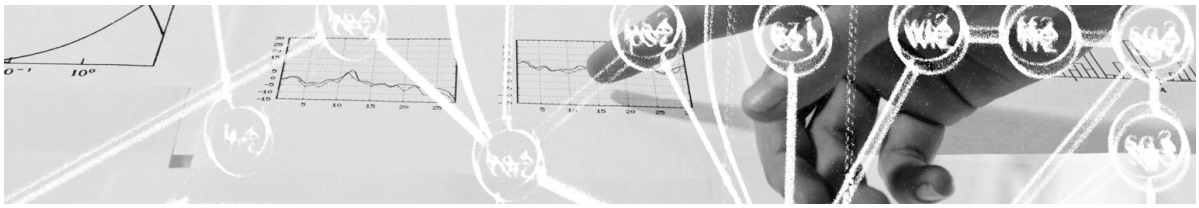
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Processes WG Report

Public Report of the Swiss edu-ID working group "Processes"



Name Surname **Petra Kauer-Ott, Rolf Brugger**
Job Title **Swiss edu-ID**

Document Type: Documentation
Version: V1.0
Created: 15.12.14
Last changes: 31.03.15
Classification: Public

Content

1 Processes Working Group

SWITCH has published its call for participation in working groups for the further development of the Swiss edu-ID in July 2014 on http://projects.switch.ch/de/eduid/working-groups/. Goals of the working group are:

- Describe IdM related processes in detail (like enrolment, exmatriculation, register & administrate users like students, staff, library users, alumni, continuing education participants, externals; allocation of multiple roles; charging of services; issue identification cards, badges, certificates and diplomas)
- Describe interfaces
- Provide input for further project steps/pilots (call 15.2.2015)

16 volunteers from 9 institutions, mainly from cantonal universities, have participated:

- Omar Benkacem, UNIGE, NTICE
- Giorgio Broggi, ETHZ, head software services
- Alain Cochard, UNIFR, head solution engineering
- Dieter Glatz, UNIBAS, assistant manager of central IT
- Lars Händler, ETHZ, ETH library, IT services
- Michael Hausherr, FHNW, corporate IT, enterprise architect
- Roberto Mazzoni, UZH, head of user services, Information Technology
- Alexandra Müller, UZH, head of office for continuing education
- Ursula Müller, ETHZ, ETH library, head library Zentrum
- Christian Oesterheld, ZB, head Customer Services
- Dominique Petitpierre, UNIGE, PRODS
- Hervé Platteaux, UNIFR, Centre NTE
- Alexandre Roy, UNIL, central IT, scientific informatics
- Swen Vermeul, ETHZ, ID Software Services
- Urs von Lerber, UNIBE head of IT services
- Bruno Vuillemin, UNIFR, head of IT security

The working group has met on October 28 2014 in Berne (hosted by UNIBE). During the workshop the participants have exchanged information about the IdM status at their institutions, experiences and plans. The members have then described existing registration processes within flow diagrams or text and in a final step identified possible starting points for Swiss edu-ID and components that shouldn't be changed/influenced. Diagrams and text as well as a field manual (see annexe) built the base for the subsequent interviews with the group members (and other people they've invited to contribute). The interviews have been conducted between Nov. 4th and Dec. 11th 2014. As additional contributors Christian Hensel (UNIBAS; central IT), Davor Kupresak (ETHZ, group leader Identity/Access Management & eServices), Tobias Marquart (UNIBAS, business data processing specialist), Robert Matathia, (UNIFR, head servers), Michael Pfister (UNIBE, system services) and Peter M. Geiser (UNIBE, system services) provided input.

The collected input was integrated in a draft report prepared by SWITCH. As not all process flow diagrams and system architecture figures can be published we've resigned to integrate them in this report. The participants provided feedback that has been used to finalize the draft version.

The working group was moderated by Petra Kauer-Ott (petra.kauer@switch.ch) and the report edited by Petra Kauer-Ott and Rolf Brugger (rolf.brugger@switch.ch).

