The "Swiss edu-ID"

The persistent Swiss academic digital identity

SWITCH

Christoph Graf
christoph.graf@switch.ch
swisseduid@switch.ch

AAI/Swiss edu-ID Info Day, University of Berne, 13.8.2014
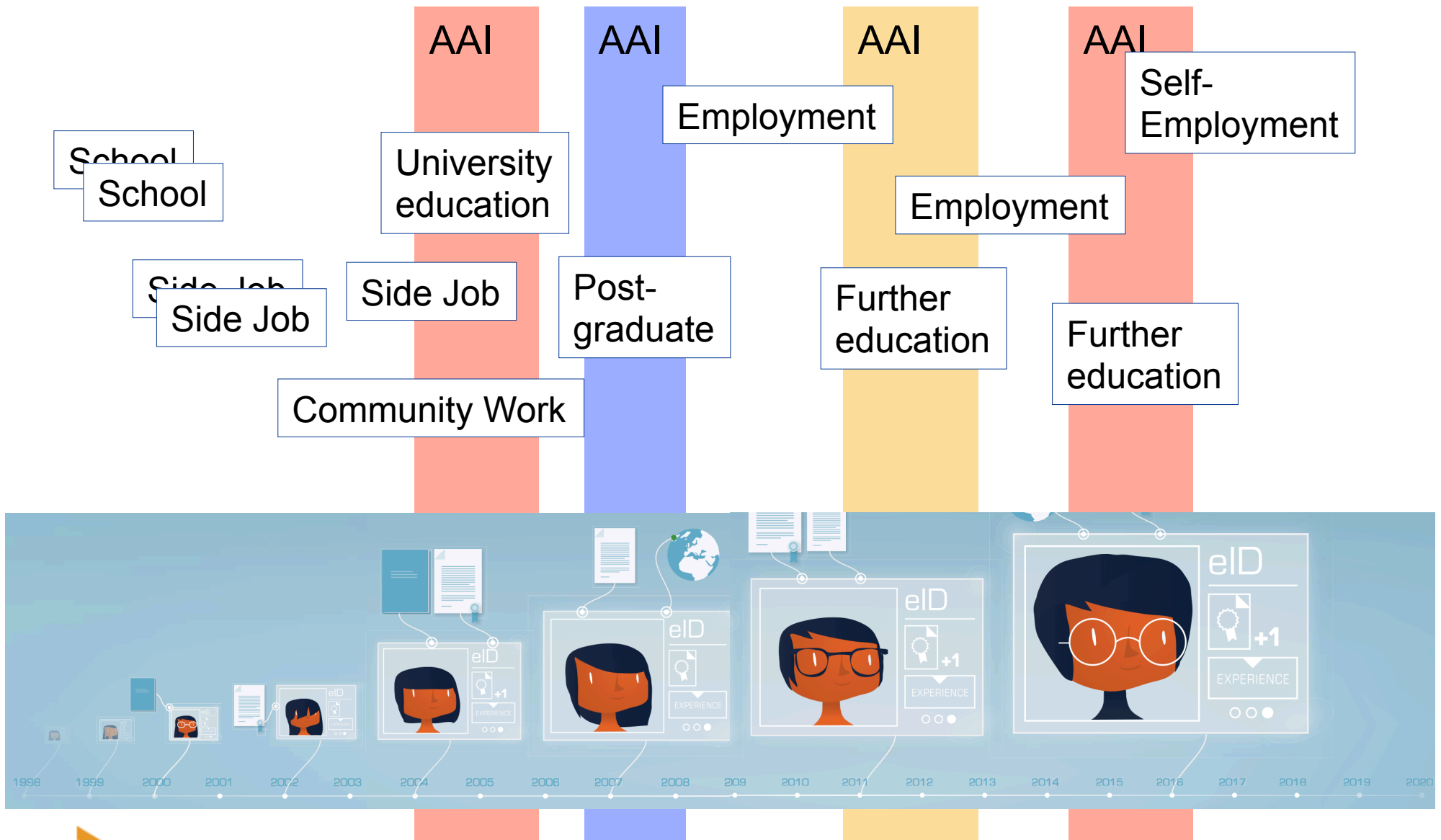
Outline

