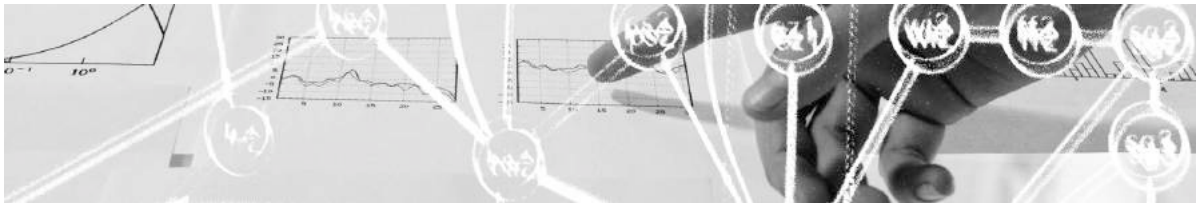
SWITCH

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

Swiss edu-ID High-Level Architecture



Omar Benkacem (Université de Genève), Kai Blanke (Universität St. Gallen), Rolf Brugger (SWITCH), Matteo Corti (ETH Zürich), Mario Gay (Università della Svizzera Italiana), Dieter Glatz (Universität Basel), Christoph Graf (SWITCH), Christopher Greiner (Université de Lausanne), Wolfgang Lierz (ETH-Bibliothek Zürich), Petra Kauer-Ott (SWITCH), Roberto Mazzoni (Universität Zürich), Christian Tschudin (Universität Basel)

Document Type:	Documentation
Version:	V1.0
Created:	10.07.14
Last changes:	24.07.14
Classification:	Public

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

Content

1 Management Summary

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.

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. 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.

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.

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.

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.

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.

Stakeholder groups will refine the operational framework of the Swiss edu-ID on the basis of this high-level architecture from mid-2014 to mid-2015 and set the cornerstone of the next version V2.0 of the Swiss edu-ID and beyond. Version V2.0 will allow participating organisations to enrich the user

attributes and thus make Swiss edu-ID identity 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 set-up of the initial version of the Swiss edu-ID service and refining the operational framework with stakeholder groups is covered by the first P-2 call project “Swiss edu-ID”. Follow-up projects (preferably within the scope of P-2) will be initiated to implement the subsequent steps in this roadmap.

2 Scope of this Document

The intended audience of this document is the management at organisations of the SWITCH Community in general, and in particular those tasked with identity management as well as integrators of identity management solutions in their services.

This report describes a high-level architecture of the envisaged future identity management solution of the SWITCH Community. It is well understood, that collaboration does not stop at national borders. Special care is taken to stay open to future developments to scale internationally and not to introduce incompatibilities with emerging trends and solutions elsewhere.

This documents aims at covering not just minimal requirements but also optional, useful elements.

The remainder of this document is structured as follows: Chapters 3-5 describe goals of and frame for a new identity management solution as well as basic concepts in a generic way and with a perspective beyond the next ten years. Chapter 6-8 introduce trust, roles and governance principles being relevant for identity management services for the SWITCH Community within the next five to ten years, and finally chapter 9 elaborates the rough specification of the Swiss edu-ID architecture that should be realized during the next five years.

3 Terms and Definitions

Generally accepted definitions for the concepts used in this document do not exist. We tried to settle on definitions based on terminology from the common language in a rather pragmatic approach.

3.1 Identity related Key Definitions

Digital Identity: Digital identity is the data that uniquely describes a person or a thing (subject) and contains information about the subject's relationships.

Subject: A person or thing that is being discussed, described or dealt with. In our context, the subject is usually a human individual also referred to as user.

Attribute: A single piece of information associated with a digital identity.

Identity Management: Identity management is the task of managing information (attributes) about users over the lifetime of the digital identity.

We can think of a digital identity as a container belonging to a specific user. It is filled with a number of attributes containing information about the user it refers to. The goal of identity management is to keep the information in the container up-to-date.

3.2 Organisational Context related Key Definitions

SWITCH Community: The SWITCH Community comprises the following categories of Swiss organisations [1]:

- Cantonal universities
- Federal institutes of technology (ETH)
- Research institutes of the ETH domain
- Universities of applied sciences
- Universities of Teacher Education
- Swiss Federal Institute for Vocational Education and Training (SFIVET)

Federation: A collection of organisations that agree to interoperate under a certain rule set.

Interfederation: Interconnection of services across the boundaries of their respective identity federations. The main goal of interfederation is to extend the user community.

The primary focus in this document is to best serve the SWITCH Community and to define an appropriate rule set for that purpose. The SWITCH Community may form a federation accepting additional organisations willing to collaborate under the rule set defined by the SWITCH Community. Connecting to services in other federations will not be covered by the federation's rule set, but by a more relaxed interfederation rule set.

4 Introduction

4.1 Main Goals

4.1.1 Vision of the Networked Individual

Technology is driving the change from yesterday's locally rooted individuals to today's networked individuals [2]. It allows for increased mobility in many ways: while the physical transportation systems allowed us to travel greater distances in increasingly shorter time or at lower cost, the Internet empowered us to virtually travel anywhere, anytime and on-demand. Mobile devices enhance the notion of “anytime” drastically and social networking allows you to stay in close virtual touch with globally distributed groups. This affects our relationships, which tend to become more global, more fragmented, more on-demand, looser and long-standing social arrangements less influential.

It also gives rise to another trend: lifelong learning. Education used to be a one-time relationship of several years with one specific educational organisation, followed by an employment period making use of the skills acquired during that time. Nowadays, acquiring skills becomes more need-driven, on-demand and overlapping.

Other things do not change that much: While we often want to reveal who we are, sometimes we prefer to stay anonymous or to hide behind a pseudonym, and on other occasions, we need to prove

who we are. While the physical world has its shortcomings with offering anonymity, user-friendly processes exist to prove who you are (e.g. by showing your passport). The Internet has a particular strength offering relative anonymity (debatable in post-Snowden times), but a weakness when it comes to disclosing your identity to others in a trustworthy manner.

4.1.2 The Role of Identity Management

Digital identities and identity management are here to overcome this weakness by exchanging attributes about subjects (users) in a trustworthy framework (e.g. the one of a federation) or even reaching beyond with the help of interfederation. At the same time the user gets empowered to chose between disclosing or hiding its identity - and maybe even the option of choosing something in between.

4.1.3 Shortcomings, current Issues

It is exactly for the purpose of solving the identity problem of the SWITCH Community that SWITCH started to develop the AAI framework back in 1999. In 2013 almost all organisations in the SWITCH Community run SWITCHaai identity providers (currently over 50 instances) and offer to almost all of their affiliated users a SWITCHaai account (currently more than 390'000 account holders). A steadily growing number of services (currently more than 700) support the SWITCHaai authentication and authorisation framework.

