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

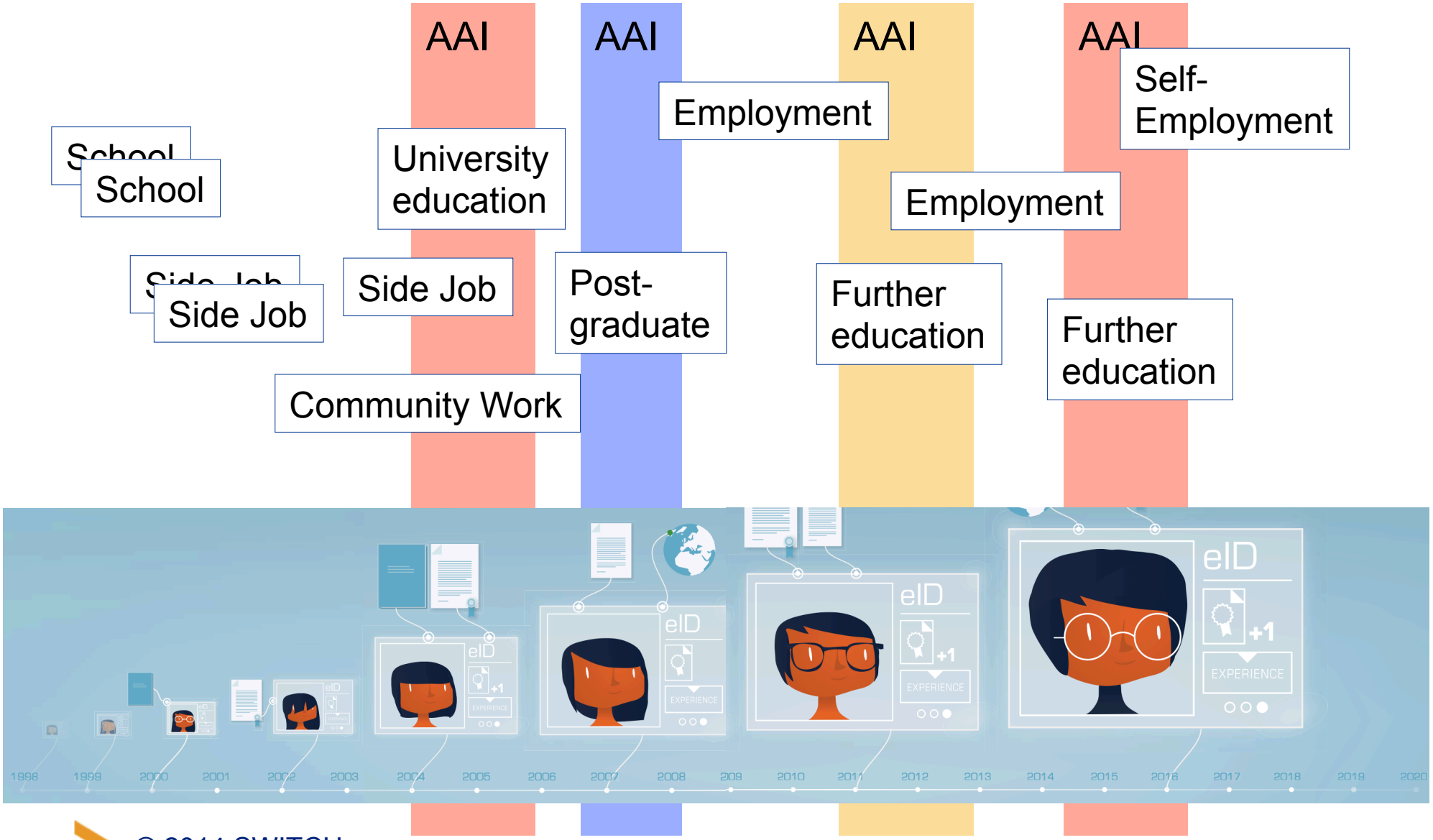
- About the Swiss edu-ID (Christoph Graf)
  - Motivation, use cases
  - Basic concepts
  - Architecture
  - Benefits for users and institutions

  (Short bio-break)

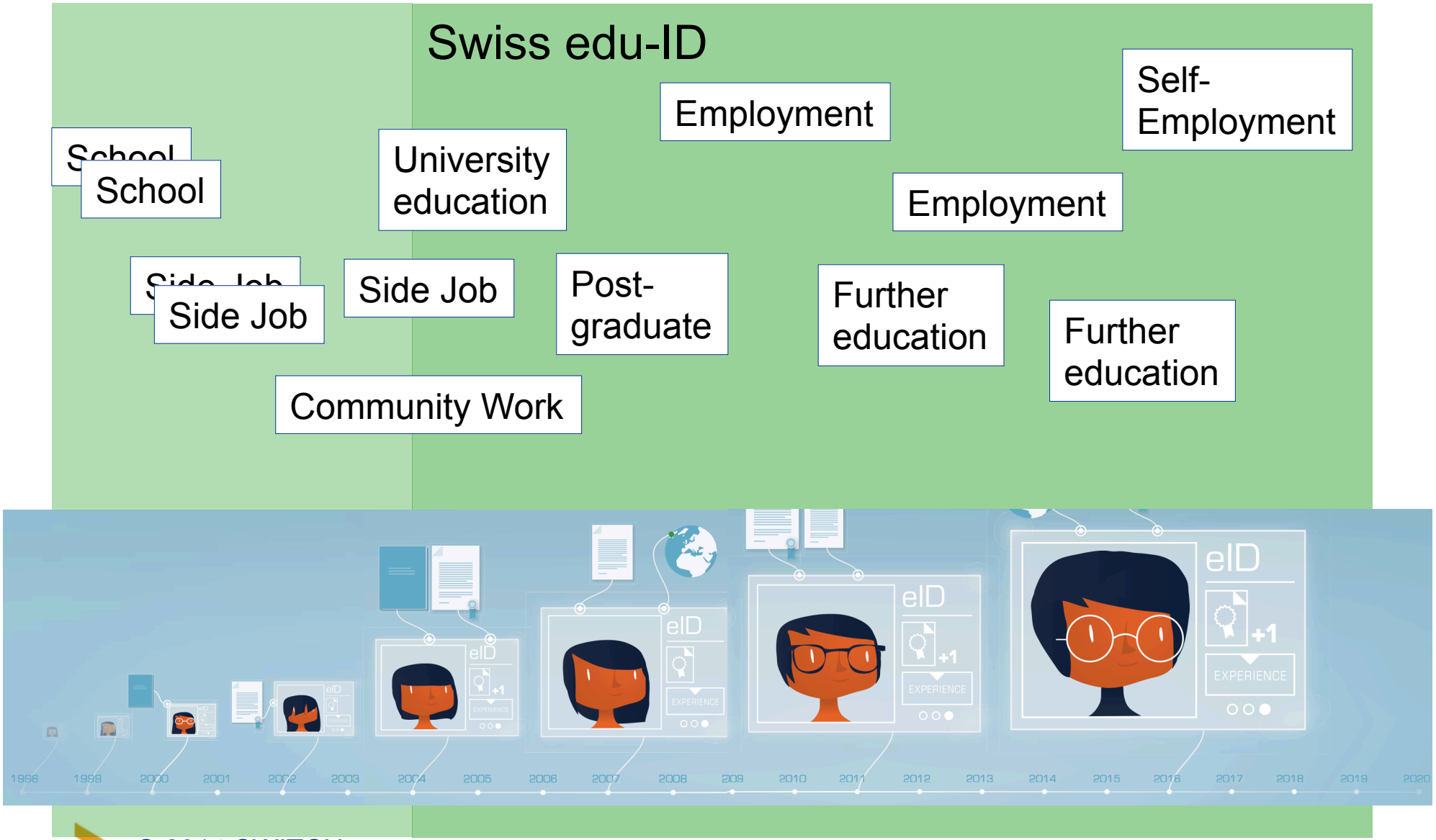
- Roadmap (Rolf Brugger)

- Working Groups (Petra Kauer-Ott)

Identity Management today…



… Identity Management tomorrow



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

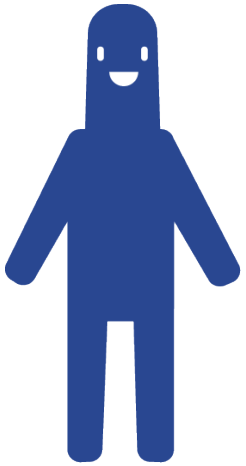
SWITCH started the first two action items before knowing the outcome of the call:

