

Switch_

Switch edu-ID Working Group

Forum Days V

Version 1.0, 19.11.2025

Switch_ edu-ID

Welcome to the Switch Forum Days 2025



Ignite



Innovate



Inspire!

Meet the edu-ID Team



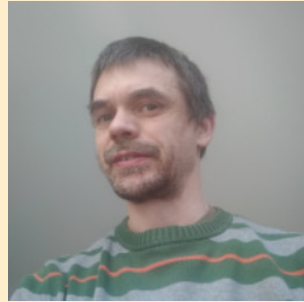
Christoph Graf



Esther Seidl-Nussbaumer



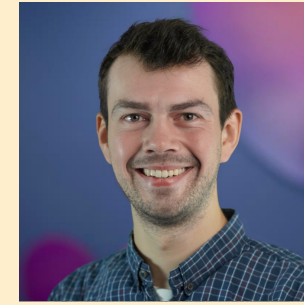
Aris Fkiaras



Daniel Lutz



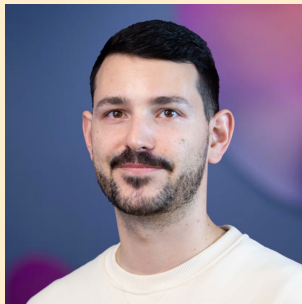
Filippo Costa



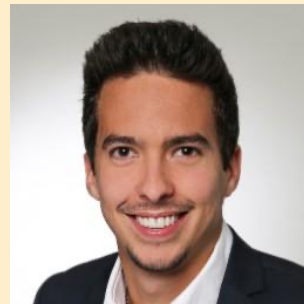
Frédéric Gerber



Lukas Hämmerle



Marco Boss



Sascha Hoppler



Rolf Brugger



Zoltán Umlauf

Agenda

- | | |
|--|-----|
| 1. Rethinking edu-ID Roadmap | 20' |
| 2. OpenID Connect Support | 20' |
| 3. Group Management Requirements | 15' |
| 4. Service Stability | 20' |
| 5. Student Validation Services via eduGAIN | 10' |



Rethinking edu-ID Roadmap

Christoph Graf

19.11.2025

Re-thinking edu-ID: The WHY



Change of identity environment

- E-ID (CH) and eID (EU)
- Prevalence of Entra-ID
- The “EU agenda”

Changing needs of beneficiaries

- Increasing relevance of regulation (e.g. data protection and security)
- Increasing complexity of IT
- Growing number of students & employees
- Decreasing funding in education and research

And the elephant in the room:

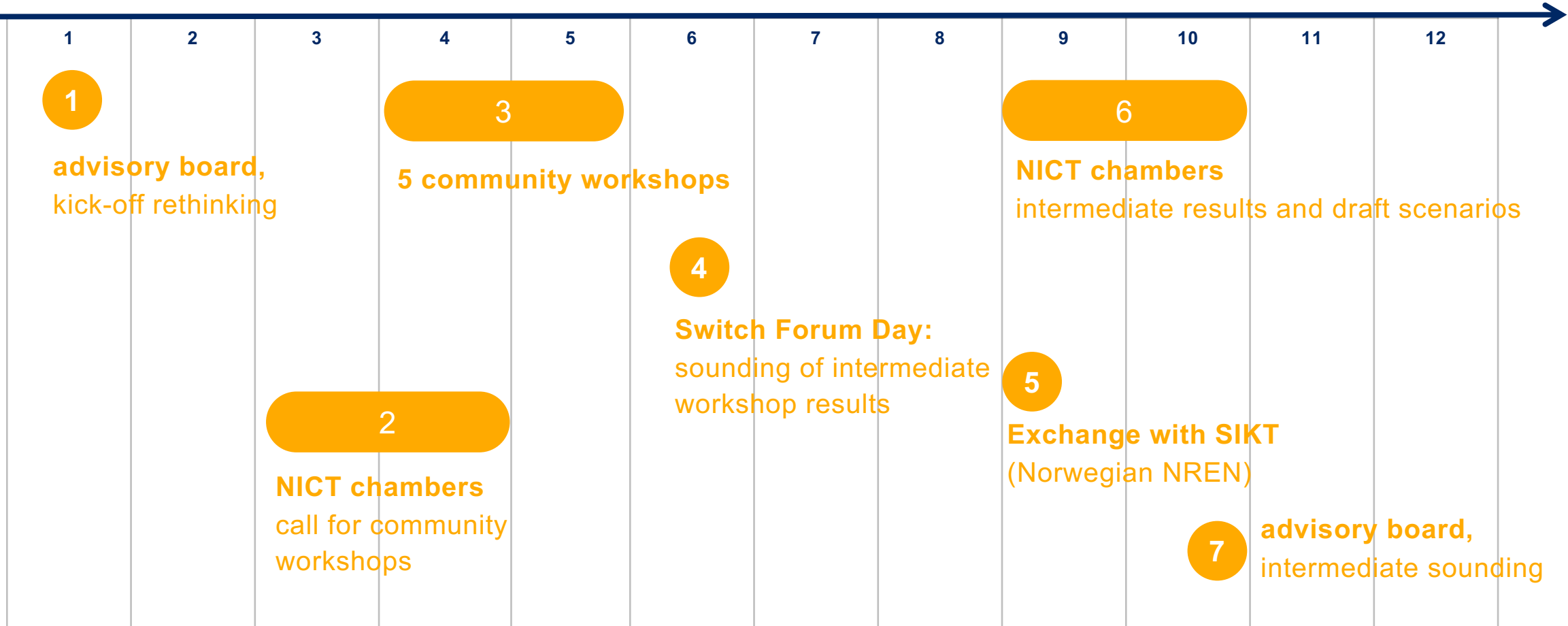
- Digital sovereignty

Common understanding:

- Getting identities done right is a precondition for success

Re-thinking edu-ID: Steps taken so far

2025



Summary of Discovery – Overview

Use Cases

- **University teaching** – main use case, clear value.
- **Lifelong learning** – potential underused.
- **Administration services** – low uptake, MS EntraID dominant.
- **European cooperation** – recognised value, limited maturity.

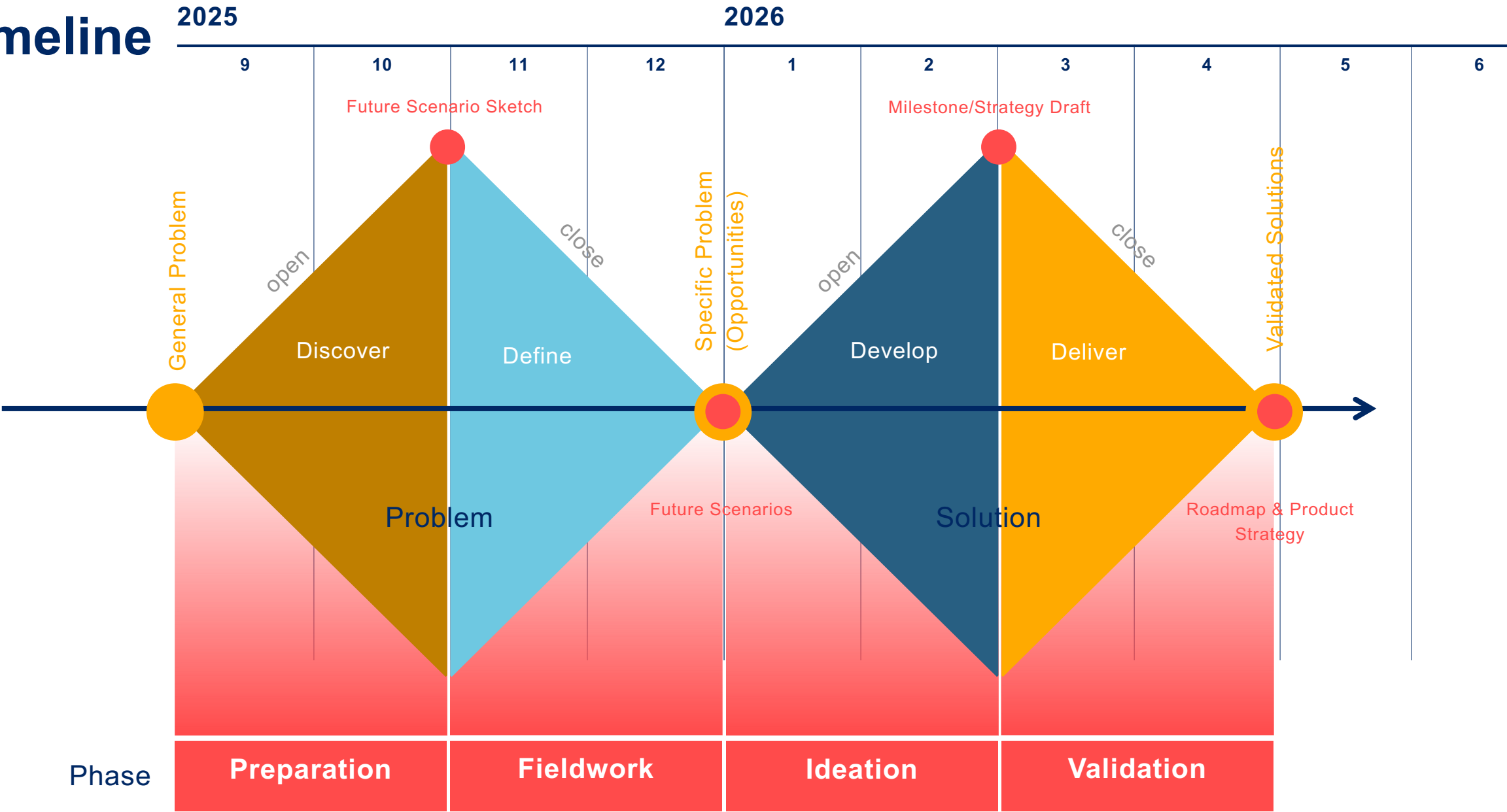
Pain Points

- **Double credentials** – parallel edu-ID & EntraID cause support issues.
- **Security policies** – fewer options vs. EntraID.
- **Protocol shift** – stable SAML, OIDC support lacking.

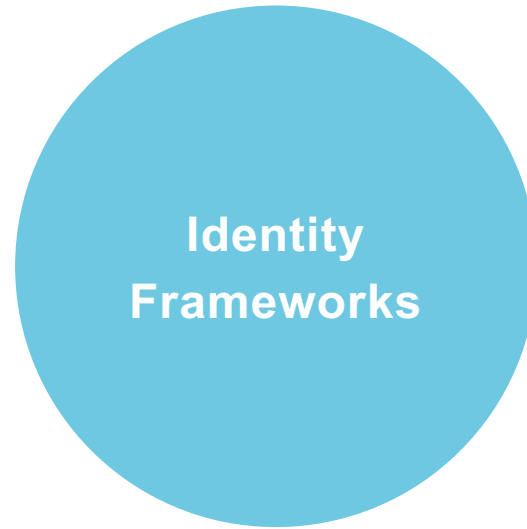
Proven Features

- **University cooperation** – inter-university services valuable, esp. teaching.
- **Lifelong learning** – enrolment & continuing education supported.
- **Identity** – edu-ID useful for roles across universities.
- **Digital sovereignty** – control over identity must stay with universities.

