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

Service Description

SWITCH edu-ID

Version 1.0.5
Valid from 1. August 2020

https://www.switch.ch/edu-id/terms/

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

1 Overview and purpose

This document defines the concept and regulations for end users who use the SWITCH edu-ID service, and the regulations for organisations and service operators that participate in the SWITCHaai Federation.

This document is structured as follows:

Chapter 3 covers the definitions and describes the functions in detail.

Chapter 4 is addressed specifically to end users.

Chapter 5 is addressed specifically to organisations that participate in the SWITCHaai Federation.

Chapter 6 contains the legal terms of use that apply to end users and participating organisations.

This document is binding in its entirety both for end users and organisations. By using the SWITCH edu-ID service, end users, organisations and service operators agree to these conditions and regulations.

The SWITCH edu-ID concept is based on the SWITCHaai concept and develops it further. This Service Description replaces the SWITCHaai Service Description V1.0 of 15 November 2011 as well as any former version of this SWITCH edu-ID Service Description.

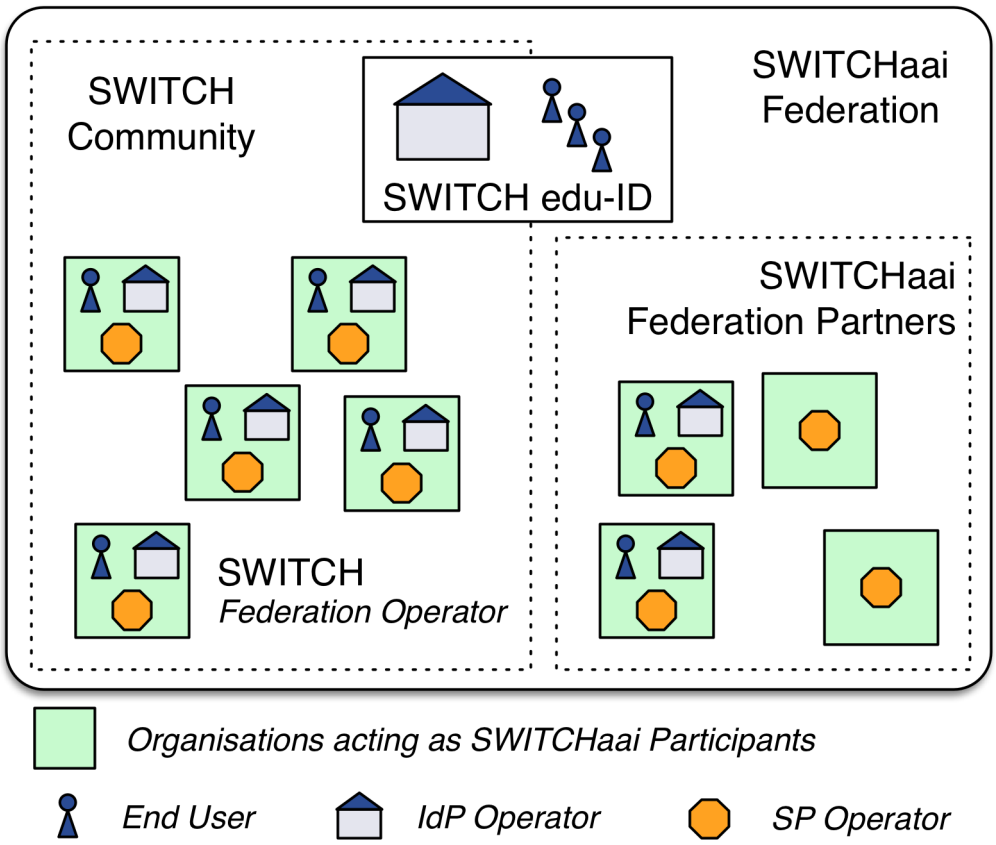
The SWITCH edu-ID service is embedded in the SWITCHaai Federation. The function of the SWITCHaai Federation is described in detail in chapter 5.

The objective of the SWITCHaai Federation is to simplify and foster the cross-organisational use of services. End users can use their digital identity to use services registered in the SWITCHaai Federation or another federation through interfederation.

In its role as Federation Operator, SWITCH coordinates the requisite activities.

For SWITCHaai Participants from the SWITCH Community, participation in SWITCHaai is based on the Service Regulations (SR)[1] in the current version. For federation partners, participation in SWITCHaai is based on the General Terms & Conditions (GTC)[2] in the current version (see chapter 6.1).

[1] https://www.switch.ch/de/about/disclaimer/service-regulations/
[2] https://www.switch.ch/de/about/disclaimer/gtc/



The descriptions of SWITCHaai and SWITCH edu-ID are publicly available[3]. End users can manage their personal data in the “My edu-ID” web application at https://eduid.ch/ (see also Chapter 3.2.3.4.

In the *Swiss edu-ID* project, concepts for further development of SWITCHaai were created and the development of the *SWITCH edu-ID* service partially financed[4].

[3] https://www.switch.ch/services/aai/
[4] https://www.swissuniversities.ch/en/organisation/projects-and-programmes/p-5/

2 Brief summary of important facts for end users

- SWITCH edu-ID is a service from SWITCH that manages digital identities for lifelong use by university members and other end users. A SWITCH edu-ID account remains valid when an end user, as the bearer of the digital identity, leaves an organisation (in contrast to a SWITCHaai account).

- The concept envisions just one SWITCH edu-ID account for each end user. End users are obliged to avoid duplicates and to merge any duplicates they may accidentally have created.

- End users undertake to provide correct information and to keep their data up to date. In particular, they ensure that the provided e-mail is working. E-mail addresses that become invalid are to be deleted and/or replaced.

- End users are responsible for all activity in connection with their SWITCH edu-ID account. They are therefore obliged to protect their SWITCH edu-ID and not to provide it to any third party. This includes the selection of secure passwords without sharing.

- SWITCH[5] operates the service and administers the data according to Swiss law. The data and servers are located in Switzerland.

- Only data required for the provision of SWITCH edu-ID services will be stored. If the end user links their SWITCH edu-ID account with other identities, such as the SWITCHaai identity at a university or ORCID[6], further use cases can be supported.

- When logging in to services, they may request data that is stored in the SWITCH edu-ID account of the end user. The end user decides whether this data is forwarded to the service.

[5] https://www.switch.ch/
[6] https://www.orcid.org/

3 Definitions and function description

3.1 Definitions

Affiliation of an end user (membership to an organisation)	An *affiliation* is a role held by an end user associated with an organisation in the SWITCHaai Federation. It is created by *linking* a base identity with the *organisation-related identity* of the user. A base identity can be linked with no, one or multiple *affiliations* of an end user. An existing affiliation is described as a *current affiliation*; a previous, no longer active, affiliation is described as a *former affiliation*.
Assertion	Attributes are usually issued in a digitally encrypted and signed *Assertion* from the IdP to the SP. An Assertion is a secure container for potentially confidential information. With the attribute received in this manner, the SP or the service protected by the SP makes a decision on the end user's access to the service.
Attribute, **Base Attribute** **Affiliation Attribute** **Complementary Attributes**	An *attribute* is a descriptive unit of information with a standardised name; e.g. name, e-mail, date of birth, telephone number, *SWITCH edu-ID identifier*, etc. The attributes used in SWITCHaai are documented and specified[7]. Attributes are frequently grouped into categories, such as *Core Attributes* and *Other Attributes* in the SWITCHaai context, and *Base Attributes*, *Affiliation Attributes* and *Complementary Attributes* in the SWITCH edu-ID context. *Base Attributes* are a component of the *base identity*. *Affiliation Attributes* are connected to the end user's *affiliation* and are managed and provided by an organisation-specific *Attribute Provider*. They have the following characteristics: • They are issued by organisations • They are issued only for the duration of the membership to that organisation *Complementary Attributes* are managed and provided by complementary *Attribute Providers*
Attribute Provider (AP)	In the context of SWITCH edu-ID, an *Attribute Provider (AP)* provides the organisation-specific Affiliation Attributes or the Complementary Attributes for a user identified uniquely by a *SWITCH edu-ID Identifier*. As part of the adoption of the SWITCH edu-ID, a *SWITCHaai Participant* replaces the existing IdP with an organisation-specific AP.
AP Administrator	The executing person at the *AP Operator* is called the *AP Administrator*.

