Switch

Switch edu-ID Community Meeting

Switch Forum Day VII
18 June 2025

Welcome to the Switch **Forum Days 2026**

Slides of this Event

https://swit.ch/eduidEvents

Agenda

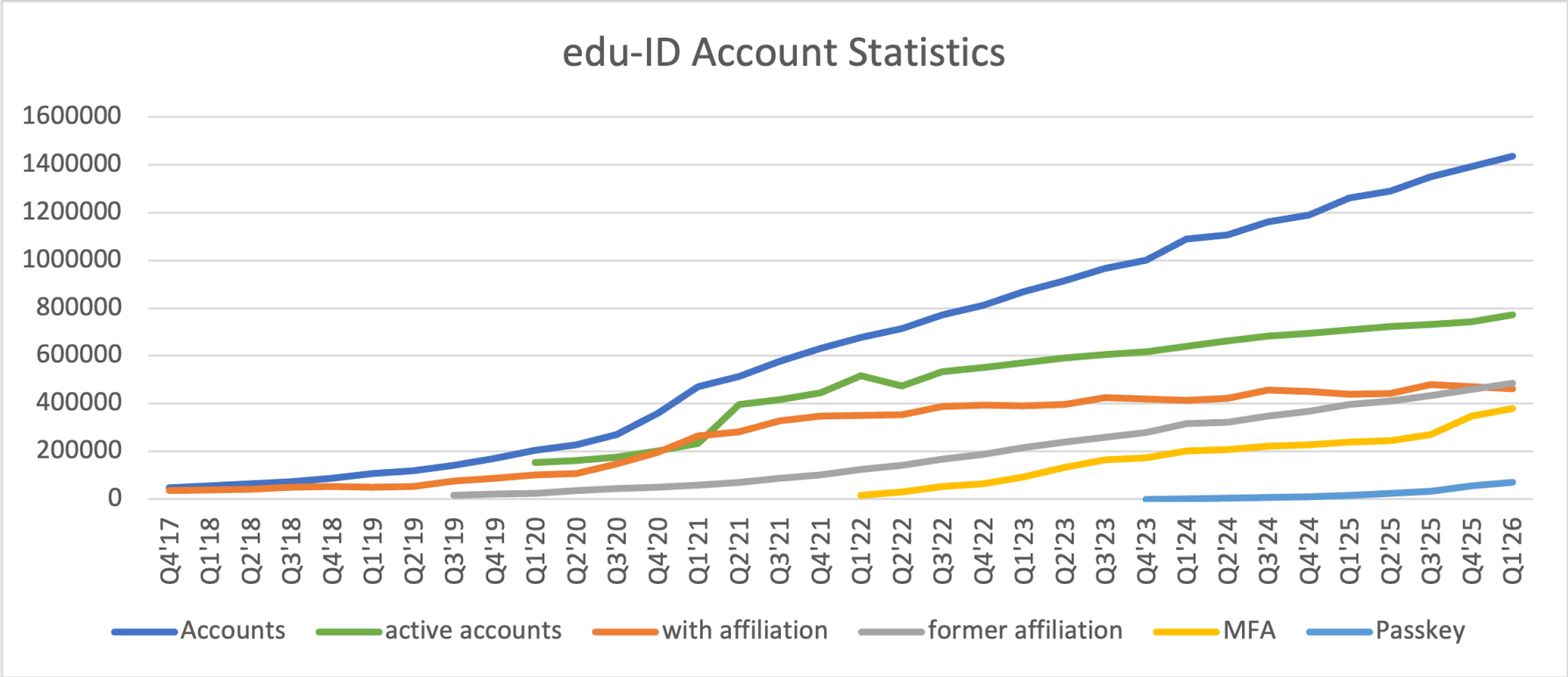
1. **Facts and figures about edu-ID**	10'
2. **edu-ID strategy/pricing update**	15'
3. **Current activities and achievements**	
A. OpenID Connect identity model	20’
B. Group management system	5'
C. Updates to the infrastructure	10'
4. **Edu-ID Usage Recommendations**	
A. MFA Everything Everywhere All at Once	15'
B. Saving Private E-Mail	10'
5. **Open session: Q&A, ideas, etc.**	5'

Switch

Facts and figures about edu-ID

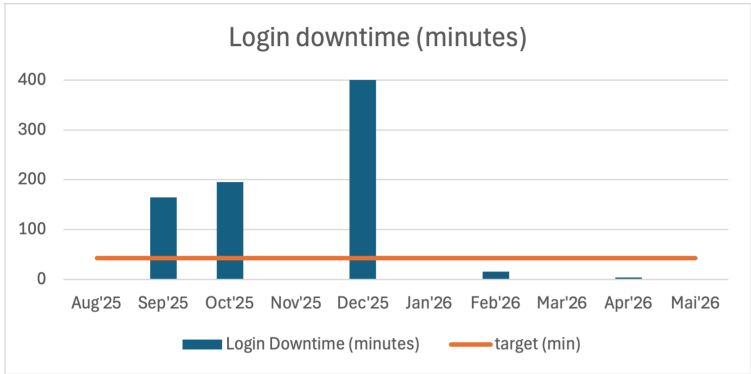
Rolf Brugger

Account Statistics



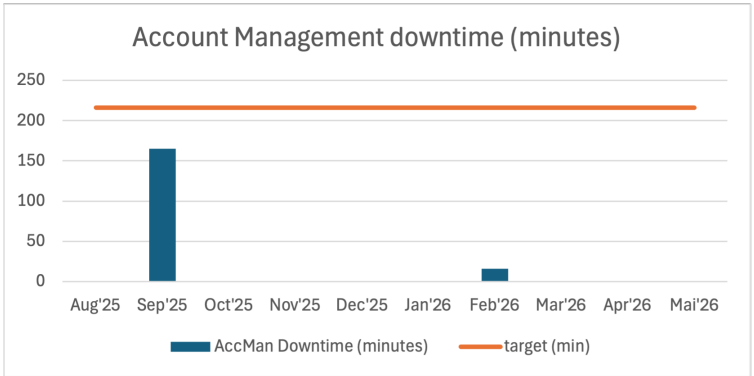
Switch edu-ID **counts over 1.4 million users**,
of which **54% have been active** during the last 12 months.
University member coverage is close to 100%.

SLA



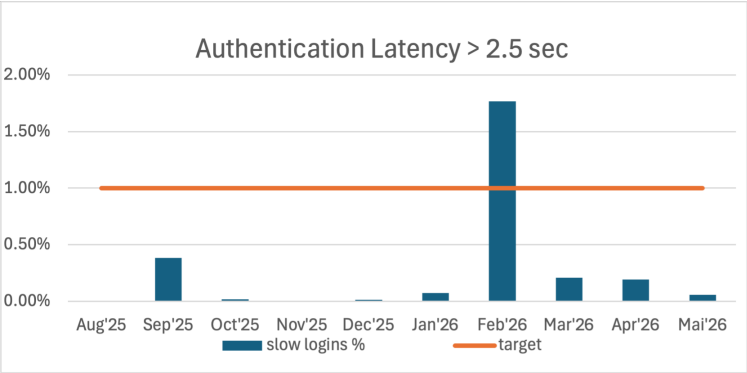
Login and **Discovery Service Availability**
Target: 99.9% per month (downtime < **43 minutes**)

*December 2025: one outage of 12h during the night of Dec 25th



Account Management Availability
Target: 99.5% per month (downtime < **3 h 36 min**)

See Presentation by Aris and Daniel on Infrastructure improvements



Login Latency
Target: 99% of requests responded to within 2.5s

*February 2026: measurement error during night-time backup.

Note: Downtimes include failures during and outside office hours.

Most used services

Unique users during March-May 2026

Service ID	Organisation	Uni members	non-Uni mem	Personal	total
https://shibboleth.brandsforstudents.ch/shibboleth	digt.ch (partner)	47518	322	470	48310
https://sdauth.sciencedirect.com/	elsevier.com (partner)	37853	452		38305
https://lms.uzh.ch/shibboleth	uzh.ch	31259	141	1951	33351
https://swisscovery.slsp.ch/mng/login	slsp.ch	26021	551	6619	33191
https://fsso.springer.com	springer.com (partner)	31114	507	140	31761
https://iam.atypon.com/shibboleth	atypon.com (partner)	28372	255	185	28812
https://cyberlearn.hes-so.ch/shibboleth	hes-so.ch	22225	97	1848	24170
https://moodle.zhaw.ch/shibboleth	zhaw.ch	22393	27	1001	23421
https://www.uzh.ch/shibboleth	uzh.ch	21536	96	142	21774
https://auth.asvz.ch/shibboleth	asvz.ch (partner)	21731	40		21771
https://iam.unil.ch	unil.ch	21352	0		21352
https://moodle.unige.ch/shibboleth	unige.ch	20870	423		21293
https://registration.slsp.ch/shibboleth	slsp.ch	10678	481	10089	21248
https://ilias.unibe.ch/shibboleth	unibe.ch	20174	34		20208
switchdrive_oidc_client_59552	switch.ch	18563	266	1096	19925
ecampus_gac_candidature	unige.ch	4570	210	14137	18917
https://moodle2.unil.ch/shibboleth	unil.ch	18343	43	51	18437
https://identity.fhnw.ch/saml2	fhnw.ch	16992	1	358	17351
https://moodle.fhnw.ch/shibboleth	fhnw.ch	16432	5	677	17114
https://age.hes-so.ch/shibboleth	hes-so.ch	16604	0		16604
pocketcampus-backend	pocketcampus.org (partner)	14874	733	550	16157
https://tube.switch.ch/shibboleth	switch.ch	12976	2651	217	15844
https://id-kslprod1.id-sys.unibe.ch/shibboleth	unibe.ch	14366	4		14370
https://iam-ext.unil.ch	unil.ch	7280	89	6637	14006
snf_portal	snf.ch	8786	239	4851	13876
https://adam.unibas.ch/shibboleth	unibas.ch	12234	6		12240

Switch

edu-ID strategy/pricing update

Christoph Graf, Rolf Brugger, Bastien Campagne

Summary

ONE MAIN GOAL

Working on reaching “**black zero**” (zero loss/benefit)

- Currently have a significant yearly deficit to balance
- Our status allows for 4 type of actions:
  - Increase market penetration
  - Reduce costs
  - Increase tariffs
  - Discontinue services

focus

Medium/long term

Several of our strategic options could lead to some savings, but with some impacts which need to be evaluated

Short term

- 2 stages (2027 & 28), focusing first on Federation Partners. Some might drop off.
- One main change would be the introduction of charges for Service Providers
- Details are under review with the Foundation Council. Final approval planned for November.

Switch

Short term: reaching Black Zero - scenario overview

1. Growth & Scale
Increase investments today to keep innovating and build a strong future proof solution

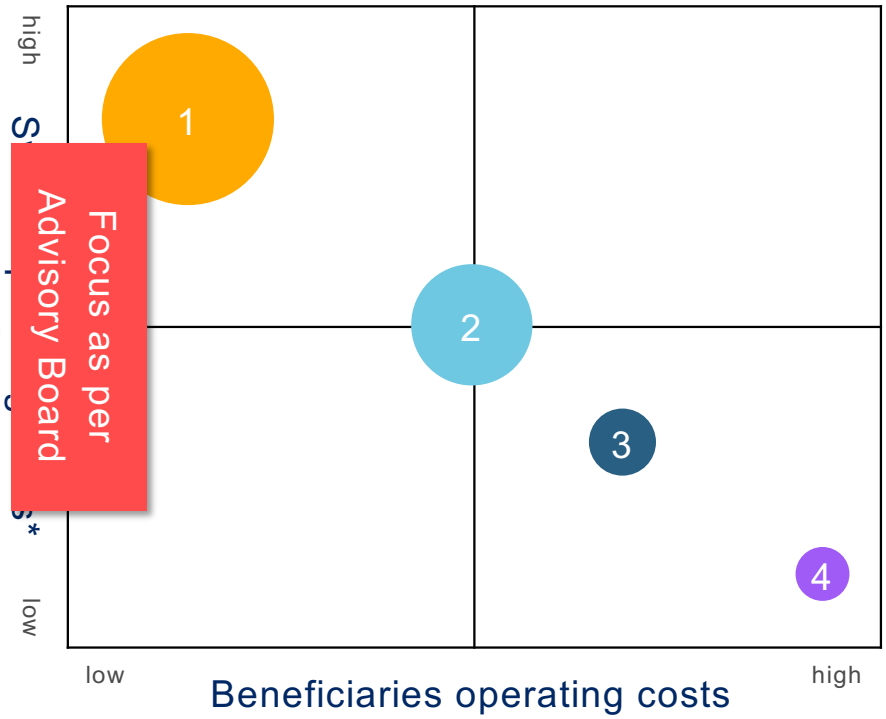
2. Value Preservation
Keep current FTE and budget. Increase tariff and/or prices to cover costs.

