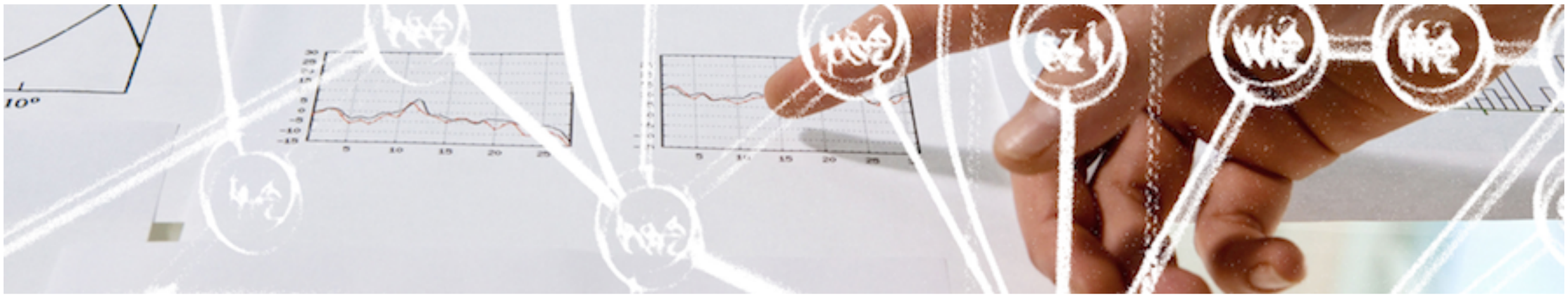
Swiss edu-ID Architecture



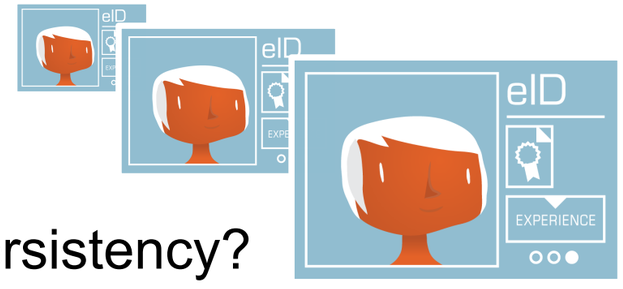
Rolf Brugger
rolf.brugger@switch.ch

Swiss edu-ID Update, Bern, 30.6.2016

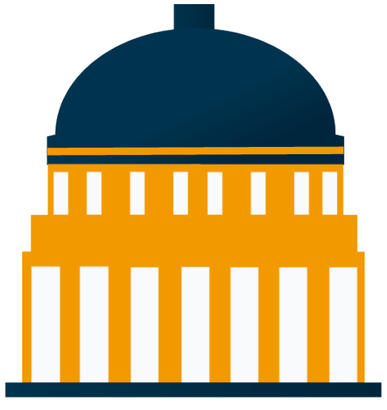
Swiss edu-ID concept corner stones

- Persistency:
  - Built to survive organisational affiliations
- User-centrism:
  - User issues his/her identity in a light-weight self-registration process
  - User brings his/her identity to the university/employer (if pre-existing)
  - User decides whether to pass on data (but usually not on its contents!)
- Organisational backing:
  - Organisations add or validate attributes of identities
- Openness:
  - Open to members of Swiss academia and people with relation to it
- Scalable quality:
  - Allow for low quality: Yes, this is a feature!
  - Foresee validation processes to increase the quality level
  - Offer quality transparency: relying parties can base decisions on quality level
- Support mobile environments and non-web use cases

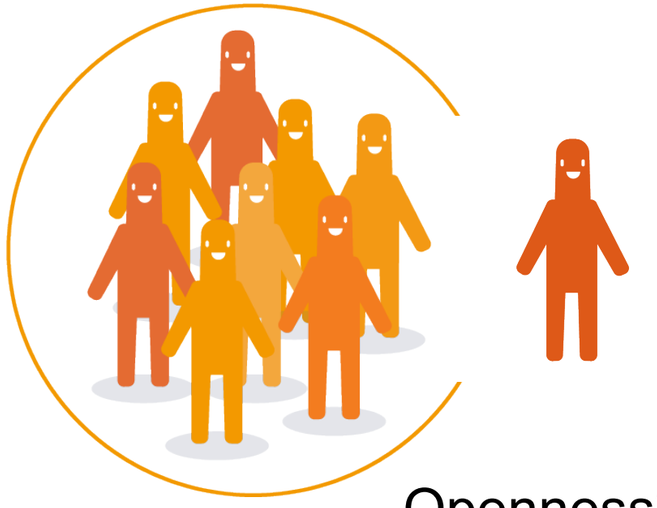
Questions from the Community



Persistency?



