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

Dienstleistungsbeschrieb

SWITCH edu-ID

Version 1.0.4
Gültig ab 18. Mai 2020

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

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

1 Übersicht und Zweck

Dieses Dokument definiert das Konzept und die Regeln für Endbenutzer (die weibliche Form ist mitgemeint), welche für die Verwaltung ihrer digitalen Identität den SWITCH edu-ID Dienst nutzen, und die Regeln für die an der SWITCHaai Federation teilnehmenden Organisationen und Dienstbetreiber.
Entsprechend ist dieses Dokument folgendermassen strukturiert:

- Kapitel 3 umfasst die Definitionen und beschreibt die Funktionen im engeren Sinn.
- Kapitel 4 wendet sich spezifisch an die Endbenutzer.
- Kapitel 5 wendet sich spezifisch an die Organisationen die an der SWITCHaai Federation teilnehmen.
- Kapitel 6 enthält die rechtlichen Nutzungsbestimmungen, welche für Endbenutzer und teilnehmende Organisationen gelten.

Dieses Dokument ist in seiner Gesamtheit verbindlich sowohl für Endbenutzer als auch für Organisationen. Durch die Benutzung des SWITCH edu-ID Dienstes erklären sich Endbenutzer, Organisationen und Dienstbetreiber mit den vorliegenden Bedingungen und Regeln einverstanden.

Das SWITCH edu-ID Konzept basiert auf dem SWITCHaai Konzept und entwickelt dieses weiter. Dieser Dienstleistungsbeschrieb ersetzt daher die SWITCHaai Service Description V1.0 vom 15. Nov 2011 sowie frühere Versionen des SWITCH edu-ID Dienstleistungsbeschriebs.

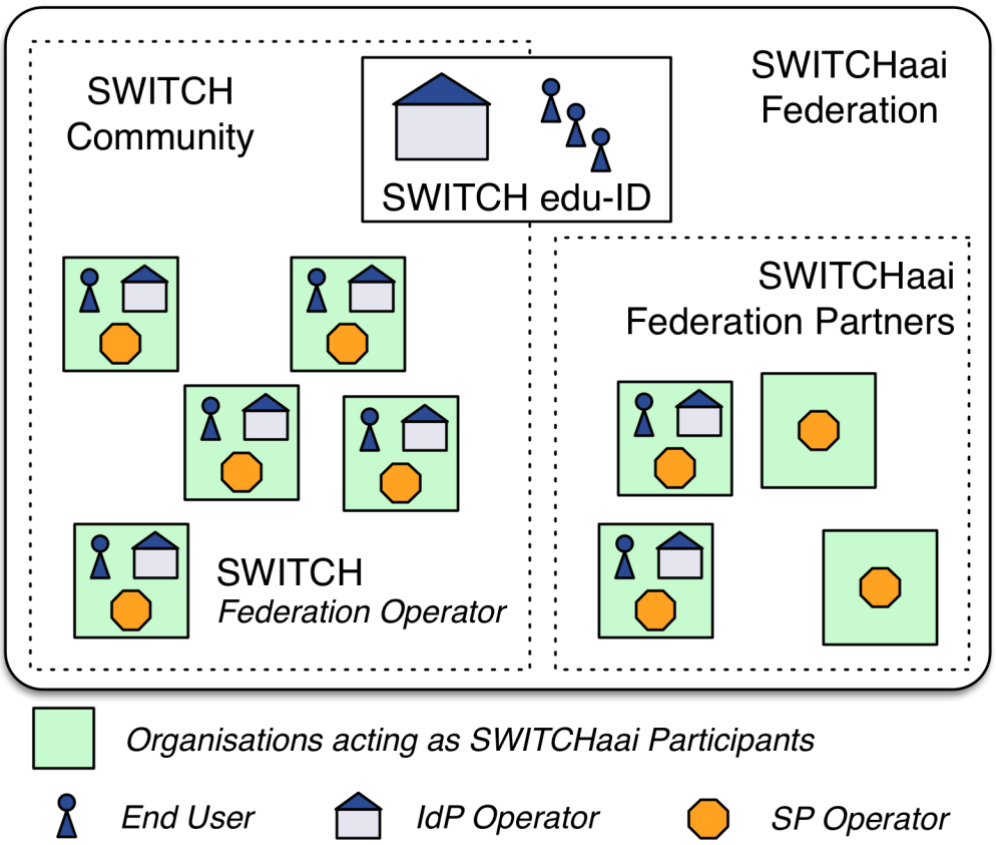
Der SWITCH edu-ID Dienst ist in die SWITCHaai Federation eingebettet. Die Funktionsweise der SWITCHaai Federation ist in Kapitel 5 ausführlich beschrieben.

Die SWITCHaai Federation hat zum Ziel, die organisations-übergreifende Nutzung von Diensten zu vereinfachen und zu fördern. Der Endbenutzer kann seine digitale Identität einsetzen um Dienste zu verwenden, die in der SWITCHaai Federation oder via Interfederation in einer andern Federation registriert sind.

In ihrer Rolle als Federation Operator koordiniert SWITCH dabei die notwendigen Aktivitäten.

Für die SWITCHaai Participants aus der SWITCH Community basiert die Teilnahme an SWITCHaai auf dem Dienstleistungsreglement (DLR)[1] in seiner jeweils gültigen Fassung. Für die Federation Partner basiert die Teilnahme an SWITCHaai auf den Allgemeinen Geschäftsbedingungen (AGB)[2] in ihrer jeweils gültigen Fassung (siehe Kapitel 6.1).

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



Die Beschreibungen von SWITCHaai und SWITCH edu-ID sind öffentlich verfügbar[3]. Die persönlichen Daten sind für Endbenutzer im eigenen Konto in der Webapplikation «Meine edu-ID» unter https://eduid.ch/ abruf- und modifizierbar (vgl. Kap. 3.2.3.4).

Im Projekt *Swiss edu-ID* wurden die Konzepte zur Weiterentwicklung der SWITCHaai geschaffen und die Entwicklung des *SWITCH edu-ID* Dienstes teilfinanziert[4].

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

2 Das Wesentliche für Endbenutzer in Kürze

- SWITCH edu-ID ist ein Dienst von SWITCH, der digitale Identitäten für den lebenslangen Einsatz durch Hochschulangehörige und weitere Endbenutzer verwaltet. Ein SWITCH edu-ID Konto bleibt insbesondere bestehen, wenn der Endbenutzer als Träger der digitalen Identität eine Organisation verlässt (im Unterschied zu einem SWITCHaai Konto).

- Pro Endbenutzer ist nur ein einziges SWITCH edu-ID Konto nötig und erlaubt. Endbenutzer verpflichten sich, Duplikate zu vermeiden und Duplikatskonten zusammenzuführen.

- Endbenutzer verpflichten sich, wahrheitsgetreue Daten anzugeben und diese aktuell zu halten. Insbesondere stellen sie sicher, dass sie unter den angegebenen E-Mail Adressen erreichbar sind. Nicht mehr gültige E-Mail Adressen sind zu löschen und/oder zu ersetzen.

- Endbenutzer sind verantwortlich für alle Aktivitäten im Zusammenhang mit Ihrem SWITCH edu-ID Konto. Sie verpflichten sich daher u.a. ihr SWITCH edu-ID Konto zu schützen und nicht Dritten zu überlassen. Auch wählen sie ein sicheres Passwort und geben dieses nicht weiter.

- SWITCH[5] betreibt den Dienst und verwaltet die Daten nach Schweizer Recht. Die Daten und die Server befinden sich in der Schweiz.

- Nur Daten, welche für die Erbringung des Dienstes SWITCH edu-ID benötigt werden, werden auch gespeichert. Wenn der Endbenutzer sein SWITCH edu-ID Konto mit anderen Identitäten verlinkt, wie z.B. der SWITCHaai Identität an einer Hochschule oder der ORCID[6], können weitere Anwendungsmöglichkeiten verfügbar werden.

- Bei der Anmeldung an Diensten können diese Daten verlangen, welche im SWITCH edu-ID Konto des Endbenutzers hinterlegt sind. Der Endbenutzer entscheidet, ob diese Daten an den Dienst weitergeleitet werden.

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

3 Definitionen und Funktionsbeschreibung

3.1 Definitionen

Affiliation eines Endbenutzers (Organisations-Zugehörigkeit)	Eine *Affiliation* bezeichnet eine Rolle eines Endbenutzers in Bezug auf eine Organisation in der SWITCHaai Federation. Sie entsteht durch das *Verlinken* einer Basisidentität mit der *organisationsbezogenen Identität* des Endbenutzers. Eine Basisidentität kann mit keiner, einer oder mehreren *Affiliationen* eines Endbenutzers verlinkt sein. Eine aktuell bestehende Affiliation wird als *current affiliation* bezeichnet, eine frühere, nicht mehr aktive Affiliation wird als *former affiliation* bezeichnet.
Allgemeine Geschäftsbedingungen (AGB)	Die Allgemeinen Geschäftsbedingungen sind Vertragsbestandteil und auf der SWITCH Webseite[7] verfügbar.
Assertion	Attribute werden üblicherweise in einer digital verschlüsselten und signierten *Assertion* des IdPs zuhanden des SPs ausgestellt. Eine Assertion ist ein gesicherter Container für potentiell vertrauliche Information. Anhand der so erhaltenen Attribute entscheidet der SP oder der durch den SP geschützten Dienst über den Zugang des Endbenutzers zum Dienst.
Attribute (Attribut), Base Attribute (Basis-Attribut), Affiliation Attribute (Affiliations-Attribut), Ergänzendes Attribut (Complementary Attribute)	Ein *Attribut* ist eine beschreibende Informationseinheit mit standardisiertem Namen, z.B. Name, E-Mail, Geburtsdatum, Telefonnummer, *SWITCH edu-ID Identifier* etc. Die in SWITCHaai verwendeten Attribute sind dokumentiert und spezifiziert[8]. Attribute werden oft in Kategorien zusammengefasst, z.B. im Kontext von SWITCHaai in *Core Attributes* und *Other Attributes*, oder im Kontext von SWITCH edu-ID in *Base Attributes*, *Affiliation Attributes* und *Complementary Attributes*. *Base Attributes* sind Bestandteil der *Basisidentität*. *Affiliation Attributes* gehören zur *Affiliation* des Endbenutzers und werden durch einen organisations-spezifischen *Attribute Provider* verwaltet und bereitgestellt. Diese haben folgende Eigenschaften: • Sie werden durch Organisationen ausgestellt; • Sie werden nur während der Dauer der Organisationszugehörigkeit ausgestellt. *Complementary Attributes* werden durch ergänzende *Attribute Provider* verwaltet und bereitgestellt.