3. Strip down edu-ID
Reduce edu-ID services. Reduce costs to the current level of funding.

4. Rollback to AAI & rebuild limited federation
Roll back to AAI only functionalities

Focus as per Advisory Board

Bubble sizes: value provided by the solution



Switch

*: estimation, compared to 2026 budget

Medium/long term potential strategical updates

Switch Cloud migration (planed for 26/27)

- Increases infrastructure management efficiency

e-ID integration

- Allows to validate some attributes automatically (identity)
- Reduces universities' verification efforts

Allow Universities to use their own authentication (Rethinking edu-ID)

- Allows Universities to use only their IdP (with provided security)
- No more authentication from edu-ID?

Educational Wallets

- Allows users to store validated documents (diplomas…)
- Reduces universities' verification efforts

Use AGOV to authenticate

- transfer authentication to AGOV
- No more authentication from edu-ID?

Transfer Support Level 1 to Universities

- Reduces support efforts on Switch
- Would require new admin APIs

Extension to Tertiary B & Sek II

- Increases audience
- Allows to split costs

Note: all are under analysis (except Cloud migration), and ***may or may not*** be implemented according to analysis results and Foundation decision.

Switch

OpenID Connect identity model

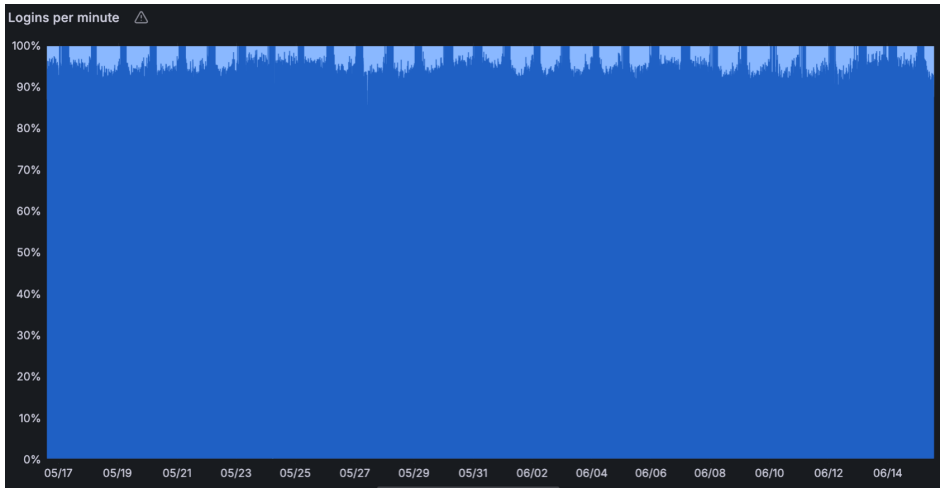
Frédéric Gerber, Sascha Hoppler, Zoltan Umlauf