1.1 Used Abbreviations

AA	Attribute Authority
AD	Active Directory
AM	Access Management
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (Loi sur la surveillance de la correspondance par poste et télécommunication)
IAM	Identity and Access Management
IdM	Identity Management
IdP	Identity Provider
IDS	Informationsverbund Deutschschweiz
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance (also assurance level or trust level)
NAS	Network Attached Storage (storage supporting file-based storage protocols
NDS	Novell Directory Services (Novell eDirectory)
NEBIS	Netzwerk von Bibliotheken und Informationsstellen in der Schweiz
NFS	Network File System (protocol for file access over network)
RADIUS	Remote Authentication Dial In User Service
SQL	Structured Query Language
SSO	Single Sign On
SUF	Shared User File

Note: Institutional information in this report was provided by the working group participants. This information does not pretend to be implicitly complete or representative for a whole organization in every case, nor for all Swiss Higher Education Institutions.
University of Geneva specific information is not available in this version of the report.

2 Outcomes

2.1 IdM challenges at Swiss HEIs

Identity and Access Management systems are a core part of the IT infrastructure of Swiss Higher education institutions. Hence those systems are very **robust** but sometimes also **heterogeneous** because of the continuous development and mutual interaction with connected systems and services.
Also if there are general similarities between the infrastructures, the structures, procedures, linking and some components differ at institutions, therefore all process flow diagrams have been unique. Nevertheless there are challenges related to IdM being relevant for all institutions, and they remain challenges - also for those having started or already finished a recent redesign:

- handle the complexity of generic systems
- provide integrated services
- manage accounts and email for members
- handle accounts for people from related units and for guests (including closure)
- grant security (measures against phishing, encryption mechanisms etc.)
- support Single Sign On
- provide group management functions (support life cycle)
- support relationship to alumni (account handling, export in separate systems, delivery of services etc.)

2.2 Current institutional IdM environments

The components/protocols all institutions use are the directories **AD** and **LDAP**. They are the “visible” output of the IdM’s or rather the part that is used to attribute roles, build groups and handle access rights. Also **RADIUS** is widely used. SQL databases (mainly Oracle and MySQL) are widely used within the interviewed institutions. For **group management** some institutions use directory functions, some have developed their own tools and others use the open-source software Grouper. Several institutions use **SAP** and interfaces to it.

Registration is at all institutions a task of local special units and performed with specialized tools provisioning data for account creation to the IdM core system or linked databases. The frequently **separately handled registration process for staff, students and others** (like guests) increase the danger of **duplicate generation**. Therefore all institutions have implemented automatic or semi-automatic duplicate detection and are able to **merge identities** if necessary – nevertheless such tasks may be demanding (time, effort).
Only few institutions can handle identities with multiple accounts and roles (staff, student). Most create **two or more records for a user** in case he/she belongs to different main groups because the **applications are not able to distinguish between the roles** of a user.

The information an identity contains in the IdM is often **not exactly the same data** set as the registration units keep within their systems. Usually data like OASI/AHV number are not stored in the IdM because the information is mainly necessary for identification and financial tasks but not for establishing permission/access right groups.

Life cycle management of identities is a complex task for all institutions since the systems contain information about a user and information from a user. Regulations and technical processes have to go hand in hand (as blocking of user names for a defined period), but the tasks may be very complex and the automatic processes can’t always be adapted as fast as regulations may change (e.g. BÜPF).

The general trend is to **use professional IdM or IAM systems** for larger organizations with thousands of members – and also to professionalize the work of IdM teams by analysing processes and systems. This trend is visible in the full **redesign attempts** of some universities. But to rebuild from scratch and in parallel a system that has grown up in several steps over the years is hardly possible without a lot of resources. Therefore some institutions limit the current IdM development on single integration steps or interface improvements.

The overall impression is, that the **institutions manage IdM tasks well** and have found solutions also for difficult tasks. But obviously there's partially a **lack of integrated solutions** and the IdM ecosystems are mainly **closed environments often not being able to handle specific rights and roles for the application level very well** (not remarkable since on application level there's often lacking support for role detection during the login process).