- “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

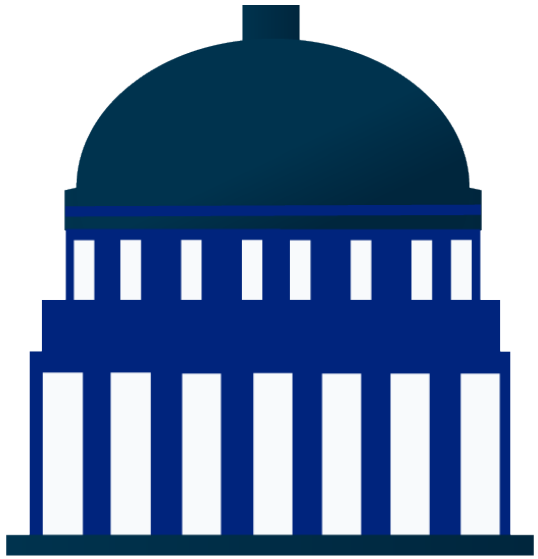
Scoping the Swiss edu-ID

Person Identity



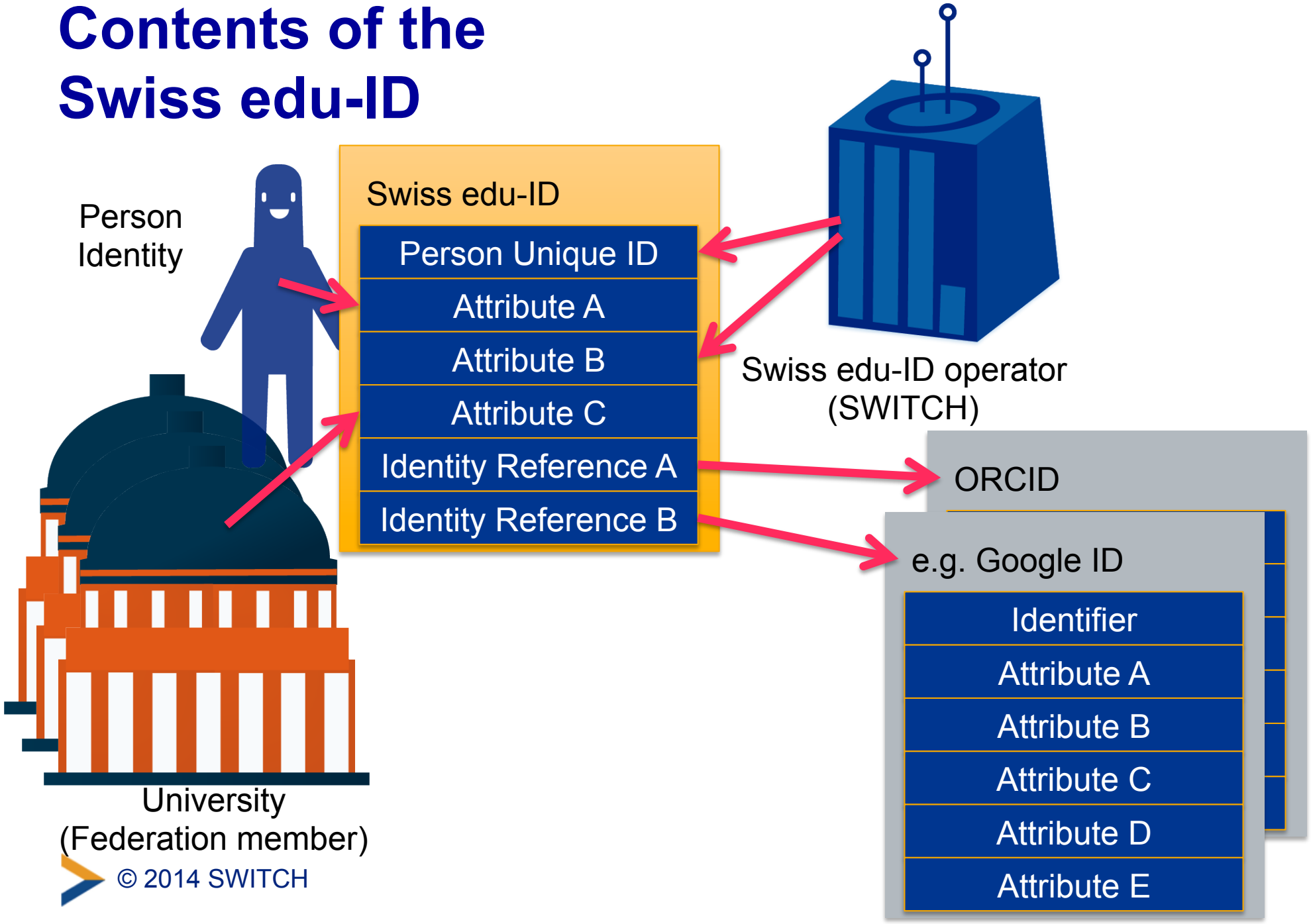
Group Identity

Organisation Identity

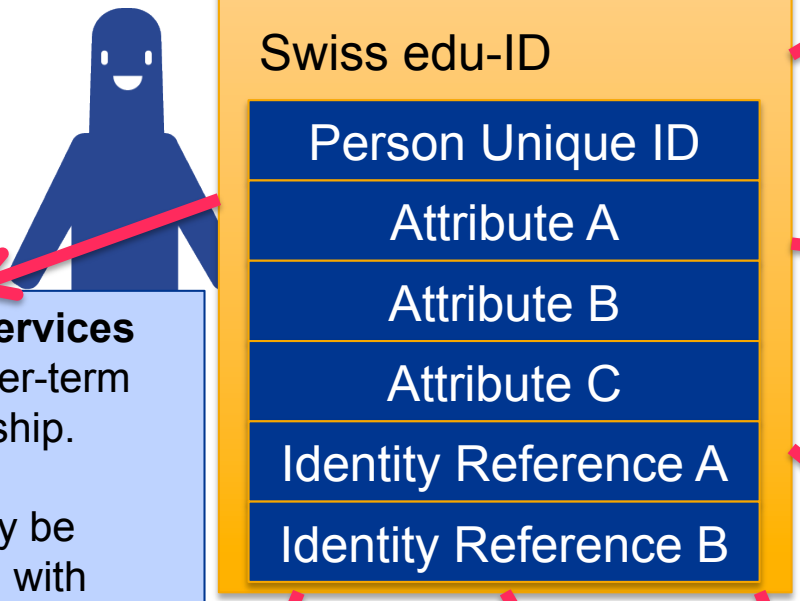


Thing Identity

Contents of the Swiss edu-ID



Use Cases/benefits



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.

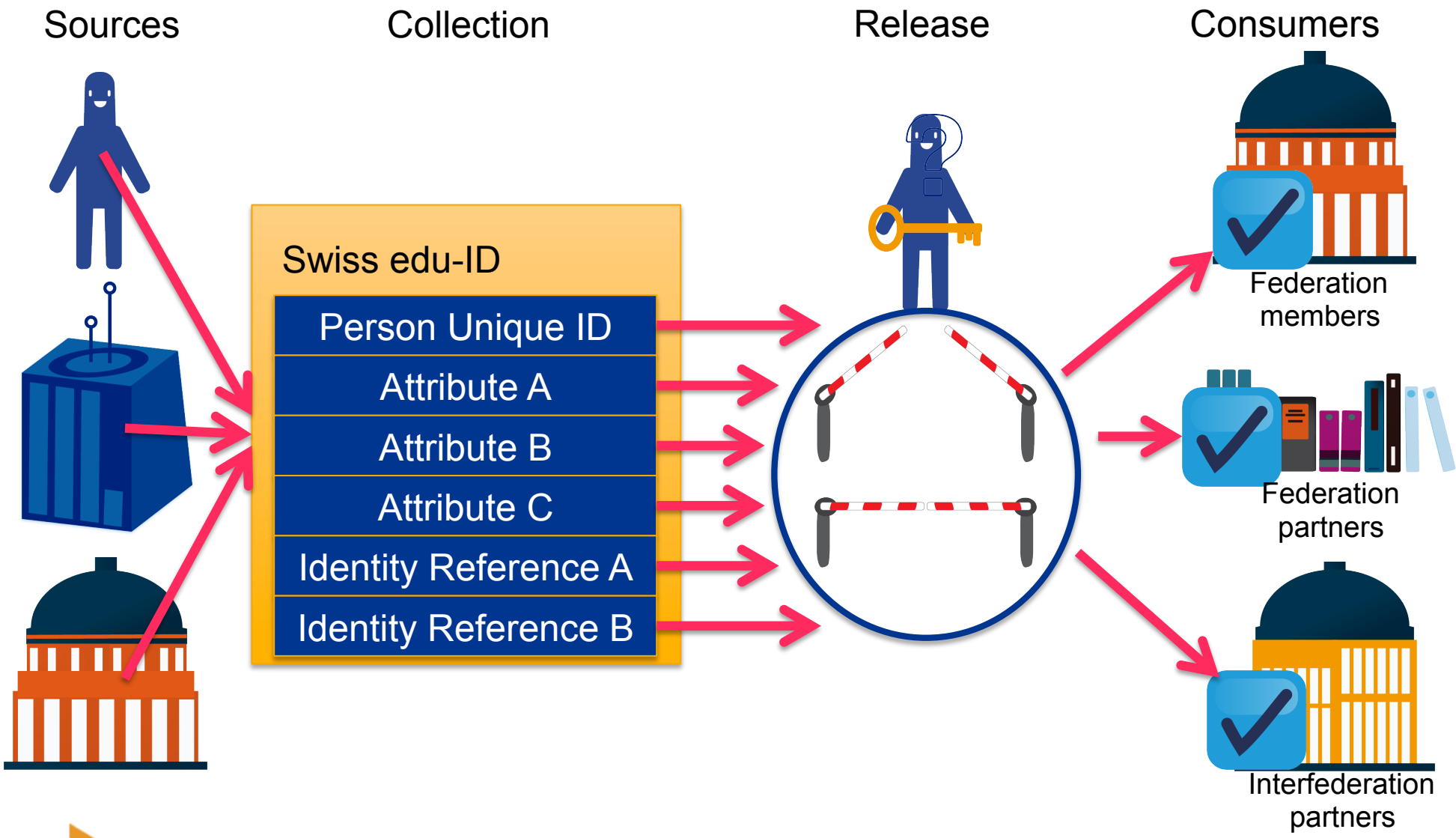
Third party services
Supports longer-term client-relationship. Offerings and conditions may be brought in line with attributes available at given time.

