

New edu-ID Features

SWITCH

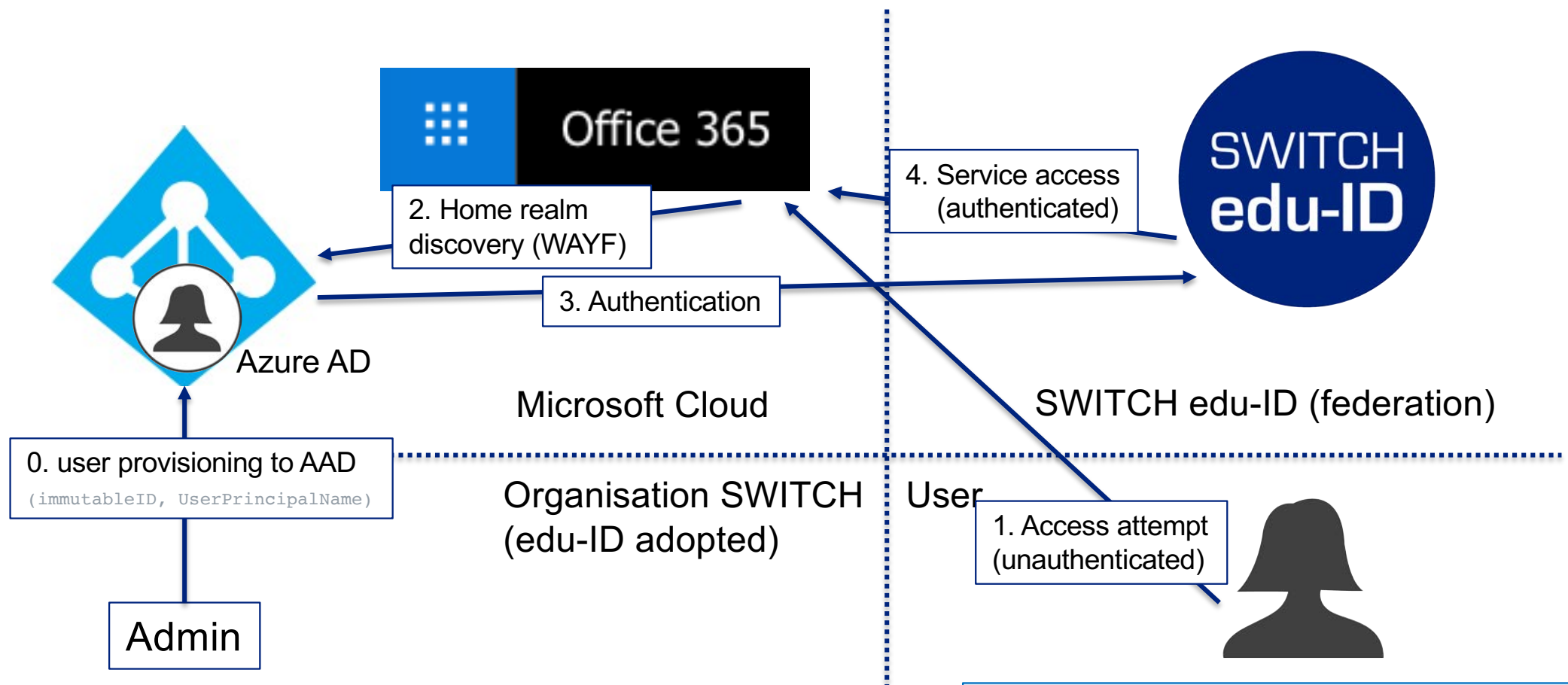
Rolf Brugger
rolf.brugger@switch.ch

TRID WG Meeting, 26.5.2021

Overview

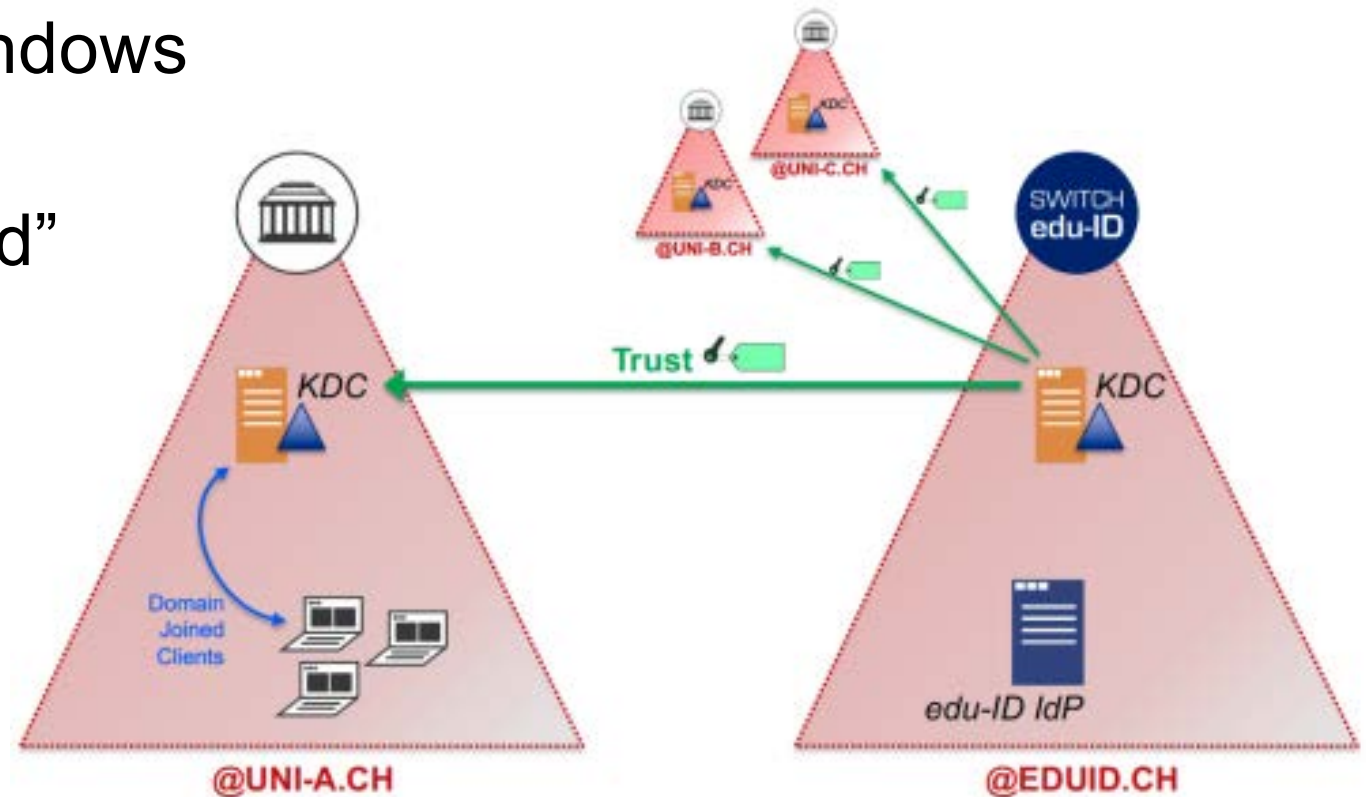
- Microsoft Interoperability: new authentication methods
- Organizational Administration Portal
- SCIM API extensions
- OpenID Connect Production
- Attribute Quality improvements
- Behind the scenes: high availability architecture

Azure AD Authentication via edu-ID



SPNEGO-based Kerberos Authentication

- edu-ID Login with Windows credentials
- For “domain controlled” devices



Kerberos Login Window

Anmeldung für: AAI Attribute Viewer

Beschreibung des Dienstes:
Displays all available attributes of a user for debugging and informational purposes.

SWITCH edu-ID

E-Mail:

Passwort:

[Passwort vergessen?](#)
[Optionen zum Schutz der persönlichen Daten](#)

Desktop-Anmeldung verwenden:

Automatisch Desktop Anmeldung versuchen, falls verfügbar.