The current success cannot hide the fact that there are some important shortcomings in the way SWITCHaai is set up:

- Digital identities of individuals are linked to the membership with a specific organisation of the SWITCH Community. Digital identities are created when such a link is established and usually destroyed when the link disappears. Thus, in the case of an individual changing university or employer, the former identity is lost and a new one created.
- Digital identities are mostly restricted to individuals who are a member of an organisation of the SWITCH Community. Therefore, it does not well support trusted interactions with external parties, e.g. in the context of project collaborations.
- In the context of life-long learning with concurrent, overlapping, intermittent relationships with educational organisations, this results in digital identities being created and destroyed many times, which is on the one hand an extra burden for the user, but also a potential for efficiency gains.
- Creating digital identities from scratch has the additional disadvantage that the multiple identities created for the same individual do not relate to each other.
- There is no support for services addressing individuals for periods extending beyond the relationship with a particular organisation, e.g. e-portfolio services.
- There is insufficient support for non-web resources and mobile applications.
- Multiple concurrent affiliations (quite common for researchers and lecturers) produce multiple, concurrent, unlinked and often unliked identities.

4.1.4 Expected Benefits

Benefits for end users:

- Changes to personal attributes only have to be made in one place, even in the case of multiple roles at different organizations.

- Identity management is no longer tied to a specific role at a specific organization. As a result, people do not lose their identity when they move to a different organization, and no parallel identities are created for people who perform multiple roles at the same time.
- Support for collaboration with partners no longer depends on the organization(s) they are member of.
- Increased usability compared to the existing AAI by integrating non-web-resources and supporting mobile environments.

Benefits for university administration and operators of identity management systems (IT services and SWITCH):

- Administrative processes can be streamlined, as personal data already recorded earlier might be re-useable in new cases. This also reduces the effort required to keep personal data up-to-date.
- In many cases, external people involved in collaborations no longer need to be added into an organization's own identity management system.
- The operation of inter-organizational platforms is simplified because collaboration partners with no direct link to an organization can also sign up for a Swiss edu-ID identity. Maintenance of guest accounts or alternative identification procedures becomes obsolete.
- Universities get a cost-effective way to extend their services to non-web-resources and mobile environments

Benefits for service providers:

- Services enhance their administrative efficiency due to outsourced identity management.
- Services can rely on high quality user information.
- Service providers can rely on a future proof infrastructure offering new interfaces (e.g. non-web-resources and support for mobile environments).

4.2 Scope

The Swiss edu-ID service mediates between individuals in their role as users and organisations offering services to their respective user base. The scope of the Swiss edu-ID service is best described by defining the scope of participating individuals, organisations and external digital identities.

The Swiss edu-ID service is managing digital identities of human individuals - especially those who are members of an organisation within the SWITCH Community, but extending to all individuals interacting with those institutions. These individuals are hereafter called users.

Organisations offering services under the umbrella of the Swiss edu-ID service are primarily member organisations of the SWITCH Community. Other organisations may join, if the SWITCH Community perceives their contribution beneficial.

The Swiss edu-ID service is not offering digital identities exclusively, other digital identities managed elsewhere may prove to be of value to the SWITCH Community (e.g. ORCID, SuisseID etc.). The linking of external identities to the Swiss edu-ID identity is foreseen, provided the SWITCH Community perceives them as beneficial.

4.3 Relevance for Higher Education in Switzerland

New, emerging services - like the ones envisaged in projects like CUS P-2 - are currently lacking support for covering all relevant stakeholders and need to take provisions to cover important identity management tasks themselves. This may lead to situations, where promising services are not being developed in the first place.

With its aim to

… cover all users that are relevant to Swiss higher education institutions including students, local and foreign researchers, walk-in clients, further education students and staff,

… cover all national higher education institutions that are part of the SWITCH Community and facilitating their identity management duties, and allowing to include other organisations of relevance to the SWITCH Community,

… linking all relevant external digital identities,

the Swiss edu-ID is a solid identity management framework enabling the development of new services.

4.4 Use Cases

Researcher's ORCID: Researchers at a Swiss university have a ORCID associated with their Swiss edu-ID identity. With their ORCID, the researchers are uniquely identified as authors of scientific publications. This is particularly useful when uploading new publications to institutional or inter-institutional document repositories, when applying for research grants, or when generating publication lists for reports and citation indices.

With the ORCID as an attribute of the Swiss edu-ID identity a researcher does not have to re-link it to new accounts when he/she leaves or moves between universities. Moreover, the technical integration with orcid.org (verification, mutations etc.) has to be implemented only once at the Swiss edu-ID identity provider.

Student's learner identification: Students who are registering at a university for the first time need to obtain a Swiss edu-ID identity that allows them access to all relevant student services like: LMS, e-portfolio, library, download of learning material, submission of term papers. The student is able to access Swiss edu-ID service enabled services at partner universities. The student keeps the Swiss edu-ID identity after graduation, and has limited access to some previously used services like e-portfolio or libraries, and gains access to new services like alumni platforms or job/career services.

When the user re-registers at a later time at another Swiss university the Swiss edu-ID identity is used to grant access to the learning and administration services. The Swiss edu-ID identity is persistent and gives access to services that are relevant for life-long learners like: management and development of the personal competence profile, maintain the professional social network, manage publications, learning material, diploma and certifications.

Without a Swiss edu-ID identity, the student can keep track of previously used services only with difficulty, and they have to re-register whenever they use services at another university.

Alumni: After graduation and exmatriculation the user's status is automatically updated in the Swiss edu-ID network to alumnus of a particular institution. The user can then access alumni resources provided by universities, alumni organizations and other institutions.

The benefit for the user is an uninterrupted access to personal resources with the same account used during the studies, while organizations providing services for alumni can rely on up-to-date profile information of users.

Physician's further education: Physicians who are employed at a university or hospital have access to e-publications and other educational resources. Self-employed physicians who were previously affiliated with a university can be granted access to the same resources based on their persistent affiliation history or attribute history.

With the Swiss edu-ID identity physicians can continue to access further education and other relevant services even after they have left the university. Service providers trust the authentic attributes of Swiss edu-ID identity owners and rely on them to manage access to services.

Researcher's Umbrella Account: Umbrella is a federated identity system for the users of the large neutron and photon facilities. Users of such facilities get an Umbrella account. It provides them a unique and persistent user identification, giving pan-European access to the local web resources at the facilities. Through the European wide single-sign-on Umbrella service users have access to: user beam time, user proposals, user experimental data, data archiving, as well as data analysis centres at the research institutes. With the Swiss edu-ID identity carrying the Umbrella-ID as attribute, users can access Umbrella resources at institutions that support this feature.

