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

Description du service

SWITCH edu-ID

Version 1.0.2

En vigueur à partir du 01. Janvier 2018

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

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

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

1 Vue d'ensemble et objectif

Le présent document définit le concept et les règles relatifs aux utilisateurs finaux qui utilisent le service SWITCH edu-ID pour la gestion de leur identité numérique, ainsi que les règles relatives aux organisations et aux exploitants du service participant à la SWITCHaai Federation.

Ce document est structuré de la manière suivante :

Le chapitre 3 présente les définitions et décrit les fonctions à proprement parler.

Le chapitre 4 s'adresse spécifiquement aux utilisateurs finaux.

Le chapitre 5 s'adresse spécifiquement aux organisations qui participent à la SWITCHaai Federation.

Le chapitre 6 contient les dispositions légales d'utilisation qui s'appliquent aux utilisateurs finaux et aux organisations participantes.

Ce document a une valeur contraignante dans son intégralité, aussi bien pour les utilisateurs finaux que pour les organisations. En utilisant le service SWITCH edu-ID, les utilisateurs finaux, les organisations et les exploitants du service acceptent les conditions et règles qui y sont énoncées.

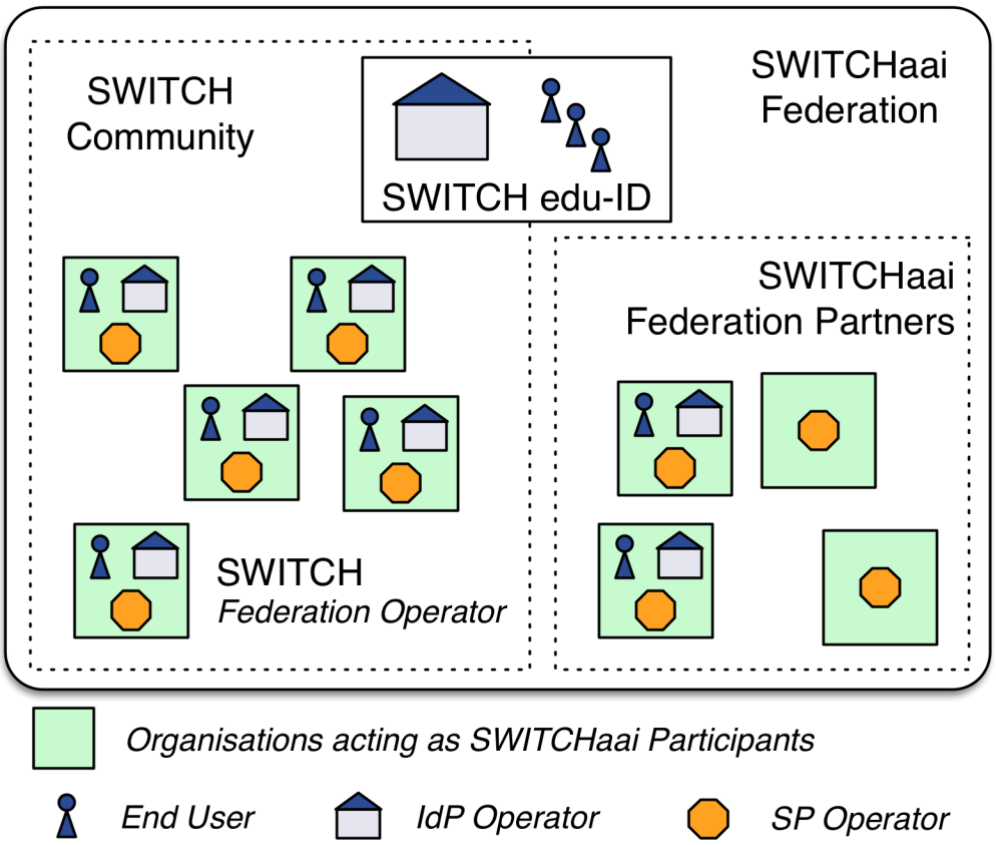
Le concept SWITCH edu-ID est basé sur le concept SWITCHaai et en poursuit le développement. Par conséquent, cette description du service remplace la description du service SWITCHaai V1.0 du 15 novembre 2011.

Le service SWITCH edu-ID est intégré dans la SWITCHaai Federation. Le fonctionnement de la SWITCHaai Federation est décrit en détail au chapitre 5.

L'objectif de la SWITCHaai Federation est de simplifier et de favoriser l'utilisation inter-organisationnelle des services. Les utilisateurs finaux peuvent se servir de leur identité numérique pour utiliser les services enregistrés dans la SWITCHaai Federation ou via Interfederation dans une autre Federation.

Dans son rôle de Federation Operator, SWITCH coordonne les activités requises.

Pour les SWITCHaai Participants issus de la SWITCH Community, la participation à SWITCHaai est basée sur le règlement relatif aux prestations (RRP) dans sa version en vigueur. Pour les Federation Partners, la participation à SWITCHaai est basée sur les conditions générales (CG) dans leur version en vigueur cf. chapitre 6.1).



Les descriptions de SWITCHaai et SWITCH edu-ID sont disponibles publiquement[1]. Le lien indiqué[2] dirige directement vers SWITCH edu-ID.

Dans le cadre du projet *Swiss edu-ID*[3], les concepts relatifs au développement ultérieur de SWITCHaai ont été élaborés et le développement du service *SWITCH edu-ID* a été partiellement financé.

[1] https://www.switch.ch/services/aai/
[2] https://eduid.ch/
[3] https://www.swissuniversities.ch/fr/organisation/projets-et-programmes/p-5/

2 L’essentiel en bref pour les utilisateurs finaux

- SWITCH edu-ID est un service de SWITCH qui gère les identités numériques en vue d’une utilisation valable à vie par les membres des Hautes écoles et d’autres utilisateurs finaux. Un SWITCH edu-ID Account continue d’exister lorsque l’utilisateur final, détenteur de l’identité numérique, quitte une organisation (contrairement à un SWITCHaai Account).

- Le concept prévoit un seul SWITCH edu-ID Account par utilisateur final. Les utilisateurs finaux sont tenus d’éviter les doublons et d’informer l’assistance SWITCH edu-ID s’il en était créés, afin que les comptes puissent être fusionnés.

- Les utilisateurs finaux sont tenus de fournir des données conformes à la réalité et à les tenir à jour.

- Les utilisateurs finaux sont responsables de toutes les activités en rapport avec leur SWITCH edu-ID Account. Ainsi, ils sont tenus de protéger leur SWITCH edu-ID Account et de ne pas le confier à des tiers. Cette obligation inclut la sélection de mots de passe sûrs et l’interdiction de les partager.

- SWITCH[4] exploite le service et gère les données selon le droit suisse. Les données et les serveurs se trouvent en Suisse.

- Seules les données nécessaires à la mise à disposition du service SWITCH edu-ID sont enregistrées. Si l’utilisateur final met en relation son SWITCH edu-ID Account avec d’autres identités, telles que l’identité SWITCHaai dans une université ou ORCID[5], d’autres possibilités d’application peuvent devenir disponibles.

- Lors de la connexion à des services, ces derniers peuvent demander les données enregistrées dans le SWITCH edu-ID Account de l’utilisateur final. L’utilisateur final décide si ces données peuvent être transmises au service.