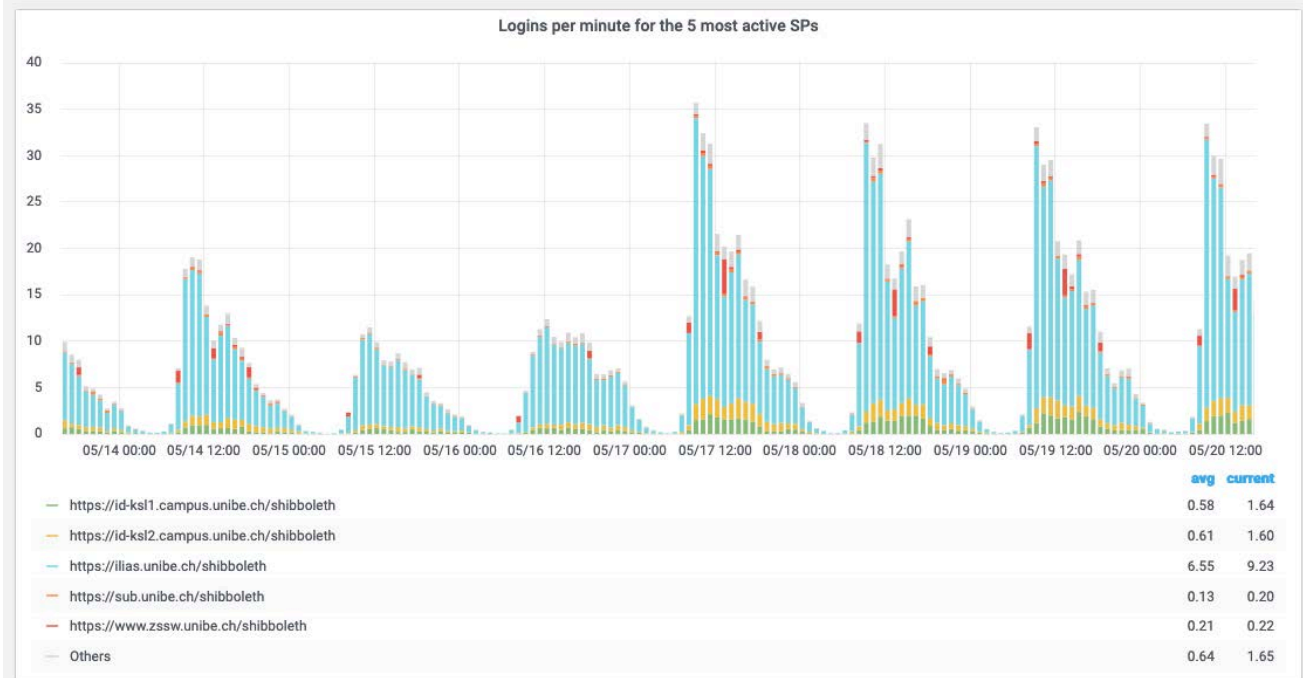
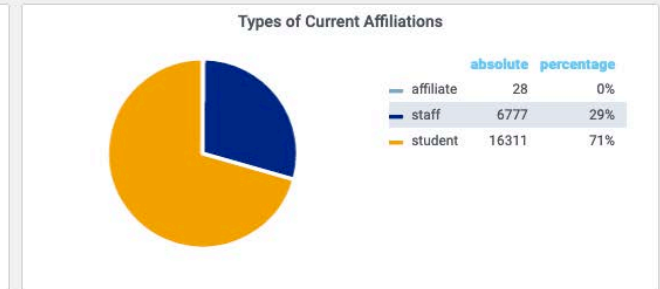
SWITCH

Edu-ID Organization Administration Portal Statistics

Statistics

Current Universität Bern affiliations:	23125
Users with a current Universität Bern affiliation:	20183
Former Universität Bern affiliations:	922
Disabled Universität Bern affiliations:	0

Timerange: 1 week



Administration Portal: Technical accounts

- Read-only accounts: user can't change account details or credentials
- Restrict access to list of services
- API to create/update technical account

Technical Accounts

The following technical accounts exist for SWITCH Staff:

 Moodle Monitoring User (edu-ID: 00005689-7b2e-445a-b084-544-0000236292525401@maclh.switch.ch)
Username/primary e-mail: 1233@example.org
Created on 8. 8. 2018 09:17:39 by [Lukas Hämmerle](#)
Last login: never logged in

[View](#) [Make read-only](#) [Restrict services](#) [Remove](#)