Therefore the IdM's currently used or planned at Swiss HEI's do **not support a proper handling of an external central ID per se**. Nevertheless newer systems have the advantage that the handling of **assurance levels** is already implemented.

Institution	Current IdM	Future IdM/IAM
ETHZ	IdM developed inhouse (in Perl) AD, LDAP RADIUS Nethz for authN & authZ Adobe Experience Manager for Intranet authN (web) Identity Authorization Service (IAS) specific attributes are added Automatic generation of groups Highly automated and digitized processes (registration, group management)	IAM DirX by ATOS implementation ongoing (ca. Nov. 14 – end of 2016 → improve governance better risk analysis and appliance; supporting LoAs, group management and mapping; guest accounts new event management tool under construction
FHNW	AD, LDAP (general roles staff/student in AD) SAP SharePoint as collaboration platform (including external users) Local group management Rights/roles on application level Partly automated duplicate check No self-registration Microsoft 365 infrastructure for alumni	Standardization of interfaces IdM project with the goal of an architectural redesign on the roadmap for 2016/17 Project for matriculation portal started
Libraries (ETH & ZB)	ILS Aleph SUF Self-registration	Not clear, ILS Aleph should be replaced NEBIS SSO Project: a) SwitchAAI for HEI members (currently ETHZ

	De facto lack of secure authentication mechanism (but scope currently limited to accessing user account) Nethz accounts (for ETH affiliates), Aleph accounts IDS and NEBIS network: identity replication via SUF	and EPFL, other institutions awaited), in production; b) SwitchAAI for non-HEI-affiliates ("Privatkunden"), in progress
UNIBAS	SAP NetWeaver IdM AD, LDAP Roles defined in directories Automated duplicate check	Redesign/streamlining of IdM finished in 2014. Preparation for use of trust levels done Self-registration and integration of telephony are planned Group management project in 2015
UNIBE	IdM Forefront Identity Manager (Microsoft) AD, LDAP Database PARIS Database StudiTracker Exchange 2010 Self-registration (throw-away identity) Kernsystem Lehre stores diploma etc. Group management with AD	No general redesign planned New technologies for some interfaces
UNIFR	AD, LDAP Oracle Scripts for access right control Several not connected DBs Exchange No self-registration	Full system analysis and redesign until 2nd term 2015 Ev. self-service for short-term accounts Shibboleth SSO for CAS
UNIL	SAP IDM (since 3 years) AD, LDAP NetWeaver SQL SAP (matriculation part was developed inhouse) Self-registration (throw-away identity) Group management tool	No general redesign Integration of group management into SAP IDM is planned (grouping of roles for applications; regrouping of access rights for several applications)
UZH	IBM Tivoli Identity Manager (since 5 years)	IdM redesign project ongoing. Currently analysis, concept end of 2014

	AD, LDAP SAP	→ Central UZH ID creation and provisioning to other systems

Table1: IdM overview

2.3 Pilot Options

One of the goals of the working group was to collect input for pilots. The challenges, possible benefits, possible starting points and pilot options that have been discussed during the interviews are described in the table below.

Most promising are pilots for

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

One institution (UNIL) is volunteering as candidate for an **Attribute Authority pilot**.

Inst.	Challenges	Benefits with Swiss edu-ID	Starting points	Pilot options
ETHZ	New IAM will be implemented supporting LoAs	Self-registration support Usage of additional attributes Integration of LoA's Automatic attribution of rights Handling of guest accounts (increase data quality)	Provide a unique identity Implement assurance levels (which standard?)	Guest accounts (self-registration, verification, assurance levels)
FHNW	IdM dispersed over various applications and tools Keep in touch with former staff/students	Keep contact with former staff/students Authentication for all resources & devices	Alumni sector (solution outside of AD) Strengthen Swiss edu-ID with official identifiers (AHV)	Alumni organizations
Libraries	Outdated system to be replaced Complex network structures and historical data to be kept Verification of identity	Verified and unique identity including address data Identify/contact inactive users Processes to regularly update user data Flexible role	Duplicate check Include several address data and primary address information Check for local storage possibilities of Swiss edu-ID and	Delivery of verified identity Identity including primary contact data Authentication for trusted access to