7 https://www.switch.ch/about/disclaimer/gtc/
8 https://www.switch.ch/aai/attributes/

Attribute Provider (AP)	Ein *Attribute Provider (AP)* stellt im Kontext von SWITCH edu-ID die organisations-spezifischen Affiliations-Attribute oder die ergänzenden Attribute für einen durch einen *SWITCH edu-ID Identifier* eindeutig bezeichneten Endbenutzer bereit. Im Rahmen des Wechsels zu SWITCH edu-ID ersetzt ein *SWITCHaai Participant* den bestehenden IdP durch einen organisations-spezifischen AP.
AP Administrator	Die ausführende Person des *AP Operators* wird als *AP Administrator* bezeichnet.
AP Operator	Die juristische Person, welche den *SWITCHaai Participant* repräsentiert und welche die Gesamtverantwortung bezüglich des Betriebs eines *Attribute Providers* übernimmt, wird *AP Operator* genannt, siehe Kapitel 5.1.3.8.
Basisidentität (persönlicher Teil der Identität), Self-Declaration, Self Provisioning, Quality Level	Die *Basisidentität* umfasst endbenutzerspezifische Informationen im engeren Sinn wie Name, Vorname, persönliche mobile Telefon-nummer oder persönliche E-Mail Adresse. Beim SWITCH edu-ID Dienst erfasst der Endbenutzer die Daten zur Basisidentität selbst. Dieser Vorgang wird Self-Declaration genannt, und die Basis-identität entsteht damit durch *Self Provisioning*. „Self-provisioned“ ist ebenfalls ein oft verwendeter Wert für den *Quality Level* der in der Basisidentität vorliegenden Informationen. Der Endbenutzer kann den Quality Level der Attribute in seiner digitalen Identität durch Validierungsprozesse erhöhen (lassen).
Classic Attribute Model	Das *Classic Attribute Model* ist kompatibel zu SWITCHaai und kann genau eine Affiliation repräsentieren (vgl. auch *Extended Attribute Model* und die Architektur[9])
Dienstleistungsreglement (DLR)	Das Reglement für den Bezug von SWITCH-Dienstleistungen ist Vertragsbestandteil und auf der SWITCH Webseite[10] verfügbar.
Digitale Identität (Digital Identity, digitale Identifikation)	Eine digitale Identität besteht aus einer Sammlung von Informationen in Form von Attributen, welche einem Endbenutzer zugewiesen werden kann. Sie wird durch einen IdP Operator ausgestellt und bewirtschaftet, welcher den Endbenutzer jederzeit identifizieren kann. Eine digitale Identität kann grundsätzlich nicht nur Personen, sondern auch Dinge beschreiben. Diese Option wird in diesem Kontext nicht vorgesehen. Das SWITCH edu-ID Konto eines Endbenutzers ist eine digitale Identität.

[9] https://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/SwissEduIDArchitecture_Rev1.pdf

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

Endbenutzer	Ein *Endbenutzer* (andernorts auch als Benutzer, Benützer, User oder Enduser benannt) ist eine natürliche Person, welche die Dienstleistung SWITCH edu-ID benutzt. Die weibliche Form ist mitgemeint. Die Nutzung beginnt, indem ein Endbenutzer sein persönliches SWITCH edu-ID Konto anlegt. Der SWITCH edu-ID Dienst richtet sich insbesondere an alle Endbenutzer mit einem Bezug zu Organisationen der SWITCH Community.
Extended Attribute Model	Im *Extended Attribute Model* werden dem Dienst neben der Basisidentität alle aktuellen Affiliationen verfügbar gemacht (s. auch *Classic Attribute Model* und die Architektur[9]).
Extended SWITCH Community	Organisationen, die in enger Verbindung zur SWITCH Community stehen, insbesondere hochschulpolitische Organisationen, Akademien, Förderinstitutionen, Bibliotheken und Spitäler sowie private Forschungseinrichtungen und Schulen im tertiären Bereich, die nicht zur SWITCH Community zählen.
Federated Authentication	Darunter wird der Anmelde-Prozess verstanden, bei welchen die eigene digitale Identität verwendet wird, um Zugang zu Diensten zu erlangen, welche von *SP Operatoren* in der Federation angeboten werden.
Federation (insbesondere die SWITCHaai Federation)	Eine Federation ist ein Zusammenschluss von Organisationen, welche sich zur Zusammenarbeit basierend auf einem gemeinsamen Regelwerk einverstanden erklären. Das Regelwerk betrifft hier die Federated Authentication and Authorization. Die SWITCHaai Federation bezeichnet den entsprechenden Zusammenschluss der schweizerischen Hochschulorganisationen[11]. Der SWITCH edu-ID Dienst ist in die SWITCHaai Federation eingebettet.
Federation Operator	Der Federation Operator verwaltet und entwickelt die Federation weiter. Er ist für die zentralen Komponenten verantwortlich und dient als Kompetenzzentrum. In der SWITCHaai Federation ist SWITCH der Federation Operator.
Federation Technology Profile	In einem Technology Profile wird definiert, welche technischen Details einer spezifischen Technologie (z.B. ein Kommunikationsprotokoll oder eine Programmierschnittstelle) im Kontext der Federation gelten oder wie sie anzuwenden sind.

[11] https://www.switch.ch/aai/participants/

Identity Provider (IdP)	Der Identity Provider ist diejenige Betriebskomponente, welche Endbenutzer authentisiert und zu Handen eines Dienstes eine Assertion über den Endbenutzer ausstellt. Eine Assertion transportiert diejenigen Attribute der digitalen Identität, welche für den Zugang zum Dienst verlangt werden. SWITCH betreibt den zentralen SWITCH edu-ID IdP. Organisationen können ihren eigenen IdP betreiben oder diese Aufgabe an SWITCH delegieren. Der zentrale SWITCH edu-ID IdP unterscheidet sich von den andern IdPs durch zusätzliche Funktionalität (siehe Kapitel 3.2.3)
IdP Administrator	Die ausführende Person des IdP Operators wird als IdP Administrator bezeichnet.
IdP Operator	Ein IdP Operator ist ein SWITCHaai Participant der die Gesamtverantwortung für den Betrieb eines IdPs übernimmt, siehe Kapitel 5.1.3.9. Dies umfasst insbesondere: • Die Identifikation von Endbenutzern; • Die Verwaltung der digitalen Identitäten; • Die Definition von Identifikationsprozessen für Endbenutzer; • Den Einsatz geeigneter Prozesse zur Ein- und Austragung von Endbenutzern, üblicherweise unter Einsatz eines Identity Management Systems (IdM). Diese Verantwortlichkeiten gelten auch für den SWITCH edu-ID Dienst.
Interfederation	Durch Interfederation kann ein Endbenutzer aus einer Federation Zugang zu Diensten aus anderen Federations erhalten. Den SWITCHaai Participants steht Interfederation grundsätzlich offen (siehe Kapitel 5.1.2.5).
Metadata	Metadata umfasst technische Details und beschreibende Information über die in der Federation teilnehmenden Komponenten, insbesondere über IdPs, APs und SPs. Metadata wird üblicherweise durch eine digitale Signatur vor Änderungen geschützt. Die Komponenten in der Federation stützen sich auf diese Metadata ab, um einander auf der technischen Ebene vertrauen zu können. In der SWITCHaai Federation werden die Metadata durch SWITCH verwaltet.
Organisation	Eine Organisation innerhalb der SWITCH Community, der Extended SWITCH Community oder ein Vertragspartner von SWITCH. Organisationen können ihre Dienste ihren eigenen Endbenutzern oder den Endbenutzern von anderen Organisationen anbieten. Umgekehrt können Organisationen ihren Endbenutzer den Zugang zu Diensten ermöglichen, die von anderen Organisationen angeboten werden, indem sie einen Identity Provider (IdP) oder einen Attribute Provider (AP) betreiben.

Quality Level für Base Attributes	Den Werten der Base Attributes kann ein Qualitäts-Indikator mitgegeben werden, welcher über ihr Zustandekommen und damit über ihr Quality Level Auskunft gibt. Bei der Self-Declaration erhalten Attribute wie E-Mail Adresse, Mobil-Nummer oder Postadresse zu Beginn das tiefste Quality Level „self-declared“. Ein Attribut kann durch einen Verifikationsprozess überprüft werden, womit sich bei Erfolg dessen Quality Level erhöhen wird.
Dienst (Service, Service Provider, SP)	Ein Dienst ist eine Webapplikation oder andere Applikation, welche von einer Organisation oder Drittpartei angeboten wird und auf welche Endbenutzer zugreifen können. Der Dienst verlässt sich auf die Authentisierung, des Endbenutzers beim SWITCH edu-ID IdP oder einem anderen IdP der Federation. Für die Autorisierung des Endbenutzerzugriffs evaluiert die Service Provider (SP) Komponente die Informationen zum Endbenutzer, die der SP in der Assertion des IdPs erhält. Auf dieser Basis entscheidet der SP ob dem Endbenutzer der Zugang zum Dienst gewährt werden soll.
SP Administrator	Die ausführende Person des SP Operators wird als SP Administrator bezeichnet.
SP Operator	Ein SP Operator ist ein SWITCHaai Participant, der die Gesamtverantwortung für den Betrieb eines SPs übernimmt, siehe Kapitel 5.1.3.10. Seine wichtigste Aufgabe besteht in der Festlegung der Kriterien für den Zugang zum Dienst (Autorisierung).
SWITCH Community	Alle Organisationen aus dem Bildungs- und Forschungsbereich die mit SWITCH verbunden sind (in Übereinstimmung mit dem Anhang zum DLR).
SWITCH edu-ID Advisory Board	Dieses Gremium[12] besteht aus Vertretern der wichtigen Stakeholder-Gruppen der SWITCHaai Federation. Es berät SWITCH in strategischen Fragen zum SWITCH edu-ID Dienst und zur SWITCHaai Federation.
SWITCH edu-ID (Dienst)	SWITCH edu-ID ist ein digitaler Identitätsdienst, welcher von SWITCH entwickelt wird für die lebenslange Verwendung durch alle Personen in Kontakt mit der Schweizer Hochschul-Community. Der Dienst SWITCH edu-ID ist in Kapitel 3.2 im Detail beschrieben.
SWITCH edu-ID (Identifier)	Der SWITCH edu-ID Identifier ist in Kapitel 3.2.2.2 beschrieben.
SWITCH edu-ID (Identity und Konzept)	Die SWITCH edu-ID Identity ist ein digitales Analogon zu einem Ausweis und kann seinem Träger, dem Endbenutzer, den Zugang zu vielen Diensten ermöglichen. Das Konzept SWITCH edu-ID ist in Kapitel 3.2.1 beschrieben.
SWITCHaai Federation Partner	Eine Organisation, welche nicht zur SWITCH Community gehört und dennoch an SWITCHaai teilnimmt, wird als SWITCHaai Federation Partner bezeichnet.
SWITCHaai Participant	Eine an SWITCHaai teilnehmende Organisation (eine juristische Person) wird als SWITCHaai Participant bezeichnet.

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

Trust & Identity WG	Diese Arbeitsgruppe besteht aus Vertretern aller an SWITCHaai und SWITCHpki teilnehmenden Organisationen der SWITCH Community sowie der Extended SWITCH Community. Sie ist einerseits ein Informationskanal und andererseits eine Austausch-plattform um Feedback zu betrieblichen oder technischen Fragen zu geben.
Verlinkte Identität(en)	Ein Endbenutzer kann seine Basisidentität mit anderen Identitäten verlinken. Verlinkt er sie mit seiner organisationsbezogenen Identität einer Organisation in der SWITCHaai Federation, entsteht eine Affiliation. Ein Endbenutzer kann sie aber auch mit einer externen Identität verlinken, wie z.B. ORCID. So wird z.B. ein externer Identifier als Attribut der Basisidentität hinzugefügt.
Vertragspartner	In diesem Dokument sind Vertragspartner Organisationen, welche mit SWITCH einen Vertrag für eine Dienstleistung abgeschlossen haben, aber weder zur SWITCH Community noch zur Extended SWITCH Community zählen.
Zustimmung zur Datenweitergabe (User Consent)	In vielen Fällen müssen die Endbenutzer der Weitergabe ihrer Attribute pro Dienst mindestens beim ersten Mal zustimmen (wahlweise jedes Mal oder nur nach Änderungen). Üblicherweise erfolgt dies in einem Fenster, welches die zu transferierenden Daten auflistet und den Endbenutzer auffordert zuzustimmen.