Role of organisations?



Openness?

User centrism?

Openness:
“*Not anyone should have a Swiss edu-ID*”

because

Having an [illegible]plies access rights

misconception

Getting access is done by a
- explicit (identify person)
- implicit (personal attribute)
registration procedure

Counterexample:
ID / Passport

User-centrism:
“*Make sure Swiss edu-ID has sufficient quality*”

because

Sharing attributes makes SPs more efficient

but

Not all SPs need high quality attributes

attribute quality

tradeoff

low entrance barrier

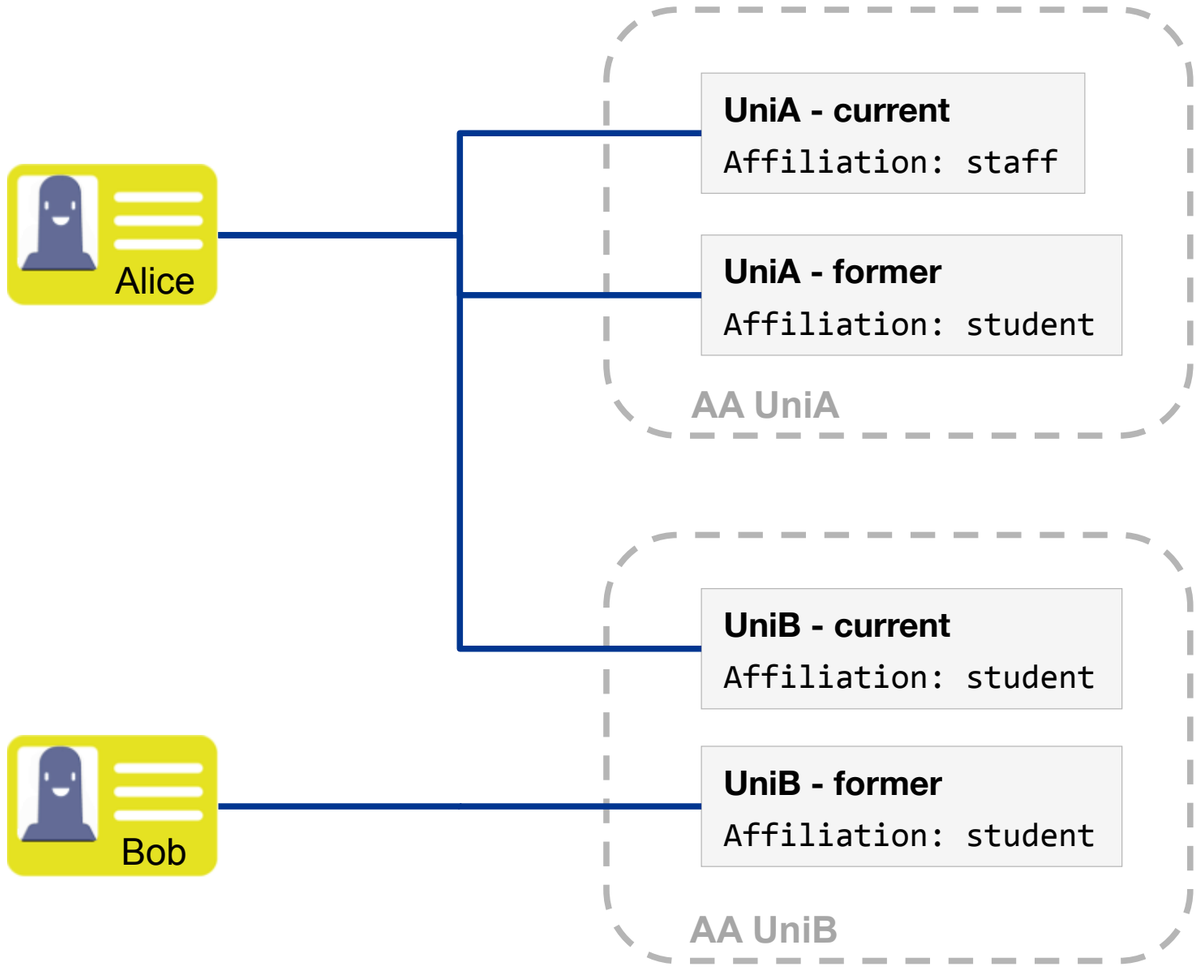
Counterexample:
Github-ID

Swiss edu-ID quality model

- Authentication quality: NIST SP 800-63-2
  - Level 1: no id proving
  - Level 2: single factor auth
  - Level 3: multi factor auth
  - Level 4: multi factor auth with hard cryptographic tokens