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

3 Définitions et description des fonctions

3.1 Définitions

Affiliation d'un utilisateur final	Une *affiliation* désigne un rôle d'un utilisateur final en rapport avec une organisation dans la SWITCHaai Federation. Elle est créée par la *mise en relation* d'une identité de base avec l'*identité organisationnelle* de l'utilisateur. Une identité de base peut être mise en relation avec aucune, une seule ou plusieurs *affiliations* d'un utilisateur final. Une affiliation existante est appelée *current affiliation* ; une ancienne affiliation, qui n'est plus active, est appelée *former affiliation*.
Assertion	Les attributs sont généralement émis dans une *Assertion* numériquement chiffrée et signée par l'IdP pour le SP. Une Assertion est un conteneur sécurisé destiné à des informations potentiellement confidentielles. Grâce aux attributs ainsi reçus, le SP ou le service protégé par le SP décide de l'accès de l'utilisateur final au service.
Attributs, **Base Attribute,** **Affiliation Attribute** **Attribut complémentaire (Complementary Attribute)**	Un *attribut* est une unité d'information descriptive possédant un nom standardisé, par ex. nom, e-mail, date de naissance, numéro de téléphone, *SWITCH edu-ID Identifier* etc. Les attributs utilisés dans SWITCHaai sont documentés et spécifiés[6]. Les attributs sont souvent regroupés en catégories, par ex. dans le contexte de SWITCHaai en *Core Attributes* et *Other Attributes*, ou dans le contexte de SWITCH edu-ID en *Base Attributes*, *Affiliation Attributes* et *Complementary Attributes*. Les *Base Attributes* font partie intégrante de l'*identité de base*. Les *Affiliation Attributes* font partie de l'*affiliation* de l'utilisateur final et sont gérés et fournis par un *Attribute Provider* spécifique à l'organisation. Ils ont les propriétés suivantes : • Ils sont émis par des organisations ; • Ils sont émis uniquement pour la durée de l'affiliation. Les *Complementary Attributes* sont gérés et fournis par des *Attribute Providers* complémentaires.
Attribute Provider (AP)	Dans le contexte de SWITCH edu-ID, un *Attribute Provider (AP)* fournit des attributs d'affiliation spécifiques à une organisation ou les attributs complémentaires pour un utilisateur identifié de manière unique par un *SWITCH edu-ID Identifier*. Dans le cadre de la migration vers SWITCH edu-ID, un *SWITCHaai Participant* remplace l'IdP existant par un AP spécifique à l'organisation.
AP Administrator	La personne physique exécutante de l'*AP Operator* est appelée l'*AP Administrator*.

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

AP Operator	La personne morale qui représente le *SWITCHaai Participant* et qui assume la responsabilité globale relative à l'exploitation d'un *Attribute Provider* est appelée l'*AP Operator*, cf. chapitre 5.1.3.8.
Conditions générales (CG)	Les Conditions générales font partie intégrante du contrat et sont disponibles sur le site web de SWITCH[7].
Extended SWITCH Community	Font partie de l'Extended SWITCH Community, les organisations qui sont en étroite relation avec la SWITCH Community, notamment les organisations de politique des universités, les académies, les institutions de promotion, les bibliothèques et les hôpitaux ainsi que les établissements de recherche privés et les écoles du secteur tertiaire qui ne font pas partie de la SWITCH Community.
Federated Authentication	Ce terme se rapporte au processus de connexion lors duquel la propre identité numérique est utilisée pour accéder à des services proposés par les *SP Operators* dans la Federation.
Federation (notamment la SWITCHaai Federation)	Une Federation est un groupement d'organisations qui ont convenu de collaborer sur la base d'un dispositif réglementaire commun. Dans ce contexte, le dispositif réglementaire concerne la 'Federated Authentication and Authorization'. La SWITCHaai Federation désigne le groupement correspondant aux organisations des universités suisses[8]. Le service SWITCH edu-ID est intégré dans la SWITCHaai Federation.
Federation Operator	Le Federation Operator gère et développe la Federation. Il est responsable des composants centraux et sert de centre de compétences. Dans la SWITCHaai Federation, SWITCH est le Federation Operator.
Federation Technology Profile	Un Technology Profile est utilisé pour définir quelles informations techniques d'une technologie spécifique (par ex. un protocole de communication ou une interface de programmation) s'appliquent dans le contexte de la Federation ou la manière dont de telles informations doivent être utilisées.
Identité de base (Base identity, private identity), Self-Declaration, Self Provisioning, Quality Level	L'*identité de base* englobe les informations spécifiques aux utilisateurs finaux au sens strict, telles que le nom, le prénom, le numéro de téléphone mobile personnel ou l'adresse e-mail personnelle. Dans le service SWITCH edu-ID, l'utilisateur final saisit lui-même les données relatives à l'identité de base. Cette opération s'appelle Self-Declaration et l'identité de base est créée par le *Self Provisioning*. «Self-provisioned» est également une valeur fréquemment utilisée pour le *Quality Level* des informations stockées dans l'identité de base. L'utilisateur final peut (faire) augmenter le Quality Level des attributs de son identité numérique grâce à des processus de validation.

[7] https://www.switch.ch/fr/about/disclaimer/gtc/
[8] https://www.switch.ch/aai/participants/

Identité mise en relation (linked identity, linked organisational identity, linked external identity)	Un utilisateur final peut mettre en relation son identité de base avec d'autres identités. S'il la met en relation avec son identité organisationnelle d'une organisation de la SWITCHaai Federation, il se forme une Affiliation. Un utilisateur final peut également mettre en relation son identité de base avec une autre identité externe, comme par ex. ORCID. C'est p. ex. ainsi qu'un Identifier externe est ajouté en tant qu'attribut de l'identité de base.
Identité numérique (Digital Identity, identification numérique)	Une identité numérique se compose d'un ensemble d'informations sous la forme d'attributs ; cet ensemble peut être affecté à un utilisateur final. Une identité numérique est émise et gérée par un IdP Operator qui peut identifier à tout moment l'utilisateur final. En principe, une identité numérique peut décrire non seulement des personnes, mais aussi des choses. Cette option n'est pas incluse dans le présent contexte. Le *SWITCH edu-ID Account* d'un utilisateur final est une identité numérique.
IdP (Identity Provider)	L'Identity Provider constitue le composant d'exploitation qui authentifie l'utilisateur et émet une Assertion relative à l'utilisateur final pour un certain Service. Une Assertion véhicule les attributs de l'identité numérique qui sont demandés pour l'accès au Service. SWITCH exploite l'IdP SWITCH edu-ID central. Les organisations peuvent exploiter leur propre IdP ou déléguer cette tâche à SWITCH. L'IdP SWITCH edu-ID central diffère des autres IdP de par une fonctionnalité supplémentaire (cf. chapitre 3.2.3).
IdP Administrator	La personne physique exécutante de l'IdP Operator est appelée l'IdP Administrator.
IdP Operator	Un IdP Operator est un SWITCHaai Participant qui assume la responsabilité globale relative à l'exploitation d'un IdP, cf. chapitre 5.1.3.9. Ceci comprend notamment : • L'identification des utilisateurs finaux ; • La gestion des identités numériques ; • La définition de processus d'identification pour les utilisateurs finaux ; • L'utilisation de processus appropriés pour la création et la suppression d'utilisateurs finaux, généralement à l'aide d'un système d'Identity Management (IdM). Ces responsabilités s'appliquent également au service SWITCH edu-ID.
Interfederation	Par le biais d'Interfederation, un utilisateur final d'une Federation peut avoir accès aux services provenant d'autres Federations. Interfederation est en principe à la disposition des SWITCHaai Participants (cf. chapitre 5.1.2.5).