	Duplicate check Assignment of correct role(s) Identification of inactive users	attribution (connected to and determining access rights etc) Swiss libraries card based on Swiss edu-ID	rules for backchannel	licensed content or to library-managed resources with partially restricted access provided to different user groups
UNIBAS	Implement self-registration Usage of trust levels Group management 2-factor authentication	Self-registration Usage of verified attributes (assurance levels)	Self-registration Risk management Assurance levels	Self-registration for continuing education (solve trust issues first)
UNIBE	2-factor authentication Role assignment (members of different institutions)	Reachability of former students/staff Access to verified portfolio information (diplomas etc.)	Consolidation (AAI -> Swiss edu-ID) with only one account. Access to non-web resources	-
UNIFR	Analysis and redesign of IdM Certification of small modules and MOOCs Keep in touch with former students/staff	Accounts for mobility students and guests Alumni contacts Additional SPs User-generated and verified identity	Self-registration Support mobility students (BENEFRI etc.) Support VO (group management)	SWITCHdrive Batches Self-registration
UNIL	Accounts for related units Group life cycle management Increase acceptance/use of 2-factor authentication	Automation of account generation Access to non-web resources Better security Control access rights with attributes Ev. Swiss edu-ID email address	AA pilot	Career centre (application for former students) AA pilot
UZH	IdM redesign Implement UZH ID and provisioning	Validated local attributes with time stamp (better security) Self-service for guest accounts	Self-registration Delivery of unique ID (UZH ID)	-

		Basic access for continuing education and guests Duplicate prevention Substitute for UZH ID		

Table 2: Pilot options

2.4 Expectations

2.4.1 Benefit

The main benefits expected by the interview partners are:

- **Resources**: simplified creation of user accounts & unified process (less resources needed for registration)
- **Automation and streamlining of processes**: automated (self-)registration and account generation process
- **Access Management**: support of access management through additional (qualified) attributes
- **Matching**: easier matching of accounts / users within own system(s)
- **Unique identity**: delivery of a unique identity including a unique identifier, and without duplicates
- **Greater variety**: support for accessing also non-web resources
- **Security**: improved security through validation of information, time stamps, proper processes and additional use of 2-factor authentication
- **Data quality**: increased data quality (levels of assurance, updated attributes, detection of inactive users)
- **Contact**: easier direct and persistent contact to alumni (e.g. transfer of contact data by user-consent or a general preference within the Swiss edu-ID)

2.4.2 Transition

Interview partners have been aware that there may be a longer transition phase with AAI and Swiss edu-ID in parallel. They expect:

- no collisions with AAI
- only few adaptations on IdP level (low effort)
- early information and clear instructions about necessary adaption on level IdP/AA

2.4.3 Coming up version of Swiss edu-ID

The following features should be solved/implemented already in the earliest possible upcoming release of Swiss edu-ID (after version 1.0):

- self-registration implemented

- unique ID (duplicate checked)
- interfaces/API for integration of Swiss edu-ID into existing local applications
- secure password reset without necessity of staff intervention
- support of assurance levels implemented
- legal framework and governance model in place (1st version)
- audit process(es) in place
- identification of non-active users

2.4.4 Long-term perspectives and expectations for Swiss edu-ID

During the interviews several points emerged showing that a persistent ID could have a deeper impact on identity management and related processes at institutions. The following perspectives have been described:

- facilitation by usage of an already **enriched and verified identity**
- **easier handling of IdP/AA** with Swiss edu-ID than yet with AAI (default: exclusion of non-members in order to limit effort for configuration)
- **additional collection of attributes** from other IdPs/AAs (also outside of the university community like from schools)
- **support of directories**/lists and backchannel
- provide **services for former members** (via alumni organizations, libraries and others)
- **access to further resources & devices** with Swiss edu-ID (non-web resources)
- better/easier control of **access rights** with additional attributes
- better **service for mobility students** (decrease complexity for students)
- **user consent** for use of local attributes within **background processes** (applications) and/or specified time periods (registration for postgraduate courses, make alumni contact-data available for alma mater etc.)
- **automatic exchange** of credit data between institutions (federal funds for student credits) if still needed in the future (changes possible because of new HFKG)
- automatic exchange of certificate/diploma data between institutions
- proper **life-cycle management** of identities
- **outsourcing** of identity management
- creation of an (“institutional”) **email address** with Swiss edu-ID (ev. as part of Swiss edu-ID -> outsourcing of email)
- **unified registration process** at/for Swiss Higher Education institutions (including libraries)
- Swiss edu-ID as **single source for validated identities**