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

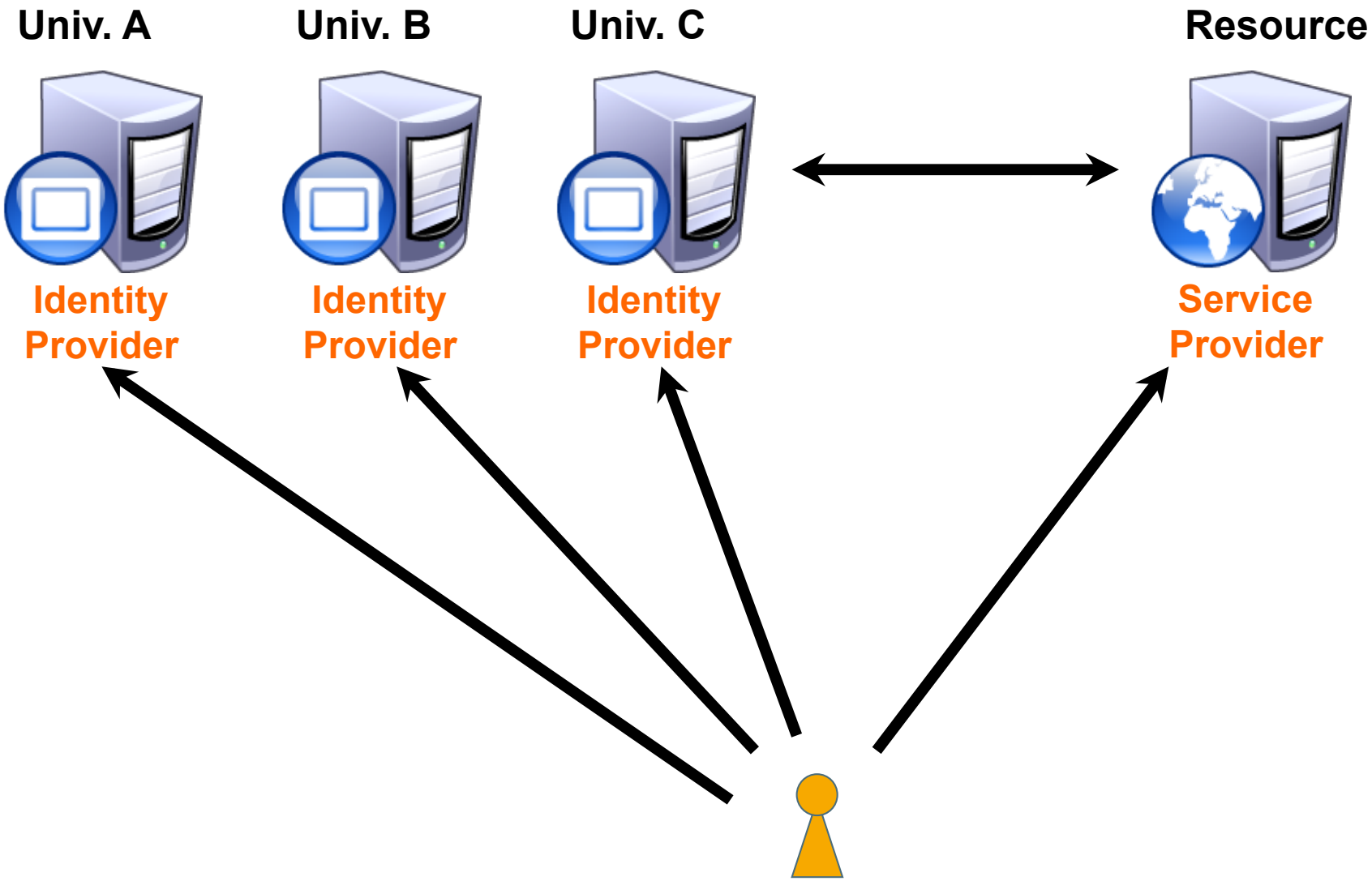
Teachers
One identity for interacting with their learners across universities and to maintain their learning materials

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).

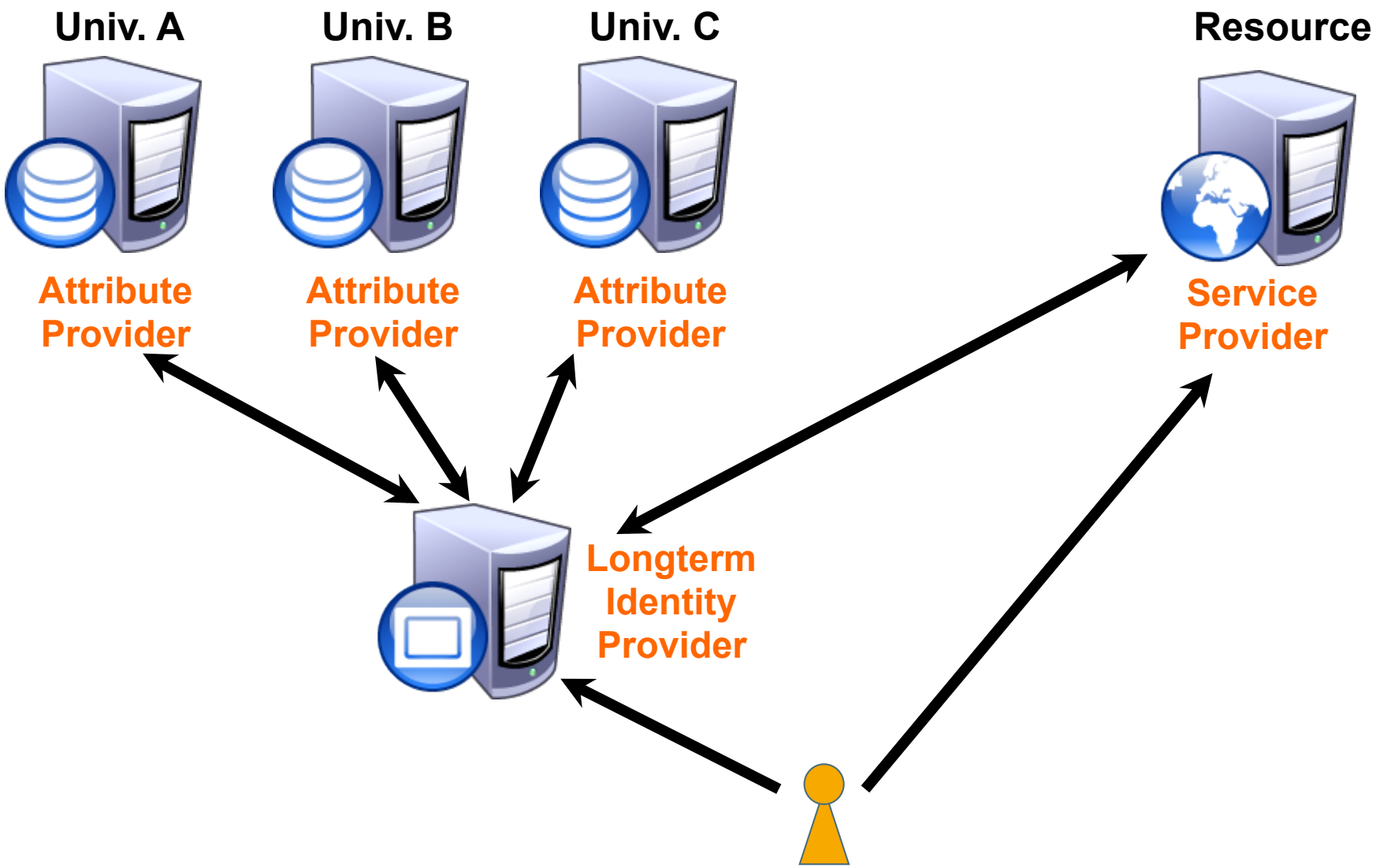
Information flow & control



The AAI architecture …



… vs. the Swiss edu-ID architecture



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?

