

The Swiss edu-ID in a Nutshell

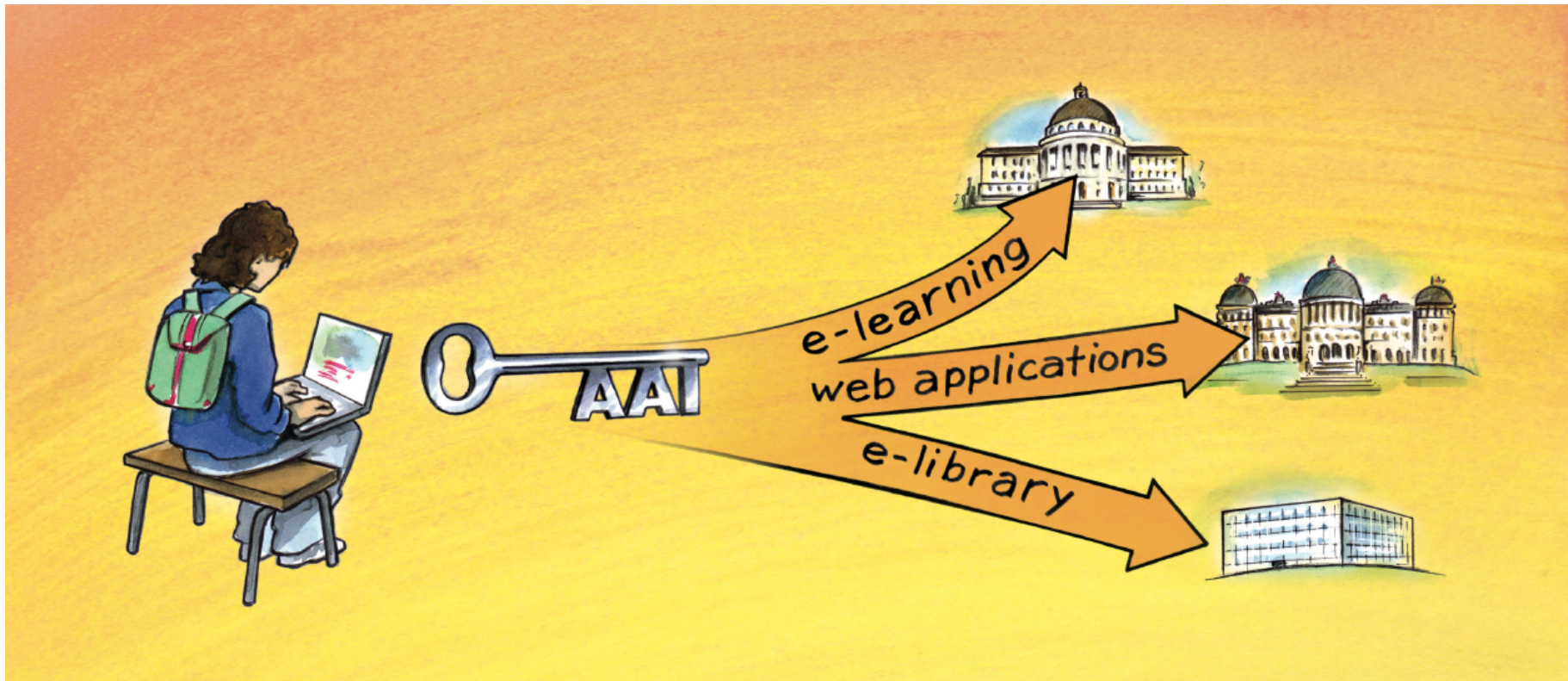


SWITCH

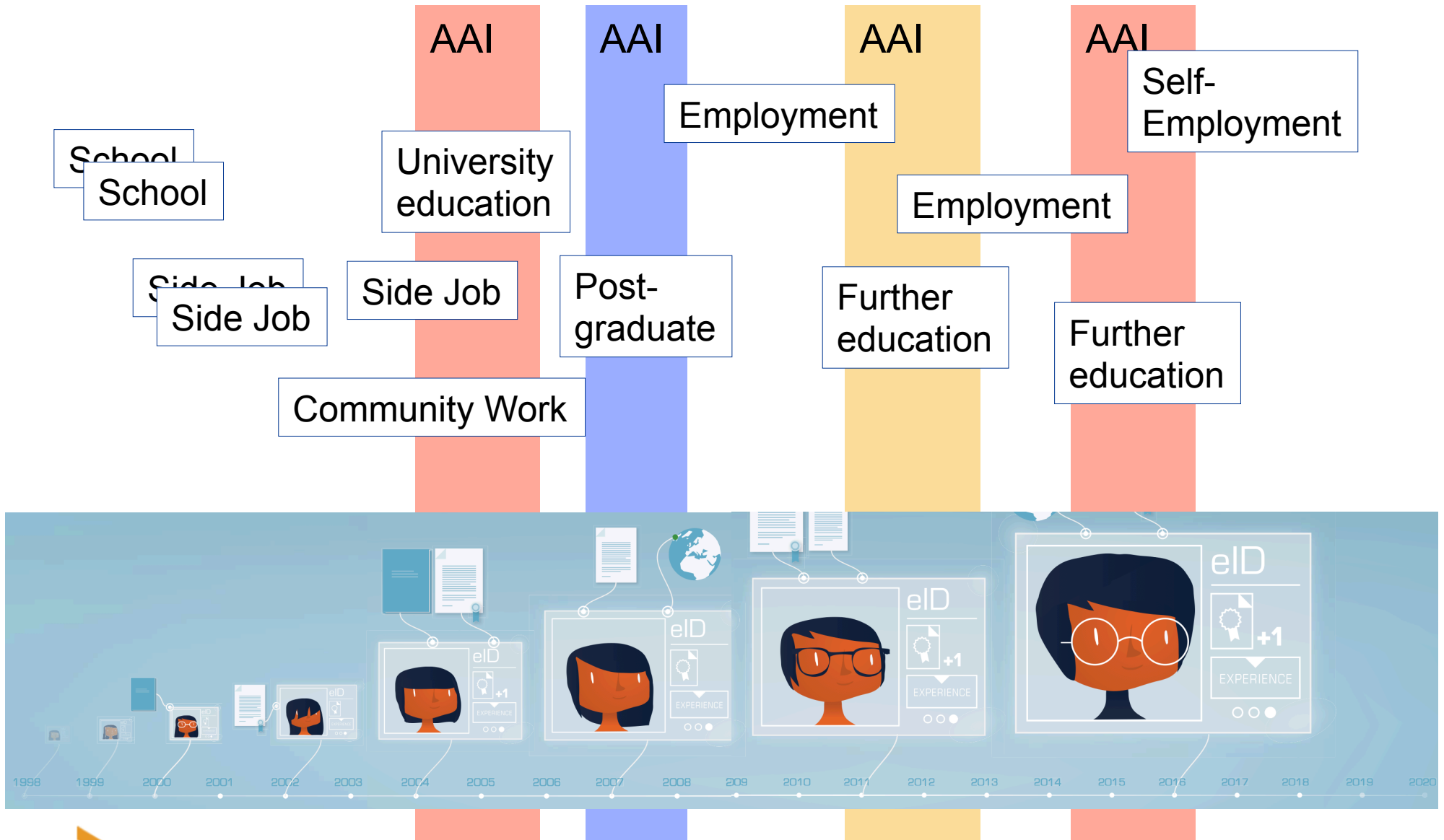
Swiss edu-ID
swisseduid@switch.ch

The success of SWITCHaai

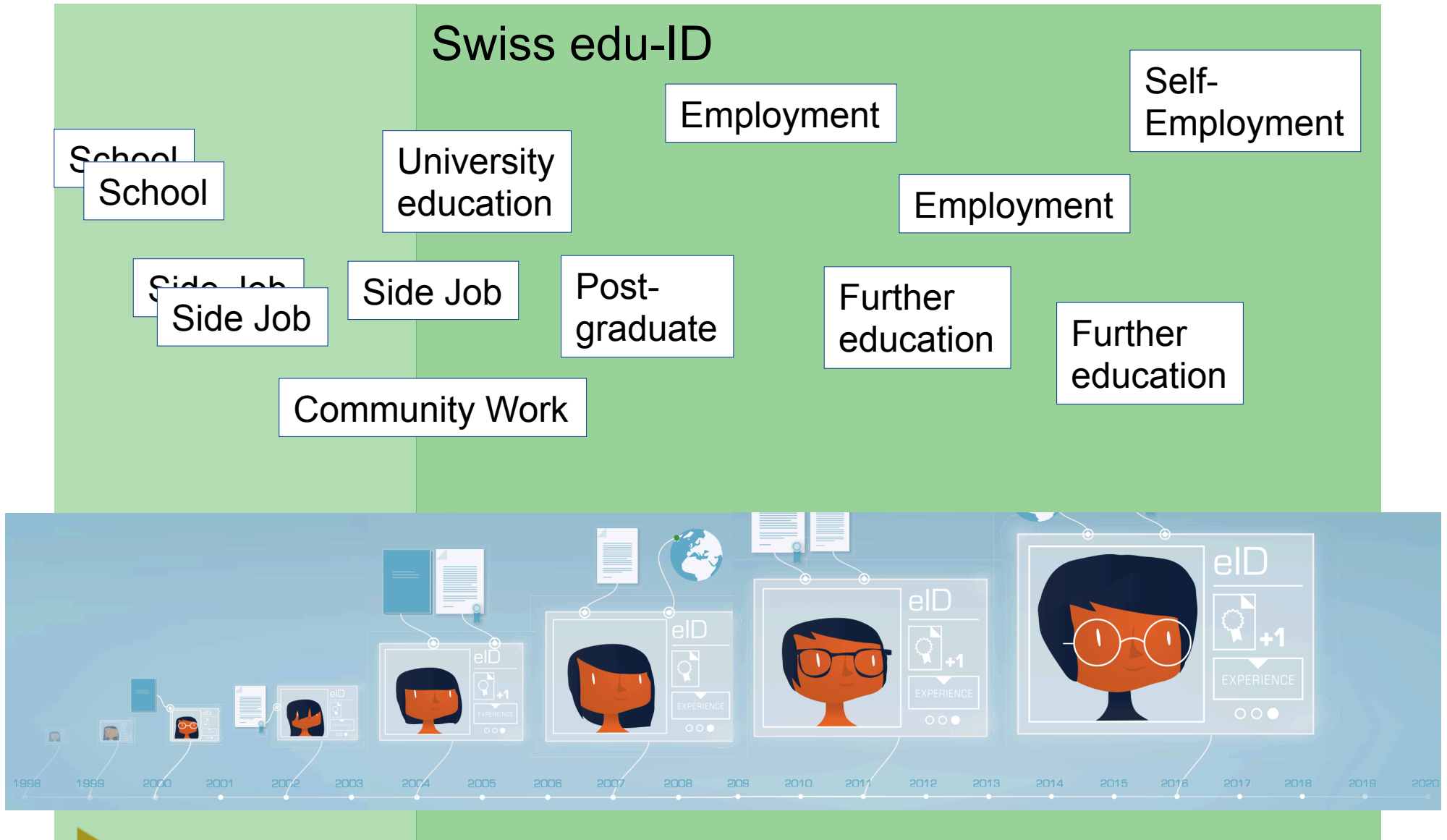
Enter higher education, get one key, access many resources



But what happens over time?



Doesn't this look much nicer?



The (overloaded) term “Swiss edu-ID”

- The concept “Swiss edu-ID”
 - In preparation for the CUS P-2 programme a “substrategy identity management” was written by an inter-university working group.
 - This paper proposed the concept of the “Swiss edu-ID” and a high-level roadmap for its implementation
- The project “Swiss edu-ID”
 - SWITCH initiated the CUS P-2 projects “Swiss edu-ID” and “Swiss edu-ID phase II” to implement the roadmap of the substrategy
- The service “Swiss edu-ID”
 - The services “Swiss edu-ID V1.0” and “Swiss edu-ID V2.0” are milestones on that roadmap

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

SWITCHaai vs. Swiss edu-ID

	SWITCHaai	Swiss edu-ID
Identity framework	Role-linked, organisation-centred federated identity	Persistent, user-centric federated identity
Identity lifetime	Limited to period of organisational affiliation	Persistent identity
Number of identities per individual	One identity for each organisational affiliation of an individual	One unique identity per individual
Role of organisations	Identity provider & Service provider	Attribute authority & Service provider
Users	Members of Swiss academia	Members of Swiss academia and people with relation to academic institutions

The Swiss edu-ID project roadmap

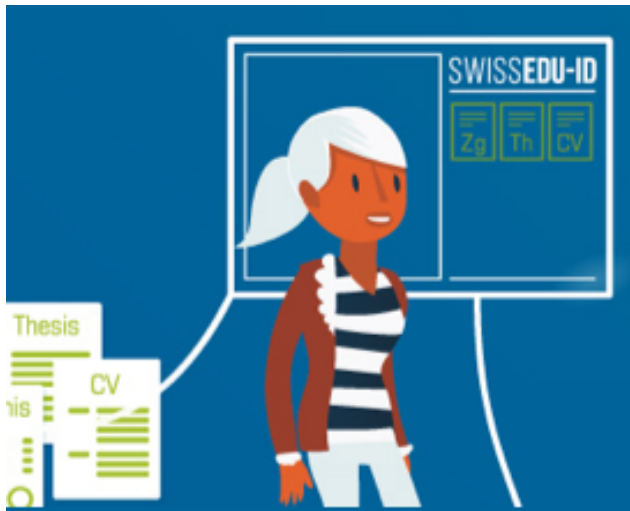
- Project “Swiss edu-ID” (finished July ’15)
 - Submitted by SWITCH to CUS P-2 competition in March ’14, approved and started mid-2014
 - Main goal: Implementing the “Swiss edu-ID V1.0” service
- Project “Swiss edu-ID phase II” (started Aug ’15)
 - Submitted by SWITCH to CUS P-2 competition in Feb ’15, approved in June ’15 and started Aug ’15, runtime until end 2016
 - Main goal: Implementing the “Swiss edu-ID V2.0” service
- Swiss edu-ID 2017-2020
 - Envisaged follow-up collaboration project
 - Main goal: migrate from SWITCHaai to Swiss edu-ID

“Swiss edu-ID” project: main deliverables

- Pilot service Swiss edu-ID V1.0 -> *Lukas Hämmerle*
- Pilot projects/Use Cases -> *Rolf Brugger*
- Community Anchoring -> *Petra Kauer-Ott*
- Market overview: solution framework for Swiss edu-ID
 - Shibboleth (main open source SW-component of SWITCHai and Swiss edu-ID V1.0) and commercial products are fit for the purpose
 - Successfully tested one of the commercial products in a PoC
 - Main weakness of Shibboleth is its lack of a solid roadmap for supporting mobile and non-web use cases
 - We stay with Shibboleth for Swiss edu-ID V2.0
 - To be revisited once mobile and non-web use cases gain ground
- Support for mobile environment/non-web -> *Rolf Brugger*

Swiss edu-ID Version 1.0

What's there already? What is coming?



SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Bern, 13. August 2015

Outline

- **Swiss edu-ID Identifier**
- **Swiss edu-ID Service**
 - What is there already?
 - What is the edu-ID identity?
 - How changing identity?
 - What will be added?

edu-ID Identifier

- **Example:** 6c17b073-3e37-4c4a-83c8-be85ee353d23
- **Main goals:** Link personal data over long time across services and institutional borders.
- **Issuance:** Swiss edu-ID service (currently)
- **Format:** UUID Version 4
- **Usage:** Note released (currently) to AAI services
- **Test range:** All values of format "0000[-a-f0-9]{32}"
- **Specification:** <http://swit.ch/edu-ID-Identifier>

No need to remember/enter your Swiss edu-ID!

edu-ID Service

Consists of:

- Registration/(self-)management web interface
- Shibboleth Identity Provider
Registered like any IdP in SWITCHaai


Allows you to:

- Create and manage your edu-ID account
 - Change/add/link data
- Log in to AAI services



edu-ID Identity

- How does it look like and what can you add/change/link?


Access your Swiss edu-ID Account



[View and Modify Account](#) | [About](#) | [Help](#) | [Terms of Use](#)

▶▶▶▶  Authentication  Account Data





This page allows you to update and extend your Swiss edu-ID account.

Account Completeness
Your Swiss edu-ID account is 100% complete: 
Check what information at maximum is released about you by [accessing the AAI Attribute Viewer](#).

[Proceed to Resource Login](#)

Attribute Quality and History

Quality of each attribute is:

-  Provided by user
-  Provided by (linked) AAI identity
-  Verified (currently e-Mail and mobile phone number)
-  Generated

All revisions (and timestamp) of identity are stored.

Changing Attributes

New value

Business Address

Name Lukas Hämmerle

Company

Additional Address Information

Street and House Number

ZIP and City

Country

Example

Beispiel AG
Musterstrasse 4
CH-1234 Example
Switzerland

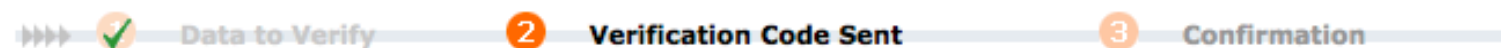
⚠ Changing this verified value lowers the overall quality of your Swiss edu-ID account. Therefore, this generally is not recommended.

Verifying Identity Data

Verify Attribute Additional E-mail



[View and Modify Account](#) | [About](#) | [Help](#) | [Terms of Use](#)



Before your E-mail address is activated, it has to be verified first. Therefore, an E-mail message has been sent to kitty84@bluewin.ch. Please follow the instructions in the E-mail in order to confirm your E-mail address.

Due to SPAM filters it may take a few minutes until you receive the e-mail. If you do not receive the e-mail within 10 minutes, please also check your SPAM folder.

Swiss edu-ID Additional E-mail Verification

Verification Code

edu-ID Identity Provider Attribute

Can release the following:

- all SWITCHaai Core attributes
- all attribute recommended by eduGAIN
- ORCID attribute
- edu-ID identifier attribute (but generally won't)

Supports standard SAML2 profiles used in AAI

Supports SAML2 ECP (Enhanced Client or Proxy Profile)
Useful for some non-browser applications.