Library access for university members and walk-in clients: To access library services patrons need a Swiss edu-ID identity. Patrons can self-register a Swiss edu-ID identity if they don't already have one. After verification of attributes required by libraries and provided the access policy criteria are met a patron is granted access.

The benefit for the clients is a simpler unified access to all Swiss libraries with public services, allowing for increased mobility for studies and jobs. Libraries can provide cooperative services more easily: they simplify their administrative processes and become ready for the future. Libraries are relieved of some identity management processes.

Authenticating university members with their cloud identities: Users have the possibility to link their identities of other identity providers to the Swiss edu-ID identity. If the external identity is sufficiently assured a user can log in with a 3rd party identity to access to Swiss higher education services.

Access to cloud resources for university members: Users have the possibility to link the Swiss edu-ID identity to services beyond the Swiss higher education community such as cloud resources. This gives users with the Swiss edu-ID identity access to 3rd party cloud resources.

Unified identification of lecturers: Lecturers at a university have a unique Swiss edu-ID identity based login for all of their other roles (teacher, staff, student) and employments (university hospital, university staff, faculty, library). All access to teaching, learning and administrative services is done with a single account/login.

4.5 Roadmap

A centrally managed identity management system installed in 2014 allows users to get a long-lived Swiss edu-ID Version 1.0 identity starting 2015. It will primarily serve these two use cases:

- Students that are about to lose their existing SWITCHaai account in the near future can set up a long-lived Swiss edu-ID identity. They will thus safeguard some capabilities of their existing SWITCHaai account, serving in particular the “Alumni” use case above.

- Individuals without a strong affiliation with an organisation in the SWITCH Community can currently not get a SWITCHaai account, but will get the option to register a long-lived Swiss edu-ID identity.

Even though those identities still lack important features (like integration into the existing SWITCHaai identity management) they can be used straight away for services with limited requirements, e.g. library access or ORCID linking and will automatically profit from added functionality available in future versions of the Swiss edu-ID.

Stakeholder groups will define the operational framework of the Swiss edu-ID Version 2.0 on the basis of this high-level architecture from mid-2014 to mid-2015. This is to prepare for the integration with the existing SWITCHaai identity management and to explore in more detail additional opportunities like major updates or redesigns of student registration processes.

The activities mentioned above are covered by the first P-2 call project “Swiss edu-ID”. Follow-up projects (preferably within the scope of P-2) will be initiated to implement the subsequent steps in this roadmap.

The implementation of this operational framework by the end of 2015 will greatly enhance the long-lived Swiss edu-ID identities and make them functionally equivalent to SWITCHaai accounts starting 2016 for users affiliated with participating universities. An important infrastructure precondition is given, so that services or projects can act to implement the remaining use cases. Furthermore, universities no longer need to issue their own identities, but can choose to rely on centrally provided identities and derive technical accounts within their respective organisations from Swiss edu-ID identities.

The main focus in the years 2017 onwards is supporting new services or adopting existing services to make full use of the new capabilities. This will also include implementing renewed student registration processes together with all relevant stakeholders as initially described in the operational framework.

5 Basic Concepts of a Digital Identity

5.1 The Subject

The definition of digital identity, which we are adhering to, is quite open with regards to its applicability to the type of subject. It allows for a wide range, e.g.:

- Identities of individuals
- Identities of objects and processes
- Identities of organisations, e.g. to describe the roles of universities in the context of education and research
- Identities of groups, e.g. of a project, where several individuals collaborate around a specific topic
- Identities of things, e.g. of machines for authenticated machine-to-machine interactions (Internet of Things)

In the context of the Swiss edu-ID, we will restrict ourselves to digital identities of individuals. Other subject types are for future consideration only and not elaborated further in this document.

5.2 Parts of the Digital Identity

Digital identities are collections of several types of data about users [3]:

- inherent attributes, which will never, or only rarely, change: e.g. date of birth, first and last names
- acquired, objective attributes, which will usually change over time: e.g. organisational affiliations and roles, communication channels
- personal preferences: e.g. nicknames or preferred communication channel

The Swiss edu-ID identities will consist of the following parts:

- Basic attributes residing outside of the organisational context of the user (inherent attributes and preferences): attributes like name, address, communication channels or personal preferences
- Role attributes describing the organisational context of the user (mainly acquired attributes): typically, those attributes document a current or former affiliation or role with an organisational member of the SWITCH Community
- Linked digital identities establishing the link to other digital identifiers or identities belonging to the same user (mix of acquired attributes and personal preferences): e.g. ORCID

The basic attributes serve the purpose to anchor the link between the individual and the Swiss edu-ID identity and to enable interaction. The basic attributes will usually not be influenced by (changing) organisational roles or affiliations of the user. By far the most important set of attributes for service authorisation purposes are the role attributes. They will be provided by participating members of the SWITCH Community, in particular by Swiss universities. They will change whenever the user is changing roles within organisations or changing affiliations. Linked digital identities enrich the set further.

5.3 Identity Domain

The identity domain describes the validity domain of a digital identity. These two examples show the possible range:

- A local identity is used in closed environments only, typically restricted to within the context of a single organisation or specific to a single service.
- A global identity is intended to act as overall identity or “digital passport”, used to identify entities in a broader, universal context.

The Swiss edu-ID is to be positioned in between: it is the identity solution for and by the SWITCH Community, but it is aiming at gaining acceptance within the research and education sector worldwide.

5.4 Identity Management

Identity management supports the intentional use of identities to assure access and traceability of use of services, resources and systems throughout the entire lifecycle of the identities being managed.

5.4.1 Identity Lifecycle

The Identity Management lifecycle starts with the creation of an identity (provisioning), followed by storing and sharing the identity data (propagating). Now the identity can be utilised actively (use). Changes of roles or assignments may be necessary (maintenance). If an identity is no longer necessary it will be removed (deprovisioning).

The lifetime of such an identity may be rather short-lived, e.g. linked to a specific episode of the subject's lifetime for identities linked to a specific role, or it may be designed to cover or even extend beyond the lifetime of the subject for a user-centric identity.

The Swiss edu-ID identity is designed to support at least the period between first interactions with organisations of the SWITCH Community (this is often the case when entering tertiary education) to as long as interacting with the SWITCH Community remains relevant to the user. Extending beyond the lifetime of the individual might be required for archival services.

5.5 Trust, Privacy and Security

A common understanding and acceptance of important quality aspects within the validity domain of an identity is of ultimate importance. Other services will rely on the attributes related to those identities for their authorisation decisions. Sharing user attributes has data privacy implications, which require adequate security of systems and processes involved, but will only be acceptable in a sufficiently trusted environment.

