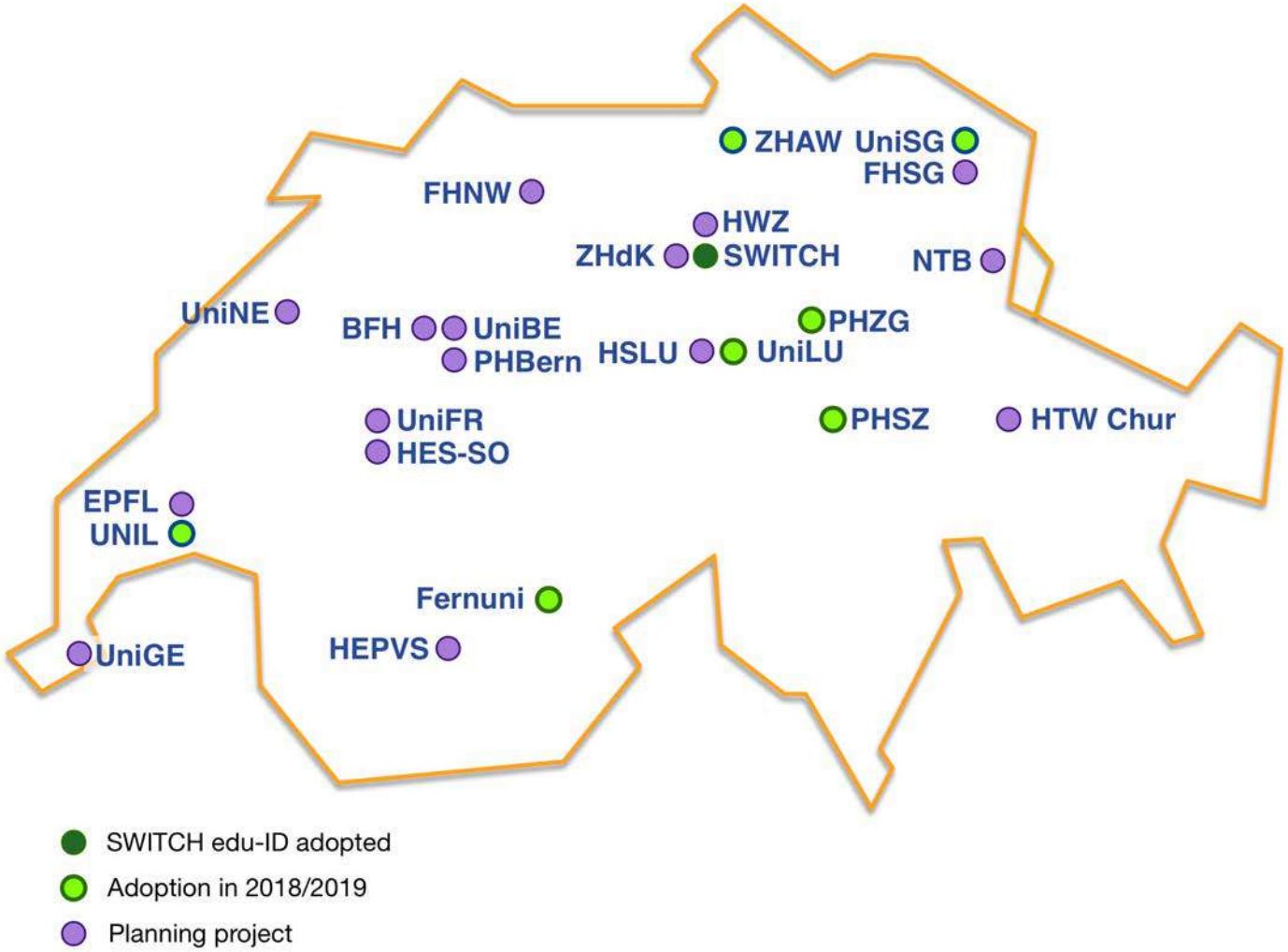
SWITCH


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

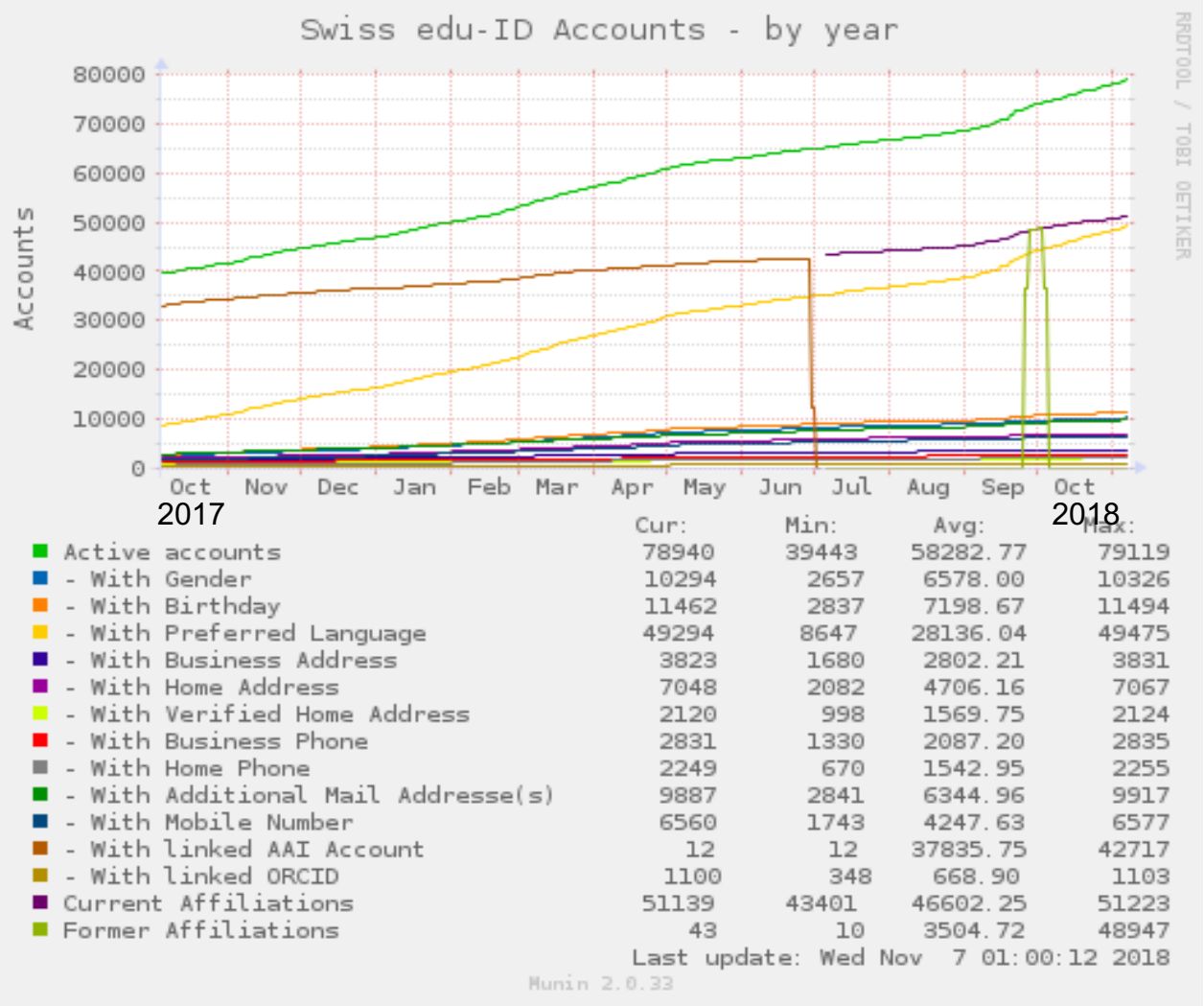
SWITCH


SWITCH edu-ID
School
School
University education
Side Job
Side Job
Post-graduate
Community Work
Employment
Employment
Further education
Self-Employment
Further education
eID
eID
eID
eID
+1
EXPERIENCE

Achievements 2018: a few institutions more …



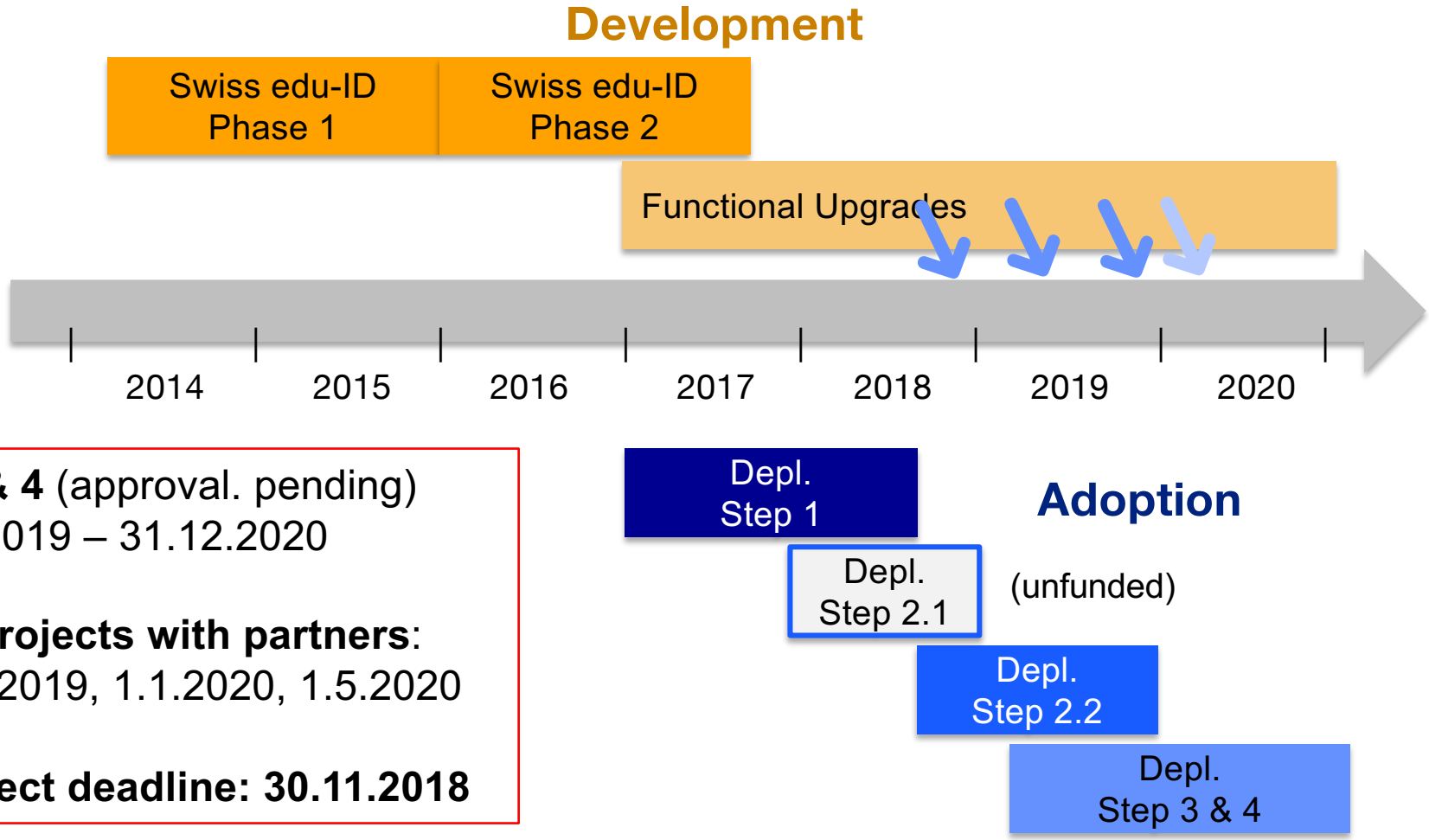
Achievements 2018: … and quite a few users more …



	Cur:	Min:	Avg:	Max:
Active accounts	78940	39443	58282.77	79119
- With Gender	10294	2657	6578.00	10326
- With Birthday	11462	2837	7198.67	11494
- With Preferred Language	49294	8647	28136.04	49475
- With Business Address	3823	1680	2802.21	3831
- With Home Address	7048	2082	4706.16	7067
- With Verified Home Address	2120	998	1569.75	2124
- With Business Phone	2831	1330	2087.20	2835
- With Home Phone	2249	670	1542.95	2255
- With Additional Mail Addresse(s)	9887	2841	6344.96	9917
- With Mobile Number	6560	1743	4247.63	6577
- With linked AAI Account	12	12	37835.75	42717
- With linked ORCID	1100	348	668.90	1103
Current Affiliations	51139	43401	46602.25	51223
Former Affiliations	43	10	3504.72	48947

Last update: Wed Nov 7 01:00:12 2018

Outlook 2019 (2/2): Project roadmap



Depl. Step 3 & 4 (approval. pending)
Duration: 1.1.2019 – 31.12.2020

Start of sub projects with partners:
1.1.2019, 1.7.2019, 1.1.2020, 1.5.2020

Next sub project deadline: 30.11.2018

Project «Swiss edu-ID Deployment Step 3&4»

Status update and what's different now?

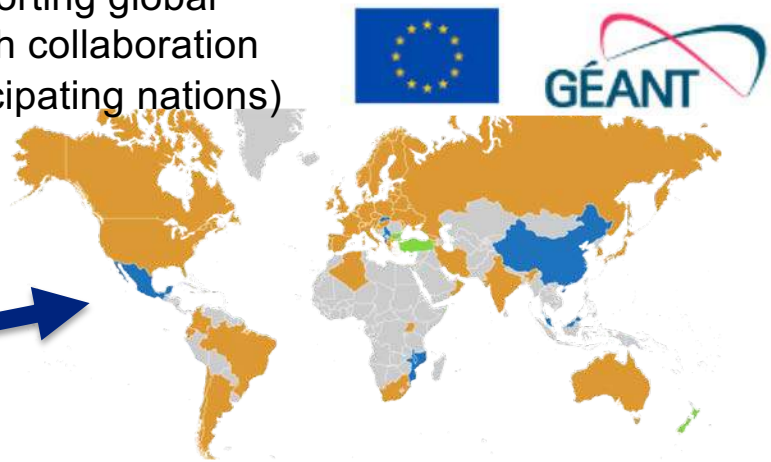
- Project submission August 2018 (in review at swissuniversities)
- Duration: 1.1.2019 – 31.12.2020 (until end of funding period)
- Scope is (again) limited to SWITCH edu-ID adoption planning, adoption implementation and functional extensions
- Contents and partners: rolling planning – **proposal defines the scope & processes, not the details**
- Partner: SWITCH, eligible partners to join later
- Funds: CHF 1'107'600 (60.5% reserved for partners)

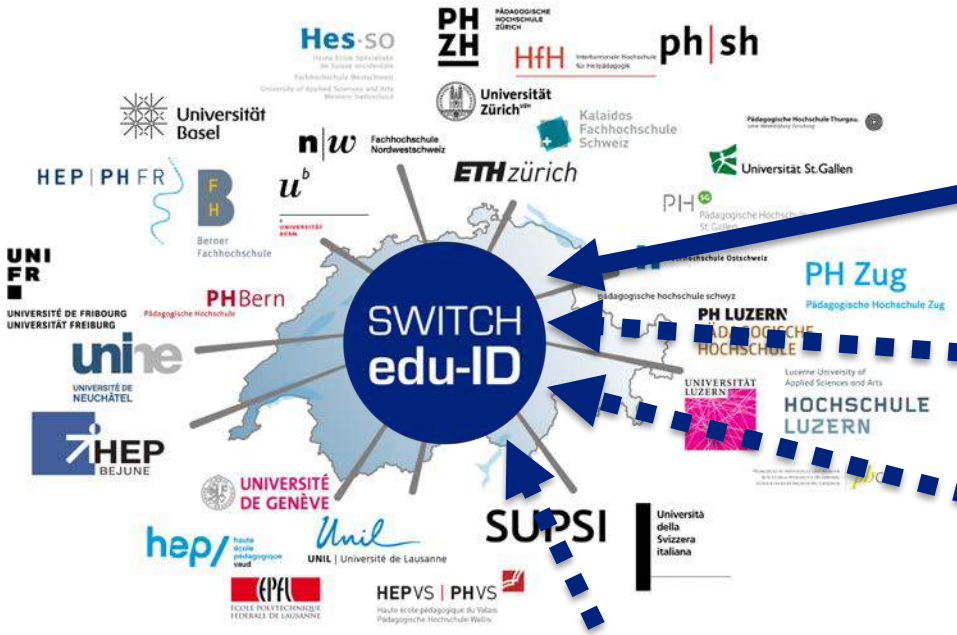
New joining process «Step 3&4»

- Subprojects may start at these dates: 1.1.19, 1.7.19, 1.1.20, 1.5.20 (as long as money lasts, 1 month's notice needed)
- **Next sub project deadline: 30.11.2018**
- Announcement and process information: https://identityblog.switch.ch/2018/10/09/submit-your-sub-project-for-planning-and-or-adoption/
- Subproject participation form to receive funding: https://projects.switch.ch/eduid/adoption/

Identity landscape

Supporting global research collaboration (58 participating nations)





SwissID i.e. for cross-sectorial collaboration use cases

E-ID law i.e. For validation use cases, now contributing to legal and technical implementation process

Project FIDES of EDK/CDIP

educa.ch ICT und Bildung · TIC et éducation · ICT e educazione · ICT ed educaziun

SWITCH supporting educa.ch for design and implementation of the identity federation of the Swiss schools