3.2 Funktionsweise der SWITCH edu-ID

3.2.1 Das SWITCH edu-ID Konzept

Die SWITCH edu-ID ist eine digitale Identität, welche von SWITCH entwickelt wird und für den lebenslangen Einsatz durch Hochschulangehörige und weitere Endbenutzer vorgesehen ist. Sie soll sicher sein und weltweit anerkannt werden. Der SWITCH edu-ID Dienst baut auf der erfolgreichen, föderierten Identity Management Lösung SWITCHaai auf. Das Identity Management der Hochschulen wird vereinfacht, und weitere Dienste sollen mit dieser digitalen Identität erschlossen werden. Der Dienst SWITCH edu-ID führt im Vergleich zu SWITCHaai folgende Neuerungen ein:

- Nutzer-Zentriertheit (User-Centric) und Langlebigkeit (Persistency): Die digitale Identität gehört dem Endbenutzer, der die Grundinformationen seiner SWITCH edu-ID jederzeit selber kontrollieren kann. Die digitale Identität ist unabhängig von einer Zugehörigkeit zu einer Organisation und bleibt daher insbesondere dann bestehen, wenn der Endbenutzer eine Organisation verlässt.
- Self-Provisioning: Jede natürliche Person kann sich eine elektronische Basisidentität anlegen und wird damit zum Endbenutzer der SWITCH edu-ID. Er behält dabei die volle Kontrolle über eine Reihe von persönlichen Attributen (Base Attributes) wie Name, Vorname, E-Mail Adresse oder Mobiltelefonnummer.
- Quality Levels von Attributen: Self-provisioning führt a priori und naturgemäss zu tiefer initialer Attributqualität. Attribute erhalten daher nicht nur einen Wert, sondern auch einen Qualitäts-Indikator, welcher den Wert ergänzt. Quality Levels können erhöht

werden durch Validierungsprozesse, oder verringert werden z.B. durch Erreichen einer Befristung (Alterung) oder manuelle Veränderung des Wertes.

- Mehrfach-Zugehörigkeit (Multiple Affiliationen): Ein Endbenutzer kann keiner, einer oder mehreren Organisationen angehören. Entsprechend kann seine Basisidentität keine, eine oder mehrere Affiliationen enthalten, je nachdem ob die Basisidentität verlinkt wurde mit den organisationsbezogenen Identitäten an Organisationen in der SWITCHaai Federation. Die zu den Affiliationen gehörenden Informationen werden dabei von teilnehmenden Organisationen übermittelt, üblicherweise durch deren Attribute Providers (APs).

3.2.2 Wie funktioniert der SWITCH edu-ID Dienst?

Verfügt der Endbenutzer über eine Basisidentität, kann er sie grundsätzlich für den Zugang zu einer Reihe von Diensten in der SWITCHaai Federation einsetzen. Der Dienst kann für den Zugang bestimmte Quality Levels für gewisse Basisattribute verlangen, oder er kann zusätzliche Attribute verlangen, welche insbesondere über bestehende Affiliationen Auskunft geben. In der Regel erteilt der Endbenutzer unmittelbar bevor diese Daten dem Dienst zugänglich gemacht werden hierzu sein Einverständnis (User Consent) (vgl. Kap. 4.5).

Nach der erfolgreichen Authentisierung des Endbenutzers überträgt der SWITCH edu-ID IdP alle vom Dienst angeforderten und vom Endbenutzer freigegebenen Attribute sicher zum Dienst. Der Dienst prüft sie und entscheidet über die Zugangserteilung aufgrund seiner Konfiguration.

Insofern erfüllt der SWITCH edu-ID IdP die Anforderungen an einen IdP in der SWITCHaai Federation. Die folgenden Konzepte zeichnen den SWITCH edu-ID Dienst aus:

3.2.2.1 Classic und Extended Attribute Model

Dienste welche mit multiplen Affiliationen umgehen können, unterstützen das *Extended Attribute Model*, d.h. ihnen können alle verfügbaren und vom Endbenutzer freigegebenen Affiliations-Informationen übermittelt werden. Der Dienst entscheidet dann, wie er mit diesen verschiedenen Affiliationen umgeht. Weitere Details können im Swiss edu-ID Architektur-dokument[13] (dort in Kapitel 2.1) nachgelesen werden. Besondere Verpflichtungen für SP Operators in diesem Zusammenhang sind unter Kap. 5.1.3.10 beschrieben.

Alle anderen Dienste erwarten genau eine Affiliation und unterstützen damit das *Classic Attribute Model*. Falls ein Endbenutzer mehrere bestehende Affiliationen besitzt, muss er dem IdP mittels Affiliation Chooser (siehe Kapitel 3.2.3.6) mitteilen, welche Affiliation er für den betreffenden Dienst verwenden will. Nur die zur ausgewählten Affiliation gehörenden Affiliations-Attribute werden dem Dienst übermittelt.

3.2.2.2 Der SWITCH edu-ID Identifier und weitere Identifier

Der SWITCH edu-ID Identifier[14] [15] identifiziert jeden Endbenutzer eindeutig und lebenslang. Dies ist der primäre, für die akademische Community in der Schweiz sektorspezifische

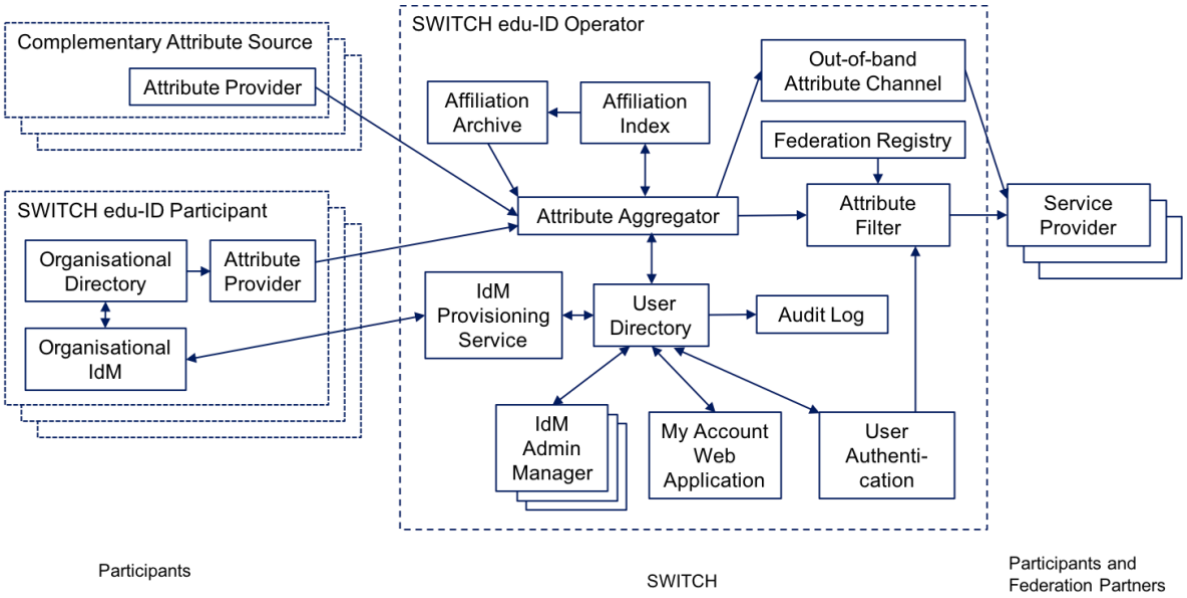
[13] https://www.switch.ch/edu-id/documents/
[14] https://www.switch.ch/aai/support/documents/attributes/swisseduid/
[15] https://swit.ch/eduidspec

Identifier, welcher verwendet wird, um eindeutig weitere Personendaten verknüpfen zu können.

Der SWITCH edu-ID Identifier schafft die Voraussetzung für die Zusammenstellung von Daten, welche als Persönlichkeitsprofil im Sinne des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1)[16] angesehen werden kann, und ist daher entsprechend zu behandeln und zu schützen (siehe Kapitel 5.1.3.12).

Der SWITCH edu-ID Identifier ist Diensten vorbehalten, die in direktem Bezug zum Identity Management an Hochschulen stehen. Benötigt ein Dienst den SWITCH edu-ID Identifier, werden dem SP Operator die entsprechenden Sorgfaltspflichten überbunden. Alle anderen Dienste müssen einen der anderen Identifier verwenden (z.B. einen Pairwise Identifier[17] oder die swissEduPersonUniqueID).

3.2.3 Komponenten des SWITCH edu-ID Dienstes



3.2.3.1 Endbenutzerverzeichnis (User Directory)

Die SWITCH edu-ID Identity (Basisidentität) wird in der zentralen SWITCH edu-ID Datenbank gespeichert. Auf diese Daten wird bei jeder Authentisierung eines Endbenutzers zugegriffen. Jedem Eintrag ist genau ein Endbenutzer zugeordnet. Jeder Endbenutzer ist für die Korrektheit der Daten in seinem Eintrag verantwortlich.

3.2.3.2 Attribute Aggregator

Der Attribute Aggregator stellt sicher, dass der Affiliation Index (s. Diagramm) aktuell ist, indem er mit den verschiedenen organisations-spezifischen Attribute Providern in Kontakt steht.

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

3.2.3.3 SP Notification

Das SP Notification Modul kann optional nach Absprache SPs über Änderungen von Attributwerten informieren. Die SPs erhalten damit die Möglichkeit, ihre eigene Benutzerdatenbank nachzuführen.

3.2.3.4 "Meine edu-ID" Webapplikation (My edu-ID)

Diese Web Applikation erlaubt es dem Endbenutzer, alle seine persönlichen Daten zu überprüfen, aktuell zu halten, ggf. zu erweitern oder verifizieren zu lassen. Zugriffe und Aktivitäten im Zusammenhang mit dem Benutzerkonto werden gespeichert.

3.2.3.5 Identity Provider (IdP)

Der Identity Provider ist für die Endbenutzer-Authentisierung (User Authentication) verantwortlich. Danach stellt er für den SP, der die Authentisierung initiiert hat, die benötigten Attribute zusammen, verlangt vom Endbenutzer falls notwendig die Zustimmung zur Datenweitergabe (User Consent) und gibt die Informationen als Assertion zu Handen des SPs weiter.

3.2.3.6 Affiliation Chooser

Der Affiliation Chooser erlaubt es dem Endbenutzer, wenn nötig, nach der Authentisierung eine seiner bestehenden Affiliationen auszuwählen, mit welcher er sich dann beim Dienst anmeldet. Der Affiliation Chooser wird bei Diensten eingesetzt, welche das Classic Attribute Model verwenden. Der Affiliation Chooser bezieht die Affiliationen aus dem Affiliation Index.

3.2.3.7 Affiliation API und Affiliation Archive

Das Affiliation API dient Attribut Providern einer Organisation dazu, Affiliationen ihrer Endbenutzer auszustellen, zu editieren und zu entfernen und diese Information an den SWITCH edu-ID IdP zu übermitteln. Dies kann via push- oder pull-Methode geschehen.