Solving trust, privacy and security issues for service offerings within the SWITCH Community are key for many services of SWITCH and the Swiss edu-ID can draw from the experience built up.

6 Trust, Privacy and Security Principles

6.1 Trust Framework

Trust within the Swiss academic community is based on the traditionally strong solidarity between Swiss universities as well as the loyalty of their members and former students. The establishment of the SWITCH foundation in 1987 is a result of this trust. The statutes and regulations of SWITCH formalise this trust relationship within the SWITCH Community, which will serve as the foundation for the Swiss edu-ID as for any other SWITCH service.

The Swiss edu-ID trust framework (i.e. a common set of rules and standards) will inherit as much as possible from the trust framework of the existing SWITCHaai service, which itself is based on the trust framework in the SWITCH Community.

6.2 Attributes

Information about users is provided in form of attributes. Attributes may originate from multiple sources.

The Swiss edu-ID service prefers sources capable of providing attributes authoritatively. The most important source are the members of the SWITCH Community themselves, e.g universities providing attributes about their students and staff members.

In other cases, attributes need to be validated against authoritative sources (e.g. instead of accessing the authoritative database of the residents registration office, the name of a user can be copied from a derived official document like an ID card).

6.3 Controlled Attribute Release

Typically, the sum of all attributes of a user will reveal a great deal of his/her personal life. As a measure to protect the privacy of users, only limited sets of attributes are made available to requesting service providers.

Generally, service providers should only ask for and only get access to attributes that are required for offering the specific service.

For the Swiss edu-ID infrastructure processes are needed to define access rules to attributes. Two basic principles are applied:

Institutional contracts: Explicit user consent for attribute transfer is not needed provided contractual rules under control of Swiss edu-ID that ensure that service providers will only ask for and will only get a reasonable set of attributes.

User consent: When connecting to services not covered by such rules under the control of the Swiss edu-ID framework, the transfer of attributes will only take place after explicit user consent.

6.4 Anonymity and Pseudonymity

Many services do not require personally identifiable information about their users. In a pseudonymous approach a service provider is still able to recognize a returning user, while in an anonymous approach the link to a specific person is completely lost.

The Swiss edu-ID service supports pseudonymity whenever a service requires only attributes with no personally identifying information. This is a very common scenario. Fully anonymous use of a service is no design goal of Swiss edu-ID.

6.5 Identity Vetting

Before a new user can use the Swiss edu-ID infrastructure that person has to be initially linked to his/her digital representation. Possible approaches for the initialization are self-registration of the user, or copying user information (attributes) from external sources.

The user accesses the data of his/her digital representation by means of secret credentials.

Curation processes are to be defined to

- validate person who is linked to digital representation
- add and delete attributes
- validate attributes
- elevate or decrease the level of assurance of attributes
- merge duplicate accounts

6.6 Levels of Assurance

The level of assurance LoA determines to which degree a specific piece of information can be trusted. We distinguish the two aspects:

Attribute LoA: Determines to which degree attribute information is correct, complete and up-to-date. The LoA may vary over time. It can be increased by validating attribute information, and it decreases when the attribute information becomes obsolete. To maintain the LoA of attributes, they may need to be periodically revalidated.

Authentication LoA: This is the degree of certainty that a user is the person he/she claims to be.

Services have varying expectations towards the quality of attribute data and may depend on LoAs to achieve their intended service quality.

6.7 Authentication

Authentication is the process of securely identifying a person.

Depending on the LoA different authentication processes may be applied. They vary from simple authentication with low LoA to extensive authentication (i.e. multi-factor) with high LoA.

In addition to authentication taking place on the Swiss edu-ID platform, a 3rd party authentication service that is linked to the Swiss edu-ID identity of a user may be used to identify that user.

6.8 Security Considerations

Swiss edu-ID targets a trusted and high quality service. To ensure overall security, all stakeholders in particular the Swiss edu-ID operator and the attribute authorities are required to adhere to specific security policies.

At the system level, the operator and the attribute authorities make sure that the infrastructure is available and reliable. The systems are protected against data theft and data tampering.

At the user level policies and processes have to be defined for business transactions like:

- recovery of lost identities and credentials
- updates of attribute information
- handling incidents like identity theft
- handling disputes
- handling deceased users including verification of death record and dealing with succession rights

7 Stakeholders and Roles

7.1 The User

When trying to connect to certain services offered by service providers, the user may be required to own a Swiss edu-ID identity.

When setting up such a digital identity, the user is responsible for providing correct information about himself. It is in the user's best interest to keep this information up-to-date during the entire lifetime of the digital identity. Some of this information (i.e. passwords) the user must keep secret.

The Swiss edu-ID operator may ask the user for explicit consent to transfer information about the user, which is stored at the Swiss edu-ID operator or at attribute authorities, to service providers.

7.2 Attribute Authorities

Attribute authorities maintain and pass on information about users to the Swiss edu-ID operator and service providers.

Attribute authorities are responsible towards the users, the service providers and operator for providing only correct and up to date information about users. They need to maintain agreed quality standards, which includes appropriate security levels for information processing systems.

7.3 Service Providers

Service providers offer services to their user base.

Service providers may get attributes about users accessing their service from the Swiss edu-ID operator and attribute authorities. Service providers may use attributes received solely for the purpose of authorising users and providing the service to them. Furthermore, they may only request required and desired attributes needed for those purposes. It lies entirely within the responsibility of the service provider to grant or deny access to individual users.

7.4 Swiss edu-ID Operator

The Swiss edu-ID operator runs services to support the interactions between users, attribute authorities and service providers.

It runs the following services on behalf of the respective stakeholder:

Users: The operator offers user-friendly interfaces for identity management tasks, validation processes for basic attributes, authentication processes and linking of external identities. The operator also implements processes to recover lost identities, and to handle incidents and disputes as described in chapter 6.8.

Attribute authorities: The operator offers interfaces for making attributes available to the operator or service provider about users trying to access their services. Furthermore, interfaces may be established to directly exchange user information between an attribute authority and the operator. Direct user data exchange can be necessary for identity provisioning at attribute authorities, or to copy, cache or archive user data at the operator.

Service providers: The operator offers interfaces and methods to service providers for receiving attributes about users trying to access their services. The operator also implements the admission policies and registration procedures for service providers.

The operator may also be tasked to define, manage, control and enforce the rule sets and policies of the relevant identity domain with a particular view on adhering to data protection principles.

8 An Identity Management Service for Swiss Higher Education

The Swiss edu-ID service aims at securing digital interactions between users and services of member organisations of the SWITCH Community and beyond, whenever those interactions rely on additional, trusted user information the service requires to authorize access.