Metadata	Les Metadata comprennent les détails techniques et les informations descriptives relatifs aux composants participant à la Federation, et notamment relatifs aux IdP, aux AP et aux SP. Les Metadata sont généralement protégées contre toute modification par une signature numérique. Les composants de la Federation se basent sur ces Metadata pour instaurer une confiance mutuelle au niveau technique. Dans la SWITCHaai Federation, les Metadata sont gérées par SWITCH.
Organisation	Une institution au sein de la SWITCH Community, l'Extended SWITCH Community ou un partenaire contractuel de SWITCH est désignée comme organisation. Les organisations peuvent offrir leurs services à leurs propres utilisateurs finaux ou aux utilisateurs finaux d'autres organisations. Inversement, des organisations peuvent accorder à leurs utilisateurs finaux un accès à des services qui sont offerts par d'autres organisations, au moyen d'un Identity Provider (IdP) ou d'un Attribute Provider (AP).
Partenaire contractuel	Dans le présent document, un partenaire contractuel est une organisation qui a conclu avec SWITCH un contrat relatif à un service mais qui n'est membre ni de la SWITCH Community, ni de l'Extended SWITCH Community.
Quality Level pour les Base Attributes	Les valeurs des Base Attributes peuvent être complété d'un indicateur de qualité qui porte une information sur leur provenance et donc leur Quality Level. Lors de la Self-Declaration, les attributs comme l'adresse e-mail, le numéro de téléphone mobile ou l'adresse postale obtiennent dans un premier temps le Quality Level le plus bas, «self-declared». La valeur d'un attribut peut parcourir un processus de vérification, ce qui augmente son Quality Level en cas de réussite.
Règlement relatif aux prestations (RRP)	Le règlement relatif aux prestations de SWITCH (règlement concernant l'utilisation des services de SWITCH, Dienstleistungsreglement, DLR) fait partie intégrante du contrat et est disponible sur le site web de SWITCH[9].
Service, Service Provider (SP)	Un Service est une application web ou une autre application qui est proposée par une organisation ou un tiers et à laquelle les utilisateurs finaux peuvent avoir accès. Le Service se base sur l'authentification de l'utilisateur final par l'IdP SWITCH edu-ID ou un autre IdP de la Federation. Pour l'autorisation relative à l'accès de l'utilisateur final, le composant Service Provider (SP) évalue les informations de l'utilisateur final qu'il reçoit dans l'Assertion de l'IdP. C'est sur cette base que le SP décide si l'utilisateur final est autorisé à accéder au Service.
SP Administrator	La personne physique exécutante du SP Operator est appelée le SP Administrator.

[9] https://www.switch.ch/fr/about/disclaimer/service-regulations/

SP Operator	Un SP Operator est un SWITCHaai Participant qui assume la responsabilité globale relative à l'exploitation d'un SP, cf. chapitre 5.1.3.10. Sa tâche la plus importante est de définir les critères d'accès au service (autorisation).
SWITCH Community	Toutes les organisations dans le domaine de la formation et de la recherche qui sont liées à SWITCH (en accord avec l'annexe au RRP).
SWITCH edu-ID Advisory Board	Ce comité[10] se compose de représentants des plus importants groupes de Participants de la SWITCHaai Federation. Il conseille SWITCH sur des questions stratégiques concernant le service SWITCH edu-ID ou la SWITCHaai Federation.
SWITCH edu-ID (Identifier)	Le SWITCH edu-ID Identifier est décrit au chapitre 3.2.2.2.
SWITCH edu-ID (Identity et concept)	Le SWITCH edu-ID Identity est l'analogue numérique d'une pièce d'identité et peut permettre à son détenteur, l'utilisateur final, d'accéder à de nombreux services. Le concept SWITCH edu-ID est décrit en détail au chapitre 3.2.1.
SWITCH edu-ID (service)	SWITCH edu-ID est un service d'identité numérique qui est développé par SWITCH pour une utilisation valable à vie par les membres des universités. Le service SWITCH edu-ID est décrit en détail au chapitre 3.2.
SWITCHaai Federation Partner	Une organisation qui ne fait pas partie de la SWITCH Community mais qui participe à SWITCHaai est appelée de SWITCHaai Federation Partner.
SWITCHaai Participant	Une organisation participant à SWITCHaai (une personne morale) est appelée SWITCHaai Participant.
Trust & Identity WG	Ce groupe de travail se compose de représentants de toutes les organisations participant à SWITCHaai et SWITCHpki dans la SWITCH Community ainsi que dans l'Extended SWITCH Community. Il est à la fois un vecteur d'information et une plate-forme d'échange destinée à fournir un feedback sur des questions d'ordre technique ou opérationnel.
Utilisateurs finaux (utilisateur, User)	Un *utilisateur final* est une personne physique qui utilise la prestation. Dans le but de simplifier la lisibilité du présent document, seule la forme masculine a été utilisée pour les désignations des personnes. L'utilisation commence lorsqu'un utilisateur final crée son SWITCH edu-ID Account personnel. Le service SWITCH edu-ID est destiné en particulier à tous les utilisateurs finaux ayant un rapport avec des organisations de la SWITCH Community.

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

3.2 Principe de fonctionnement de SWITCH edu-ID

3.2.1 Le concept SWITCH edu-ID

SWITCH edu-ID est une identité numérique développée par SWITCH en vue d'une utilisation valable à vie par les membres des universités et d'autres utilisateurs finaux. Le service SWITCH edu-ID est prévu pour être sécurisé et reconnu dans le monde entier. Il est fondé sur SWITCHaai, la solution d'Identity Management fédérée et couronnée de succès. Il simplifie l'Identity Management des universités et permet la mise à disposition d'autres services avec cette identité numérique. Par rapport à SWITCHaai, SWITCH edu-ID introduit les nouveautés suivantes :

- Orientation utilisateur (user-centric) et longévité (persistency) : l'identité numérique appartient à l'utilisateur final qui peut contrôler lui-même à tout moment les informations de base de son SWITCH edu-ID. L'identité numérique est indépendante d'une affiliation à une organisation et continue donc d'exister si l'utilisateur final quitte l'organisation.
- Création en libre-service (Self Provisioning) : chaque personne physique peut se créer une identité numérique électronique de base et devient donc un utilisateur final de SWITCH edu-ID. Elle conserve le contrôle total sur une série d'attributs personnels (Base Attributes) tels que le nom, le prénom, l'adresse e-mail et le numéro de téléphone mobile.
- Quality Levels des attributs : le libre-service entraîne, a priori et de par sa nature, une qualité d'attributs initialement plus faible. Ainsi, les attributs ne reçoivent pas seulement une valeur, mais aussi un indicateur de qualité qui complète la valeur. Les Quality Levels peuvent être augmentés par des processus de validation, voire même diminués, par ex. s'ils atteignent une date d'expiration (vieillissement) ou si la valeur est modifiée manuellement.
- Affiliations multiples (multiple affiliations) : un utilisateur final peut appartenir à aucune, une seule ou plusieurs organisations. En conséquence, son identité de base peut contenir aucune, une seule ou plusieurs affiliations, selon la mise en relation de l'identité de base avec des identités provenant d'organisations dans la SWITCHaai Federation. Les informations se rapportant aux affiliations sont alors fournies par les organisations participantes, généralement par le biais de leurs Attribute Providers (AP).

3.2.2 Comment le service SWITCH edu-ID fonctionne-t-il?

Si l'utilisateur final dispose d'une identité de base, il peut en principe l'utiliser pour accéder à un ensemble de services au sein de la SWITCHaai Federation. Pour accorder l'accès, le service peut exiger certains Quality Levels pour certains attributs de base, ou encore demander des attributs complémentaires qui informent sur les affiliations existantes. Dans ce cas, l'utilisateur final donne son consentement (user consent) immédiatement avant que ces données soient mises à la disposition du service.

Lors de la connexion au service, l'IdP SWITCH edu-ID collecte dans une Assertion tous les attributs requis approuvés d'un utilisateur final et les transfère au service de manière sécurisée. Le service vérifie l'Assertion et décide de l'octroi de l'accès sur la base de sa configuration.

Dans cette mesure, l'IdP SWITCH edu-ID satisfait aux exigences d'un IdP dans la SWITCHaai Federation. Le service SWITCH edu-ID se distingue par les concepts suivants :

3.2.2.1 Classic et Extended Attribute Model

Les services qui peuvent traiter des affiliations multiples prennent en charge le *Extended Attribute Model*, c'est-à-dire que les informations relatives à toutes les affiliations disponibles et approuvées par l'utilisateur final peuvent leurs être transmises. Le service décide alors de la manière dont il traite ces différentes affiliations. Des informations plus détaillées peuvent être consultées dans le document d'architecture[11] Swiss edu-ID (chapitre 2.1).

Tous les autres services attendent exactement une affiliation et prennent ainsi en charge le *Classic Attribute Model*. Si un utilisateur final possède plusieurs affiliations existantes, il doit indiquer à l'IdP au moyen d'un Affiliation Chooser (cf. chapitre 3.2.3.6) quelle affiliation il souhaite utiliser pour le service concerné. Seuls les attributs d'affiliation appartenant à l'affiliation sélectionnée sont transmis au service.