- About the Swiss edu-ID (Christoph Graf)
  - Motivation, use cases
  - Basic concepts
  - Architecture
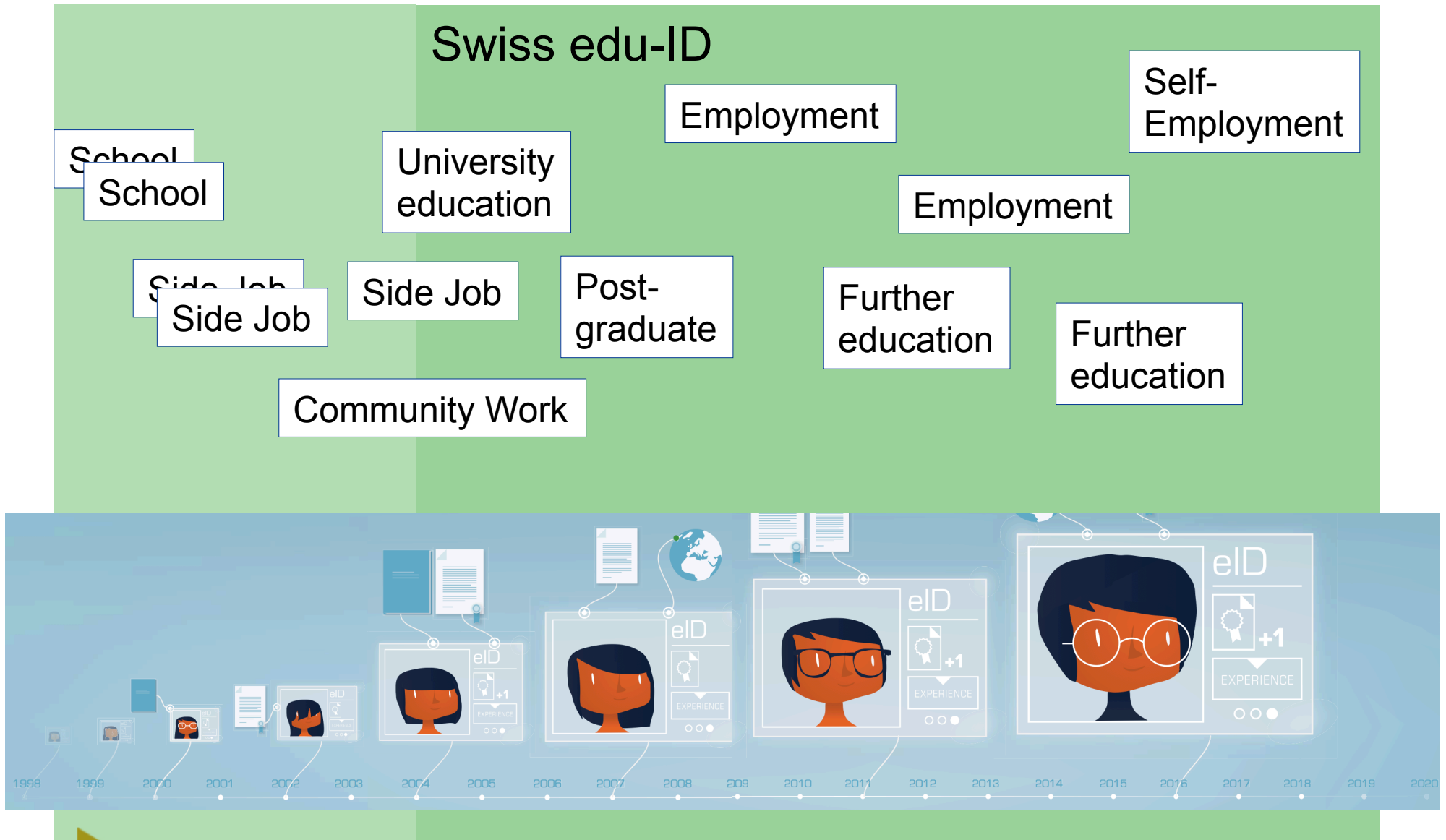 - Benefits for users and institutions

  (Short bio-break)

- Roadmap (Rolf Brugger)

- Working Groups (Petra Kauer-Ott)

Identity Management today…

AAI   AAI   AAI   AAI

School

School

University
education

Employment

Self-
Employment

Side Job

Side Job

Side Job

Post-
graduate

Employment

Further
education

Further
education

Community Work

3

... Identity Management tomorrow

Swiss edu-ID

School

School

University education

Employment

Self-Employment

Employment

Side Job

Side Job

Side Job

Post-graduate

Further education

Further education

Community Work

Identity Management @ CUS P-2

- Use cases collected in spring '13, conclusions Aug '13:
  Prominent role of identity management confirmed