- Attribute validation quality: eCH-0171 quality model
  - Level 1 “low”:
    Minimal trust in asserted value
  - Level 2 “medium”:
    Basic processes and control mecha-nisms. Verification with non-official ID or certificate
  - Level 3 “high”:
    Processes and control mechanisms are supervised by external entity. Verification with more than one non-official ID or certificate
  - Level 4 “very high”:
    Processes backed by legal standards. Supervision by accredited entity. Veri-fication with official ID or certificate

Attribute Model Extension



Attribute Model in Swiss edu-ID

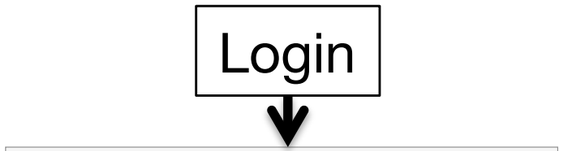
Extended Model

- Represents multiple or no affiliations in a single attribute statement
- Supports quality model (for user provided attributes)
- Attribute specification based on aai

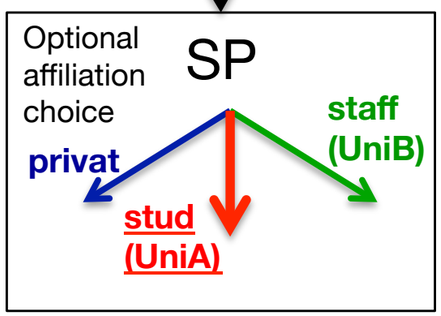
Classic Model

- Represents exactly one affiliation
- Fully compatible with aai

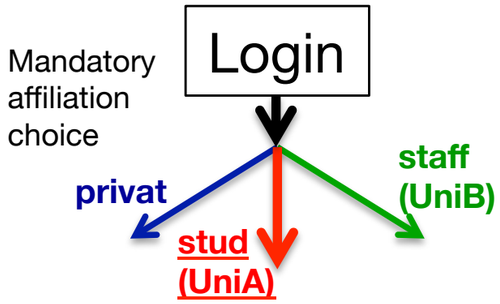
“Extended Model”



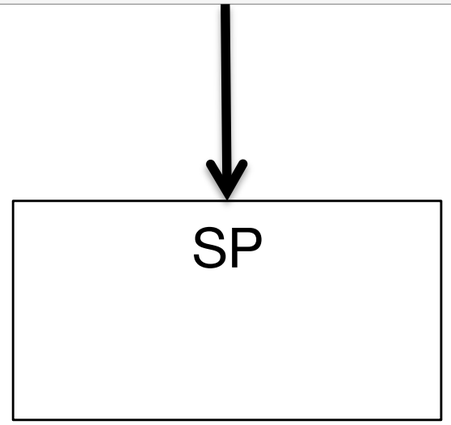
Unique/pers-edu-ID
HomeOrg eduid.ch
Name
Email (user-managed)
Home postal address
Mobile phone
Date of birth
ORCID
Affiliation student@UniA
study branch
Email (affil) johnd@uniA.ch
Affiliation staff@UniB
Email (affil) johnd@UniB.ch
landline phone
Business postal address



“Classic Model”



Unique/pers-ID id@UniA
HomeOrg UniA
Name
Home postal address
Mobile phone
Date of birth
ORCID
Affiliation student@UniA
study branch
Email (affil) johnd@uniA.ch



Quality in Both Models

"Extended Model"

Unique/pers-edu-ID
HomeOrg eduid.ch
Name **quality 1..4**
Email (user-managed) **quality 1..4**
Home postal address **quality 1..4**
Mobile phone **quality 1..4**
Date of birth **quality 1..4**
ORCID **quality 1..4**