3.2.2.2 Le SWITCH edu-ID Identifier

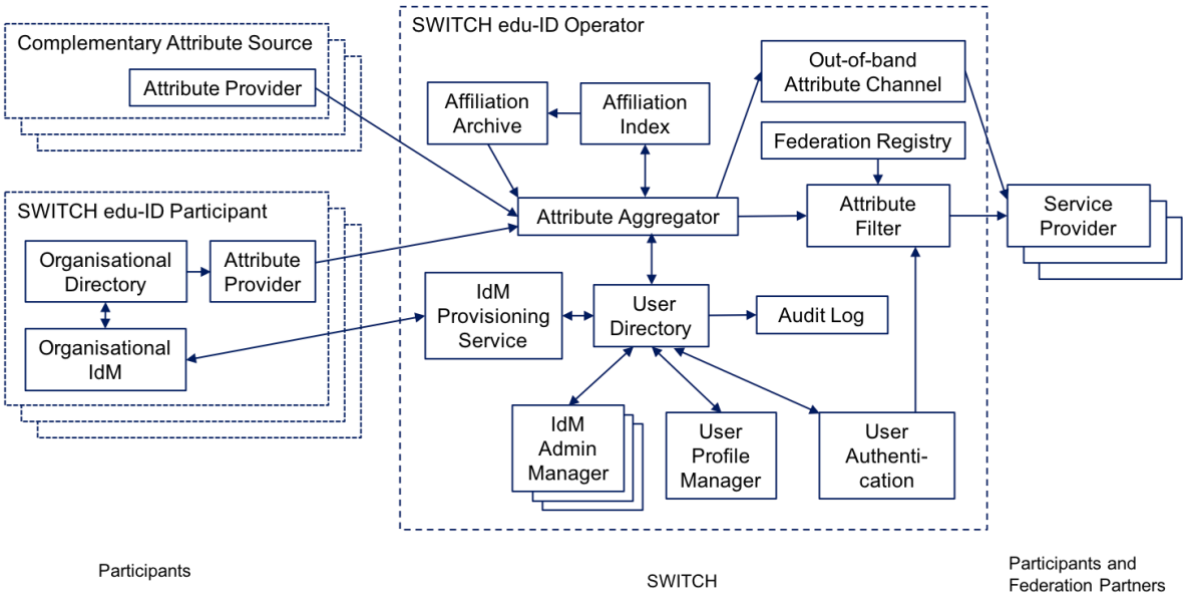
Le SWITCH edu-ID Identifier[12] [13] identifie chaque utilisateur final de manière unique et à vie. Il s'agit de l'identifiant primaire, spécifique au secteur pour la communauté académique en Suisse, qui est utilisé pour pouvoir lier de manière unique d'autres données personnelles.

Le SWITCH edu-ID Identifier constitue le prérequis pour la compilation de données qui peut être considérée comme un profil de personnalité au sens de la loi fédérale sur la protection des données du 19 juin 1992 (LPD ; SR 235.1)[14] et doit être traité en conséquence (cf. chapitre 5.1.3.12).

Si possible, les services doivent utiliser l'un des autres identifiants (par ex. un identifiant dédié au service ou le swissEduPersonUniqueID), à moins qu'ils n'aient une raison impérative d'utiliser le SWITCH edu-ID Identifier. Si un service requiert le SWITCH edu-ID Identifier, les obligations de diligence correspondantes sont transférées au SP Operator.

[11] https://www.switch.ch/edu-id/documents/
[12] https://www.switch.ch/aai/support/documents/attributes/swisseduid/
[13] https://swit.ch/eduidspec
[14] https://www.admin.ch/ch/f/sr/c235_1.html

3.2.3 Composants du service SWITCH edu-ID



3.2.3.1 Registre des utilisateurs finaux (User Directory)

La SWITCH edu-ID Identity (identité de base) est stockée dans la base de données centrale SWITCH edu-ID. Un accès à ces données est établi à chaque fois qu'un utilisateur final est authentifié. Un seul utilisateur final est affecté à une inscription. Chaque utilisateur final est responsable de l'exactitude des données dans son inscription.

3.2.3.2 Attribute Aggregator

En prenant contact avec les divers Attribute Providers spécifiques à chaque organisation, l'Attribute Aggregator s'assure que l'Affiliation Index (cf. schéma) est à jour.

3.2.3.3 SP Notification

Le module SP Notification peut, de manière optionnelle et après concertation, informer les SP sur les modifications des valeurs d'attributs. Les SP ont ainsi la possibilité de mettre à jour leur propre base de données utilisateur.

3.2.3.4 Système de gestion du profil de l'utilisateur final (User Profile Manager)

Cette application web permet à l'utilisateur final de vérifier l'ensemble de ses données personnelles, de les mettre à jour, de les compléter si nécessaire ou de les faire vérifier. Toutes les transactions sont journalisées à des fins de traçabilité.

3.2.3.5 Identity Provider (IdP)

L'Identity Provider est responsable de l'authentification des utilisateurs finaux (user authentication). A ce titre, il collecte les attributs requis à l'attention du SP qui a initié l'authentification, demande à l'utilisateur final, si nécessaire, son approbation pour le partage des données (user consent) et transmet les informations au SP en tant qu'Assertion.

3.2.3.6 Affiliation Chooser

Après l'authentification, l'Affiliation Chooser permet à l'utilisateur final de sélectionner, si nécessaire, l'une de ses affiliations existantes avec laquelle il se connecte alors au service. L'Affiliation Chooser intervient pour les services qui utilisent le Classic Attribute Model. L'Affiliation Chooser obtient les affiliations de l'Affiliation Index.

3.2.3.7 Affiliation Archive

Si l'Attribute Aggregator détermine qu'une affiliation n'est plus renouvelée par l'Attribute Provider, il déplace ses informations encore existantes dans l'Affiliation Archive des anciennes affiliations qui ne sont plus actives. Ceci permet de conserver l'information selon laquelle l'utilisateur final était précédemment affilié à l'organisation. De futurs services, par exemple pour les organisations d'alumni, pourraient s'adresser spécifiquement à de tels groupes d'utilisateurs – sous réserve d'obtenir la permission adéquate.

3.2.3.8 Autres systèmes d'assistance : Test Federation et sites de démonstration

SWITCH exploite et maintient une Test Federation[15] dans le but de tester de nouveaux composants et de nouvelles configurations. À des fins de démonstration, elle contient les composants requis, comme par ex. un IdP, un AP ou un SP qui présentent en détail le principe de fonctionnement de SWITCHaai et les possibilités de configuration.

3.2.3.9 Autres systèmes d'assistance : Attribute Viewer

Sous le nom d'Attribute Viewer[16], SWITCH fournit un SP qui demande autant d'attributs que possible auprès de l'IdP, puis les affiche sur un site web à l'attention de l'utilisateur final.

- Un IdP peut l'utiliser pour vérifier que ses attributs sont émis correctement.
- Les utilisateurs finaux peuvent voir quels attributs leur IdP émet à leur sujet.
- Si les SP Administrators ou les utilisateurs finaux avancés suspectent un manquement de leur SP, ils peuvent vérifier si leur IdP fonctionne correctement avec l'Attribute Viewer et ainsi délimiter un problème éventuel.

L'Attribute Viewer prend en charge le *Classic Attribute Model* mais pourrait être modifié ultérieurement si nécessaire pour prendre en charge l'*Extended Attribute Model*.

3.3 Disponibilité et assistance

En principe, le service est disponible 24 heures sur 24 et 7 jours sur 7. SWITCH réalise les travaux de maintenance planifiés généralement en dehors des heures de bureau habituelles et annonce de telles interventions au moins une semaine à l'avance sur la page de connexion de l'IdP SWITCH edu-ID. L'objectif de SWITCH est d'atteindre une disponibilité du service et de chaque composant d'au moins 99,99%. Les dérangements portant préjudice à la prestation demeurent réservés.

[15] https://www.switch.ch/aai/demo/
[16] https://attribute-viewer.aai.switch.ch/

Pendant les heures de bureau habituelles, SWITCH s'engage à prendre des mesures en vue de la suppression des dérangements ou dysfonctionnements du service et à les mettre en œuvre.