[7] https://www.switch.ch/aai/attributes/

AP Operator	The legal entity that represents the *SWITCHaai Participant* and which bears overall responsibility for the operation of an *Attribute Provider* is called the *AP Operator*; see chapter 5.1.3.8.
Base identity (aka private identity) **Self-declaration** **Self-provisioning** **Quality level**	The *base identity* encompasses end user-specific information in the strict sense, such as the surname, name, personal telephone number and personal e-mail address. In the SWITCH edu-ID service, the end user enters the data personally for the base identity. This process is called self-declaration, and the base identity itself is created through *self-provisioning*. 'Self-provisioned' is also a frequently used value for the *quality level* of the information stored in the base identity. End users can raise the quality level of the attributes in their digital identity (or have it done for them) through validation processes.
Classic Attribute Model	The *Classic Attribute Model* is compatible with SWITCHaai and can represent exactly one affiliation (see also *Extended Attribute Model* and the architecture document[8])
Contractual Partner	In this document, a Contractual Partner is an organisation that has concluded a contract for a service with SWITCH, but which is not a member of the SWITCH Community or the Extended SWITCH Community.
Digital identity	A digital identity comprises a collection of information in the form of attributes that can be assigned to the end user. It is issued and managed by an IdP Operator, which can identify the end user at any time. A digital identity can describe not only persons, but also things. This option is not included in this context. The *SWITCH edu-ID Account* of an end user is a digital identity.
End user **(user)**	An *end user* is an individual person who uses the service. Use begins when a user creates their personal SWITCH edu-ID account. The SWITCH edu-ID service is addressed particularly to all end users with an association to organisations within the SWITCH Community.
Extended Attribute Model	In the *Extended Attribute Model*, all affiliations, instead of just one, will be made available towards the service (see also the *Classic Attribute Model* and the architecture document[6]).
Extended SWITCH Community	Organisations that have a close connection with the SWITCH Community, including university policy organisations, academies, funding institutions, libraries and hospitals, and private research institutions and tertiary institutions that are not part of the SWITCH Community.
Federated Authentication	This refers to the login process in which the own digital identity is used to gain access to services offered by *SP Operators* in the federation.

8 https://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/SwissEduIDArchitecture_Rev1.pdf

Federation (particularly the SWITCHaai Federation)	A federation is a group of organisations that have agreed to collaborate on the basis of a common set of rules. The rules apply here to Federated Authentication and Authorization. The SWITCHaai Federation refers to the corresponding group of Swiss university organisations[9]. The SWITCH edu-ID service is embedded in the SWITCHaai Federation.
Federation Operator	The Federation Operator manages and further develops the federation. It is responsible for the central components and functions as a competence centre. In the SWITCHaai Federation, SWITCH is the Federation Operator.
Federation Technology Profile	A Technology Profile is used to define which technical details of a specific technology (e.g. a communication profile or a programming interface) apply in the context of the federation or how they are to be used.
General Terms & Conditions (GTC)	The General Terms & Conditions are part of the contract and are available on the SWITCH website[10].
Identity Provider (IdP)	The Identity Provider is the operating component that authenticates users and issues an Assertion about the user to a given service. An Assertion transports the attributes of the digital identity required for access to the services. SWITCH operates the SWITCH edu-ID IdP. Organisations can operate their own IdP or delegate this task to SWITCH. The central SWITCH edu-ID IdP differs from other IdPs through additional functionality (see chapter 3.2.3).
IdP Administrator	The executing person at the IdP Operator is called the IdP Administrator.
IdP Operator	An IdP Operator is a SWITCHaai Participant that assumes overall responsibility for the operation of an IdP; see chapter 5.1.3.9. In particular, this includes: • The identification of end users • Management of digital identities • Definition of identification processes for end users • The use of suitable processes for on- and offboarding of end users, usually using an Identity Management System (IdM) These responsibilities also apply to the SWITCH edu-ID service.
Interfederation	Through interfederation, an end user can gain access to services of other federations from their own federation. Interfederation is generally available to SWITCHaai Participants (see chapter 5.1.2.5).

[9] https://www.switch.ch/aai/participants/
[10] https://www.switch.ch/about/disclaimer/gtc/

Linked identity (linked organisational identity, linked external identity)	An end user can link their base identity with other identities. If the user links it with their organisation-based identity from an organisation in the SWITCHaai Federation, an affiliation is formed. An end user can also link it to an external identity, such as ORCID; for example, the addition of an external identifier as an attribute of the base identity.
Metadata	Metadata encompasses technical details and descriptive information about the components participating in the federation, and in particular about IdPs, APs and SPs. Metadata is usually protected against changes with a digital signature. The components in the federation rely on this metadata to trust each other on the technical level. In the SWITCHaai Federation, the metadata is managed by SWITCH.
Organisation	An organisation within the SWITCH Community, the Extended SWITCH Community or a Contractual Partner of SWITCH. Organisations can offer their services to their own end users or the end users of other organisations. Organisations can, in turn, also offer their end users access to services offered by other organisations through an Identity Provider (IdP) or an Attribute Provider (AP).
Quality level for Base Attributes	Values of Base Attribute can be enhanced with corresponding quality indicators which indicate their origin and therefore their quality level. With self-declaration, attributes such as the e-mail address, mobile phone number and postal address receive the lowest quality level, 'self-declared'. An attribute can be checked through a verification process, which then raises its quality level if successful.
Service, Service Provider (SP)	A service is a web application or other application offered by an organisation or third party that can be accessed by end users. The service relies on the authentication of the end user by SWITCH edu-ID IdP or another IdP in the federation. For authorisation of end user access, the Service Provider (SP) component evaluates the information about the end user that the SP received in the Assertion from the IdP. Based on this, the SP decides whether the end user should be granted access to the service.
Service Regulations (SR)	The regulations for use of SWITCH services are part of the contract and are available on the SWITCH website[11].
SP Administrator	The executing person at the SP Operator is called the SP Administrator.
SP Operator	An SP Operator is a SWITCHaai Participant that assumes overall responsibility for the operation of an SP; see chapter 5.1.3.10. The SP Operator's most important task is to define the criteria for access to the service (authorisation).
SWITCH Community	All organisations in the education and research area connected with SWITCH (in accordance with the appendix to the SR).