How to get your edu-ID

- Start at <https://eduid.ch> and click on "Create & Manage" or
- Select in the AAI WAYF/Discovery Service

Login






Login with: > AAI

 ▼

Last used

ID Swiss edu-ID

Universities of Applied Sciences

-  HEP-PH FR - University of Teacher Education Fribourg
-  HfH - University of Applied Sciences of Special Needs Education
-  PH Zug - University of Teacher Education Zug
-  PHBern - University of Teacher Education Bern
-  ph - University of Teacher Education Graubünden

Outlook I

- **Release Additional edu-ID attributes**
Quality of identity data and/or attributes.
Work on specification starting in Q3 2015.
- **Postal address verification**
Is implemented when there is a use-case for it
- **REST/JSON interface or simplified account view**
To check if an account with given email exists, let remote site create edu-ID account or provide a simplified form.
Requested by FHNW/SUPSI for a use-case.

Outlook II

- **OAuth2/OpenID Connect**
Is implemented when there is a use-case for it (edu-ID Mobile App project)
- **Two-Factor Authentication**
Which second factor and when?
- **Group Management Capabilities**
Requirements analysis starting in Q3 2015.
- **SAML Attribute Queries**
To update/extend edu-ID attributes by querying IdP (e.g. ETHZ) for linked AAI identities.

Swiss edu-ID Pilot Projects



SWITCH

Rolf Brugger
rolf.brugger@switch.ch

Call one year ago

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)

Pilot Projects in the Pipeline

Confirmed pilot projects

- Swiss edu-ID authentication on swissbib
- Migration of other services using aai guest login
- Swiss edu-ID authentication on mySNF (SNF)
- Swiss edu-ID authentication on SWITCHdrive
- Mobile Edu App (Mobile WG)
- Registration of prospective students (SUPSI)
- Transfer alumni portfolios to SWITCHportfolio (UniGE)
- Organization as Attribute Authority (UniL)
- Swiss edu-ID authentication on i-brain.ch (HES-SO)

Under evaluation

- Access and management of digital diploma (HES-SO)
- Self registration for prospective students (UNIBAS)
- Low-threshold registration for information events (FHNW)
- Eduroam for advanced studies (UniBAS)
- Guest-accounts (ETHZ)
- rechtsquellen.ch
- Adult learning information center (alice.ch) to adopt SWITCHportfolio

Completed case: SWITCHportfolio

- Students use and maintain a personal competence portfolio during their studies
 - Didactical tool
 - Proof for achieved competencies
 - Develop personal competencies
 - Continuing usage after studies
- Alumni-Tenant in SWITCHportfolio with Swiss edu-ID Login



Possible improvement:
Automatically migrate users
to alumni-tenant

Abandoned Case: Users of the University Library (UB) Bern

- UB clients (legal obligation)
 - University Bern affiliates
 - Residents of canton of Bern

- Swiss edu-ID Login for residents of the canton of Bern
 - Residence check using postal mail performed in Swiss edu-ID

The screenshot displays the website of the Universitätsbibliothek Bern. At the top, there are navigation links: Suchen, Kontakt, Lageplan, A-Z Index, and Sitemap. The main header includes the library name and the University of Bern logo (u^b UNIVERSITÄT BERN). A central section titled 'Datenbanken' (Databases) features a search form with fields for 'database name contains', 'database subject', 'database type', 'database region', 'database time period', and 'access'. To the right, there are two informational boxes: 'Zugriff von ausserhalb' (Access from outside) with links for VPN Clients, WebVPN, and SWITCHaai; and 'Zugriff für Kantonskunden' (Access for canton customers) with a link to 'Swiss edu-ID'. A 'Quicklinks' section at the bottom right lists links for FAQ, user accounts, VPN portal, and questions.

Confirmed Pilot Projects

Case: Swissbib

- Personal profile: preferences, contact information, bookmarks, wish-list, history, etc.
- User:
 - higher education members
 - lecturers at multiple universities
 - former students (Alumni)
- Profile with Swiss edu-ID login
- Migration of guest login

The screenshot shows the Swissbib search results page for the query 'identity management'. The page is in German and displays four search results. Each result includes a title, authors/contributors, year, format, and the number of libraries that hold the item. A sidebar on the right allows for refining the search by library network and author/contributor.

swissbib

identity management

/ Search: identity management

Q Results

Showing 1 - 20 of 3'982

Page: 1 of 200

Sort by: Relevance

Results per page: 20

Refine search

Library network	Count
Informationsverbund Deutschschweiz	3'845
NEBIS	2'747
IDS Basel Bern	1'425
IDS St. Gallen	1'396
Réseau Romand	1'030
IDS Luzern	864

» more ...

Authors/Contributors	Count
Institute of Electrical and Electronics Engineers (New York, NY)	24
Goffman, Erving	17
Association for Computing Machinery (United States)	13
Bruhn, Manfred	11
Hilb, Martin	10
Tomczak, Torsten	10
Regenthal, Gerhard	9
Fischer-Hübner, Simone	8
Herbst, Dieter	8
Homburg, Christian	8
Birkigt, Klaus	7

» more ...

Format	Count
Buch	3'601
E-Book	357

Identity management

concepts, technologies, and systems

Authors/Contributors: Elisa Bertino, Kenji Takahashi

Year: 2011

Format: Buch (online)

2 Libraries

List

Identity management

Authors/Contributors: Patrick Litscher

Year: 2009

Format: Buch (Hochschulschrift)

2 Libraries

List

Identity management

a primer

Authors/Contributors: Graham Williamson ... [et al.]

Year: 2009

Format: Buch (online)

1 Library

List

Identity management

eine Einführung : Grundlagen, Technik, wirtschaftlicher Nutzen

Authors/Contributors: Christian Mezler-Andelberg

Year: 2008

Format: Book

3 Libraries

List

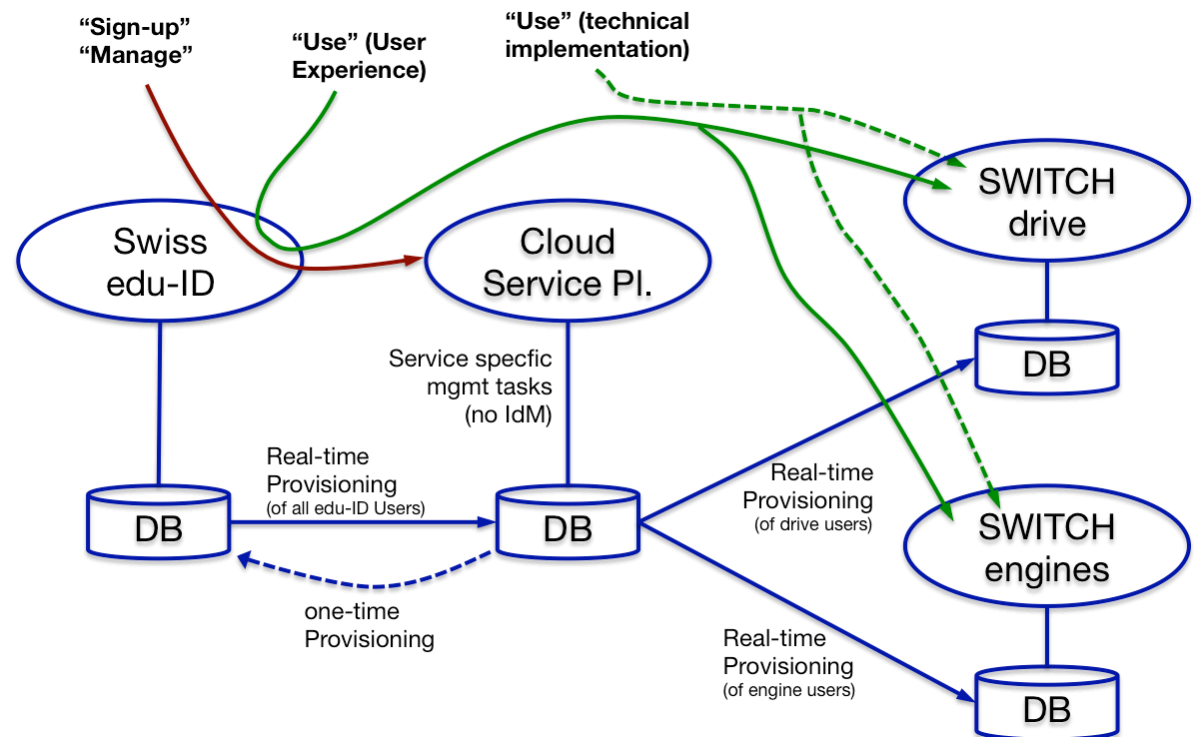
Migration of other services using the SWITCHaai guest login

- ETHZ Sharepoint
- ETHZ Blogs
- SWITCHtoolbox
- Some other tools

- Accounts are manually consolidated
 - writing conventions
 - duplicates
 - non-personal accounts
- User can re-use the same password