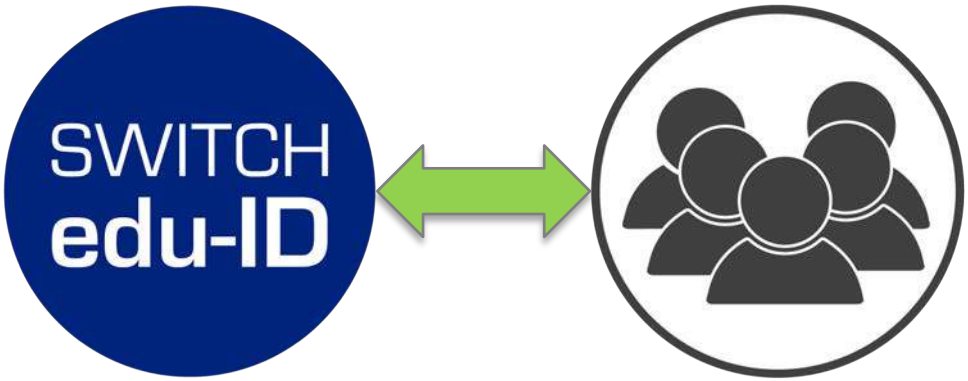
Improve Usage & ensure Privacy Compliance

SWITCH

Petra Kauer-Ott
petra.kauer@switch.ch

Zurich, 13.11.2018

Focus on Users (& Product)



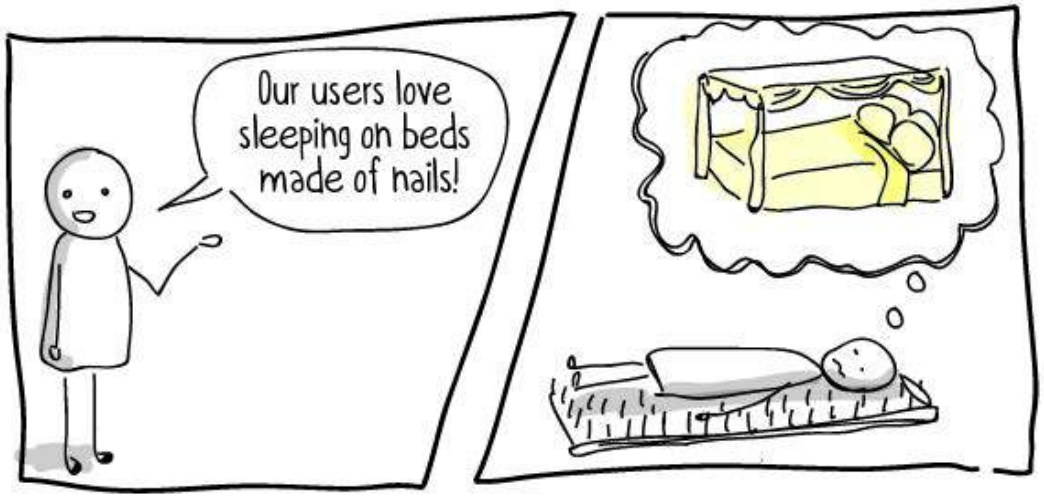
→ better user experience

→ less support / documentation

→ less rework

Tests with Experts & Users

Avoid:



swissuniversities

HTW Chur
Schweizerisches Institut für Informationswissenschaft

Bernard Bekavac,
Mara Hellstern, Yves Studer

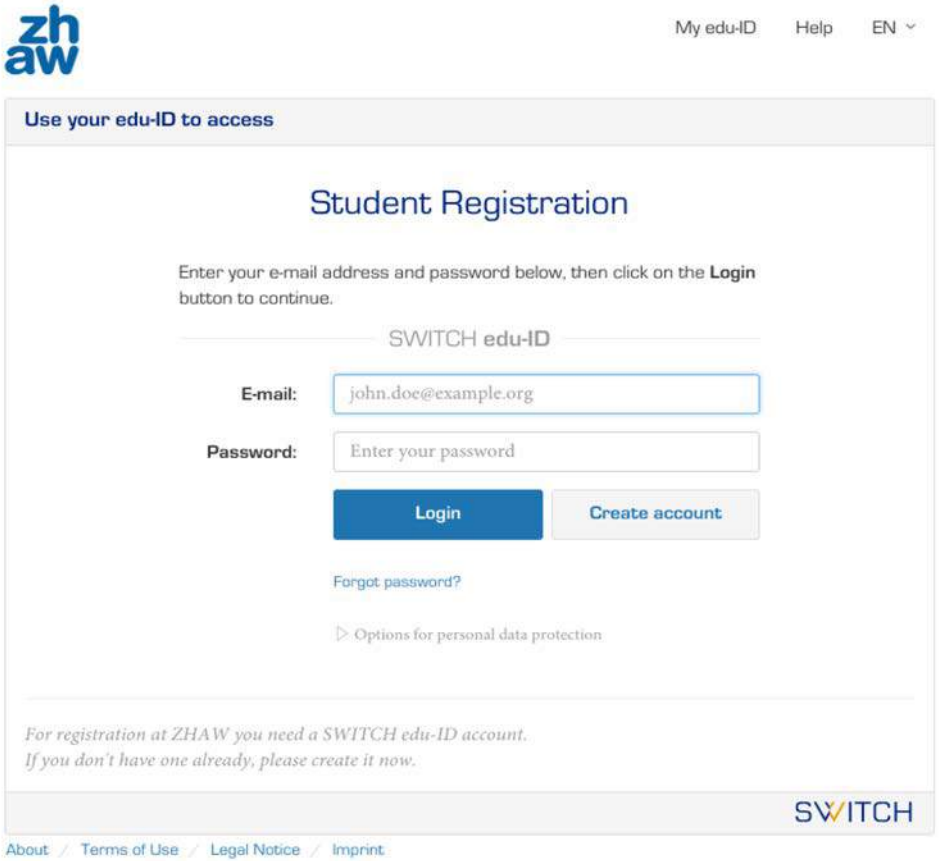
h e g
Haute école de gestion
Genève

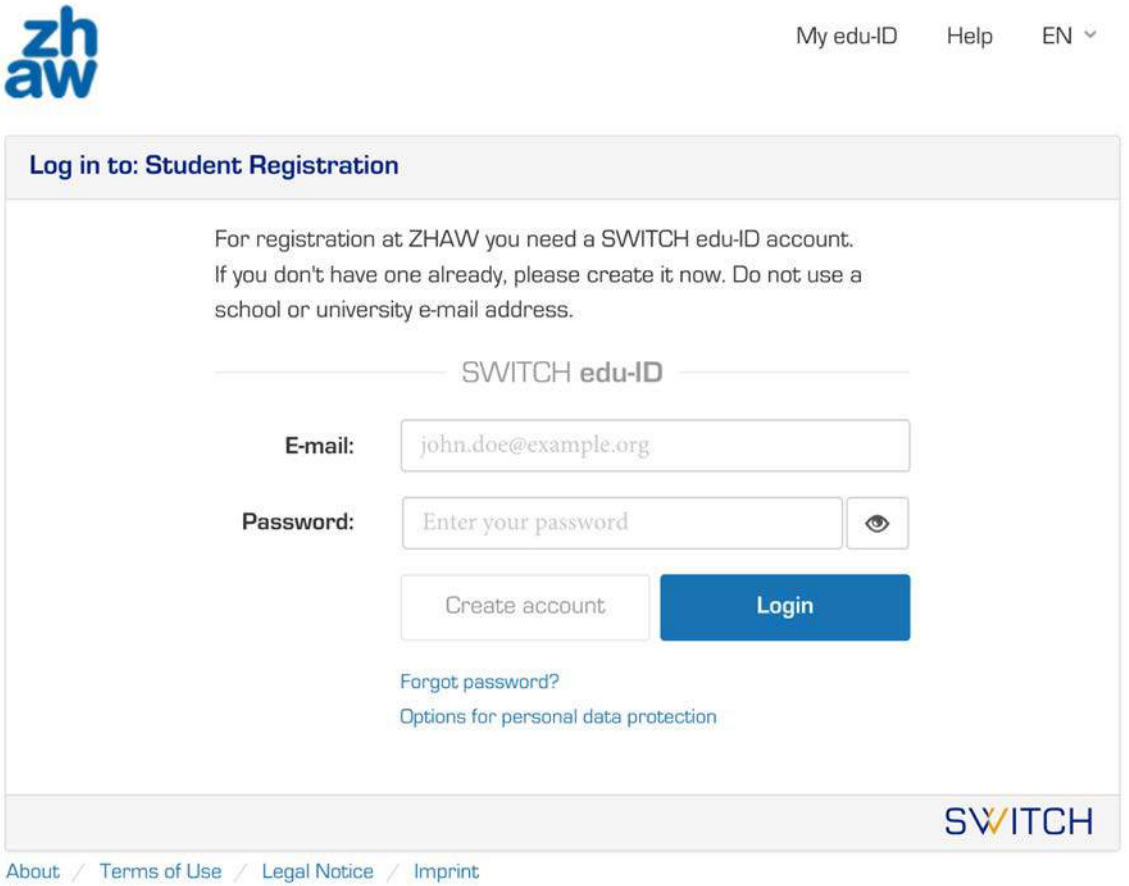
Dép. Information documentaire

René Schneider, Julien A. Raemy

Image Source: https://uxdesign.cc/a-crash-course-in-ux-design-research-ea00c3307c82

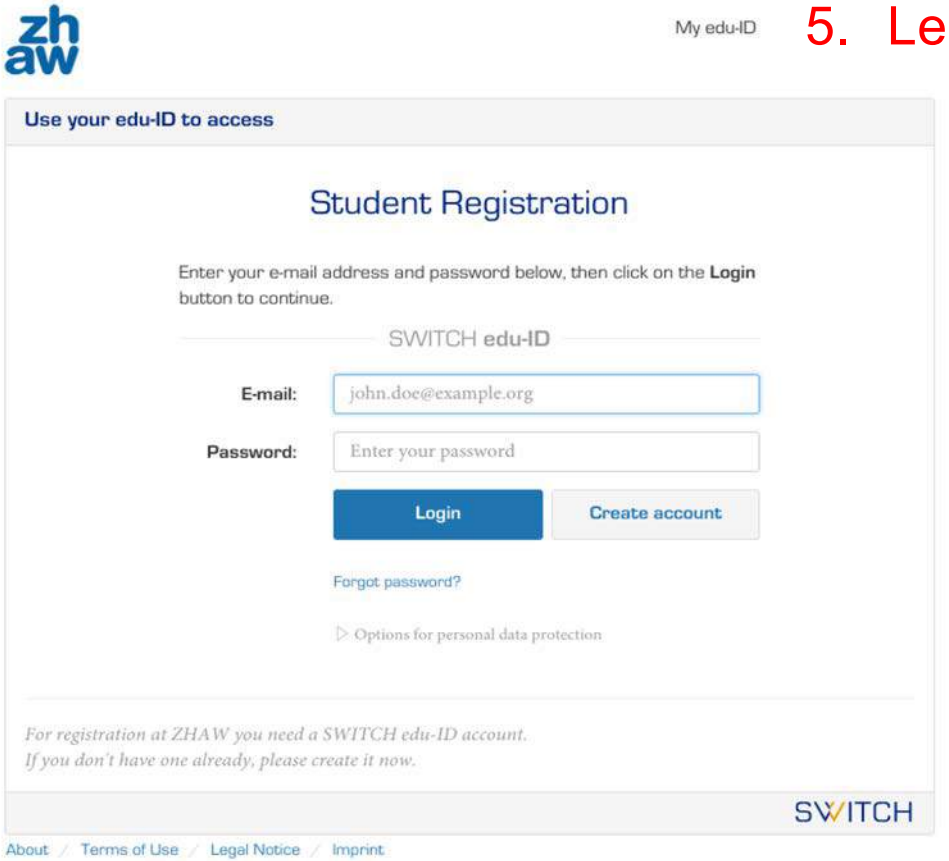
Find the differences!

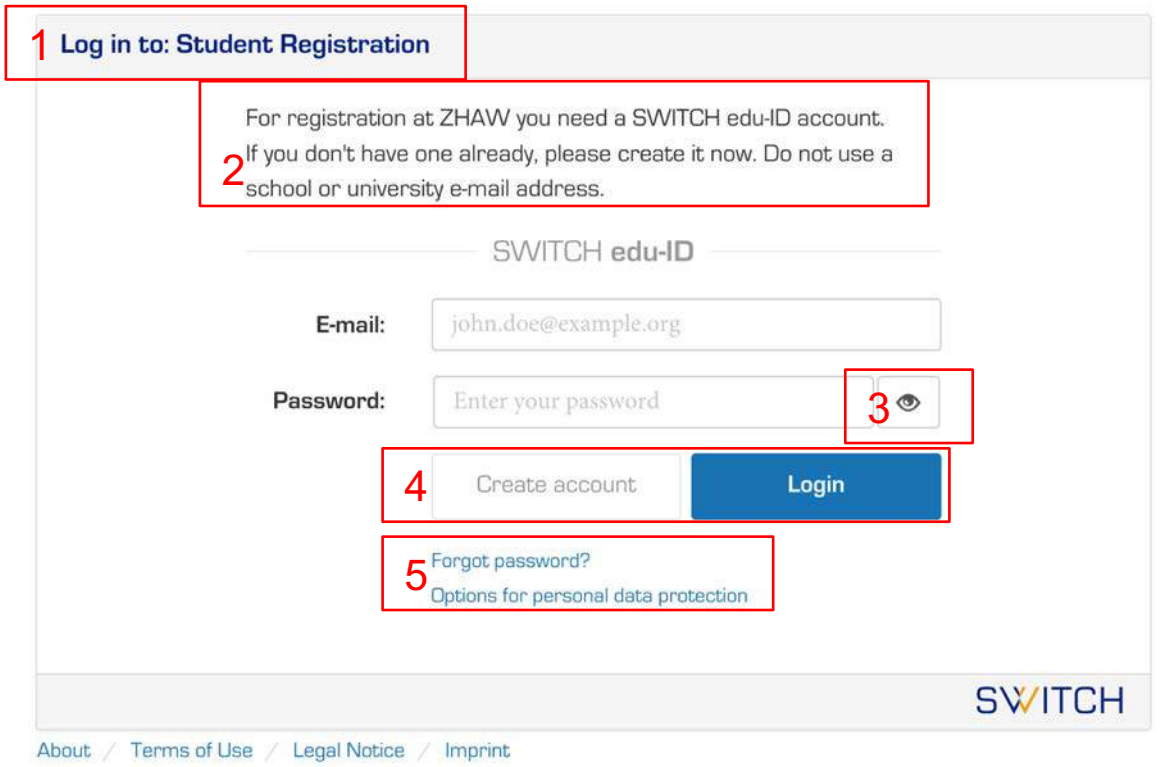




Found them?

1. Clear localisation
2. Purpose and instructions on top
3. Show password function
4. Favorite button on the right, buttons always visible
5. Less styles, easy setting for user consent





SWITCH

Good Grades but Space for Improvement

- clear and well programmed website
- easily to walk through
- proper guidance for the user to fulfil the interaction required

→ avoid loosing users by
  - fixing structural mistakes in the information architecture
  - using wizards, sequence maps and breadcrumbs

→ layout and design is accepted but could be improved (rational prosaic interfaces decrease acceptance)

→ reduce written text

→ mobile first

Some trade-off between usability, transparency and security necessary

Another Trade-Off …

Is edu-ID Data Protection Law Compliant ?

Data Protection
Law compliant

SWITCH
edu-ID

Done so far

- **Regulation WG:** Collect legal questions (2014)
- **Cantonal data protection officers:** Sent questions to them (2015)
- **Federal data protection officer:** Several queries because of expected written answer (2015 - …)
- **Law in CH and EU:** Legal developments observed (2014 - …)
- **E-ID consultation:** Participation (May 2017)
- **AHVN13:** Situation analysed with FHNW (2017)
- **SWITCH edu-ID database:** officially declared (2017)
- **Service Description:** published (federation policies adopted; 2018)

That’s good but…

- more insights (relevant questions)
- opinions of data protection officers
- interpretation with regard to future Swiss law and GDPR

Legal FAQs

https://swit.ch/edu-id_faqs

Example

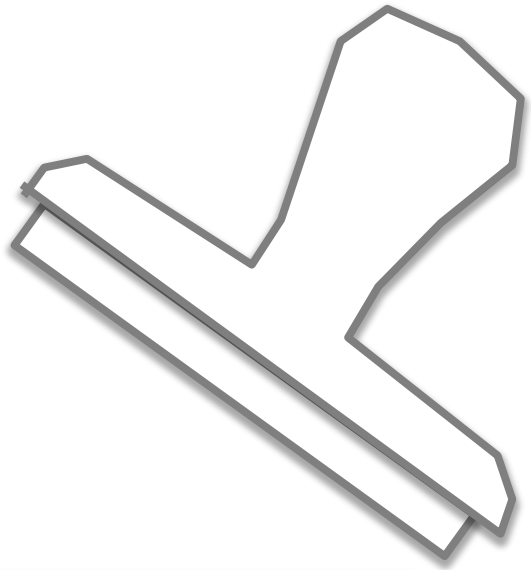
Question: Is it compliant to obtain permission for further use at the entrance of a user in a university?

Answer: An opt-out regarding the continued use of SWITCH edu-ID accounts after leaving a university is generally permissible.

Details: The DPO ZH and FR consider an opt-out to be feasible, even if they would prefer an opt-in with regard to the European data protection basic regulation. The DPO LU calls for an opt-in. He justified his answer with the fact that the accounts were personality profiles or particularly sensitive personal data.

Additions: The question of whether obtaining consent can be structured as an opt-out depends primarily on whether the Swiss Data Protection Act for private individuals or the DSGVO are used as a benchmark. It also depends on how the "opt-out solution" is concertedly designed. In Switzerland, for example, boxes that have already been ticked are still regarded as valid consent if the box is the subject of a declaration that is itself subject to a clear expression of the will of the person concerned.