Stellt der Attribute Aggregator (Pull-Methode) fest, dass eine Affiliation durch den Attribute Provider nicht mehr erneuert wird, verschiebt er seine noch vorliegende Information ins Affiliation Archive der früheren, nicht mehr aktiven Affiliationen. So wird die Information aufbewahrt, dass der Endbenutzer früher einmal mit der Organisation verbunden war. Zukünftige Dienste, z.B. bei Alumni-Organisationen, können sich – die entsprechende Erlaubnis der Endbenutzer vorausgesetzt – spezifisch auf solche Benutzergruppen ausrichten.

3.2.3.8 Administration Interface

Dieses Interface dient der Dienstbetreiberin SWITCH zur Einsicht in Statistiken sowie zur Verwaltung von Endbenutzer- und technischen Konten im Rahmen von Supportanfragen. Das Interface ist einer begrenzten Anzahl von Administratoren zugänglich. Der Zugriff ist nur mit erhöhten Sicherheitsvorkehrungen erlaubt (2-Faktor Authentisierung) und nur für die vorgesehenen Zwecke. Zugriffe und Aktivitäten werden gespeichert.

3.2.3.9 Organisation Administration Interface

Das Interface dient Administratoren von Organisationen zur Einsicht in Statistiken, zur Einsicht und limitierten Verwaltung von Endbenutzerkonten der Organisation sowie der

Verwaltung von technischen Konten der Organisation (vgl. 5.1.3.7). Die Verwendung ist Administratoren der Organisationen vorbehalten und nur für die vorgesehenen Zwecke erlaubt. Zugriffe und Aktivitäten werden gespeichert.

3.2.3.10 Weitere Assistenzsysteme: Test Federation und Demo Sites

SWITCH betreibt und unterhält eine Test Federation[18] zum Zweck des Testens von neuen Komponenten und Konfigurationen. Darin enthalten sind zu Demonstrationszwecken die benötigten Komponenten wie z.B. ein IdP, ein AP oder ein SP, welche die Funktionsweise von SWITCHaai und die Konfigurationsmöglichkeiten im Detail aufzeigen.

3.2.3.11 Weitere Assistenzsysteme: Attribute Viewer

SWITCH stellt unter dem Namen Attribute Viewer[19] einen SP zur Verfügung, der so viele Attribute wie nur möglich vom IdP verlangt, und diese auf einer Webseite zu Handen des Endbenutzers anzeigt.

- Ein IdP kann ihn benutzen, um zu überprüfen, ob seine Attribute korrekt ausgestellt werden.
- Endbenutzer können sehen, welche Attribute ihr IdP über sie ausstellt.
- SP Administratoren oder fortgeschrittene Endbenutzer können bei Verdacht auf Fehlverhalten ihres SPs prüfen, ob ihr IdP korrekt mit dem AAI Attribute Viewer zusammenarbeitet, und so ggf. ein Problem eingrenzen.

Der Attribute Viewer unterstützt derzeit das *Classic Attribute Model*, kann aber bei Bedarf später auch umgebaut werden, um das *Extended Attribute Model* zu unterstützen.

3.3 Verfügbarkeit und Support

Die Dienstleistung steht während 24 Stunden und 7 Tagen pro Woche zur Verfügung. SWITCH erledigt geplante Wartungsarbeiten grundsätzlich ausserhalb der üblichen Bürozeiten und kündigt diese mindestens eine Woche vorher auf der Anmeldeseite des SWITCH edu-ID IdPs an. SWITCH strebt eine Verfügbarkeit des Dienstes und jeder Teilkomponente von mindestens 99.99% an. Störungen, welche zur Beeinträchtigung der Dienstleistung führen, bleiben vorbehalten.

SWITCH verpflichtet sich, innerhalb der üblichen Bürozeiten Massnahmen zur Behebung von Störungen und Fehlfunktionen der Dienstleistung in Angriff zu nehmen bzw. durchzuführen.

Der Endbenutzer-Support[20] ist während der üblichen Bürozeiten besetzt.

Die üblichen Bürozeiten sind im Dienstleistungsreglement (DLR) resp. den Allgemeinen Geschäftsbedingungen (AGB) in der jeweils gültigen Fassung festgehalten.

SWITCH trifft ausserdem Vorkehrungen, um auch ausserhalb der Bürozeiten je nach Dringlichkeit und eigenem Ermessen eine gute Dienstleistungsqualität zu gewährleisten.

18 https://www.switch.ch/aai/demo/
19 https://attribute-viewer.aai.switch.ch/
20 https://help.switch.ch/eduid/

3.4 Monitoring und Logging

Der Betriebszustand des SWITCH edu-ID Dienstes wird auf der öffentlichen SWITCH Webseite laufend dargestellt[21].

Weiterführende Informationen zum Betriebszustand werden den SWITCHaai Participants im Kundenportal[22] zur Verfügung gestellt.

SWITCH kann in Koordination mit den Organisationen deren Komponenten (insbesondere IdPs und APs) überwachen und die Resultate weiteren Organisationen in geeigneter Form zugänglich machen. SWITCH bewirtschaftet zu diesem Zweck dedizierte technische Konten.

Bei Betriebsstörungen befolgt SWITCH den SWITCH-internen Incident Management Prozess. Dieser umfasst die Kommunikation gegen aussen.

SWITCH kann Änderungen im Betriebszustand sowie Transaktionen betreffend Endbenutzerdaten zum Zweck der Rückverfolgbarkeit aufbewahren. Insbesondere können Validierungsprozesse protokolliert werden. Vorhandene Protokolle werden den Endbenutzern auf geeignete Weise zur Verfügung gestellt.

SWITCH erfasst die Nutzung der Dienstleistung durch die Endbenutzer oder die Organisation. Wo möglich erfolgt dies pro Organisation. SWITCH liefert den Organisationen anonymisierte Statistiken zur Nutzung von SWITCH edu-ID.

21 https://www.switch.ch/monitoring/
22 https://portal.switch.ch/

4 Endbenutzerspezifische Informationen

4.1 Erstellung und Zugang

a) Alle Endbenutzer, welche interessiert sind, sich eine lebenslange digitale Identität für den Zugang zu Diensten zu erstellen, können vom SWITCH edu-ID Dienst profitieren.

b) Um den SWITCH edu-ID Dienst zu nutzen, wird ein SWITCH edu-ID Konto benötigt. Dazu müssen mindestens folgende Daten angeben werden:

- Der vollständige Name
- eine gültige und persönliche E-Mail Adresse, und
- ein sicheres Passwort.

c) Endbenutzer können ihren angegebenen Namen, ihre E-Mail Adresse(n) und das Passwort ihres SWITCH edu-ID Kontos jederzeit ändern.

d) Spezifische Dienste können zusätzliche persönliche Attribute wie Geburtsdatum, Wohnadresse, Mobiltelefonnummer etc. verlangen. Zum Beispiel kann eine Bibliothek nur dann Bücher nach Hause senden, wenn eine Wohnadresse angegeben wurde.

e) Service Provider können für die Basisattribute die *Quality Level* Information verlangen. Ein Attribut kann durch einen Verifikationsprozess überprüft werden, womit sich bei Erfolg dessen Quality Level erhöhen wird. So kann z.B. für eine Mobiltelefonnummer hinterlegt werden, dass der Endbenutzer über diese Nummer erreichbar war.

Eine Verifikation kann der Endbenutzer, SWITCH oder eine Organisation durchführen. Eine Verifikation kann einmal oder mehrfach durchgeführt werden. Die Quality Levels sind in der 'Meine edu-ID' Webapplikation ersichtlich.

f) Endbenutzer können ihr SWITCH edu-ID Konto neu anlegen oder aus einem bestehenden SWITCHaai Konto ableiten. Letzteres hat den Vorteil, dass das SWITCH edu-ID Konto bereits (in die eine Richtung, d.h. zur SWITCHaai Identität) verlinkt ist und bestehende Basisattribute bereits in das SWITCH edu-ID Konto übernommen werden können. Bei der Erstellung des SWITCH edu-ID Kontos werden diese Daten bereits als nicht-editierbare Felder dargestellt.

g) Endbenutzer können ihr SWITCH edu-ID Konto auch später mit einem oder mehreren bestehenden SWITCHaai-Konten verlinken und so als Affiliationen hinzufügen. Ebenso ist eine Verlinkung mit externen Identitäten wie z.B. ORCID möglich. Solche Verlinkungen können notwendig sein, falls das SWITCH edu-ID Konto für den Zugang zu Diensten verwendet wird, welche die Identifikatoren der verlinkten Identitäten benötigen.

h) Die Organisationen in der SWITCHaai Federation bestimmen autonom, welche Ihrer Dienste sie individuellen Endbenutzern zur Verfügung stellen wollen und welche Bedingungen für deren Nutzung erfüllt sein müssen. Der Endbenutzer hat grundsätzlich keinen Anspruch auf Zugang zu den Diensten.

4.2 Kontaktinformationen und SWITCH edu-ID-Hilfeseite

Für Fragen in Zusammenhang mit dem SWITCH edu-ID Konto ist die Hilfeseite[23] zu beachten.

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

4.3 Verwaltung von Endbenutzer-Konten

a) Ein SWITCH edu-ID Konto kann durch den Endbenutzer oder mit Vermittlung durch eine Organisation erstellt werden.

b) Da es dem lebenslangen Lernen dient, besteht ein SWITCH edu-ID Konto weiter, wenn der Endbenutzer eine Organisation, z.B. eine Universität oder Forschungsinstitution verlässt (im Gegensatz zu einem SWITCHaai Konto, welches üblicherweise beim Verlassen einer Organisation aufgehoben wird).

c) Nach der Zusammenführung von zwei Konten wird das nicht mehr verwendete Konto gelöscht.

d) Die Löschung einer lebenslangen SWITCH edu-ID Identität widerspricht im Grundsatz deren Zweck. Für die Löschung eines SWITCH edu-ID Kontos kontaktiert der Endbenutzer den SWITCH edu-ID Support[24] per E-Mail. Bei Löschung eines SWITCH edu-ID Kontos werden alle Endbenutzerdaten unwiderruflich gelöscht. Gelöschte Daten verbleiben im Backup gespeichert (üblicherweise während 12 Monaten). Eine Revozierung der Löschung ist jedoch nicht möglich. Ein SWITCH edu-ID Konto kann nur gelöscht werden, wenn es nicht mit *current affiliations* einer Organisation verbunden ist, da sonst der Zugriff auf gewisse Dienste der Organisation(en) nicht mehr möglich ist und die Organisation die Verwendung eines SWITCH edu-ID Kontos voraussetzt.

e) Im Todesfall können Angehörige des Endbenutzers den SWITCH edu-ID Support kontaktieren zwecks Sperrung und/oder Löschung und legen dazu die entsprechenden offiziellen Dokumente vor.

4.4 Der Umgang mit Affiliations-Attributen bei der Beendigung der Organisations-Zugehörigkeit

Wird eine Affiliation beendet, typischerweise beim Austritt von Studierenden oder Mitarbeitenden, können die von der Organisation ausgestellten Affiliations-Attribute naturgemäss nicht mehr weiterverwendet werden.