Timeline

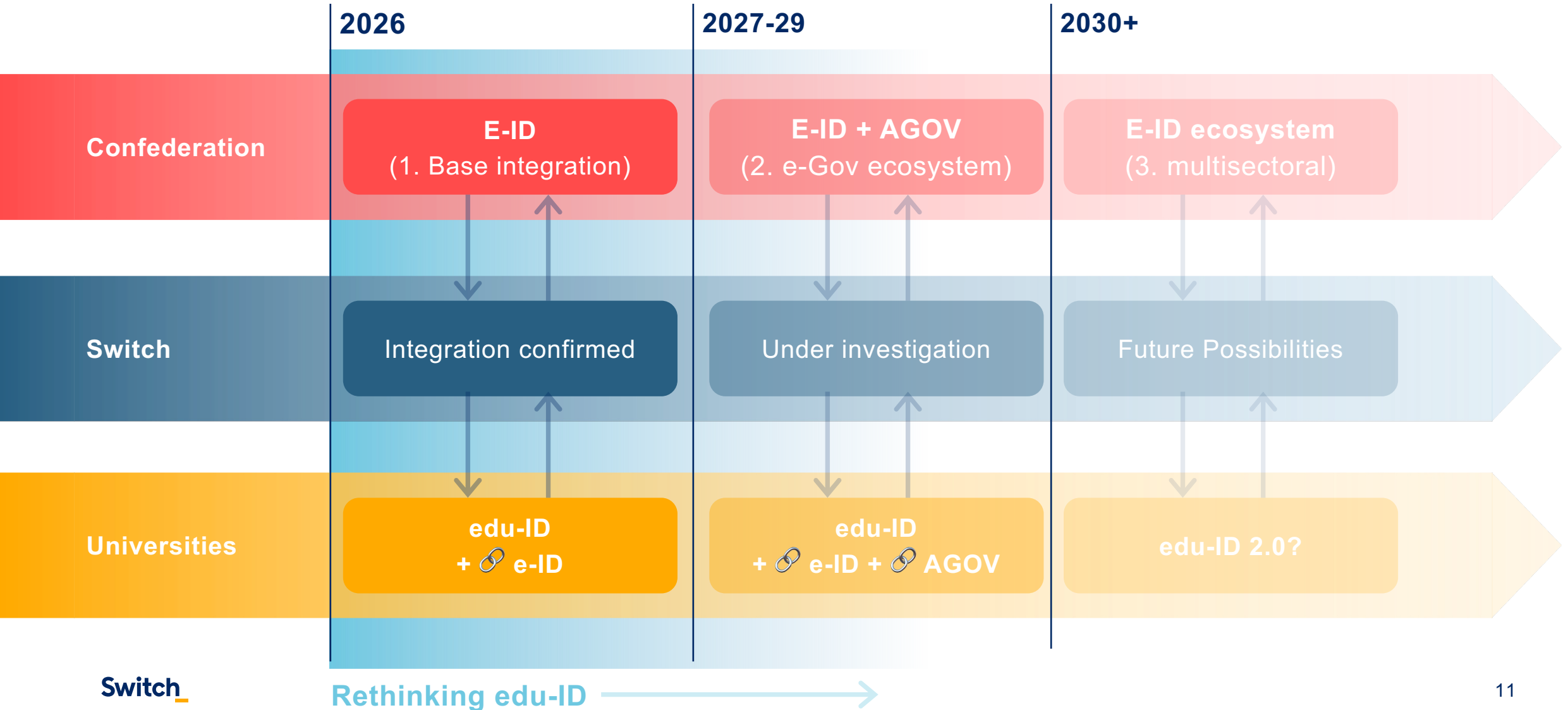


Main influences for Edu-ID



- E-ID Example
- Integration of all relevant identity frameworks (CH/EU/GÉANT)

The e-ID and edu-ID Relationship



Main influences for edu-ID



Strategic Digital Sovereignty

- High tensions (geopolitical, platform dependencies)
- Unclear due to lack of requirements
- Backup scenario with missing weighting

Identity Frameworks

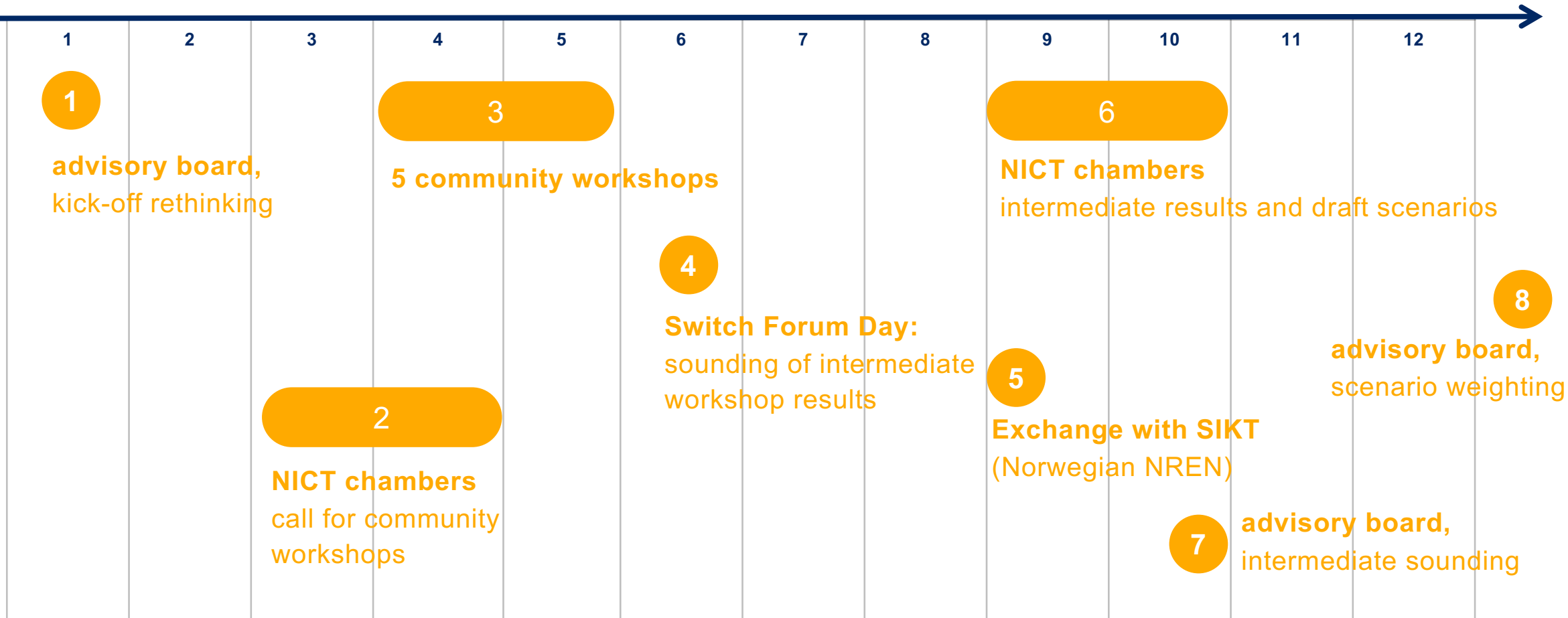
- E-ID Example
- Integration of all relevant identity frameworks (CH/EU/GÉANT)

Industry Standard

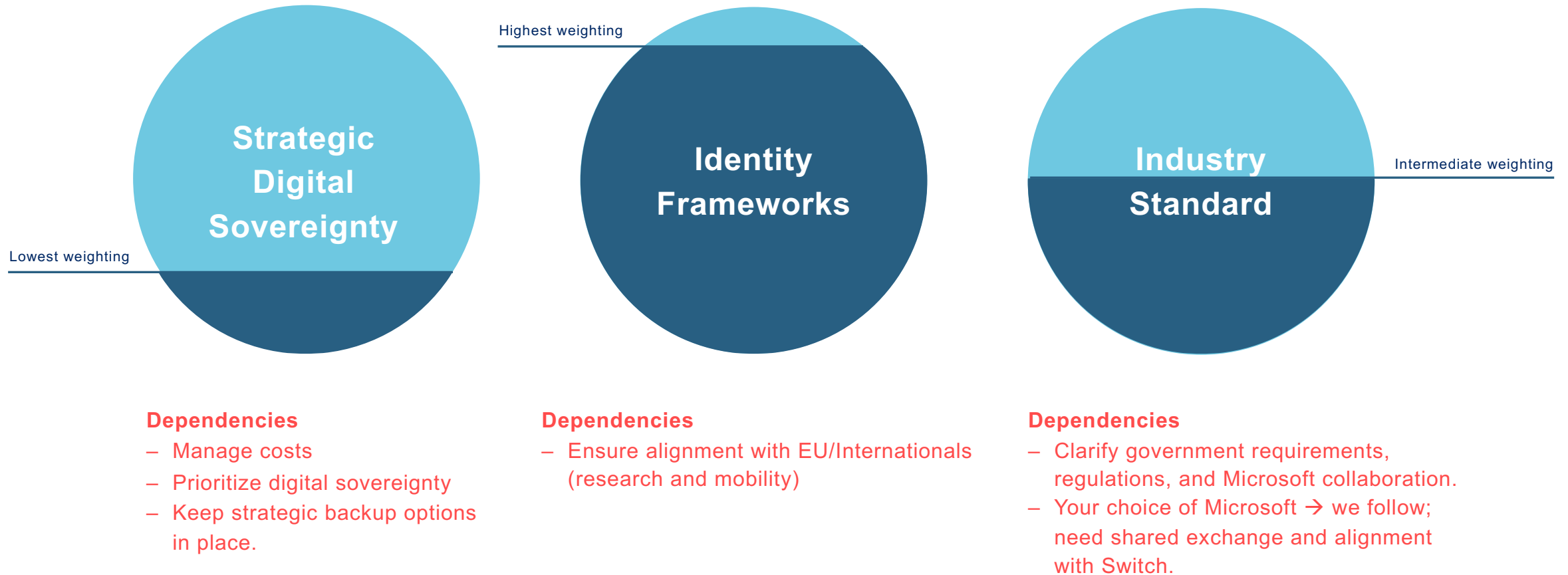
- MS-Standards adoption (dominance)
- Follow our customer
- Future Interplay Edu-ID + MS (e.g. Entra)