- Sub-strategy groups deliver by 11 Oct '13:
  "Identity Management" group proposes the "Swiss edu-ID"

- Project submission "Swiss edu-ID" by 10 March '14:
  Implementing the first year of the sub-strategy's roadmap

- Conditional approval in April, final P-2 approval received June '14:
  Swiss edu-ID is the first project of the first call receiving green light

- High-level architecture document released July '14:
  Further refining and detailing the sub-strategy, see
  http://www.switch.ch/export/sites/default/uni/projects/eduid/documents/
  SwissEduIDArchitecture.pdf

"Swiss edu-ID" project brief

Proposed runtime:
- 1 May '14 – 30 June '15

Funded Partners:
- SWITCH

Unfunded partners:
- participants in community task forces

Funding:
- efforts total: 950kCHF
- P-2 contribution: 475kCHF
- Main expenditure class: 80% staff

Project status

SWITCH started the first two action items before knowing the outcome of the call:

- "Attribute specification":
  - Task force formed and first meeting held 9 April '14
  - Proposal based on input being finalised

- "High level architecture":
  - together with (extended) sub-strategy authors
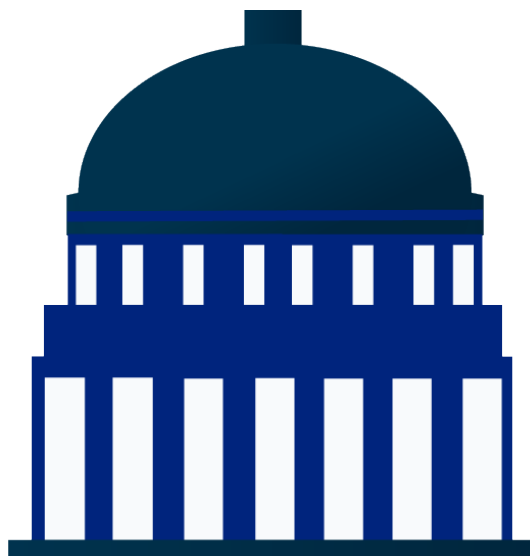   -> see next slides