Is edu-ID Data Protection Law Compliant ?



We are compliant with the different applicable data protection laws

Data Protection Law compliant

SWITCH edu-ID

Questions ?

You can also discuss questions with

legalteam@switch.ch
Anna Kuhn

New edu-ID Features

Past and Future

SWITCH

Rolf Brugger
Rolf.brugger@switch.ch

Zürich, November 13th 2018

Overview

Done!

1. **Affiliation Chooser**
2. **Single logout**
3. **User-Driven Deduplication**
4. **Custom Views**
5. **APIs**
6. **Password Policy**
7. **Ethical Hacking Test**

Doing!

1. **2FA**
2. **OIDC**
3. **eduroam**

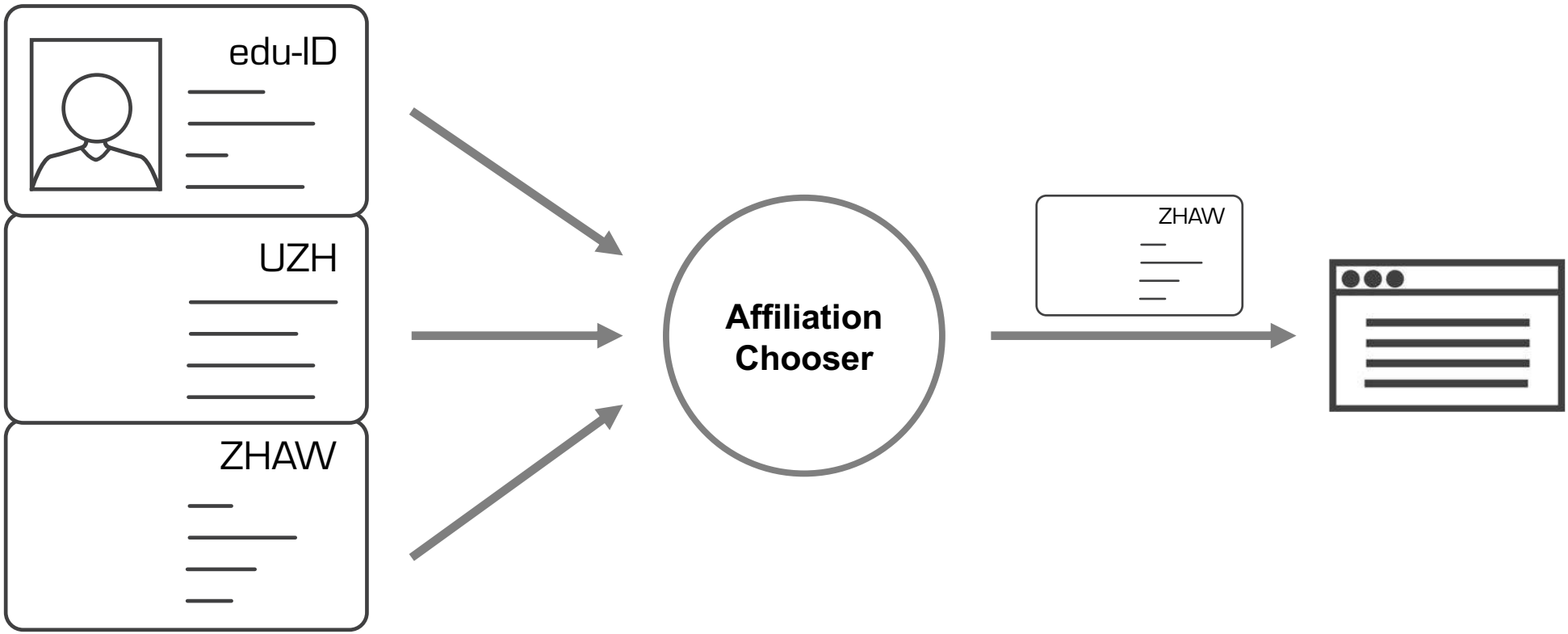
Covered in other presentations: usability improvements, login to microsoft services, organizational administrations interface, technical accounts.

1. Affiliation Chooser

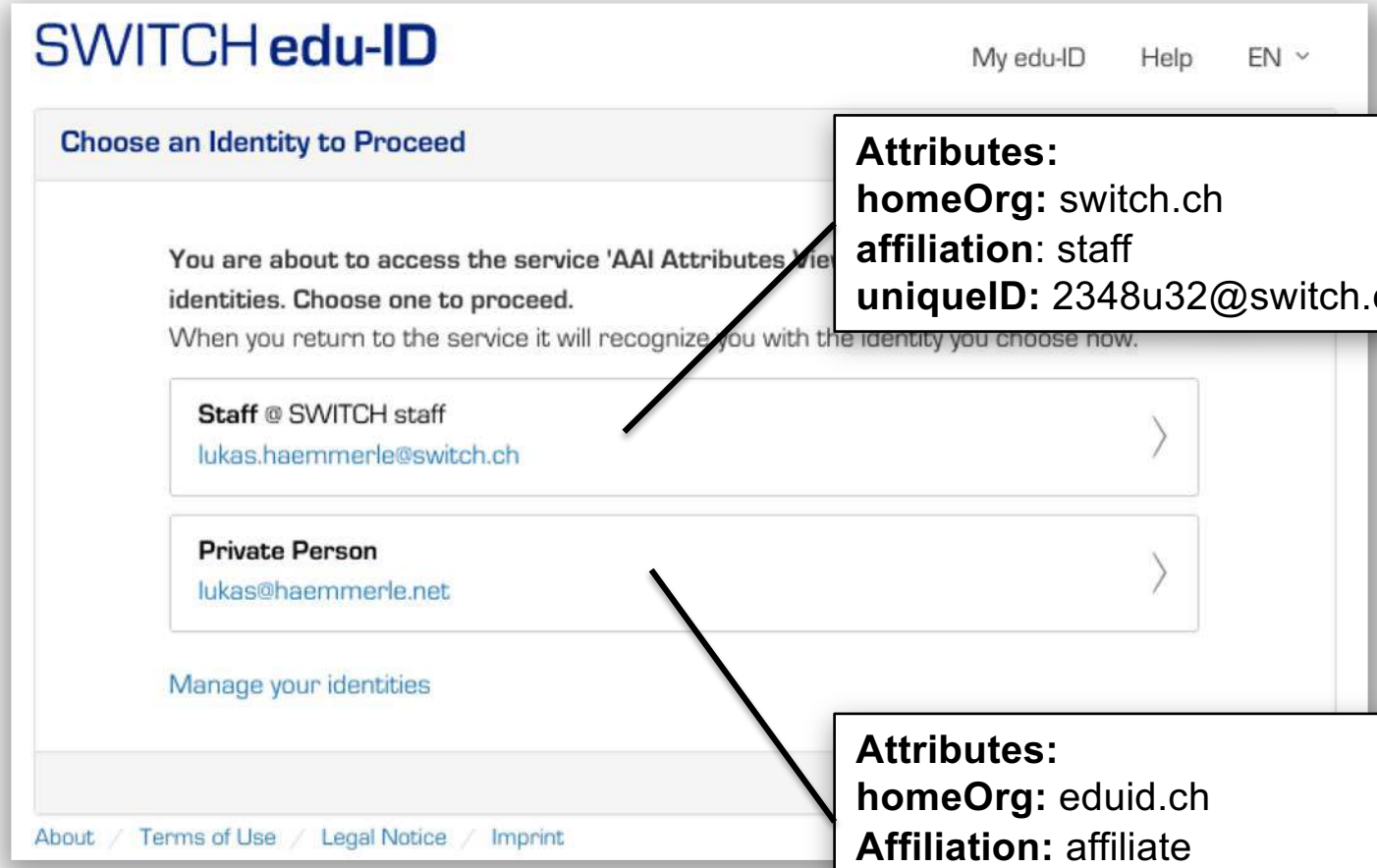
- Edu-ID introduces a more comprehensive identity schema
  - ➔ Private / personal attributes
  - ➔ Affiliations with organizations

- **Goal**: backward compatibility with SPs for edu-ID users with multiple affiliations

User Chooses Affiliation



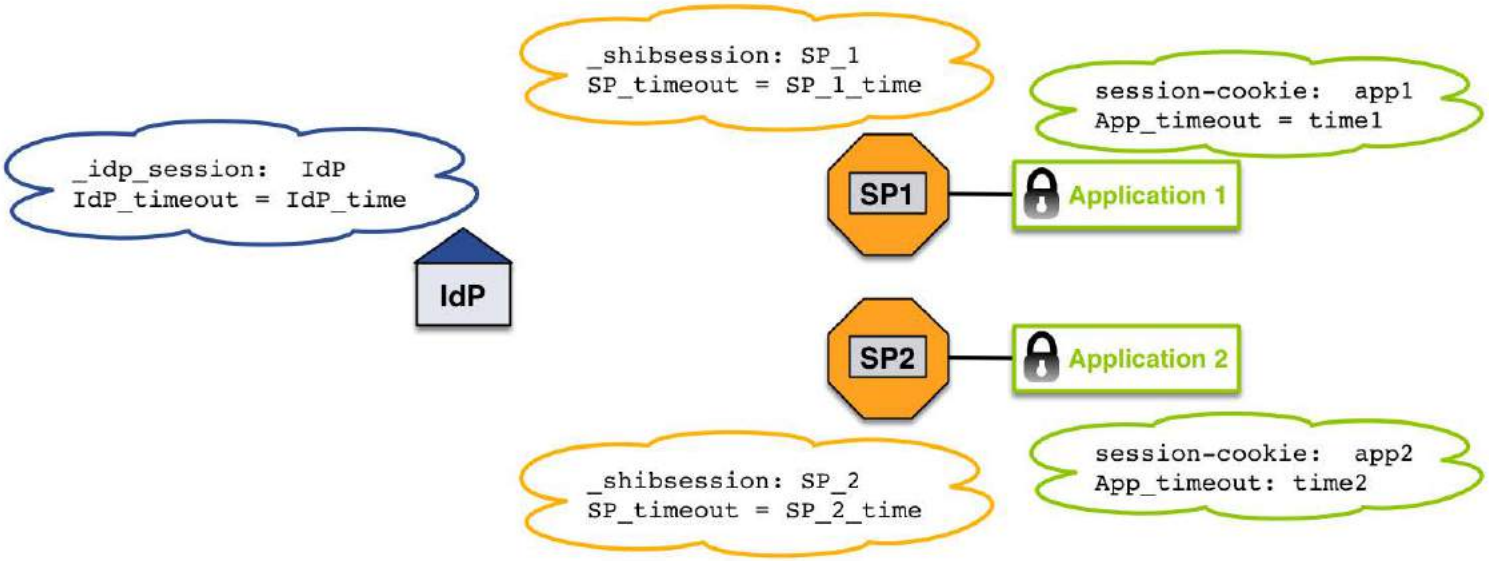
Affiliation Chooser Screenshot



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

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

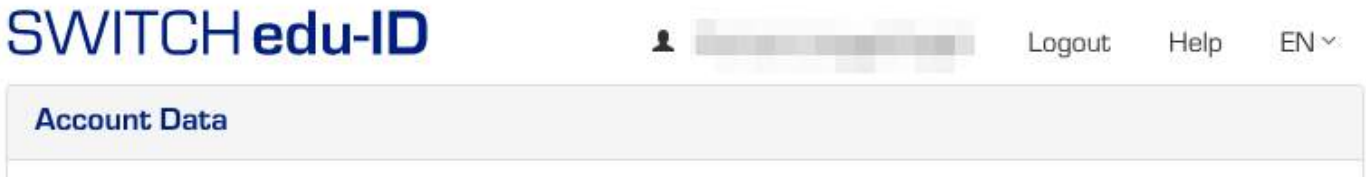
2. Single Logout



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

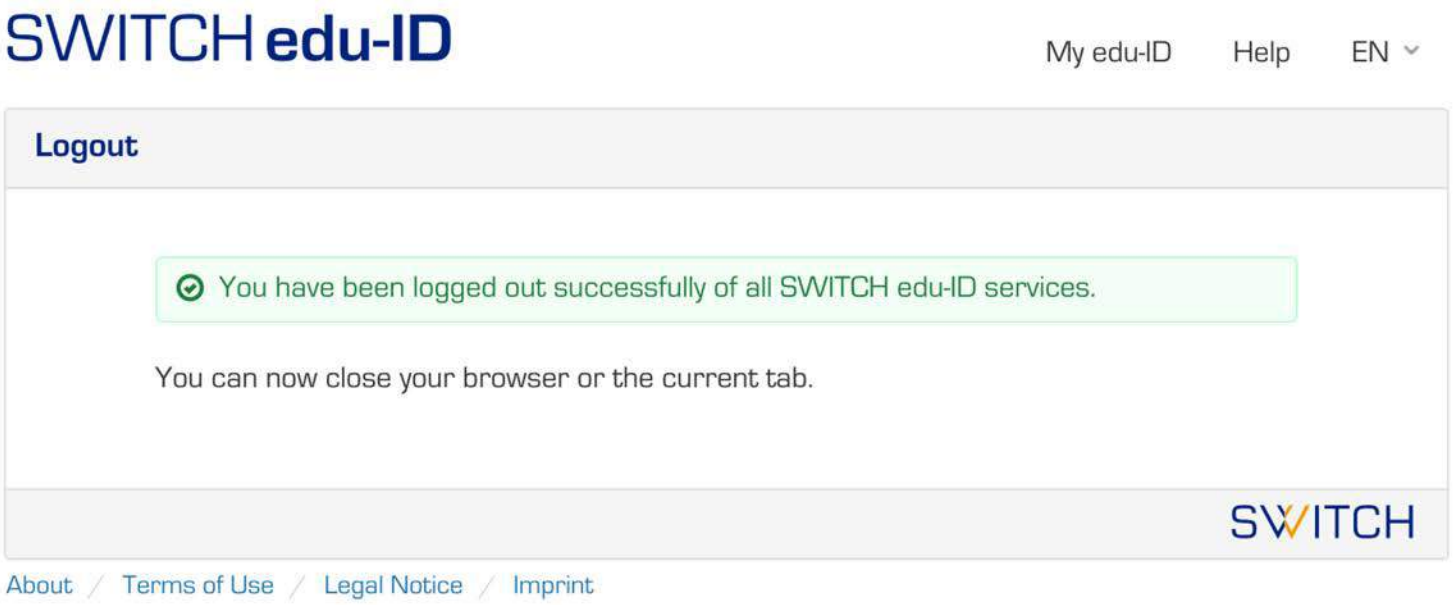
SLO at edu-ID IdP

- 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



Learn more about SLO

Single Logout Guide for SPs with edu-ID

https://www.switch.ch/aai/guides/sp/logout/

3. User-Driven Deduplication

Situation

- Duplicate account = same user has > 1 edu-ID accounts
- Duplicate accounts are bad
- Duplicate accounts cannot be 100% prevented
- Duplicate accounts are sometimes useful for developers

➔ Rather use edu-ID technical accounts!