The Swiss edu-ID service will focus on identities of users. Extending the service to also cover group identities, organisational identities or machine and process identities are subject to further studies only.

The existing trust framework of the SWITCH Community, as laid out in the statutes of SWITCH and derived regulations, form the foundation for the Swiss edu-ID service.

The Swiss edu-ID is rooted in Switzerland, but aiming at global acceptance.

Wherever possible, the Swiss edu-ID will reuse existing service elements of the SWITCHaai.

8.1 Swiss edu-ID Service Participation

The Swiss edu-ID is a framework for the Swiss higher education sector, governed by the SWITCH Community. While all organisations of the SWITCH Community are automatically eligible to become part of the framework, third party organisations may only enter this framework if they are perceived to add relevant value to the SWITCH Community. The following participation categories exist:

Swiss edu-ID member: Membership is restricted to member organisations of the SWITCH Community. They govern the Swiss edu-ID service through the governing structures of SWITCH. Swiss edu-ID members are entitled to operate services within the framework of the Swiss edu-ID and to act as attribute authorities. Example: a university in Switzerland.

Swiss edu-ID user: Any individual may become a user, but the main focus is on individuals with a strong relationship to one or more Swiss edu-ID Members. Examples: a student, an alumnus.

Swiss edu-ID partner: Any organisation is eligible to become a Swiss edu-ID partner, but needs passing an approval process based on the perceived value to the SWITCH Community. Swiss edu-ID partners are entitled to operate services within the framework of the Swiss edu-ID, but they have to adhere to Swiss edu-ID regulations for partners. Swiss edu-ID partners may optionally act as attribute authorities. Examples: a software vendor, a publisher, a cantonal library, a university hospital.

Swiss edu-ID interfederation participants: This category covers organisations registered with a federation outside of Switzerland for which an interfederation arrangement exists. Swiss edu-ID interfederation participants are entitled to operate services within the framework of the Swiss edu-ID. They adhere to interfederation regulations. Example: a university in Norway.

8.2 Business Model

The service value of the Swiss edu-ID is assessed in several stages of a presumed typical identity lifecycle on purely qualitative grounds in chapter 8.2.1. Where appropriate, we compare the anticipated situation of a rolled-out Swiss edu-ID service with the current situation with the existing SWITCHaai service. Chapter 8.2.2 summarises key findings, which lead to the proposed financing model in chapter 8.2.3.

8.2.1 Service Value Considerations across Identity Lifecycle

In a presumed typical Swiss edu-ID service usage scenario, a prospective student at a Swiss university will initially create a Swiss edu-ID identity as part of the university enrolment process. This identity is then used throughout a typical career scenario:

Pre-study: Universities offer an enrolment process to prospective students. By using the Swiss edu-ID, they can rely on a pre-established user identity with verified attributes like email, phone number or postal address, thus simplifying the enrolment process of the university.

Study period: The student uses the Swiss edu-ID service for the day-to-day interactions with the IT services offered by the university for studying. The university still has to maintain up-to-date information about all their students and thus enriches the Swiss edu-ID identity. But the university benefits from reduced identity management efforts and no longer needs to operate access management services, where growing demands are expected in the future (e.g. mobile support, non-web-browser access).

Becoming alumnus: Alumni organizations are relieved from re-collecting and maintaining personal information like contact data and can focus on their genuine networking tasks. Universities are interested in maintaining the contact with their former students.

Job seeking: Protected by user consent, users could easily provide high quality profile data to the job market. Recruiters benefit from a focused access to qualified job seekers in a secure environment.

Researchers: Universities benefit from research-specific attributes like ORCID and increased support to access non-Web resources. Since all people interacting with universities may get a Swiss edu-ID identity, no special arrangement need be made to accommodate external project collaborators or foreign researchers.

Further education: Private or public further education institutions can more specifically address their audience. Their identity management processes are simplified at registration, and during the courses users can continue to use their preferred learning and collaboration tools.

Overall educational career: Universities can trace the history of students and use the information to build and update a Student-CRM (Consumer Relationship Management)

8.2.2 Service Value Summary

- In all stages, the universities are facing increasingly important identity management challenges: linking of existing identities, providing services to users without affiliation to universities, optimizing registration processes, keeping in touch and providing services to alumni and life-long learners etc. With Swiss edu-ID the universities benefit from an effective and sustainable solution to these challenges.
- Some of the benefits can only be achieved if the complete user base can be migrated to the Swiss edu-ID service.
- The reason for the user to create and maintain its identity and to interact with the identity management system is purely motivated by the wish to access interesting services.
- No specific benefits to the Swiss edu-ID operator are identified above.

8.2.3 Financing Model

Main principles:

- Since achieving a complete coverage of the user base is important for the benefits to the universities, it is proposed not to charge the users for basic identity management.
- Since the Swiss edu-ID operator is not itself a beneficiary of the service and yet covers substantial efforts, it should get paid for the services offered.
- The main service beneficiaries are the universities and third parties.

Proposed approach:

- The Swiss edu-ID operator (SWITCH) and the universities have to agree on a cost-sharing model for the service operation efforts within the governance structures of SWITCH.
- A service charge to users is not recommended at the initial stage of the service.
- A service charge to third parties is an option to consider.

8.3 Service Operation

SWITCH will act as operator of the Swiss edu-ID service: SWITCH is responsible for operating all central components of the Swiss edu-ID service, orchestrating the collaboration of all parties contributing to the Swiss edu-ID service, maintaining and enforcing all relevant standards and concepts and further developing the service and its policy framework in close collaboration with the SWITCH Community.

8.4 Governance

The Swiss edu-ID is a service of SWITCH and all governing structures in place to govern SWITCH services are applicable to the Swiss edu-ID as well. This includes in particular service related tasks like:

- Yearly review of all SWITCH services by the SWITCH foundation council based on key indicators
- Approval of next year's budget, including cost estimates of individual service groups

To better steer SWITCH services with complex stakeholder constellations, SWITCH often sets up long-lived stakeholder groups with specific mandates. In the case of the Swiss edu-ID service, the stakeholder groups established for the SWITCHaai service will - where reasonable - receive an extended mandate to cover aspects of the Swiss edu-ID. The following long-lived stakeholder groups are foreseen during the start-up phase of the Swiss edu-ID:

- The existing AAI Advisory Committee will be extended to cover service strategy aspects of both SWITCHaai and Swiss edu-ID
- The existing AAI Attribute Taskforce will be extended to provide guidance on both SWITCHaai and Swiss edu-ID

This takes into account, that both SWITCHaai and Swiss edu-ID need be further developed in a coordinated fashion. SWITCH will decide - in close consultation with the SWITCH Community - on the establishment of additional consultation groups as seen fit for the purpose at any time.