Insbesondere verliert der Endbenutzer bei Beendigung der Organisations-Zugehörigkeit die Möglichkeit, die in seiner nun nicht mehr gültigen Affiliation (also neu nun eine former affiliation) enthaltenen E-Mail Adressen für die Anmeldung in seinem SWITCH edu-ID Konto oder zur Anmeldung bei Diensten mit SWITCH edu-ID Authentisierung zu verwenden.

Der Endbenutzer ist deshalb verpflichtet, seine Basisattribute, namentlich seine E-Mail Adresse(n), nachzuführen, um das SWITCH edu-ID Konto weiterhin verwenden zu können. Organisation und SWITCH edu-ID benachrichtigen den Endbenutzer frühmöglichst über die angekündigte Beendigung einer Affiliation und informieren ihn über seine Möglichkeiten.

4.5 Zustimmung zur Datenweitergabe (User Consent)

Endbenutzer werden bei der Weitergabe ihrer Attribute an einen Service Provider mindestens beim ersten Zugriff auf den Service gefragt, ob sie dieser Weitergabe ihrer Daten zustimmen. Die Zustimmung erfolgt für jeden Service Provider einzeln. Der Endbenutzer kann darüber hinaus entscheiden, ob er die Zustimmung bei jeder einzelnen Weitergabe von Attributen

[24] eduid-support@switch.ch

oder nur bei einer Änderung der weitergegebenen Attribute erneut erteilen möchte. Üblicherweise erfolgt dies in einem Fenster, welches die weiterzugebenden Attribute auflistet und den Endbenutzer auffordert zuzustimmen.

Technische Identifikatoren und deren jeweilige Werte (vgl Attributspezifikation[25]) werden im User Consent nicht angezeigt, da sie nur maschinenlesbar sind und keine persönlichen Daten enthalten. Die entsprechenden Identifikatoren sind auf der SWITCH edu-ID Webseite[26] beschrieben (vgl. auch Kap. 3.2.2.2).

Gewisse Dienste können ggf. Attribute und deren Werte im Hintergrund aktualisieren oder zusätzliche Attribute beziehen, wenn sie die Benutzer entsprechend informiert haben. Will ein Endbenutzer nicht mehr, dass seine Daten weiterhin bei einem solchen Dienst aktualisiert werden, weil er diesen nicht mehr verwendet, so muss er dies direkt dem betreffenden Dienst mitteilen (vgl. Kap. 5.1.3.10).

4.6 Automatische Deaktivierung und Löschung von Konten

SWITCH edu-ID Konten, welche längere Zeit unbenutzt bleiben, werden in den automatisierten Archivierungs- und Löschprozess aufgenommen. Daneben sind auch Löschungen auf Wunsch des Endbenutzers (siehe Kapitel 4.3) und aufgrund missbräuchlicher Nutzung (siehe Kapitel 6.7) möglich.
Das Vorgehen beim automatischen Deaktivierungs- und Löschprozess sieht wie folgt aus:

- Jährliche Inaktivitäts-Erinnerungen: Der Endbenutzer wird über seine Kontakt-Email Adresse kontaktiert und auf die Nichtbenutzung während 365 Tagen hingewiesen mit der Aufforderung, das SWITCH edu-ID Konto wieder zu benutzen bzw. Kontakt-Daten im Konto zu aktualisieren.
- Nach Ablauf von 4 Jahren erweiterte Inaktivitäts-Erinnerung: Der Endbenutzer wird nun über alle im Konto hinterlegten E-Mail Adressen (auch solche in Affiliationen) daran erinnert, sein Konto wieder zu verwenden bzw. zu aktualisieren, um das Konto weiterhin benutzen zu können.
- Sperrung nach Wartefrist von einem weiteren Jahr: Erfolgt keine Kontaktnahme und bleibt das Konto während weiteren 12 Monaten unbenutzt, so wird dieses mit Mitteilung an alle bekannten E-Mail Adressen gesperrt und kann nicht mehr für eine Anmeldung bei Diensten verwendet werden. Eine Entsperrung kann nun nur noch über den SWITCH edu-ID Support erfolgen.
- Löschung des Kontos nach Ablauf weiterer 5 Jahren: Hat ein Endbenutzer sein SWITCH edu-ID Konto danach während einer Frist von 5 Jahren nicht entsperren lassen, so wird das Konto schliesslich nach 10 Jahren unwiderruflich gelöscht.

Eine Wiedereröffnung kann bei Konten ohne gültige E-Mail Adresse oder bei gesperrten Konten nur über den SWITCH edu-ID Support und nur nach erfolgreicher Identifizierung des Kontoinhabers erfolgen.

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

Gelöschte Daten verbleiben im Backup (üblicherweise während 12 Monaten). Gelöschte SWITCH edu-ID Konten können jedoch nicht wiedereröffnet werden.

5 Die SWITCHaai Federation Policy

5.1 Governance und Rollen

5.1.1 Governance

SWITCH betreibt als Federation Operator die SWITCHaai Federation und konsultiert sowohl das SWITCH edu-ID Advisory Board als auch die Trust & Identity Working Group[27].

Im SWITCH edu-ID Advisory Board sind die wichtigsten Stakeholder Gruppen der teilnehmenden Organisationen vertreten, darunter Vertreter aus der SWITCH Community, aus politischen Gremien im Bildungsbereich und SP Operators. Das SWITCH edu-ID Advisory Board handelt als beratendes Organ hinsichtlich der langfristigen Strategie des SWITCH edu-ID Dienstes.

SWITCH berät sich mit dem SWITCH edu-ID Advisory Board z.B. über Themen wie:

- Welche Kategorien von Federation Partnern akzeptiert werden sollen
- Welche Kategorien von Federation Partnern einen IdP oder AP betreiben dürfen
- Interfederation Vereinbarung
- Planung der zukünftigen Entwicklung der SWITCH edu-ID und der SWITCHaai Federation, sowie administrativer respektive technischer Optimierungen.
- Änderungen in der Verwaltung der SWITCHaai Federation oder dieses Dienstleistungsbeschriebs sowie weiterer spezifisch für die Federation relevanten Dokumente

Das SWITCH edu-ID Advisory Board hat keine Entscheidungsbefugnis. SWITCH entscheidet zusammen mit den mandatierenden Organisationen über die Zusammen-setzung des SWITCH edu-ID Advisory Boards.

Die Trust & Identity WG besteht aus Vertretern aller an SWITCHaai und SWITCHpki teilnehmenden Organisationen der SWITCH Community sowie der Extended SWITCH Community. Diese Gruppe ist informell eingebunden und erhält bei Fragen oder Änderungen die Möglichkeit Feedback zu geben.

SWITCH unterhält enge Beziehungen zu den SWITCHaai Participants. SWITCH organisiert Anlässe an welchen SWITCHaai Participants, insbesondere AP, IdP und SP Administratoren, von neuen Entwicklungen im Bereich *Federated Authentication and Authorization* erfahren und sich darüber austauschen können.

SWITCH verbreitet die Information über die in SWITCH edu-ID und in der SWITCHaai Federation umgesetzten Ideen und Konzepte bei Interessengruppen und Organisationen, welche ähnliche Konzepte übernehmen könnten. Der Fokus liegt dabei auf denjenigen Gruppen, welche das beste Nutzenpotential für die SWITCH Community versprechen.

SWITCH agiert als ein Kompetenzzentrum für *Federated Authentication and Authorization* im akademischen Bildungsbereich. SWITCH testet Software, empfiehlt und dokumentiert Lösungen und stellt Anleitungen bereit zur Installation und/oder Konfiguration ausgewählter

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

Softwarepakete auf gewissen Betriebssystemen zur Verwendung in der SWITCHaai Federation. Beispielkonfigurationen erleichtern dabei die Integration von weiteren Produkten.

Sofern Teilfunktionen nicht anderweitig verfügbar sind, kann SWITCH selber oder durch Auftragserteilung an Dritte fehlende Komponenten entwickeln.

5.1.2 Rechte und Pflichten des Federation Operators

5.1.2.1 Allgemeines

SWITCH ist verantwortlich für den Betrieb der Federation und für die formale Einbindung von relevanten nationalen und internationalen Organisationen.

SWITCH führt und publiziert eine Liste der SWITCHaai Participants[28].

5.1.2.2 Resource Registry (RR)

SWITCH betreibt und unterhält für die Verwaltung der Federation die Resource Registry[29]. APs, IdPs und SPs werden im Kontext der Resource Registry als Ressourcen bezeichnet.

AP, IdP und SP Administrators der SWITCHaai Participants halten alle relevanten Informationen über ihre jeweiligen Ressourcen aktuell. Dies umfasst die Kontakt- und Supportinformation, Einzelheiten zur technischen Konfiguration, Attribute Requirements, Attribute Release Policies, Intended Audience, etc.

Alle diese Daten werden in einer Datenbank gespeichert. Aus dieser Datenbank generiert SWITCH verschiedene Typen von weiteren Dateien welche anderswo verwendet werden, wie z.B. Metadata Dateien oder Attribute Release Konfigurationen für APs und IdPs etc.

Neue SP Einträge sowie Änderungen an bestehenden SPs in der Resource Registry benötigen eine Genehmigung, bevor sie aktiv werden und in den Metadata erscheinen. Dafür sind die "AAI Resource Registration Authority Administrators" des SWITCHaai Participants verantwortlich, der für den SP zuständig ist. Nach entsprechender Überprüfung auf Korrektheit und Konformität genehmigen sie den neuen Eintrag oder die Änderung. Vgl. die Dokumentation zur Resource Registry[30].

5.1.2.3 Metadata Service

SWITCH betreibt und unterhält den Metadata Service[31] welcher die Eigenschaften der SWITCHaai Participants digital signiert und publiziert. Zur Signierung unterhält SWITCH eine speziell dafür vorgesehene offline SWITCHaai Root Certification Authority (CA)[32] deren Zertifikate als Trust Anchor für die Metadata-Überprüfung dienen.

5.1.2.4 Discovery Service (DS)

SWITCH betreibt und unterhält einen zentralen Discovery Service (auch "Where Are You From" (WAYF) Service genannt). SPs können entweder diesen zentralen Discovery Service nutzen oder einen lokalen Discovery Service konfigurieren. SWITCH stellt den SP

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

Administrators die dazu notwendigen Informationen zur Verfügung.

5.1.2.5 Interfederation

SWITCH ist verantwortlich für die Pflege der Beziehungen mit nationalen und internationalen Interessenvertretern im Bereich *Federated Authentication and Authorization* vorwiegend im Hochschul-Bildungsbereich. Dies umfasst insbesondere die Kontakte hinsichtlich Interfederation[33] Aktivitäten.

Sofern dadurch Nutzen für die SWITCH Community entsteht, kann SWITCH im Namen der SWITCHaai Federation Vereinbarungen eingehen und z.B. Metadata mit andern Federations und/oder mit Interfederation Diensten austauschen.

Organisationen können durch die Teilnahme an Interfederation einerseits ihre Dienste Endbenutzern aus anderen Federations anbieten, und andererseits ihren eigenen Endbenutzern den Zugang zu Diensten in anderen Federations ermöglichen. Mit der Teilnahme an Interfederation helfen die Organisationen die Zahl von lokalen Endbenutzer-Konten zu reduzieren.

5.1.2.6 Virtual Home Organisation (VHO)

Die Virtual Home Organisation[34] ist der „IdP of last resort" für einen kleinen Teil der Endbenutzer, welche Zugang zu einzelnen durch SWITCHaai geschützte Dienste erhalten sollten, von der jeweiligen Organisationen jedoch keine digitale Identität erhalten.