2.5 Requirements

The below listed requirements for Swiss edu-ID have been deduced from the interviews as most relevant for the current development steps:

No	Requirement	ETHZ	FHNW	Libraries	UNIBAS	UNIBE	UNIFR	UNIL	UZH
1	Uniqueness of identity granted (e.g. duplicate-checked)	**X**	x	**X**	x	x	x	**X**	**X**
2	Self-registration	**X**	o	**X**	**X**	**X**	**X**	**X**	**X**
3	Validation of e-mail address	x	**X**	**X**	**X**	**X**	**X**	**X**	**X**
4	Validation of residence address	x	**X**	**X**	o	**X**	/	x	x
5	Verification of identity (e.g. visual control of pieces of identification)	x	**X**	**X**	**X**	**X**	x	**X**	**X**
6	Verification of added or changed attributes	**X**	x	x	**X**	x		x	x
7	Import and change of attributes supported	x	x	x	x	x		x	x
8	Binding rules & process for changes of core attributes (as name, based on role)	**X**	**X**	**X**	**X**	**X**	**X**	x	x
9	Sustainable concept for Levels of Assurance for attributes	**X**		x	**X**	x	o		**X**
10	LoAs compatible with LoA standard and own IdM	x			x	x	x		x
11	Care concept for LoAs (technically supported processes)	x		x	**X**	x		x	x
12	Additional official identifier attributes (as OASI/AHV etc.)	o	**X**	o[1]	x	o	**X**	x	x
13	Additional contact attributes (like office address)	**X**	x	**X**	x		x	x	**X**
14	Additional "Portfolio" attributes (like diplomas, certificates etc.)	o	x	/	o	x	**X**		x
15	Support of local attributes	x	x	x	x[2]	x			**X**
16	Building attribute sets (e.g. similar data, with same LoA)	x			x				
17	Attribute status active/passive (detection of inactive users)	x	x	**X**	x	x	x	x	x
18	Processes for regular updates & "incentives" /information for users	x	**X**	x	o		x	x	x
19	Time stamps for attributes	x	x	**X**	**X**	x		x	**X**
20	History for attributes	x	x	**X**	**X**	**X**	x	x	x
21	Support of group management functions	/	o	/	x	o	x	/	/
22	Support attribution of access rights (with specific attributes -> basic roles)	x	**X**	**X**	**X**	**X**	**X**	**X**	x
23	Enforce user-consent for external resource access	o	**X**	x	**X**	x			**X**
24	2-factor authentication	/	/		o	x	/	x	/

[1] The important identifiers are matriculation number and ORCID; OASI can help to avoid duplicates but may increase sensibility of data.
[2] Support of local attributes by the federation is essential.

25	Levels of Assurance for authentication method enforcement	o	/		o				/
26	Legal framework	**X**	x	x	**X**	x	x	x	**X**
27	Validation rules (accepted and controlled)	**X**	x	**X**	**X**	x		x	**X**
28	Auditing of own and partner behaviour (governance)	x	x		**X**	x		x	x
29	Email provided with Swiss edui-ID (lifelong)	o	o	o	x	o	o	x	x

Table 3: Requirements for Swiss edu-ID: **X**: essential, x: important, o: nice to have, /: not required. If there's no entry the importance of the requirement is not clear.

In table 4 below is distinguished between essential, important and nice to have requirements accordingly to the ratings in table 3.

