New edu-ID Features

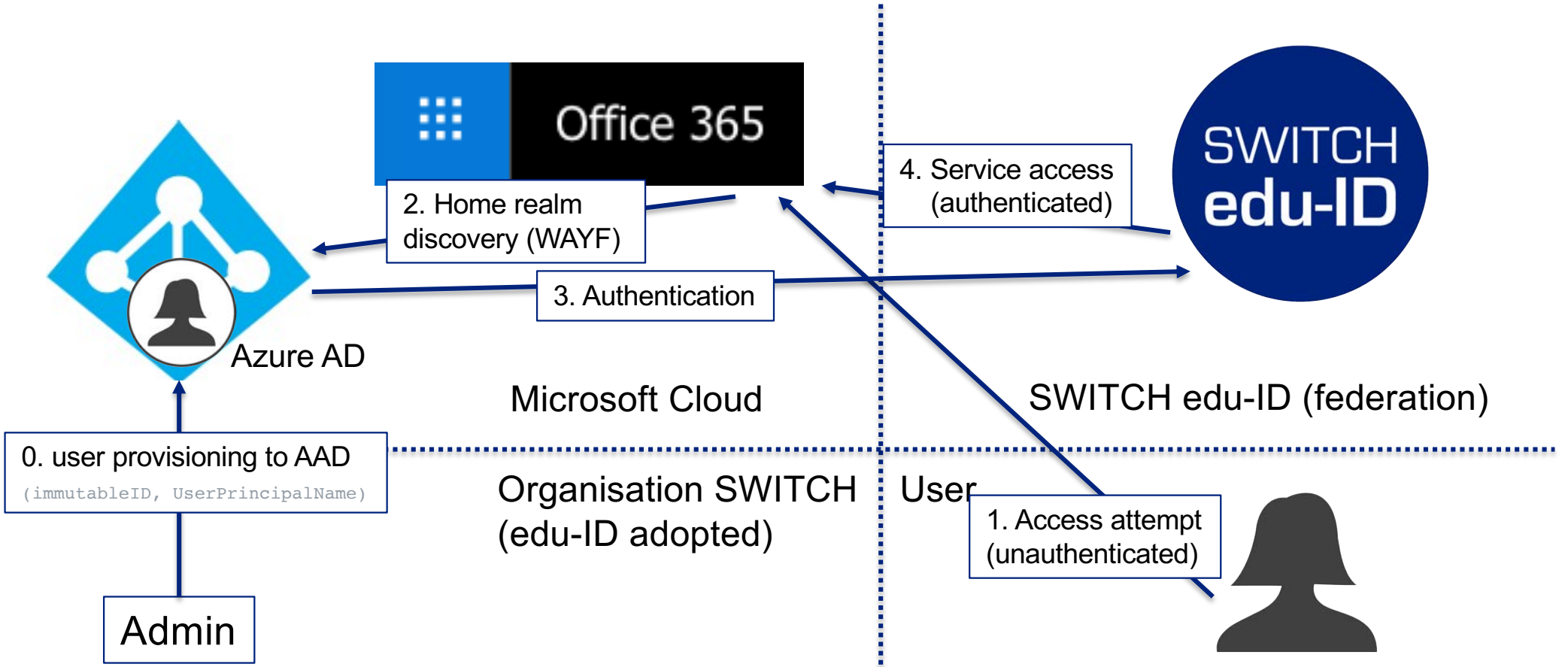
Rolf Brugger
rolf.brugger@switch.ch

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

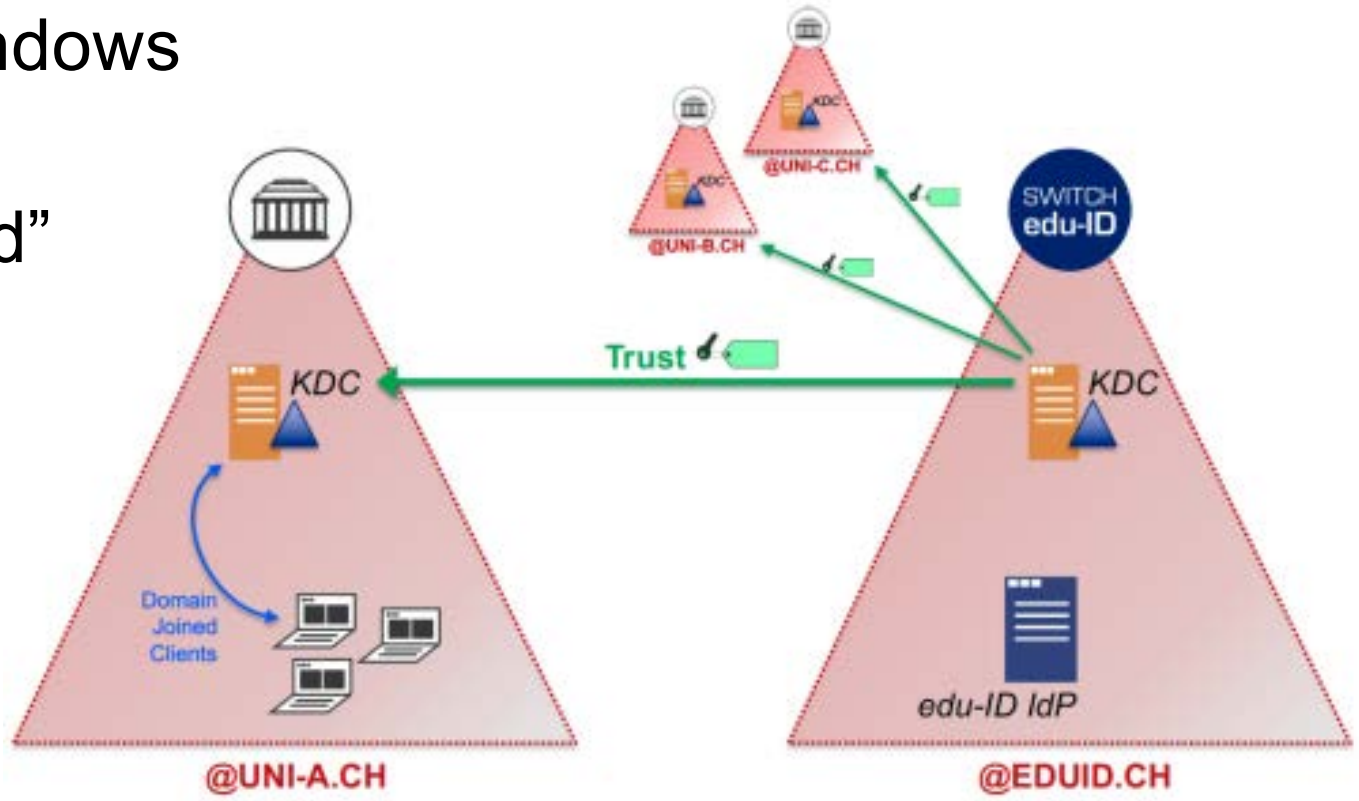
Azure AD Authentication via edu-ID



→ https://www.switch.ch/edu-id/docs/unis/tech/aad/