L'assistance dédiée aux utilisateurs finaux[17] est disponible pendant ces mêmes heures.

Les heures de bureau habituelles sont définies dans le règlement relatif aux prestations (RRP) ou dans les conditions générales (CG) dans leur version en vigueur.

En outre, SWITCH prend des précautions pour garantir une bonne qualité de service même en dehors des heures de bureau, en fonction de l'urgence et à son entière discrétion.

3.4 Surveillance du service et journalisation

L'état d'exploitation du service SWITCH edu-ID est présenté[18] en continu sur le site web public de SWITCH.

Des informations complémentaires relatives à l'état d'exploitation sont fournies aux SWITCHaai Participants sur le portail clients[19].

En coordination avec les organisations, SWITCH peut surveiller leurs composants (notamment IdP et AP) et mettre les résultats à disposition d'autres organisations sous une forme adéquate. A cette fin, SWITCH gère des comptes techniques dédiés.

En cas de dérangements perturbant l'exploitation, SWITCH applique son processus de gestion d'incident interne. Il comprend la communication externe.

SWITCH peut enregistrer les modifications apportées à l'état d'exploitation ainsi que les transactions relatives aux données des utilisateurs finaux à des fins de traçabilité. Les processus de validation peuvent notamment être journalisés. Les journaux existants sont mis à la disposition des utilisateurs finaux sous une forme appropriée.

SWITCH consigne l'utilisation du service par l'utilisateur final ou par l'organisation. Si possible, ceci est effectué par organisation. SWITCH fournit aux organisations des statistiques anonymisées quant à l'utilisation de SWITCH edu-ID.

[17] https://help.switch.ch/eduid/
[18] https://help.switch.ch/eduid/status/
[19] https://portal.switch.ch/

4 Informations spécifiques aux utilisateurs finaux

4.1 Création et accès

a) Tout utilisateur final intéressé par la création d'une identité numérique valable à vie et permettant d'accéder à des services peut bénéficier du service SWITCH edu-ID.

b) Un SWITCH edu-ID Account est requis pour pouvoir utiliser le service SWITCH edu-ID. À cette fin, les utilisateurs finaux doivent fournir au minimum les données suivantes :

- Leur nom complet
- Une adresse e-mail valable et
- Un mot de passe sûr.

c) Les utilisateurs finaux peuvent modifier à tout moment le nom, la ou les adresse(s) e-mail et le mot de passe de leur SWITCH edu-ID Account qu'ils ont précédemment fournis.

d) Des services spécifiques peuvent solliciter des attributs personnels supplémentaires, comme la date de naissance, l'adresse de résidence, le numéro de téléphone mobile, etc. Une bibliothèque ne peut, par exemple, adresser des livres au domicile de l'utilisateur final que s'il a fourni une adresse de résidence.

e) Les Service Providers peuvent demander le *Quality Level* des attributs de base. Un attribut peut être vérifié par le biais d'un processus de vérification, ce qui augmente son Quality Level en cas de réussite. Par exemple, un numéro de téléphone mobile peut être saisi avec la mention que celui-ci a permis de joindre l'utilisateur par le passé.

L'utilisateur final, SWITCH ou une organisation peut effectuer une vérification. Une telle vérification peut être effectuée une ou plusieurs fois. Les Quality Levels peuvent être consultés dans le système de gestion du profil de l'utilisateur final.

f) Les utilisateurs finaux peuvent indépendamment créer leur SWITCH edu-ID Account ou le baser sur un SWITCHaai Account existant. Cette dernière procédure présente l'avantage que le SWITCH edu-ID Account est automatiquement mis en relation avec l'identité SWITCHaai et que les attributs de base existants peuvent d'emblée être repris dans le SWITCH edu-ID Account. Ces données seront alors affichées dans des champs non modifiables.

g) Les utilisateurs finaux peuvent également mettre en relation leur SWITCH edu-ID Account avec un ou plusieurs SWITCHaai Accounts et les ajouter en tant qu'Affiliations. Il est aussi possible de créer une relation avec des identités externes, comme par ex. ORCID. De telles relations peuvent être nécessaires si le SWITCH edu-ID Account est utilisé pour accéder à des services ayant besoin d'identifiants de ces identités liées.

h) Les organisations faisant partie de la SWITCHaai Federation déterminent de manière autonome quels services elles souhaitent mettre à disposition des utilisateurs finaux individuels, ainsi que les conditions qui doivent être remplies pour leur utilisation. En principe, l'utilisateur final n'a pas de droit d'accès aux services.

4.2 Informations de contact et site d'aide SWITCH edu-ID

Le site d'aide[20] doit être consulté pour toutes questions relatives au SWITCH edu-ID Account.

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

4.3 Administration des utilisateurs finaux

a) Un SWITCH edu-ID Account peut être créé par l'utilisateur final ou par le biais d'une organisation.

b) Si l'utilisateur final quitte une organisation, par exemple une université ou un institut de recherche, son SWITCH edu-ID Account continue d'exister, contrairement à un SWITCHaai Account qui est supprimé à son départ de l'organisation.

c) Pour supprimer un SWITCH edu-ID Account, l'utilisateur final doit contacter par e-mail l'assistance SWITCH edu-ID[21]. L'utilisateur final doit être conscient que la suppression de son identité valable à vie est en contradiction avec l'objectif de celle-ci. La suppression d'un SWITCH edu-ID Account entraîne la suppression définitive de toutes les données de l'utilisateur final.

Certaines affiliations existantes auprès d'organisations dans la SWITCHaai Federation peuvent empêcher la suppression du SWITCH edu-ID Account.

d) En cas de décès, les proches de l'utilisateur final peuvent contacter l'assistance SWITCH edu-ID afin de bloquer et/ou de supprimer le SWITCH edu-ID Account, sur présentation des documents officiels correspondants.

4.4 Archivage automatique et suppression des SWITCH edu-ID Accounts

Les SWITCH edu-ID Accounts qui ne sont pas utilisés pendant une très longue période sont placés dans le processus automatisé d'archivage et de suppression. Une suppression sur demande de l'utilisateur final (cf. chapitre 4.3) ou en raison d'une utilisation inappropriée (cf. chapitre 6.7) est possible.

Dans la phase initiale du processus d'archivage, l'utilisateur final est contacté au moyen de ses adresses et ses identités liées, notamment ses affiliations existantes, et est notifié de leur non-utilisation avec une demande de réactivation de son SWITCH edu-ID Account. Les délais peuvent être consultés sur la page FAQ[22].

À la phase suivante, le SWITCH edu-ID Account est bloqué si l'utilisateur final ne donne pas suite à la demande de réactivation dans le délai fixé (cf. ci-dessus). Une réouverture ne peut se faire que par l'assistance SWITCH edu-ID et uniquement après une identification réussie du titulaire du SWITCH edu-ID Account.

Dans la troisième phase, le SWITCH edu-ID Account est supprimé et les attributs techniques permanents (notamment le SWITCH edu-ID Identifier et le swissEduPersonUniqueID) sont archivés afin d'éviter de nouvelles affectations. Les données personnelles sont supprimées conformément à la loi en vigueur, sur la base des buts déclarés de SWITCH edu-ID.

[21] eduid-support@switch.ch
[22] https://help.switch.ch/eduid/faqs/

5 La SWITCHaai Federation Policy

5.1 Gouvernance et rôles

5.1.1 Gouvernance

En tant que Federation Operator, SWITCH exploite la SWITCHaai Federation et consulte à la fois le SWITCH edu-ID Advisory Board[23] et le Trust & Identity WG.

Le SWITCH edu-ID Advisory Board comprend les représentants des plus importants groupes de parties prenantes des organisations participantes, y compris les représentants de la SWITCH Community, d'instances politiques dans le domaine de l'enseignement et des SP Operators. Le SWITCH edu-ID Advisory Board agit en qualité d'organe de conseil en ce qui concerne la stratégie à long terme du service SWITCH edu-ID.