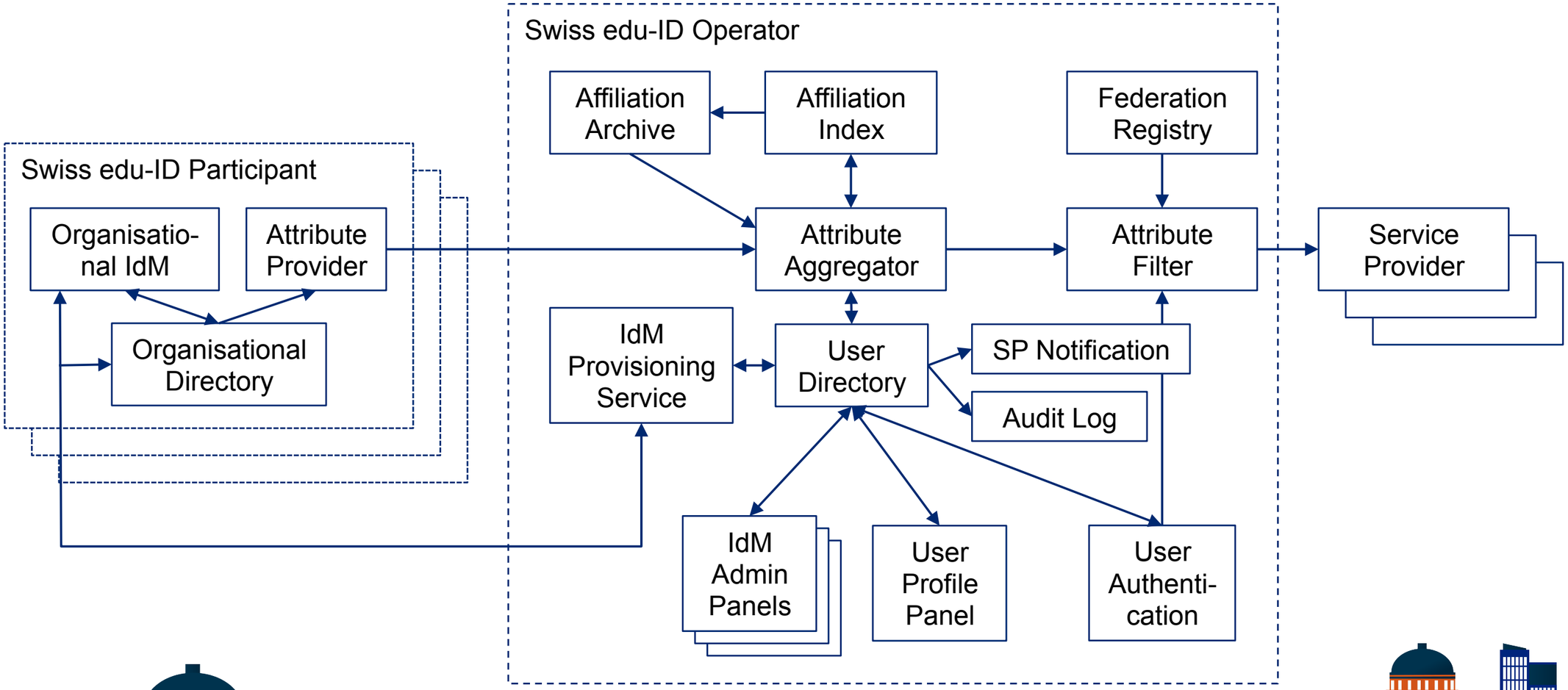
AAI-quality
Affiliation student
study branch
Email (affil) johnd@uniA.ch
Affiliation staff@UniB
Email (affil) johnd@UniB.ch
landline phone
Business postal address

"Classic Model"

Unique/pers-ID id@UniA
HomeOrg UniA

AAI-quality
Name
Home postal address
Mobile phone
Date of birth
ORCID
Affiliation student@UniA
study branch
Email (affil) johnd@uniA.ch