[11] https://www.switch.ch/de/about/disclaimer/service-regulations/

SWITCH edu-ID Advisory Board	This board[12] comprises representatives of the most important stakeholder groups in the SWITCHaai Federation. It advises SWITCH on strategic questions concerning the SWITCH edu-ID service and the SWITCHaai Federation.
SWITCH edu-ID (service)	SWITCH edu-ID is a digital identity service developed by SWITCH for lifelong use by all persons with a relationship to the Swiss academic community. The SWITCH edu-ID service is described in detail in chapter 3.2.
SWITCH edu-ID (identifier)	The SWITCH edu-ID Identifier is described in detail in chapter 3.2.2.2.
SWITCH edu-ID (identity and concept)	The SWITCH edu-ID Identity is a digital analogue of a traditional ID and enables its holder, the end user, to access many services. The SWITCH edu-ID concept is described in detail in chapter 3.2.1.
SWITCHaai Federation Partner	An organisation that is not part of the SWITCHaai Community, but which participates in SWITCHaai is called a SWITCHaai Federation Partner.
SWITCHaai Participant	A SWITCHaai participating organisation (a legal entity) is called a SWITCHaai Participant.
Trust & Identity WG	This working group comprises representatives of all SWITCHaai and SWITCHpki participating organisations in the SWITCH Community and the Extended SWITCH Community. It is both an information channel and a platform for communication in order to give feedback and address technical questions.
User Consent	By default, end users have to give their consent when the IdP passes their data to some SP. For usability reasons, this decision is memorized. End users can choose whether to give their consent again at the next login, or when their data changes. They are then provided with an additional view that lists the data to pass, and a request to approve or deny.

3.2 Operation principles of the SWITCH edu-ID

3.2.1 The SWITCH edu-ID concept

SWITCH edu-ID is a digital identity developed by SWITCH intended for lifelong use by university members and other end users. It should be secure and internationally recognised. The SWITCH edu-ID service builds on the successful, federated identity management solution SWITCHaai. This simplifies the organisation's identity management and enables the provision of other services with this digital identity. Compared with SWITCHaai, the SWITCH edu-ID introduces the following new features:

- User-centricity and persistency: the digital identity belongs to the end user, who can check and update the basic information of their SWITCH edu-ID at any time. The digital identity is independent of membership in an organisation and therefore remains valid even when the end user leaves an organisation.

[12] https://www.switch.ch/edu-id/governance/

- Self-provisioning: every individual can create an electronic base identity and thus become an end user of SWITCH edu-ID. The person retains full control over a series of personal attributes (Base Attributes), such as their surname, name, e-mail address and telephone number.
- Attribute quality level: self-provisioning leads *a priori* and naturally to lower initial attribute quality. Attributes therefore receive not just a value, but also a quality indicator that complements the value. Quality levels can be raised through validation processes, or lowered, for example, if they reach an expiry date (ageing) or by manual variation of the value.
- Multiple affiliations: an end user can belong to no, one or multiple organisations. The user's base identity can accordingly contain no, one or multiple affiliations, depending on whether the base identity is linked with the organisation-based identities of organisations in the SWITCHaai Federation. The information attached to the affiliations is supplied by the participating organisation, typically through its Attribute Provider (AP).

3.2.2 How does the SWITCH edu-ID service work?

If the end user has a base identity, they can use it to access a range of services in the SWITCHaai Federation. To grant access, the service can request specific quality levels for specific Base Attributes, or additional attributes that provide information about existing affiliations. Typically, the end users provide their consent (user consent) immediately before this information is made accessible to the service (see also chap. 4.5).

After successful authentication of the end user, the SWITCH edu-ID IdP gathers all the required and approved attributes in an assertion and transfers them securely to the service. The service checks them and decides whether to grant access based on its configuration.

Thus, the SWITCH edu-ID IdP fulfils the requirements of an IdP in the SWITCHaai Federation. The following concepts distinguish the SWITCH edu-ID service:

3.2.2.1 Classic and Extended Attribute Model

Services that can handle multiple affiliations support the *Extended Attribute Model*; i.e. all available and end user-approved affiliation information can be transferred. The service then decides how it will handle these different affiliations. Further details can be found in chapter 2.1 of the Swiss edu-ID architecture document[13]. Specific obligations for operators of SPs requiring the Extended Attribute Model are described in section 5.1.3.10 .

All other services are expecting exactly one affiliation and thus support the *Classic Attribute Model*. If an end user has multiple existing affiliations, they must inform the IdP of which affiliation they wish to use for the respective service via an Affiliation Chooser (see chapter 3.2.3.6). Only the Affiliation Attributes belonging to the selected affiliation are transferred to the service.

[13] https://www.switch.ch/edu-id/documents/

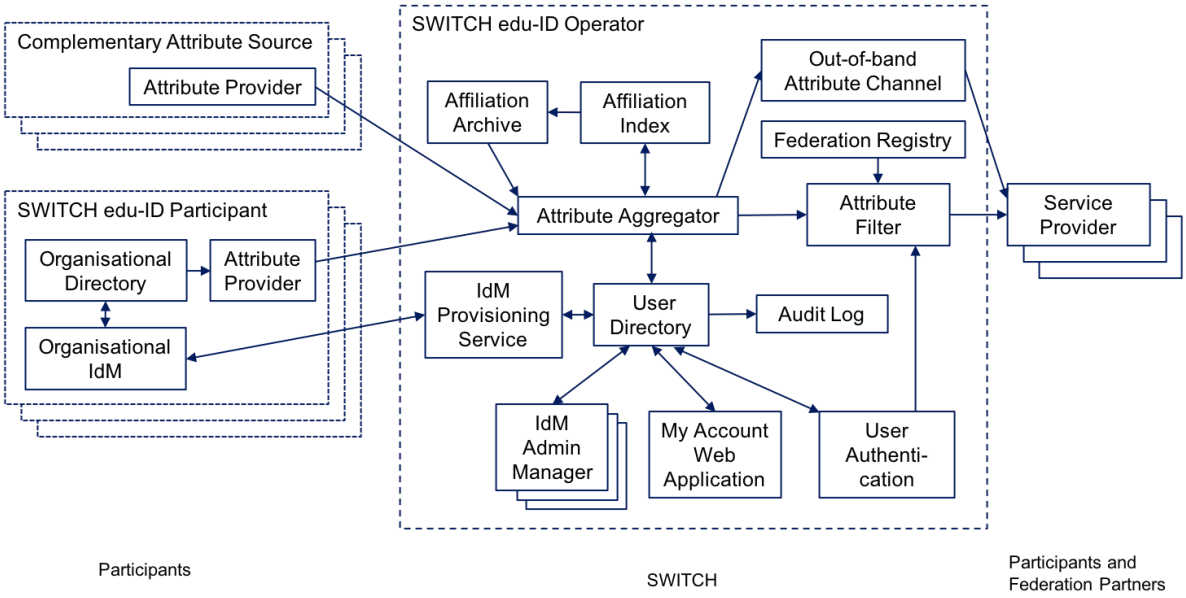
3.2.2.2 The SWITCH edu-ID identifier and further identifiers

The SWITCH edu-ID identifier[14] [15] identifies every end user uniquely and persistently for a lifetime. This is the primary, sector-specific identifier for the academic community in Switzerland used to uniquely link additional personal information.

The SWITCH edu-ID identifier creates the prerequisite for the collection of data that can be regarded as a personal profile in the sense of the Federal Act of 19 June 1992 on Data Protection (FADP; SR 235.1)[16] and must therefore be treated and protected as such (see chapter 5.1.3.12).

The SWITCH edu-ID identifier is reserved to services that are directly related to the identity management at organisations. If a service requires the SWITCH edu-ID identifier, the related due diligence obligations are transferred to the SP Operator. All other services must use one of the other identifiers (e.g. a pairwise identifier[17] or the swissEduPersonUniqueID) unless they have a compelling reason to use the SWITCH edu-ID identifier.

3.2.3 Components of the SWITCH edu-ID service



3.2.3.1 User Directory

The SWITCH edu-ID identity (base identity) is stored in the central SWITCH edu-ID database. This data is accessed every time an end user is authenticated. Each entry is assigned to exactly one end user. The end user is responsible for ensuring the correctness of the data in their entry.