8.5 Risks

The following risks were identified and measures proposed:

Acceptance problem of a centralised solution: Both, the existing identity management solution SWITCHaai and Swiss edu-ID are based on a decentralised model, whereas the Swiss edu-ID is

centralising certain elements. This may lead to acceptance problems and as a consequence to low take-up by universities. To counter this risk, the involvement of identity managers at Swiss universities will be sought in all stages of development of standards and services.

Difficulties to validate users initially: validating user information in an automated process is not well supported by e-Government processes in Switzerland and alternative solutions must be found. SWITCH will seek expert advice on this topic.

Integration problems with business processes within universities: Changing key processes - like student registration - is complex and time consuming. To give enough lead time, addressing student registration opportunities needs to start as early as possible (stakeholder group phase).

Too low coverage of users (acceptance issue): One promise of the Swiss edu-ID is to allow service providers to settle on one identity management solution only. If users are not willing to sign up for a Swiss edu-ID identity, this will question this promise. SWITCH will have to carefully monitor acceptance level to be able to address such issues in time.

Low number of available resources for former students: In order to be motivated to actively use and maintain their Swiss edu-ID identity, alumni will need to have access to a set of attractive services. The adoption of the Swiss edu-ID by service providers should be increased by improving technical support and by providing models for simplified administrative processes.

Challenging mobile integration: The integration of the Swiss edu-ID on mobile platform is technically demanding. A clean integration depends on future developments of the manufacturers of mobile platforms and mobile apps.

9 The "Swiss edu-ID" Architecture

We can single out the main components of the Swiss edu-ID in the following way, which holds equally true for the existing SWITCHaai service:

- Identity provider
- Attribute authority
- Service provider

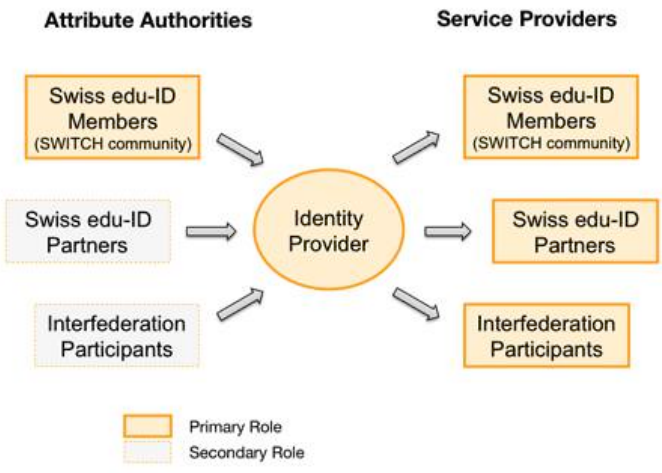


Figure 1: Swiss edu-ID stakeholders and flow of attributes

In short, a service requiring additional information about a user will connect to the appropriate identity provider in order to learn how to get the missing information from attribute authorities. The architecture of the Swiss edu-ID explained in this chapter orchestrates the interplay between these components.

9.1 Evolving from the SWITCHaai Architecture

SWITCHaai and the Swiss edu-ID share many concepts, components and policies. While the role of service providers and attribute authorities remains largely unchanged, the single most important change affects the now centralised identity provider component and it therefore receives increased attention in the subchapters following this one. This table shows the main difference on a rather abstract level:

	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 identity provider)	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

9.1.1 Architecture comparison between SWITCHaai and Swiss edu-ID

The main reasoning for leaving roles unchanged or introducing change are the following ones:

Identity provider: The introduction of a centrally provided identity management service allows for long-lived identities, without the need for universities to maintain accounts beyond active affiliation of their users.

Attribute Authority: The university provided attributes were so far, and will remain the most important attributes for authorisation decisions. Universities will continue to keep complete control over them. Mostly, basic and user-provided additional attributes are maintained on the centralised identity management platform, although, if required, the platform may also cache or archive attributes from the attribute authorities.

Service providers: Service providers outnumber attribute authorities and identity providers by far, and are therefore an important cost factor to consider when introducing changes to them. While the Swiss edu-ID will add additional features, almost complete backward compatibility will be preserved.

9.2 Identity Management Considerations

The Swiss edu-ID identity can be regarded as a container, containing attributes (information) about a particular user. Some of those attributes are of a personal nature (e.g. name, home address,

nickname, preferences, communication channels), some is linked to present or past roles (e.g. organisational role, study branch and level, former roles, achievements, certificates) and yet other attributes contain third party identifiers, which create a link to external identities belonging to the same user (e.g. SuisseID, AHVN13, ORCID or social networks).

Whenever possible, attributes should be provided directly from the “natural authority” of those attributes. In the case of an assertion that a user is a student of university X within the SWITCH Community, the best option will be university X to provide this attribute itself. If this is not feasible or in the case of user-provided input, the Swiss edu-ID service needs to take appropriate steps to validate such information. Validation can be done by organisational members of the SWITCH Community (e.g. universities), it can rely on processes offered by linked identity providers for their respective identifiers (e.g. ORCID, social networks), or it can be done by contracted trust service operators (e.g. notary verified name, “Gelbe Identifikation” service of the Swiss Post).

The Swiss edu-ID will define its own primary, long-lived identifier to link users to the Swiss edu-ID identity in a one-to-one relationship. Re-using existing identifiers like AHVN13 or SuisseID as primary key is explicitly not recommended due to incomplete coverage within the user base and restrictions imposed on using the identifier. But given clear benefits and feasibility, it might prove useful to add such external identifiers as attributes (linked identities).

Tasks such as a student enrolment at a university or a user becoming a new staff member of a research institute will most likely require new local accounts being created at those organisations. At the same time, the organisation is likely to start issuing attributes on behalf of this user. Both processes can be simplified, if the Swiss edu-ID service offers a provisioning interface:

- The Swiss edu-ID should offer a provisioning interface for the creation of derived accounts at member organisations and, conversely, organisations of the SWITCH Community need processes to tell the Swiss edu-ID service for which users they offer additional attributes
- The Swiss edu-ID service is to consider support for the provisioning protocol SCIM[4].

9.3 Identity Management Platform

The Swiss edu-ID service relies on one single, central identity management platform operated by SWITCH and is designed for longevity.

This platform offers the following services:

Identity creation and management: performing identity vetting, issuing of the primary identifier and access credentials for all Swiss edu-ID users, collecting and validating a basic set of attributes for each user and offering identity management interfaces and processes for those tasks. However, attributes relating to activities or roles at Swiss edu-ID member or partner organisations are not managed on this platform, but by members or partners (the “natural authority” for those attributes).