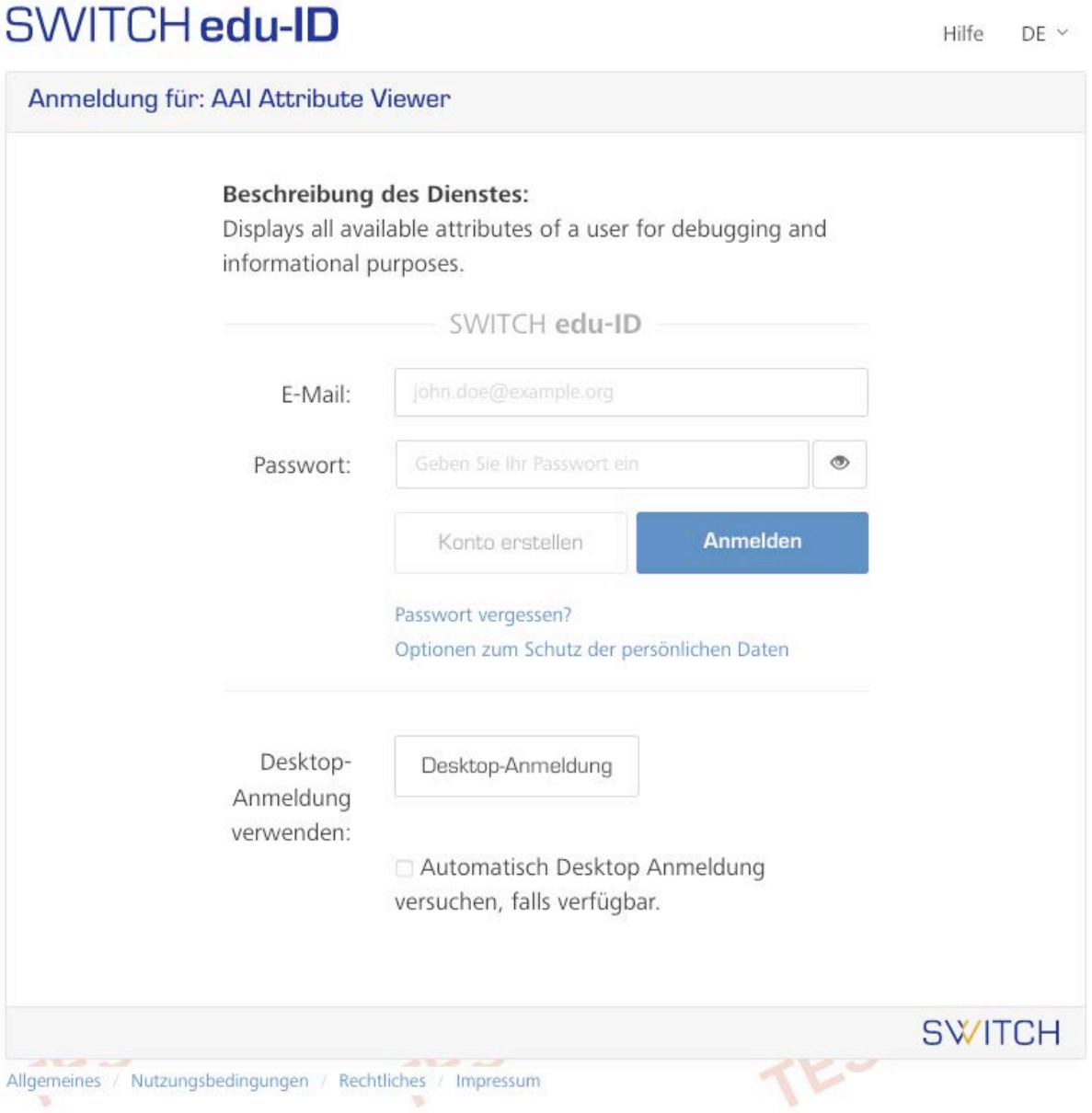
SPNEGO-based Kerberos Authentication

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

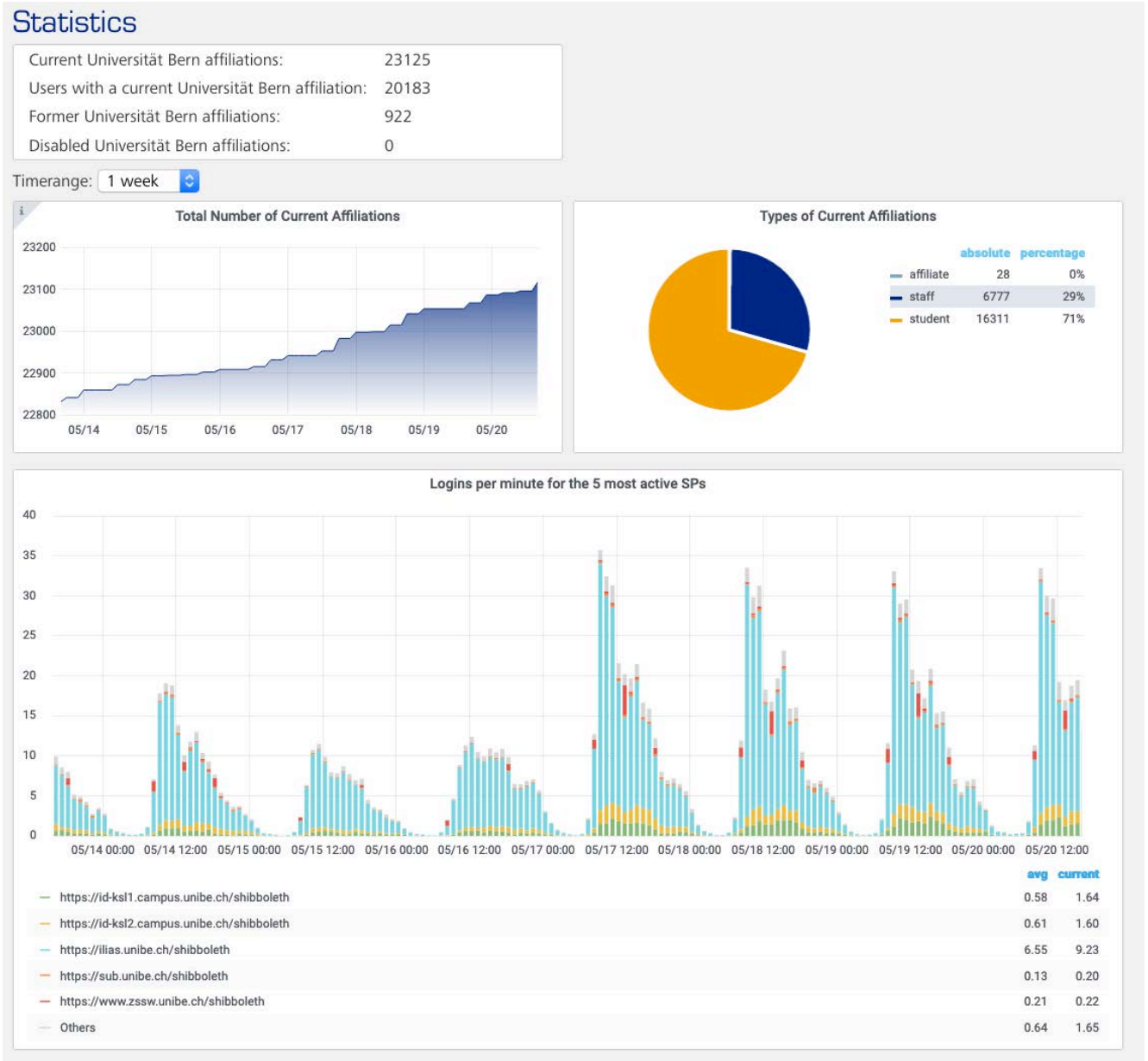


→ https://www.switch.ch/edu-id/docs/unis/tech/spnego-kerberos-authentication/

Kerberos Login Window



Edu-ID Organization Administration Portal Statistics