Re-thinking edu-ID: Steps taken so far & upcoming

2025



Weighting / Dependencies

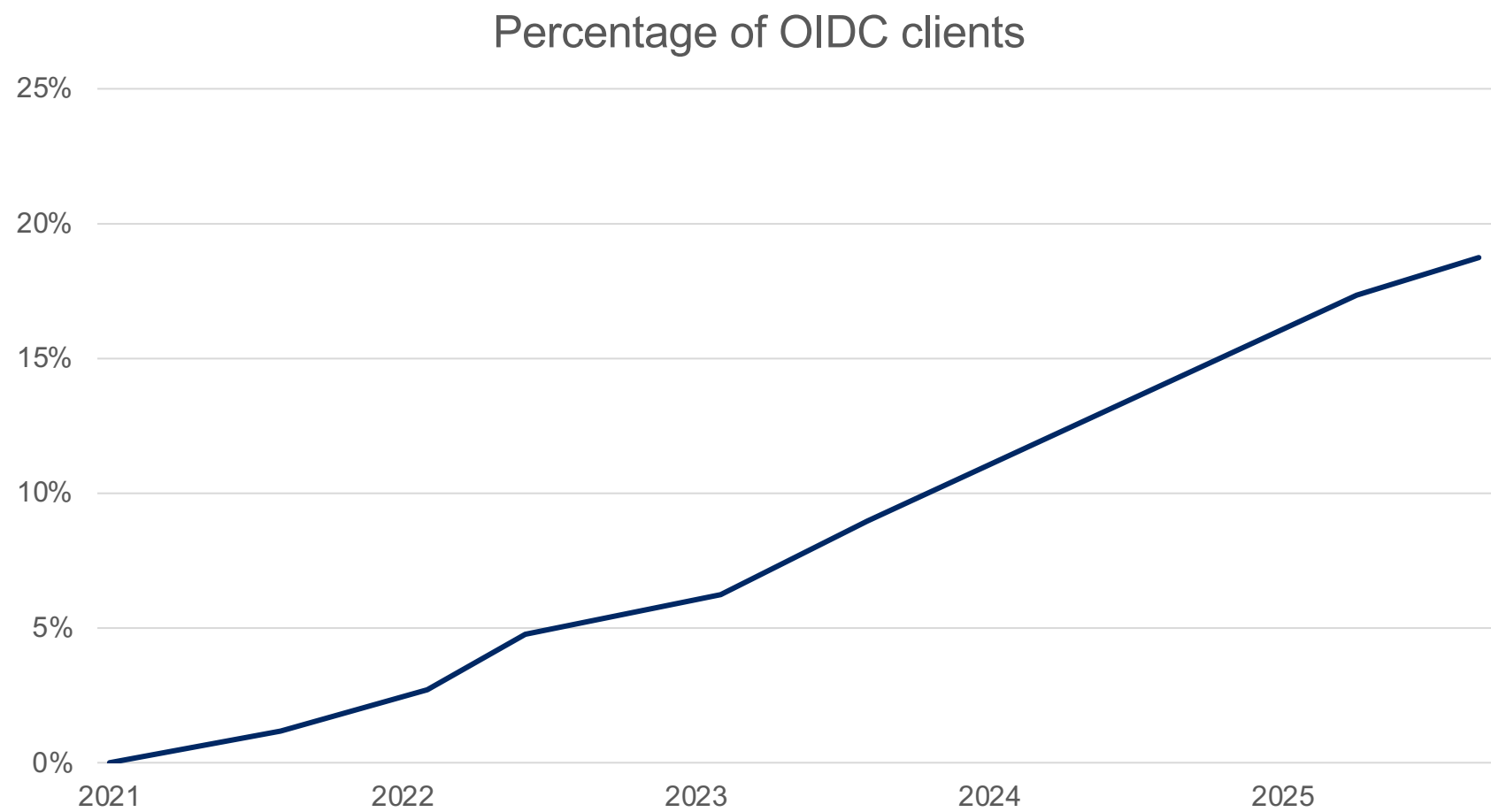


Update on OIDC support in edu-ID

Sascha Hoppler, Daniel Lutz

19.11.2025

OIDC clients in the edu-ID federation



SAML vs OIDC

	SAML	OIDC	
Classic Attribute Model Service gets data of organisational identity	✓	✗	→ Roadmap
Extended Attribute Model Service gets data provided by user, plus some info about potentially all their affiliations	✓	✓	
Interfederation (eduGAIN) International interoperability of Services and IdPs in eduGAIN	✓	✗	→ OpenID Fed
More complex use cases Like OAuth 2.0 with different resource servers	✗	✓	
Friendly for mobile- and single-page applications	✗	✓	
Future-oriented, still worked on	✗	✓	

Improvements

Available from October/November 2025

- Enforce **Refresh Token Rotation**
- Make **Refresh Token Lifetimes** configurable *
- **Logout** support for OIDC
- Make set of **claims in ID Token** configurable
- Support for **login_hint**
- Same **set of attributes/claims** in SAML and OIDC (Extended Attribute Model)
- Proper support for **resource servers** (backends / APIs) *
- Improved **documentation** *

* To be finished

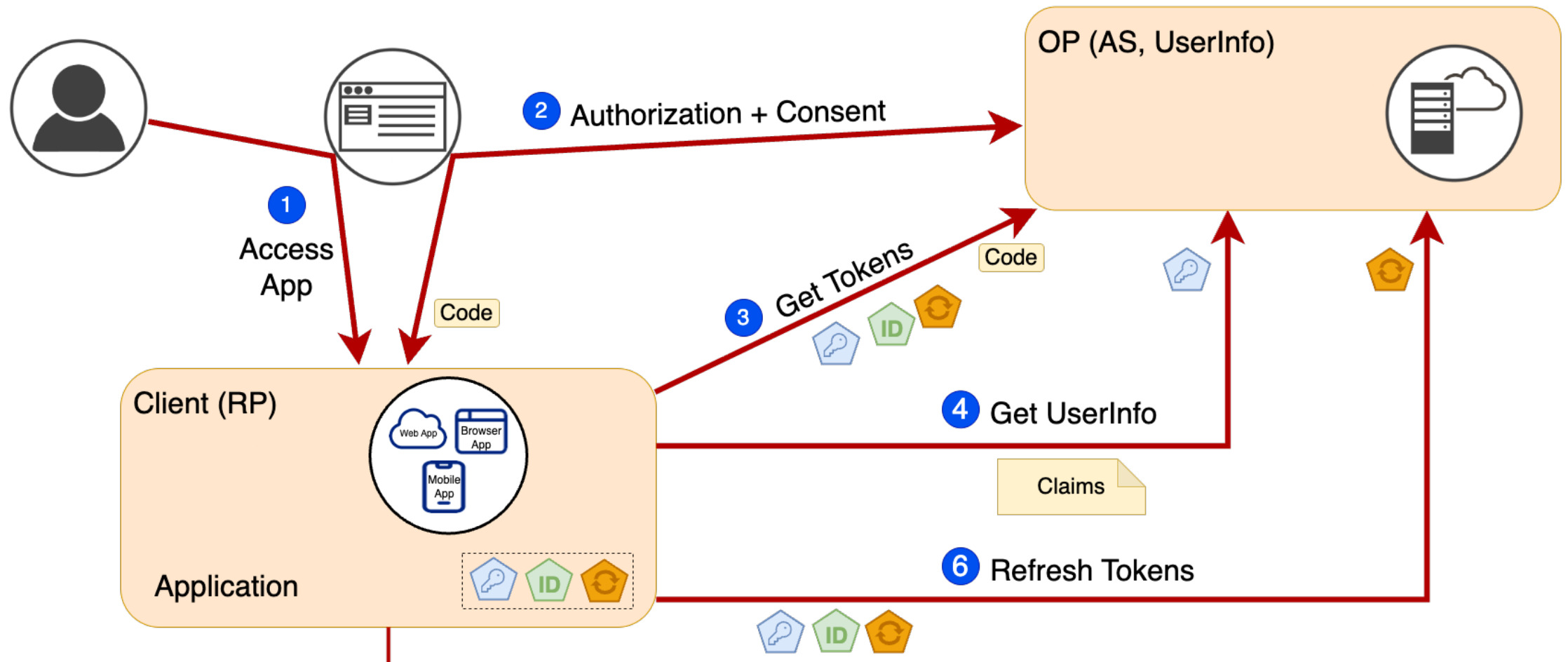
Release planned for Q2 2026

- Classic Attribute Model for OIDC

What the further future holds...

- Interfederation (OpenID Federation)
- Evaluation of more use cases of OIDC and OAuth 2.0

Basic OIDC Flow



Client types

Web Applications

Confidential web clients

- Page rendering on webserver
- Can securely store secrets
- Can use OIDC client authentication

Confidential

Public web clients (Single-page applications)

- Page rendering in webserver
- Can **NOT** securely store secrets
- **Must use PKCE**
- Might access a resource server

Public

Native Applications

Mobile and Desktop Apps

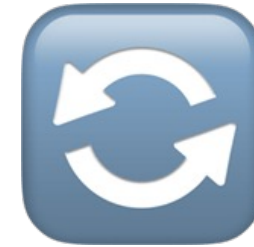
- Might use OS-storage to store data
- **Must use PKCE**
- Should have long-living user session

Public

Making OIDC more secure

Enforce Refresh Token rotation

- If **offline_access** is configured, clients can obtain **refresh tokens**
- With a refresh token, the client can obtain a **new access token, ID token and refresh token**
- Now, when using a refresh token twice, the whole **chain of tokens is invalidated**
→ Protection **against malicious usage** of refresh tokens



Making OIDC more secure

Make refresh token lifetimes configurable (To be finished)

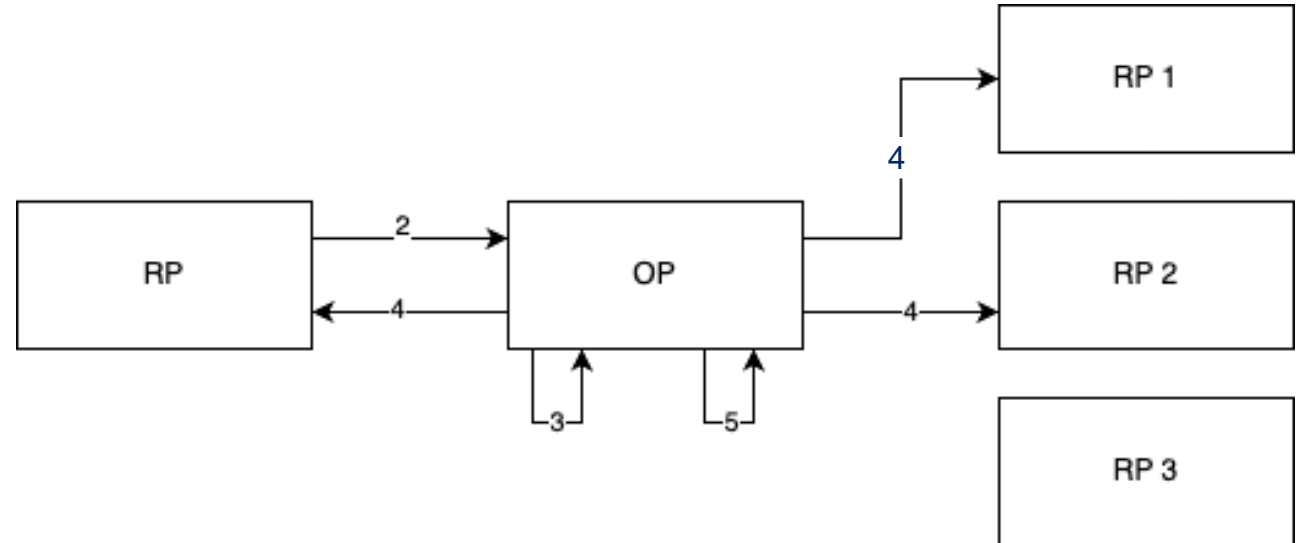
- Different types of clients have a **different usages** of refresh tokens
 - Native apps: Long-running user session. You don't want to authenticate every time you open an app
 - Confidential clients: refresh token can be used to refresh information about user or if the session is based on a token
 - SPA: It is rather insecure to have refresh token, especially long-living ones.
- We therefore make the **token lifetimes configurable**
 - Lifetime of a single refresh token
 - Lifetime of the whole chain of refresh tokens
- Provide **best practices** for clients.



OIDC Logout

Support RP-initiated logout

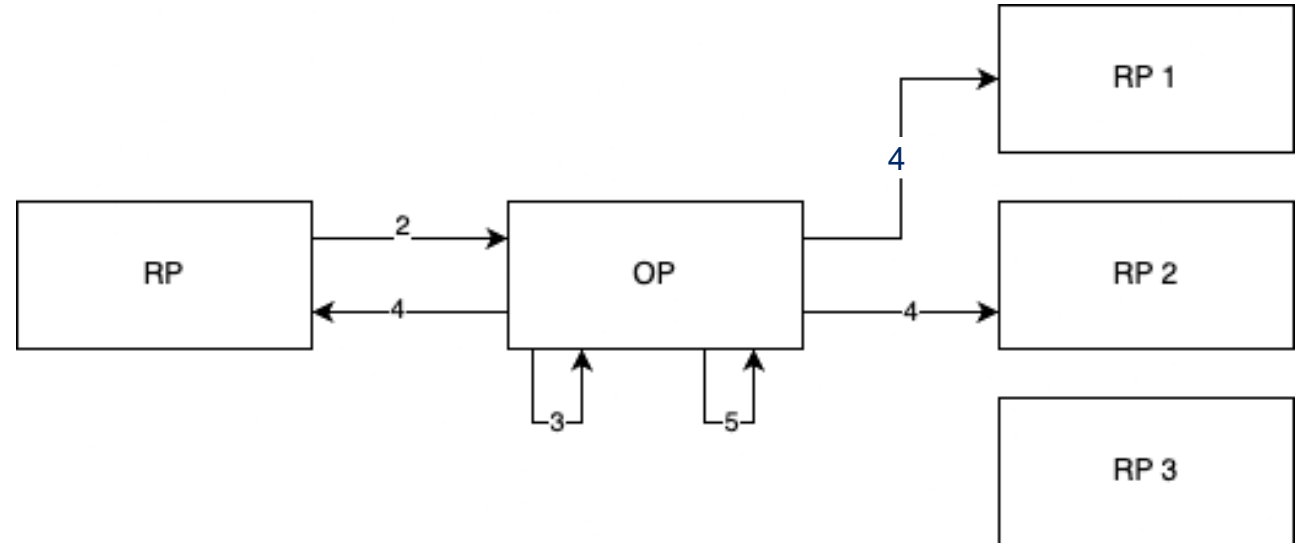
1. User initiates logout in application
2. Client sends user to the end-session endpoint of the OP (edu-ID IdP)
3. OP ends the session of the user in the browser and asks user whether to log out from other services accessed in this browser (OIDC and SAML)
4. (optional) Logout is propagated to all accessed services supporting logout propagation
5. User is shown the logout result (whether logged out everywhere). She is NOT redirected to the client, flow ends on the OP



OIDC Logout

Support OIDC Logout propagation

- Clients can register endpoints for that propagation
- Propagation can be made via front-channel or back-channel
- Client is expected to completely remove the session of the user



Release of claims

Support full set of attributes

Not all attributes that are supported in the extended attribute model for SAML have been implemented for OIDC.