Basic Components of Swiss edu-ID



Participants

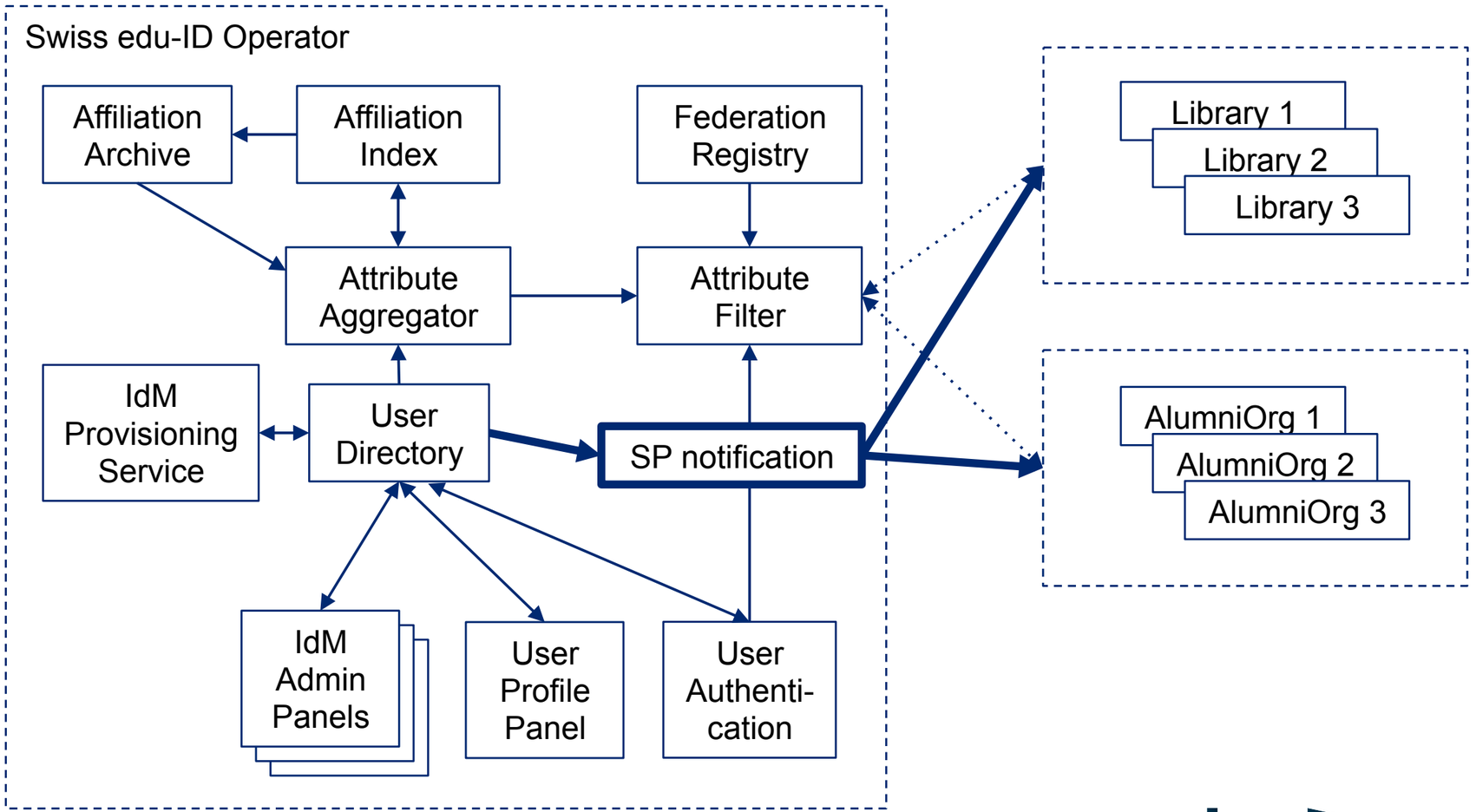
Operator

Participants and Federation Partners

Roles and Responsibilities

Role	Description
Service Registration Administrator at Participant	Confirms/rejects Service Providers from own organisation
Service Registration Administrator at Operator	Confirms/rejects Service Providers from Federation Partners without Attribute Provider
Service Administrator	Registers and updates Service Provider descriptions in Federation Registry
Attribute Release Administrator	Defines attribute release policy for all Service Providers
IdM Administrator	Handles IdM updates
Participant IdM Admininstrator	Signs federation partner agreement