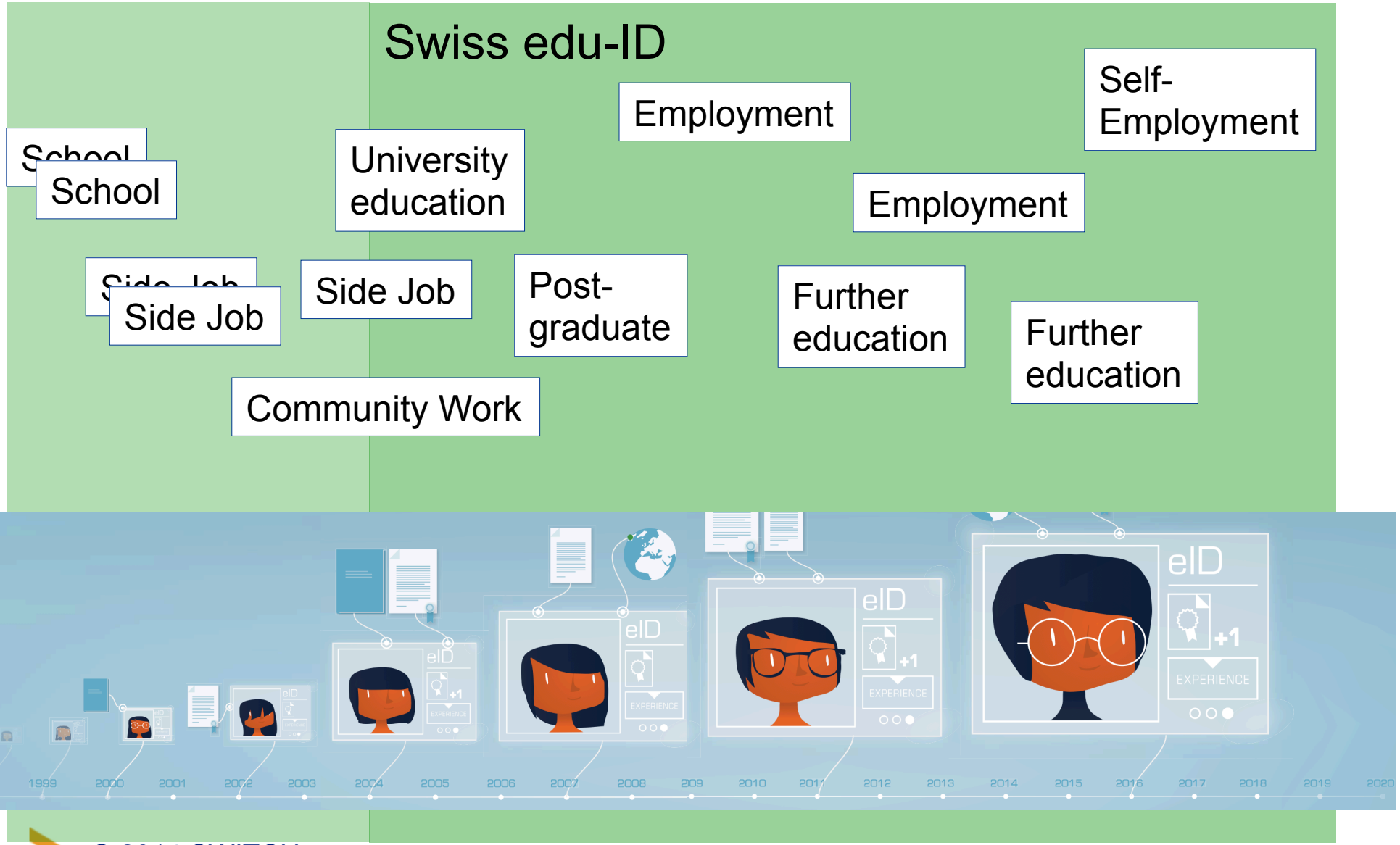
- How to represent different roles in different contexts (affiliations)?
  e.g. affiliation ➔ scopedAffiliation
- How to represent different roles over time?
- How to represent study results?
  e.g. Bachelor@UniX, Master1@UniY, Maste

Or (information differently?

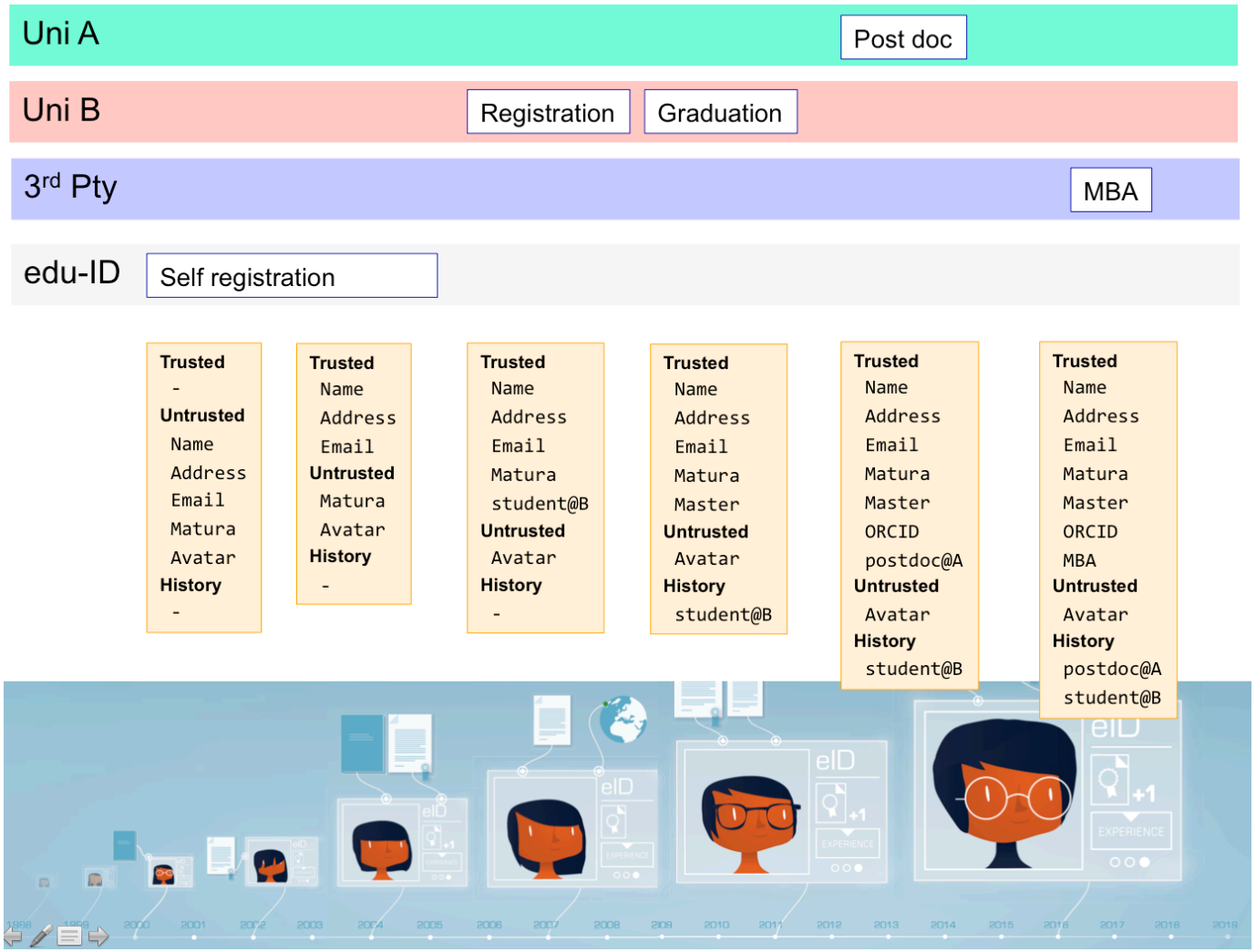
- T attributes are strings: some multi-valued, some scoped or a sequence of strings
- Even more complex use cases might come up
- Will we need to go XML or JSON?