Now, all these attributes can be obtained as OIDC claims.

Note that this does not cover the classic attribute model.

Claims in ID Token

User-related claims should be obtained via the userInfo endpoint.

However, some client implementations rely on the set of claims in the ID Token

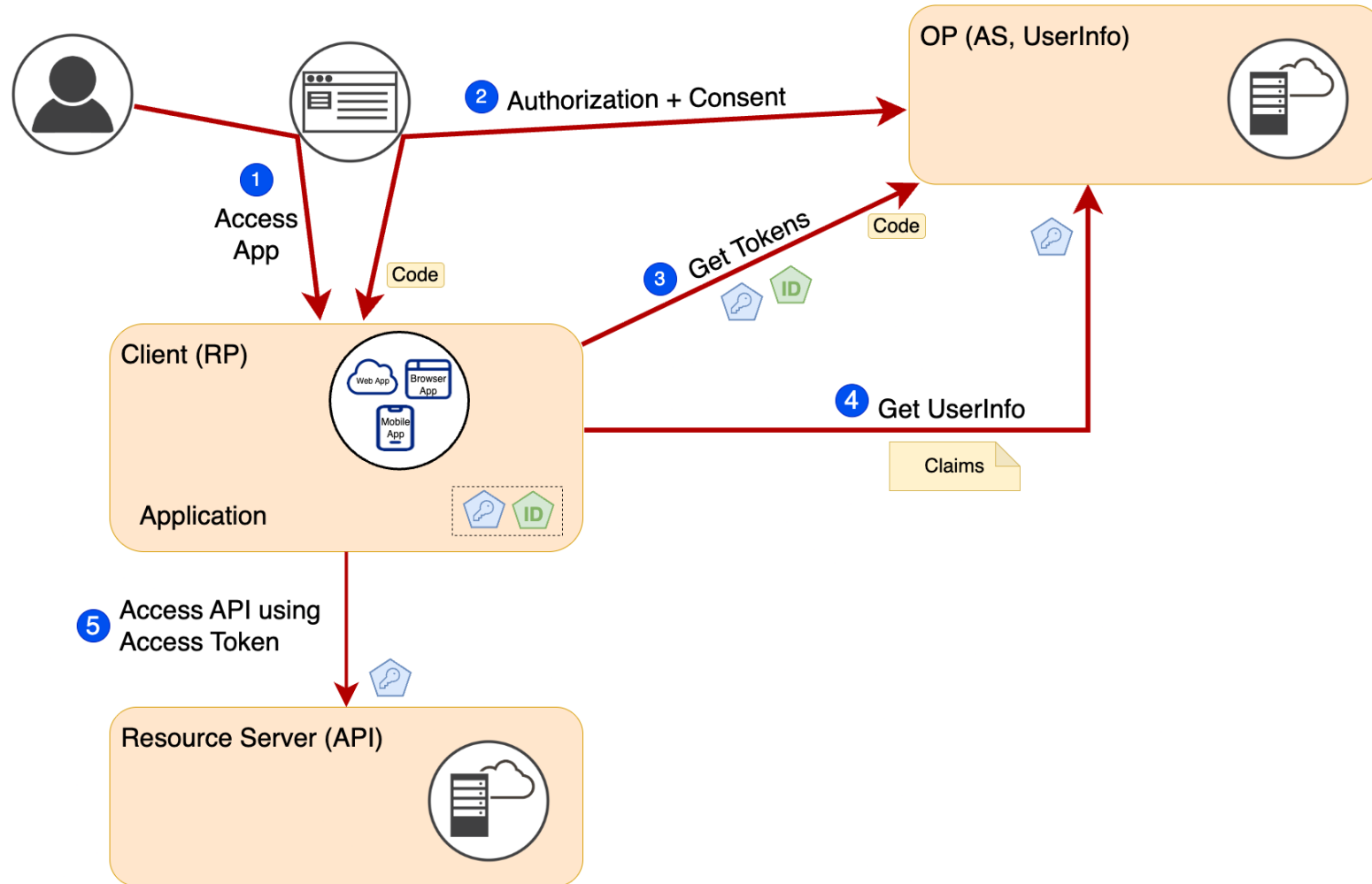
→ The resource registry now supports that claims can be selectively added to the ID Token if required.

Support for the login hint

- If a client knows the username of the user to be authenticated, it can be passed in the authorization request.
- The hint is then pre-filled in the form as username.
- The username form is not submitted automatically, the user can still change the username



Supporting Resource Servers (currently on request)



Enhance Documentation and Guidance



Entrypoint: <https://help.switch.ch/eduid/docs/services/openid-connect/>

What is to come?

Interfederation (OID Federation)

- Keep informed about the eduGAIN OID Fed PoC
- Join the PoC?

Classic attribute model for OIDC

- Start with conceptual phase Q4 2025
- Start implementation Q1 2026

Evaluate more use cases of OIDC and OAuth 2.0

- Self-service registration of resource servers
- Pushed authorization
- ...

What else are you missing?

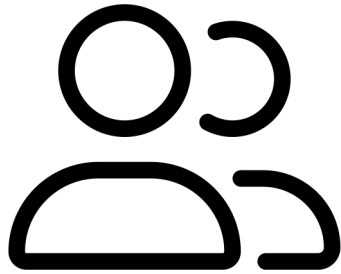


Group Management Requirements

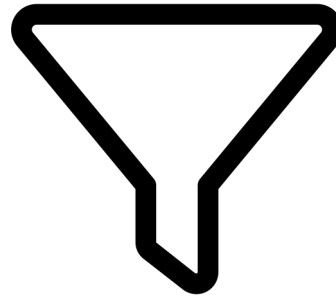
Rolf Brugger

19.11.2025

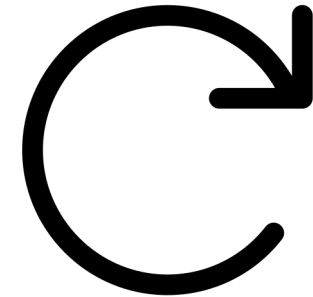
Group Management



Users / Identities



Access rules



Web Service
Application

- Flexibility to build groups
- Import group information
- Flexibility to define access rules

Motivation: Why now?

VHO

- Account for non affiliated persons (now done in edu-ID)
- Limit access to group members
- **end of life**



Shared attributes API

- Manage entitlement attribute via API
- Limited functionality
- Doesn't scale well
- **end of life**



New access management requirements

- Extended attribute model
- Research platforms



Rethink edu-ID

Use Cases

UniBE further education

- The course teacher receives a list of registered participants
 - Teacher creates a group by uploading the list
 - Members of the group get access to course platform Ilias
- ❖ Group is closed when course ends

DeepL SSO access

- University orders a set of licences
 - License is assigned to a member (by adding them to a group)
 - Member with license gets access to DeepL service
- ❖ Licenses are revoked individually

Digital library content for pupils

- Pupil adds school-email address to edu-ID account
 - Library assigns license based on email-domain in the pupil's account
 - Pupil accesses digital content
- ❖ Yearly renewal of email address

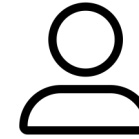
User & Group Lifecycle

Groups



- Flexible creation & management of groups
- Self-service process
- Delegation of group administrator rights
- Provide groups with sub-groups
- Group management API

Members

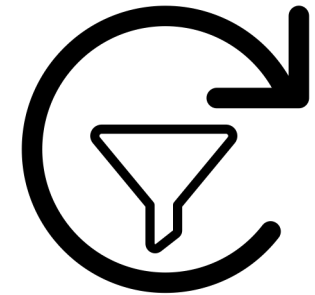
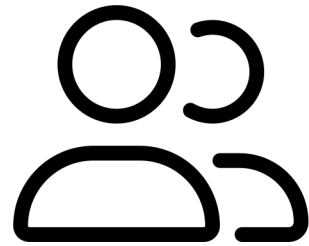


- Variety of registration processes
 - Registration by invitation from group administrator
 - Group can be subscribed to with confirmation by group administrator
 - Mass enrolment by list upload
- Membership management API

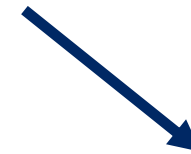
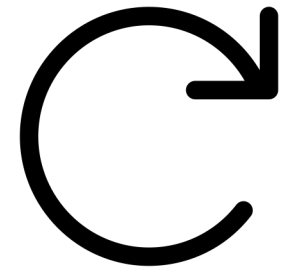
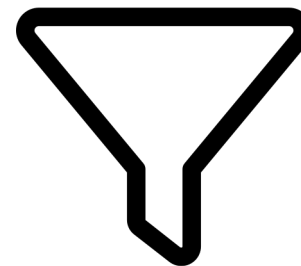
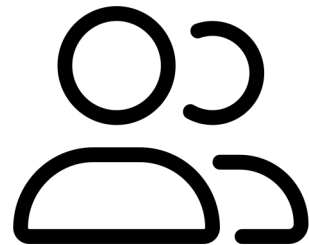
Access Management

