Adoption Path for an Organization

• API: Organization notifies edu-ID about new affiliations
• API: edu-ID knows current attributes for a person
  • edu-ID requests current attributes when they are needed (polling)
  • Organization notifies edu-ID about attribute changes (pushing)
• Make sure all organization members …
  • Have an edu-ID
  • Linked to organizational identity
    ➔ Current and future members
• Shut down local Shib-IdP
Onboarding of new (future) Users, Offboarding and Attribute Updates
On-/off-boarding in the “Leading System” approach

Member enrolment
(online form with edu-ID Login)

Email, Name, ID

Email, Name, ID, …

Member un-enrollment

Email
Name
ID

on-/off-boarding, updates (notification)

ID, affiliation

User data flow

edu-ID protected web site
Decentral On-/off-boarding in the “Meta Directory” approach

Member enrolment

Member enrolment

Member enrolment

Employee mgt system

Student mgt system

Cont. educ. mgt system

Meta DB

Full edu-ID coverage

Member un-enrolment

edu-ID IdP

edu-ID IdM

Email, Name, ID

on/off-boarding, updates (notification)

ID, affiliation

User data flow

edu-ID protected web site
Centralized On-/off-boarding in the “Meta Directory” approach (synchronous)

Member enrolment → Employee mgt system

Member enrolment → Student mgt system

Member enrolment → Cont. educ. mgt system

Member enrolment → Meta DB

edu-ID Linking (i.e. mail invitation)

Account Creation

onboarding (notification)

idP

IdM

Member un-enrolment

User data flow

edu-ID protected web site
Centralized On-/off-boarding in the “Meta Directory” approach (asynchronous)

- Member enrolment
- Employee mgt system
- Student mgt system
- Cont. educ. mgt system
- Member un-enrolment

“Meta” DB
Partial edu-ID coverage

edu-ID Linking

- edu-ID IdP
  - onboarding (notification)
  - affiliation

- edu-ID IdM
  - offboarding, updates (by periodical polling)

User data flow
edu-ID protected web site
edu-ID Linking Page

University: user profile

https://eduid.ch/link
?code=123XYZ
&ret=uni.ch/uprofile

edu-ID login

create edu-ID

edu-ID linked

https://uni.ch/uprofile
?code=123XYZ
&id=f7b83c42-9f3d-45de-8146-1e00e15938a9

Onboarding “add affiliation”

edu-ID IdP
API to Update Affiliation Status (SCIM)

- Organization informs edu-ID IdP about affiliation changes
  - Add/remove affiliation
  - Update affiliation (attribute push as alternative to attribute polling)

- SCIM REST API (Draft)

**Add an affiliation:**
PUT https://eduid.ch/api/v1/Users/04111fb2-5e82-4b20-81bf-fa0f4f86aa07
{
  swissEduIDLinkedAffiliation: "student@organization.org",
  swissEduIDAffiliationPeriodBegin: "2017-12-01"
}

**Remove an affiliation:**
PUT https://eduid.ch/api/v1/Users/04111fb2-5e82-4b20-81bf-fa0f4f86aa07
{
  swissEduIDAffiliationPeriodEnd: "2017-12-01"
}
Basic Components - Simplified

- Swiss edu-ID Participant
  - Organisational IdM
  - Attribute Provider
  - Organisational Directory

- Swiss edu-ID Operator
  - Attribute Aggregator
  - Attribute Filter
  - User Directory, Attribute Archive
  - SP Notification
  - IdM Provisioning Service
  - IdM Administration UI
  - User UI

- Service Provider

Attribute polling
Attribute push
Equip all Current Organization Members with an edu-ID
Adoption Path

Linked

Integrated

© 2017 SWITCH | 12
Scenario 1: Involve all Users before Day X

Preparation: invite users to create and link edu-ID account

Before day X: linked accounts have limited functionality. Users can’t access to classic SPs as Org-members.

At day X: Merge linked accounts
Scenario 2: Involve Users after Day X

At day X:
- Users lose federation account

After day X:
- Invite users to create and link account

At day X:
- Merge linked accounts
Scenario 3: create edu-ID for Users

At day X:
create edu-ID accounts

Duplicate resolution

At day X:
Merge linked accounts