SWITCH betreibt und unterhält den Virtual Home Organisation IdP kombiniert mit einer Web Applikation zur Administration der VHO Konten, solange dies erforderlich ist.

SP Administrators können bei SWITCH einen Antrag stellen um ihre eigene Gruppe solcher Endbenutzer in der VHO zu administrieren. Sie halten sich dabei an die SWITCHaai VHO Policy[35].

Jeder SWITCHaai Participant kann zudem für sich ein VHO Konto zu Testzwecken beantragen.

SWITCH kann die erforderlichen Funktionalitäten für die Verwaltung solcher organisationsfremder Identitäten, von Gruppenzugehörigkeiten oder Affiliationen von Organisationen ohne eigenen AP auch mittels anderer Komponenten bereitstellen.

5.1.3 Rechte und Pflichten der SWITCHaai Participants

5.1.3.1 Zusammenarbeit

Der SWITCHaai Participant arbeitet mit SWITCH zusammen und ergreift seinerseits alle für ein reibungsloses Funktionieren der SWITCHaai Federation notwendigen Massnahmen. Dies umfasst z.B. die Bereitstellung der notwendigen Informationen, Daten, Sachmitteln, (Zugriffs-)Rechte und anderen Dienste. Der SWITCHaai Participant verzichtet insbesondere darauf, die in der SWITCHaai Federation betriebenen Dienste und Systeme abzuändern oder sie in zweckfremder Art zu benutzen.

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

Als AP Operator ist die Organisation zuständig für das korrekte Bereitstellen der Affiliations-Attribute zu einer bestehenden SWITCH edu-ID Basisidentität. Siehe Kapitel 5.1.3.8.

Als IdP Operator ist die Organisation verantwortlich für die korrekte Abwicklung der Authentisierung sowie die korrekte Ausstellung der Base Attributes. Siehe Kapitel 5.1.3.9.

Die SWITCHaai Participants sind verpflichtet, personelle Änderungen bei ihren AP, IdP und SP Administrators unverzüglich SWITCH zu melden. Andernfalls kann SWITCH den Zugriff auf betriebsrelevante Daten des SWITCHaai Participants nicht gewährleisten.

5.1.3.2 Compliance

Der SWITCHaai Participant versichert, dass er

- die unter seiner Verantwortung stehenden AP, IdP und SP Komponenten gemäss den Federation Technology Profiles installiert, betreibt und benutzt;
- SWITCH die benötigten technischen und administrativen Kontakte nennt;
- ohne das schriftliche Einverständnis von SWITCH keinem Dritten Zugang zur SWITCHaai Federation gibt (seine Endbenutzer ausgenommen);
- nur wahrheitsgemässe und von ihm geprüfte Angaben über eigene Endbenutzer an die SWITCHaai Federation weiterleitet.

5.1.3.3 Zusammenarbeit mit Administratoren der Organisationen

Den AP und IdP Administrators die in der Resource Registry eingetragen sind, stellt SWITCH einen 3rd-level Service Desk zur Verfügung. Dieser ist während der üblichen Bürozeiten per E-Mail und Telefon[36] erreichbar.

5.1.3.4 Support

Der SWITCHaai Participant stellt seinen Endbenutzern einen 1st-level Support (z.B. Service Desk) zur Verfügung, welcher die Anfragen während der lokalen Bürozeiten selber beantworten kann. Der SWITCHaai Participant stellt seinen SP Administratoren einen 2nd-level Support zur Verfügung.

5.1.3.5 Design Guidelines

SWITCHaai Participants verpflichten sich, die SWITCHaai Design-Guidelines[37] für Endbenutzer Interface Elemente zu befolgen.

Die Logos von SWITCH dürfen nur wie in den Design Guidelines beschrieben verwendet werden. Die Logos von SWITCH stehen unter Markenschutz. Jegliche Verwendung durch Dritte ausserhalb der Design Guidelines bleibt vorbehalten und bedarf der schriftlichen Zustimmung von SWITCH.

5.1.3.6 Bilaterale Abmachungen innerhalb der SWITCHaai Federation

SWITCHaai Participants können bilaterale Abmachungen betreffend Erbringung von und/oder Zugang zu Dienstleistungen treffen. Die SWITCHaai Participants haften für die

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

daraus entstehenden Konsequenzen, und SWITCH übernimmt diesbezüglich keine Verantwortung.

5.1.3.7 Technische Konten bei SWITCH edu-ID

AP Operators können technische Konten erstellen und mit Affiliationen der betreffenden Organisation versehen. Technische Konten sind für folgende Zwecke vorgesehen:

- für die Durchführung von Tests
- für technische Belange wie Monitoring (z.B. automatisierte Logins auf einem SP)
- bei zwingender Notwendigkeit unpersönliche edu-ID Konten einzusetzen
- bei zwingender Notwendigkeit ein generisches edu-ID Konto für die Verwendung durch mehrere Endbenutzer einzusetzen (z.B. für Tätigkeiten, bei welchen sich mehrere Personen eine Rolle teilen).

Der AP Operator übernimmt in allen Fällen die Haftung für von ihm selbst oder auf seinen Wunsch durch SWITCH erstellten technischen Konten, welche im Organisation Administration Interface erfasst sind. Er kann die Haftung intern an einen seiner AP Administrators delegieren und stellt sicher, dass an den hinterlegten E-Mail Adressen auch E-Mails empfangen werden können. Bei Nichtgebrauch löscht der AP Operator das technische Konto unverzüglich. SWITCH sendet regelmässig Erinnerungen über solche Konten an den AP Operator.

5.1.3.8 Verpflichtungen eines AP Operators

Der AP Operator hält diesen Dienstleistungsbeschrieb ein und versichert, dass seine Endbenutzer ihn ebenfalls einhalten. Missbrauch von Attributwerten, welche von einem AP stammen wird dem entsprechenden AP Operator zugewiesen.

Der AP Operator

- stellt die Korrektheit der von ihm den Endbenutzern zugeordneten Attributwerte sicher;
- legt seine IdM-Prozesse auf Verlangen eines andern SWITCHaai Participants offen (insbesondere Vergabe und Rücknahme von Affiliations-Attributen);
- meldet erkannte Duplikate und/oder festgestellten Missbrauch von Endbenutzer - Konten unverzüglich an SWITCH weiter;
- ermöglicht dem SWITCH edu-ID Dienst die Datenaktualisierung seiner zwischengespeicherten Informationen soweit sie die Affiliation betreffen.

5.1.3.9 Verpflichtungen eines IdP Operators

Der IdP Operator hält diesen Dienstleistungsbeschrieb ein und versichert, dass seine Endbenutzer ihn ebenfalls einhalten. Missbrauch einer digitalen Identität wird dem IdP Operator zugewiesen, auf dessen IdP der entsprechende Endbenutzer authentisiert wurde.

Der IdP Operator

- stellt sicher, dass er seine Endbenutzer identifizieren kann;
- legt seine IdM-Prozesse auf Verlangen eines andern SWITCHaai Participants offen (inkl. Identifikation, Authentisierung, On- und Off-Boarding);

- verpflichtet sich bei der Teilnahme an Interfederation beim IdP den User Consent Dialog[38] zu aktivieren.

5.1.3.10 Verpflichtungen eines SP Operators

SPs verlassen sich für die Zugangserteilung, die Erbringung der Dienstleistung und die Datenbereinigung auf die erfolgreiche Authentisierung beim IdP sowie auf die erhaltenen Attribute. SP Operators verpflichten sich, die erhaltenen Daten inkl. Personendaten nur für diesen Zweck zu verwenden.

Dienste, welche das Extended Attribute Model verlangen und damit potentiell auf zusätzliche oder sämtliche Affiliations-Attribute eines Endbenutzers zugreifen können, sind verpflichtet, von den Endbenutzern das Einverständnis über die Weitergabe von Daten bei der SWITCH edu-ID an diesen Dienst einzuholen (z.B. in den Nutzungsbedingungen des jeweiligen Dienstes). Die SP Operators sind verpflichtet den Endbenutzer zu informieren, dass der Dienst diese Daten aktuell halten muss und sie daher abfragen und aktualisieren kann, auch wenn der Endbenutzer gerade nicht online oder beteiligt ist. SWITCH erteilt einen API-Zugang nur, wenn der Dienst diese Vorgaben erfüllt (vgl. auch Kap. 6.3.6).

Ein Endbenutzer ist berechtigt, beim Dienst zu verlangen, dass seine Daten nicht mehr aktualisiert werden, sofern er den Dienst nicht mehr verwendet. Der Dienst muss sicherstellen, dass danach keine Abfrage/Aktualisierung für den entsprechenden Benutzer mehr erfolgt.

5.1.3.11 Datenaktualisierung bei Service Providers

Bei jedem Zugriff eines Endbenutzers auf einen Dienst erhält der SP Operator Attribute über den Endbenutzer und kann diese, soweit in Zusammenhang mit der Nutzung des Dienstes notwendig, bei sich abspeichern. Diese Daten, welche der Dienst via SWITCH edu-ID IdP erhalten hat, können veralten. Der Dienst kann falls nötig zum Zweck der Datenaktualisierung beim SWITCH edu-ID IdP die aktuellen Attributdaten erhalten, ohne dass der Benutzer dazu nochmals seine explizite Einwilligung geben muss.

5.1.3.12 Sicherheit des SWITCH edu-ID Identifiers

AP Operators können zur eindeutigen Verlinkung mit der lokalen organisationsbezogenen Identität den SWITCH edu-ID Identifier[39] ihrer Endbenutzer erhalten. Sie verpflichten sich dabei, diesen Identifier

1. Jederzeit vertraulich aufzubewahren und zu behandeln, und insbesondere nicht Dritten zugänglich zu machen;
2. Ausschliesslich zum Zweck des Nachschlagens von weiteren persönlichen Attributen zu Handen des SWITCH edu-ID IdPs oder für Prozesse des Identitätsmanagements, insbesondere für die Verhinderung von Duplikaten zu verwenden. Für alle anderen Zwecke sind andere Identifier zu verwenden;
3. Nur auf den dazu benötigten Systemen abzuspeichern, und
4. Endbenutzern nicht ohne explizite Nachfrage zugänglich zu machen.

[38] https://www.switch.ch/aai/guides/idp/
[39] https://www.switch.ch/aai/support/documents/attributes/swisseduid/

SWITCH unterstützt die Organisationen in der Schulung ihrer Mitarbeitenden zum Umgang mit dem SWITCH edu-ID Identifier und weiteren personenbezogenen Daten.

5.1.3.13 Die Einführung der SWITCH edu-ID bei einer Organisation

SWITCH steht den Organisationen bei der Einführung der SWITCH edu-ID beratend zur Seite. Üblicherweise wandelt die Organisation dabei ihren IdP in einen AP um, und ein Teil der Abläufe innerhalb der Organisation (insbesondere On-boarding/Off-boarding) wird angepasst.

Bis zur Einführung der SWITCH edu-ID ist der IdP der Organisation für die korrekte Benutzer-Authentisierung (User Authentication) verantwortlich, danach der SWITCH edu-ID IdP.

Bis zur Einführung der SWITCH edu-ID stellt der IdP der Organisation dem SP das komplette Set der benötigten Attribute bereit; danach übernimmt dies der SWITCH edu-ID IdP, welcher dazu einen Teil der Informationen beim AP der Organisation bezieht.