Will keep us busy in the years to come

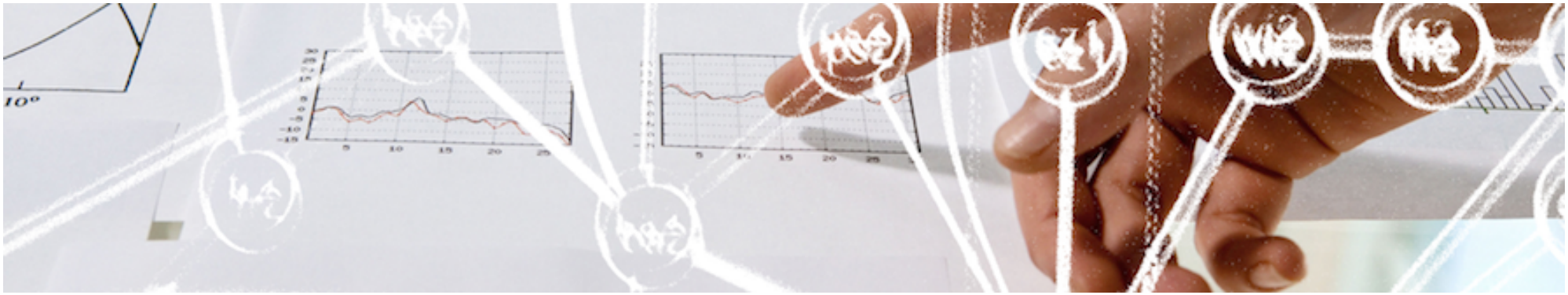
… Identity Management tomorrow



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



Swiss edu-ID Roadmap

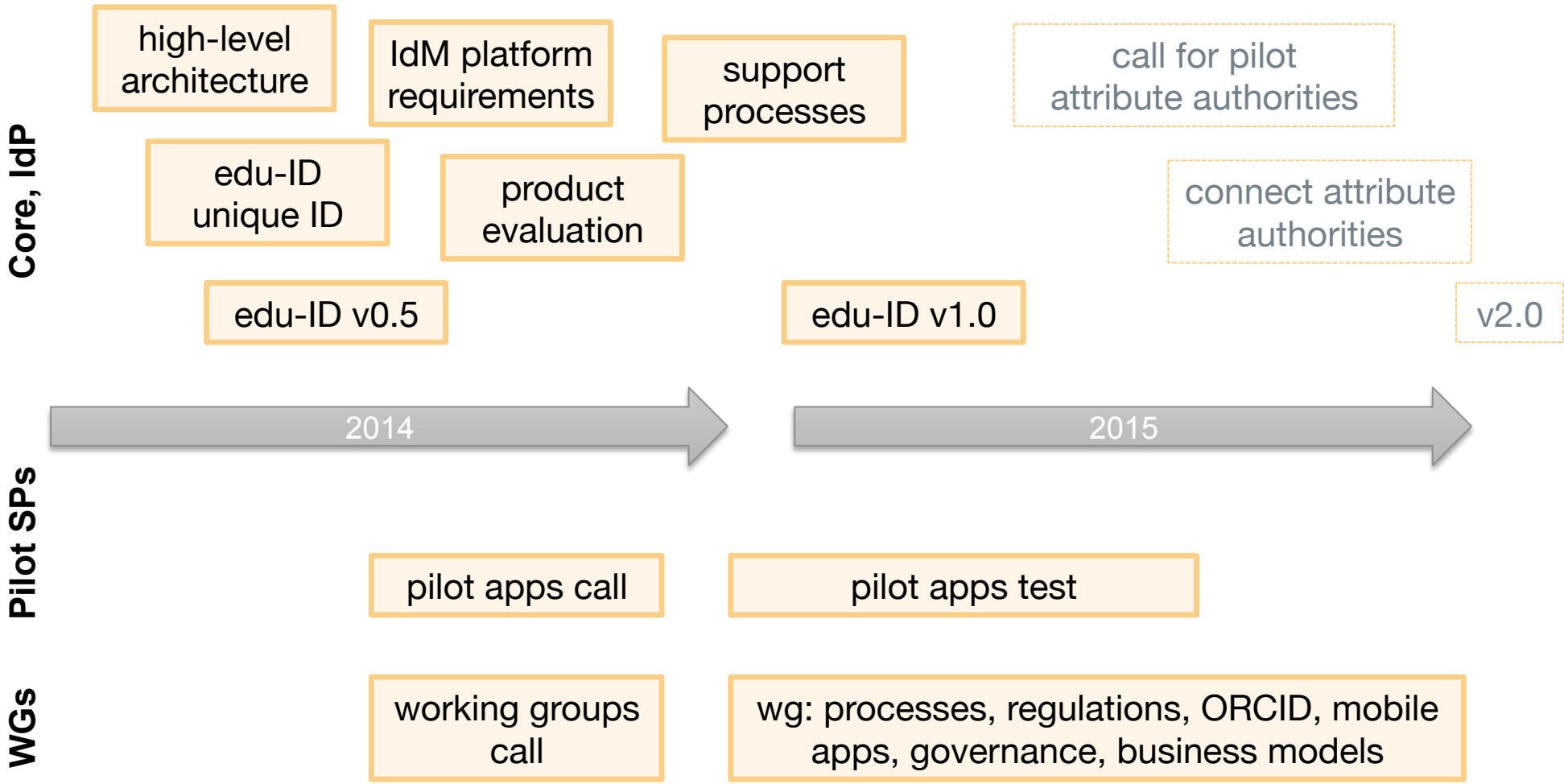


SWITCH

Rolf Brugger
rolf.brugger@switch.ch

Bern, 13.8.2014

Roadmap Overview

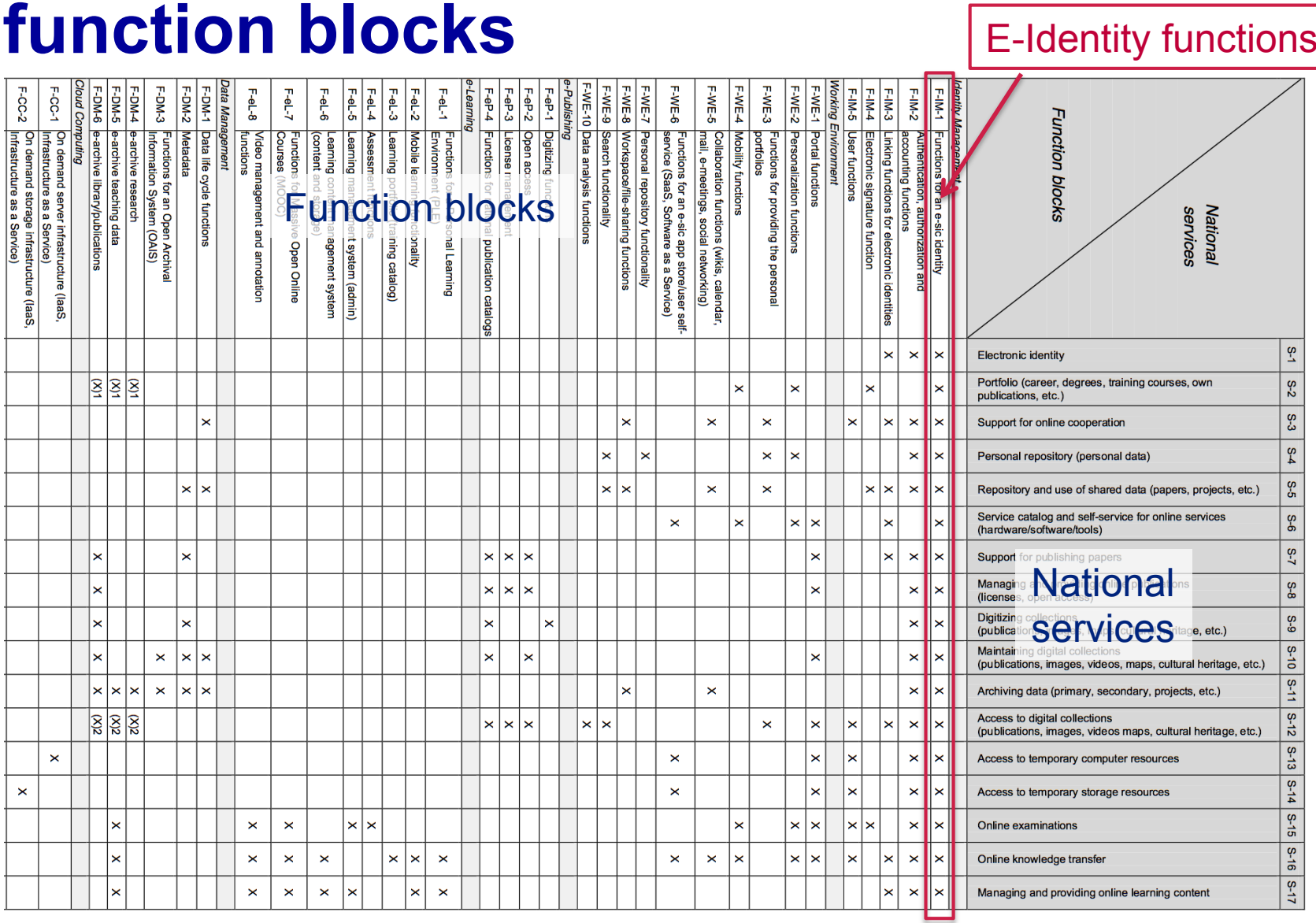


The first small step – version 0.5

- Purpose: provide an early testbed for developers of other SUC projects
- Two new attributes in AAI test federation
  - `swissEduUniqueID`
    Swiss edu-ID unique identifier as life-long identifier for Swiss Higher Education users
  - `eduPersonOrcid`
    ORCID is a persistent digital identifier to link researchers to their professional activites (mainly publications)

User: `eduid-demouser`
Pwd: `demo`
https://attribute-viewer.aai.switch.ch/aai/
(in the AAI Test Federation choose Demo Home Org)