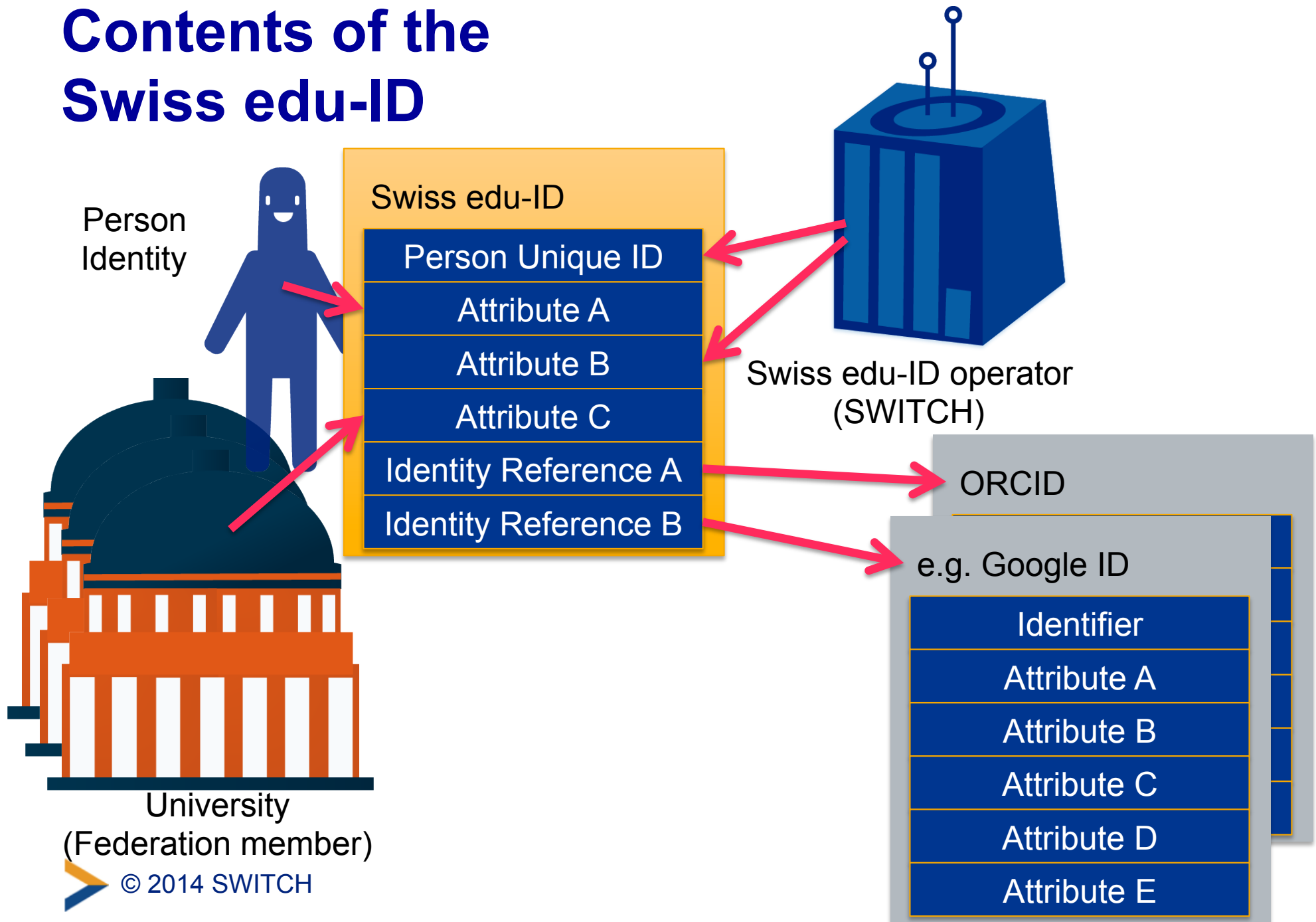# Scoping the Swiss edu-ID