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

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

→ https://switch.ch/edu-id/docs/services/openid-connect/

Maintaining Attribute Quality

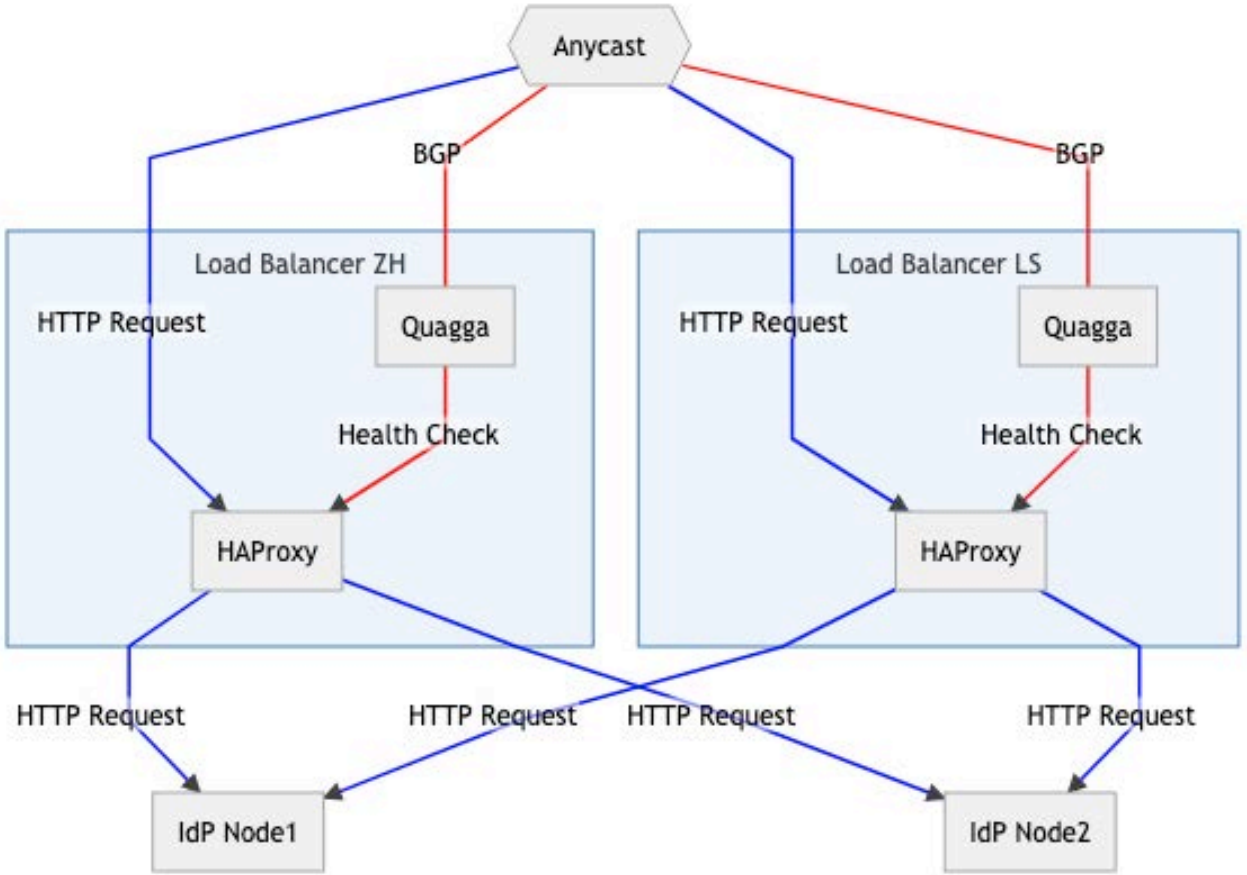
- Email address quality is important
  - Login name
  - Password reset
- bounced messages from contact email address
  - Heuristics (retry after 5 days, remove/deactivate email address)
- periodic email verification of all non-organizational addresses
  - Once per year
  - GDPR compliant service Bouncer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