In the past 30 days…

OIDC logins

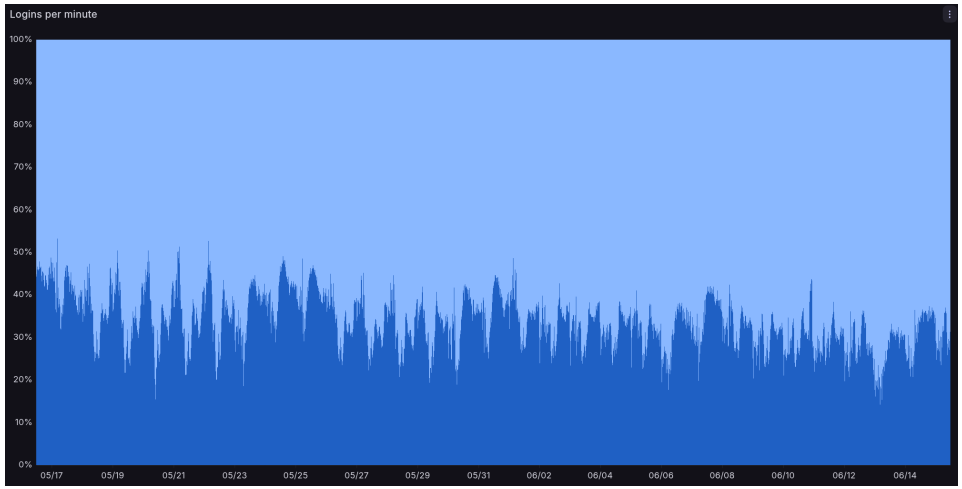
SAML logins

🇨🇭



Switch edu-ID

🇳🇴

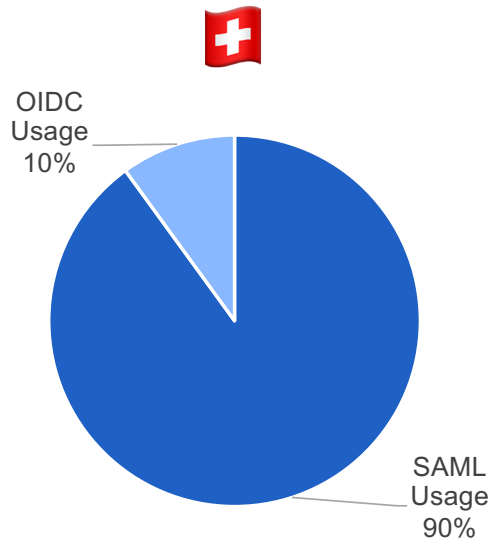


Feide

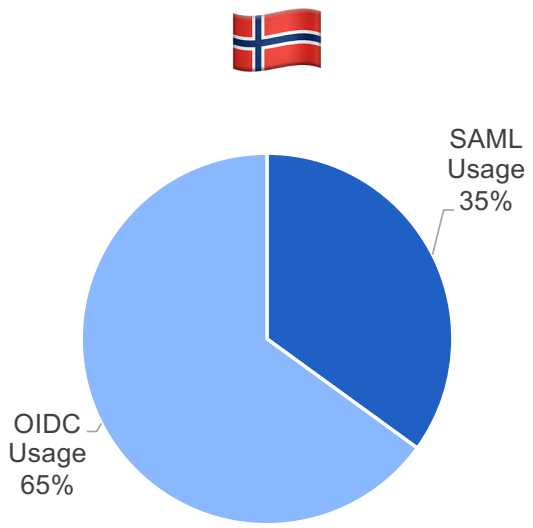
SAML vs OIDC Usage

OIDC logins

SAML logins

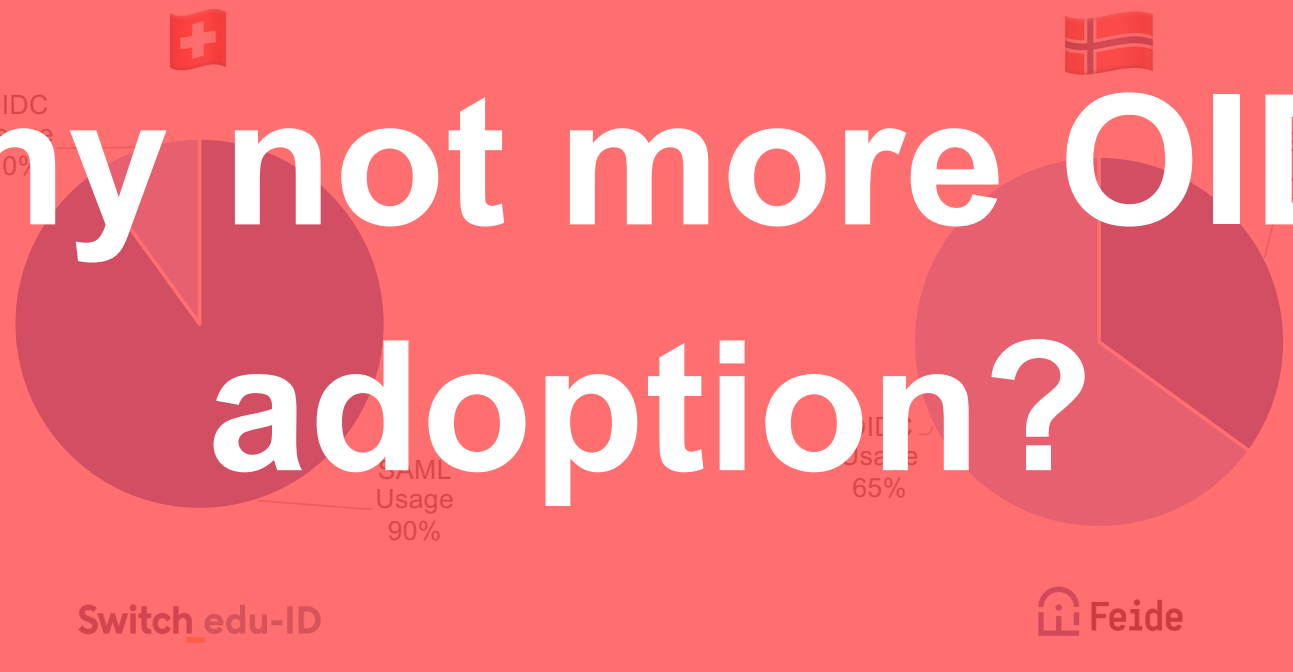


Switch edu-ID



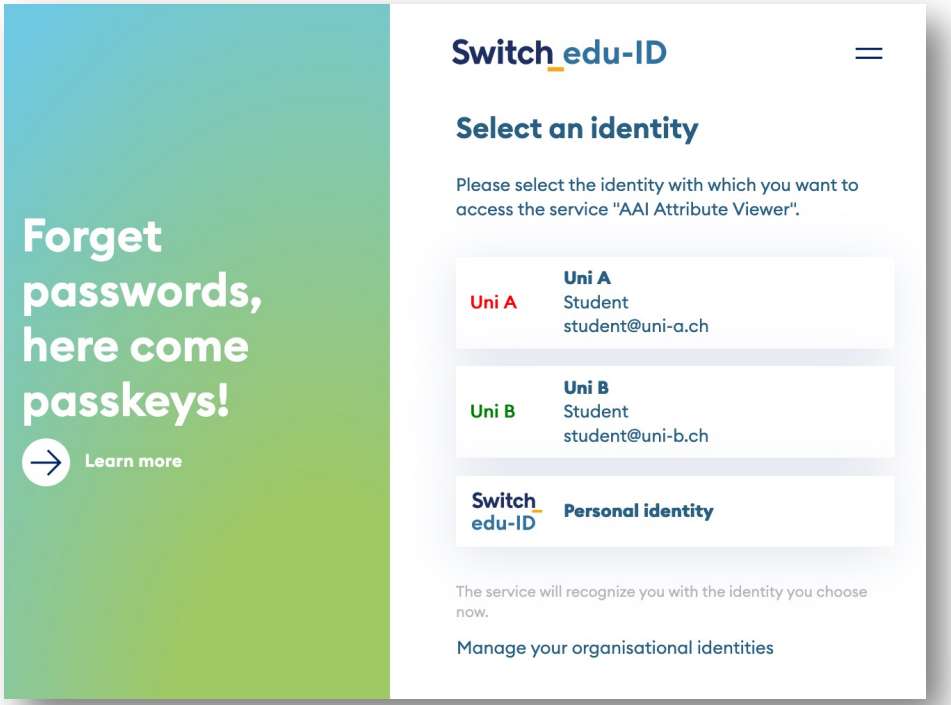
Feide

SAML vs OIDC Usage



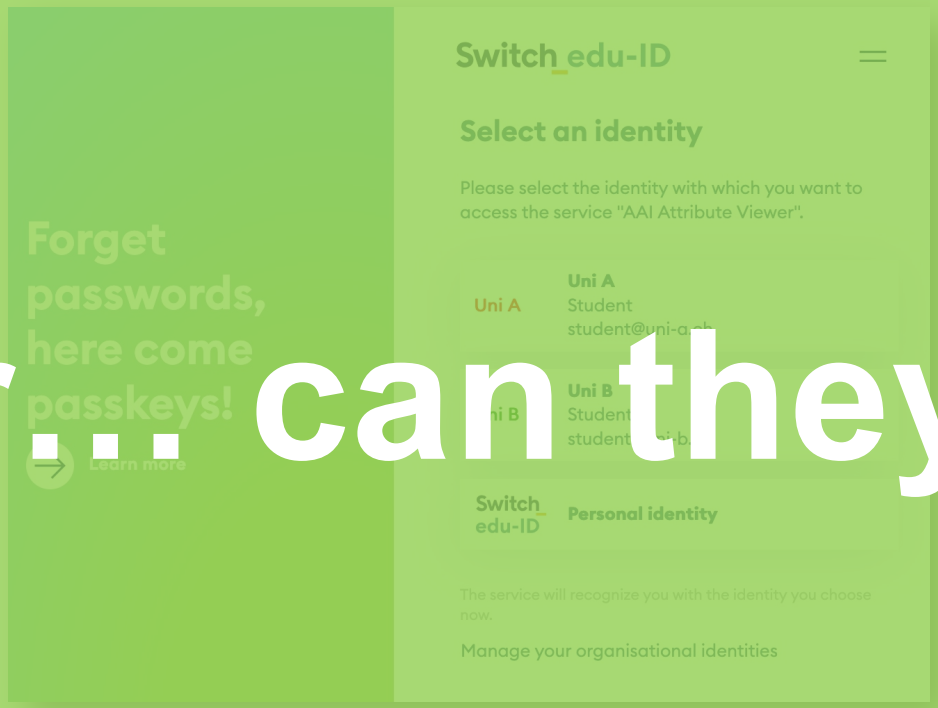
Why not more OIDC adoption?

With SAML, users can choose an identity when they log in



With OIDC, they cannot!

With SAML, users can choose an identity when they log in

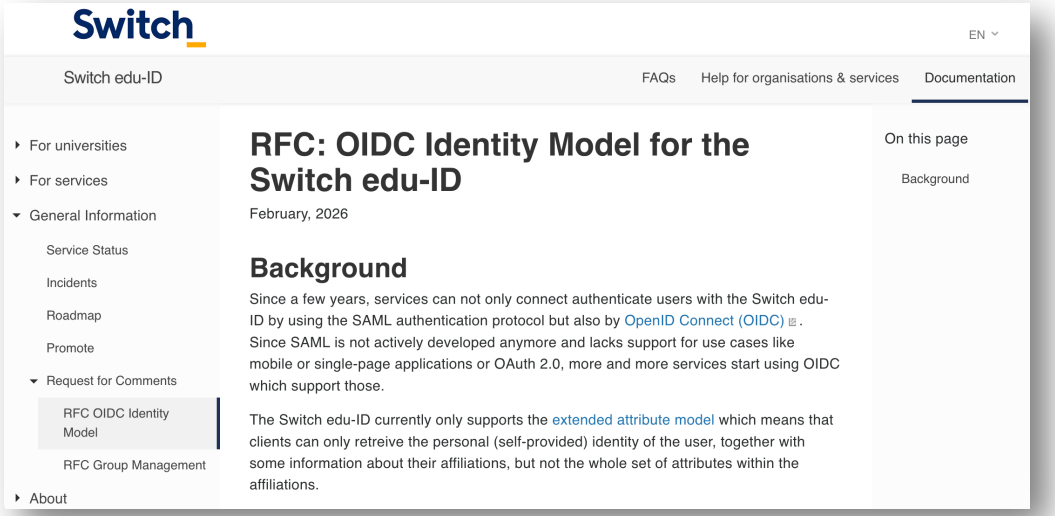


or... can they?

With OIDC, they cannot!

Request For Comments (RFC): OIDC Identity Model

February	March	April	May	June	Summer 2026
Published RFC	Received feedback	Implementation + internal testing			



https://help.switch.ch/eduid/docs/gen/rfc/rfc2026oidc/

Let's do some terminology lesson

Personal identity

```
swissEduPersonUniqueID: 0000597199059855@eduid.ch
mail: alex.taylor@example.org
givenName: Alex
surname: Taylor
swissEduPersonSshPublicKey: ssh-rsa AAAA...
```

Affiliation identities

```
swissEduPersonUniqueID: 2490257@uni-demo.ch
swissEduPersonHomeOrganisation: uni-demo.ch
mail: alex.taylor@uni-demo.ch
eduPersonAffiliation: ["student", "member"]

givenName: Alex Tim
surname: Taylor
uid: ataylor
unidemoSapUserID: 212599
```

```
swissEduPersonUniqueID: 123876@uni-partner.ch
swissEduPersonHomeOrganisation: uni-partner.ch
mail: alex.taylor@uni-partner.ch
eduPersonAffiliation: ["staff", "member"]

givenName: Alex
surname: Taylor
uid: a.taylor
uniPartnerChPublicId: alex.taylor
uniPartnerChRoles: ["admin", "user"]
```

Personal identity model

```
"sub": "MFRGGZBAMVTGO2AKN5YHC4RAON2HK5QK",
"swissEduPersonUniqueID":
"0000597199059855@eduid.ch",
"email": "alex.taylor@example.org",
"family_name": "Taylor",
"given_name": "Alex",
"swissEduPersonSshPublicKey":, "ssh-rsa AAAA...",
...
```

Affiliation identity model

(formerly known as classic model)

```
"sub": "N5XGQ3DPMRUW42LONFZHG5KAMJ2GKZRA",
"swissEduPersonUniqueID": "2490357@uni-demo.ch",
"swissEduPersonHomeOrganisation": "uni-demo.ch",
"email": "alex.taylor@uni-demo.ch",
"family_name": "Taylor",
"given_name": "Alex Tim",
"uid": "ataylor",
"eduPersonAffiliation": [
  "studenet",
  "member"
],
"unidemoSapUserID": "212599",
...
"swissEduIDUniqueID": "0000597199059855@eduid.ch"
```

Extended identity model

```
"sub": "MFRGGZBAMVTGO2AKN5YHC4RAON2HK5QK",
"swissEduPersonUniqueID":
"0000597199059855@eduid.ch",
"email": "alex.taylor@example.org",
"family_name": "Taylor",
"given_name": "Alex",
"swissEduPersonSshPublicKey":, "ssh-rsa AAAA...",
...
"swissEduIDLinkedAffiliationUniqueID": [
  "2490257@uni-demo.ch",
  "123876@uni-partner.ch"
],
"swissEduIDLinkedAffiliation": [
  "member@uni-demo.ch",
  "student@uni-demo.ch",
  "member@uni-partner.ch",
  "staff@uni-partner.ch"
],
"swissEduIDLinkedAffiliationMail": [
  "alex.taylor@uni-demo.ch",
  "alex.taylor@uni-partner.ch"
]
```

Implementation: Do not reinvent the wheel

OID Federation

Same functionality as for SAML*

*and more

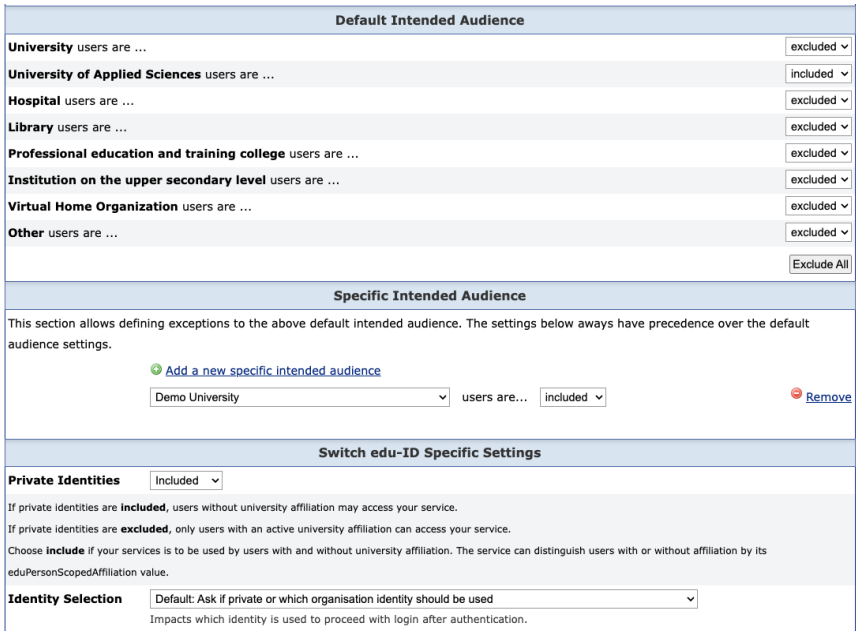
Make use of OIDC specifications

(Virtual) issuer per organisation

Implementation: Do not reinvent the wheel

…and which identity do I get now? → You decide!