Keeping SPs up to date



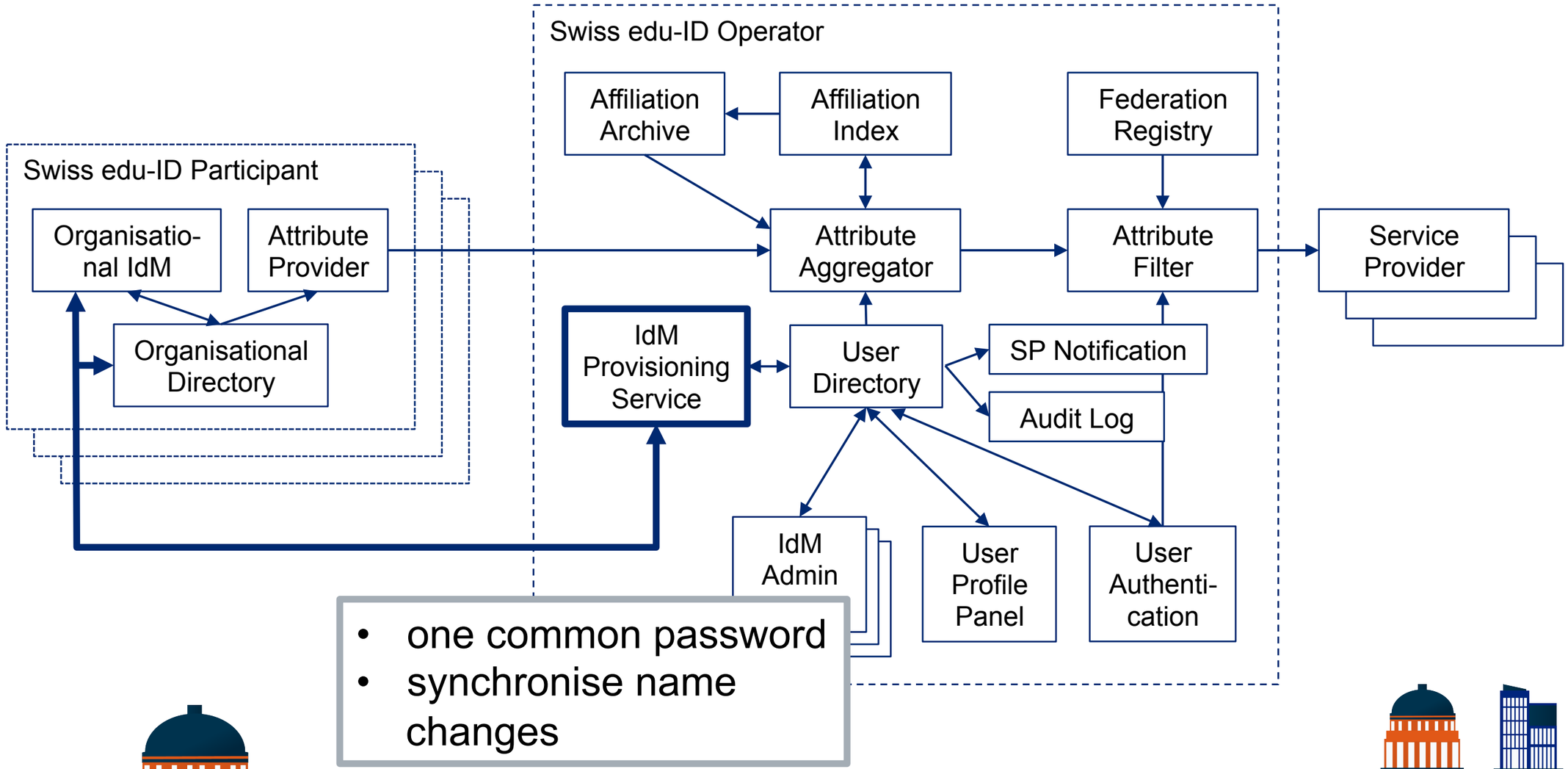
SWITCH

Operator

SWITCH

Participants and Federation Partners

Synchronize IdM of Universities and Swiss edu-ID



Participants

Operator

Participants and Federation Partners

Identity Management Processes

- Account…
  - Creation
  - Blocking / unblocking
  - Deletion
- Death of a user
- Attribute…
  - Editing
  - Verification
- Duplicate account…
  - Detection
  - Resolution
- Current affiliations…
  - Person enters an organisation (add affiliation)
  - Person leaves an organisation (transform affiliation “current -> former”)
- Former affiliations…
  - Add
  - Edit
  - Delete

Blog: identityblog.switch.ch

Website: eduid.ch