---

[14] https://www.switch.ch/aai/support/documents/attributes/swisseduid/
[15] https://swit.ch/eduidspec
[16] https://www.admin.ch/ch/d/sr/c235_1.html
[17] https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd01/saml-subject-id-attr-v1.0-csprd01.html#_Toc497819494

3.2.3.2 Attribute Aggregator

The Attribute Aggregator ensures that the Affiliation Index (see diagram) is up to date through contact with the various organisation-specific Attribute Providers.

3.2.3.3 SP Notification

The SP notification module can optionally notify SPs of changes to attribute values. The SPs thus have the opportunity to update their own user database.

3.2.3.4 'My edu-ID' Web Application

This web application allows the end user to check, update and, if desired, add to or verify all their personal data. Access and activities related to the 'My edu-ID' web application are logged.

3.2.3.5 Identity Provider (IdP)

The Identity Provider (IdP) is responsible for end user authentication. It then gathers the required attributes for the SP that initiated the authentication, if necessary requests the user's consent for release of the data, and passes the information to the SP as an Assertion.

3.2.3.6 Affiliation Chooser

After authentication, the Affiliation Chooser allows the end user, if necessary at all, to choose one of their existing affiliations with which they want to log in to the service. The Affiliation Chooser is used for services that use the Classic Attribute Model. The Affiliation Chooser takes the affiliations from the Affiliation Index.

3.2.3.7 Affiliation API and Affiliation Archive

The purpose of the Affiliation API is to provide a means for the organisations to register and administrate affiliations of their end users in the SWITCH edu-ID user directory. The SWITCH edu-ID offers two methods to do that, a push- and a pull-method.

If the Attribute Aggregator (pull method) determines that an affiliation is no longer to be renewed by the Attribute Provider, it moves the still existent information into the archive of the former, no longer active affiliations, called the Affiliation Archive. Future services – e.g. alumni organisations – can, assuming proper permission, obtain such information.

3.2.3.8 Administration Interface

This interface allows the service operator SWITCH to obtain some statistics and to administer end user as well as technical accounts in relation to support tickets. Only a limited number of administrators is allowed to access this interface, and they must use two-factor-authentication. Access and manipulations are logged.

3.2.3.9 Organisational Administration Interface

This interface allows administrators of the organisations to obtain some statistics and to administer their end user as well as technical accounts in relation to support tickets (for technical accounts see also 5.1.3.7). Access and use of this interface are limited to administrators of the organisation in question. Access and manipulations are logged.

3.2.3.10 Other assistance systems: Test Federation and demo sites

SWITCH operates and maintains a Test Federation[18] for the purpose of testing new components and configurations. It contains the required components, such as an IdP, AP or SP, which demonstrate the functionality of SWITCHaai and the configuration options in detail.

3.2.3.11 Other assistance systems: Attribute Viewer

SWITCH provides an SP known as the Attribute Viewer[19] that requests as many attributes as possible from the IdP, and displays them for the end user on a website.

- An IdP can use it to check whether its attributes are issued correctly.
- End users can see which attributes are issued by their IdP.
- If they suspect misconduct on the part of their SP, SP Administrators and advanced end users can check whether their IdP is working correctly with the AAI Attribute Viewer and thus narrow down the possible cause.

The Attribute Viewer currently supports the *Classic Attribute Model*, but can be modified later to support the *Extended Attribute Model*.

3.2.3.12 External assistance systems

SWITCH may integrate external assistance systems, such as to regularly verify the validity of registered e-mail addresses, or to send tokens by postal mail or SMS to the registered postal addresses and the mobile phone numbers, respectively. SWITCH publicly declares these integrated assistance systems[20] and shall ensure that the relevant processors are bound by their obligations in this respect in accordance with current data protection legislation.

3.3 Availability and support

The service is available 24/7. SWITCH always conducts planned maintenance work outside normal business hours and announces such work at least one week in advance on the login page of SWITCH edu-ID. SWITCH aims to achieve availability of at least 99.99% for the service and every sub-component. Disruptions that compromise the service remain reserved.

SWITCH undertakes to initiate or complete measures to remedy disruptions and malfunctions of the service within normal business hours.

End user support[21] is staffed during normal business hours.

The normal business hours are defined in the Service Regulations (SR) and the General Terms & Conditions (GTC) in the most recent version.

SWITCH also takes precautions to ensure good service quality outside business hours depending on urgency and its own assessment of the situation.

[18] https://www.switch.ch/aai/demo/
[19] https://attribute-viewer.aai.switch.ch/
[20] https://www.switch.ch/edu-id/about/external-services/
[21] https://help.switch.ch/eduid/

3.4 Monitoring and logging

The operating state of the SWITCH edu-ID service is displayed continuously on the public SWITCH website[22].

Additional information about the operating state is provided to SWITCHaai Participants on the customer portal[23].

In coordination with the organisations, SWITCH can monitor their components (particularly IdPs and APs) and make the results accessible to other organisations in a suitable form. SWITCH manages dedicated technical accounts for this purpose.

When disruptions occur, SWITCH applies the internal Incident Management Process. This includes external communications.

SWITCH can store changes to the operating state and transactions concerning end user data for the purpose of traceability. Validation processes can also be logged. Existing logs are made available to end users in an appropriate manner.

SWITCH records the use of the service by the end user or the organisation. Where possible, this is done per organisation. SWITCH provides the organisation with anonymised statistics on the use of SWITCH edu-ID.

[22] https://www.switch.ch/monitoring/
[23] https://portal.switch.ch/

4 End user-specific information

4.1 Creation and access

a) All end users who are interested in creating a lifelong digital identity for access to services can benefit from the SWITCH edu-ID service.

b) A SWITCH edu-ID account is required to use the SWITCH edu-ID service. Users must provide at least the following information:

- complete name
- valid and personal e-mail address
- secure password

c) End users can change the name, e-mail address(es) and password of their SWITCH edu-ID account at any time.

d) Specific services may require additional personal attributes, such as date of birth, home address, mobile phone number, etc. For example, a library can send books to the user's home only if they have specified a home address.

e) Service Providers can request the *quality level* of the base attributes. An attribute can be checked through a verification process, which then raises its quality level if successful. For example, a mobile phone number may be accompanied by the information that the end user was reached via that number.

A verification can be conducted by the end user, SWITCH or an organisation. A verification can be carried out once or several times. The quality levels can be viewed in the 'My edu-ID' web application.

f) End users can create their SWITCH edu-ID account or base it on an existing SWITCHaai account. The advantage of the second approach is that the user account is already linked (in one direction; i.e. to the SWITCHaai identity) and existing base attributes can be transferred immediately to the SWITCH edu-ID account. When creating the SWITCH edu-ID account, this data is displayed in non-editable fields.

g) End users can later link their SWITCH edu-ID account to one or more existing SWITCHaai accounts and add them as affiliations. It is also possible to link to external identities, such as ORCID. Such links may be necessary if the SWITCH edu-ID account is used to access services that require the identifiers of the linked accounts.

h) Organisations in the SWITCHaai Federation determine independently which of their services they wish to make available to individual end users and the conditions that must be met for their use. The end user has no intrinsic right to access the services.

4.2 Contact info and SWITCH edu-ID help page

For questions relating to the SWITCH edu-ID account, consult the help page[24].