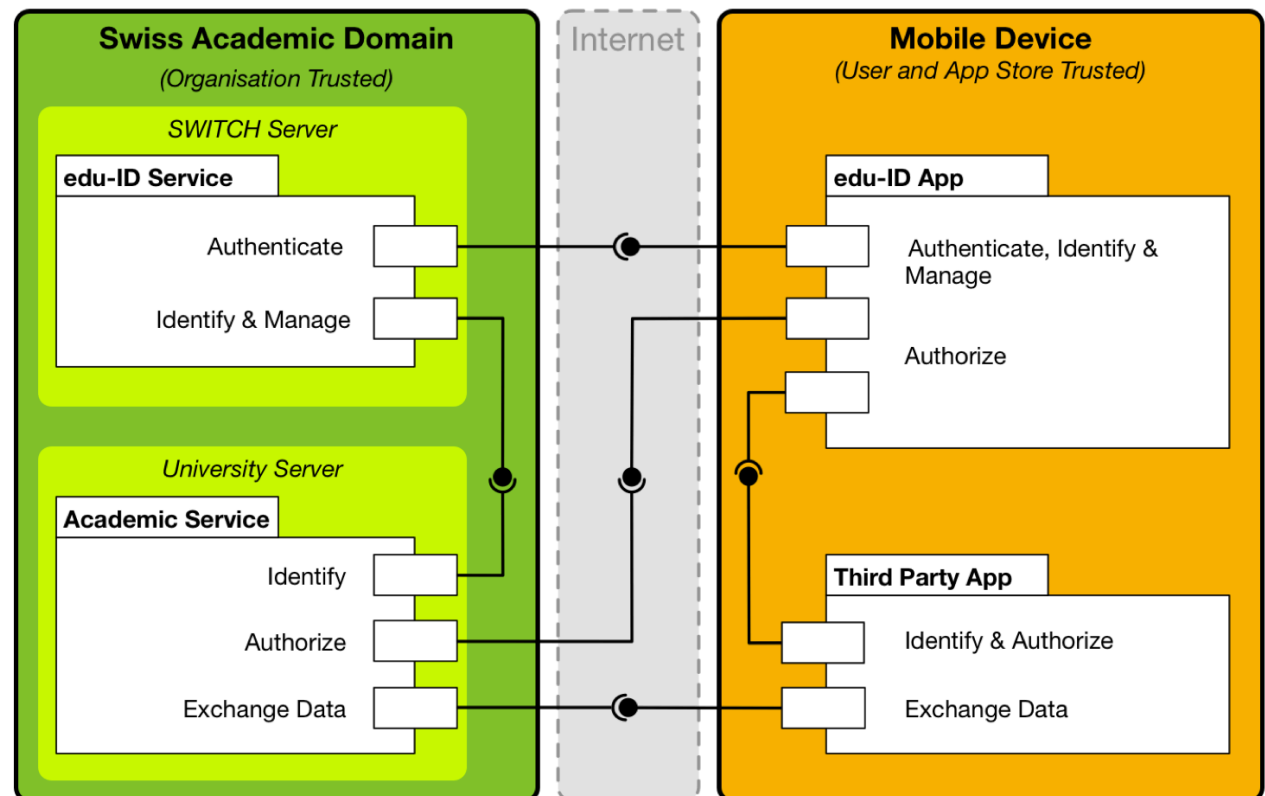
Case: SWITCHdrive and SWITCHengines

- Current cloud accounts to be replaced by Swiss edu-ID
- Multiple clients to be supported
 - Web client
 - Non-web clients: ssh, WebDAV, native Client
- Deal with multiple affiliations



Pilot Project: Mobile App

- One single authentication app authorizes many local third party apps
- Supports native apps and hybrid mobile apps
- Proof-of-concept:
 - Integrate mobile apps and LMS
 - Integration with Swiss edu-ID



Case: Registration of Prospective Students (SUPSI)

- Current registration process:
 1. Create an initial registration account (throw-away id)
 2. Applicant provides information and documents required for registration
 3. Admission office checks the applicants request
 4. If the application request is accepted the applicant is officially enrolled and he/she gets an official identity
- Project aim:
 - Replace throw-away id with Swiss edu-ID

More Pilot Projects

- i-brain (HES-SO)
 - Collaborative idea management and brainstorming platform
 - to be used by university members and public



Chalet village

Which services should be proposed in a chalet village for the vacation to be a success?

renforcer le rituels sociaux de l'année



marque fortement les rituels sociaux de l'année collectifs ou i...

#79 - caro fleury - 8. Aug 23:59 - 👍 1

je m'engage et mon énergie investie baisse ma c...



encourager les engagements à la participation à la vie local: ...

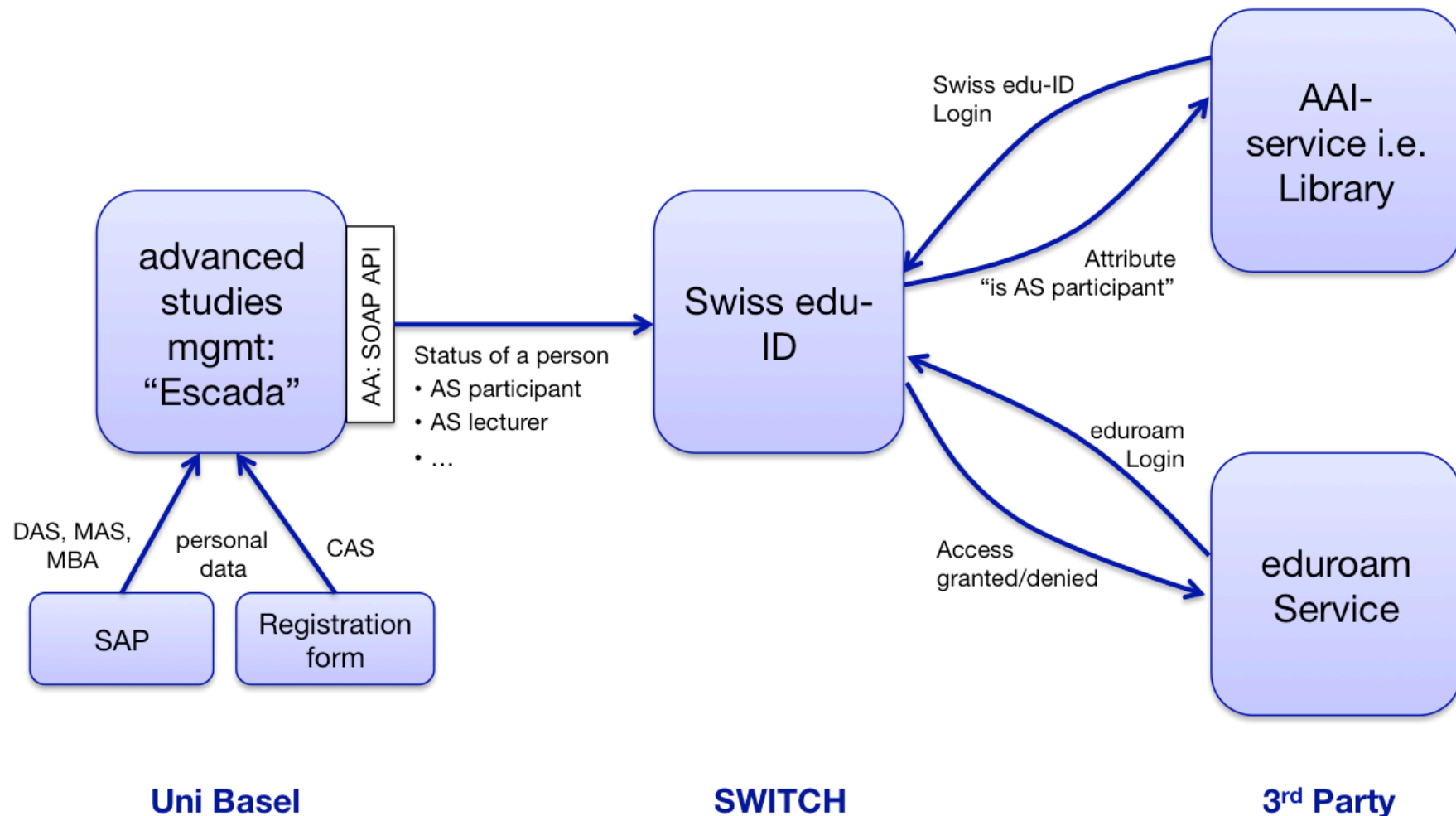
#78 - caro fleury - 8. Aug 23:55 - 👍 1

- Transfer alumni portfolios to SWITCHportfolio (UniGE)
 - Locally hosted e-portfolios are transferred to national SWITCHportfolio service for alumni

Pilot Projects under Evaluation

Case: eduroam for Further Education Students at the University of Basel

- CAS students are not centrally registered



Case: Event Registration at FHNW

- Simple / low-threshold registration
 - For large public (non-students, non-staff)
 - IT services provide registration API (exposed to the public)
 - Departments implement customized registration forms using the API
 - Users allow registration forms to access the institutional person information system (access delegation)
- Requires OAuth 2.0 / OpenID Connect

More Cases under Evaluation

- Access an management of digital diploma (HES-SO)
- Self registration for prospective students (UNIBAS)
- Guest-accounts (ETHZ)
- Law Sources Foundation (rechtsquellen.ch) of Swiss Lawyers Society
- Adult learning information center (alice.ch) to adopt SWITCHportfolio