Resource Registry



Authentication request

```
https://login.eduid.ch/idp/profile/oidc/authorize?
  response_type=code
  &client_id=unidemo_moodle

&scope=openid%20profile%20email%20https%3A%2F%2Flogin.eduid.ch%2Fauthz%2FUser.Read
  &redirect_uri=https%3A%2F%2Fclient.example.org%2Fredirect
  &state=af0ifjsldkj
  &claims=%7B%22id_token%22%3A%7B%22eduid_idp%22%3A%7B%22essential%22%3Atrue%2C%22
          values%22%3A%5B%22uni-demo.ch%22%2C%22eduid.ch%22%5D%7D%7D%7D
```

```
"claims": {
  "id_token": {
    "eduid_idp": {
      "essential": true,
      "values": ["uni-demo.ch", "eduid.ch"]
    }
  }
}
```

ID Token: *(signed by https://login.eduid.ch/)*

```
{
  "sub": "MFRGGZBAMVTGO2AKN5YHC4RAON2HK5QK",
  "iss": "https://login.eduid.ch/",
  "eduid_idp": "eduid.ch",
  "aud": "unidemo_moodle",
  ...
  "swissEduPersonUniqueID": "0000597199059855@eduid.ch",
  "email": "alex.taylor@example.org",
  ...
}
```

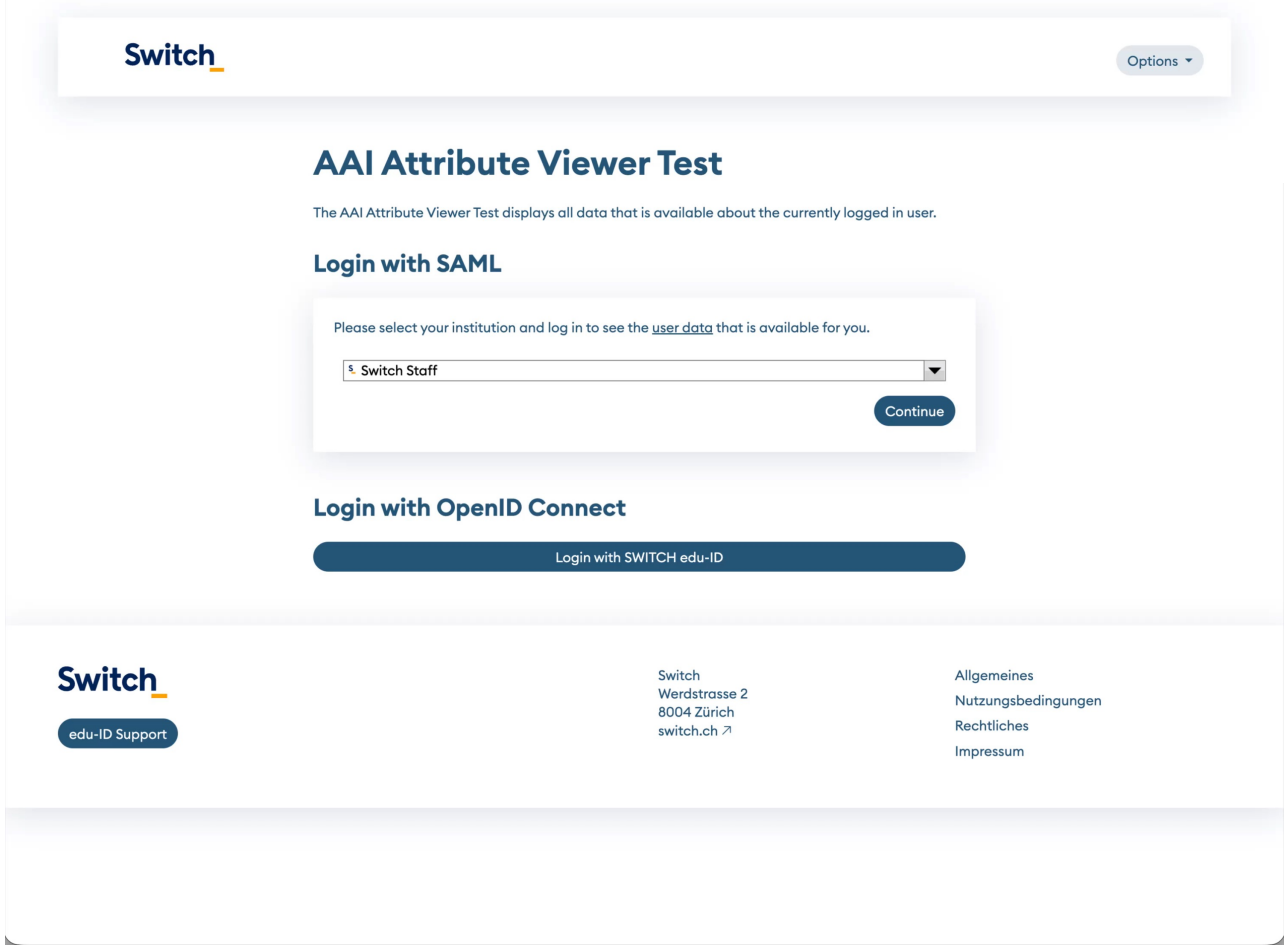
ID Token: *(signed by https://login.eduid.ch/)*

```
{
  "sub": "N5XGQ3DPMRUW42LONFZHG5KAMJ2GKZRA",
  "iss": "https://login.eduid.ch/",
  "eduid_idp": "uni-demo.ch",
  "aud": "unidemo_moodle",
  ...
  "swissEduPersonUniqueID": "2490357@uni-demo.ch",
  "email": "alex.taylor@uni-demo.ch",
  ...
}
```

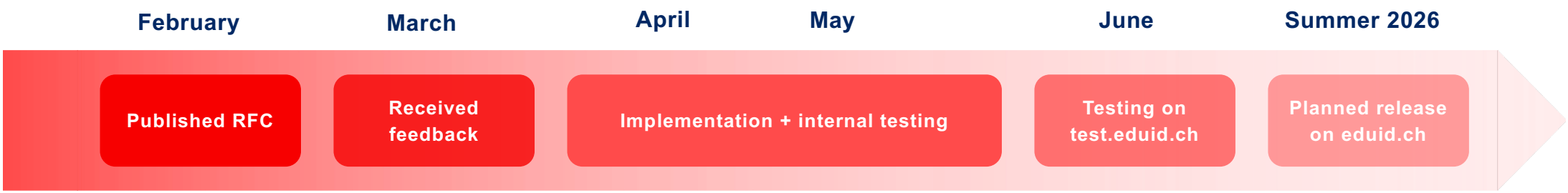
See RFC for details

Demo

https://attribute-viewer.aai.switch.ch/?lang=en&expert_view



Call For Action and Planned Release



How to get started

- In the Resource Registry's "edu-ID Test: SAML and OIDC" federation register your OIDC client (if new)
  - Under "Intended Audience and Expert Settings" include at least some organizational identities
- Create test affiliations for your test edu-ID account in the Account Management
  - Make sure you have at least one affiliation that is allowed by your RR service configuration
- Point your OIDC client to our test IdP: Well-Known Config endpoint with all the details
  - Alternatively, you can repeat our demo with the Attribute Viewer. Just make sure to select "Login with Switch edu-ID test" to get routed to our test IdP
- More detailed guidance will follow, as we revamp our documentation pages!

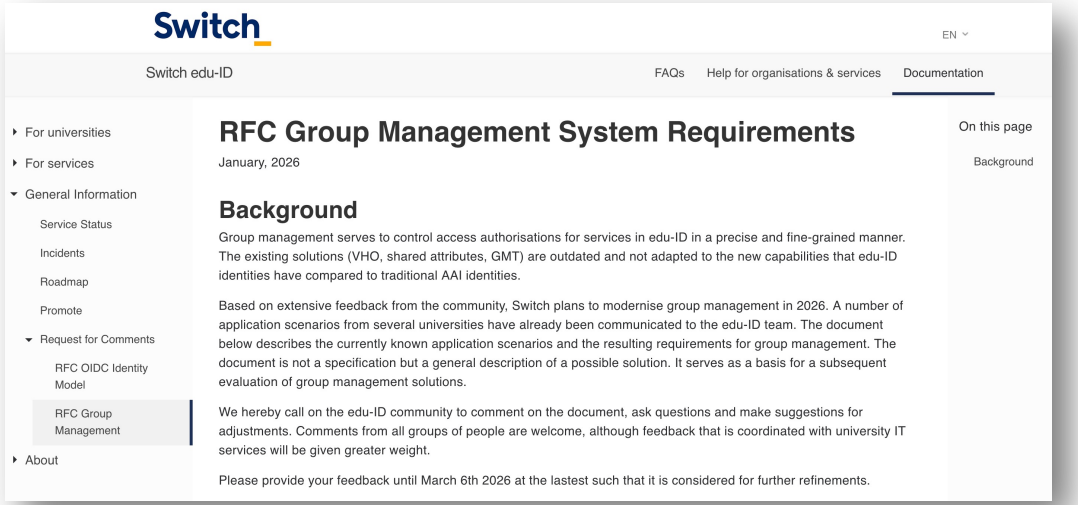
Switch

Group management system

Rolf Brugger

Request For Comments (RFC): Group Management System

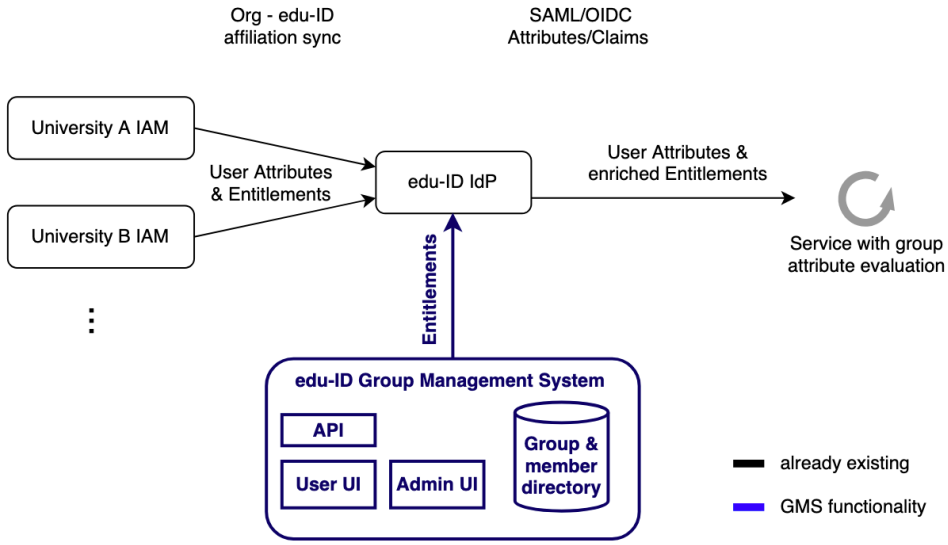
February	March	April	May	June	Summer
Published RFC	Received feedback	Finalizing requirements	Pre-evaluation of GMS candidates		Evaluation of GMS shortlist



Final version of requirements
https://help.switch.ch/eduid/docs/gen/rfc/rfc2026gms/

Summary of Requirements

- 7 concrete use cases at universities.
- RFC feedback from 6 universities.
- Switch requirements to replace VHO and shared attributes API.
- Collected cases over the past years.



- Delegated member management
  - Member addition/removal by email: individual or mass invitation by CSV list
  - Member addition/removal by SCIM API
- Hierarchical groups
- Freely definable entitlement values
- Membership lifecyle with auto expiration

Evaluation short list

Grouper

CoManage

OpenConext Teams

Switch

Improvements to the infrastructure

Daniel Lutz, Aris Fkiaras

Improvements since last year

After a few incidents last year, we took actions to improve our resilience and automate fail-over:

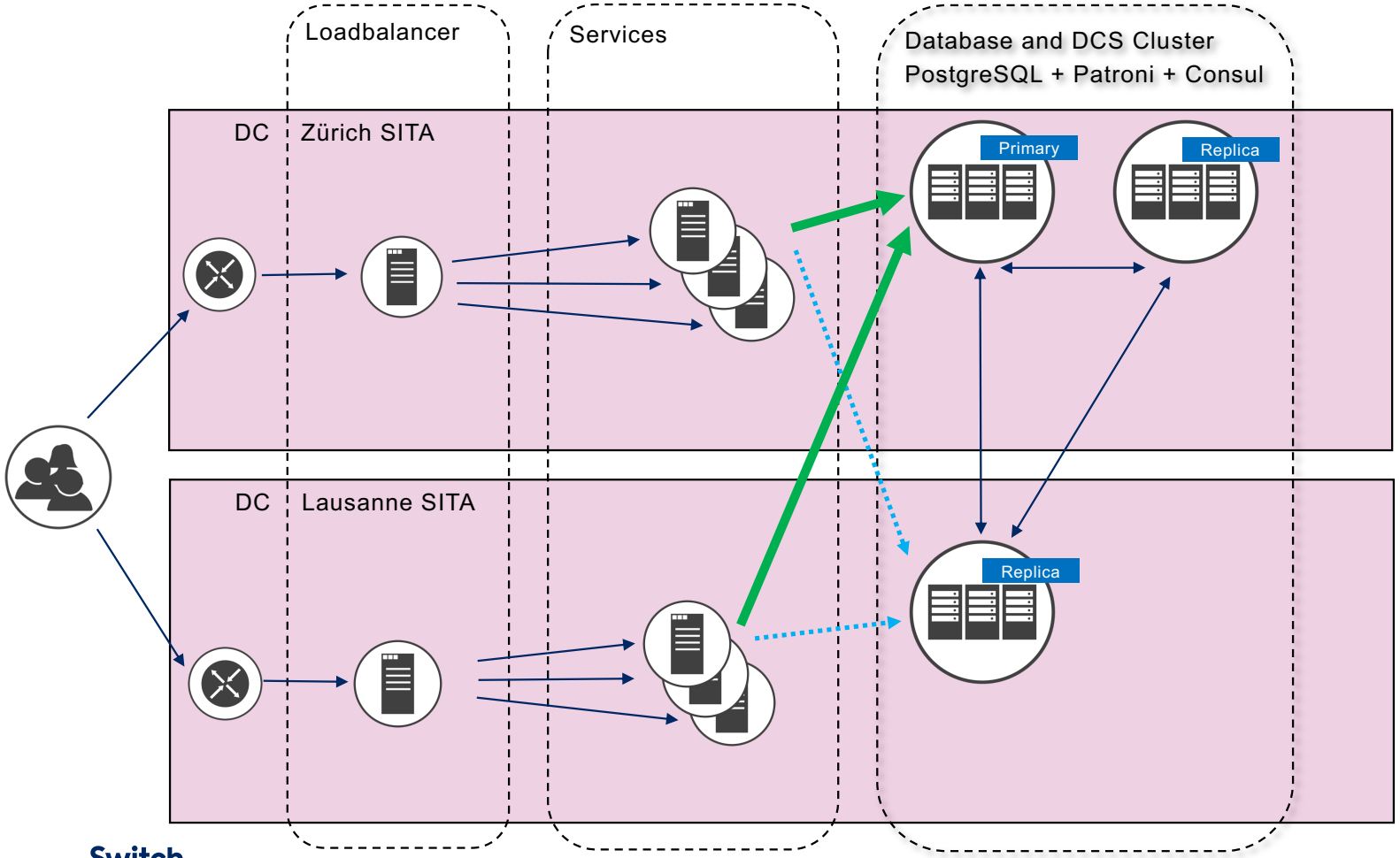
- The database cluster is now resilient to outage of a datacenter.
- All TLS certificates are automatically managed via ACME. Monitoring of the certificates ensures that failures are detected early to prevent any outage.
- We hired a new HA Infrastructure Specialist to strengthen the team for managing the edu-ID specific infrastructure.

Switch

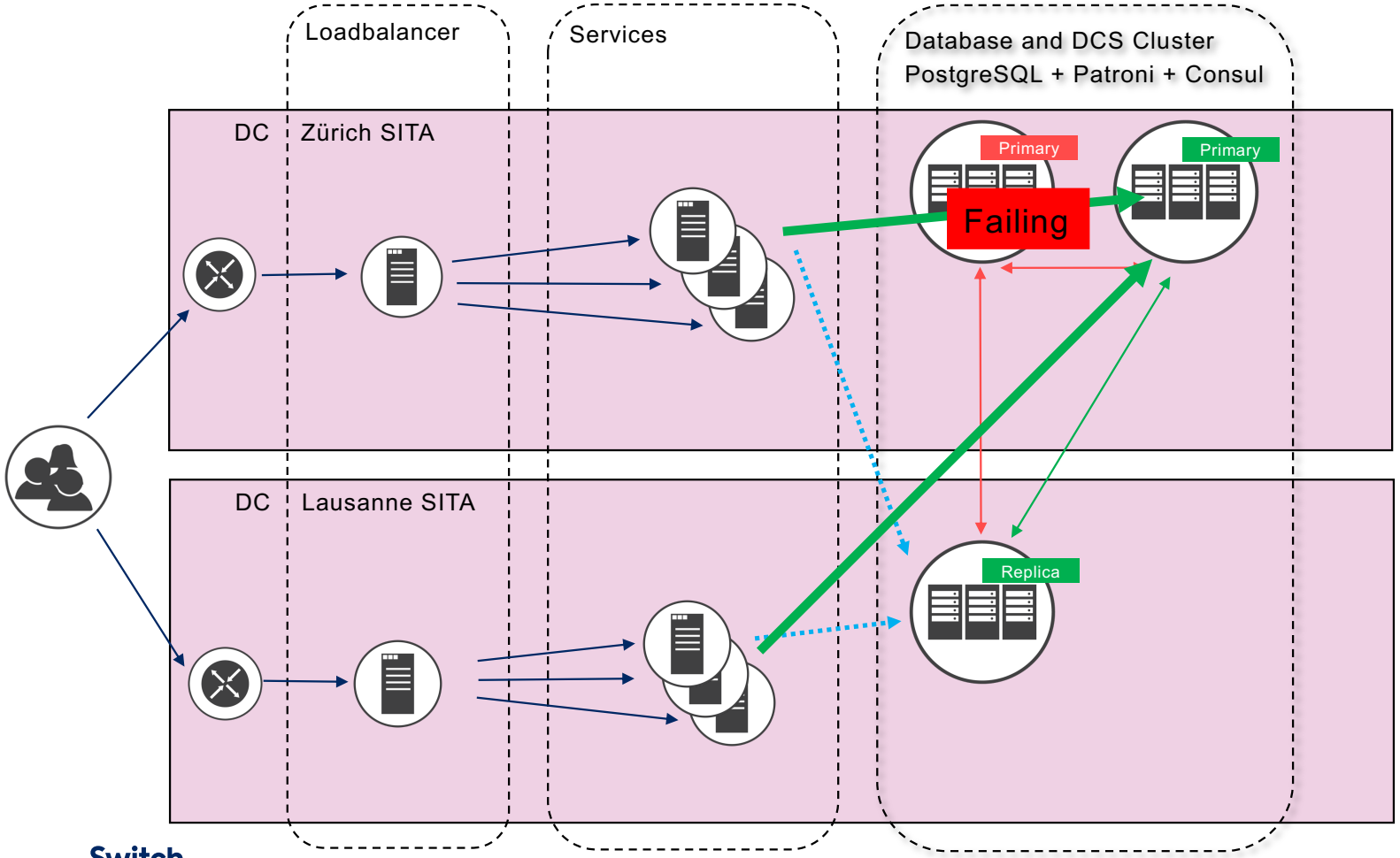
What happens if a datacenter fails?

Daniel Lutz, Aris Fkiaras

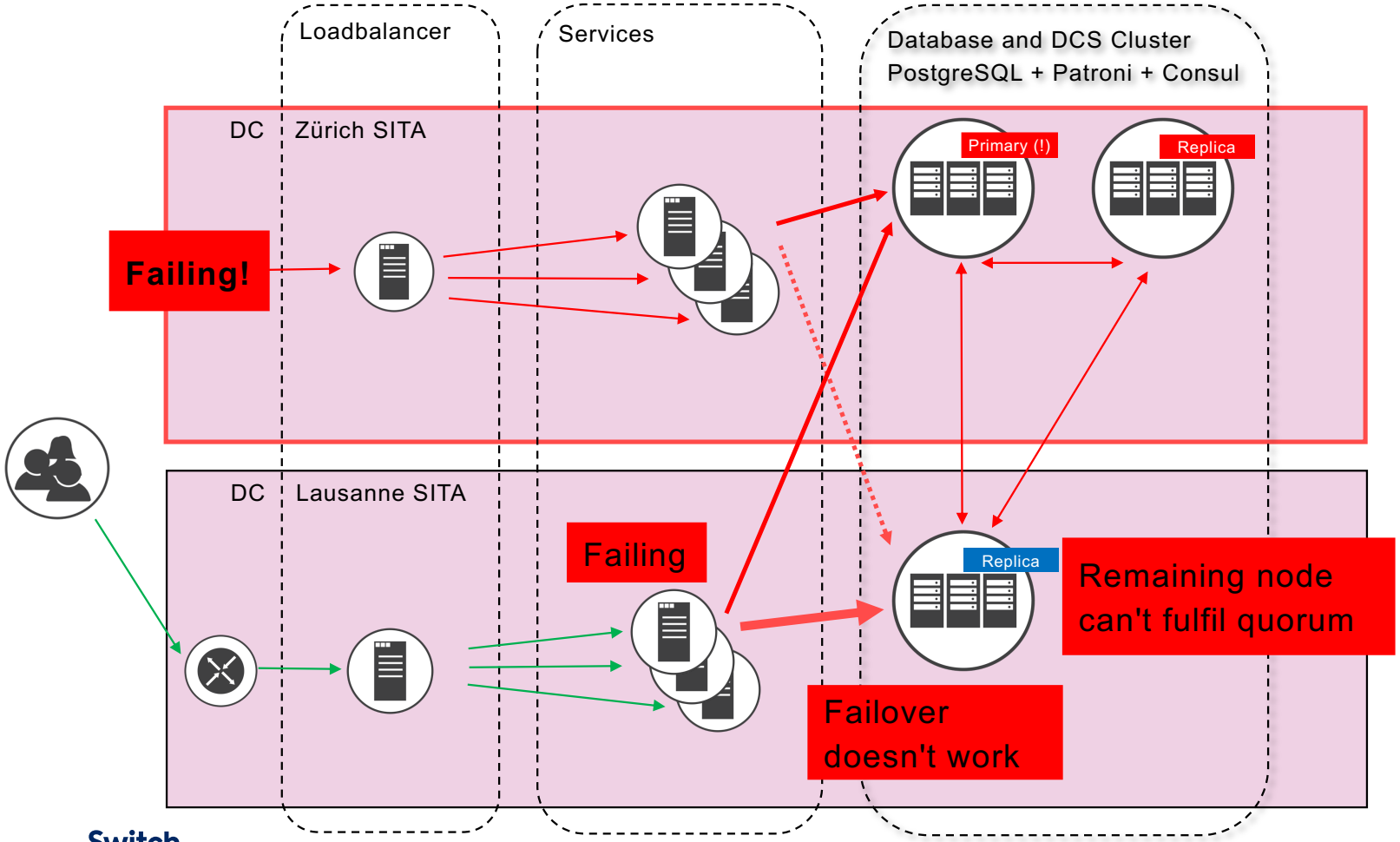
Looking back: Outages in October/December 2025