[24] https://help.switch.ch/eduid/

4.3 Administration of end user accounts

a) A SWITCH edu-ID account can be created by the end user, independently or by arrangement through an organisation.

b) In order to support life-long learning, a SWITCH edu-ID user account will continue to exist when the end user leaves an organisation, e.g. a university or research institute, unlike a SWITCHaai account, which is deactivated in this moment.

c) When two accounts are merged, the one account that is no longer used will be deleted.

d) Deletion of a life-long SWITCH edu-ID violates in principle its purpose. To delete a SWITCH edu-ID account, the end user must contact SWITCH edu-ID support[25] via e-mail. Deletion of a SWITCH edu-ID account includes permanent deletion of all related end user data. They will remain in the backup (usually for 12 months), though. It is not possible to undo a deletion. A SWITCH edu-ID account can only be deleted, when all related *current affiliations* have been removed beforehand. This is due to the fact that a current affiliation is in a certain sense a proof that the account is active.

d) In the event of death, relatives of the end user can contact SWITCH edu-ID support to lock and/or delete the account by presenting the proper official documents.

4.4 Handling affiliation attributes when membership to an organisation is revoked

When a current affiliation is removed, typically when students or collaborators leave the organisation, they can by nature no longer use the affiliation attributes as they did beforehand.

Special attention has to be given to the e-mail address(es) that went with the affiliation. Organisations can reassign this address(es) to further individuals.

End users are therefore obliged to update their base attributes, in particular their e-mail address(es). Organisations and the SWITCH edu-ID usually notify the end user about upcoming termination of affiliations.

4.5 User Consent

End users are by default asked to give their consent to the disclosure of their personal attributes when they are about to log in to some service that asks for it. This consent is asked for each service separately, and at least at the first login attempt to that service of the user in question, or when the values have changed. In addition, end users can check a box such that they will be asked anyway at the next login to that service. When asking for the consent, the IdP also presents to the end user the attributes that are about to be sent.

Technical identifiers and their respective values (see attribute specification[26]) are not shown in this user consent dialog, as they are only machine readable and do not contain any personal data. The corresponding identifiers are described on the SWITCH edu-ID web page[27] (see also chapter 3.2.2.2).

---

[25] eduid-support@switch.ch
[26] https://www.switch.ch/aai/support/documents/attributes/
[27] https://www.switch.ch/edu-id/services/login/user-consent/

Specific services can, in certain cases, update attribute values without the end user being present, or they can get additional attribute values from the IdP. In any case, in order to do that, they have to obtain the consent beforehand from the end user in question. If end users wish that their data is no longer updated at such a service, e.g. because they don't use it any more, then they have to contact the service directly (see also chapter 5.1.3.10).

4.6 Automatic archiving and deprovisioning of SWITCH edu-ID accounts

SWITCH edu-ID accounts that are not used for an extended period of time are placed in the automatic archiving and deprovisioning process. Deprovisioning at the request of the end user (see chapter 4.3) and due to inappropriate use (see chapter 6.7) are also possible. The automatic deactivation and deletion process looks as follows:

- Reminder of inactivity every year: A notification is sent to the registered primary e-mail address informing about the non-use for 365 days, together with a call to at least log into the 'My edu-ID' web application and to check whether the personal data has to be updated.
- After 4 years, the notification is extended to all registered e-mail addresses including those related to an affiliation.
- Locking after one more year: If, during 12 more months, the account isn't used to log in to some service, including the 'My edu-ID' web application, then the account is locked and a notification about this is sent to all known e-mail addresses. The account can no longer be used, and in order to unlock the account, the end user has to contact the SWITCH edu-ID support.
- Automatic deletion after 5 more years: If no unlocking has taken place during 5 more years, then the SWITCH edu-ID account is eventually and irrevocably being deleted after a total of 10 years.

Unlocking a locked account, or an account without a valid e-mail-address requires the help of the SWITCH edu-ID support. The support agent will need to go through a successful out-of-band identification of the end user.

Data of deleted accounts remain in the backup (usually for 12 months). Deleted accounts cannot be undeleted, though.

5 The SWITCHaai Federation Policy

5.1 Governance and roles

5.1.1 Governance

As the Federation Operator, SWITCH operates the SWITCHaai Federation and consults both the SWITCH edu-ID Advisory Board[28] and the Trust & Identity Working Group.

The SWITCH edu-ID Advisory Board includes representatives of the most important stakeholder groups, including representatives from the SWITCH Community, political bodies in the field of education and SP Operators. The SWITCH edu-ID Advisory Board acts as an advisory body concerning the long-term strategy of the SWITCH edu-ID service.

SWITCH consults with the SWITCH edu-ID Advisory Board concerning topics such as:

- which categories of Federation Partners should be accepted
- which categories of Federation Partners may operate an IdP or AP
- interfederation agreement
- planning of the future development of the SWITCH edu-ID and the SWITCHaai Federation, and administrative and technical optimisations
- changes to the administration of the SWITCHaai Federation or this Service Description, and other documents specific to the federation

The SWITCH edu-ID Advisory Board has no decision-making authority. SWITCH decides on the composition of the SWITCH edu-ID Advisory Boards, together with the mandating organisations.

The Trust & Identity WG comprises representatives of all SWITCHaai and SWITCHpki participating organisations in the SWITCH Community and the Extended SWITCH Community. This group is informally involved and has the opportunity to provide feedback if there are questions or changes.

SWITCH maintains close relations with the SWITCHaai Participants. SWITCH organises events at which SWITCHaai Participants, and in particular AP, IdP and SP Administrators, learn about and have the opportunity to discuss new developments in the field of *Federated Authentication and Authorisation*.

SWITCH disseminates the information on the ideas and concepts implemented in SWITCH edu-ID and the SWITCHaai Federation to interest groups and organisations that may adopt similar concepts. The focus is placed on those groups that demonstrate the greatest potential for benefit to the SWITCH Community.

SWITCH acts as a centre of expertise for *Federated Authentication and Authorization* in the academic sector. SWITCH tests software and recommends and documents solutions. SWITCH provides manuals for the installation and/or configuration of selected software packages on specific operating systems for use in the SWITCHaai Federation. Example configurations simplify the integration of other products.

[28] https://www.switch.ch/edu-id/governance/

If certain functionality of part thereof is not otherwise available, SWITCH itself or a third party commissioned by it may develop the missing components.

5.1.2 Rights and obligations of the Federation Operator

5.1.2.1 General information

SWITCH is responsible for operation of the federation and the formal incorporation of relevant national and international organisations.

SWITCH compiles and publishes a list of SWITCHaai Participants[29].

5.1.2.2 Resource Registry (RR)

SWITCH operates and maintains the Resource Registry[30] for the administration of the federation. APs, IdPs and SPs are called resources in the context of the Resource Registry.

AP, IdP and SP Administrators of SWITCHaai Participants keep all relevant information about their respective resources up to date, including contact and support information, technical configuration details, attribute requirements, attribute release policies, intended audience, etc.

This data is stored in a database. From this database, SWITCH generates various types of other data used elsewhere, such as metadata files or attribute release configurations for APs and IdPs.

New SP entries and changes to existing SPs in the Resource Registry require approval before they become active and appear in the metadata. This is the responsibility of the AAI Resource Registration Authority Administrators of the SWITCHaai Participant accountable for the SP. After a check for correctness and compliance, they approve the new entry or change. See also documentation for the Resource Registry[31].

5.1.2.3 Metadata Service

SWITCH operates and maintains the Metadata Service[32], which digitally signs and publishes the properties of SWITCHaai Participants. For signature purposes, SWITCH maintains a dedicated off-line SWITCHaai Root Certificate Authority (CA)[33] the certificates of which function as a trust anchor for the metadata check.

5.1.2.4 Discovery Service (DS)

SWITCH operates and maintains a central Discovery Service (also known as a Where Are You From (WAYF) service). SPs can either use this central Discovery Service or configure a local Discovery Service. SWITCH provides the SP administrators with the information they require.