Related CUS-P2 Projects

- Digital Lifecycle Management
 - Group management
- Swiss edu-ID Mobile App
 - Access for mobile clients

Implicitly related

- Data Analysis Service
- National Licences

Call one year ago = today

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

- Common web service, preferably of a library 9 1
- Non-web resource 4
- Application for mobile devices 1
- Resource using ORCID -
- Resource using a community-ID or social service -
- Resource interfacing/using existing ID-frameworks (STORK, SuisseID, Mobile ID, Swiss passport) -

Swiss edu-ID Working Groups

Results and Further Steps



SWITCH

Petra Kauer-Ott
petra.kauer@switch.ch

Berne, August 13 2015

Pre-Project Work

- **AAI Attribute Task Force**

Discussion about eduPerson, swissEduLibraryPerson, ORCID, Swiss edu-ID/Identifier

→ Result: **Input for Identifier Specification**

- **Identifier Specification WG**

2 institutions: BFH, ETH library

→ Result: [Unique Identifier Specification](#) (Nov. 2014)

- **High Level Architecture WG**

7 institutions: ETHZ, ETH Library, UNIBAS, UNIGE, UNIL, UNISG, USI, UZH

→ Result: [HLA Document](#) (July 2014)

Phase I Working Groups

- A. Processes**
- B. Regulations**
- C. ORCID**
- D. Mobile App Support**
- E. Governance Model**
- F. Business Model**



Thank you!

A. Processes WG



<p>IdM processes specification</p> <ul style="list-style-type: none">• describe IdM related processes in detail• describe interfaces	<p>Members</p> <p>9 institutions: ETHZ, FHNW, UNIBAS, UNIBE, UNIFR, UNIGE, UNIL, UZH, ZB (Moderation: Petra Kauer-Ott)</p>
<p>Collection of process descriptions, institutional plans, pilot ideas, issues and questions</p>	<p>Meeting Oct 28 2014 & individual interviews</p>

Processes WG - Results

Processes WG report

Identification of most promising pilots:

1. **e-portfolio transfer** to national instance (access to resources for alumni)
2. **authentication** for SWITCHdrive
3. **self-registration** for candidates and guests
4. **validated identities** for library users

UNIL volunteering as candidate for an **Attribute Authority pilot**

Processes WG – Essential Features

- E-Mail address validation
- Self-registration process (-> integration into services)
- Verification of identity
- Binding rules & process for changes of core attributes (as name, based on role)
- Support attribution of access rights (with specific attributes -> basic roles)
- Uniqueness of identity (e.g. duplicate-checked -> Guest IdP migration to test duplicate checks)
- Legal framework (-> Regulations WG)
- Attribute history (-> recovery/reset process)
- Validation rules (accepted and controlled)

Processes WG – Important Features

- Additional contact attributes (like office address)
- Attribute status active/passive (detection of inactive users)
- Time stamps for attributes (history of changes)
- Validation of residence address (prepared)
- Verification of added or changed attributes (for AAI Attributes)
- Additional official identifier attributes (as OASI/AHV etc.)
- Enforce user-consent for external resource access
- Support of local attributes
- Import and change of attributes supported
- Sustainable concept for Levels of Assurance for attributes
- Processes for regular updates & "incentives"/information for users
- Care concept for LoAs (technically supported processes)
- Auditing of own and partner behaviour (governance)

Processes WG – Nice to have Features

- Additional "Portfolio" attributes (like diplomas, certificates etc.)
- Email provided with Swiss edu-ID (lifelong)
- LoAs compatible with LoA standard and own IdM
- 2-factor authentication (-> use case at UNIGE)
- Support of group management functions (-> working group)
- Building attribute sets (e.g. similar data, with same LoA)
- Levels of Assurance for authentication method enforcement

B. Regulations WG



Legal framework <ul style="list-style-type: none">• identify regulations and discuss/clarify relevant questions within institutions• define policies institutions need• bring in institutional experiences with end user policies	Members <p>6 institutions: ETHZ, UNIFR, UNIGE, UNIL, USI, ZHAW (Moderation: Esther Zysset)</p>
Collection of questions	Meeting Nov 20 2014

Regulations WG – First Results

Data Protection Commissioners consultations:

- Zurich (March 2015)
- Federal (June 2015)
- Lucerne (July 2015)

Planned:

- Fribourg (August 2015)
- 1-2 additional meetings with Data Protection Commissioners
- Collection of relevant institutional regulations

→ no show-stoppers have been identified

→ attributes will have to be transferred to the Central Identity Provider once a person has left the University

A summary of conclusions from the various Commissioners will be made available to the Working Group

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

- presentations of status at institutions
- ideas for ORCID projects

Members

7 institutions:

ETHZ, MDPI, SNF, UNIBE, UNIGE, UZH, ZB

(Moderation: Rolf Brugger)

1 online meeting and 1 meeting in Berne, Oct 16 2014

ORCID WG - Results

1. [ORCID WG report](#)

- ORCID implementations at UNIBE library and MDPI
- Project plans at ETHZ, SNF and UZH

2. ORCID integrated into Swiss edu-ID as linked ID

3. Follow-Up meeting organized by community (libraries, research output measurement) (24.6.2015, Berne)

- Usage of ORCID grows
- Swiss Consortium under construction
- Differentiation to Swiss edu-ID necessary

D. Mobile App Support WG



Better mobile support <ul style="list-style-type: none">• describe requirements of institutions/users• discuss ideas for better mobile support• evaluate existing solutions	Members <p>6 institutions: ETHZ, FHNW, HES-SO, HTW Chur, UNIFR, UNIGE (SWITCH: Lukas Hämmerle)</p>
<ul style="list-style-type: none">- Status at institutions- Possible candidates for pilots	Individual interviews and one group interview

Mobile App Support WG - Results

Mobile App Support WG report:

- Support of mobile applications is **a must but not a high priority**
- **Long authentication session timeout** is a precondition for additional functions like learning analytics

- 1. Low number of mobile applications*
- 2. Several Apps work without authentication*
- 3. Low number of users per App*
- 4. Web-Apps can use authentication with AAI
(some universities avoid native development)*
- 5. Small interest in AAI Mobile Proxy*

→ *Pilot Project for a mobile authentication App was submitted by Christian Glahn, HTW Chur and partners.*

E. Governance Model WG



Governance documents <ul style="list-style-type: none">• act out cases to check usability and robustness of governance model• identify points to be adapted/improved• discuss issues with legal representatives at institution	Members <p>4 institutions: FHNW, UNIGE, UNISG, USI (Moderation Christoph Graf)</p>
Discussion of Governance structures and measures to take	Meeting May 4 2014

Governance Model WG - Results

[Governance Model WG report](#)

is base for the future Governance Model for Swiss edu-ID

1. Use existing Governance structures
2. Expand AAI Community Group with additional stakeholder groups:
 - University administrations
 - Continuing Education
 - Alumni Organisations
 - third party Service Providers (depending on Business Model)
3. Discussion of Governance changes with AAI Advisory Committee
4. Additional input of Processes WG
5. Technical Standards Taskforce (Attribute TF with enlarged scope)

F. Business Model WG



Business models <ul style="list-style-type: none">• discuss and evaluate different model options	Members <p>4 institutions: FHNW, UNIGE, UNISG, USI (Moderation: Christoph Graf)</p>
Description of assumptions, methods and further steps to elaborate final version of Business Model	Meeting May 4 2014

Business Model WG - Results

Business Model WG report

- assumption that institutions will use Swiss edu-ID
- not charge the users
- increase user-base is necessary
- keep parallel operation period of SWITCHaai and Swiss edu-ID short
 - **early migration important!**
- involve new stakeholder groups (including third parties)

Working Groups Phase II

Open Calls for

1. Group Management
2. Processes II

Regulations WG (continuation)

Ev. group for Roadmap 2017+

Call Group Management WG

<p>Provide input for Swiss edu-ID group management functions</p> <ul style="list-style-type: none">• Elaborate use cases• Define requirements based on real cases	<p>Member Profile:</p> <ul style="list-style-type: none">• responsables of tools or projects with a need for group management functionalities• people involved in group management projects• knowledge about group management tools and functions
<p>Individual follow-up meetings to elaborate use cases/pilots</p>	<p>ca. 1 day; Aug.- Oct. 2015 1 meeting in person</p>

Call Processes II WG

<p>Requirement catalogue for Swiss edu-ID Version 2.0 and later:</p> <ul style="list-style-type: none">• attribute definitions• attribute aggregation• quality levels• attribute verification• interface descriptions• etc.	<p>Member Profile:</p> <ul style="list-style-type: none">• Processes WG• profound understanding of IdM/IAM processes within institution• able to identify weak or critical points of current and future solutions• discuss issues with stakeholders at institution
<p>Feedback about the draft requirement catalogue</p>	<p>ca. 1 day; Oct. – Dec. 2015 meeting in person, additional topical discussions</p>

Make it yours!