SWITCH confère avec le SWITCH edu-ID Advisory Board sur des thèmes comme, par exemple :

- les catégories des Federation Partners qui doivent être acceptées;
- les catégories des Federation Partners qui peuvent exploiter un IdP ou un AP;
- la convention Interfederation;
- la planification du futur développement de SWITCH edu-ID et de la SWITCHaai Federation, ainsi que les optimisations administratives ou techniques;
- les changements apportés à l'administration de la SWITCHaai Federation ou de la présente description du service, ainsi que les modifications d'autres documents spécifiques à la Federation.

Le SWITCH edu-ID Advisory Board n'a pas de pouvoir de décision. SWITCH décide de la composition du SWITCH edu-ID Advisory Board.

Le groupe de travail Trust & Identity WG se compose de représentants de toutes les organisations participant à SWITCHaai et SWITCHpki dans la SWITCH Community ainsi que dans l'Extended SWITCH Community. Ce groupe est impliqué de manière informelle et a la possibilité de fournir un feedback si des questions lui sont posées ou si des changements sont effectués.

SWITCH entretient des relations étroites avec les SWITCHaai Participants. SWITCH organise des événements lors desquels les SWITCHaai Participants, notamment les AP, IdP et SP Administrators découvrent les nouveaux développements dans le domaine *Federated Authentication and Authorization* et ont la possibilité d'échanger leurs impressions à ce sujet.

SWITCH diffuse les informations sur les idées et concepts mis en œuvre dans SWITCH edu-ID et dans la SWITCHaai Federation auprès de groupes d'intérêts et d'organisations qui pourraient adopter des concepts similaires. L'accent est mis sur les groupes qui promettent le plus grand potentiel d'utilité pour la SWITCH Community.

SWITCH agit en tant que centre de compétences pour les domaines *Federated Authentication and Authorization* dans le secteur de l'enseignement académique. SWITCH

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

teste des logiciels, recommande et documente des solutions. SWITCH fournit des instructions d'installation et/ou de configuration de composants logiciels sélectionnés sur certains systèmes d'exploitation, en vue d'une utilisation dans la SWITCHaai Federation. Des exemples de configuration facilitent l'intégration d'autres produits.

Si des fonctions complémentaires ne sont pas disponibles d'une autre manière, SWITCH peut elle-même développer les composants manquants ou mandater un tiers pour le faire.

5.1.2 Droits et obligations du Federation Operator

5.1.2.1 Généralités

SWITCH est responsable de l'exploitation de la Federation et de l'intégration formelle d'organisations nationales et internationales pertinentes.

SWITCH établit et publie une liste des SWITCHaai Participants[24].

5.1.2.2 Resource Registry (RR)

SWITCH exploite et maintient le Resource Registry[25] pour l'administration de la Federation. Les AP, IdP et SP sont qualifiés de ressources dans le contexte du Resource Registry.

Les AP, IdP et SP Administrators des SWITCHaai Participants tiennent à jour toutes les informations concernant leurs ressources respectives, ceci inclut les informations de contact et d'assistance, des détails relatifs à la configuration technique, les Attribute Requirements, les Attribute Release Policies, les Intended Audience, etc.

Toutes ces données sont enregistrées dans une base de données. C'est à partir de celle-ci que SWITCH génère divers types d'autres données utilisées ailleurs, comme par exemple les fichiers de Metadata ou les configurations d'Attribute Release pour les AP et les IdP etc.

Les nouvelles entrées de SP ainsi que les changements apportés aux SP existants dans le Resource Registry nécessitent une approbation avant de devenir actifs et d'apparaître dans les Metadata. Ceci relève de la responsabilité des « AAI Resource Registration Authority Administrators » du SWITCHaai Participant qui est responsable du SP. Après vérification de l'exactitude et de la conformité, ils approuvent la nouvelle entrée ou la modification. Les détails sont disponibles dans la documentation relative au Resource Registry[26].

5.1.2.3 Metadata Service

SWITCH exploite et maintient le Metadata Service[27] qui signe numériquement et publie les charactéristiques des SWITCHaai Participants. À des fins de signature, SWITCH maintient une autorité de certification hors-ligne dédiée « SWITCHaai Root Certification Authority » (CA) [28] dont les certificats servent comme ancre de confiance (trust anchor) pour le contrôle des Metadata.

[24] https://www.switch.ch/aai/participants/
[25] https://rr.aai.switch.ch/
[26] https://www.switch.ch/aai/docs/AAI-RR-Guide.pdf
[27] https://www.switch.ch/aai/metadata/
[28] https://www.switch.ch/pki/aai/

5.1.2.4 Discovery Service (DS)

SWITCH exploite et maintient un Discovery Service central, également connu sous le nom de service «Where Are You From» (WAYF). Les SP peuvent soit utiliser ce Discovery Service central, soit configurer un Discovery Service local. SWITCH met les informations nécessaires à la disposition des SP Administrators.

5.1.2.5 Interfederation

SWITCH est responsable du suivi des relations avec les parties prenantes nationales et internationales dans le domaine *Federated Authentication and Authorization*, en particulier en ce qui concerne l'enseignement dans les universités. Ceci inclut notamment les contacts concernant les activités[29] Interfederation.

Si cela présente un intérêt pour la SWITCH Community, SWITCH peut conclure des conventions au nom de la SWITCHaai Federation et, par exemple, échanger des Metadata avec d'autres Federations et/ou avec des services Interfederation.

En participant à l'Interfederation, les organisations peuvent offrir leurs services aux utilisateurs finaux d'autres Federations et permettre à leurs propres utilisateurs finaux d'accéder aux services d'autres Federations. Elles contribuent ainsi à la réduction du nombre de comptes utilisateurs locaux.

5.1.2.6 Virtual Home Organisation (VHO)

La Virtual Home Organisation[30] est l'« IdP of last resort » pour une petite partie des utilisateurs finaux qui devraient avoir accès à certains services protégés par SWITCHaai mais qui n'ont pas reçu d'identité numérique de la part de leur organisation.

SWITCH exploite et maintient l'IdP Virtual Home Organisation en combinaison avec une application web pour l'administration des VHO Accounts, dans la mesure où ceci est nécessaire.

Les SP Administrators peuvent soumettre une demande à SWITCH pour gérer leur propre groupe de d'utilisateurs finaux dans la VHO. Ils doivent alors se conformer à la SWITCHaai VHO Policy[31].

De plus, chaque SWITCHaai Participant peut demander un VHO Account à des fins de test.

SWITCH peut fournir les fonctionnalités nécessaires à l'administration de telles identités non-organisationnelles, d'appartenance à un groupe ou d'affiliation à une organisation ne possédant pas son propre AP au moyen d'autres composants.

5.1.3 Droits et obligations des SWITCHaai Participants

5.1.3.1 Coopération

Le SWITCHaai Participant travaille en coopération avec SWITCH et prend toutes les mesures nécessaires à la garantie du fonctionnement sans heurts de la SWITCHaai Federation. Ceci inclut, par exemple, la mise à disposition des informations, données, équipements, droits

[29] https://www.switch.ch/aai/interfederation/
[30] https://www.switch.ch/aai/vho/
[31] https://www.switch.ch/aai/docs/AAI_VHO_Policy.pdf

(d'accès) et autres services nécessaires. Le SWITCHaai Participant renonce notamment à toute modification des services et systèmes exploités dans la SWITCHaai Federation ou à une utilisation contraire à leur objectif.

En tant qu'AP Operator, l'organisation est responsable de l'émission correcte des Affiliation Attributes pour une identité de base SWITCH edu-ID existante, cf. chapitre 5.1.3.8.

En tant qu'IdP Operator, l'organisation est responsable du traitement correct de l'authentification ainsi que de l'émission correcte des Base Attributes, cf. chapitre 5.1.3.9.

Les SWITCHaai Participants s'engagent à notifier immédiatement SWITCH de tout changement de personnel parmi leurs AP, IdP et SP Administrators. À défaut de quoi, SWITCH ne pourra plus garantir l'accès aux données opérationnelles des SWITCHaai Participants.