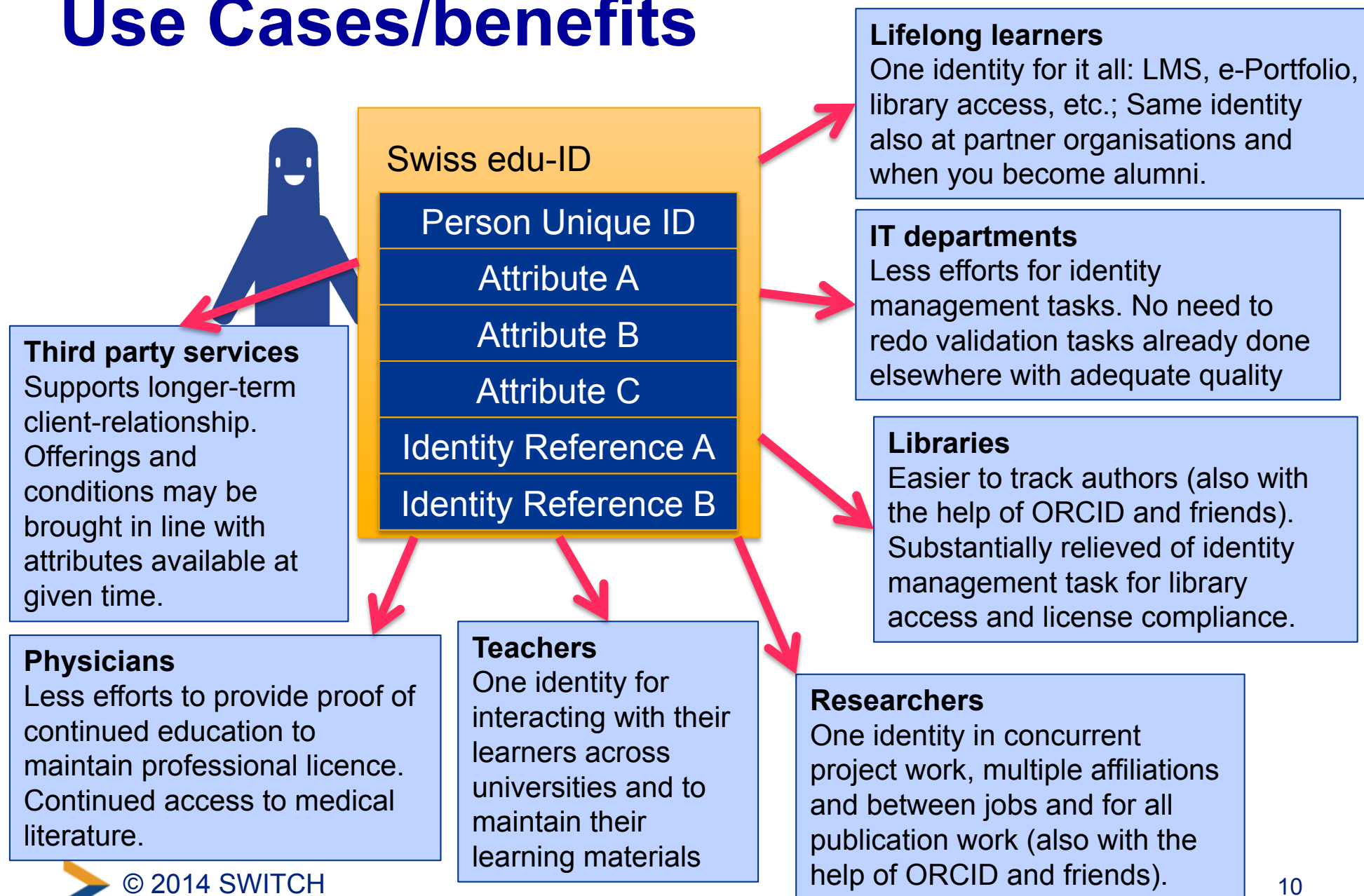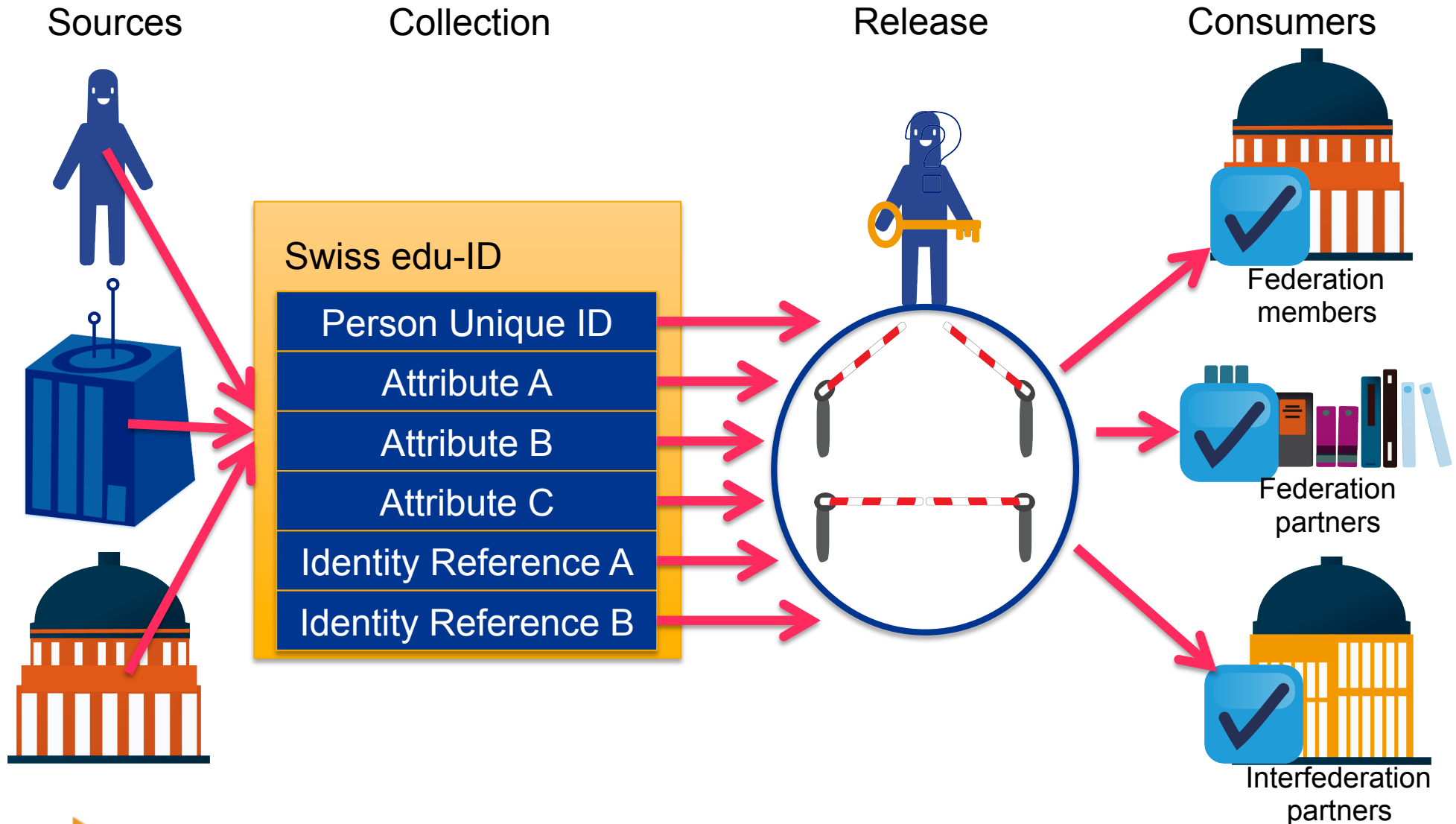Person Identity
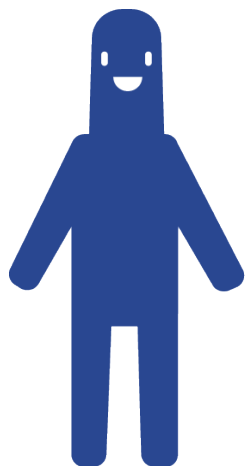
Group Identity