Spread the call

and contact us for

- presentations/discussions
- comments & suggestions
- pilot options

Contact:

swisseduid@switch.ch

Details about current call:

http://swit.ch/eduid_workgroups



OAuth 2.0 and OpenID Connect in the Swiss edu-ID



SWITCH

Rolf Brugger
rolf.brugger@switch.ch

Motivation to consider OAuth 2.0 and OpenID Connect

- Enable native mobile applications and non-web resources
 - Shibboleth/SAML is a web browser based technology
- Provide more developer-friendly environment
 - Shibboleth setup and configuration is complex
 - But complexity of scalable OIDC federation unknown

OAuth 2.0



- Framework for authorization protocols
 - Avoid password proliferation
 - Protect APIs
 - Mobile access to server systems
 - User authentication
- Specifies a set of message flows
- Based on http and JSON
- Specification finalized: October 2012 (RFC6749)

OpenID Connect

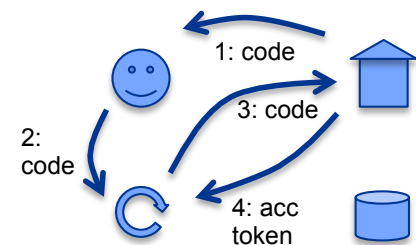
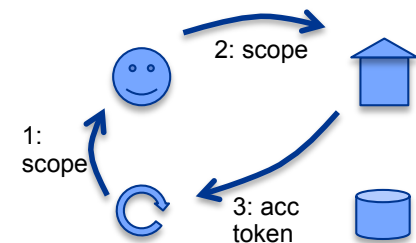
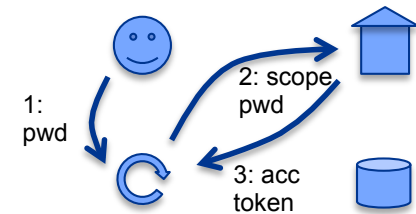
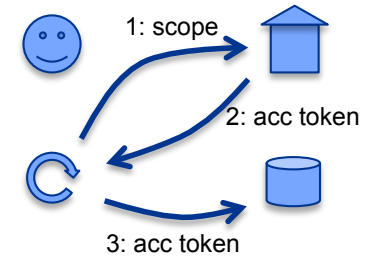


- Provides identity services: adds user attributes (ID Token)
 - User ID, profile data, authentication meta information
- Based on OAuth 2.0
- Scalable security model (ISO/IEC29115 LoA1...4)
- Base specification finalized: February 2014
 - Missing application profiles like interoperable attribute specifications

OAuth 2.0 Flows

OAuth 2.0 usage scenarios (flows)

- Service-service communication: *client credential flow*
 - Without involving a user
- Trusted clients: *resource owner password credential flow*
 - Client sees password
- Untrusted clients: *implicit flow*
 - Password not revealed to client
- Client runs on server: *authorization code flow*
 - Token stored on server side (ORCID case)



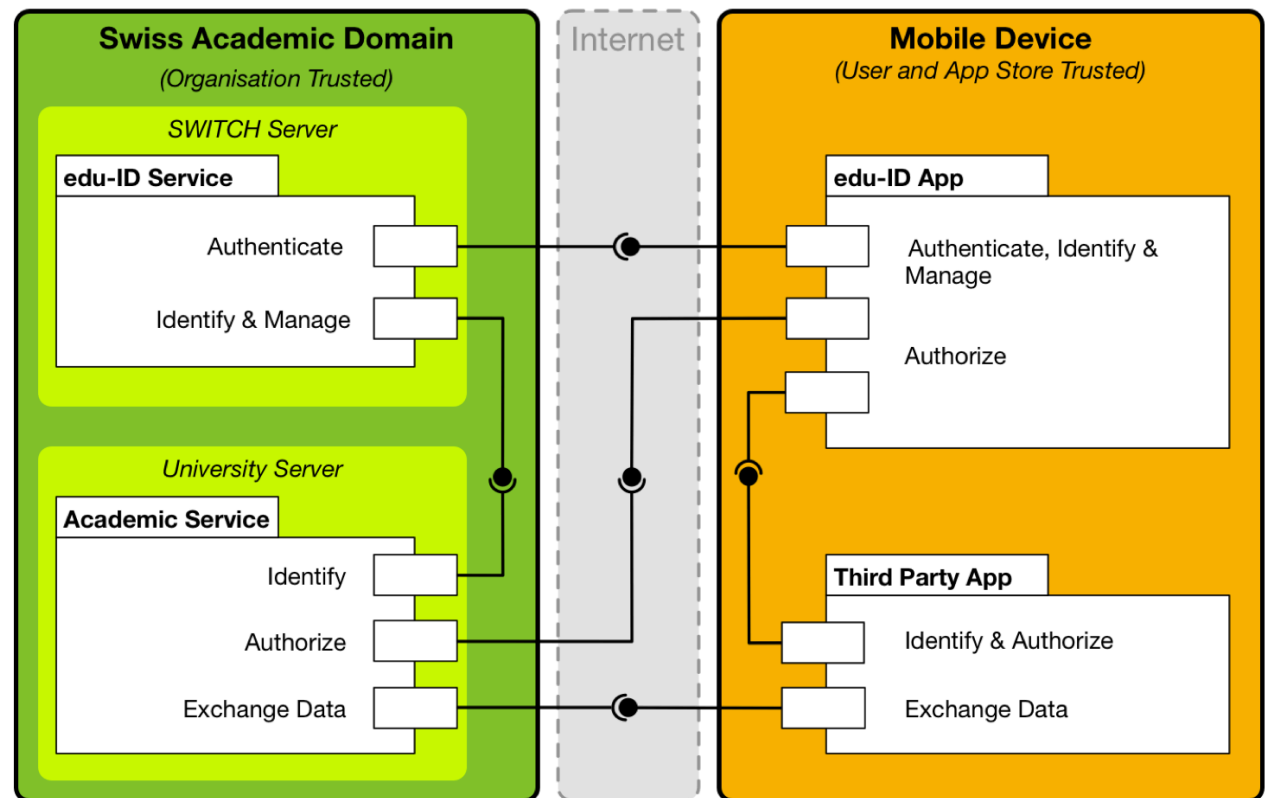
Differences between SAML and OIDC

	SAML/shibboleth	OpenID Connect
Federation support	yes	no (no federation metadata)
Developer friendliness	Not required	Relying party libraries for various languages
Setup and operation of service	Shibboleth software suite, updates, certificates	OIDC library installation
Non-web / mobile application support	no	yes
Access delegation	difficult (ECP)	yes, including user-initiated token revocation

No fundamental differences: attribute provider, user consent, IdP middleware/server, application registry

Pilot Project: Mobile App

- One single authentication app authorizes many local third party apps
- Supports native apps and hybrid mobile apps
- Proof-of-concept:
 - Integrate mobile apps and LMS
 - Integration with Swiss edu-ID



Other prospective Pilot Projects

- Event registration at FHNW
 - IT services provide registration API (exposed to the public)
 - Departments implement customized registration forms using the API
 - Users allow registration forms to access the institutional person information system (access delegation)

Support for OAuth and OIDC in Swiss edu-ID

Option: Extend Shibboleth

- Shibboleth 3.0 IdP has modular architecture
- OIDC and OAuth are on Shibboleth roadmap with status “under discussion”
- Pilots are possible with 3rd party OAuth suites outside of shibboleth

Option: alternative AM product OpenAM

- OpenAM fully supports OAuth 2.0 and OIDC
- Proof-of-concept (July 2015): OpenAM can be made compatible to the SWITCHaaI federation