Dependencies of national services and function blocks

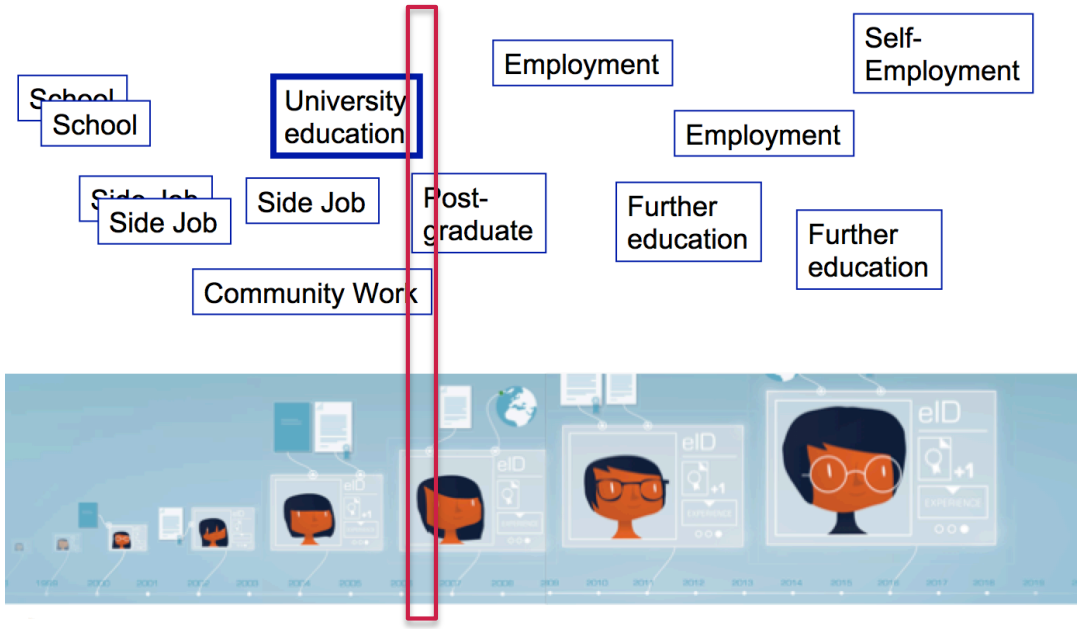


Function blocks / National services		S-1	S-2	S-3	S-4	S-5	S-6	S-7	S-8	S-9	S-10	S-11	S-12	S-13	S-14	S-15	S-16	S-17
		Electronic identity	Portfolio (career, degrees, training courses, own publications, etc.)	Support for online cooperation	Personal repository (personal data)	Repository and use of shared data (papers, projects, etc.)	Service catalog and self-service for online services (hardware/software/tools)	Support for publishing papers	Managing digital collections (licenses, open access)	Digitizing collections (publications, images, videos, maps, cultural heritage, etc.)	Maintaining digital collections (publications, images, videos, maps, cultural heritage, etc.)	Archiving data (primary, secondary, projects, etc.)	Access to digital collections (publications, images, videos maps, cultural heritage, etc.)	Access to temporary computer resources	Access to temporary storage resources	Online examinations	Online knowledge transfer	Managing and providing online learning content
Identity Management																		
F-IM-1	Functions for an e-sic identity	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
F-IM-2	Authentication, authorization and accounting functions	x		x	x	x		x	x	x	x	x	x	x	x	x	x	x
F-IM-3	Linking functions for electronic identities	x		x		x	x	x	x	x	x	x	x				x	x
F-IM-4	Electronic signature function		x			x							x					
F-IM-5	User functions			x									x	x	x	x	x	
Working Environment																		
F-WE-1	Portal functions							x	x		x	x	x	x	x	x	x	x
F-WE-2	Personalization functions		x		x		x		x							x	x	x
F-WE-3	Functions for providing the personal portfolios			x	x	x							x					
F-WE-4	Mobility functions		x				x									x	x	
F-WE-5	Collaboration functions (wikis, calendar, mail, e-meetings, social networking)			x		x						x					x	
F-WE-6	Functions for an e-sic app store/user self-service (SaaS, Software as a Service)						x							x	x			
F-WE-7	Personal repository functionality				x													
F-WE-8	Workspace/file-sharing functions			x		x						x						
F-WE-9	Search functionality				x	x							x					
F-WE-10	Data analysis functions												x					
e-Publishing																		
F-eP-1	Digitizing functions									x								
F-eP-2	Open access							x	x				x					
F-eP-3	License management							x	x				x					
F-eP-4	Functions for digital publication catalogs							x	x	x			x					
e-Learning																		
F-eL-1	Functions for Personal Learning Environment (PLE)										x						x	x
F-eL-2	Mobile learning functionality																x	x
F-eL-3	Learning portfolio (training catalog)																x	
F-eL-4	Assessment functions																	
F-eL-5	Learning management system (admin)											x				x		x
F-eL-6	Learning content management system (content and usage)																x	x
F-eL-7	Functions for Massive Open Online Courses (MOOC)															x	x	x
F-eL-8	Video management and annotation functions										x					x	x	x
Data Management																		
F-DM-1	Data life cycle functions			x							x	x						
F-DM-2	Metadata										x	x						
F-DM-3	Functions for an Open Archival Information System (OAIS)										x	x						
F-DM-4	e-archive research																	(X)2
F-DM-5	e-archive teaching data																	(X)2
F-DM-6	e-archive library/publications																	(X)2
Cloud Computing																		
F-CC-1	On demand server infrastructure (IaaS, Infrastructure as a Service)																	
F-CC-2	On demand storage infrastructure (IaaS, Infrastructure as a Service)																	

Swiss edu-ID version 1.0

With v1.0 we want to be able to

- Register Students approaching the end of their studies
- Give them continuing access to selected resources

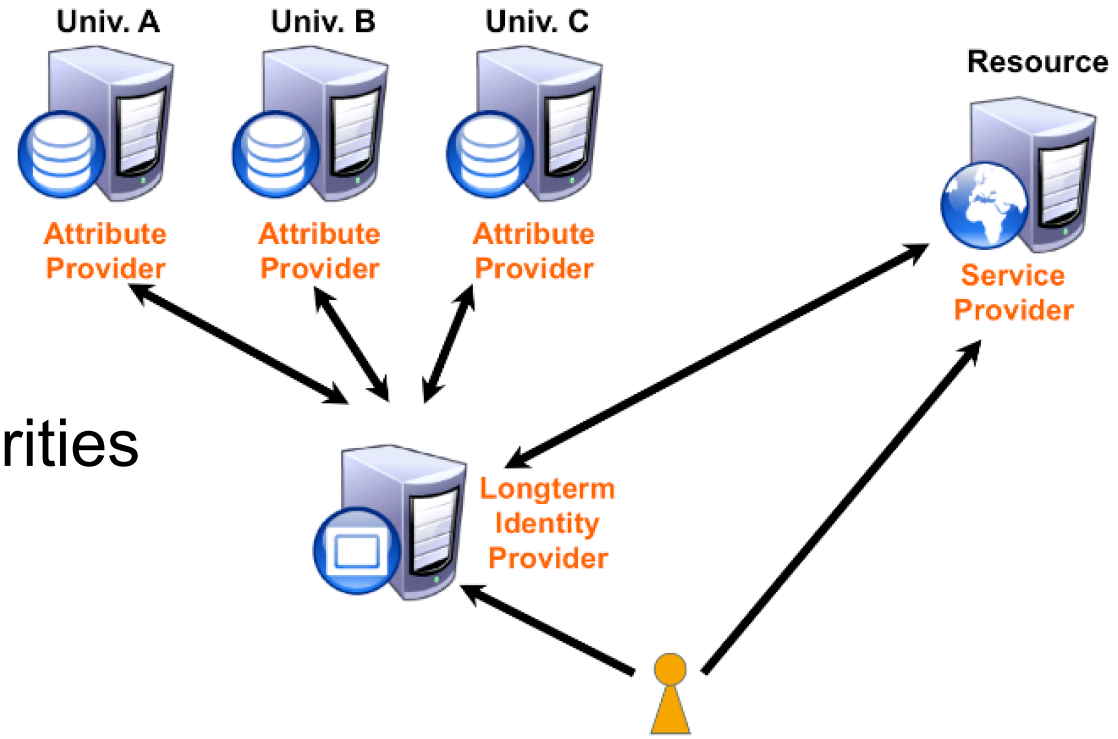


v1.0 Requirements

- Set up an identity management platform with
  - Sign-up processes
  - Account recovery processes
  - Attribute validation processes
  - Processes to link AAI-based identities to the Swiss edu-ID
  - Processes to link external identities such as the ORCID

- Functional requirements
  - AAI compatibility
  - Suitable for non-web resources
  - Openness towards other interfaces:
    OAuth2, OpenID Connect, Suisse ID, STORK, …

Version 2.0



Main feature:

- Connect attribute authorities

Preparation:

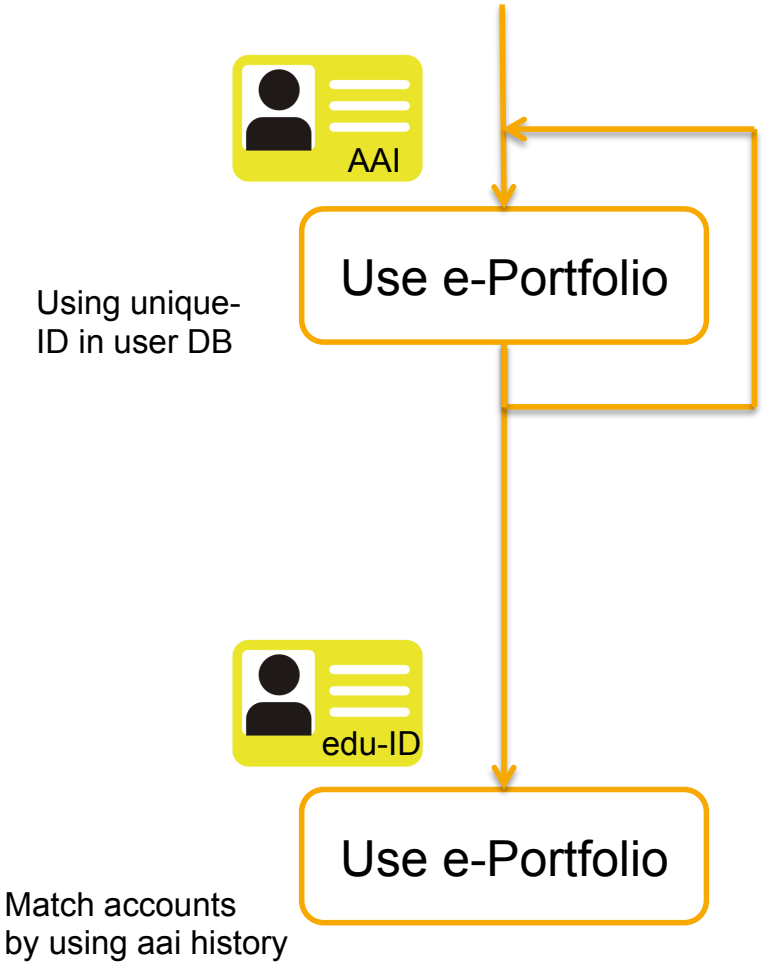
- working groups
  - Processes
  - Legal issues
- Attribute aggregation on IdM platform

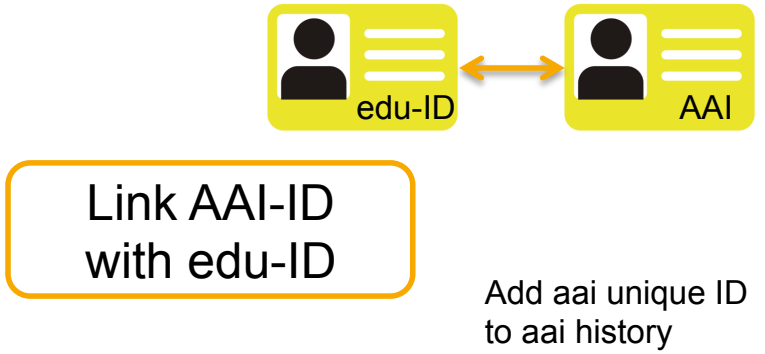
Enabling services for v1.0

- Early candidates to support Swiss edu-ID
  - Attractive for students who are about to leave the university
  - ➜ SWITCHportfolio
  - ➜ SWITCHdrive

- Usability: Coexistence of AAI and Swiss edu-ID should not confuse Users

Pilot: SWITCHportfolio





- Students have to establish the ID-link as long as the AAI-ID is active

Pilot: SWITCHdrive

Currently

- A “Cloud-ID” is created, protected by AAI
- Use Cloud-ID password to access:
  - Web Client
  - Mobile Client
  - WebDAV service
- LDAP authentication

With edu-ID

- Optimal approach: full integration with edu-ID
  - Web Client (SAML, Shibboleth)
  - Mobile Client (OpenID Connect/OAuth2)
  - WebDAV service (?)

Call for pilot projects

Wanted: more services to be enabled for Swiss edu-ID.

Examples:

- Common web service, preferably of a library
- Non-web resource
- Application for mobile devices
- Resource using ORCID
- Resource using a community-ID or social service
- Resource interfacing/using existing ID-frameworks (STORK, SuisseID, Mobile ID, Swiss passport)

Deadline for project submission at CRUS: Feb 15th 2015

Working Groups

Swiss edu-ID – a joint effort

SWITCH

Petra Kauer-Ott
petra.kauer@switch.ch

Berne, August 13 2014

Goals

Record the community's needs as to

- user-centrism
- specific IdM processes
- interoperability
- implementation of Swiss edu-ID

and transfer them to exemplary applications:

Pilots

Later we will look also for Pilot Attribute Authorities !

Pre-Project Work

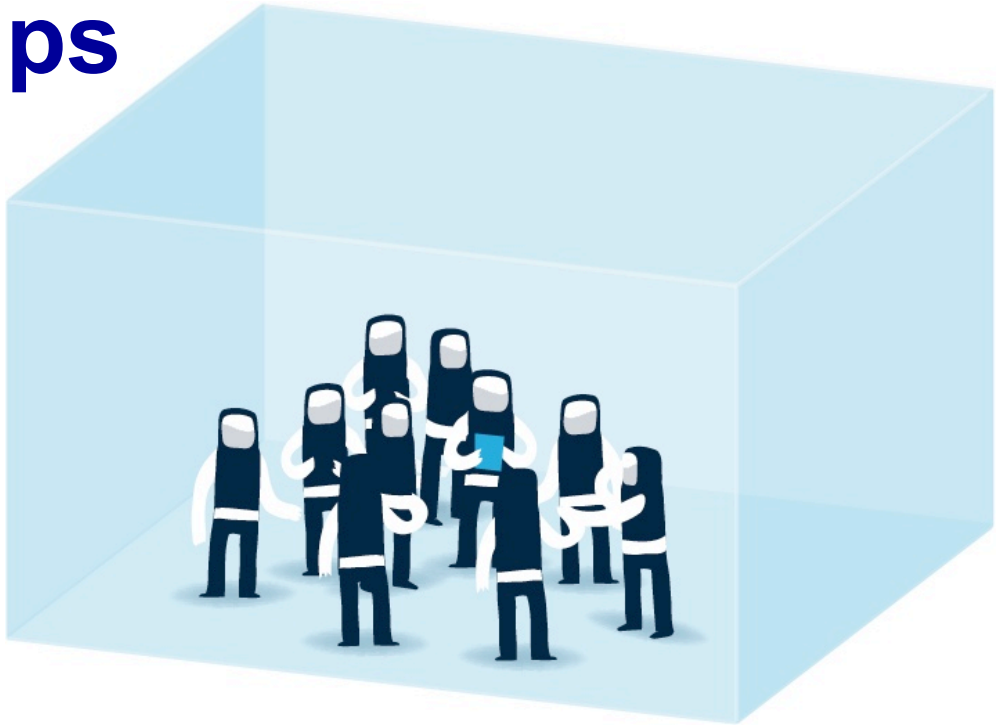
3 groups already active:

- **High Level Architecture WG**:
  ETHZ, ETH Library, UNIBAS, UNIGE, UNIL, UNISG, USI, UZH, SWITCH

- **AAI Attribute Task Force**:
  Discussion about eduPerson, swissEduLibraryPerson, ORCID, Swiss edu-ID/Identifier

- **Identifier Specification WG**:
  BFH, ETH library, SWITCH

Call Working Groups



A. Processes

B. Regulations

C. ORCID

D. Mobile App Support

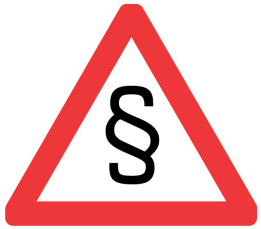
E. Governance Model

F. Business Model

A. Processes WG

Work	**Profile of participants**
Remarks	**Workload and timeframe**

B. Regulations WG



Legal framework • identify regulations and discuss/clarify relevant questions within institutions • define policies institutions need • bring in institutional experiences with end user policies	**Member Profile:** • legal know-how • overview of regulations, policies and IdM-related processes within institution • contacts with legal representatives • work at cutting point between technical and administrative tasks
Group will be accompanied by legal experts	2 days, Nov. – May 2 meetings, document review, feedback

C. ORCID WG

ORCID integration • describe current and possible future use of ORCID • describe processes for integration at institutions & possibilities of ORCID provisioning for institutional processes	**Member Profile:** • institutions considering implementation of ORCID • involved in development of systems and services with relation to ORCID • librarians • managers and developers of publication systems
→ further project steps → **pilots (call 15.2.2015)**	1-2 days, Oct. – Jan. Meetings, ev. visits, feedback

D. Mobile App Support WG

Better mobile support • describe requirements of institutions/users • discuss ideas for better mobile support • evaluate existing solutions	**Member Profile:** • experience with integration of mobile solutions • mobile developers and integrators with knowledge about protocols as OAuth2 • IdM and application managers • researchers (in the field of mobile technologies)
→ further project steps → **pilots (call 15.2.2015)**	1-2 days, Oct. – Jan. 2 meetings, feedback

E. Governance Model WG

Governance documents • act out cases to check usability and robustness of governance model • identify points to be adapted/improved • discuss issues with legal representatives at institution	**Member Profile:** • knowledge of governance models • familiar with SWITCH governance and governance of AAI
→ some important changes of roles (IdP, AA, user)	1 day, Q1 2015 1-2 meetings in person

F. Business Model WG

Business models • discuss and evaluate different model options	**Member Profile:** • good knowledge of business models • background knowledge about SWITCH and tariff
→ medium- & long-term perspectives	Ca. ½ day, Q2 2015 1 meeting in person

Participate !