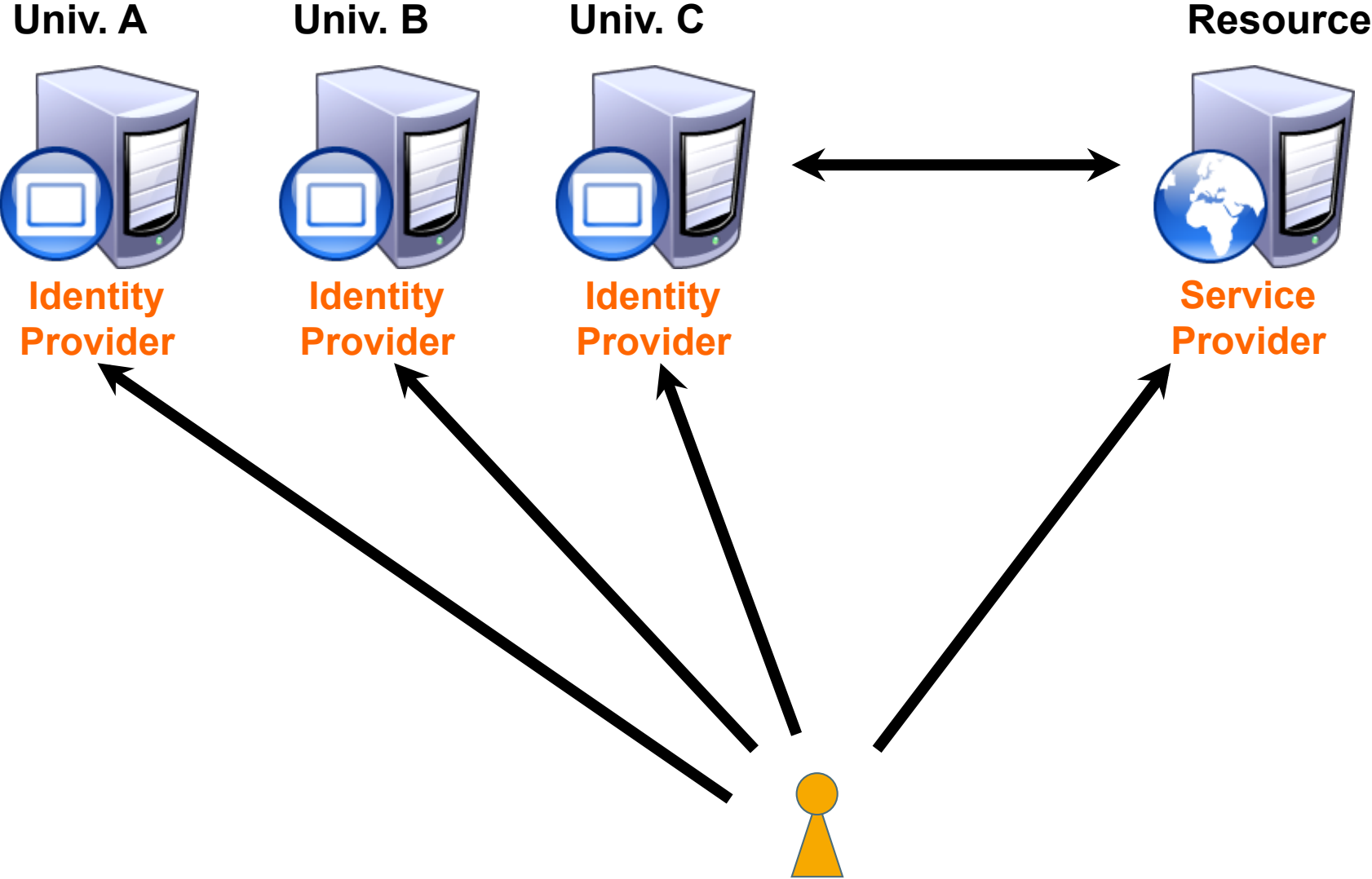Organisation Identity

Thing Identity

8

Contents of the Swiss edu-ID

Use Cases/benefits

Swiss edu-ID

- Person Unique ID
- Attribute A
- Attribute B
- Attribute C
- Identity Reference A
- Identity Reference B

Lifelong learners
One identity for it all: LMS, e-Portfolio, library access, etc.; Same identity also at partner organisations and when you become alumni.

IT departments
Less efforts for identity management tasks. No need to redo validation tasks already done elsewhere with adequate quality

Libraries
Easier to track authors (also with the help of ORCID and friends). Substantially relieved of identity management task for library access and license compliance.

Third party services
Supports longer-term client-relationship. Offerings and conditions may be brought in line with attributes available at given time.

Physicians
Less efforts to provide proof of continued education to maintain professional licence. Continued access to medical literature.

Teachers
One identity for interacting with their learners across universities and to maintain their learning materials

Researchers
One identity in concurrent project work, multiple affiliations and between jobs and for all publication work (also with the help of ORCID and friends).

10

Information flow & control

Sources   Collection   Release   Consumers

Swiss edu-ID

- Person Unique ID
- Attribute A
- Attribute B
- Attribute C
- Identity Reference A
- Identity Reference B

Federation members

Federation partners

Interfederation partners

The AAI architecture …

Univ. A — Identity Provider

Univ. B — Identity Provider

Univ. C — Identity Provider

Resource — Service Provider

12

... vs. the Swiss edu-ID architecture

Univ. A

Univ. B

Univ. C

Resource

Attribute Provider

Attribute Provider

Attribute Provider

Service Provider

Longterm Identity Provider

Interoperability considerations

Interoperability with SWITCHaai (including interfederation), for linking attribute authorities, maybe social media

> SAML

Interoperability with e-Gov initiatives and for attribute validation: SuisseID, eID/STORK

> X.509, SAML

Linking attribute authorities and external identities like ORCID, social media identities. Mobile device support/integration

> OAuth2/OpenID Connect

More? Additional APIs?

> We'll see as we go along…

Some open questions (1/3)

Unique Identifier for Swiss edu-ID needed
- What are the requirements for such an identifier?
- Restrictive release policy due to persistence?

due:
mid 2014

One person, multiple roles
- Must fit into one single identity
- Will user need to select the appropriate role?
(after authentication, before user consent)
- How about SSO? Acceptable user experience?

due:
end 2014

Some open questions (2/3)

Levels of assurance needed?

– Attributes from multiple sources

– Varying verification procedures

– Old attributes (e.g. historic affiliations)

– Self-declared attributes (e.g. avatar, phone numbers)

– Levels of assurance even needed for individual attributes?