SCIM API Extensions

Affiliation API

- get all affiliations of an organization
`GET api.eduid.ch/scim/Affiliations`
- get subset of affiliation attributes for an API user (read only)
`mail, eduPersonScopedAffiliation,
swissEduPersonHomeOrganization,
swissEduPersonHomeOrganizationType`

Users API

- Creation / update of technical accounts

OpenID Connect Production Service

- OIDC Extension integrates well into existing setup with Shibboleth IdP
→ performance, availability, security
- SAML/OIDC Protocol entirely transparent for users
→ identical login window, user consent
- Support for 2-step login
- Regulations based on existing SWITCHaai legal framework
- Supported attributes:
 - extended attribute model
 - most personal edu-ID attributes
- Restrictions: no classic attribute model, manual service registration

Maintaining Attribute Quality

- Email address quality is important
 - Login name
 - Password reset
- bounced messages from contact email address
 - Heuristics (retry after 5 days, remove/deactivate email address)
- periodic email verification of all non-organizational addresses
 - Once per year
 - GDPR compliant service Bouncer checks mail servers
 - **deliverable** ✓ **undeliverable, risky, unknown** → bounce process

Work “behind the scenes”

Performance metrics

1. **Powerful:**

capacity, speed, scalability.

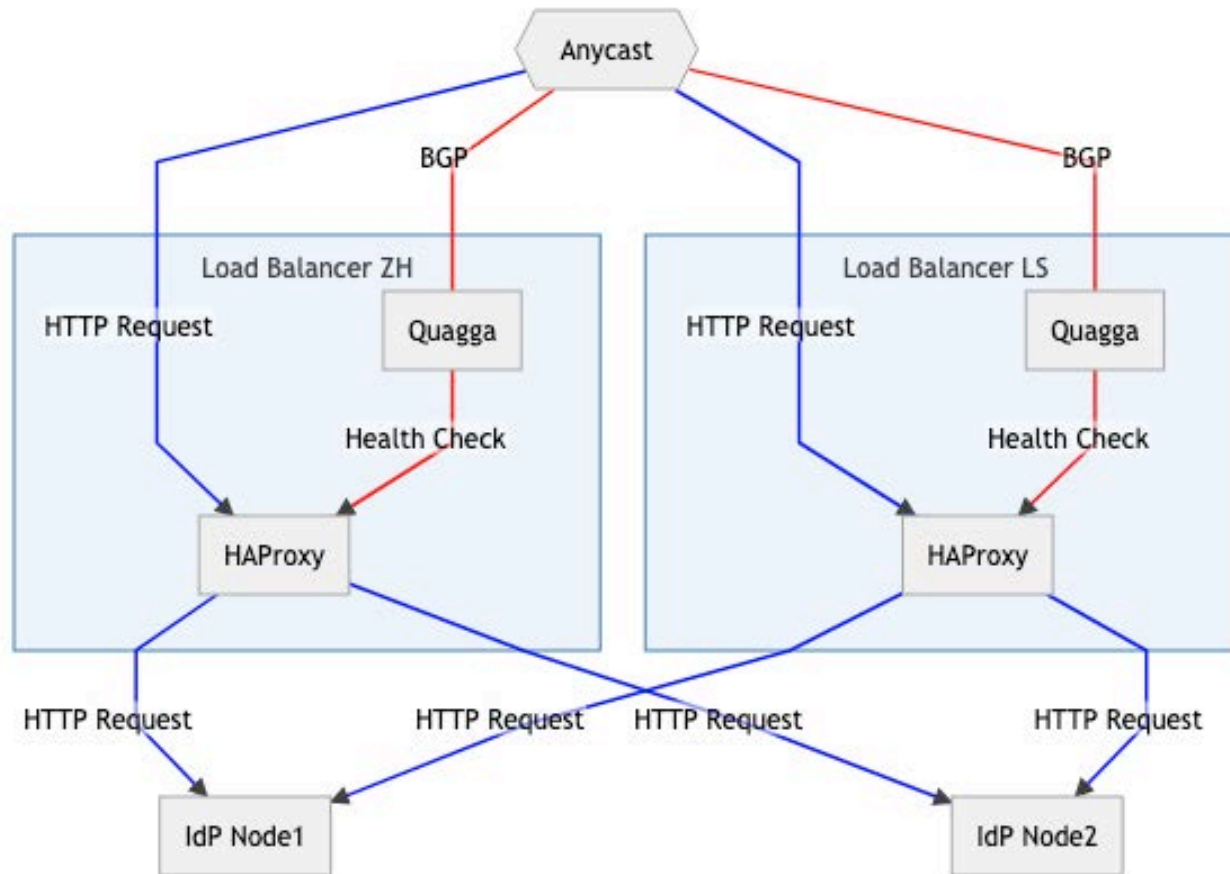
2. **Reliable:**

Availability, robustness, recovery, security.