Account Creation Recapitulation

Minimum data to create edu-ID account:

- First name - Not unique
- Last name - Not unique

} 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

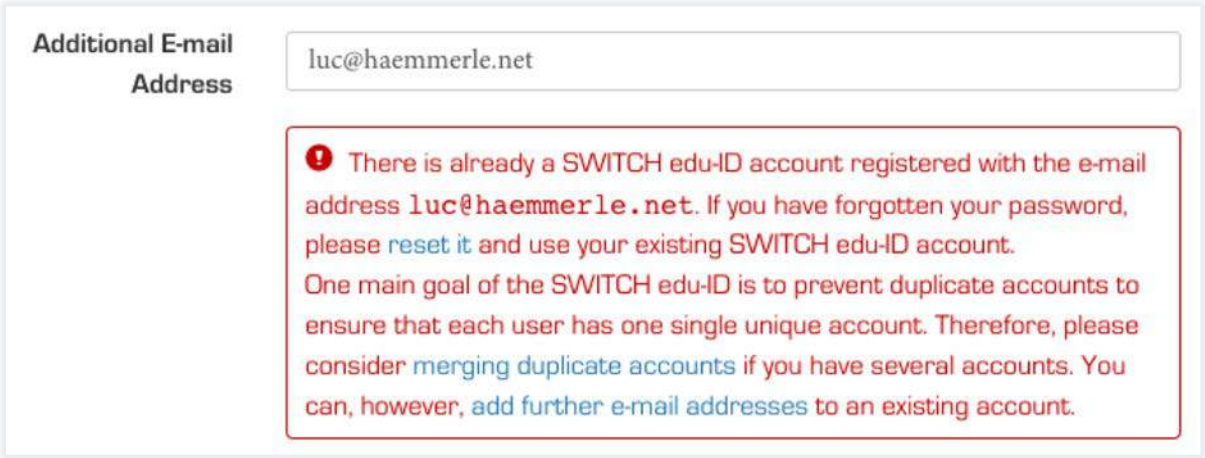
1. Try to **prevent** as many duplicates as possible
   - I.e. based on cookie and unique data

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

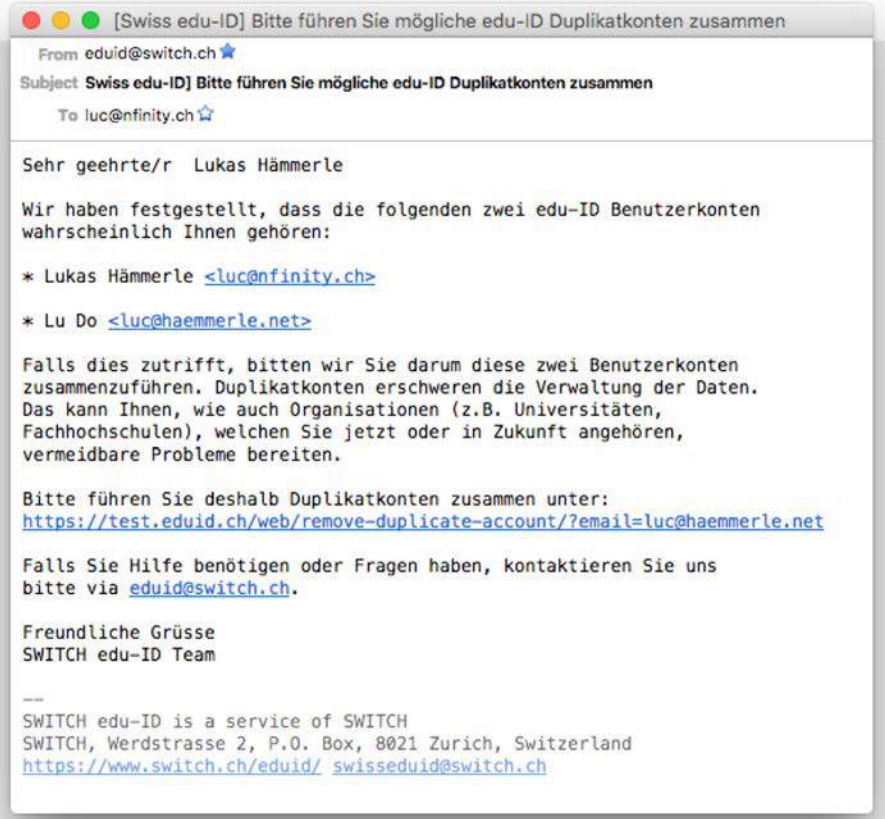
Identifying Duplicates



- 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



[Swiss edu-ID] Bitte führen Sie mögliche edu-ID Duplikatkonten zusammen

From eduid@switch.ch
Subject Swiss edu-ID] Bitte führen Sie mögliche edu-ID Duplikatkonten zusammen
To luc@nfinity.ch

Sehr geehrte/r Lukas Hämmerle

Wir haben festgestellt, dass die folgenden zwei edu-ID Benutzerkonten wahrscheinlich Ihnen gehören:

* Lukas Hämmerle <luc@nfinity.ch>

* Lu Do <luc@haemmerle.net>

Falls dies zutrifft, bitten wir Sie darum diese zwei Benutzerkonten zusammenzuführen. Duplikatkonten erschweren die Verwaltung der Daten. Das kann Ihnen, wie auch Organisationen (z.B. Universitäten, Fachhochschulen), welchen Sie jetzt oder in Zukunft angehören, vermeidbare Probleme bereiten.

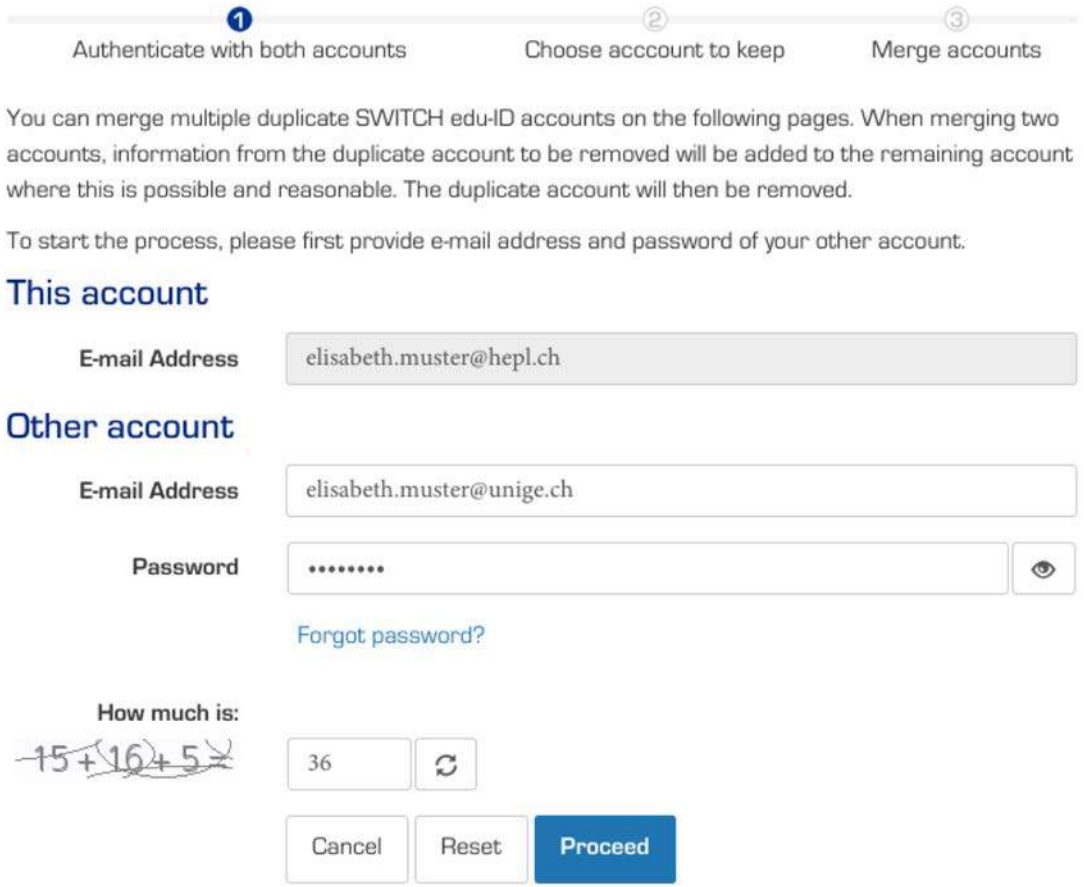
Bitte führen Sie deshalb Duplikatkonten zusammen unter:
https://test.eduid.ch/web/remove-duplicate-account/?email=luc@haemmerle.net

Falls Sie Hilfe benötigen oder Fragen haben, kontaktieren Sie uns bitte via eduid@switch.ch.

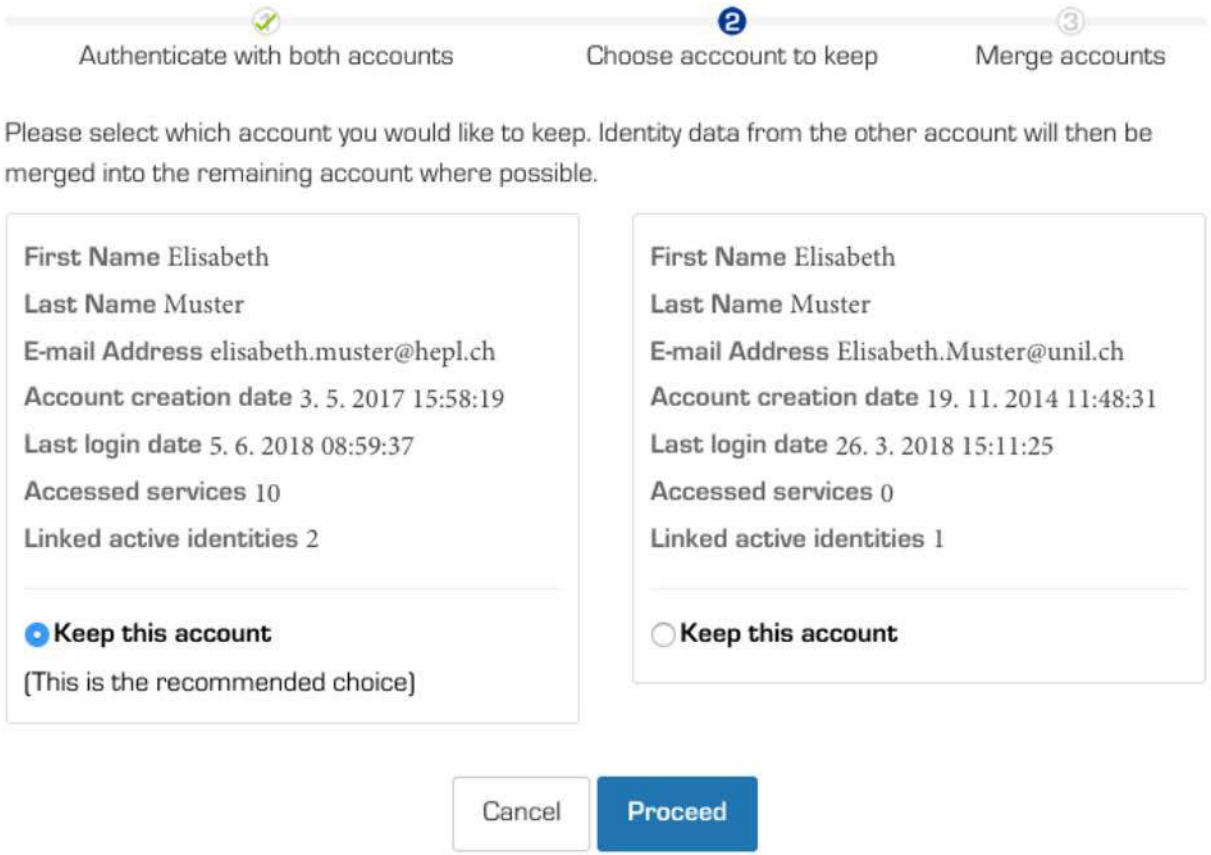
Freundliche Grüsse
SWITCH edu-ID Team

--
SWITCH edu-ID is a service of SWITCH
SWITCH, Werdstrasse 2, P.O. Box, 8021 Zurich, Switzerland
https://www.switch.ch/eduid/ swisseduid@switch.ch

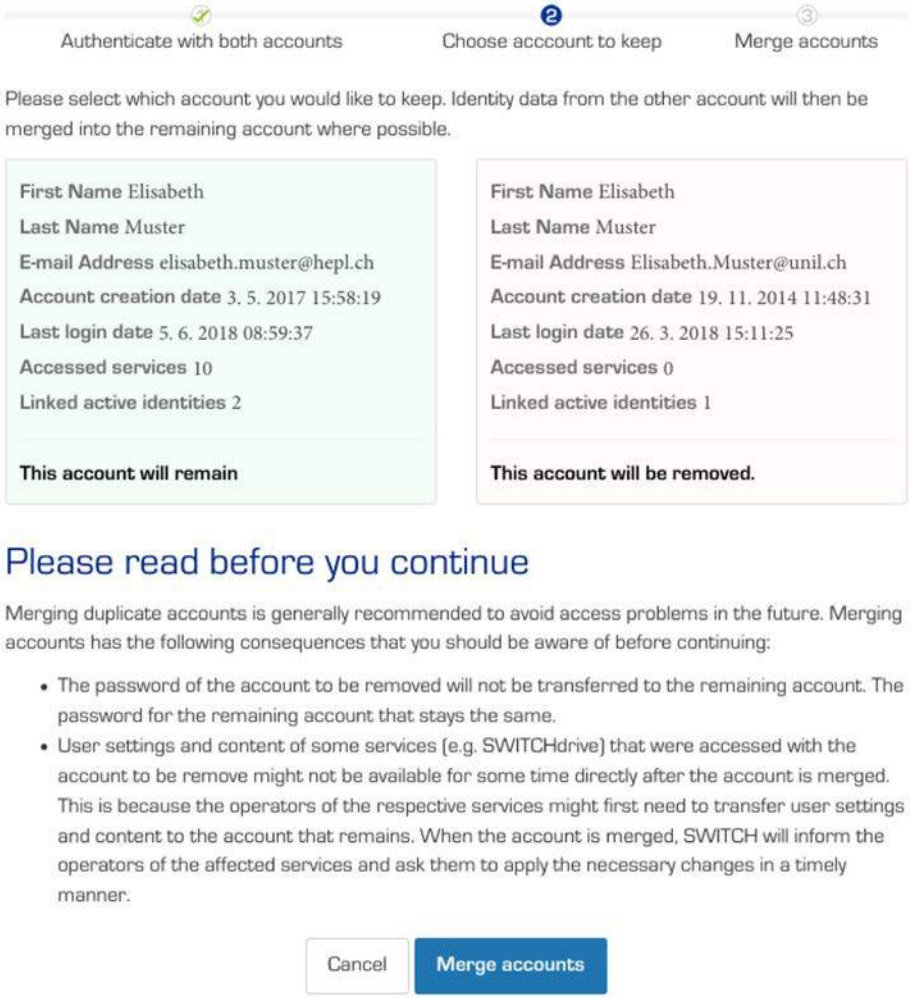
Account Merge by User: Step 1



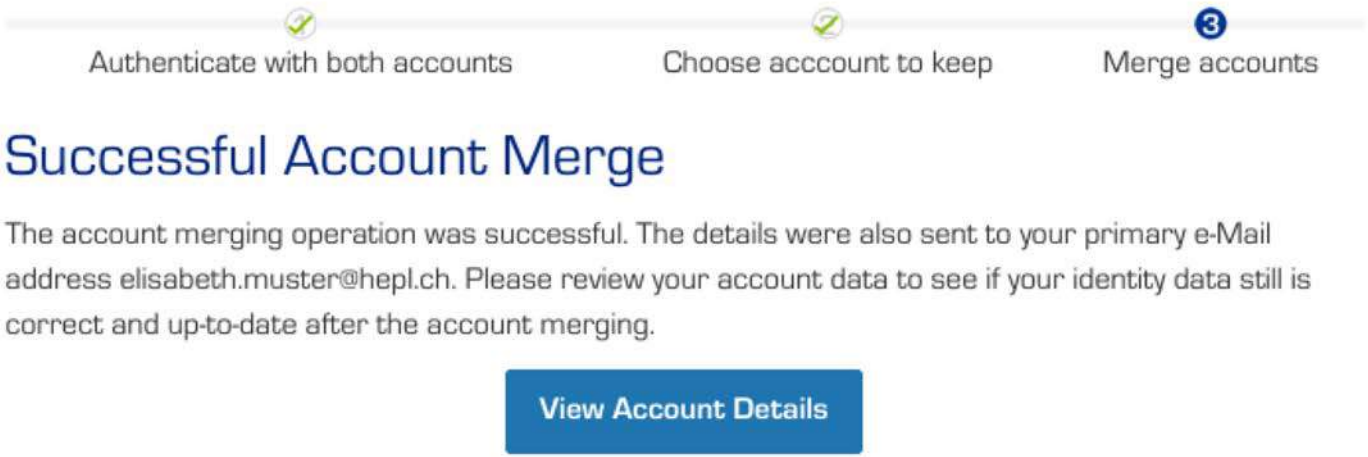
Account Merge by User: Step 2



Account Merge by User: Step 3



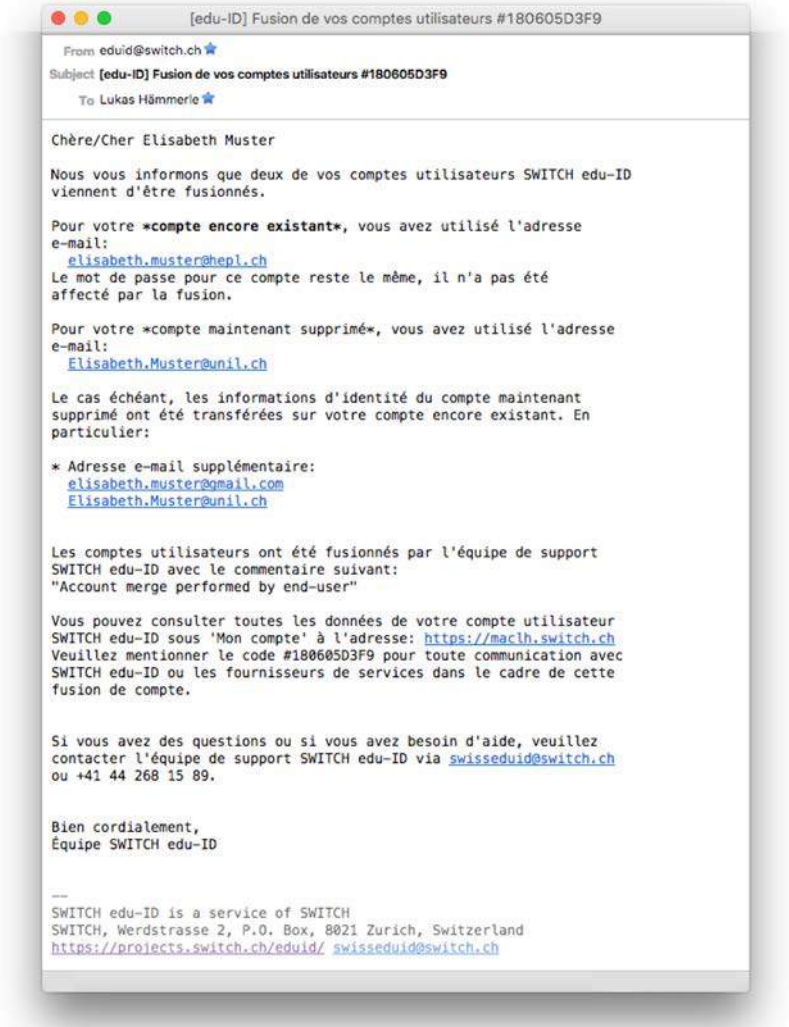
Account Merge by User: Result



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)



[edu-ID] Fusion de vos comptes utilisateurs #180605D3F9

From eduid@switch.ch
Subject [edu-ID] Fusion de vos comptes utilisateurs #180605D3F9
To Lukas Hämmerle

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@hepl.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://maclh.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 swisseduid@switch.ch ou +41 44 268 15 89.