Call for Participation

- Tell us your use-cases
- Let's start pilot projects together

The Future of Identities

The future of AAI and Swiss edu-ID & Outlook to Swiss edu-ID 2.0



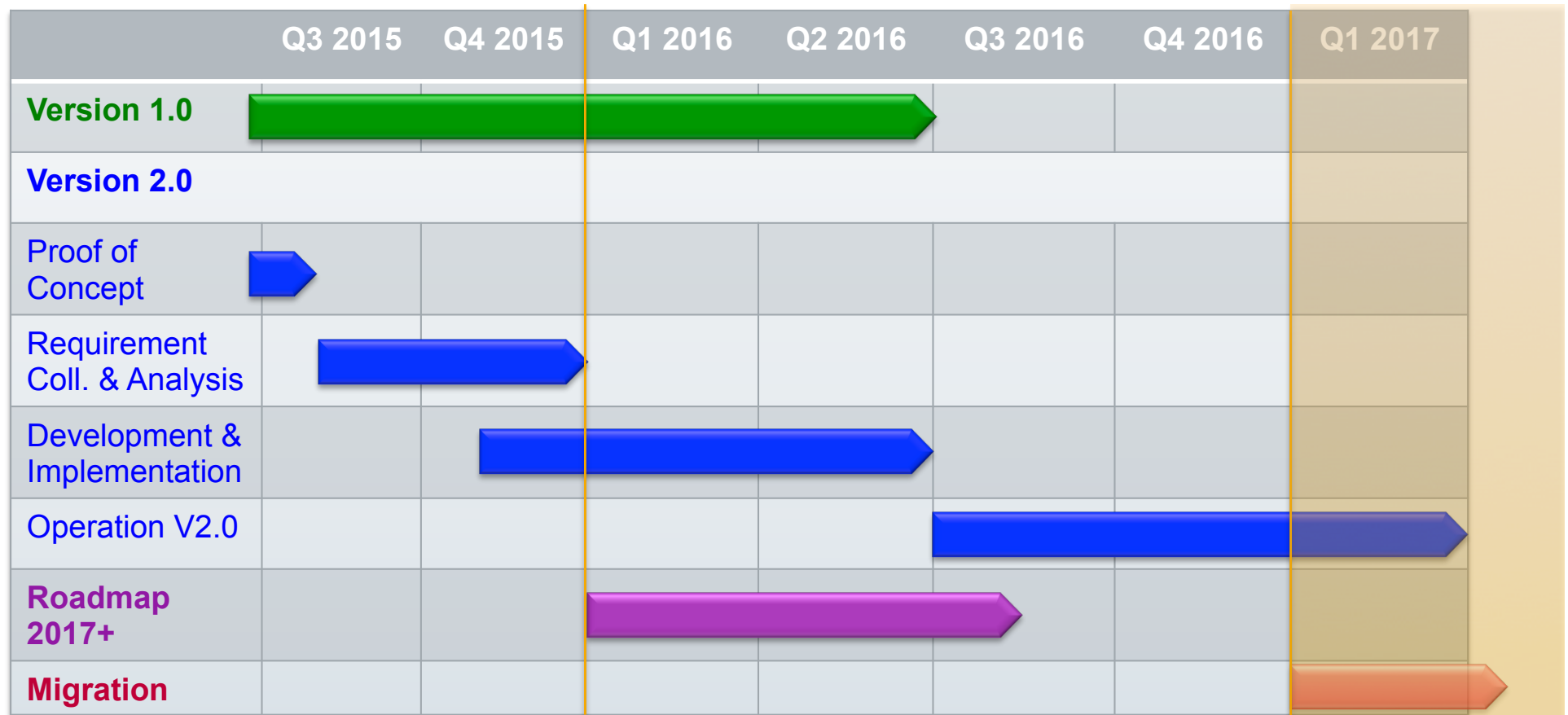
SWITCH

Swiss edu-ID
swisseduid@switch.ch

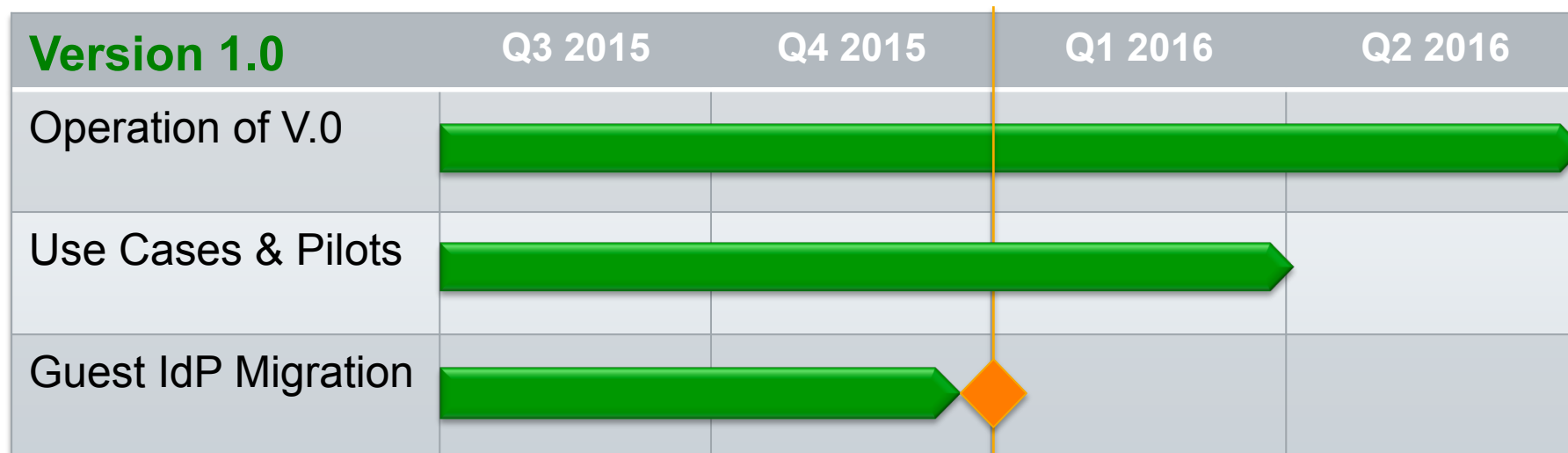
The Future of Identities

- The project “Swiss edu-ID phase II” (Aug 2015-Dec 2016)
 - Goal: Implementing Swiss edu-ID V2.0 and planning next steps
 - Vehicle: Our current CUS P-2 project with financial support from swissuniversities
- Outlook 2017-2020
 - Goal: Dissemination, migration from SWITCHaai to Swiss edu-ID
 - Vehicle: a new collaboration project supporting universities (also financially) migrating to Swiss edu-ID
- The international perspective
- How to stay informed and to contribute to Swiss edu-ID

Roadmap Phase II - Overview

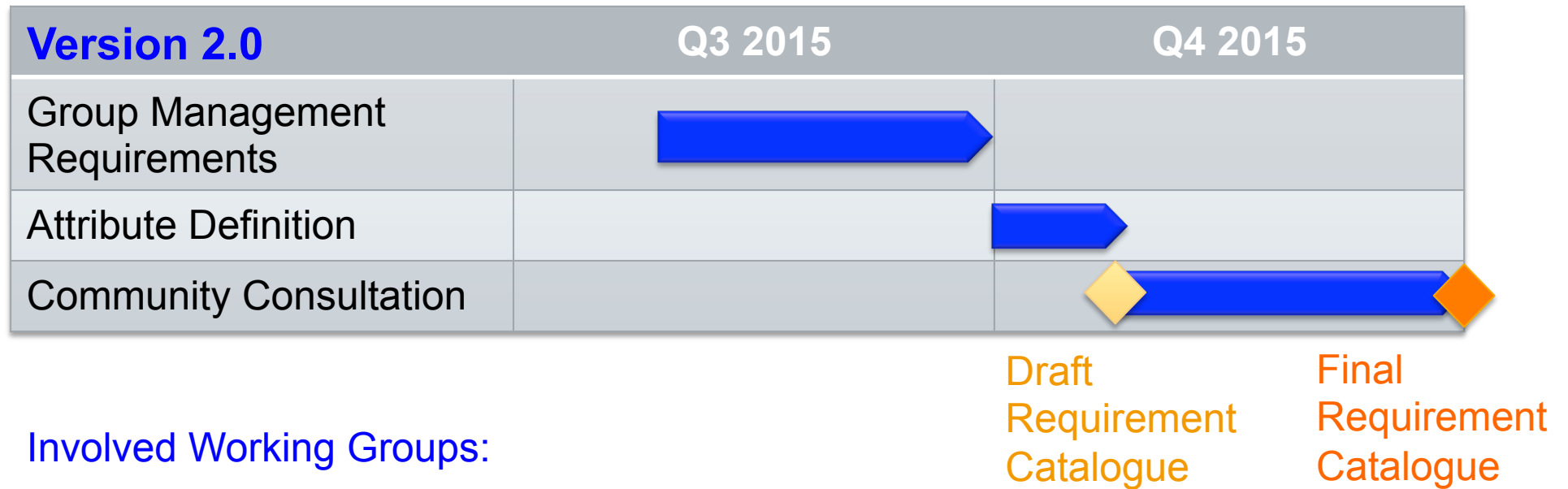


Version 1.0



Guest IdP will be migrated to Swiss edu-ID until end of 2015

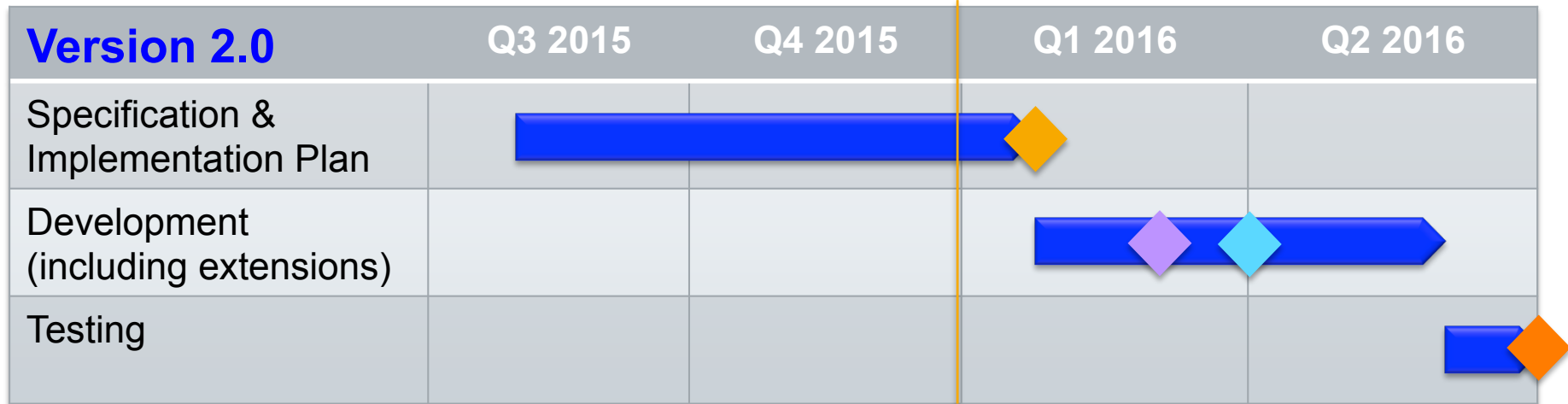
Requirements Version 2.0



Involved Working Groups:

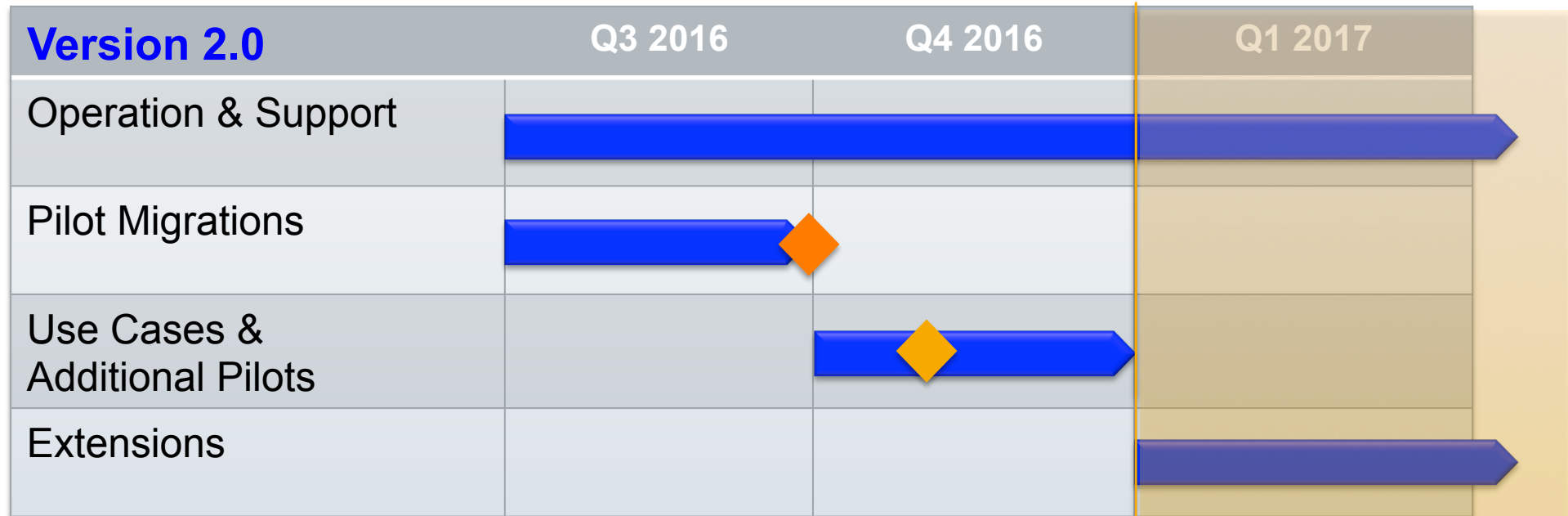
- Group Management
- Attribute Task Force
- Processes II

Development & Implementation



Specification & Implementation Plan completed
 Legal feasibility checked
 Change Management Process implemented
 Operational Concept V2.0 ready
Test report completed, V2.0 ready

Operation of Version 2.0



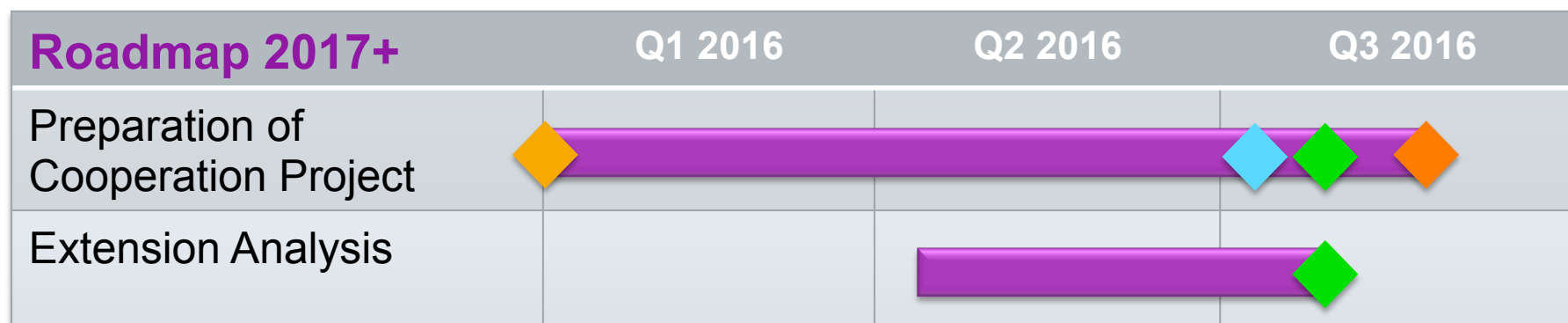
SWITCH migrated as one of the pilots

Governance Structures in place

Policies implemented

Business Model ready for decision

Preparing the Roadmap 2017+



Preparation of a cooperation project for migration of institutions 2017-2020

Working Group to prepare the migration concept

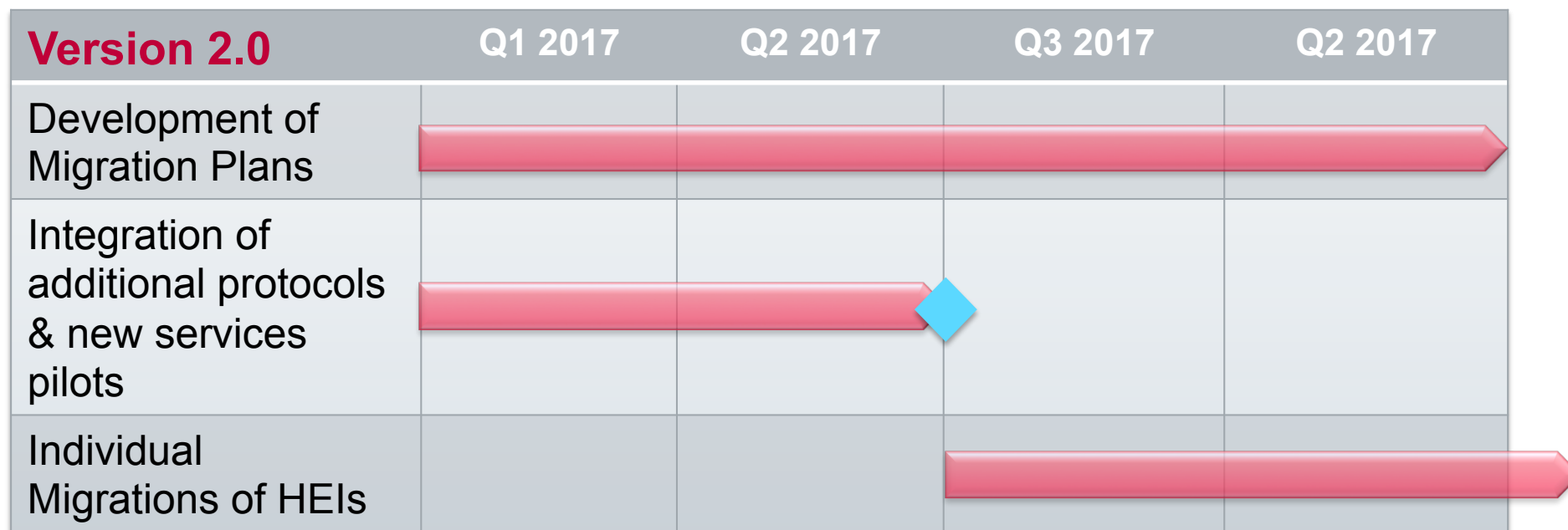
Migration pre-study ready

Migration concept completed

Legal feasibility checked

Application for cooperation project

Outlook: Migration 2017 - 2020



Follow-Up project to support migration of institutions

Manuals & Support material ready

The international perspective

SWITCHaai



International promotion
in GÉANT community

Service innovation
efforts

eduGAIN

“the internationalised SWITCHaai”



Swiss edu-ID

“SWITCHaai next generation”



International promotion
in GÉANT community

eduKEEP

“brainstorming usercentric eduGAIN”



1999

2005

2010

2015

Events featuring the Swiss edu-ID

- 13.8.2015 AAI & Swiss edu-ID Update (public)
- 9./10.11.2015 ICT Focus Basel (IT departments)
- end Oct. 2015 P-2 project presentations (public)
- 27./28.1.2016 eduhub days Fribourg (e-learning comm.)
- (tbd) 31.3.2016 Executive Focus (univ. administration)
- summer 2016 Swiss edu-ID Update (public)

Informing and contributing

- Project website: <http://projects.switch.ch/eduid/>
- SWITCH identity blog: <http://identityblog.switch.ch/>
- Working groups: <http://projects.switch.ch/eduid/working-groups/>
- Contact: swisseduid@switch.ch