Essential (> 20 points)	E-Mail address validation
	Self-registration process
	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)
	Legal framework
	Attribute history
	Validation rules (accepted and controlled)
Important (15-20 points)	Additional contact attributes (like office address)
	Attribute status active/passive (detection of inactive users)
	Time stamps for attributes
	Validation of residence address
	Verification of added or changed 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)
Nice to have (<15 points)	Additional "Portfolio" attributes (like diplomas, certificates etc.)
	Email provided with Swiss edui-ID (lifelong)
	LoAs compatible with LoA standard and own IdM

	2-factor authentication
	Support of group management functions
	Building attribute sets (e.g. similar data, with same LoA)
	Levels of Assurance for authentication method enforcement

Table 4: Ranking of requirements (overall rating based on the following values for X: 3, x: 2, o: 1, / and no entry: 0)

2.6 Risks

Several risks have been mentioned. They should be considered and minimized as far as possible during the development phase:

- **Acceptance**: may be low because of too low benefit (for institutions and/or users) or too high effort.
- **Abandon**: orphaned accounts or deletion having impact on related services.
- **Dominance of local accounts**: may limit benefit of Swiss edu-ID.
- **Dependency**: some institutions may fear to be dependent on a central IdP (warranty is necessary that IdP will always be available) .
- **Effort**: the implementation and changes may need to many resources at institutions. The impact on local IdPs is not clear yet. A set default “open” for resources may cause a lot of effort to close them (as with AAI).
- **Privacy/Control**: transfer of too many attributes without sufficient control.
- **Responsibility**: institutions must be able to “track” users to prevent/prosecute abuse. A single institution may have to define access rules (attributes) for external services (as a company selling software for students) without having the necessary background information or resources.
- **Security**: a central IdP may increase the risk for attacks (identity theft) and may cause problems for the local resources (maintenance, down-time).
- **Trust**: institutions may not trust the information that was delivered by another organization, because verification is not sufficient or the process to validate data is not respected.

2.7 Recommendations for Swiss edu-ID development

The project in general was rated as ambitious, with a potential to replace todays solutions, but also considerable risks.

There have been some recommendations on a very general or specific level, mentioned as essential for a successful development and implementation:

- publish mid- and long-term **roadmap for Swiss edu-ID**
- further support of **Single Sign On** (as with AAI)
- **concentrate on IdM** (not on AM)
- **evaluate commercial systems** too
- **focus** on not yet existing, badly functioning and resource intensive **processes** (may also include risks)

- **enrich core processes** (do not change them)
- create **immediate benefit**
- enable **additional attributes and assurance levels**
- brace Swiss edu-ID with an **official identifier** (as OASI/AHV)
- use OASI/AHV number as non-mandatory attribute only (to avoid resulting problems)

2.8 Legal framework implications

The interview partners have been clearly aware of legal implications since they have often to adapt technical processes to changed regulations and requirements.
The legal framework of Swiss edu-ID has a central role. It defines the rules for all participants (institutions and individuals) and is therefore the base for trust building and the processes to be implemented.

The following points have been mentioned and should be described within the legal framework (between others):

Responsibilities:

1. Central IdP, AAs and users
2. Data quality
3. Validation of attributes
4. Authorities for attribute delivery (central points at institutions)
5. Community circles[3] & long-term maintenance of data
6. Provision and prevention of attribute transfer to external services (allowed and prohibited usages)
7. Identity creation for others
8. Definition of required assurance levels
9. Separation/fusion and status changes of institutions (data consistency and longevity)

Identity:

1. Minimum dataset for an identity / necessary set for registration
2. Identity validation (processes & responsibilities)
3. Prevention of duplicate identities
4. Deletion of identities & death
5. Dispute processes (claiming of identities)

Attributes:

1. Usage of Unique Identifier (delivery, protection, replacement, deletion)
2. Definition of mandatory and non-mandatory attributes (rules, control)
3. Usage of OASI/AHV number as attribute (ev. delivered by central IdP)
4. Delivery of additional attributes, also of confidential and financial data as remaining federal subsidies for students

[3] Circles of partners within the federation community with different duties and rights

Users:

1. User rights & duties (later validation of attributes, corrections, privacy etc.)
2. Information of users (attribute transfer, changes, user-consent)
3. Traceability of users

3 Reports per Institution

Chapter 3 is not for public distribution. It is restricted to the target audience: University staff, library staff, members of the Processes working group.