User authentication: users can authenticate against this platform with the help of their access credentials

Identity linking: The user is offered processes to link identifiers of external identity management platforms to the Swiss edu-ID identity (e.g. social networks, ORCID).

Attribute release: under the direct control of the user, the platform releases attributes to requesting services. This covers attributes from the basic set maintained on the platform itself together with attributes fetched from member or partner organisations.

9.4 Attribute Authorities

Attribute authorities assert information about users. In the case of the Swiss edu-ID, the Swiss edu-ID members, selected Swiss edu-ID partners and the Swiss edu-ID operator can act as attribute authorities. For the time being, interfederation participants and most partners are not eligible to become attribute authorities.

The most important attribute authorities will be the Swiss edu-ID members (e.g. the Swiss universities) as they contribute affiliation and role information, which are commonly used for service authorisation decisions.

9.4.1 The User

Swiss edu-ID users maintain their own personal attributes like name, nicknames, address, communication channels and personal preferences. Some of those attributes require additional documentation or passing ownership verification processes (e.g. email or postal mail challenge tokens, OAuth2 handshake for ORCID).

9.4.2 Swiss edu-ID Operator

The operator issues the primary identifier and access credentials to all users and maintains, where required, validation processes for user provided attributes. The operator may to this end collaborate with Swiss edu-ID members and trusted third party validation services. The operator implements processes to handle disputes and incidents.

9.4.3 Swiss edu-ID Members

Swiss edu-ID members - usually universities - enrich the set of attributes with role information (e.g. staff or student) and additional information (e.g. study related information, like study level or branch)

9.4.4 Swiss edu-ID Partners

Swiss edu-ID partners entitled to operate an attribute authority may further enrich the set of attributes. Libraries might want to add role information relevant to other libraries, while project structures might want to add role information relevant to services run to support project partners.

9.5 Levels of Assurance

The level of assurance a service provider can expect from an assertion about a connecting user depends mainly on two elements:

The quality of the attributes provided: is the information correct?

The quality of the authentication: is the information relating to the correct user?

The following assurance levels are proposed and need to be specified in detail:

Assurance level	Attribute quality	Authentication quality
Basic Assurance	Self-asserted information with little confidence. Placeholder for future use, not defined yet	Username and password acceptable
Standard Assurance	Corresponds to the current assurance level of the existing SWITCHaai. All attributes are verified	Username and password acceptable
Elevated Assurance	Placeholder for future use, not defined yet	Multifactor authentication required

Usage considerations:

Basic Assurance: This allows for not much more than recognising connections from the same user again. Basic Assurance may be acceptable for granting access to external project collaborators, where the required trust can be achieved by other means. Will be defined later based on specific service requirements.

Standard Assurance: The vast majority of services will require Standard Assurance, as this corresponds to the assurance level in the current SWITCHaai

Elevated Assurance: Will be defined later based on requirements of services needing something better than Standard Assurance

9.6 Identity Vetting

Swiss edu-ID identities are created by self-registration by the future bearer of that identity. Only a very basic set of attributes is collected and put through a verification process (e.g. email and postal addresses). The resulting identity is of level Basic Assurance.

The Swiss edu-ID operator will document procedures to promote Basic Assurance identities to Standard Assurance identities. This may require the collaboration with Swiss edu-ID members or third party trust services. An existing SWITCHaai account may assist this process further.

9.7 Service Providers

In order to get the right to receive information about users from the Swiss edu-ID service, service providers need to fall under the legal framework of the Swiss edu-ID. Only services operated by a Swiss edu-ID member (including the Swiss edu-ID operator) or a Swiss edu-ID partner are eligible.

Services operated by a interfederation participant are not covered by the legal framework of the Swiss edu-ID, but by a more lightweight interfederation framework only. They need the explicit consent from the connecting user to receive information about users.

9.8 Interoperability Considerations

Since the Swiss edu-ID service is a mediation service between users and services, it is important to name services the Swiss edu-ID service is expected to interwork with and also to name the standards the Swiss edu-ID needs to adopt for that purpose.

9.8.1 Interoperability with SWITCHaai

Interoperability and co-existence with SWITCHaai is required on both the technical level as well as regarding the policy framework:

- Existing service providers shall be able to reuse already existing mechanisms to authorise Swiss edu-ID users. There are three kinds of existing service providers:
    - SWITCHaai Participants from the SWITCH Community
    - SWITCHaai Participant as SWITCHaai Federation Partner
    - SP Operators who registered their interfederation enabled service provider in another federation.
- Existing SWITCHaai identity providers shall be able to reuse existing components of SWITCHaai to become attribute authorities within the framework of the Swiss edu-ID.
- The IdP of the Swiss edu-ID service needs to become a member of the SWITCHaai federation.
- A SWITCHaai identity and a Swiss edu-ID identity owned by the same user shall be linked in such a way, that Swiss edu-ID enabled services can recognise this fact regardless of which identity was chosen to connect to the service.
- The Swiss edu-ID service needs to support the SAML protocol.

9.8.2 Interoperability with similarly scoped International Services

As much as international collaboration is important for Swiss edu-ID users and members, it is up to the Swiss edu-ID to interoperate with existing or future services with similar scope outside of Switzerland. Furthermore, the existing structures set up by SWITCHaai should be re-used whenever possible:

- Swiss edu-ID shall seek interoperability with interfederation participants of SWITCHaai by contributing to the existing and emerging interfederation frameworks and standards (e.g. code of conduct, LoA).
- Swiss edu-ID shall seek interoperability with similarly scoped services outside of Switzerland and actively promote the set-up of such services.

9.8.3 E-Government Standards and Services

Many processes in higher education and research involve federal or cantonal authorities (e.g. student admission, research grants). Furthermore, services offered by the government might offer substantial help in identity management tasks (e.g. relocation of users, proof of name or address):

- The Swiss edu-ID should consider adopting relevant existing or emerging national standards and services like e-CH standards (e.g. eCH-0170 “eID Qualitätsmodell”, eCH-0171 “Qualitätsmodell der Attributwertbestätigung zur eID”, or eCH-0172 “IAM-Maturitätsmodell”) and their international counterparts (e.g. eID/STORK).
- The Swiss edu-ID to seek interoperability with the frameworks of the SuisseID and the emerging passport/ID-card '17.
- The Swiss edu-ID needs to support the SAML protocol and user certificate standards (X.509).