Attribute based access management

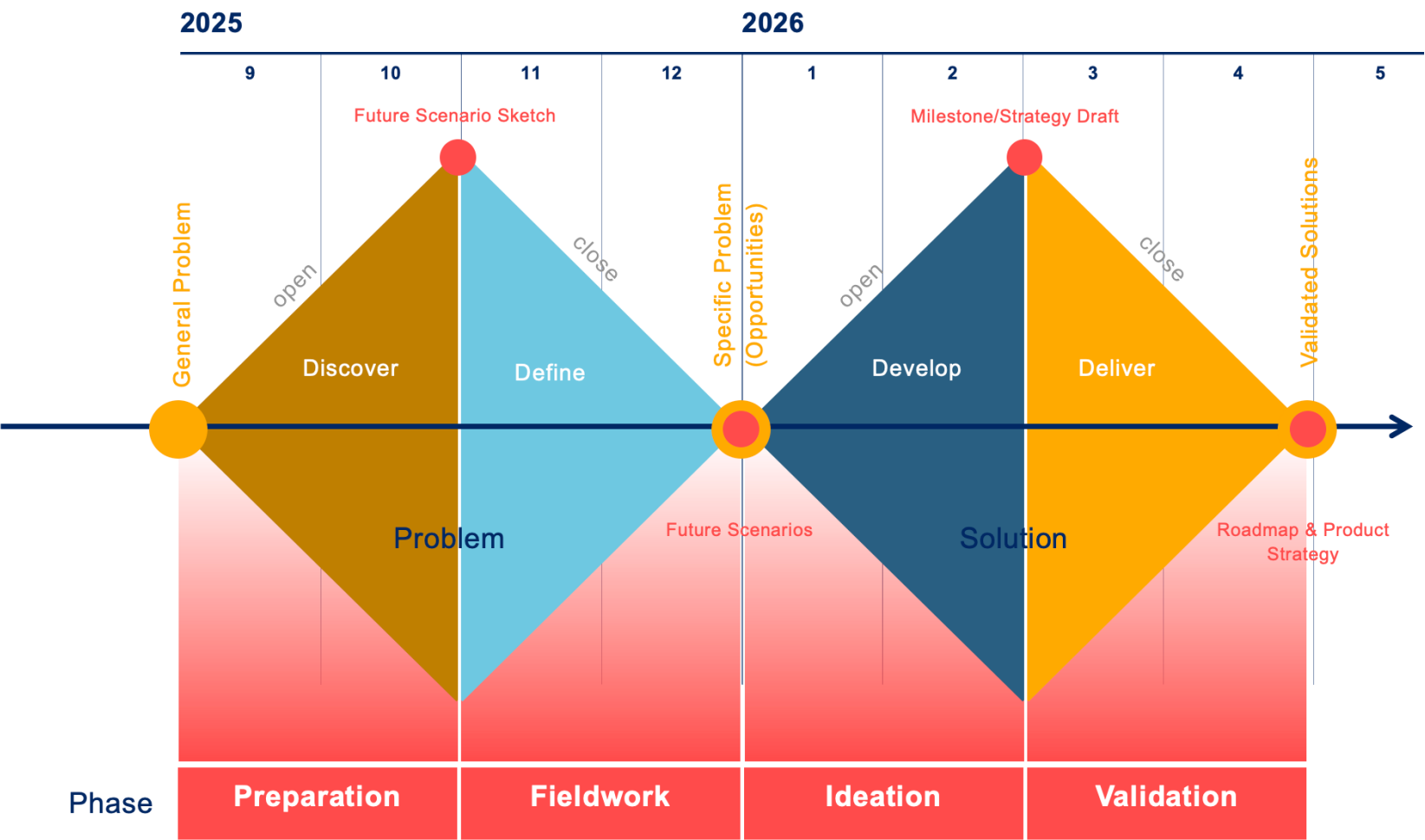
Access rules
built into service



Policy enforce-
ment point



Roadmap



 OpenConext

 CManage™

 Grouper™

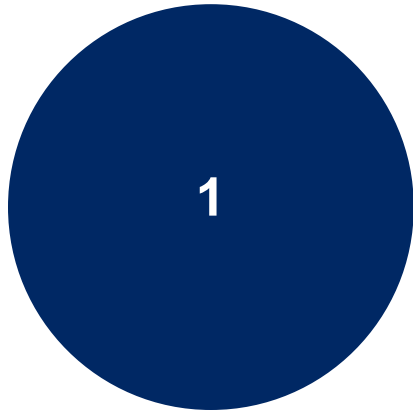
 eosC

Service Stability

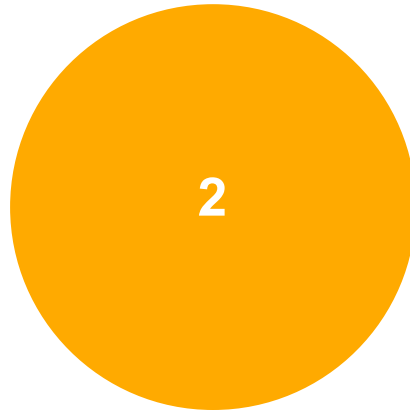
Zoltán Umlauf, Frédéric Gerber, Filippo Costa

19.11.2025

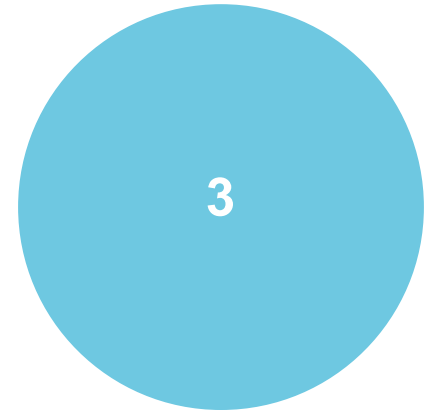
Roadmap



Load Testing



Service Level Agreements



Recent Incidents &
Preventive Measures

Load Testing



Remember dark times...

*“Even though load tests were performed on the internal MFA API **before it was enabled** in Spring 2024 and even though the MFA API has been used for months without problems, this problem remained **hidden** until a massive number of logins by many different users triggered it.”*



16.09.2024 edu-ID Login not working for some users

Date, Time, Duration	16.09.2024, 07:50, 2 hours
Severity	level 2 - service disruption
Incident Summary	On Monday morning at around 8.00, start of fall semester for all Swiss universities, it was noticed the edu-ID login failed or was delayed for some users, while for others it went through smoothly.
Affected users	Because not all users were affected and many users eventually managed to login after a few attempts, it is difficult to estimate the number of users. But about 200 additional support tickets, several phone calls and direct emails were retrieved by the edu-ID team and the Switch front desk. It is estimated that several thousand users were affected.
Root cause analysis	<p>There were several factors that played a role in this issue: The many user logins (about 5x higher than in past weeks) due to semester start and the increased usage of MFA were two of them. However, the actually relevant cause was a missing index on a database table that consumed a lot of CPU in combination with the above.</p> <p>Even though load tests were performed on the internal MFA API before it was enabled in Spring 2024 and even though the MFA API has been used for months without problems, this problem remained hidden until a massive number of logins by many different users triggered it.</p>
Resolution and recovery	The creation of a database index immediately solved the issue.
Preventive measures, future actions and other learnings	<ul style="list-style-type: none">• Improve PostgreSQL SLIs to identify more quickly database congestions• Check for other missing indices in database• Improve SLIs and alerting of other critical components where possible• Speed up notification of users. Prepare messages that can quickly be published on the IdP and the load balancer• The incident was not displayed on https://status.switch.ch/. Add "edu-ID login" to status page in addition to account management.• The internal incident management had to be improvised due to team personnel changes. Improve handover processes. Conduct trainings for successors. Update incident management kit and checklist.

Remember dark times...

“Even though load tests were performed on the internal MFA API before it was enabled in Spring 2024, and even though the MFA API has been used for months without

problems, this problem remained hidden until a massive number of logins by many different users triggered it.

We need more

thorough load tests!

16.09.2024 edu-ID Login not working for some users	
Date, Time, Duration	16.09.2024, 07:50, 2 hours
Severity	level 2 - service disruption
Incident Summary	On Monday morning at around 8:00, start of fall semester for all Swiss universities, it was noticed the edu-ID login was down for some users. For others it went through smoothly.
Affected users	Because not all users were affected, many users eventually managed to login after a few attempts, it is difficult to estimate the number of users. About 200 additional support tickets, several phone calls and direct emails were received by the edu-ID team and the Switch front desk. It is estimated that several thousand users were affected.
Root cause analysis	There were several factors that played a role in this issue: The many user logins (about 5x higher than in past weeks) due to semester start and the increased usage of MFA were two of them. However, the actually relevant cause was a missing index on a database table that consumed a lot of CPU in combination with the above.
Solution and follow-up	Even though load tests were performed on the internal MFA API before it was enabled in Spring 2024 and even though the API had been used for months without problems, this problem remained hidden until a massive number of logins by many different users triggered it.
Resolution and follow-up	The creation of a database index resolved the problem. The issue is resolved.
Preventive measures, future actions and other learnings	<ul style="list-style-type: none">• Improve PostgreSQL SLIs to identify more quickly database congestions• Check for other missing indices in database• Improve SLIs and alerting of other critical components where possible• Speed up notification of users. Prepare messages that can quickly be published on the IdP and the load balancer• The incident was not displayed on https://status.switch.ch/. Add "edu-ID login" to status page in addition to account management.• The internal incident management had to be improvised due to team personnel changes. Improve handover processes. Conduct trainings for successors. Update incident management kit and checklist.

Working in a parallel universe

- We don't want to interfere with legitimate logins
- We don't want to use personal user data
- We don't want to pollute our logs and metrics

PRODUCTION environment

increased resources

personal data

publicly accessible

STAGING environment

replica with analogous resources

fully anonymized realistic data

not publicly accessible

How many logins should we simulate?

5 logins / second?

50 logins / second?

500 logins / second?

5000 logins / second?

Findings

Setting up “another” edu-ID from scratch takes some time

- But it is feasible 😊

Load test results are very sensitive to tiny infrastructure changes

- Port forwarding, load balancing, amount of CPU cores, ...

We were ready for double the amount of logins / second

- September 2024 (1.1M users): 45 logins / second (observed)
- September 2025 (1.3M users): ~55 logins / second (expected) → **load tested ~100 logins / second**

Just to be safe, increased resources for semester start

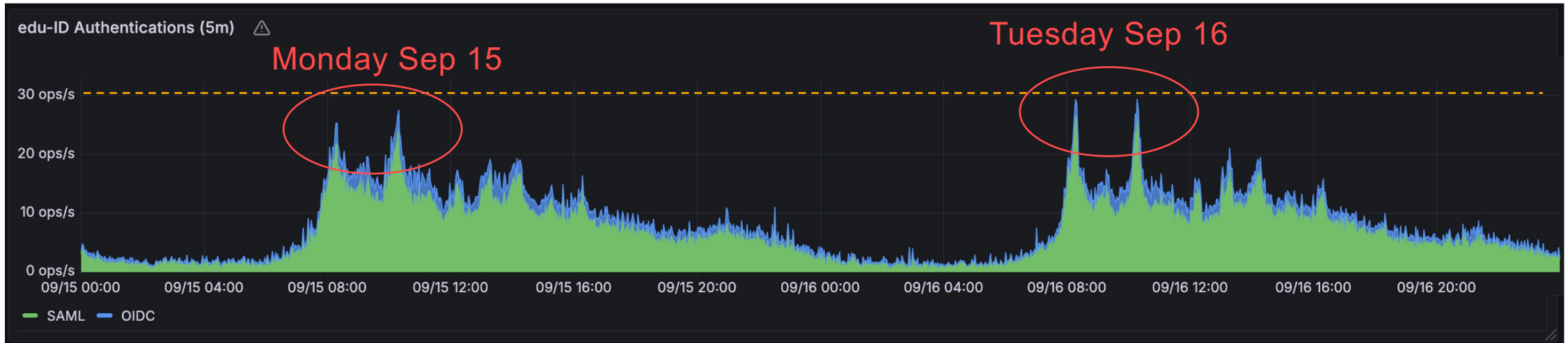
- Added our standby node to the pool of IdPs and ordered two additional nodes just in case

Results: Semester Start 2025




Drum roll...

Results: Semester Start 2025




- This year, we never had more than **30 logins / second** during semester start
- Most of last year's login requests were likely users retrying
- We are ready for >3 times the amount 😊
- In the future, we plan to do load tests a few weeks before each semester start (August and January)


More details



Identity Blog



Load Testing the edu-ID IdP



Daniel Lutz
24/09/2025
Load Testing, Operations, SWITCH
edu-ID

On a Monday morning, at the start of the fall semester 2024, many students were unable to log into their edu-ID account. A nightmare for students, IT administrators – and also the edu-ID team who was working actively to fix the issue as soon as possible.

What was the cause of this incident? A retrospective analysis found that the issue was a missing index in a database table. Really, a missing index? Why did we not detect this earlier, even though this problematic table had been in use for several months without any problem? It turns out, we load tested the new MFA API when launching it, but it seems that it wasn't with a sufficiently large and diverse dataset. Therefore, it was only at semester start that such a high load made the problem apparent.


But the learning is clear:

We need more thorough load tests!

We accepted the challenge and started working on a parallel edu-ID system. In fact:

- We did not want to interfere with legitimate logins;
- We did not want to use personal user data;
- We did not want to pollute our monitoring.