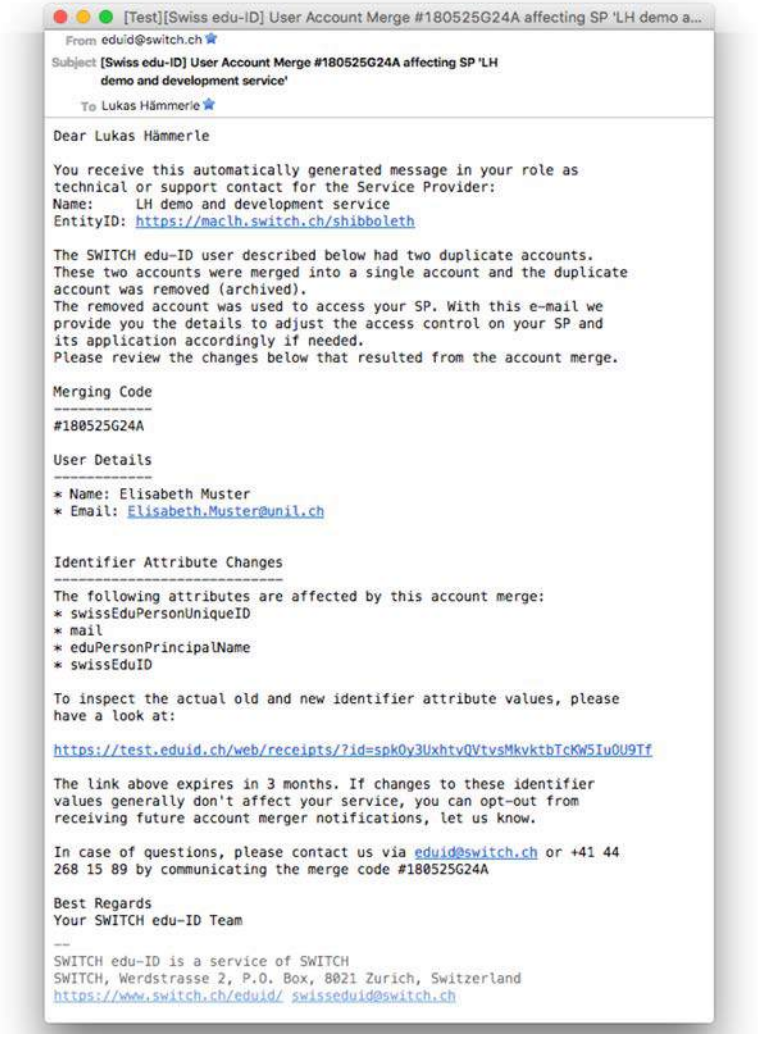
Bien cordialement,
Équipe SWITCH edu-ID

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



[Test][Swiss edu-ID] User Account Merge #180525G24A affecting SP 'LH demo a...

From eduid@switch.ch

Subject [Swiss edu-ID] User Account Merge #180525G24A affecting SP 'LH demo and development service'

To Lukas Hämmerle

Dear Lukas Hämmerle

You receive this automatically generated message in your role as technical or support contact for the Service Provider:
Name: LH demo and development service
EntityID: https://maclh.switch.ch/shibboleth

The SWITCH edu-ID user described below had two duplicate accounts. These two accounts were merged into a single account and the duplicate account was removed (archived).
The removed account was used to access your SP. With this e-mail we provide you the details to adjust the access control on your SP and its application accordingly if needed.
Please review the changes below that resulted from the account merge.

Merging Code

#180525G24A

User Details
---
* Name: Elisabeth Muster
* Email: Elisabeth.Muster@unil.ch

Identifier Attribute Changes

The following attributes are affected by this account merge:
* swissEduPersonUniqueID
* mail
* eduPersonPrincipalName
* swissEduID

To inspect the actual old and new identifier attribute values, please have a look at:

https://test.eduid.ch/web/receipts/?id=spkOy3UxhtvQVtvsMkvktbTcKW5IuOU9Tf

The link above expires in 3 months. If changes to these identifier values generally don't affect your service, you can opt-out from receiving future account merger notifications, let us know.

In case of questions, please contact us via eduid@switch.ch or +41 44 268 15 89 by communicating the merge code #180525G24A

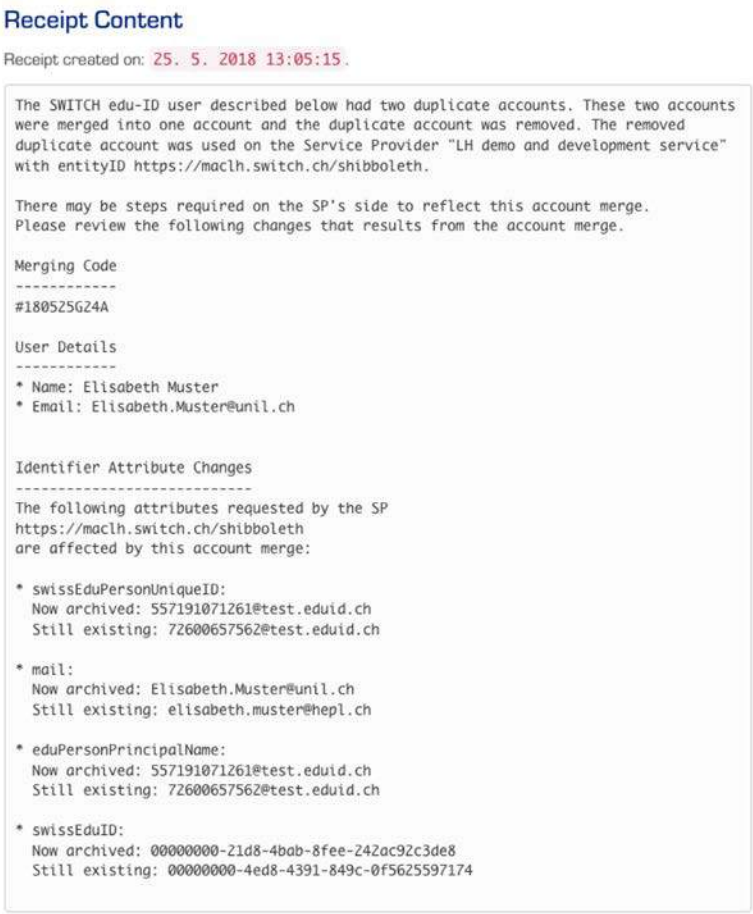
Best Regards
Your SWITCH edu-ID Team

--
SWITCH edu-ID is a service of SWITCH
SWITCH, Werdstrasse 2, P.O. Box, 8021 Zurich, Switzerland
https://www.switch.ch/eduid/ swisseduid@switch.ch

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
------------
#180525G24A

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:

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

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

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

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

Read more about Deduplication

Identity Blog Posting

https://identityblog.switch.ch/2018/06/15/clone-wars/

Summary

1. Affiliation Chooser

- For now only relevant for migrated organisations

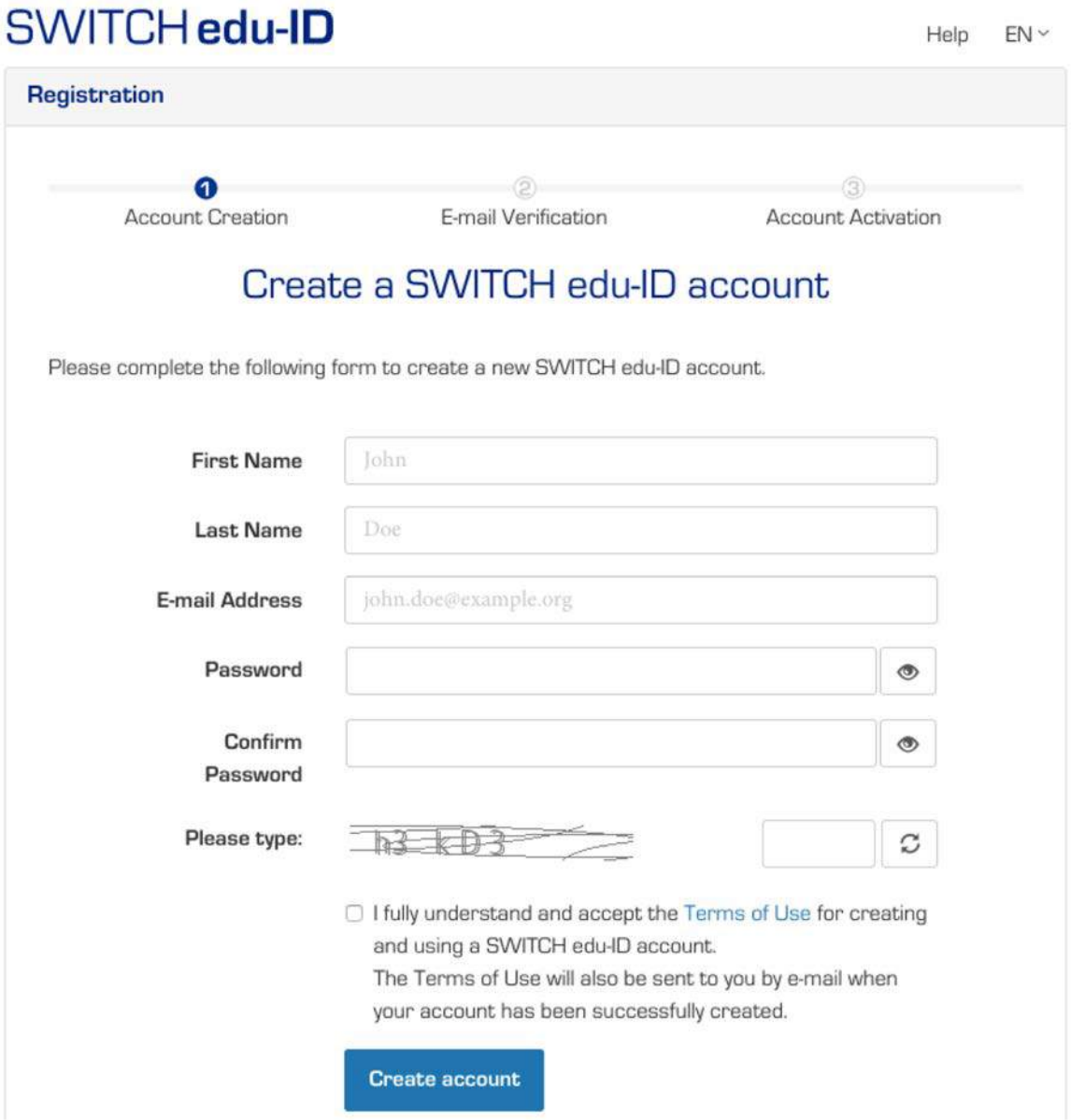
2. Single Logout

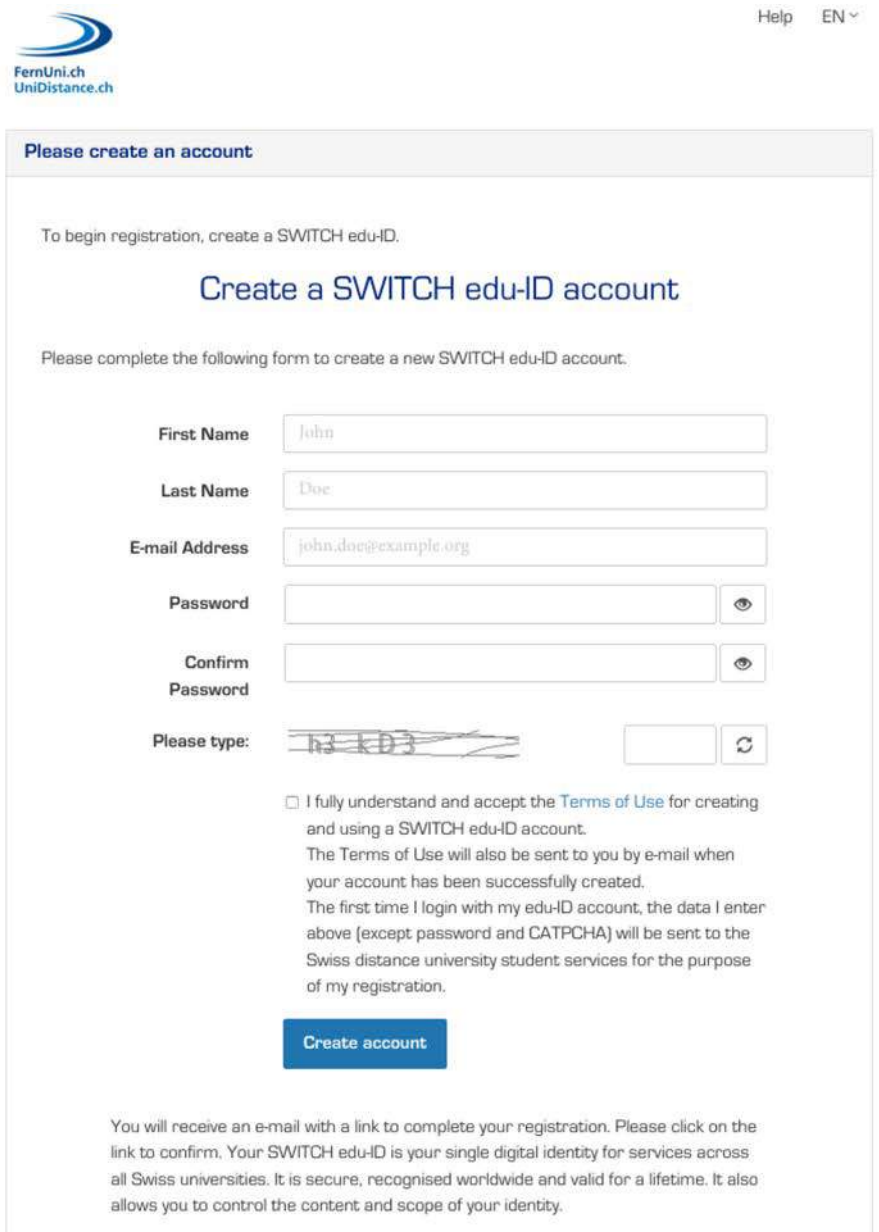
- Requires SP to publish SLO URLs and maybe changes in web app

3. User-Driven Deduplication

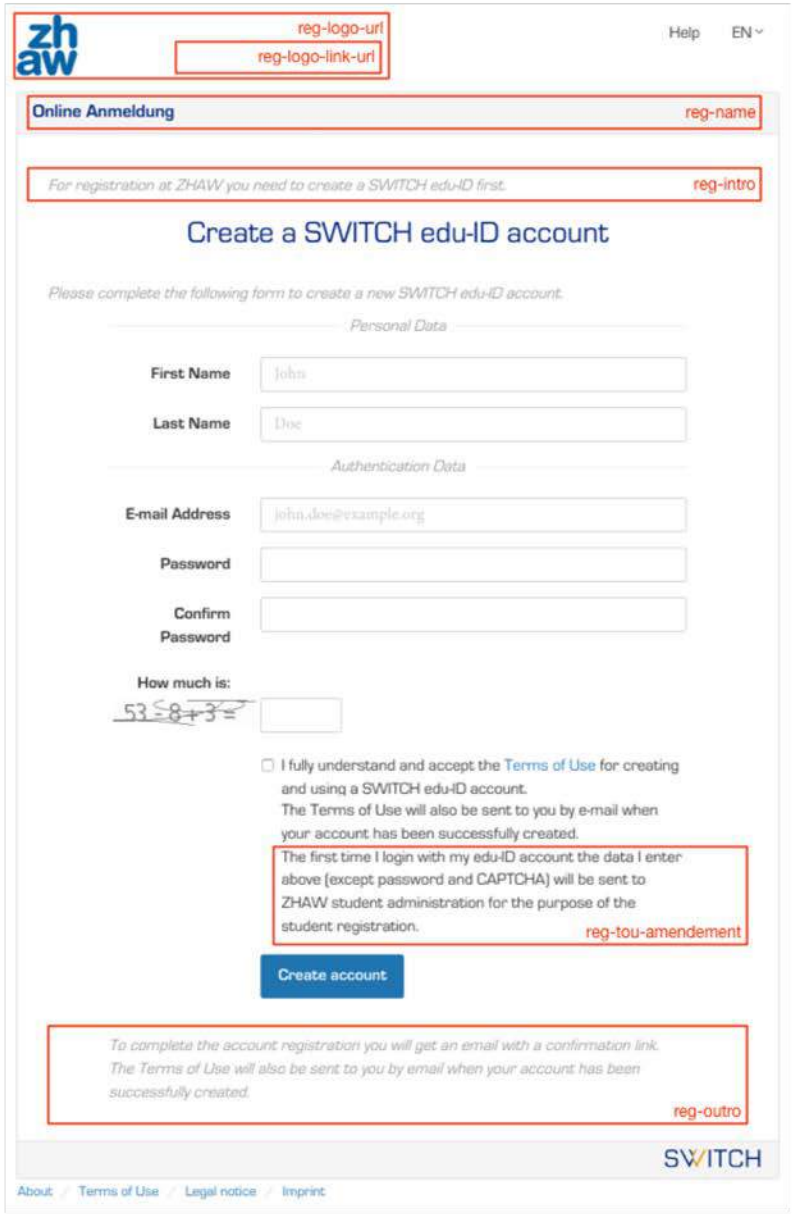
- Users can deduplicate accounts on their own with as few side effects as possible