Please distribute the call within your institution!

Use the **feedback form** for comments, working group subscriptions and pilot suggestions.

Details about call:
http://swit.ch/eduid_workgroups

Contact:
swisseduid@switch.ch

Outlook

- Project Updates at info events of SUK P-2:
  - Sept. 11, 2014 in Lausanne
  - Sept. 25, 2014 in Bern

- October/November : first working group meetings
- February 15 2015 next call SUK P-2

Call: Swiss edu-ID - the next generation Identity Management for Swiss HEI's

Would you like to play a part in the next phase of AAI's evolution towards a user-centric identity management solution?
We are looking for members of universities, libraries and research institutions to help us create a new digital identity known as the Swiss edu-ID.

Contribute to one of the working groups with your expertise and practical know-how (details: http://swit.ch/eduid_workgroups):

- Processes
- Regulations
- ORCID
- Mobile App Support
- Governance Model
- Business Model

Please contact us and let us know for what working group with an open call you would volunteer: swisseduid@switch.ch

Swiss edu-ID

The next-generation Swiss Educational Identity Management

Consider future needs & expectations
Technological change increasingly impacts the behaviour and working environments of students, researchers, life-long learners and university staff. While in the past the individuals' working environment was mostly preset and specified by the organization they were affiliated with, we can now observe a trend towards more self-reliant personalities. They tend to choose their individual set of tools and they autonomously develop their skills to manage and protect personal data. In addition to the classical desktop working mode, ubiquitous mobile access to personal and professional data is preferred.

Substantially extend AAI towards a user-centric IdM
To address these trends SWITCH is suggesting a substantial extension of the existing AAI infrastructure. Identity management, which controls access to tools and data is to become more user-centric and less organization-centric.

Provide a long-living identity
From the perspective of an individual the digital identity is stabilized and sustained. With the first contact of an individual with a higher education institution the individual is assigned a permanent Swiss edu-ID. The barriers for an individual to create a Swiss edu-ID are low. After leaving a university, the Swiss edu-ID will no longer carry role information from that university, but otherwise remain active. The individual can still update personal information on an on-going basis, and will still get access to resources not requiring such role information. Re-entering a university for further education purposes as well as cross-organisational activities are simplified.

Streamline institutional Identity Management
From the perspective of an organization, identity management is streamlined. New identities do not have to be constructed from scratch, but can be initialized based on existing profile information from an individual's Swiss edu-ID. While AAI is based on a widely decentralized architecture, the Swiss edu-ID is substantially relying on centrally provided services run by SWITCH to operate elements like storage of long-term core attributes, authentication service and interfaces to resources and attribute authorities. Providing high quality attribute information about individuals will remain in the authority of participating organisations, e.g. the universities, as is the case today in AAI.

Embed new Identity Provider & support identity linking
The central platform of the Swiss edu-ID will become an Identity Provider in the AAI framework and thus maintain full interoperability including interfederation.
The Swiss edu-ID will allow linking of relevant external identifiers like ORCID. Linking with social media identities will further improve interoperability with popular 3rd party communication and collaboration services.

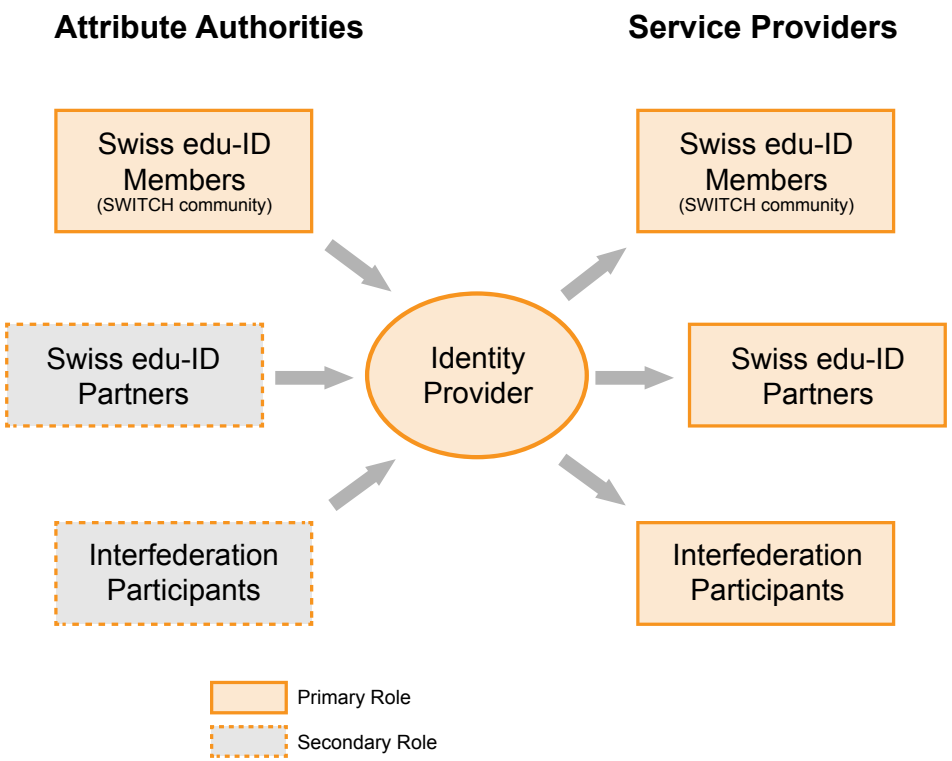
The Swiss edu-ID will actively seek interoperability with relevant e-Government standards and services nationally, e.g. SuisseID, and internationally, e.g. eID/STORK.

	SWITCHaai	Swiss edu-ID
Identity Provider	Run by each university individually for their current users	One central instance run by SWITCH
Attribute Authority	Run by each university individually for their current users (as part of the IdP)	Run by each university individually for their current and former users
Service Providers	SWITCH Community, Swiss edu-ID partners, interfederation participants	SWITCH Community, Swiss edu-ID partners, interfederation participants

Swiss edu-ID compared to SWITCHaai

Initial version functional in 2015

An initial version V1.0 of the Swiss edu-ID service with limited capabilities will be operable starting 2015. It will allow individuals to create a long-lived Swiss edu-ID identity. Focus is on students who are soon going to lose their existing SWITCHaai account and on individuals without a strong affiliation with an organisation in the SWITCH Community and therefore without possibility to get a SWITCHaai account.



Swiss edu-ID stakeholders and flow of attributes

Assure high quality & extension possibilities

The Swiss edu-ID is built to match the requirements of the SWITCH Community. This means that high security and data protection standards are adopted to gain trust and acceptance. This also means that 3rd party organizations can participate in Swiss edu-ID provided that the SWITCH Community requires it. The proven governance and financing models of the SWITCH Community will be fully applied to Swiss edu-ID.

Take the next steps

Stakeholder groups will refine the operational framework of the Swiss edu-ID on the basis of the high-level architecture from mid-2014 to mid-2015 and set the cornerstone of the next version 2.0 of the Swiss edu-ID and beyond. Version 2.0 will allow participating organisations to enrich the user attributes and thus make the Swiss edu-ID cover all functionality of SWITCHaai identities with additional longevity.

The main focus in the years 2017 onwards is to increase service adoption. This will also include implementing renewed student registration processes together with all relevant stakeholders.

The program P-2 covers two substantial activities of the “Swiss edu-ID“ project, i.e. the set-up of the initial service version and the refinement of the operational framework in collaboration with the stakeholder groups. Follow-up projects (preferably within the scope of P-2) will be initiated to implement the subsequent steps in this roadmap.

Call: Participate in working groups & pilots

Interested people are welcome to participate in one of the initiated working groups (please find details at http://swit.ch/eduid_workgroups):

Processes: IdM related processes, issuing, interfaces

Regulations: existing regulations & policies, needs, user policies

ORCID: possible use, integration processes

Mobile App Support: requirements, improved support, evaluation

Governance Model, Business Model

The integration possibilities will be tested and demonstrated with some pilots. Test candidates should be **web and non-web applications** (e.g. based on OAuth2 or Open ID connect), **mobile applications**, **applications using ORCID, other IDs & ID frameworks** (e.g. community IDs, SuisseID, Mobile ID, STORK).

Contact / News / Registration for working groups: swisseduid@switch.ch

Events: Sept. 11 at UNIL and Sept. 25 2014 at UniBE: CUS P-2 Project Update

This flyer is mainly an extract of the “Swiss edu-ID High Level Architecture” document:
http://swit.ch/eduid/SwissEduIDArchitecture.pdf