---

[29] https://www.switch.ch/aai/participants/
[30] https://rr.aai.switch.ch
[31] https://www.switch.ch/aai/docs/AAI-RR-Guide.pdf
[32] https://www.switch.ch/aai/metadata/
[33] https://www.switch.ch/pki/aai/

5.1.2.5 Interfederation

SWITCH is responsible for maintaining relationship with national and international stakeholders in the area of *Federated Authentication and Authorization*, primarily in the academic sector. This includes in particular relationship with interfederation[34] activities.

If it benefits the SWITCH Community, SWITCH can enter into agreements on behalf of the SWITCHaai Federation and exchange metadata; for example, with other federations and/or interfederation services.

Through participation in interfederation, organisations can offer their services to end users of other federations and enable their own end users to access the services of other federations. Through participation in interfederation, organisations help reduce the number of local end user accounts.

5.1.2.6 Virtual Home Organisation (VHO)

The Virtual Home Organisation[35] is the IdP of last resort for the small subset of end users who should have access to a given SWITCHaai protected service, but who have not received a digital identity from their organisation.

SWITCH operates and maintains the Virtual Home Organisation IdP combined with a web application for the administration of VHO Accounts, insofar as this is necessary.

SP Administrators can submit a request to SWITCH to manage their own group of such end users in the VHO. They must comply with the SWITCHaai VHO Policy[36].

Every SWITCHaai Participant can also request a VHO account for testing purposes.

SWITCH can provide the required functions for the administration of such non-organisational identities, group memberships or affiliations of organisations without their own AP through the provision of other components.

5.1.3 Rights and obligations of SWITCHaai Participants

5.1.3.1 Cooperation

The SWITCHaai Participant works with SWITCH and takes all measures required to ensure the smooth functioning of the SWITCHaai Federation. This includes the provision of required information, data, equipment, (access) rights and other services. In particular, the SWITCHaai Participant refrains from modification of the services and systems operated in the SWITCHaai Federation, or use of them in a manner contrary to the purpose.

As the AP Operator, the organisation is responsible for the correct provision of the Affiliation Attributes for an existing SWITCH edu-ID base identity. See chapter 5.1.3.8.

As the IdP Operator, the organisation is responsible for correct authentication processing and the correct issuance of Base Attributes. See chapter 5.1.3.9.

SWITCHaai Participants are obliged to notify SWITCH immediately of personnel changes to their AP, IdP and SP Administrators; otherwise, SWITCH cannot ensure access to

[34] https://www.switch.ch/aai/interfederation/
[35] https://www.switch.ch/aai/vho/
[36] https://www.switch.ch/aai/docs/AAI_VHO_Policy.pdf

operationally relevant data of the SWITCHaai Participant. In addition, SWITCHaai Participants are in that case obliged to change relevant passwords, in particular the API passwords used by the SWITCHaai Participants.

5.1.3.2 Compliance

The SWITCHaai Participant affirms that it will

- install, operate and use the AP, IdP and SP components under its control in accordance with the Federation Technology Profiles
- inform SWITCH of the requisite technical and administrative contacts
- not grant any third party access to the SWITCHaai Federation (its end users excepted) without the written consent of SWITCH
- transfer only truthful information about its own end users, which he has verified, to the SWITCHaai Federation

5.1.3.3 Collaboration with administrators of the organisations

SWITCH provides a 3rd level Service Desk for the AP and IdP Administrators entered in the Resource Registry. This can be reached via e-mail and telephone[37] during normal business hours.

5.1.3.4 Support

The SWITCHaai Participant provides its end users with 1st level support (e.g. Service Desk), which can handle queries independently during local business hours. The SWITCHaai Participant provides its SP Administrators with 2nd level support.

5.1.3.5 Design Guidelines

SWITCHaai Participants are obliged to follow the SWITCHaai Design Guidelines[38] for end user interface elements.

SWITCH logos may be used only as described in the Design Guidelines. SWITCH logos are protected by trademark. Any use by third parties in breach of the Design Guidelines is reserved and requires the written consent of SWITCH.

5.1.3.6 Bilateral agreements within the SWITCHaai Federation

SWITCHaai Participants may enter into bilateral agreements concerning the provision of and/or access to services. SWITCHaai Participants are liable for any consequences resulting from such agreements and SWITCH bears no responsibility for them.

5.1.3.7 Technical accounts in SWITCH edu-ID

AP Operators may create technical accounts and assign them one or more of their affiliations. Use cases for technical accounts are:

[37] https://www.switch.ch/aai/
[38] https://www.switch.ch/aai/guides/design/

- Execution of tests
- Use for technical purposes like monitoring (e.g. for the automated login on a particular SP)
- When the use of impersonal accounts is mandatory
- When several end users must use one generic SWITCH edu-ID (e.g. when sharing a role).

In such cases, the AP Operator assumes liability for each account which is registered in his Organisation Administration Interface. The AP Operator may delegate liability internally to one of his AP Administrators and he ensures that e-mails can be received by the e-mail addresses registered in these accounts. When not in use, the AP Operator must delete the technical or test account immediately. SWITCH sends regular reminders about such accounts to the AP Operator.

5.1.3.8 Obligations of an AP Operator

The AP Operator complies with this Service Description and ensures that its end users also comply with it. Misuse of attribute values from an AP will be attributed to the relevant AP Operator.

The AP Operator

- ensures the correctness of the attribute values assigned by it to the end users
- discloses its IdM processes to another SWITCHaai Participant on request (in particular about the issuance and the withdrawal of Affiliation Attributes)
- reports detected duplicates and/or detected misuse of end user accounts immediately to SWITCH
- enables the SWITCH edu-ID service to update the data of its cached information insofar as it concerns the affiliation

5.1.3.9 Obligations of an IdP Operator

The IdP Operator complies with this Service Description and also ensures compliance of its end users. Misuse of a digital identity is attributed to the IdP Operator on which IdP the respective end user was authenticated.

The IdP Operator

- ensures that it can identify its end users
- discloses its IdM processes to another SWITCHaai Participant on request (including identification, authentication, on and off-boarding)
- undertakes to activate the User Consent Dialog[39] when participating in interfederation with the IdP

[39] https://www.switch.ch/aai/guides/idp/

5.1.3.10 Obligations of an SP Operator

In order to grant access, provide the service and data cleaning, SPs rely on successful authentication by the IdP, and the received attributes. SP Operators are obliged to use the received data, including personal information, for this purpose only.

Services requesting the Extended Attribute Model can potentially access additional or all affiliation attributes of an end user. They are therefore obliged to request and obtain the consent of the end user about the recurring transfer of their data from the SWITCH edu-ID IdP (e.g. in their own terms of use). The SP operators are obliged to inform the end user that they will query or update their data without the end user being online or involved. SWITCH grants access to an API for such a purpose only when the service meets these requirement (see also chapter 6.3.6).

End users are authorized to request that a service ceases to update their data, given that they won't use the service any more. The service must then ensure that no further query or update takes place from then on.

5.1.3.11 Data updates at Service Providers

With each access to a service by an end user, the service receives personal information about the end user which the service is permitted to store, provided that this is needed in order to provide the service. This data that have been obtained through the SWITCH edu-ID IdP, may become obsolete. If deemed necessary for the provision of the service, the service may request updates at the SWITCH edu-ID IdP, without an additional explicit user consent once again.