5.1.3.2 Conformité

Le SWITCHaai Participant garantit qu'il :

- installera, exploitera et utilisera les composants AP, IdP et SP qui sont sous sa responsabilité conformément aux Federation Technology Profiles;
- déclarera à SWITCH les contacts techniques et administratifs requis;
- n'accordera pas l'accès à la SWITCHaai Federation à des tiers sans le consentement écrit de SWITCH (à l'exception de ses utilisateurs finaux);
- transmettra à la SWITCHaai Federation uniquement des informations conformes à la réalité sur ses propres utilisateurs finaux.

5.1.3.3 Collaboration avec les administrateurs des organisations

SWITCH fournit une assistance de 3^{e} niveau aux AP et IdP Administrators enregistrés dans le Resource Registry. Elle est joignable aux heures de bureau habituelles par e-mail et par téléphone[32].

5.1.3.4 Assistance

Le SWITCHaai Participant fournit à ses utilisateurs finaux une assistance de 1er niveau (par ex. Service Desk) capable de traiter elle-même les demandes pendant les heures de bureau locales. Le SWITCHaai Participant fournit à ses SP Administrators une assistance de 2^{e} niveau.

5.1.3.5 Design Guidelines

Les SWITCHaai Participants s'engagent à suivre les Design Guidelines SWITCHaai[33] pour les éléments d'interface graphique destinés aux utilisateurs finaux.

Les logos SWITCH ne peuvent être utilisés que de manière conforme aux Design Guidelines et sont une marque déposée. Toute utilisation par des tiers en violation des Design Guidelines est réservée et requiert le consentement écrit de SWITCH.

---

[32] https://www.switch.ch/aai/
[33] https://www.switch.ch/aai/guides/design/

5.1.3.6 Accords bilatéraux au sein de la SWITCHaai Federation

Les SWITCHaai Participants peuvent conclure des accords bilatéraux concernant la mise à disposition de services et/ou l'accès à ces services. Les SWITCHaai Participants sont responsables de toutes les conséquences de ces accords et SWITCH n'assume aucune responsabilité les concernant.

5.1.3.7 Comptes techniques et de test dans SWITCH edu-ID

Les AP Operators peuvent créer un petit nombre de comptes techniques ou de test (test accounts) à des fins spécifiques et leur affecter une de leurs affiliations. Dans ce cas, l'AP Operator assume la responsabilité pour chaque compte. L'AP Operator peut déléguer la responsabilité en interne à l'un de ses AP Administrators et doit s'assurer que les e-mails peuvent être reçus par les adresses e-mail spécifiées. Lorsqu'un compte technique ou de test n'est plus utilisé, l'AP Operator doit le supprimer immédiatement. SWITCH envoie des rappels réguliers concernant ces comptes à l'AP Operator.

5.1.3.8 Obligations d'un AP Operator

L'AP Operator respecte la présente description du service et s'assure que ses utilisateurs finaux la respectent également. Tout abus des valeurs d'attributs provenant d'un AP sera attribué à l'AP Operator concerné.

L'AP Operator

- s'assure de l'exactitude des valeurs d'attributs qu'il affecte à ses utilisateurs finaux;
- révèle ses processus de gestion d'identité à un autre SWITCHaai Participant sur demande (en particulier concernant la délivrance et le retrait des Affiliation Attributes);
- signale immédiatement à SWITCH tout doublon et/ou abus détectés d'un compte d'un utilisateur final;
- permet au service SWITCH edu-ID de mettre à jour ses informations en cache dans la mesure où ceci concerne l'affiliation.

5.1.3.9 Obligations d'un IdP Operator

L'IdP Operator respecte la présente description du service et s'assure également que ses utilisateurs finaux la respectent. Tout abus d'une identité numérique sera attribué à l'IdP Operator de l'IdP auprès duquel l'utilisateur final correspondant a été authentifié.

L'IdP Operator

- s'assure qu'il peut identifier ses utilisateurs finaux;
- révèle ses processus de gestion d'identité à un autre SWITCHaai Participant sur demande (dont l'identification, l'authentification, la création et la suppression);
- prend en charge l'activation du dialogue sur l'approbation par l'utilisateur de la transmission de ses attributs (user consent dialog)[34] lors de la participation à l'Interfederation avec son IdP

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

5.1.3.10 Obligations d'un SP Operator

Afin d'accorder l'accès, de fournir le service et l'entretien des données, les SP se basent sur une authentification réussie par l'IdP et sur les attributs reçus. Les SP Operators doivent utiliser les données reçues, dont les informations personnelles, uniquement à cette fin.

5.1.3.11 Mises à jour des données pour les Service Providers

Lors de chaque accès à un service par un utilisateur final, le service reçoit des informations personnelles concernant l'utilisateur final et a le droit de les stocker, pour autant que cela soit nécessaire à l'utilisation du service. Ces données peuvent devenir obsolètes et le service peut demander à l'IdP SWITCH edu-ID si elles sont toujours valides afin de les mettre à jour. L'IdP SWITCH edu-ID peut, à son tour, mettre en œuvre des mesures techniques pour s'assurer que le service n'ait accès à cette fonction de requête qu'uniquement pour les identités qu'il connaît déjà (par exemple en autorisant la requête via un identifiant dédié au SP, comme l'eduPersonTargetedId[35]).

5.1.3.12 Sécurité du SWITCH edu-ID Identifier

Afin d'établir une mise en relation incontestable avec l'identité organisationnelle locale, les AP Operators peuvent recevoir les SWITCH edu-ID Identifiers[36] de leurs utilisateurs finaux. Si c'est le cas, ils sont tenus

1. de stocker et manipuler ce SWITCH edu-ID Identifier de manière confidentielle à tout moment et d'éviter tous accès par des tiers;
2. d'utiliser le SWITCH edu-ID Identifier exclusivement dans le but de rechercher d'autres attributs personnels liés à l'IdP SWITCH edu-ID ou pour des processus de gestion d'identité, en particulier la prévention des doublons; Pour tout autre but, d'autres identifiants doivent être employés
3. de stocker le SWITCH edu-ID Identifier uniquement sur les systèmes qui en ont besoin et
4. d'éviter tout accès au SWITCH edu-ID Identifier par les utilisateurs finaux sauf dans le cas d'une requête explicite.

SWITCH aide les organisations à la formation des employés concernant l'utilisation du SWITCH edu-ID Identifier et autres données personnelles.

5.1.3.13 Adoption de SWITCH edu-ID par une organisation

SWITCH conseille les organisations quand elles adoptent le SWITCH edu-ID. Généralement, l'organisation convertit son IdP en un AP et certains des processus dans l'organisation (en particulier la création et la suppression de comptes) sont adaptés.

Jusqu'à l'adoption du SWITCH edu-ID, l'IdP de l'organisation est responsable de l'authentification correcte de l'utilisateur. Ensuite, l'IdP SWITCH edu-ID reprend cette fonction.

---

[35] https://www.switch.ch/aai/support/documents/attributes/edupersontargetedid/
[36] https://www.switch.ch/aai/support/documents/attributes/swisseduid/

Avant l'adoption de SWITCH edu-ID, l'IdP de l'organisation fournit au SP l'ensemble complet des attributs requis. Après l'adoption, cette tâche est prise en charge par l'IdP SWITCH edu-ID qui extrait certaines informations de l'AP de l'organisation.

Pour l'adoption de SWITCH edu-ID, l'organisation redéfinit et met en œuvre ses procédures de création de comptes afin qu'aucune nouvelle identité numérique ne soit créée pour les nouveaux utilisateurs finaux. À la place, une nouvelle Affiliation est mise en relation avec une identité de base SWITCH edu-ID existante. L'AP fournit les Affiliation Attributes respectifs. La suppression de comptes est simplifiée d'une manière similaire par l'annulation de l'Affiliation.

Avec l'adoption de SWITCH edu-ID, l'organisation accepte les conditions de la présente description du service.