FOLLOW US VIA RSS-FEED

 [RSS - Posts](#)

RECENT POSTS

- [edu-ID September Newsletter](#)
- [The new semester has started](#)
- [Load Testing the edu-ID IdP](#)
- [August Newsletter for edu-ID Operators](#)
- [edu-ID July Newsletter](#)

CATEGORIES

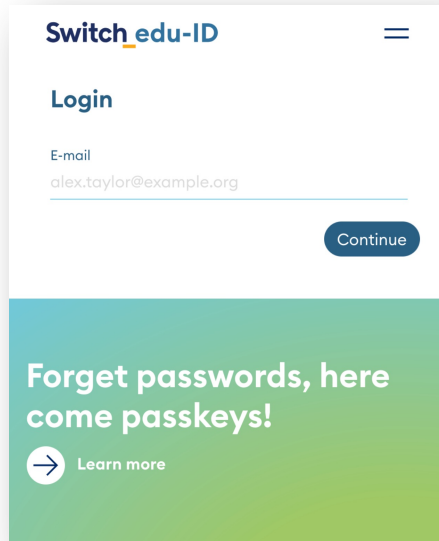
- [Digital Identities](#)
- [E-ID](#)
- [How-Tos](#)

Service Level Agreements



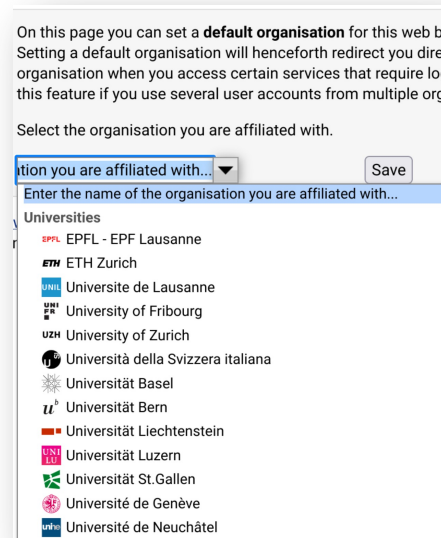
2

Proposals for SLAs



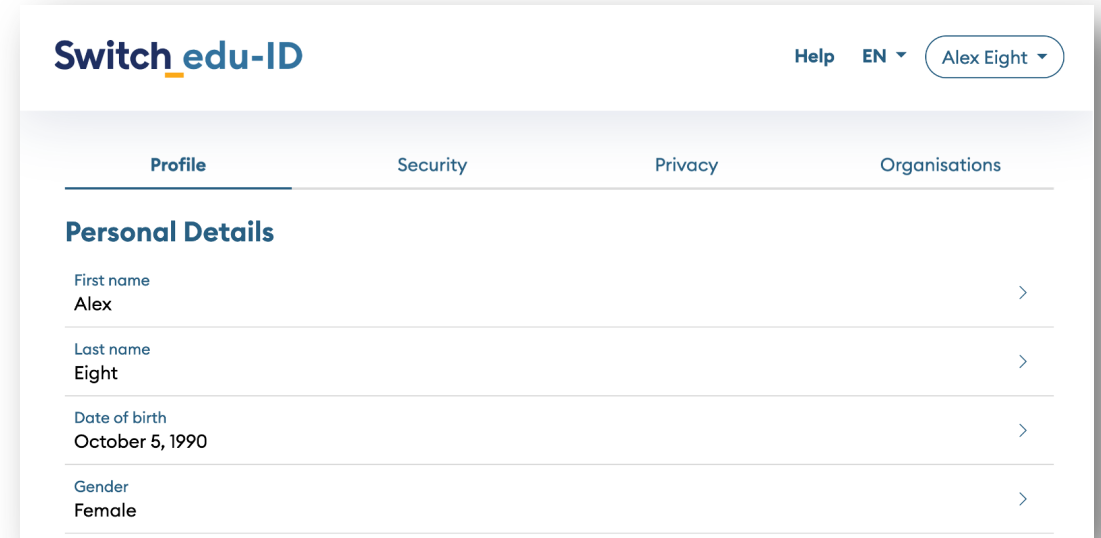
The login screen features the 'Switch edu-ID' logo and a hamburger menu icon. Below the logo is a 'Login' heading. An email input field contains 'alex.taylor@example.org'. A 'Continue' button is positioned to the right of the input field. A green banner at the bottom contains the text 'Forget passwords, here come passkeys!' and a 'Learn more' link with a right-pointing arrow.

Login



The discovery service screen explains how to set a default organisation. It includes a dropdown menu titled 'Select the organisation you are affiliated with.' and a 'Save' button. A list of universities is displayed, including EPFL, ETH Zurich, and various Swiss universities. The list is titled 'Enter the name of the organisation you are affiliated with...'.

Discovery Service



The account management screen shows the 'Switch edu-ID' logo, a 'Help' link, and a user profile 'Alex Eight'. Below the header are tabs for 'Profile', 'Security', 'Privacy', and 'Organisations'. The 'Profile' tab is active, displaying 'Personal Details' with fields for 'First name' (Alex), 'Last name' (Eight), 'Date of birth' (October 5, 1990), and 'Gender' (Female). Each field has a right-pointing arrow indicating it can be edited.

Account Management

Availability:

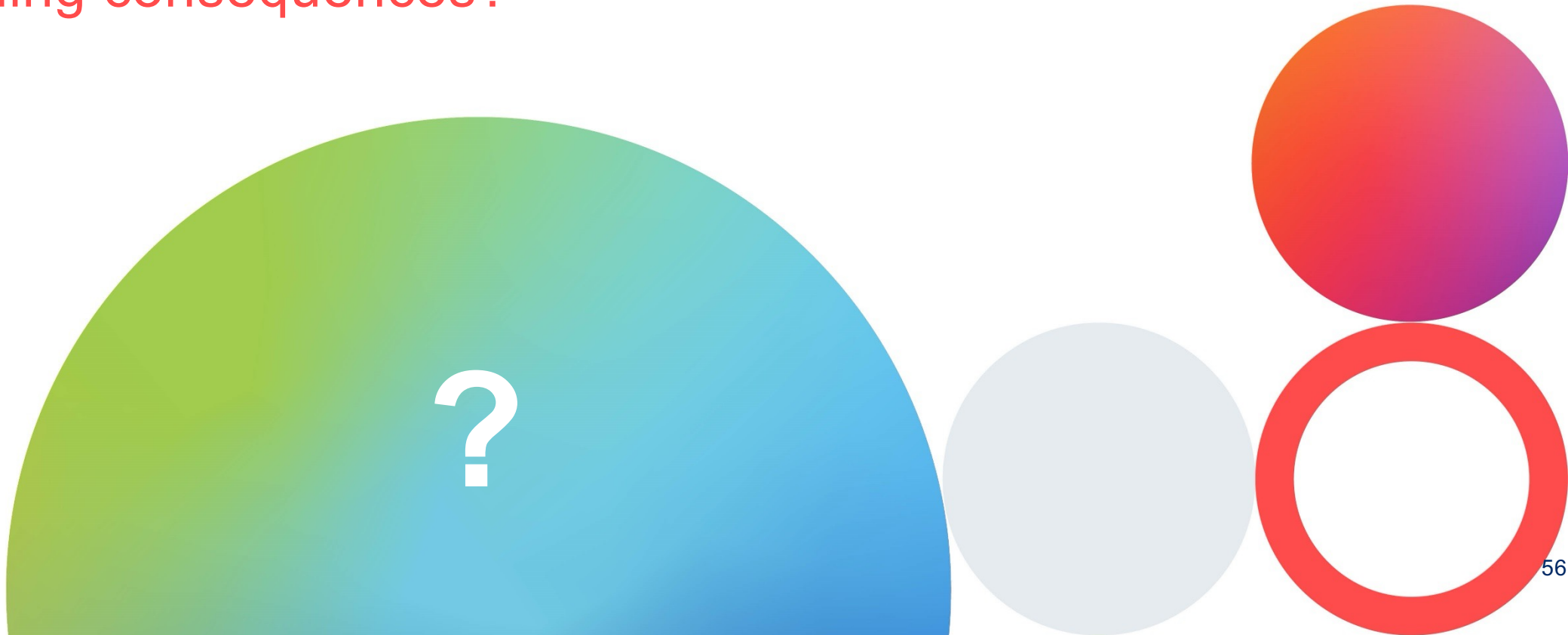
- **Login and Discovery Service:** 99.9% per month
- **Account Management:** 99.5% per month

Latency:

- **Login:** 99% of requests responded to correctly within 2.5s

What is your opinion on these topics?

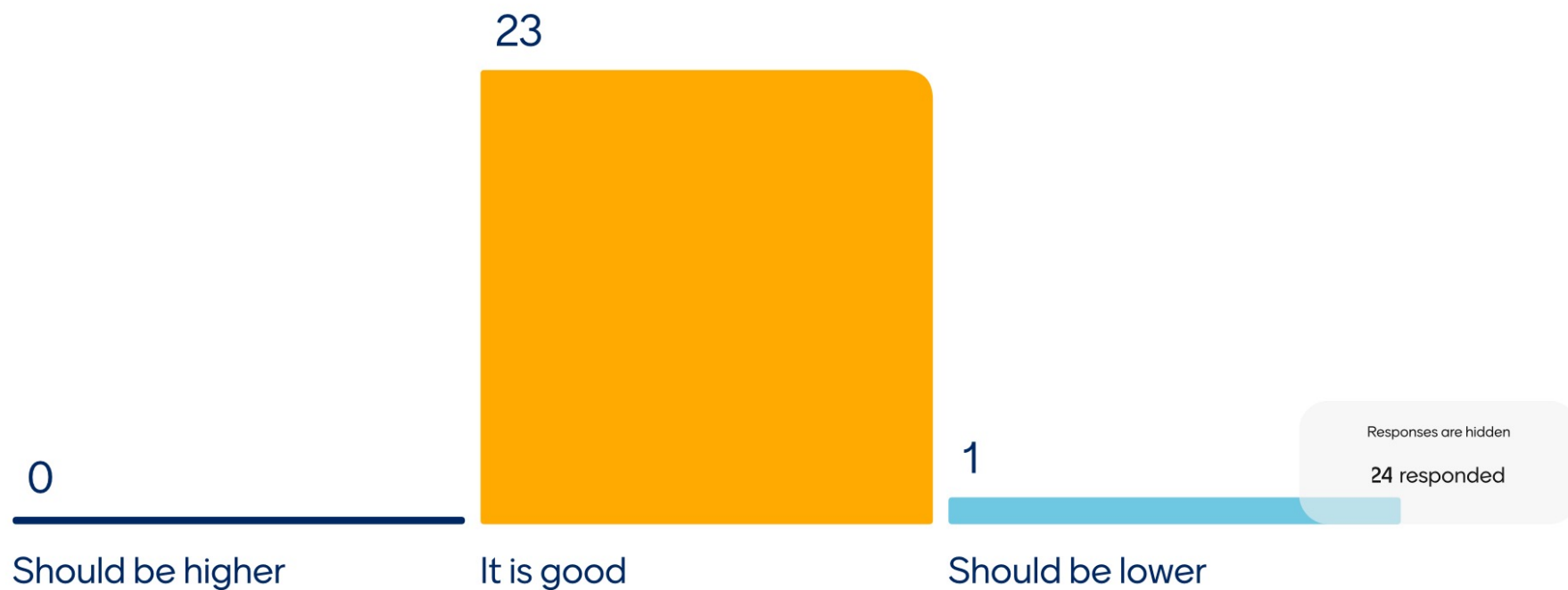
- Availability guarantees?
- Defining consequences?



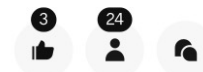
Join at menti.com | use code 3702 8425

Switch

Is 99.9% availability per month satisfactory, when considering costs?