Für die Einführung der SWITCH edu-ID definiert und implementiert die Organisation ihre On-boarding-Abläufe neu so, dass für neue Endbenutzer keine neuen digitalen Identitäten mehr erstellt werden, sondern dass eine neue Affiliation mit einer bestehenden SWITCH edu-ID Basisidentität verlinkt wird. Der AP stellt die entsprechenden Affiliations-Attribute bereit. Analog wird der Off-boarding-Ablauf vereinfacht, indem nur noch die Affiliation aufgehoben wird.

Mit der Einführung der SWITCH edu-ID akzeptiert die Organisation die Bestimmungen in diesem Dienstleistungsbeschrieb.

Vom Zeitpunkt der Einführung der SWITCH edu-ID beim ersten SWITCHaai Participant findet ein Mischbetrieb statt, in welchem die einen Organisationen noch selbst digitale Identitäten erstellen, andere hingegen nur noch ihre Affiliation(en) mit der SWITCH edu-ID Identität verlinken.

5.2 Teilnahmebedingungen

5.2.1 Zielpublikum

An SWITCHaai teilnehmen können Organisationen der SWITCH Community, der Extended SWITCH Community, sowie weitere Organisationen sofern sie Nutzen für die SWITCH Community generieren.

5.2.2 Gebühren

SWITCH behält sich vor, von SWITCHaai Federation Partnern für die Teilnahme an SWITCHaai sowie die Nutzung weiterer Dienstleistungen Gebühren zu erheben.

Insbesondere kann SWITCH von Federation Partnern eine Teilnahmegebühr für die Interfederation Option erheben.

Gebühren sind jeweils innert 30 Tagen fällig. Verstreicht die Frist, werden die entsprechenden Vereinbarungen hinfällig.

5.3 Abläufe

5.3.1 Vorgehen bei Eintritt

Neue Organisationen können SPs und unter entsprechenden Voraussetzungen einen AP oder – in begründeten Fällen – einen IdP betreiben.

Grundsätzlich kann jede Organisation, welche durch den Betrieb von Diensten zur SWITCHaai Federation beitragen will einen entsprechenden Antrag an SWITCH stellen, um so ihre Dienste den SWITCHaai Participants zugänglich zu machen.

Eine Organisation, die nicht der SWITCH Community angehört stellt für die Aufnahme in die SWITCHaai Federation ein formelles Beitrittsgesuch. Dabei beurteilt SWITCH insbesondere den Nutzen des Beitritts für die SWITCH Community. SWITCH entscheidet abschliessend über den Beitritt.

Voraussetzung für die Aufnahme einer Organisation als SWITCHaai Federation Partner ist die Unterzeichnung des SWITCHaai Federation Partner Agreements.

Eine Organisation aus der Extended SWITCH Community, welche der SWITCHaai Federation beitritt, wird zum *Federation Partner Basic* wenn sie nur Dienste anbietet und keinen AP oder IdP betreibt. Unter gewissen Bedingungen kann sie auch berechtigt werden, einen AP oder einen IdP in der SWITCHaai Federation zu betreiben. Sie erhält damit entsprechend die Rolle des AP Operators oder eines IdP Operators und wird so zum *Federation Partner Plus*.

Für SWITCHaai Federation Partner sind die Preisliste, dieses Dokument sowie die Allgemeinen Geschäftsbedingungen (AGB) anwendbar.

5.3.2 Vorgehen bei Kündigung der Dienstleistung

Bezüglich Kündigung der Dienstleistung gelten die Bestimmungen des Dienstleistungs-reglements (DLR) bzw. der Allgemeinen Geschäftsbedingungen (AGB) in ihrer jeweils gültigen Fassung[40].

[40] https://www.switch.ch/de/about/disclaimer/

6 Rechtliche Nutzungsbestimmungen

6.1 Anwendbare Bestimmungen

Der Endbenutzer stimmt diesem Dienstleistungsbeschrieb zu, wenn er sein SWITCH edu-ID Konto anlegt oder erstmals den SWITCH edu-ID Dienst benutzt.

Für die Nutzung der Dienstleistung sind für Organisationen und Endbenutzer folgende Bestimmungen in der jeweils gültigen Fassung anwendbar:

- Für Organisationen der SWITCH Community sowie für Endbenutzer, welche einer Organisation der SWITCH Community angehören:
  - dieser Dienstleistungsbeschrieb
  - der jeweils gültige Tarif
  - das Dienstleistungsreglement (DLR)

  Bei Widersprüchen geht dieser Dienstleistungsbeschrieb dem Tarif und der Tarif dem DLR vor.
- Für Organisationen der Extended SWITCH Community, für Endbenutzer, welche einer Organisation der Extended SWITCH Community angehören, für Vertragspartner sowie für Endbenutzer, welche einem Vertragspartner angehören:
  - dieser Dienstleistungsbeschrieb
  - das SWITCHaai Federation Partner Agreement
  - die Allgemeinen Geschäftsbedingungen (AGB)

  Bei Widersprüchen gehen dieser Dienstleistungsbeschrieb dem Federation Partner Agreement und das Federation Partner Agreement den AGB vor.
- Für Endbenutzer, welche keiner Organisation der SWITCH Community, der Extended SWITCH Community und keinem Vertragspartner angehören:
  - dieser Dienstleistungsbeschrieb
  - die AGB

  Bei Widersprüchen geht dieser Dienstleistungsbeschrieb den AGB vor.

6.2 Vorgehen bei Änderungen

SWITCH kann jederzeit und ohne Vorankündigung gegenüber den Endbenutzern diesen Dienstleistungsbeschrieb abändern (siehe Kapitel 5.1.1 Governance). Je nach Gewicht dieser Änderungen kann SWITCH die Endbenutzer informieren oder deren Einverständnis abholen, bevor diese ihr SWITCH edu-ID Konto weiter nutzen können.

Gewicht der Änderungen und deren Handhabung:

a) **Unbedeutend**: Bei kleineren Änderungen oder Korrekturen ohne wesentliche Auswirkung auf die Vereinbarungen kann eine Änderung ohne Benachrichtigung an die Endbenutzer stattfinden und publiziert werden. Gegebenenfalls können die Endbenutzer auf die Änderungen hingewiesen werden (z.B. per E-Mail oder in der 'Meine edu-ID' Webapplikation).

b) Wesentlich: Eine oder mehrere Änderungen, welche eine direkte Auswirkung auf die Vereinbarungen haben, gelten als wesentlich. Wesentliche Änderungen werden vorgängig mit dem SWITCH edu-ID Advisory Board und der Trust & Identity WG

diskutiert wie in Kapitel 5.1.1 vorgesehen. Den Organisationen werden diese Änderungen anschliessend in geeigneter Weise kommuniziert. Ohne Widerspruch innert 30 Tagen ab Mitteilung der Änderung treten diese in Kraft. Ein Widerspruch durch eine Organisation hat eine Vertragsbeendigung zur Folge. Bei wesentlichen Änderungen müssen die Endbenutzer die Nutzungsbedingungen nach Hinweis auf die Änderungen bei der nächsten Anmeldung an einem Dienst erneut akzeptieren.

Das Gewicht der Änderungen wird jeweils von der Rechtsabteilung von SWITCH eingestuft.

6.3 Datenschutz und Datensicherheit

SWITCH richtet sich hinsichtlich Datenschutz und Datensicherheit nach dem Dienstleistungsreglement bzw. den Allgemeinen Geschäftsbedingungen in der jeweils gültigen Version[41].

SWITCH stellt durch geeignete Massnahmen Vertraulichkeit, Integrität und Verfügbarkeit der anvertrauten Daten sicher. Diese Massnahmen umfassen unter anderem:

- Bauliche Massnahmen und Zugangsbeschränkungen zur Server-Infrastruktur
- Zugriffsregelung (Benutzerkonzept, Firewall und dergleichen)
- Regelmässige Serverwartungen
- Automatisierte Dienstüberwachung
- Redundantes Betriebskonzept und Anlegen von Backups zum Schutz vor Datenverlusten
- Datenverschlüsselung und Signatur bei der Übermittlung von Daten
- Förderung einer Kultur der Sparsamkeit bei der Datenweitergabe innerhalb der Federation
- Einbindung des Endbenutzers in Prozesse, welche seine Daten betreffen
- Sensibilisierung des Personals für Datenschutzfragen durch Workshops
- Reglemente und Weisungen
- Verträge

6.3.1 Datenstandort

Die für die Dienstleistung SWITCH edu-ID bei SWITCH gespeicherten Daten befinden sich in der SWITCH Infrastruktur in der Schweiz.

6.3.2 Datenbearbeitung durch SWITCH

Der SWITCH edu-ID Dienst speichert Daten, welche von Endbenutzern hinterlegt werden, solche aus verlinkten Identitäten und allenfalls weitere Daten, welche von Attribut Providern hinterlegt werden. SWITCH trifft die nötigen Massnahmen, um diese Daten aktuell zu halten.

Zu Handen der Organisationen und Vertragspartner erstellt SWITCH anonymisierte Statistiken.

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

6.3.3 Dauer der Datenbearbeitung

SWITCH speichert Personendaten um die Dienstleistung SWITCH edu-ID bereitzustellen, bis diese Daten nicht mehr benötigt werden oder bis das betreffende SWITCH edu-ID Konto gelöscht wird. Darüber hinaus können Daten aufgrund gesetzlicher Aufbewahrungs- und Dokumentationspflichten oder betrieblicher Notwendigkeit wie beispielsweise Backups gespeichert werden.

6.3.4 Verantwortung des SWITCHaai Participants

Der SWITCHaai Participant hält jederzeit sowohl die Bestimmungen des schweizerischen Bundesgesetzes über den Datenschutz als auch die kantonalen Bestimmungen ein, soweit sie den SWITCHaai Participant und die Bearbeitung von Personendaten innerhalb der SWITCHaai Federation betreffen. Zudem hält er die EU Standard Contractual Clauses (oder jegliche strengere Auslegung in bestimmten Rechtssprechungen) ein und stellt sicher, dass die entsprechenden Abschnitte in die weiteren Verträge aufgenommen werden, welche den Transfer von Personendaten betreffen.

Zu diesem Zweck trifft der SWITCHaai Participant geeignete technische und organisatorische Massnahmen gegen unbefugte oder gesetzeswidrige Verarbeitung von Daten und gegen unbeabsichtigten Verlust oder Zerstörung dieser Daten. Er beachtet allfällige diesbezügliche Empfehlungen von SWITCH.

Jeder AP Operator und jeder IdP Operator ist verpflichtet, die Anleitungen betreffend *Legal Templates for SWITCHaai*[42] zu beachten.

6.3.5 Verantwortung des Endbenutzers

Alle durch den Endbenutzer eingetragenen Daten wie Name, E-Mail Adresse, Postadresse etc. müssen der Wahrheit entsprechen. Zur Unterstützung kann der SWITCH edu-ID Dienst Erinnerungen an den Endbenutzer senden.

Der Endbenutzer muss ein sicheres Passwort wählen und so schützen, dass sein SWITCH edu-ID Konto nicht von Dritten verwendet werden kann.