Failure of a single node: Automatic failover



Failure of datacenter: Outage



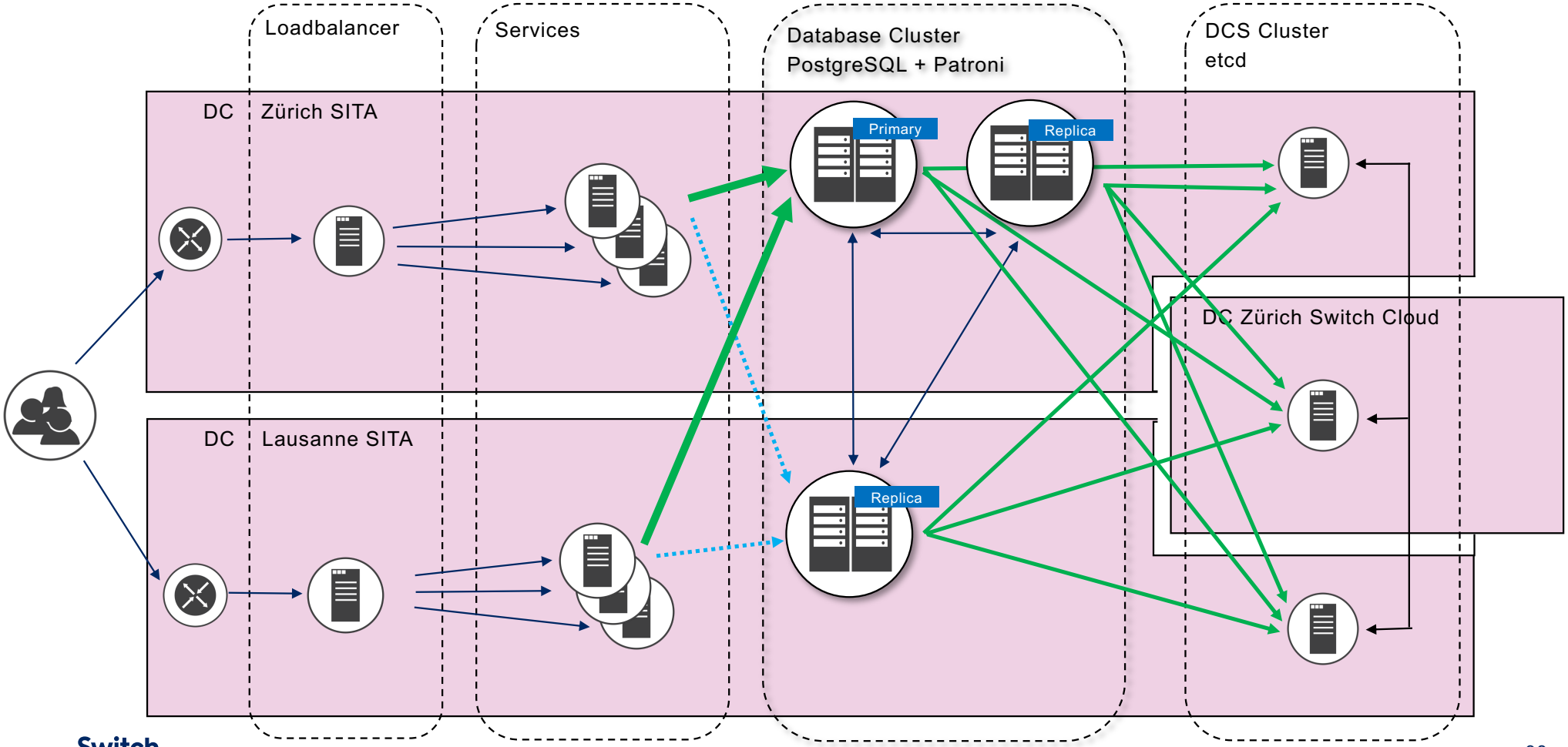
Looking back: Outages in October/December 2025

Setup:
– HA PostgreSQL cluster with 1 primary node (r/w) and 2 replica nodes (r/o), with (fast) asynchronous replication
– Using Patroni to manage the PostgreSQL replication automatically
– Using Consul as DCS for Patroni (DCS: "Dynamic Configuration Store", Consul: HA key-value store)

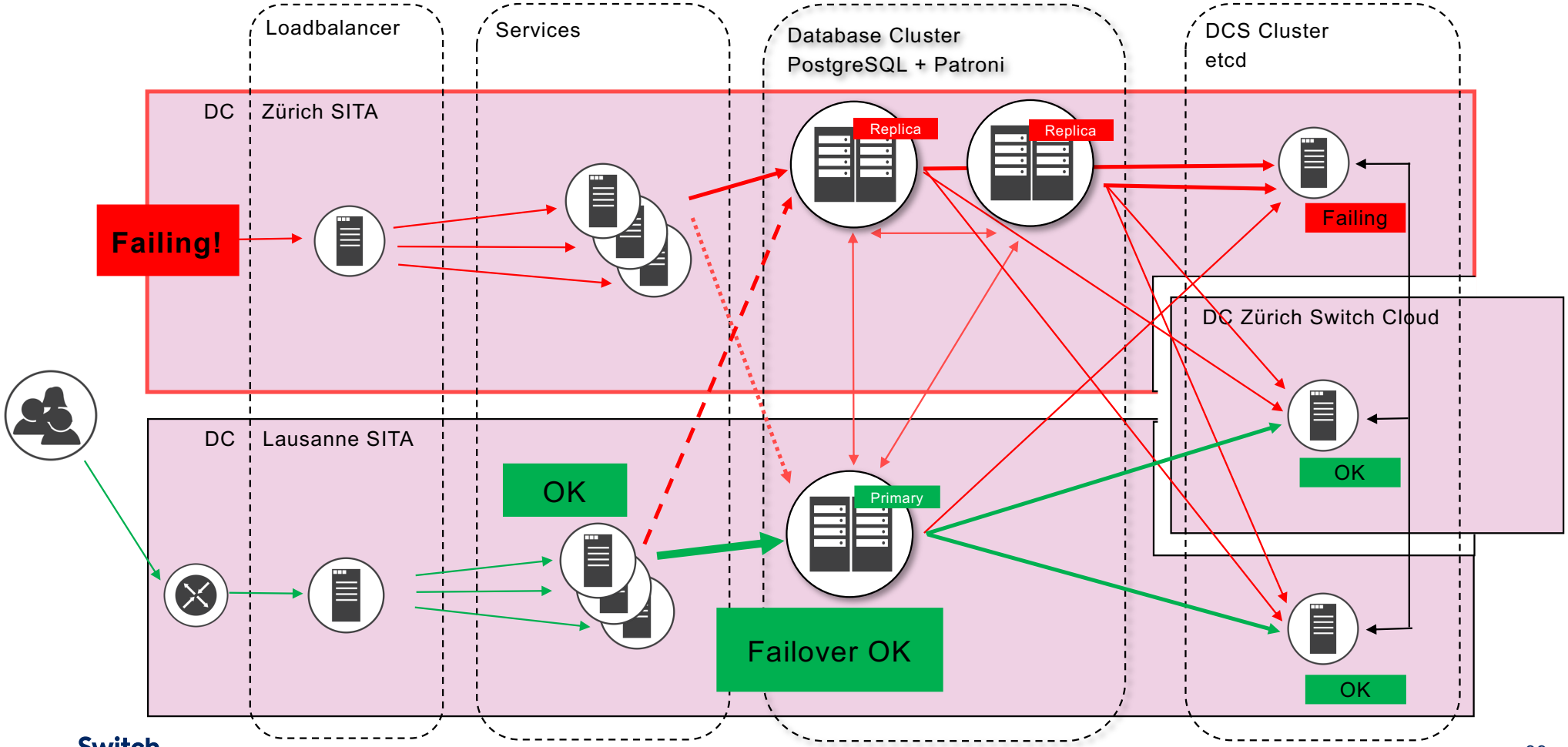
Outage:
– If a single PostgreSQL node fails, another one can take over as primary.
– But: There were full outages of the datacenter "SITA Zürich" due to power issues in the datacenter
– All requests to the Switch edu-ID services were re-directed to the datacenter "SITA Lausanne" (via Anycast)
– But: Patroni couldn't do an automatic failover, since the single Consul node in the datacenter "SITA Lausanne" couldn't get the quorum

Problem:
– The Patroni cluster with Consul wasn't designed for an outage of a datacenter.
– A manual failover was tricky, and it required experienced people to be available.
– On December 25 in the evening, we couldn't risk to do the manual failover. We could do it in the morning of the 26 December.

Improvement: A datacenter might fail!



Improvement: A datacenter might fail!



Improvement: A datacenter might fail!

Setup:

– HA PostgreSQL cluster with 1 primary node (r/w) and 2 replica nodes (r/o), with (fast) asynchronous replication
– Using Patroni to manage the PostgreSQL replication automatically
– Using **etcd** as DCS for Patroni (DCS: "Dynamic Configuration Store", **etcd**: HA key-value store) (simpler than Consul)
– etcd runs as a cluster in **3 datacenters**

Outage:

– There might be a full outage of the datacenter "SITA Zürich", e.g. due to power issues in the datacenter
– All requests to the Switch edu-ID services are re-directed to the datacenter "SITA Lausanne" (via Anycast)
– *Patroni needs to failover the primary node to the datacenter "SITA Lausanne"*

Solution:

– The Patroni cluster with etcd and 3 datacenters is now ready for an outage of one datacenter.
– Patroni can do a failover automatically, since the DCS (etcd) is still healthy.

Switch

Migration to Switch Cloud

Daniel Lutz, Aris Fkiaras

From SITA to Switch Cloud

In the second half 2026 and 2027, Switch services running on our internal enterprise virtualisation platform "SITA" are migrated to the Switch Cloud. This includes the Switch edu-ID service.

Key differences:

SITA	Switch Cloud
RHEV based, central Switch Support	OpenStack based, self-service
Internal to Switch only	Community solution
Very stable, in use for many years	Stable, but new

Plan

- Run most edu-ID components in Switch Cloud Kubernetes to reduce maintenance effort, automate operations and increase our velocity
- Perform load testing and reliability testing before any switch-over
- All edu-ID components are designed to be resilient to outages

What it means for you

- The switch-over will be transparent, there should not be any impact for users.
- Reduced capacity of the Switch edu-ID team in Q3/Q4 for new features, but for the sake of strengthening our service
- After the migration, we will be able to release new features more frequently and with greater confidence, and the costs for operations are expected to be lower.

Switch

MFA Everything Everywhere All at Once

Lukas Hämmerle, Rolf Brugger, Filippo Costa


MFA
EVERYTHING
EVERYWHERE
ALL AT ONCE

MFA in Switch edu-ID

<table>
<tr><td colspan="3">MFA = 2FA + Other Measures</td></tr>
<tr><td colspan="2">Two-Factor Authentication (2FA)*
(= require more factors (e.g. smth. you know, you have, you are))</td><td rowspan="4">Other Measures
(= more factors or risk-based access control)</td></tr>
<tr><td>Two-Step Login
(= requires login in 2 steps)</td><td>Passkey
(= single step login)</td></tr>
<tr><td>Username / Password</td><td rowspan="2">Phone, Computer, Hardware
+
User Verification</td></tr>
<tr><td>TOTP or mTAN</td></tr>
</table>

Why is MFA so important?

- Passwords are often reused and occasionally get leaked
- Strong / Multi Factor Authentication ensures that password compromise does not allow direct access to user resources

- Data shows that the user is the weak link of the security chain
  - But, we cannot expect that all the users behave perfectly and we cannot blame them

It is our responsibility to provide robust-enough systems

From: 🔗 **Top security risk? Framing people as the weakest link**
Cornelia Puhze, Switch, at TNC26

What do we provide?

SMS

+ Simple and understood

- Depends on the phone network
- Considered less secure
- Additional costs

Not recommended!