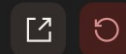


→ Show responses

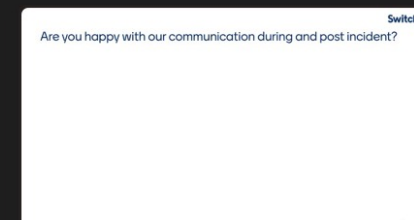
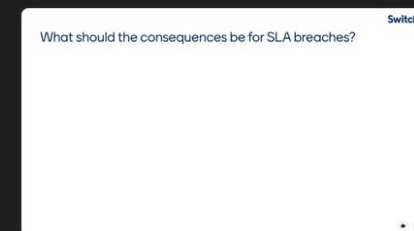
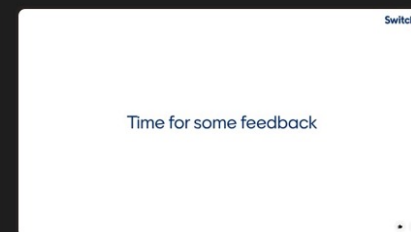


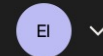
Menti

Forum Days V feedback



Choose a slide to present

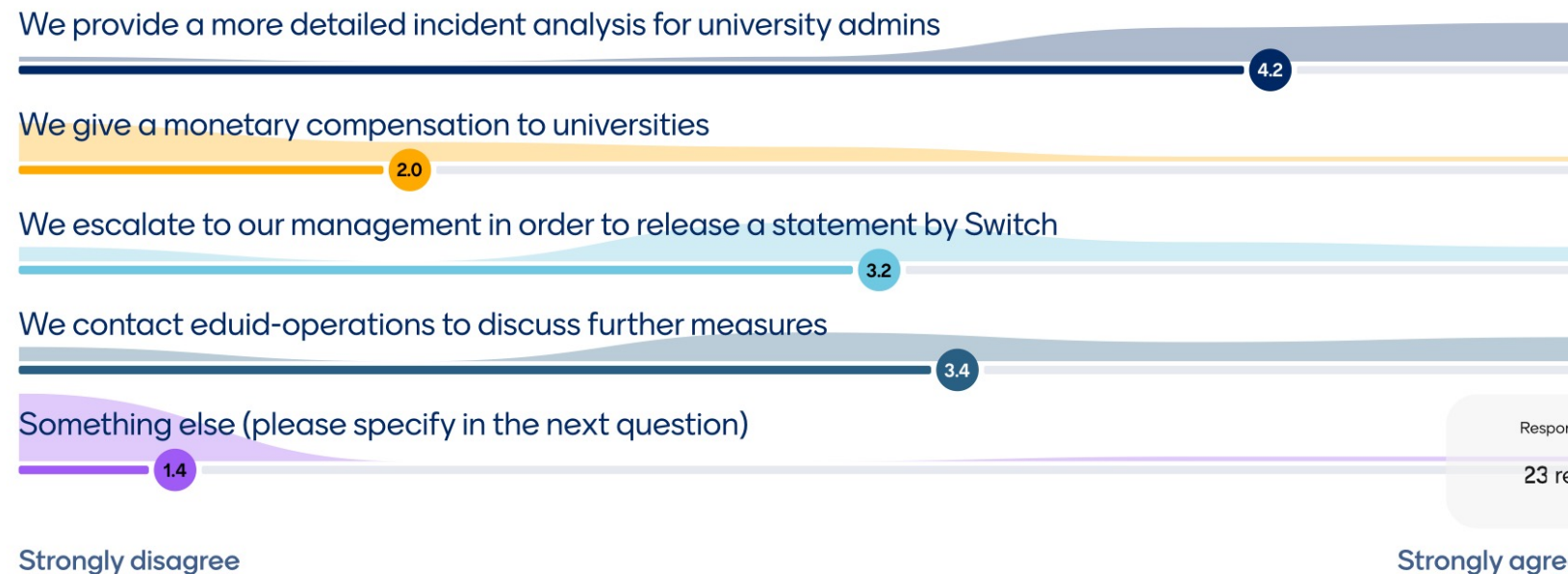




Join at menti.com | use code 3702 8425

Switch

How important are these consequences for you in case of SLA breaches?



Responses are hidden

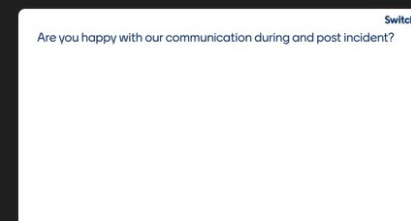
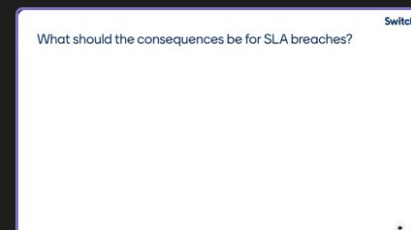
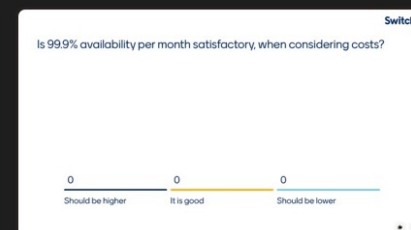
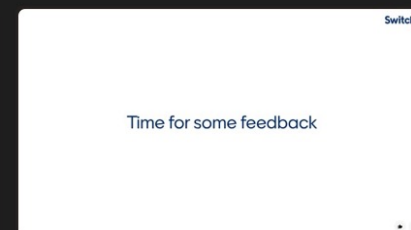
23 responded

Menti

Forum Days V feedback



Choose a slide to present



→ Show responses



Join at menti.com | use code 3702 8425

Switch

Any other feedback? Are you happy with our communication during and post incident?

yes very happy

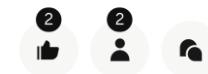
very happy

nice work

Responses are hidden

2 responded

→ Show responses



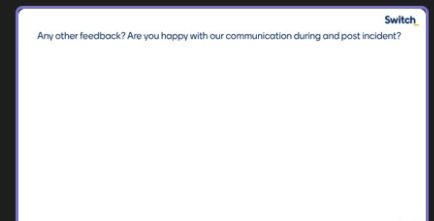
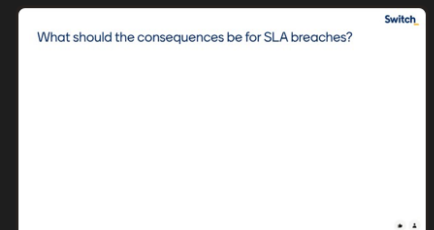
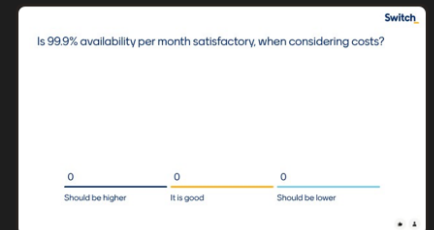
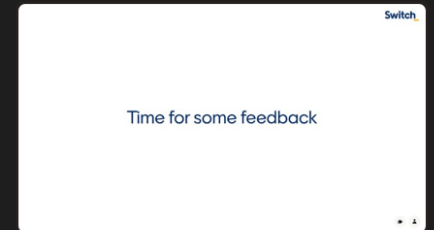
EI

Menti

Forum Days V feedback



Choose a slide to present



Recent Incidents & Preventive Measures



Incident Alerts from status.eduid.ch

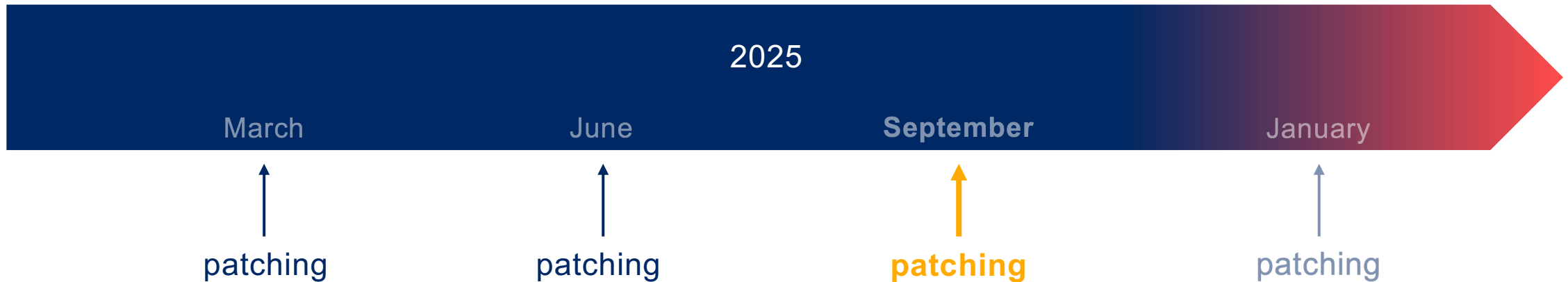
2. Sync between StatusIQ and operations mailing list improved

As part of our efforts to improve communication channels, we have integrated incident communication into the operations mailing list. Concretely, we have subscribed eduid-operations@lists.switch.ch to our service status page status.eduid.ch. If you are currently subscribed to these status updates already separately from this mailing list, you would now get two alerts. Please remove your personal email address from our status page if you do not wish to get a duplicate notification.

Please subscribe again to status.eduid.ch!

We will follow up in the mailing list about the topic

Review VM patching process



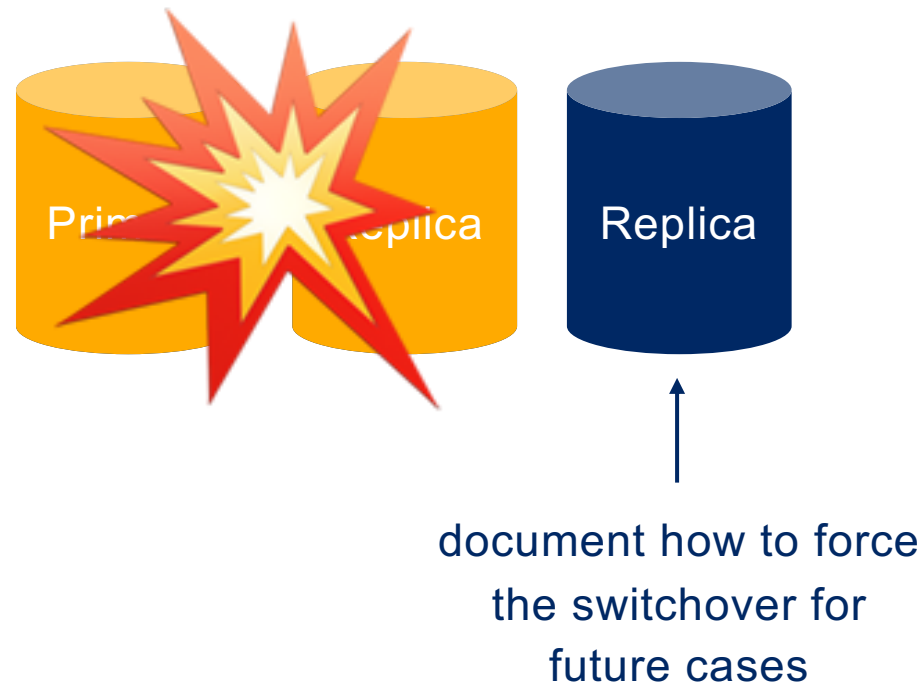
On September 3rd, one load balancer node was not restarted automatically after the patching (outside office hours)

Improvements:

- Improve Anycast host management script
- Monitor restarts in the future
- Ability to manually reboot

Improve database switchover

On October 20th, two DB nodes were down due to a power failure in our Zürich datacenter. The remaining one didn't take over.



Student Validation Services via eduGAIN

Lukas Hämmerle

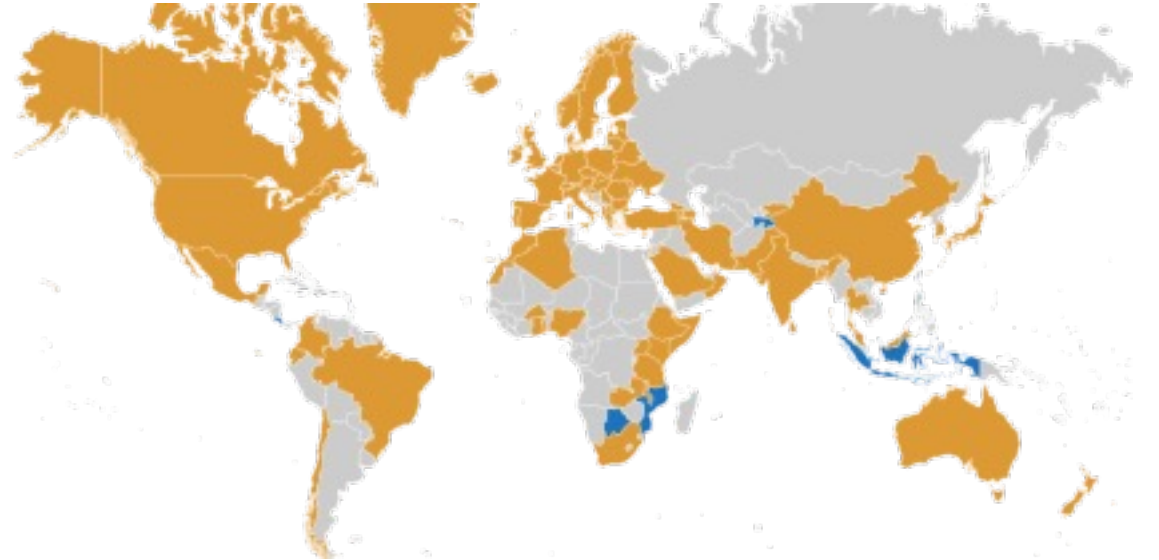
19.11.2025

What awaits you

1. What is eduGAIN again?
2. Student validation services
3. Proposal

eduGAIN ^{EST 2010} – Interfederation Service

- Allows SAML login across federation boundaries
- Governed by member federations
- An IDP or SP typically “opts-in” to eduGAIN
- Federations have slightly different policies