Confidentiality Notice:

This is the public version of the Processes working group report without internal information of the institutions of the working group members. The full version of the report is community confidential and for personal use only. It is not allowed to give away or further distribute the full version of the report.

Members of the SWITCH community can request a copy of the confidential version from the Swiss edu-ID project group at http://projects.switch.ch/eduid/contact/

The public version of this report can be downloaded from the Swiss edu-ID website at http://projects.switch.ch/eduid/documents/

Annexe

Interview questions

The following questions will be used as guidance for the interviews. The questionnaire is neither exhaustive nor must all questions be discussed (e.g. if questions have been already answered or if they have no relevance for the specific case).

*Questions we rate as essential are marked **bold**.*

A. Identity Management System & User administration

1. What IdM or IAM system is used at your institution? Is it a central one or has it distributed components? What is the base (LDAP, Active Directory, AAI, …) ? What interfaces to the IdM exist?
2. Is an IdM redesign planned or already under construction? What's the roadmap for it?
3. How are users entered, administered and deleted? Which units are involved?
4. What roles are used within the system?
5. How are user data/attributes recorded and used? Which ones are essential for access rights to resources?
6. **How are matriculation numbers created, recorded and validated? (new registration, re-registration, multiple registrations, checking of degrees etc.)**
7. Who is responsible for data quality?
8. How is the procedure if a part of the data is missing?
9. How is the procedure for later mutations of user data?
10. How are data and privacy protection regulations handled?
11. How long and where is user data stored? When/why will they be deleted?
12. How is user data made available and usable?

B. Process and possible synergies

(Choose a process you think could have the potential for a larger benefit at your institution when it will be implemented with Swiss edu-ID)

Current process

13. **For which service and process do you expect a possible improvement/ simplification by using Swiss edu-ID?**
14. **What is the goal of the process?**
15. **How does the process currently look like? What are the process steps (for users, staff, systems etc.). Are there usable process descriptions available (documentation, flow diagrams, manuals, etc.)**
16. **Is the process described/covered within legal documents/regulations?**
17. Which interfaces to the IdM are of relevance?
18. What is your role within the described process?
19. Who is responsible for planning and execution of the process? (units, people)
20. Who else is involved in the process? In which roles?
21. Are there preconditions for the process execution? (side user or institution)
22. How is the process supported ? (technical assistance, support)
23. Is the process lineally (without interruptions/media breaks/time delays/unit breaks) or does it include breaks or workarounds ?
24. Which problems appear in relation to this process ? (sporadically, repeating, small or big extent)
25. Which requirements are not fulfilled with the process (yet or in the future) ?

26. Are changes of the process planned already (without Swiss edu-ID) ?
27. Are there specialities at your institution that distinguishes the process from what other institutions are doing? Is it unique or are there institutions with similar processes?

Future process

28. **How would the process look like ideally in the future? (with or without Swiss edu-ID)**
29. **Where should Swiss edu-ID join exactly to generate a real benefit for your institution?**
30. **What changes of the process could solve current problems when using Swiss edu-ID in the future?**
31. What are your safety requirements/security levels to be supported? (kind of authentication, 2 factor authentication etc.)
32. **What are the requirements for data quality and validation (levels of assurance etc.)**
33. **What are new requirements that could evolve with the usage of Swiss edu-ID? (data storage, restore etc.)**
34. **What would be the time frame for an adaptation of the process(es)/integration of Swiss edu-ID ?**

C. Possible implementation of Swiss edu-ID

35. **Is the process a possible candidate for a pilot or early implementation of Swiss edu-ID ?**
36. Who must be involved in the planning and who will decide if a pilot will be done?
37. Which other processes would be also affected?
38. How does the time frame look like for an implementation (forerun, legal clarification, process changes) ?
39. Is a funding by SUC P-2 possible/ necessary? (pilot or productive implementation)
40. What will be the effort/necessary resources?
41. **Would the institution be a possible candidate for an Attribute Provider pilot ?**