TOTP

+ Always available (with a phone)
+ Generally secure

- Not always understood
- Needs care/backup when phone is changed or lost

Passkeys

+ Quick and secure
+ No password required

+/- New technology

- Depends on browser support
- Credentials have to be available
- Backup and transfer can be cumbersiome

MFA usage

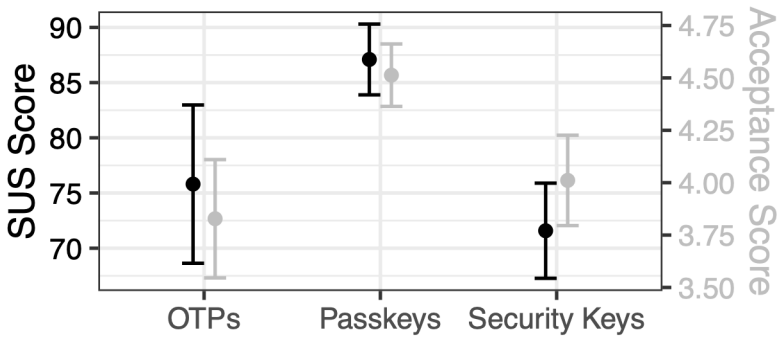
at the end of…	May 2024	May 2025	May 2026
Active users	1'095'000	1'295'000 (+18%)	1'455'000 (+12.3%)
With MFA	205'000	242'000 (+18%)	400'000 (+65.3%)
With TOTP	134'000	160'000 (+19.5%)	261'000 (+63%)
Share of TOTP	65.3%	66.1%	65.1%
With one or more passkeys	~ 0	18'000	78'000 (x4.3)
Weekly authentications with MFA			750'000
When SMS/mTAN was requested *		26'000	29'000 (+11.5%)
When TOTP was requested *		72'000	106'000 (+47%)
With a passkey		30'000	103'000 (x3.4)
Weekly authentications without MFA			300'000
Monthly sent SMS		146'200	153'600
- Reduction in costs due to provider contract changes			- 20%

* Second factor can be stored up to 30 days and it is not requested at every login

Passkeys and usability

Organisation: Munich University of Applied Sciences, about 19k students and 2k employees
MFA options: password + TOTP or security key (FIDO2) as second factor, passkeys without password

Lab tests (n=92)



	Usability (SUS)	Acceptance	Speed (sum)
Passkeys	87.10	4.51	559s
TOTP	75.81	3.83	676s
Sec. keys	71.58	4.01	801s

Setup time

Method	n	Median	p25	p75	p90
TOTP	28,455	42.0 s	26.0 s	79.0 s	150.6 s
Passkeys	16,097	12.0 s	9.0 s	23.0 s	37.0 s
ND-FIDO2	3,482	18.0 s	10.0 s	32.0 s	56.0 s

Setup success rate

	Success		Failed		Abandoned	
Method	n	%	n	%	n	%
TOTP	28,455	53.91	5,069	9.60	19,260	36.49
Passkeys	16,097	72.40	0	0.00	6,135	27.60
ND-FIDO2	3,482	14.88	566	2.42	19,357	82.70

Login time

Method	n	Median total	Median password	Median MFA
Passkey	1,257,912	4.48 s	–	4.48 s
PW+TOTP	2,004,362	22.64 s	4.45 s	15.17 s
PW+FIDO2	237,088	15.56 s	4.03 s	8.23 s

Data from E. Kupris, F. Ritterhoff - Hochschule München
🔗 TNC26, Passkeys for R&E, T&I Trial Mix session

Organizational MFA Policy

→ Policy under **control of the organisation** for its members

→ Is a **per-affiliation setting**

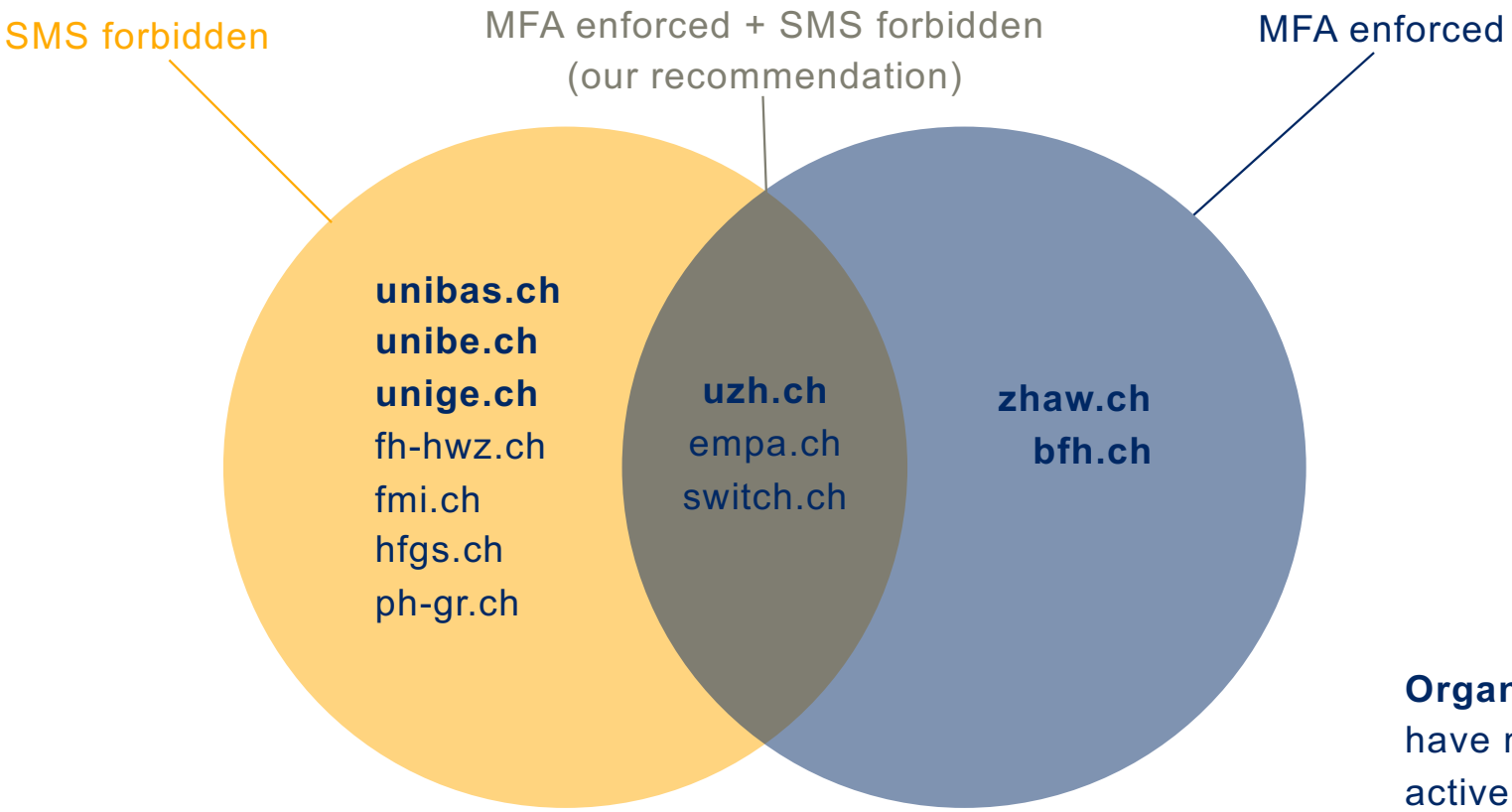
Set up by adapting the connector
- Affiliation push: Organisation
- Affiliation pull
  - Self-developed connector: Organisation
  - hosted connector: Switch

Attribute: `swissEduIDAffiliationSecurityPolicy`

```
{ "mfaPolicy":
  {
    "mode": "enforced",
    "maxDeviceTrustDuration": "P15D",
    "allowedSecondFactorTypes": ["totp", "sms"]
    }
}
```

User must use MFA for all services.
User has to renew the MFA session after 15 days.
User may use totp or mTAN/SMS as second factor.

Who has enabled what (26.05.2026)



Organisations in bold have more than 5000 active affiliations

Switch

MFA @UZH

Roberto Mazzoni (UZH)

SWITCH edu-ID & MFA

Roberto Mazzoni
16. Juni 2026

Ausgangslage

- März 2020
  - Corona Lockdown
  - Vorbereitung Rollout M365 (Microsoft TEAMS) in Vorbereitung
  - **Ausrollung TEAMS – von Beginn weg NUR MIT MFA (!)**
    https://www.news.uzh.ch/de/articles/2020/IT-Digitatlisierung.html
- Sensibiliseurng
  - https://www.uzh.ch/blog/zi/2022/12/13/wichtigkeit-der-multifaktor-authentifizierung-an-der-uzh
- 2022/2023:
  - Grosser Cyberangriff auf Uni Zürich: Polizei ermittelt
  - Universität Neuenburg wird erneut Opfer einer Cyberattacke
  - Report zur Cyberattacke an der HAW Hamburg | API Magazin

Unerfreuliche Massnahme

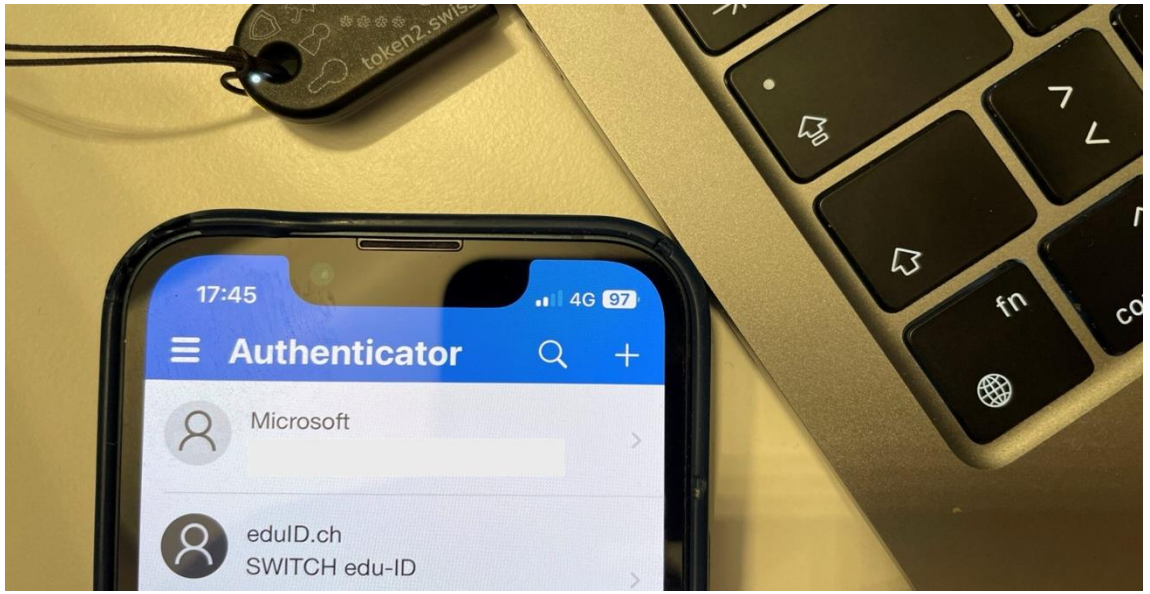
- Februar 2023: Alle Angehörigen der UZH müssen ALLE ihre Passwörter ändern
  - ADFS schon mit MFA
  - edu-ID und weitere Logins (auch VPN …) noch ohne MFA
- Sensibilisierung
  - https://www.uzh.ch/blog/zi/2023/02/28/it-sicherheit-eine-gemeinsame-verantwortung/
- Was wir schon 2020 wussten:
  - Login/Passwort alleine ist nicht sicher genug
  - MFA ist zwingend notwendig
  - Oder reklamiert jemand bei MFA bei den Bankapplikationen ?
  - Und weshalb soll das an den Hochschulen anders sein ?
- Und SWITCH? Kündigt enforcing von MFA für die edu-ID erst an …
  - https://identityblog.switch.ch/2023/08/29/two-step-login-changes/#more-3561

Es geht vorwärts

- Januar 2024
  - SWITCH edu-ID ermöglicht Passkeys (BRAVO)!
    - https://identityblog.switch.ch/2023/08/29/two-step-login-changes/#more-3561
    - Voraussetzung für Deaktivierung des 2. Faktors via SMS
    - Weil kein Smartphone für eine Authenticator App vorhanden sei …
  - VPN Lösung wird an der UZH durch eine MFA-fähige Lösung ersetzt
    - https://www.uzh.ch/blog/zi/2024/01/23/vpn-zugang-zum-uzh-netzwerk-mit-ivanti/
- September 2024: Endlich die Erlösung, MFA kann durch die Hochschulen erzwungen werden
  - https://identityblog.switch.ch/2024/09/05/enforcing-multi-factor-authentication-for-university-members/#more-3909
    - Wieso für jede Benutzer:in einzeln zu aktivieren statt für die OU ? Anforderung an SWITCH hätte nicht umgesetzt werden dürfen
    - Wieso Deaktivierung für SMS auch für jede Benutzer:in?