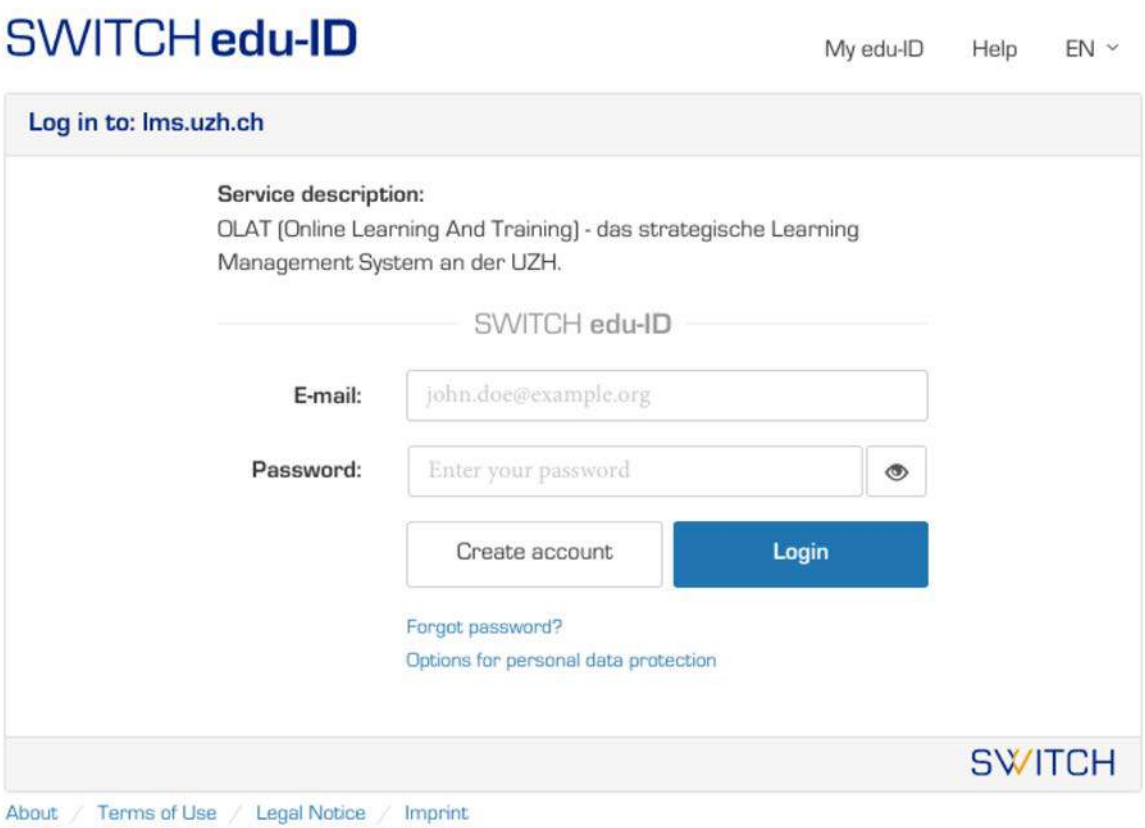
4. Custom Views

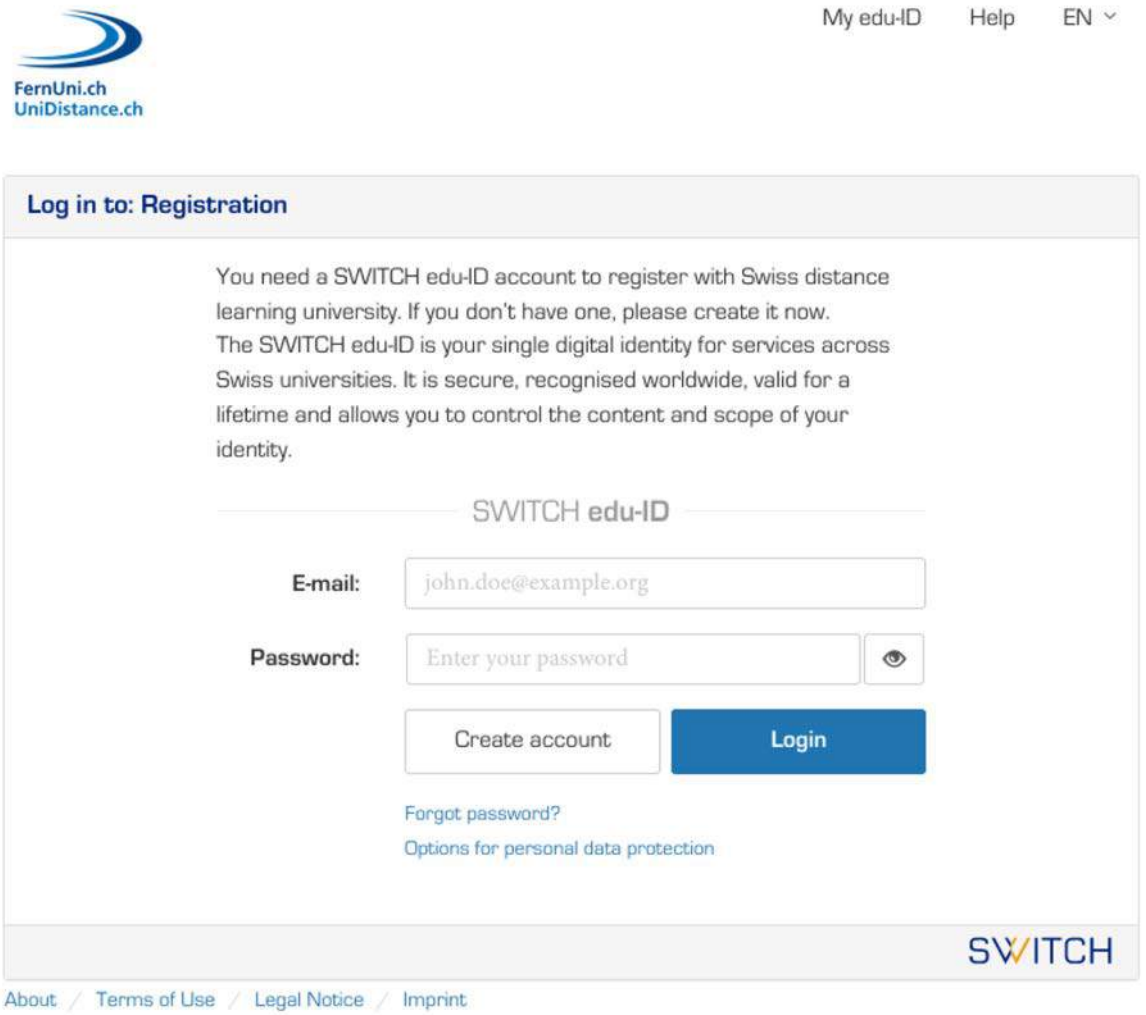

SWITCH edu-ID
Help
EN
Registration
1
Account Creation
2
E-mail Verification
3
Account Activation
Create a SWITCH edu-ID account
Please complete the following form to create a new SWITCH edu-ID account.
First Name
John
Last Name
Doe
E-mail Address
john.doe@example.org
Password
Confirm Password
Please type:
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


FernUni.ch
UniDistance.ch
Help
EN
Please create an account
To begin registration, create a SWITCH edu-ID.
Create a SWITCH edu-ID account
Please complete the following form to create a new SWITCH edu-ID account.
First Name
John
Last Name
Doe
E-mail Address
john.doe@example.org
Password
Confirm Password
Please type:
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.
The first time I login with my edu-ID account, the data I enter above (except password and CATPCHA) will be sent to the Swiss distance university student services for the purpose of my registration.
Create account
You will receive an e-mail with a link to complete your registration. Please click on the link to confirm. Your SWITCH edu-ID is your single digital identity for services across all Swiss universities. It is secure, recognised worldwide and valid for a lifetime. It also allows you to control the content and scope of your identity.

SWITCH


reg-logo-url
reg-logo-link-url
Help
EN
Online Anmeldung
reg-name
For registration at ZHAW you need to create a SWITCH edu-ID first.
reg-intro
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
Authentication Data
E-mail Address
john.doe@example.org
Password
Confirm Password
How much is:
53-8+3=
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.
The first time I login with my edu-ID account the data I enter above (except password and CAPTCHA) will be sent to ZHAW student administration for the purpose of the student registration.
reg-tou-amendement
Create account
To complete the account registration you will get an email with a confirmation link. The Terms of Use will also be sent to you by email when your account has been successfully created.
reg-outro
SWITCH
About
Terms of Use
Legal notice
Imprint


SWITCH edu-ID
My edu-ID
Help
EN
Log in to: lms.uzh.ch
Service description:
OLAT (Online Learning And Training) - das strategische Learning Management System an der UZH.
SWITCH edu-ID
E-mail:
john.doe@example.org
Password:
Enter your password
Create account
Login
Forgot password?
Options for personal data protection
SWITCH
About
Terms of Use
Legal Notice
Imprint


FernUni.ch
UniDistance.ch
My edu-ID
Help
EN
Log in to: Registration
You need a SWITCH edu-ID account to register with Swiss distance learning university. If you don't have one, please create it now.
The SWITCH edu-ID is your single digital identity for services across Swiss universities. It is secure, recognised worldwide, valid for a lifetime and allows you to control the content and scope of your identity.
SWITCH edu-ID
E-mail:
john.doe@example.org
Password:
Enter your password
Create account
Login
Forgot password?
Options for personal data protection
SWITCH
About
Terms of Use
Legal Notice
Imprint

More Information about Customization

edu-ID Website

https://www.switch.ch/edu-id/support/howto/customization/

5. SWITCH edu-ID APIs

Application programming interfaces

- For Organizations – to integrate edu-ID with organizational identity management processes
- For Services – to use special edu-ID features

- Access to APIs is restricted
- Request access at edu-ID team (eduid@switch.ch)

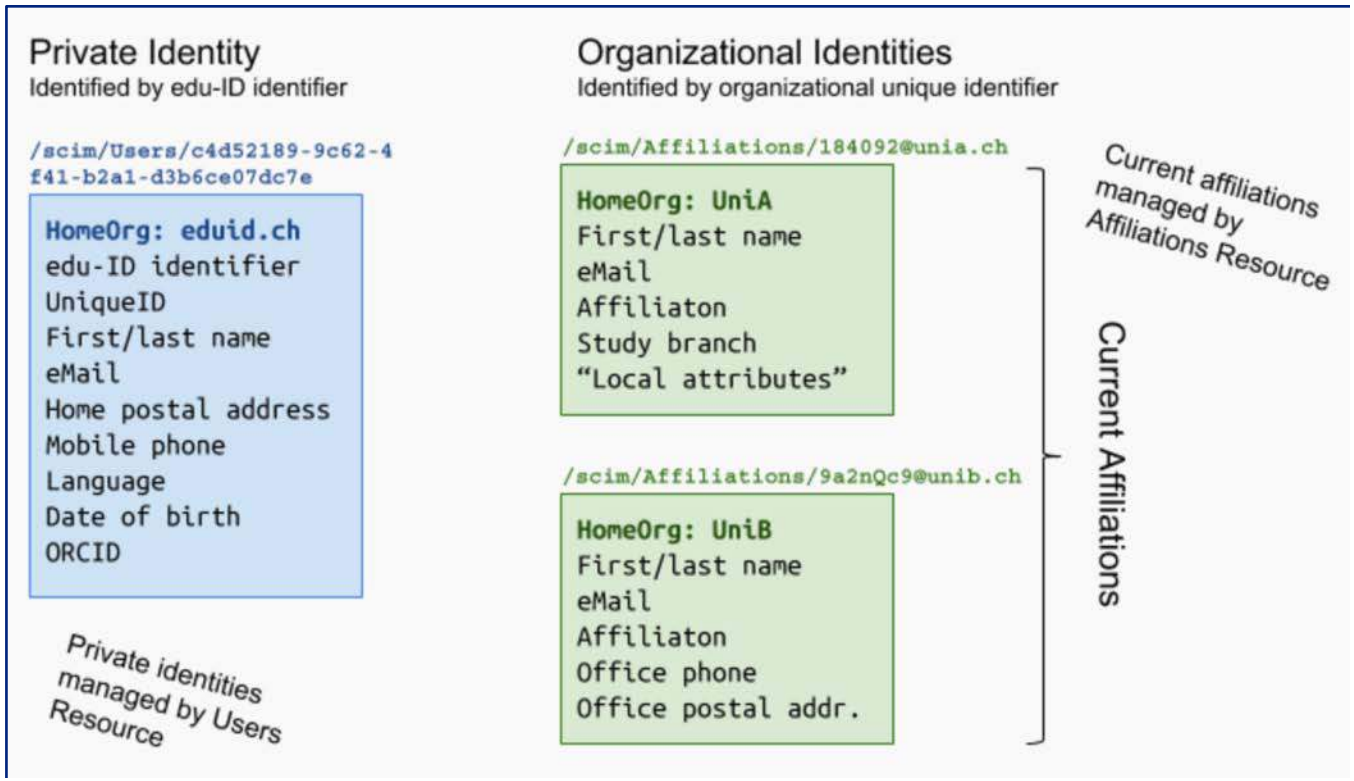
SCIM API

Give universities access to edu-ID personal data

- Current affiliations
  - Create
  - Read
  - Update
  - Delete

In the future:

- Private identity
- Group membership



Shared Attribute API

“Mini Group Management”

- Create a group
- Add edu-ID users to group
- Remove edu-ID users from group
- For group members: edu-ID IdP adds an entitlement attribute

- Example: entitlement set if “*user complies with regulations for national-license service*”

Tools API

Various helper functions for edu-ID:

- Check if an email address is already registered in an edu-ID account
- Bulk-check if edu-ID accounts still exist
- Special purpose functions
  - Set the last login time for a user's edu-ID account
  - Create a current affiliation for a new member of an organization

Read more about edu-ID APIs

edu-ID Website

https://www.switch.ch/edu-id/support/specifications/api-specification/

6. Password Policy

Background:

- edu-ID Passwords are managed by SWITCH
- NIST Special Publication 800-63B:
  Digital Identity Guidelines
  - https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret
  - Released June 2017
  - Chapter about Memorized Secrets (”Passwords”)

➔- New recommendations based on empirical research

Remarkable Changes

- Removed **periodic password change** requirements
- Dropped **password complexity requirements**
- Introduced check of passwords against lists of **commonly used or compromised passwords**
- Recommends **long** passwords

© W.C. Pope

NIST Password Rules: **SHALL**

	edu-ID
• Minimum 8 characters long	✓
• No hint/reset questions stored	✓
• Compare password against list of commonly-used passwords	✓
• Rate limiting	X
• Encrypted channel to check password	✓
• Salted Password hashes	✓
• Salt length min. 32 bit	✓
• Approved random number generator	?
• No truncation	✓

NIST Password Rules: **SHOULD**

	edu-ID
• No complexity requirements	✓
• Password at least up to 64 characters	✓
• All printing ASCII and space characters accepted	✓
	n.a.
• Warning when unicode characters are used	✓
• Password-strength meter	✓
• Allow pasting password	✓
• A memory-hard hash function	(✓)
• 10,000 hash iterations	X
• Additional hashing operation with secret salt stored in hardware module	

Choosing a Password

- Users choose their passwords, edu-ID provides guidelines

- Not all passwords are accepted. Depends on password score:
  - Length
  - Uppercase
  - Lowercase
  - Numbers
  - Symbols

- Score must exceed a certain threshold

- Password must not be leaked
  - **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 320M leaked password hashes (password/full hash are not sent to service)

Conclusion

- **Edu-ID cares 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 end of 2018
  - First: SMS One Time Password
  - Then: Time-based One Time Password

Read more about the edu-ID Password Policy

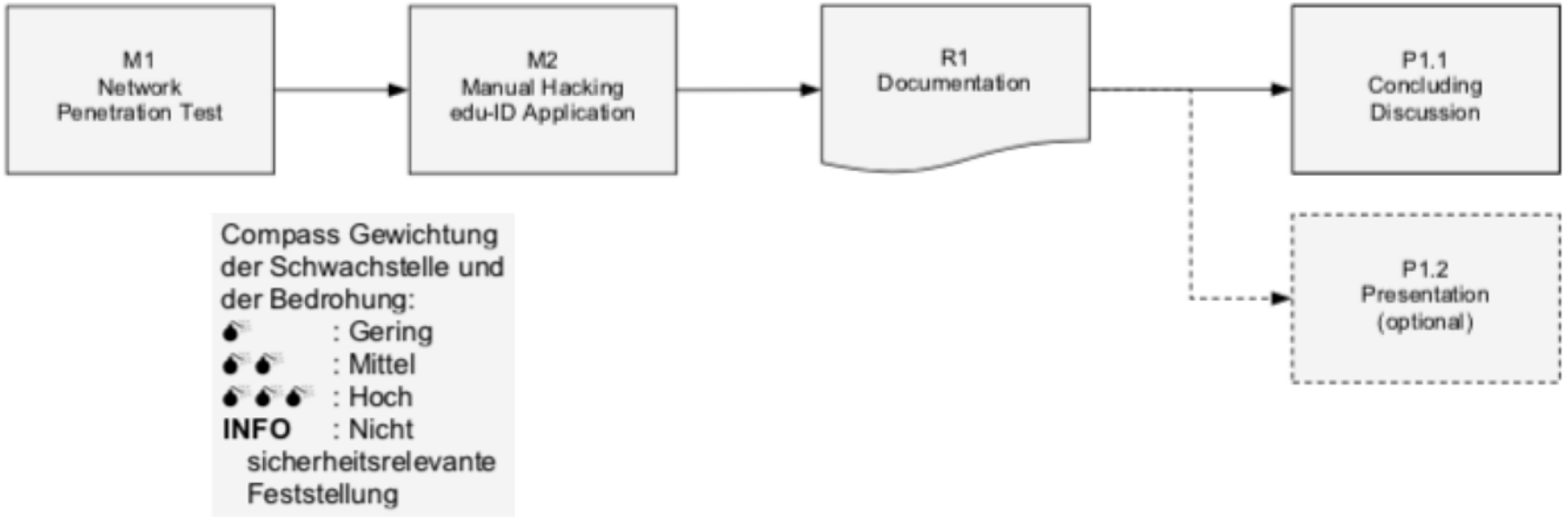
edu-ID Website

https://www.switch.ch/edu-id/support/specifications/password-policy/

7. Ethical Hacking Test

Procedure Compass

- Test period: one week in July on production service



- Presentation of test results, written report

Results

2.5 Ergebnisse

Die Applikation baut auf modernen Web-Technologien auf, dies verkleinert die Angriffsoberfläche, es konnten keine Schwachstellen wie z.B. SQL Injection festgestellt werden. Weiter war es nicht möglich Daten anderer Nutzer oder Institutionen einzusehen, die Autorisierung ist gut umgesetzt.