Work “behind the scenes”

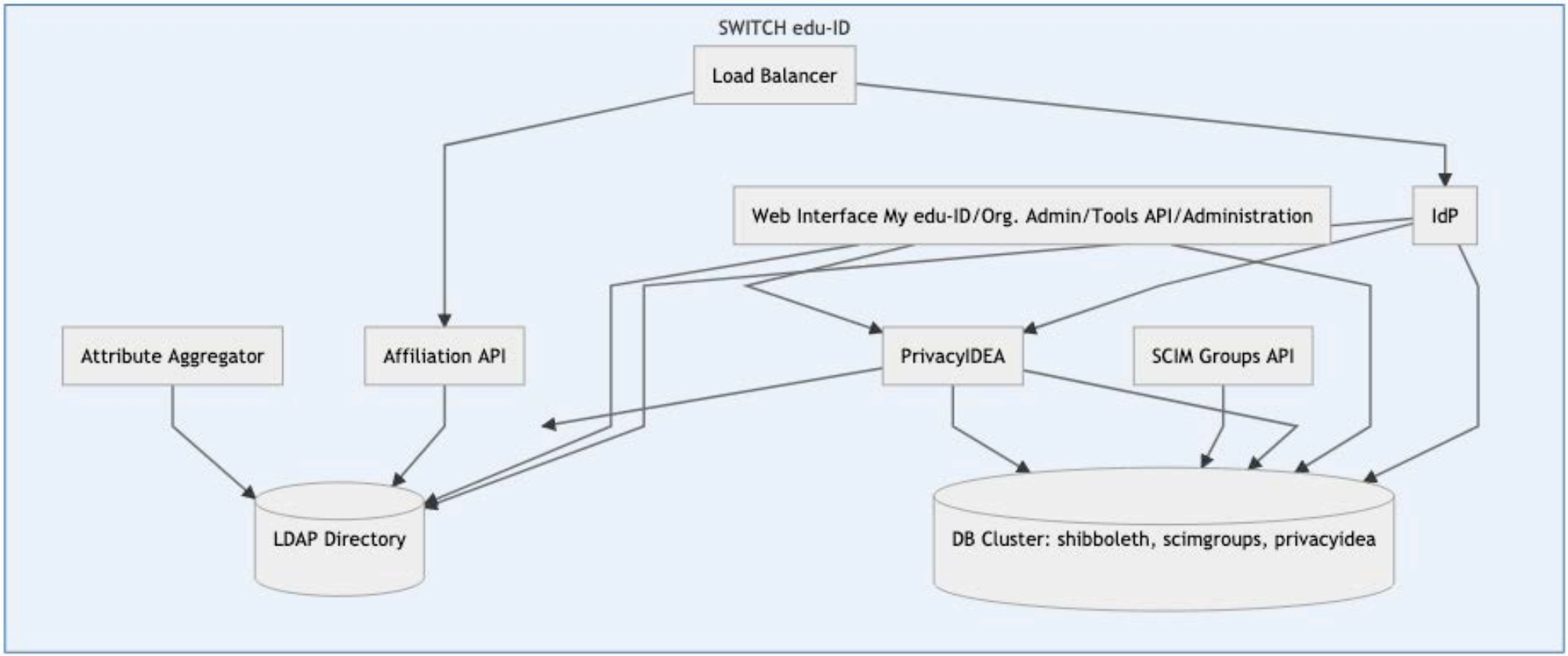
Performance metrics

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