9.8.4 Linking External Identities of Relevance to Higher Education and Research

There exists a multitude of identifiers or identities with associated services, which are relevant to higher education and research in Switzerland. Some are discipline specific (e.g. UMBRELLA), others span many disciplines (e.g. ORCID, ResearchGate) and many Swiss edu-ID users will maintain such identities in parallel with the Swiss edu-ID. The Swiss edu-ID is not meant to replace those identities, but to offer the option to link the primary identifier (and possibly additional information) of those external identities to the Swiss edu-ID identity. Many external identities already offer specific processes to establish trusted links between identities:

- External identities with relevance to higher education and research shall be identified.
- The Swiss edu-ID service should consider offering processes to link such external identities to the Swiss edu-ID.
- The Swiss edu-ID service needs to support the OAuth2 protocol to be able to link to ORCID and possibly further external identities.

9.8.5 Linking Social Media Identities

The majority of Swiss edu-ID users is expected to maintain multiple social media identities. Some will prefer to keep private and professional life as separate as possible and might not want to link their social media identities to the Swiss edu-ID identity. Others do not make that a clear distinction and use whatever tool serves them best, be it in a more professional or private context. The Swiss edu-ID should offer the second group the option to link the primary identifier of their social media identities to the Swiss edu-ID identity and make that link potentially visible to service providers. The main purpose of many social media identities is to offer access to communication and collaboration tools. Linking to the Swiss edu-ID identity makes it easier for users to document communication channels and collaboration options of their liking. Some social media services offer generic authentication and single-sign-on services. This might serve the Swiss edu-ID service as a low-trust authentication option:

- The Swiss edu-ID service should allow its users processes to link social media identities to their Swiss edu-ID identity. Priority is given to social media identities offering popular communication and collaboration services.
- The Swiss edu-ID service needs to support the OAuth2 and OpenID Connect protocol to be able to link to social media identities, and to a lesser extent also the older OpenID 2.0 protocol as well.

10 Bibliography

[1] Service Regulations for Services by SWITCH, 2009: https://www.switch.ch/export/sites/default/uni/terms/DL-Reglement_SWITCH_en.pdf

[2] Networked, The New Social Operating System, Lee Rainie & Barry Wellman, ISBN: 9780262017190, April 2012 (http://mitpress.mit.edu/books/networked)

[3] http://www.fidis.net/resources/fidis-deliverables/mobility-and-identity/int-d111000/doc/20/

[4] http://www.simplecloud.info

11 Glossary

AAI
Authentication and Authorization Infrastructure supporting easy and secure inter-organizational access to web applications within a federation.

Account
Typically a formal business agreement for providing regular transactions and services between a principal and the business service providers.

Affiliation
Specifies the relationship(s) to organisation(s).

Anonymity
Quality or state of being anonymous, which is the condition of having a name or identity that is unknown or concealed.

Assertion
Statement made by an entity without accompanying evidence of its validity.

Assurance
A measure of certainty that a statement or a claim is true.

Assurance Level (AL)
(also Trust level)

Degree of certainty that a claimant has presented a credential that refers to the claimant's identity. Each assurance level expresses a degree of confidence in the process used to establish the identity of the individual to whom the credential was issued and a degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Attribute
A single piece of information associated with a digital identity. Some attributes are general; others are personal. Some subset of all attributes defines a unique individual. Examples of an attribute are name, phone number, and group affiliation.

Attribute Authority
System entity that produces attribute assertions.

Authentication
Process of proving the identity of a previously registered subject.

Authorization
Process of granting or denying access rights for a resource to an authenticated End User.

Consent
General permission granted by an individual to a requesting entity to use the individual's personal information in some agreed manner. Consent can be expressed, implied, or provided through an authorized representative.

Credential(s)
Set of data presented as evidence of a claimed identity and/or entitlements.

Digital Identity (e-Identity)
Data that uniquely describes a person or a thing (subject) and contains information about the subject's relationships.

Federation
Collection of organizations that agree to interoperate under a certain rule set.

Identification
Process of recognizing an entity by contextual characteristics.

Identifier
Thing that is used to repeatedly recognise an individual. The identifier isn’t required to demonstrate the identity of the individual but only to recognise the same recurring individual.

Identity
see Digital Identity

Identity Managment (IdM)
Task of managing information (attributes) about users over the lifetime of the digital identity.

Identity Provider (IdP)
System component that issues assertions on behalf of subjects who use them to access the services of service providers.

Interfederation
Interconnection of services across the boundaries of their respective identity federations. The main goal of interfederation is to extend the user community.

Lifelong Learning
All general education, vocational education and training, non-formal education and informal learning undertaken throughout life, resulting in an improvement in knowledge, skills and competencies within a personal, civic, social and/or employment related perspective.

ORCID
Open Researcher and Contributor ID including the ORCID identifier and the ORCID record.

Password
Shared secret character string used in authentication protocols. In many cases the claimant is expected to memorize the password.

persistent
Existing and able to be used in services outside the direct control of the issuing assigner, without a stated time-limit.

Privacy
Ability of an individual to control access to personal information about themselves and the right to control the collection, storage, and dissemination of that information. It includes the right to see what

personal information is stored and to correct or remove the access to that information as far as the law permits.

Privilege
Right that, when granted to an entity, permits the entity to perform an action.

Profile
Profile of an entity or a group of entities is an organized set of attributes that characterizes the specific properties of that entity or entities within a given context for a specific purpose.

Pseudonymity
State of disguised identity. The pseudonym identifies a subject not known or is known to only a limited extent, within the context in which it is used. A pseudonym can be used to avoid or reduce privacy risks associated with the use of identifier bindings which may reveal the identity of the entity.

Registration
Process in which the subject is identified and/or other attributes are corroborated. Because of the registration, a partial identity is assigned to the subject for a certain context.

Resources
Material to which access is granted, e.g. applications, websites, databases, systems, etc.

Role
Set of one or more authorisations related to a specific application or service.

Self-asserted Identity
Identity that an entity declares to be its own.

Service Provider (SP)
System component that evaluates the Assertion from an IdP and uses the information from the Assertion for controlling access to protected services.

Subject (entity, individual, user)
Person or thing that is being discussed, described or dealt with. In our context, the subject is usually a human individual also referred to as user.

SWITCH Community
Community comprising the following categories of Swiss organisations (as per the service regulations for services by SWITCH in force at the time of writing):

- Cantonal universities
- Federal institutes of technology
- Research institutes of the ETH domain
- Universities of applied sciences
- Universities of Teacher Education
- Swiss Federal Institute for Vocational Education and Training

Trust
Firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context.

Trust Level
see Assurance Level

User
see Subject

user-centric
Users having more control, more choices or more flexibility as in the previous system. Higher usability because of a development based on the users tasks, goals and characteristics. In the context of Swiss edu-ID: a subject has as much control over the data transferred and exchanged about himself/herself as possible and manageable. The processes support transparency vis-à-vis the subject and the system operates on a scale that is relevant for the subject.

Verification
Process or instance of establishing the authenticity of something.