But also three issues category 💣💣💣:

- **Cross Site Scripting**:
  Input validation only filtered HTML tags rausgefiltert, but not ”
  In certain cases it was possible to execute JS

- **CAPTCHA Bypass**:
  The math question was too simple (solution space too small) and without throttling.
  However, also complaints with the new captcha

- **Cross Site Request Forgery:**
  Evil third party had possibility to introduce a link like
  https://eduid.ch/web/make-primary/?attribute=swisseduperson additionalemail&value=foo@bar.com
  to change primary email address

Consequences and ToDos

- Issues category 💣💣💣 and 💣💣 were fixed within a few days
  - Most 💣 category issues and INFO fixed as well
  - Learnings used for new developments

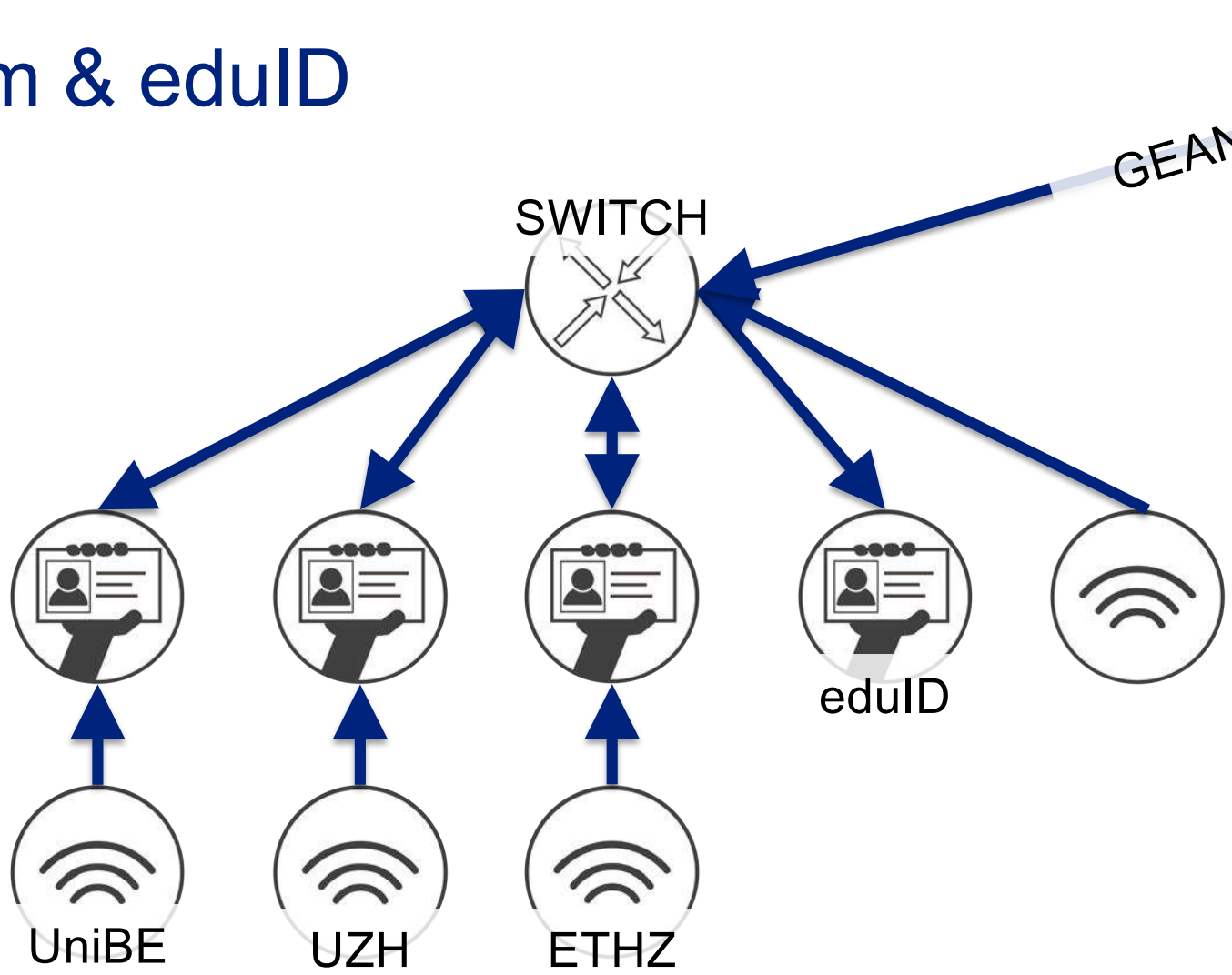
- For some issues we deliberately take the risk in favor of a better user experience

➔ The report was comprehensive and very useful

Outlook to new Features ahead

- Strong authentication
- eduroam integration
- OpenID Connect Provider
- Group Management
- Ongoing work: Usability, Org-Admin Interface, Integration with Microsoft protocols and services, APIs, …

Eduroam & eduID



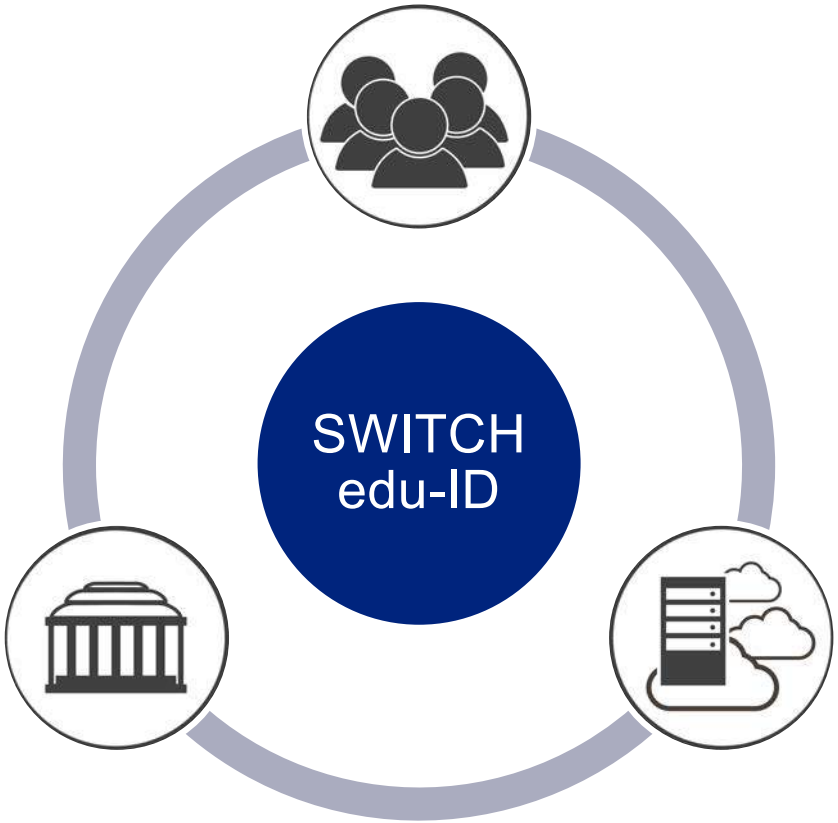
Organisation Administration Interface & Technical Accounts

SWITCH

Andres Aeschlimann
andres.aeschlimann@switch.ch

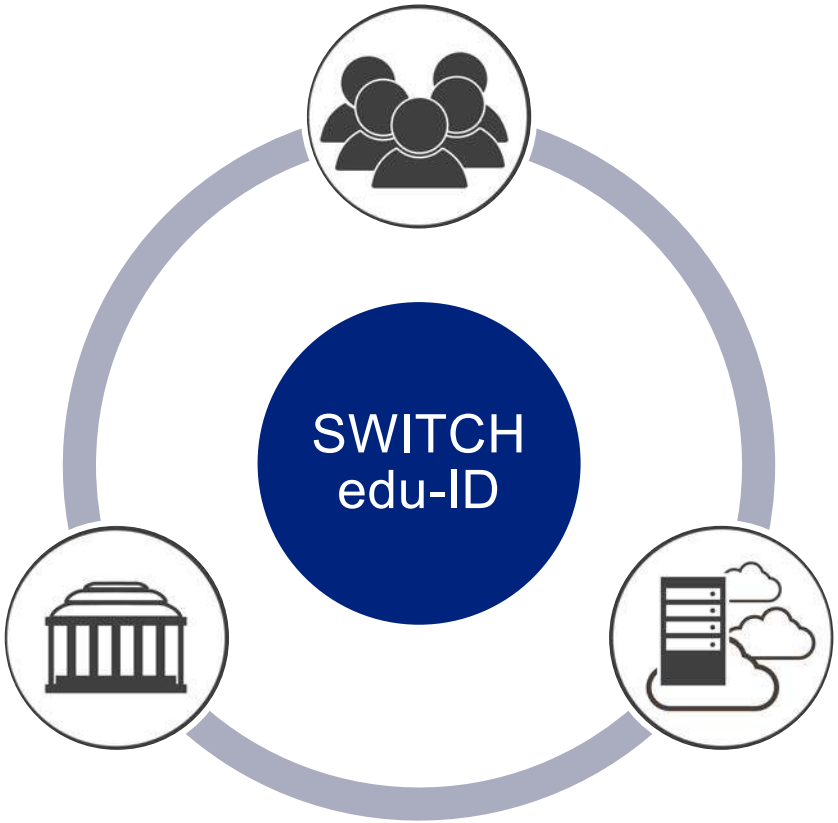
Zurich, 13.11.2018

Why?



- Because Organisations want to verify and/or update *their user data*.
- Because Organisations want to administer *their technical accounts*.

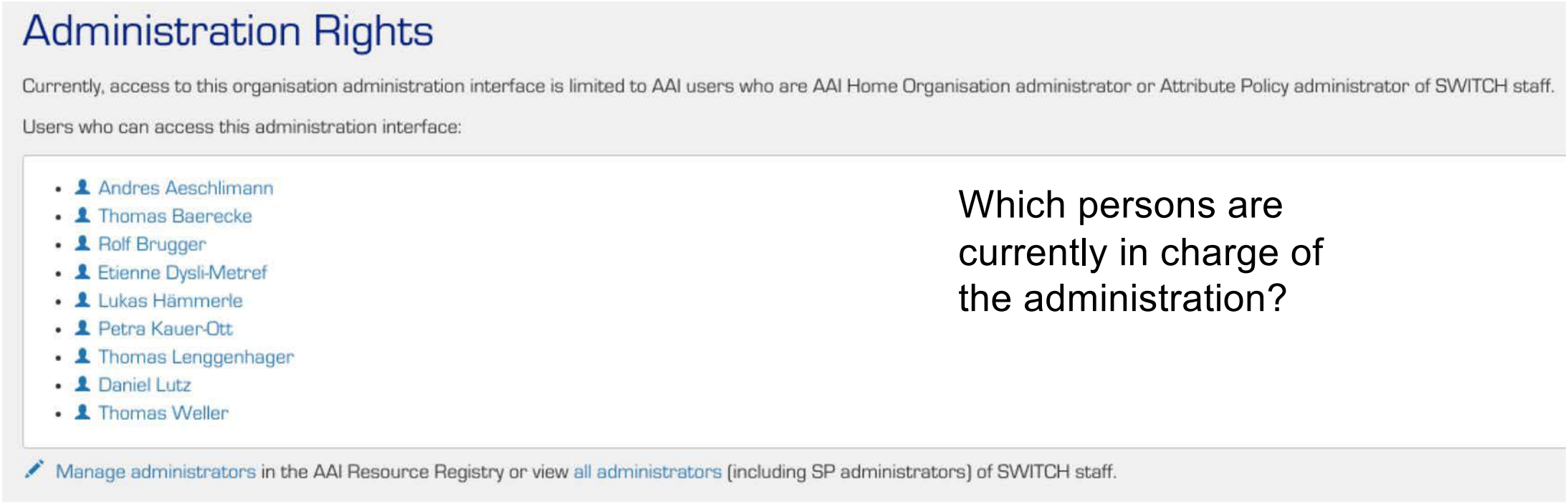
In any case, administration includes:



Which persons are currently in charge of the administration?

What has been done recently?

In any case, administration includes:



Which persons are currently in charge of the administration?

- Only for people with a linked affiliation
- Adding/removing administrators is done through the resource registry

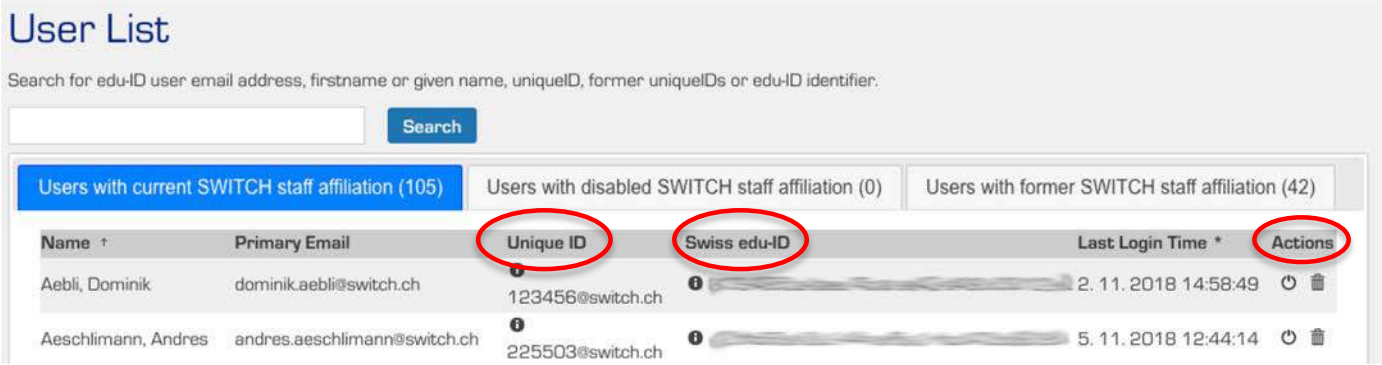
In any case, administration includes:

What has been done recently?

Checking the data

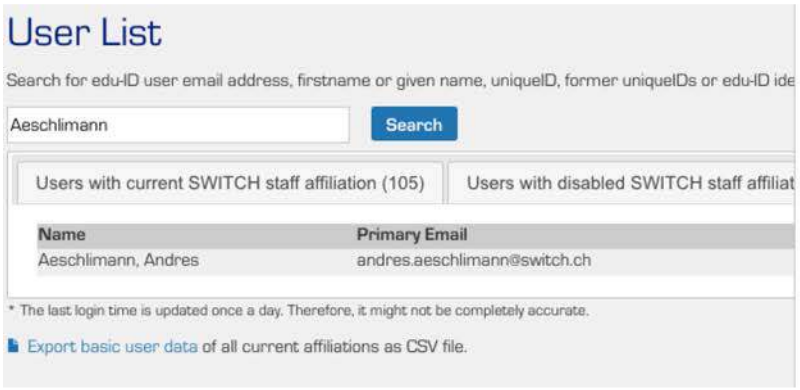
Did the last affiliation pull run complete?

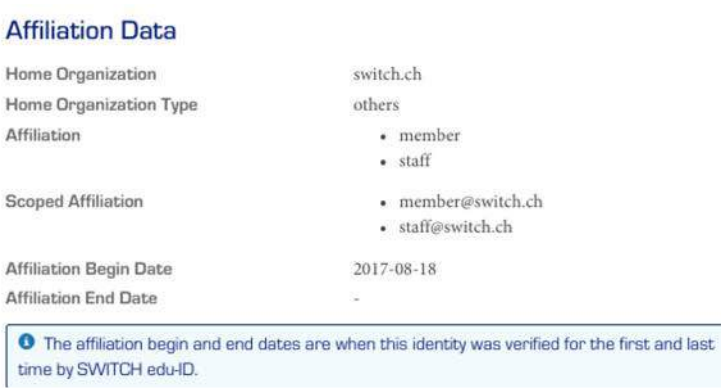
Checking the data



Browse through the user list.