Der Endbenutzer darf nicht mehr als ein SWITCH edu-ID Konto führen. Irrtümlich erstellte Duplikate sind vom Endbenutzer selbst, oder wenn das nicht möglich ist, vom SWITCH edu-ID Support[43] zusammenzuführen. Allfällige durch Zusammenführung von Konten verursachte Datenverluste, z.B. bei zuvor benutzten Diensten, sind vom Endbenutzer zu korrigieren.

Unzulässige oder missbräuchliche Nutzung eines SWITCH edu-ID Kontos oder des SWITCH edu-ID Dienstes, oder ein Verstoss gegen die in diesem Dokument formulierten Nutzungsbedingungen kann zur Sperrung oder Löschung des betroffenen SWITCH edu-ID Kontos führen (siehe Kapitel 6.7).

6.3.6 Datenbearbeitung durch den SP Operator

Bei jedem Zugriff eines Endbenutzers auf einen Dienst kann der SP gewisse Daten über den Endbenutzer verlangen. Dabei ist die Zustimmung des Endbenutzers notwendig, damit seine Daten vom IdP zu Handen des SPs freigegeben werden können. Diese Zustimmungsfunktion

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

(User Consent) zeigt dem Endbenutzer die freizugebenden und zu übertragenden Daten auf und hilft ihm, seine persönlichen Daten zu schützen. Vorbehalten bleibt Kap. 5.1.3.10.

Persönliche Daten (Attribute) des Endbenutzers wie z.B. Name, E-Mail Adresse oder Geburtsdatum dürfen von Service Providern ausschliesslich für die folgenden Zwecke benutzt und weitergegeben werden:

- Für die Erbringung der von Service Providern angebotenen Dienstleistungen inklusive mit der Nutzung des Dienstes verbundener Support
- Authentisierung und Autorisierung
- Um den Endbenutzer nötigenfalls zu kontaktieren
- Um Duplikate und frühere, nicht mehr aktive Affiliationen aufzuspüren und zu bereinigen.

Für Dienste, welche ihre Authentisierung über die SWITCH edu-ID abwickeln, können spezifische Nutzungsbedingungen bezüglich Datenschutz gelten.

6.3.7 Audits

Der SWITCH edu-ID Dienst wird regelmässig im Rahmen eines ISMS[44]-Prozesses überprüft. Dadurch werden die notwendigen technischen und organisatorischen Massnahmen zum Betrieb des Dienstes festgelegt und regelmässig angepasst.

Die SWITCHaai Federation Policy (siehe Kapitel 5) sieht a priori keine Audits bei den SWITCHaai Participants (inkl. SWITCH) vor. Gewisse Umstände können Audits nötig machen. Diese bleiben daher vorbehalten.

6.3.8 Auskunftsrecht

Datenauskünfte werden auf Anfrage von Endbenutzern, Organisationen, Diensten oder Dritten erteilt, sofern sie gemäss Bundesgesetz über den Datenschutz dazu berechtigt sind.

6.4 Zusammenarbeit mit Dritten im In- oder Ausland

Sofern sowohl die beteiligten Organisationen als auch die beteiligten Endbenutzer ihr Einverständnis geben, können Personendaten zwecks der in Kapitel 3.2.3.5 beschriebenen Authentisierung und der damit verbundenen Ausstellung von Attributen zu einem SP in der Schweiz oder im Ausland gelangen.

SWITCHaai Participants akzeptieren, dass Teile der Information, welche sie beim Eintragen ihrer Dienste (Ressourcen) in die Resource Registry erfassen für andere Teilnehmer in der SWITCHaai Federation zugänglich werden und im Web oder in den Metadata als frei zugängliche Beschreibung dienen. Falls solche Information durch Nutzungsbedingungen, Copyright Statements oder anderweitigen Aussagen zu geistigem Eigentum ergänzt ist, muss der Konsument dieser Information diese Einschränkungen befolgen oder mit SWITCH in Kontakt treten, um die Nutzung zu klären.

[44] ISMS: Information Security Management System

6.5 Zugriff auf Daten von Mitarbeitenden

Werden Daten zur Bearbeitung an SWITCH ausgelagert, kann es vorkommen, dass eine Organisation/ein Vertragspartner aus betrieblichen Gründen Zugriff auf Daten benötigt, welche durch einen nicht erreichbaren Mitarbeitenden im Auftrag der Organisation/des Vertragspartners abgelegt wurden.

Die Organisation/der Vertragspartner muss in jedem Fall ausführlich und nachvollziehbar darlegen, dass sie/er berechtigt ist, auf die entsprechenden Daten zuzugreifen. Wo dieser Nachweis nicht eindeutig erbracht wird oder aus sonstigen Gründen ein für SWITCH nicht tragbares Haftungsrisiko bleibt, ist SWITCH befugt, diesen Zugriff zu verweigern.

6.6 Zulässige Nutzung der Dienstleistung

Jegliche Benutzung der Dienstleistung ist nur zulässig, sofern damit keine Verletzung dieser Nutzungsbestimmungen, der Rechte Dritter oder der anwendbaren Gesetze erfolgt.

6.7 Unzulässige Nutzung der Dienstleistung

Bezüglich der unzulässigen Nutzung der Dienstleistung gelten die Bestimmungen des DLR bzw. der AGB in ihrer jeweils gültigen Fassung.

Die Organisationen, denen fehlbare Endbenutzer angehören, können nebst den Endbenutzern für alle Schäden, die bei SWITCH oder Dritten durch die unzulässige Nutzung der Dienstleistung durch diese Endbenutzer entstehen, zur Verantwortung gezogen bzw. vollumfänglich haftbar gemacht werden.

Auf erste Aufforderung von SWITCH hin ist die Organisation, welcher der fehlbare Endbenutzer angehört, verpflichtet, auf eigene Kosten Ansprüche abzuwehren, welche Dritte gegen SWITCH im Zusammenhang mit der unzulässigen Nutzung der Dienstleistung erheben. Die Organisation welcher der fehlbare Endbenutzer angehört, hat die SWITCH gerichtlich oder vergleichsweise auferlegten Kosten, Lizenzgebühren und/oder Schadenersatzpflichten solidarisch zu übernehmen, sofern SWITCH die betroffene Organisation schriftlich über den erhobenen Anspruch informiert und sie im Rahmen des anwendbaren Prozessrechts zur Führung und Beilegung des Rechtsstreits, insbesondere auch mittels gerichtlichen oder aussergerichtlichen Vergleichs, ermächtigt hat.

SWITCH behält sich vor, bei Vorliegen eines begründeten Verdachts der gesetzes- oder vertragswidrigen Nutzung der Dienstleistung sofort und ohne vorgängige Benachrichtigung der betroffenen Endbenutzer oder Organisationen, die betroffenen Konten unverzüglich zu löschen und/oder die betroffenen Endbenutzer temporär oder permanent zu sperren, ohne dass diesen Endbenutzern oder Organisationen deshalb Ersatzansprüche zustehen.

Ferner kann SWITCH zur Sicherstellung eines geordneten Betriebs von den registrierten Endbenutzern auch ohne Verdacht auf eine unzulässige Nutzung jederzeit verlangen, dass diese ihr Passwort neu setzen, bzw. ihr Authentifizierungsverfahren neu initiieren oder eine stärkere Authentisierung (z.B. MFA) einsetzen.

Endbenutzer und Organisationen sind verpflichtet, SWITCH bei der Aufklärung von Vorfällen unzulässiger Nutzung, Erfüllung von Straftatbeständen und von sonstigen Schadensfällen zu unterstützen.

Des Weiteren behält sich SWITCH in allen Fällen, wo dies gesetzlich verlangt ist oder angebracht erscheint, das Recht vor, mit den zuständigen staatlichen Behörden zusammen zu arbeiten und ihnen in diesem Zusammenhang alle notwendigen Informationen zur Verfolgung der gesetzlichen Verstösse zu liefern.

6.8 Gewährleistung

Betreffend Gewährleistung gelten die Bestimmungen des DLR bzw. der AGB in ihrer jeweils gültigen Fassung in Verbindung mit der in Kapitel 3.3 zugesicherter Verfügbarkeit.

SWITCH übernimmt keine Gewähr für einen bestimmten Erfolg im Zusammenhang mit einem Dienst bei einer Organisation, dessen Authentisierung über den SWITCH edu-ID Dienst abgewickelt wird.

6.9 Haftung

6.9.1 Haftung von SWITCH

Die Haftung von SWITCH gegenüber den Organisationen der SWITCH Community richtet sich nach den Bestimmungen des DLR in seiner jeweils gültigen Fassung. SWITCH trägt keine Verantwortung für die rechtmässige Nutzung der Dienstleistung.

Die Haftung von SWITCH gegenüber den Organisationen der Extended SWITCH Community richtet sich nach den Bestimmungen der AGB in ihrer jeweils gültigen Fassung.

Die Haftung von SWITCH gegenüber Endbenutzern und Dritten, welche die Dienstleistung von SWITCH ohne eigenen Vertrag mit SWITCH aber mit Einverständnis der Organisation nutzen, wird, soweit gesetzlich zulässig, wegbedungen. Insbesondere kann SWITCH keine Haftung übernehmen für Datenschutzverletzungen durch Organisationen oder Erbringer von Diensten, deren Authentisierung über den SWITCH edu-ID Dienst abgewickelt wird.

6.9.2 Haftung der Organisationen

Die Organisationen haften SWITCH gegenüber solidarisch im gesetzlichen Umfang für Schäden, die SWITCH durch die unzulässige Nutzung der Dienstleistung entstehen, sowie für sonstige indirekte Schäden. Dieser Haftungsanspruch bleibt auch bestehen, wenn involvierte SWITCHaai- bzw. SWITCH edu-ID-Konten möglicherweise bereits gelöscht sind.

Die Haftung umfasst insbesondere technische Konten bei SWITCH edu-ID, vgl. Kap. 5.1.3.7.

6.9.3 Haftung des Endbenutzers

Der Endbenutzer ist für alle im Zusammenhang mit seinem SWITCH edu-ID Konto erfolgten Aktivitäten verantwortlich und kann dafür von AP Operators, IdP Operators, SP Operators oder SWITCH haftbar gemacht werden.

Der Endbenutzer haftet SWITCH gegenüber im gesetzlichen Umfang für Schäden, die SWITCH durch die unzulässige Nutzung seines SWITCHaai- bzw. SWITCH edu-ID Kontos entstehen, sowie für sonstige indirekte Schäden. Dieser Haftungsanspruch bleibt auch bestehen, wenn das SWITCHaai- bzw. SWITCH edu-ID-Konto möglicherweise bereits gelöscht ist.

Der Endbenutzer hat bei Missbrauch im Zusammenhang mit seiner digitalen Identität keine Haftungsansprüche gegenüber AP Operators, IdP Operators, SP Operators oder SWITCH.

6.10 Anwendbares Recht und Gerichtsstand

Die Nutzung des SWITCH edu-ID Kontos untersteht schweizerischem Recht.

Betreffend anwendbarem Recht und Gerichtsstand gelten die Bestimmungen des DLR bzw. der AGB in ihrer jeweils gültigen Fassung.

6.11 Sprachversionen

Dieser Dienstleistungsbeschrieb existiert in deutscher, französischer, italienischer und englischer Fassung. Alle Sprachversionen sind gleichwertig.

6.12 Revisionen

Die jeweils gültige Fassung dieses Dokuments, sowie vorherige Versionen sind unter https://www.switch.ch/edu-id/terms/ verfügbar.