5.1.3.12 Security of the SWITCH edu-ID identifier

To establish an unambiguous link to the local organisation-related identity, AP Operators may receive the SWITCH edu-ID identifier[40] of their end users. If they do so, they are obliged

1. To store and treat this identifier confidentially at all times and to prevent access by third parties
2. To use the identifier exclusively for the purpose of looking up further personal attributes related to the SWITCH edu-ID IdP or for identity management processes, in particular the prevention of duplicates; for all other purposes, other identifiers should be used
3. To store the identifier only on the required systems
4. To prevent access by end users except in the case of an explicit query

SWITCH supports organisations in their employee training in the use of the SWITCH edu-ID identifier and other personal information.

5.1.3.13 Adoption of the SWITCH edu-ID in an organisation

SWITCH advises organisations as they introduce the SWITCH edu-ID. Typically, the organisation converts its IdP into an AP and some of the processes within the organisation (particularly on and off-boarding) are adapted.

[40] https://www.switch.ch/aai/support/documents/attributes/swisseduid/

Until adoption of the SWITCH edu-ID, the organisation's IdP is responsible for the correct user authentication; then the SWITCH edu-ID IdP takes over.

Until adoption of the SWITCH edu-ID, the organisation's IdP provides the SP with the complete set of required attributes. After the adoption, the task is assumed by the SWITCH edu-ID IdP, which draws some of the information from the organisation's AP.

For the adoption of the SWITCH edu-ID, the organisation defines and implements its on-boarding procedures such that now no new digital identities are created for new end users; instead, a new affiliation is linked to an existing SWITCH edu-ID base identity. The AP provides the respective Affiliation Attributes. The off-boarding is simplified in a similar fashion through cancellation of the affiliation.

With the adoption of the SWITCH edu-ID, the organisation accepts the conditions in this Service Description.

From the time of adoption of the SWITCH edu-ID for the first SWITCHaai Participant, a mixed operation scenario emerges in which some organisations still create digital identities, while others now link their affiliations only to the SWITCH edu-ID identity.

5.2 Conditions of participation

5.2.1 Target audience

SWITCHaai participation is open to organisations of the SWITCH Community, the Extended SWITCH Community and other organisations that generate a benefit for the SWITCH Community.

5.2.2 Fees

SWITCH reserves the right to charge SWITCHaai Federation Partners a fee for their participation in SWITCHaai and the use of other services.

In particular, SWITCH may charge Federation Partners a participation fee for the inter-federation option.

Fees are due within 30 days. If the deadline passes, the respective agreements are void.

5.3 Procedures

5.3.1 Admittance procedure

New organisations may operate SPs and, given the appropriate conditions, an AP or – where justified – an IdP.

In principle, any organisation that wishes to contribute with their services to the operation of SWITCHaai Federation, can submit a corresponding request to SWITCH in order to make its services accessible to SWITCHaai Participants.

An organisation that is not part of the SWITCH Community must submit an official membership application. SWITCH assesses the usefulness of the membership to the SWITCH Community. SWITCH then decides whether membership will be offered.

Another prerequisite for acceptance of an organisation as a SWITCHaai Federation Partner is signature of the SWITCHaai Federation Partner Agreement.

An organisation from the Extended SWITCH Community that joins the SWITCHaai Federation becomes a *Federation Partner Basic* if it offers only services and does not operate an AP or IdP. Under certain circumstances, it may be permitted to operate an AP or IdP in the SWITCHaai Federation. It then receives the role of AP Operator or IdP Operator, and thus becomes a *Federation Partner Plus*.

For SWITCHaai Federation Partners, the price list, this document and the General Terms & Conditions (GTC) apply.

5.3.2 Cancellation procedure

Cancellation of the service is subject to the provisions of the Service Regulations (SR) and the General Terms & Conditions in the current versions[41].

[41] https://www.switch.ch/about/disclaimer/

6 Legal conditions of use

6.1 Applicable provisions

The end user accepts this Service Description when they create their SWITCH edu-ID or use the SWITCH edu-ID service for the first time.

The following provisions, in the current version, apply to organisations and end users for use of the service:

- For organisations of the SWITCH Community and end users that belong to an organisation of the SWITCH Community:
  - this Service Description
  - the respective valid tariff
  - the Service Regulation (SR)

  In the event of disputes, this Service Description takes precedence over the tariff and the tariff over the SR.
- For organisations of the Extended SWITCH Community, for end users that belong to an organisation of the Extended SWITCH Community, for Contractual Partners and end users that belong to a Contractual Partner:
  - this Service Description
  - the SWITCHaai Federation Partner Agreement
  - the General Terms and Conditions (GTC)

  In the event of disputes, this Service Description takes precedence over the Federation Partner Agreement and the Federation Partner Agreement over the GTC.
- For end users that do not belong to any organisation of the SWITCH Community, the Extended SWITCH Community or a Contractual Partner:
  - this Service Description
  - the GTC

  In the event of disputes, this Service Description takes precedence over the GTC.

6.2 Change procedure

SWITCH may change this Service Description at any time and without prior warning to end users; see chapter 5.1.1 Governance. Depending on the significance of these changes, SWITCH may inform end users or obtain their consent before they can continue to use their SWITCH edu-ID account.

Significance of changes and their handling:

a) **Negligible**: For small changes or corrections without a significant effect on the agreements, a change may be carried out and published without notice to end users. If necessary, end users may be notified of the change (e.g. via e-mail or in the 'My edu-ID' web application).

b) Significant: One or more changes that has a direct effect on the agreements is considered significant. Significant changes are discussed in advance with the SWITCH edu-ID Advisory Board and the Trust & Identity WG, as described in chapter 5.1.1.

These changes are then communicated to the organisations in an appropriate manner. If no objection is lodged within 30 days of notification of the change, the change goes into effect. Objection by an organisation will result in termination of the contract. In the event of a significant change, end users must re-accept the terms of use, after notification of the change, when they next log in to a service.

The importance of the change is assessed in each case by the SWITCH legal department.

6.3 Data protection and data security

SWITCH policies concerning the protection and security of data are based on the Service Regulations and the General Terms and Conditions in the most current version[42].

By taking appropriate measures, SWITCH ensures confidentiality, integrity and availability of the entrusted data. These measures include:

- Constructional measures and access limitations to the server infrastructure
- access regulations (user concept, firewall and similar)
- regular server maintenance
- automated service monitoring
- redundant operating concept and creation of back-ups to protect against data loss
- data encryption and signature for transmission of data
- promotion of a culture of privacy by design and by default in terms of data transferred within the federation
- involvement of the end user in processes concerning their data
- staff awareness of data protection issues by means of workshops
- Regulations and instructions
- Contracts

6.3.1 Site of data storage

The data for the service SWITCH edu-ID and in the responsibility of SWITCH are stored on SWITCH infrastructure in Switzerland.

6.3.2 Data processing by SWITCH

The service SWITCH edu-ID is storing data that is entered by end users, other data originating from linked identities, and potentially further data entered by attribute providers. SWITCH takes the appropriate measures to keep these data up to date.

SWITCH generates anonymised statistics for the attention of the organisations and the contract partners.

6.3.3 Duration of the data processing

SWITCH is storing personal data in order to provide the service SWITCH edu-ID, until this data is no longer needed, or until the SWITCH edu-ID account in question is removed. In addition, data may be

[42] https://www.switch.ch/about/disclaimer/

stored according to legal obligations for safekeeping and documentation, or based on operational needs like, e.g., backups.

6.3.4 Responsibility of the SWITCHaai Participant

The SWITCHaai Participant will at all times comply with the applicable provisions and obligations imposed by the Swiss Data Protection Act and the applicable cantonal legislation, insofar as they relate to the processing of personal data within the SWITCHaai Federation. It will also comply with the EU Standard Contractual Clauses (or any stricter terms in certain jurisdictions) and ensure that the relevant sections are included in all agreements relating to the transfer of personal data.