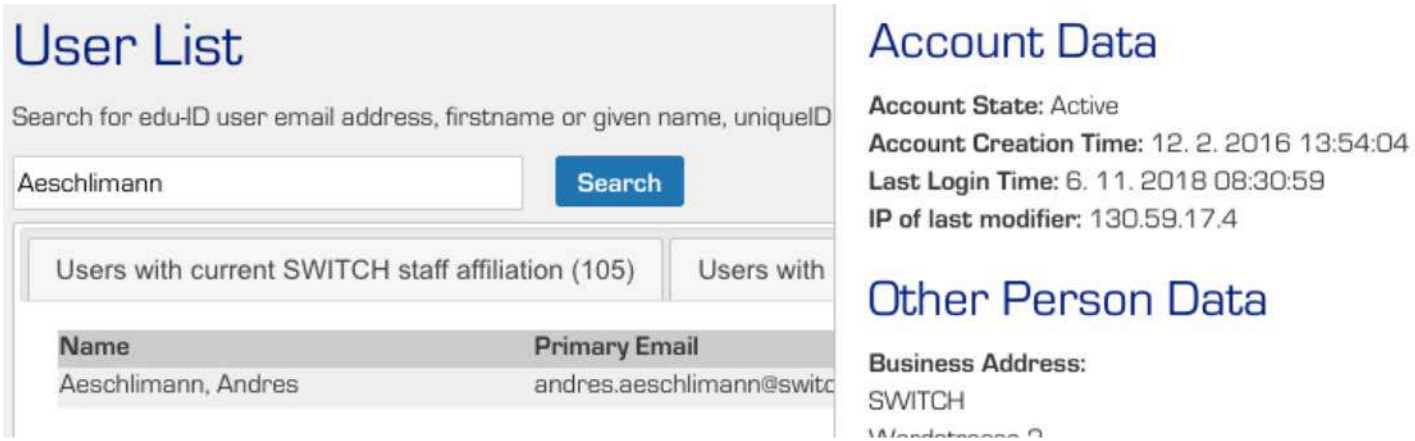
Checking the data





Affiliation: All kind of role specific information

Checking the data

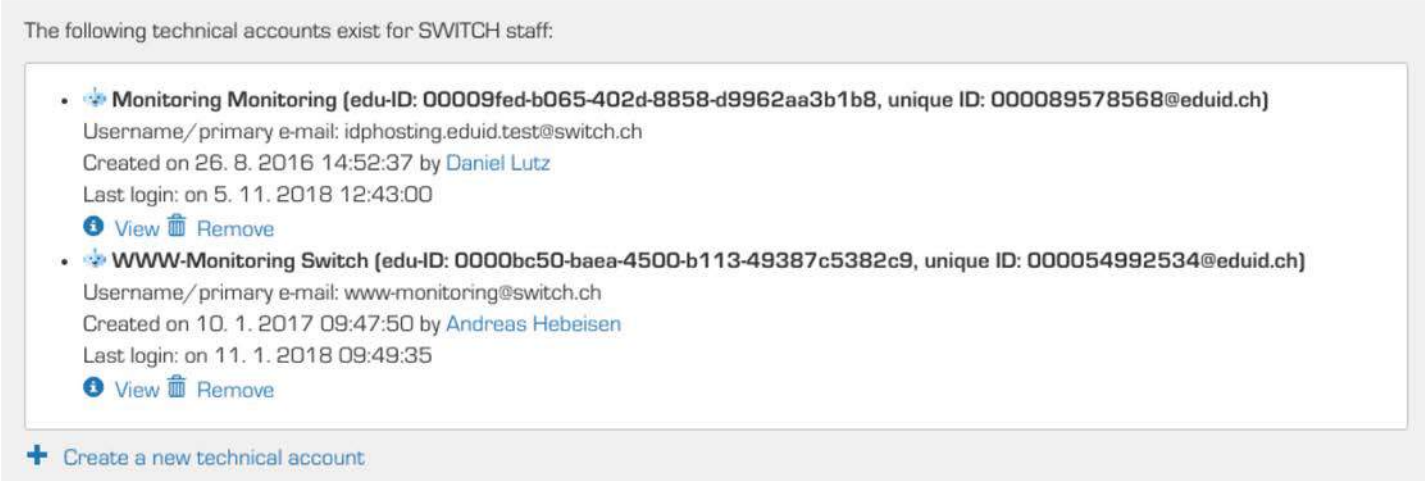


Base identity: All kind of information about the person

Technical Accounts

A technical account is a SWITCH edu-ID account used primarily for testing, debugging or monitoring purposes.

Technical Accounts



Technical Accounts

“Organisation are […] liable to SWITCH […] for damage […], in particular by technical and test accounts.” “
The AP Operator may delegate liability internally to one of its AP Administrators and must ensure that e-mails can be received by the specified e-mail addresses.” (See 6.9.2 and 5.1.3.7)

Links

https://eduid.ch/web/organisation-administrator/
https://eduid.ch/spec/technical-account/

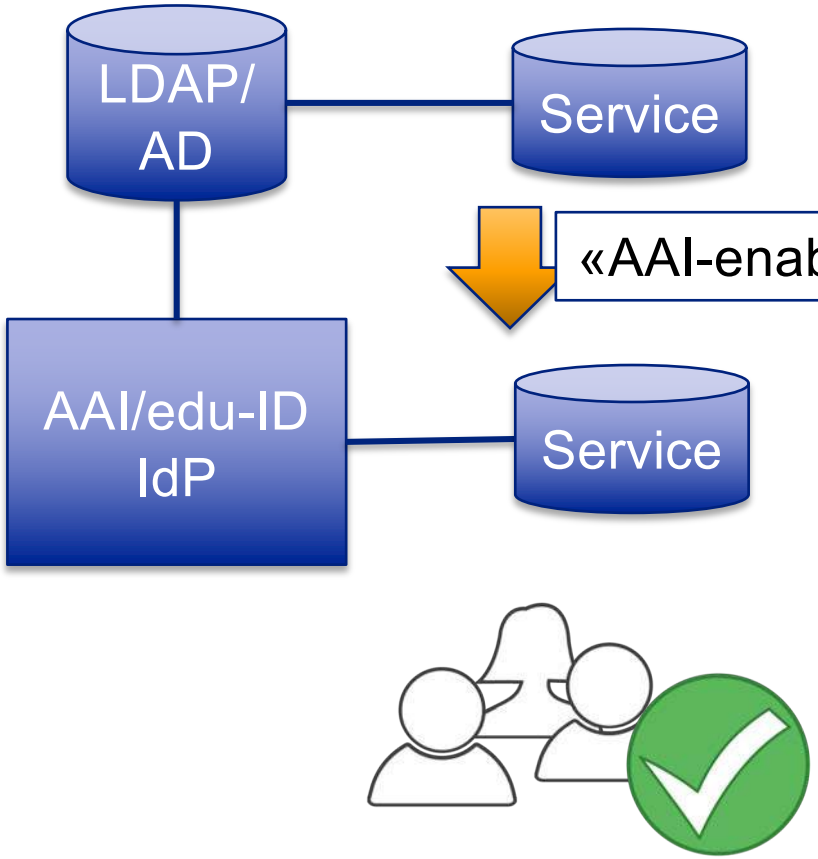
SWITCH edu-ID

edu-ID meets Office365 and Azure

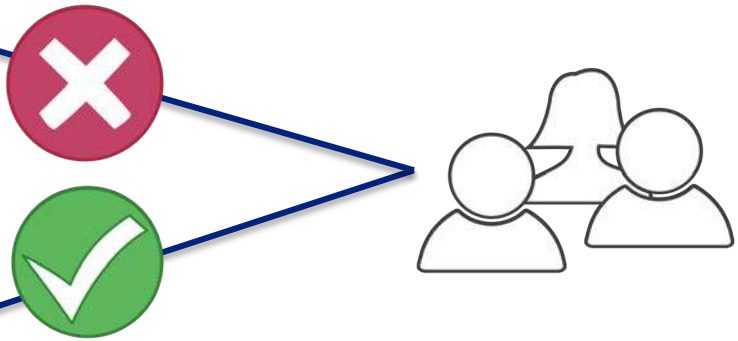
Christoph Graf
christoph.graf@switch.ch

Zürich, November 13th 2018

University



Identity federation / Community

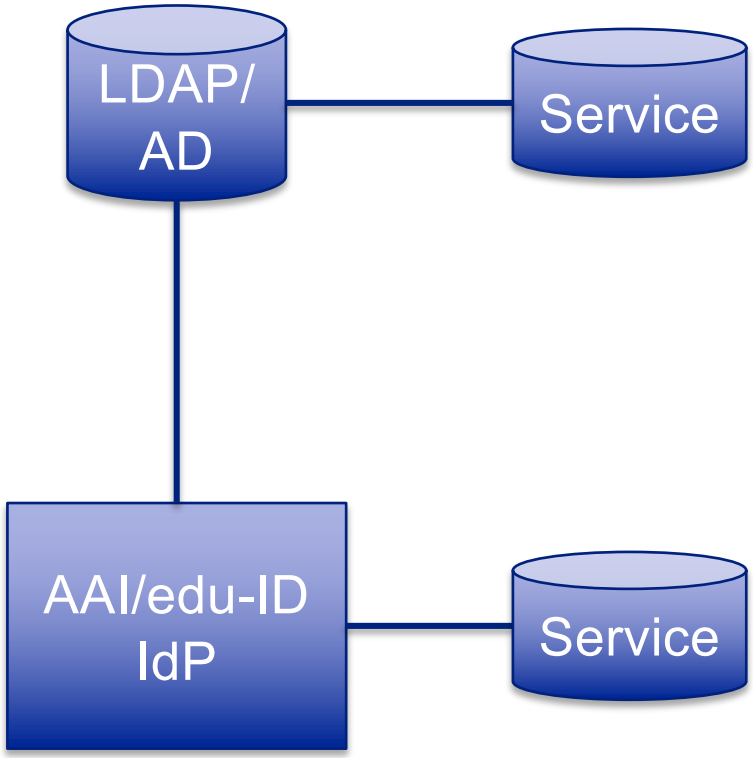


AAI-enabling only «half-way» done:

- often implemented for *shared* Web-Resources
- usually not implemented for LDAP/AD-integrated *local* resources

Why does this matter?...

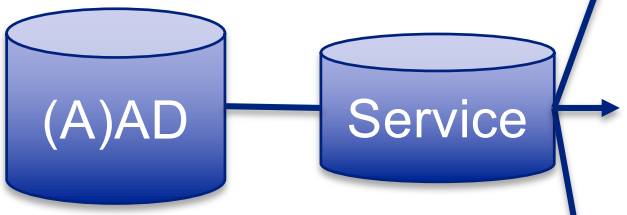
University



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 AD-connected 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

Edu-ID login shown at update event ‘18

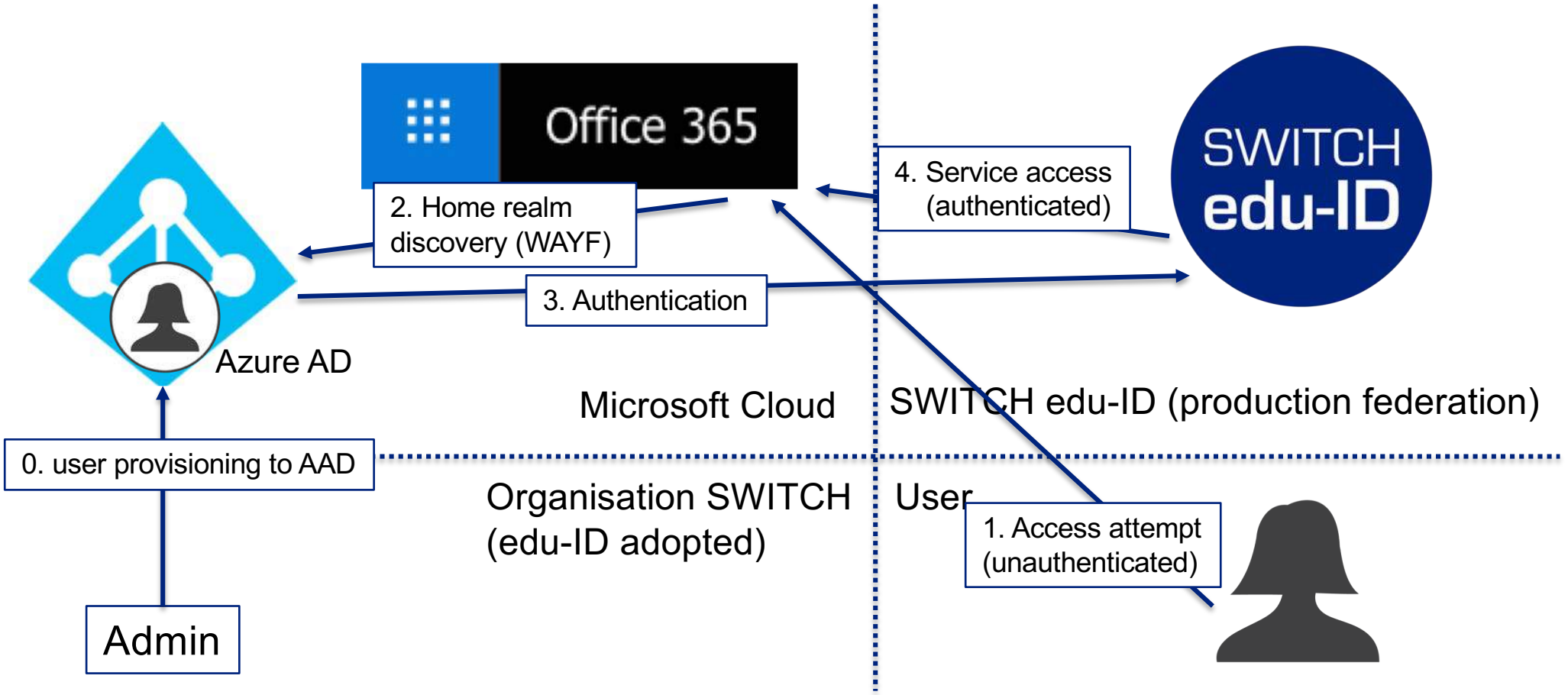
Edu-ID login shown at update event ‘18

edu-ID auth

To be assessed

AAD = Azure AD

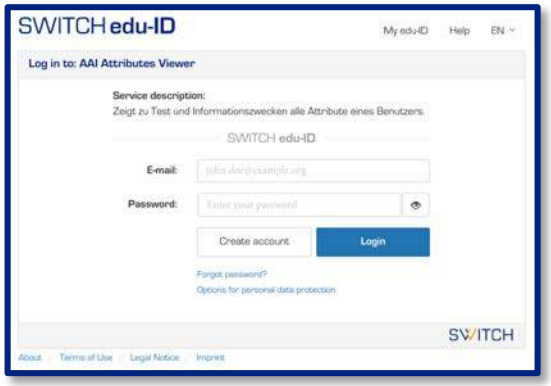
Operational: O365 for SWITCH employees



Edu-ID for O365

- Pre-conditions:
  - Edu-ID adoption completed
  - Own tenant with O365 licenced
  - Users provisioned to AAD
    - With or without local AD
    - Some magic: put the right attributes in the right place

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 (shown at update event June 2018)

- 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)

What happened since June 2018?

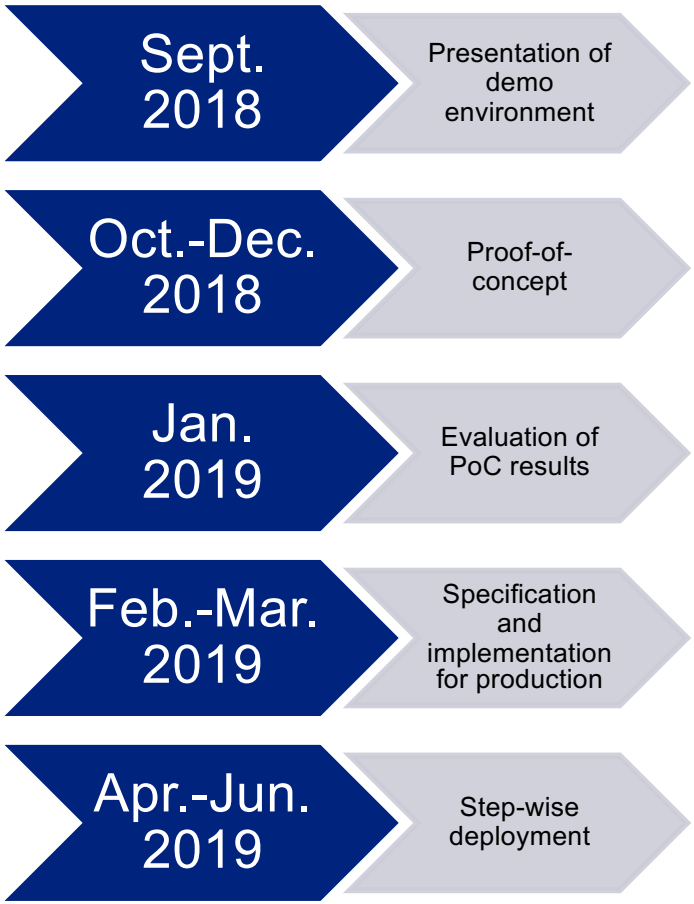
- Validation workshops with specialists from our community
- The following prioritised list of use cases emerged:
  1. The “guest use case”:
     - How to share MS-protected resources with other edu-ID users (not necessarily existing members of a Azure tenant)
  2. Service offering (Alumni, continued education etc.):
     - Known users, but without organisational mail address («bring your own email»)
  3. Legacy applications:
     - Including «lab users» with their macs or PCs (not necessarily domain-joined) to access shares
     - Printing and other
  4. Passwort-(Hash)-Synchronisation:
     - If needed for the cases above

Intermediate results

Current state regarding those use cases:

- #1 (and possibly #2): probably to require a «fall-back tenant» for the edu-ID (requiring a @eduid.ch mail address and users to choose the «right» address)
- #3: exploring coverage with SPNEGO, with #4 as fallback

Roadmap


Sept. 2018
Presentation of demo environment
Oct.-Dec. 2018
Proof-of-concept
Jan. 2019
Evaluation of PoC results
Feb.-Mar. 2019
Specification and implementation for production
Apr.-Jun. 2019
Step-wise deployment

SWITCH

Working for a better digital world