… und konsequent umgesetzt

- November 2024
  - Reglement über den Einsatz von Informatikmitteln an der Universität Zürich (REIM) wird ergänzt: Aus dem Internet zugängliche Services müssen mit MFA geschützt werden
    https://www.uzh.ch/blog/zi/2024/11/11/reim-neu-mit-vorgabe-zur-multifaktor-authentifizierung/
  - SMS als zweiter Faktor wird deaktiviert (Kosten, Instabilität, Sicherheit)
    https://www.uzh.ch/blog/zi/2024/11/22/switch-edu-id-mit-zwei-faktor-authentifizierung-sms-option-faellt-weg/
    - Kurz vor Prüfungen mit OLAT, geschützt durch SWITCH edu-ID
    - Mit Hilfe von SWITCH werden Prüfungsteilnehmende ermittelt, die noch keinen 2. Faktor eingerichtet hatten und diese angeschrieben
    - Danach - das ist die einzige E-Mail an alle Benutzer:innen im Zusammenhang mit MFA/SMA - werden alle angeschrieben



Universität Zürich[UZH]

Switch

Saving Private E-Mail

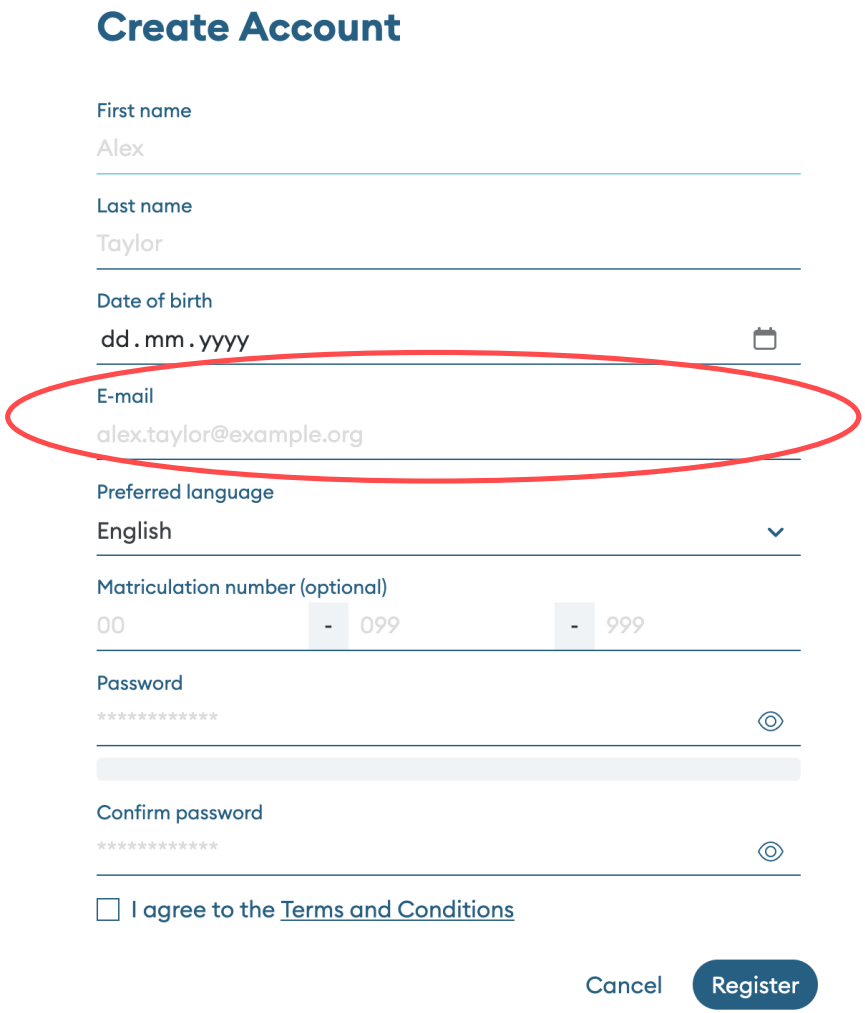
Lukas Hämmerle

edu-ID Account Creation

- edu-ID provides life-long identity
  - University "life" is shorter than real life
  - University e-mail address is lost after employment/studies

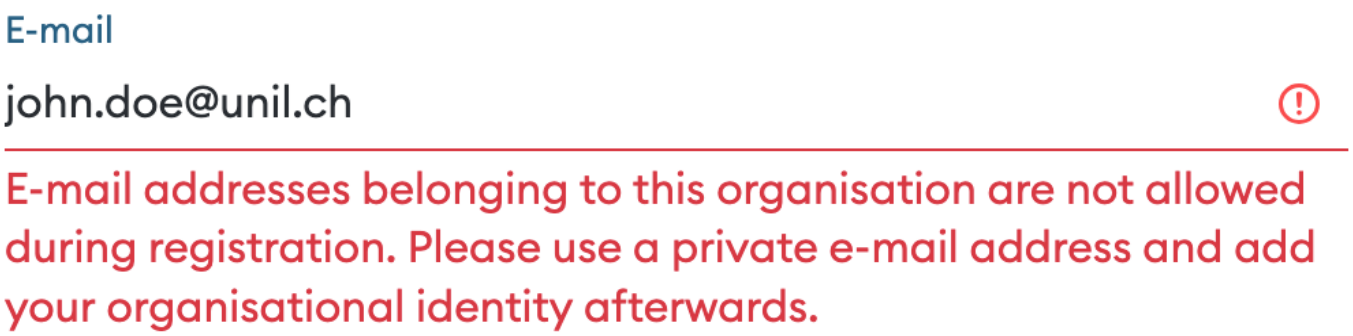
- edu-ID account always needs working e-mail address
  - Therefore, at least one private e-mail should be added
  - Private e-mail from an e-mail provider like Bluewin/Gmail/GMX/... that is long term available.

- edu-ID encourages users to have at least one private e-mail besides university e-mail
  - But this is not always enough



How to require a private e-mail

- Block university e-mail address during account creation
- University e-mail address can (and should) still be added **after account creation.**



Today: Two steps to block e-mail domains

Resource Registry (rr.aai.switch.ch) – Home Organisation Description – Descriptive Information

1

Organisation e-Mail Domain Names

hesge.ch eesp.ch hefr.ch hetsl.ch heig-vd.ch he-arc.ch hevs.ch hes-so.ch hesav.ch ecolelasource.ch changins.ch hemu-cl.ch ecal.ch

Space-separated list of e-mail domain names that are used for e-mail addresses controlled by this organisation. These domain names are also used by edu-ID to determine if an e-mail address is an organisation address.

Example value: `fernuni.ch unidistance.ch`

2

edu-ID Settings

The settings below affect the behaviour of the Switch edu-ID service for users of this organisation.

Block e-mail domains

☑ Block e-mail addresses matching domain hints during account creation

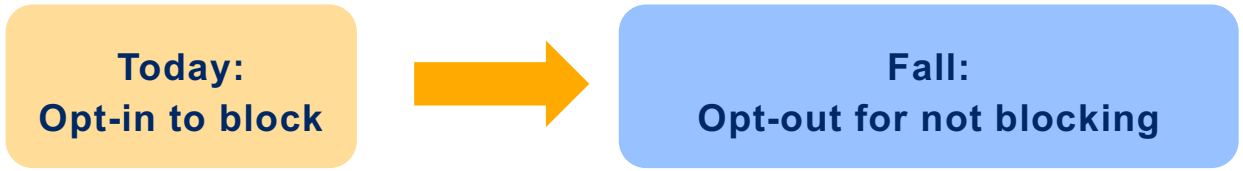
If enabled edu-ID users cannot create an account using an e-mail address matching a (sub-) domain name mentioned in the Organisation e-Mail Domain Names form above. This ensures that users provide a personal e-mail address for account creation instead of an organisational e-mail address. Organisational e-mail addresses can of course be added later after account creations, e.g. to link an organisational identity.

Please note that changing the domain names above or this setting may take a while until changes become active due to caching.

Tomorrow: Block by default

- Currently: 16 (~25%) of 67 organisations block own e-mails during account creation.
  - No issues known with this approach
- 80% of all 458'000 users with an affiliation already have a private e-mail.
  - For 7 organisations less than half have a private e-mail
- We propose to change default in fall 2026
  - By default all university domains would be blocked
  - Opt-out still would be possible via Resource Registry

What do you think about proposal?



- Are there users who don't have a private e-mail address?
- Do students/staff members already require a university e-mail when creating an edu-ID account?
- When would be a good time to introduce this new default?
  - Our proposal is e.g. October/November after semester start
  - Universities that want this feature can enable it any time already now

Switch

Open session: Q&A, ideas, etc.

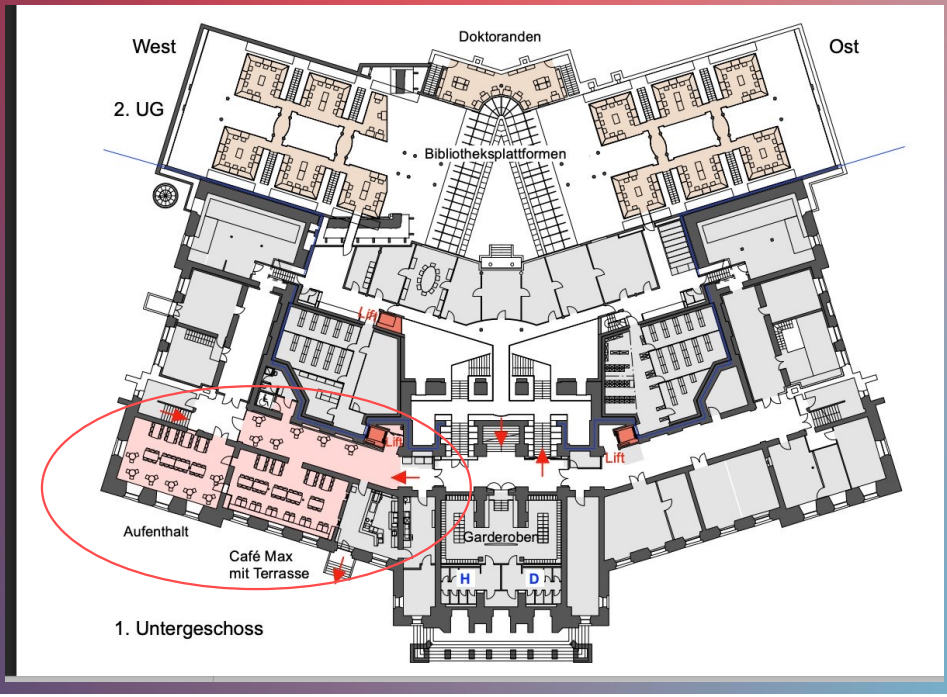
Switch edu-ID Team

Switch

Next

Farewell Coffee & Networking
3:00 – 4:00 PM

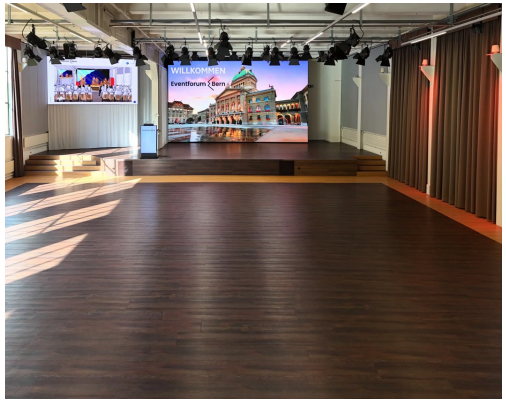
East corridor area, ground floor



Next Switch Events

23 June 2026

EVENTFORUM BERN



Cloud Forward

22 October 2026

Zentrum Paul Klee Bern

Human Centred Security Day

24 November 2026

verkehrshaus

Forum Day November

Switch

Feedback

Switch

Thank You


Switch_