The SWITCHaai Participant must ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of data, and against accidental loss or destruction of this data. The SWITCHaai Participant undertakes to observe any recommendations made by SWITCH in this regard.

All AP Operators and IdP Operators are obliged to follow the instructions concerning *Legal Templates for SWITCHaai*[43].

6.3.5 Responsibility of the end user

All the data entered by the end user – e.g. name, e-mail address, postal address, etc. – must be correct. In order to assist the end user, the SWITCH edu-ID may send reminders.

The end user must choose a secure password and protect it to prevent use by a third party.

The end user must not keep more than one SWITCH edu-ID user account. Duplicates that have been created by mistake must be merged by the end user, or if this is not possible with the aid from the SWITCH edu-ID support[44]. Any data loss caused by merging of accounts – e.g. at previously used services – must be corrected by the end user.

Improper use or misuse of a SWITCH edu-ID account or of the SWITCH edu-ID service, or a breach of these terms of use, may lead to the locking or deletion of the SWITCH edu-ID account in question (see chapter 6.7).

6.3.6 Data processed by the SP operator

Whenever an end user accesses an SP, the SP can request certain data about the end user. The end user's consent is then necessary to release data from the IdP to the SPs. This consent function shows the end user the data prepared for transfer and helps protect their personal information. Chapter 5.1.3.10 remains reserved.

The end user's personal data, such as their name, e-mail address or date of birth attributes, may be used and passed on by service providers exclusively for the following purposes:

- provision of the services offered by Service Providers, including support related to using that service;
- authentication and authorisation
- to contact the end user when necessary

[43] https://www.switch.ch/aai/legaltemplates/
[44] eduid-support@switch.ch

- to find and remove duplicates and out-of-date affiliations

For services using the SWITCH edu-ID for authentication, specific terms of use for data protection may apply.

6.3.7 Audits

The SWITCH edu-ID service is audited regularly in the context of an ISMS[45] process. This involves definition and regular adjustment of the requisite technical and organisational measures for operation of the service.

The SWITCHaai Federation Policy (see chapter 5) does not stipulate *a priori* audits of the SWITCHaai Participants (incl. SWITCH). Certain circumstances may make audits necessary. The right to conduct an audit remains reserved.

6.3.8 Right to information

SWITCH undertakes to respond to enquiries of end users, organisations, services or third parties as foreseen by the Federal Act on Data Protection.

6.4 Collaboration with third parties in Switzerland or abroad

If the organisation and the end user give their consent, personal information may be transmitted to an SP (in Switzerland or abroad) for the purpose of authentication described in chapter 3.2.3.5 and the associated issuance of attributes.

SWITCHaai Participants accept that parts of the information they record when entering their resources in the Resource Registry will be accessible to other participants in the SWITCHaai Federation, and used on the web or in metadata as freely accessible descriptions. If such information is accompanied by terms of use, copyright statements or other statements related to intellectual property, the consumer of this information must comply with these restrictions or contact SWITCH to clarify the use situation.

6.5 Access to data by employees

If data is transferred to SWITCH for processing, it may occur for operational purposes that an organisation/Contractual Partner requires access to data that was stored at the behest of an organisation/Contractual Partner by an employee who is now unavailable.

The organisation/Contractual Partner must then demonstrate with due rigour that it is authorised to access the data in question. If this cannot be adequately demonstrated or for another reason there remains an untenable liability risk to SWITCH, SWITCH is entitled to refuse access.

6.6 Permissible use of the service

Use of the service is permissible only if it does not result in any violation of these terms of use, the rights of third parties or applicable laws.

[45] ISMS: Information Security Management System

6.7 Improper use of the service

Improper use of the service is subject to the provisions of the SR and the GTC in their current versions.

The organisations to which the offending end user belongs can, in addition to the end user, be held responsible and fully liable for all damages incurred by SWITCH or third parties through the improper use of the service by the end user.

On first notice from SWITCH, the organisation to which the offending end user belongs is obliged to defend at its own expense all claims brought against SWITCH in connection with the improper use of the service. The organisation to which the offending end user belongs is obliged to assume jointly and severally all court-related or otherwise associated costs, licence fees and/or damages incurred by SWITCH, provided that SWITCH has informed the organisation concerned in writing of the claim, and has authorised it to conduct and resolve the legal dispute within the scope of the applicable procedural law, in particular through judicial or out-of-court settlement.

SWITCH reserves the right, in the event of well-founded suspicion of illegal or non-contractual use of the service, to immediately delete the affected accounts and/or temporarily or permanently block the registered end user without prior notification of the end user or organisation concerned, without entitlement of the end user or organisation concerned to any compensation claims.

Moreover, in order to ensure proper operation, SWITCH may at any time and without suspicion of improper use, require that registered end users reset their passwords, re-initiate their authentication procedure, or utilize strong authentication, like, e.g. MFA.

End users and organisations are required to assist SWITCH in clarifying incidents of improper use, criminal acts and other cases of damage.

Furthermore, SWITCH reserves the right in all cases, where this is legally required or appropriate, to work together with the responsible state authorities and to provide all information necessary to prosecute the legal violation in this connection.

6.8 Warranty

The warranty is subject to the provisions of the SR and the GTC in the current version in conjunction with the availability affirmed in chapter 3.3.

SWITCH assumes no liability for any particular outcome in connection with a service provided by an organisation where authentication is processed via the SWITCH edu-ID service.

6.9 Liability

6.9.1 Liability of SWITCH

The liability of SWITCH vis-à-vis the organisations of the SWITCH Community is governed by the provisions of the SR in its current version. SWITCH bears no responsibility for the lawful use of the service.

The liability of SWITCH vis-à-vis the organisations of the Extended SWITCH Community is governed by the provisions of the GTC in its current version.

The liability of SWITCH vis-à-vis end users and third parties that use the service from SWITCH without a separate contract with SWITCH but with the consent of the organisation is, to the extent permitted by law, excluded. In particular, SWITCH cannot assume any liability for data protection violations by organisations or providers of services where authentication is processed via the SWITCH edu-ID service.

6.9.2 Liability of organisations

Organisations are jointly and severally liable to SWITCH within the statutory limits for damage incurred by SWITCH due to improper use of the service, and for other indirect costs. This liability claim remains in effect even if the SWITCHaai or SWITCH edu-ID accounts have already been cancelled.

In particular, the liability includes the technical and test accounts in SWITCH edu-ID, see chapter 5.1.3.7.

6.9.3 Liability of the end user

The end user is responsible for all activities undertaken in connection with their SWITCH edu-ID account, and can be held liable for such by AP Operators, IdP Operators, SP Operators and SWITCH.

The end user is liable to SWITCH within the statutory limits for damage incurred by SWITCH due to the improper use of its SWITCHaai or SWITCH edu-ID account, and for other indirect costs. This liability claim remains in effect even if the SWITCHaai or SWITCH edu-ID account has already been deleted.

In the event of misuse related to their digital identity, the end user has no liability claim against AP Operators, IdP Operators, SP Operators or SWITCH.

6.10 Applicable law and jurisdiction

Use of the SWITCH edu-ID account is subject to Swiss law.

The applicable law and jurisdiction is defined by the provisions of the SR and the GTC in their current versions.

6.11 Language versions

This Service Description exists in a German, a French, an Italian and an English version. All versions are equivalent.

6.12 Revisions

The currently valid version of this document and previous versions are available at https://www.switch.ch/edu-id/terms/