due:
end 2014

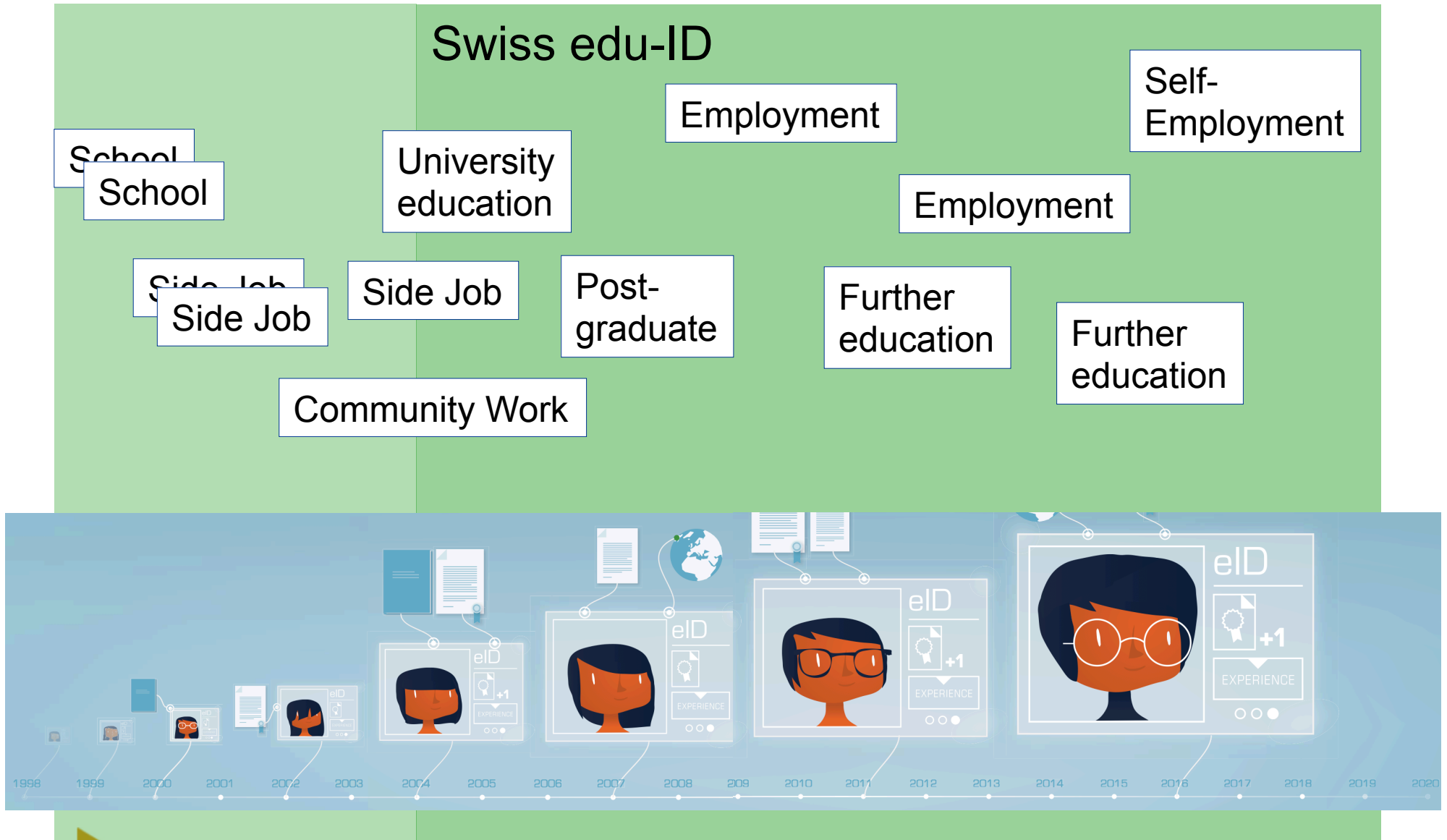# Some open questions (3/3)

Still doable with attributes?

- How to represent different roles in different contexts (affiliations)?
  e.g. affiliation ➜ scopedAffiliation
- How to represent different roles over time?
- How to represent study results?
  e.g. Bachelor@UniX, Master1@UniY, Maste...

Or ...mation differently?

- To..., ...ttributes are strings: some multi-valued, some scoped or a sequence of strings
- Even more complex use cases might come up
- Will we need to go XML or JSON?

Will keep us busy in the years to come

... Identity Management tomorrow

Swiss edu-ID

School

School

Employment

Self-Employment

University education

Employment

Side Job

Side Job

Post-graduate

Further education

Further education

Community Work

Life goes on... So does the Swiss edu-ID

Uni A		Post doc

Uni B	Registration	Graduation

3rd Pty		MBA

edu-ID	Self registration

Trusted
-
Untrusted
Name
Address
Email
Matura
Avatar
History
-

Trusted
Name
Address
Email
Untrusted
Matura
Avatar
History
-

Trusted
Name
Address
Email
Matura
student@B
Untrusted
Avatar
History
-

Trusted
Name
Address
Email
Matura
Master
Untrusted
Avatar
History
student@B

Trusted
Name
Address
Email
Matura
Master
ORCID
postdoc@A
Untrusted
Avatar
History
student@B

Trusted
Name
Address
Email
Matura
Master
ORCID
MBA
Untrusted
Avatar
History
postdoc@A
student@B

© 2014 SWITCH

19