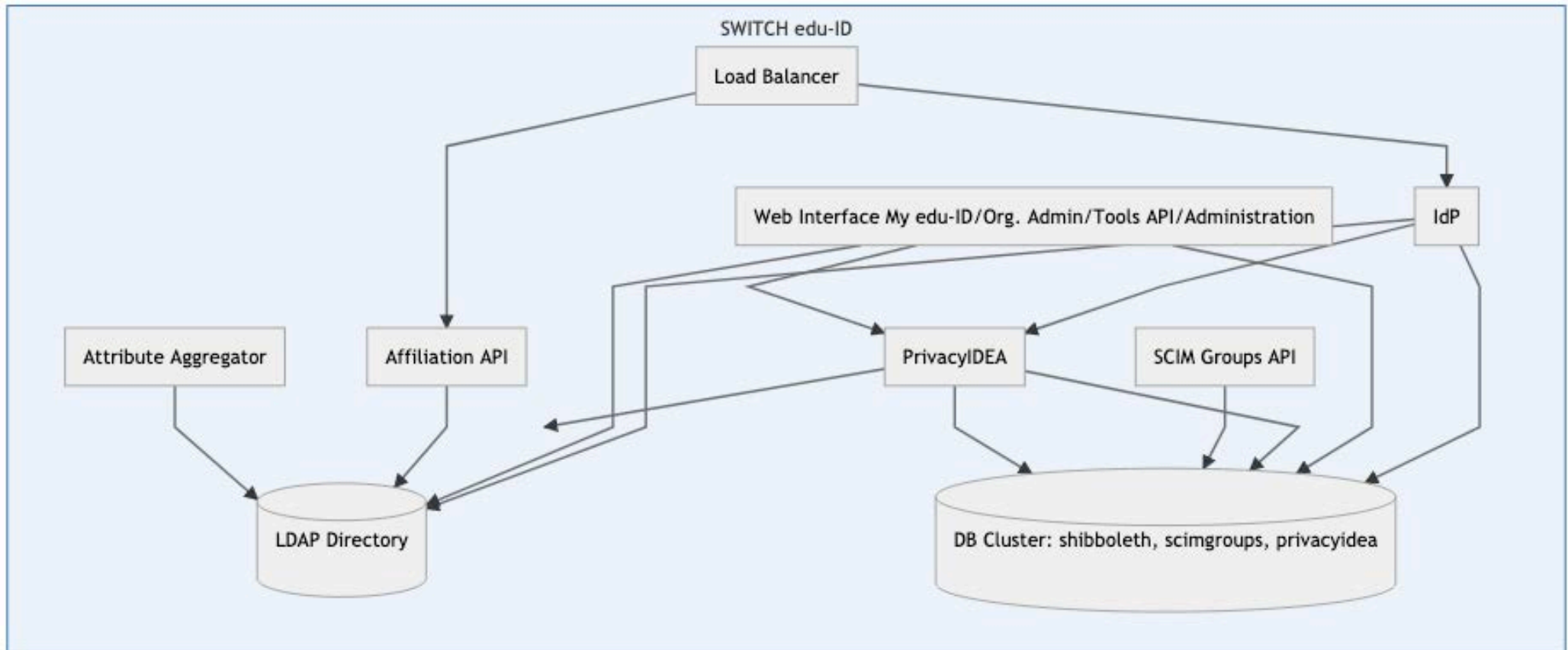
3. **Efficient:**

efficient and balanced usage of resources.

High availability setup for IdP



Edu-ID service components



Online documentation

- Reorganized Website
- New “getting started” guides for organizations and services
- Roadmap