Switch edu-ID Federation Opt-Ins:

- 27 Service Provider in eduGAIN
= users from other federations could access these services
- 62 of 69 Identity Providers to eduGAIN
= IDP loads eduGAIN metadata with more than 3'500 services
= their users could access eduGAIN SPs

83 federations

6'100 IdPs

3'500 SP

Discounts for students Example 1



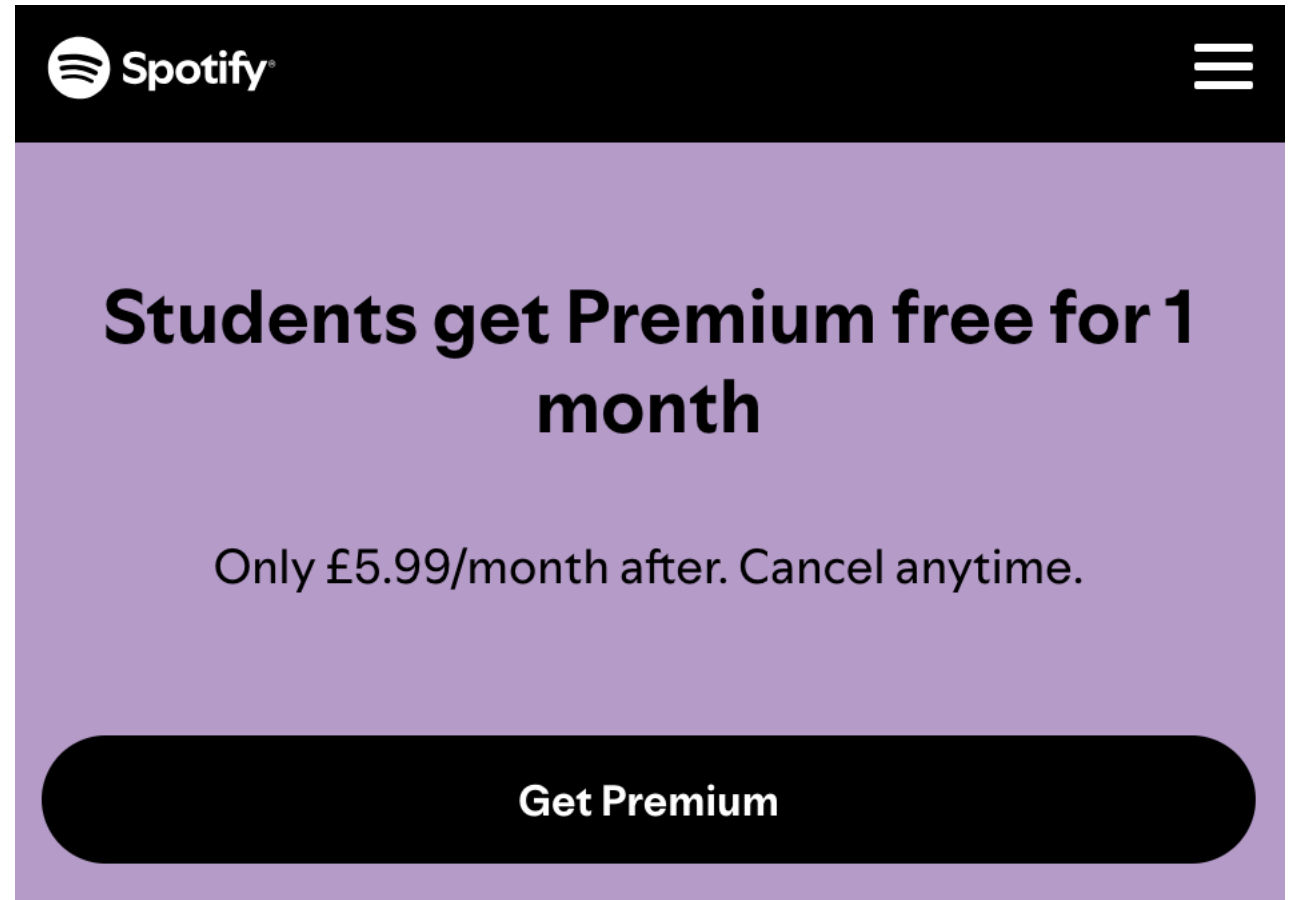
Student Economy: Swiss führt neuen Studententarif ein

Die Swiss bietet ein neues Angebot für Studentinnen und Studenten an. Es umfasst zwei Freigepäckstücke und reduzierte Preise. Doch wie viel günstiger ist das wirklich?

Das Angebot gilt für interkontinentale Hin- und Rückflugtickets. Allerdings sind Flüge von und nach Japan, Kanada und USA davon ausgeschlossen. Studierende müssen sich dafür mit dem Lufthansa-Login Travel-ID und der **SheerID** zum Nachweis der Immatrikulation verifizieren.

Discounts for students Example 2

Students get discounts for some services. But how to know if somebody is a student?



Commercial Student Validation Services

- **Sell the information** if a user is a student
 - They currently can be used via eduGAIN.
- **Students benefit:** They get a discount!
- **Student validation services benefit:** They monetize university data almost for free
- **Universities don't benefit**
 - Probably limited interest in these kind of services
- **Operate outside our federation's policies** because accessible via eduGAIN
 - Some don't care very much about security and data protection
 - Could hardly join Switch edu-ID federation directly because no sponsor
 - Federation Partners like Digitec/Galaxus, Apple, Microsoft, etc. (Federation Partners) are contractually bound to Switch edu-ID federation rules.

Login Numbers seen on edu-ID

April/Mai 2025

September/October 2025

SheerID

10'500

27'000

UNiDAYS

2'300

2'360

StudentBeans

25

70

proXI-ID

680

580

uniperks

0

0

InAcademia Student Validation Service



- Link: <https://inacademia.org/>
- Student Validation Service created by GÉANT project.
 - GÉANT association runs the service (as well as e.g. [eduroam](#))
 - GÉANT is owned by Switch and other European National Research and Education Networks
- InAcademia provides secure and privacy-preserving student validation that is easy to deploy
 - Charges apply per validation.
 - Excess income of InAcademia is used to finance operation of eduGAIN.
 - Can reduce edu-ID team workload: Use InAcademia instead of setting up SAML/OIDC yourself

Proposal

1. Filter out these commercial services from eduGAIN metadata stream

Keep InAcademia and non-commercial service by International Student Identity Card (ISIC)

Inform contacts from these services a few months ahead about change:

- SheerID.com
- MyUnidays.com
- StudentBeans.com
- Proxi.id
- Uniperks.pl

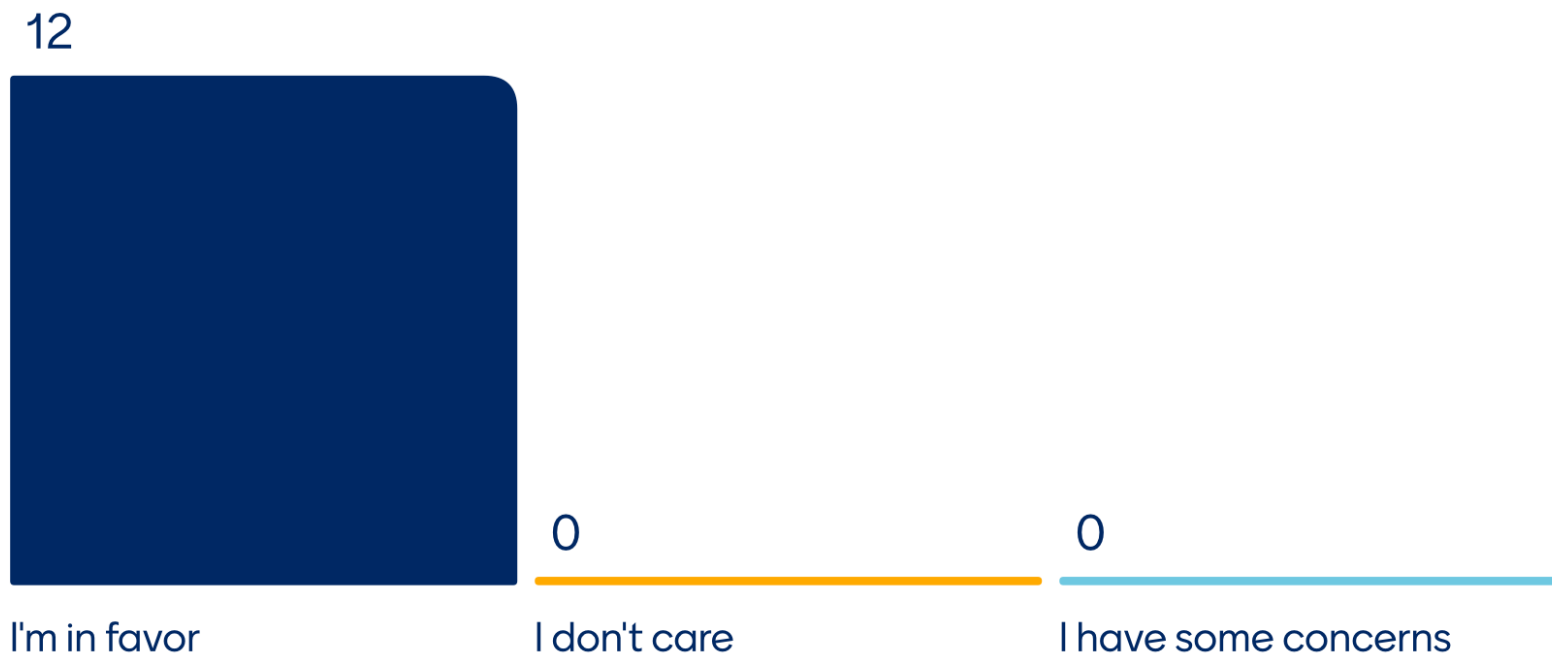
2. Actively recommend InAcademia if a new service only needs student validation

- Safe, privacy-preserving, operated by GÉANT, indirectly benefits our community
- Less support needed from edu-ID Team to help integrating service.

Join at menti.com | use code 3702 8425

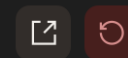
Switch

What do you think about this proposal?

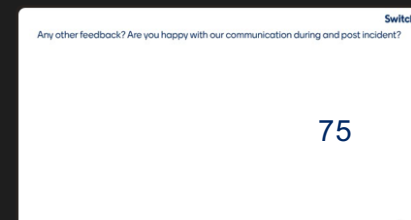
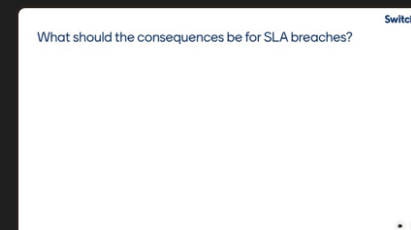
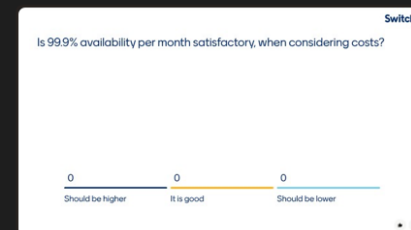
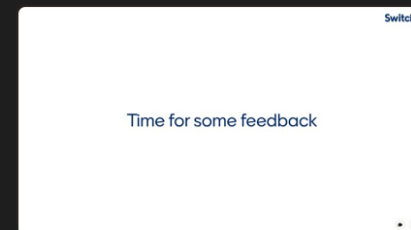


Menti

Forum Days V feedback



Choose a slide to present



Switch_

Thank You

Switch_

Feedback



Next Forum Days 2026

11 March 2026

WELLE 7



Procurement WG, Video WG, ISMS WG, SCLC WG & Cloud

Switch_

Next

Day Recap 3:15 – 4:00 PM

Campussaal

Followed by a Farewell Coffee & Networking

Switch

A solid orange horizontal bar positioned directly beneath the end of the word "Switch".