Au moment de l'adoption de SWITCH edu-ID pour le premier SWITCHaai Participant, un scénario d'utilisation mixte apparaît, dans lequel certaines organisations créent toujours des identités numériques par elles-mêmes, tandis que d'autres mettent uniquement en relation leurs Affiliations avec l'identité SWITCH edu-ID.

L'adoption de SWITCH edu-ID ne doit pas entraîner la création de doublons.

5.2 Conditions de participation

5.2.1 Public cible

La participation à SWITCHaai est ouverte aux organisations de la SWITCH Community, de l'Extended SWITCH Community et aux autres organisations qui apportent un avantage pour la SWITCH Community.

5.2.2 Frais

SWITCH se réserve le droit de facturer aux SWITCHaai Federation Partners des frais pour leur participation à SWITCHaai et l'utilisation d'autres services.

En particulier, SWITCH peut facturer aux Federation Partners des frais de participation à l'option Interfederation.

Les frais sont payables dans un délai de 30 jours. Si le délai est dépassé, les accords respectifs sont annulés.

5.3 Procédures

5.3.1 Procédure d'admission

Les nouvelles organisations peuvent exploiter des SP et, dans les conditions appropriées, un AP ou – dans les cas justifiés – un IdP.

En principe, toute organisation souhaitant contribuer par l'offre de ses services à la SWITCHaai Federation peut envoyer une requête correspondante à SWITCH afin de rendre ses services accessibles aux SWITCHaai Participants.

Une organisation ne faisant pas partie de la SWITCH Community doit soumettre une demande d'adhésion officielle. SWITCH évalue l'utilité de l'adhésion pour la SWITCH Community. SWITCH décide ensuite si l'adhésion est accordée.

Un autre prérequis à l'acceptation d'une organisation en tant que SWITCHaai Federation Partner est la signature du SWITCHaai Federation Partner Agreement.

Une organisation de l'Extended SWITCH Community qui rejoint la SWITCHaai Federation devient un *Federation Partner Basic* si elle ne fait qu'offrir des services et n'exploite pas d'AP ou d'IdP. Dans certaines circonstances, elle peut être autorisée à exploiter un AP ou un IdP dans la SWITCHaai Federation. Elle reçoit donc le rôle d'AP Operator ou d'IdP Operator et devient ainsi un *Federation Partner Plus*.

Pour les SWITCHaai Federation Partners, la liste des prix, le présent document et les conditions générales (CG) s'appliquent.

5.3.2 Procédure de départ

L'annulation du service est soumise aux conditions du règlement relatif aux prestations (RRP) et aux conditions générales (CG) dans leur version en vigueur.

6 Conditions juridiques d'utilisation

6.1 Dispositions applicables

L'utilisateur final accepte la présente description du service lorsqu'il crée son SWITCH edu-ID ou utilise le service SWITCH edu-ID pour la première fois.

Les présentes dispositions s'appliquent dans leur version en vigueur aux organisations et aux utilisateurs finaux au titre de l'utilisation du service :

- Pour les organisations de la SWITCH Community ainsi que pour les utilisateurs finaux qui font partie d'une organisation de la SWITCH Community :
  - la présente description du service
  - le tarif en vigueur
  - le RRP

  En cas de contradiction, la présente description du service a préséance sur le tarif et le tarif sur le RRP.
- Pour les organisations de l'Extended SWITCH Community, pour les utilisateurs finaux qui font partie d'une organisation de l'Extended SWITCH Community, pour les partenaires contractuels ainsi que pour les utilisateurs finaux qui sont rattachés à un partenaire contractuel :
  - la présente description du service
  - le SWITCHaai Federation Partner Agreement
  - les CG.

  En cas de contradiction, la présente description du service a préséance sur le SWITCHaai Federation Partner Agreement et le SWITCHaai Federation Partner Agreement sur les CG.
- Pour les utilisateurs finaux qui ne font partie ni d'une organisation de la SWITCH Community, ni de l'Extended SWITCH Community et qui ne sont pas rattachés à un partenaire contractuel :
  - la présente description du service
  - les CG.

  En cas de contradiction, la présente description du service a préséance sur les CG.

6.2 Procédure en cas de modifications

SWITCH peut modifier la présente description du service à tout moment et sans avertir au préalable les utilisateurs finaux, cf. chapitre 5.1.1 Gouvernance. En fonction de l'importance desdites modifications, SWITCH peut informer les utilisateurs finaux et demander leur consentement avant qu'ils puissent continuer à utiliser leur SWITCH edu-ID Account.

Importance des modifications et de leur traitement:

a) **Négligeable**: Pour de petites modifications ou corrections sans impact important sur les accords, une modification peut être effectuée et publiée sans avis adressé aux utilisateurs finaux. Le cas échéant, les utilisateurs finaux peuvent être informés des modifications (par exemple par e-mail ou dans le système d'administration du profil de l'utilisateur final).

b) Important : Une ou plusieurs modifications qui ont un impact direct sur les accords sont qualifiées d'importantes. Des modifications importantes font l'objet d'une discussion préalable avec le SWITCH edu-ID Advisory Board et le groupe Trust & Identity WG, tel que prévu au chapitre 5.1.1. Lesdites modifications sont ensuite communiquées aux organisations sous une forme appropriée. Elles entrent en vigueur si aucune objection n'est émise dans un délai de 30 jours à compter de leur notification. Une objection émise par une organisation entraîne une résiliation du contrat. Dans le cas de modifications importantes, les utilisateurs finaux doivent accepter de nouveau les conditions d'utilisation, après la notification des modifications, lors de leur prochaine connexion à un Service.

L'importance des modifications est évaluée par le service juridique de SWITCH.

6.3 Protection et sécurité des données

6.3.1 Traitement des données par SWITCH

En ce qui concerne le traitement de données personnelles, SWITCH se base sur le RRP et les CG dans leur version en vigueur.

En outre, SWITCH crée des statistiques anonymisées destinées aux organisations et aux partenaires contractuels. Des cas d'abus demeurent réservés.

Le service SWITCH edu-ID enregistre les données qui résultent d'identités mises en relation et les tient à jour.

Les services auxquels l'utilisateur final a déjà accédé peuvent demander au service SWITCH edu-ID des valeurs actualisées de leurs informations existantes, afin de tenir à jour leur base de données d'utilisateurs.

Grâce aux mesures appropriées, SWITCH garantit la confidentialité, l'intégrité et la disponibilité des données qui lui sont confiées. Ces mesures comprennent notamment :

- des mesures structurelles et des restrictions d'accès à l'infrastructure des serveurs
- un règlement relatif à l'accès (concept utilisateur, firewall et dispositifs similaires)
- une maintenance régulière des serveurs
- une surveillance automatisée des services
- un concept d'exploitation redondant et la création de copies de sauvegarde comme protection contre les pertes de données
- le chiffrement des données et une signature lors de leur transmission
- la promotion d'une culture de modération lors de la transmission de données au sein de la Federation
- l'implication de l'utilisateur final dans les processus qui concernent ses données
- la sensibilisation du personnel aux questions de protection des données à travers des ateliers
- les règlements et les instructions
- les contrats.

6.3.2 Lieu de stockage des données

Les serveurs contenant toutes les données enregistrées par SWITCH se trouvent au sein de l'infrastructure SWITCH en Suisse.

6.3.3 Responsabilité des SWITCHaai Participants

Le SWITCHaai Participant se conforme à tout moment aux dispositions de la loi fédérale suisse sur la protection des données ainsi qu'aux dispositions cantonales, dans la mesure où elles concernent le SWITCHaai Participant et le traitement de données personnelles au sein de la SWITCHaai Federation. De plus, il se conforme aux EU Standard Contractual Clauses (ou à toute formulation plus stricte dans certaines juridictions) et garantit que les sections correspondantes sont incluses dans tous les contrats relatifs au transfert de données personnelles.

A cette fin, le SWITCHaai Participant prend les mesures techniques et organisationnelles appropriées pour éviter un traitement non autorisé ou illégal des données et une perte accidentelle ou une destruction desdites données. Il respecte les recommandations éventuelles faites par SWITCH à cet égard.

Chaque AP Operator et chaque IdP Operator est tenu de respecter les instructions relatives au *Legal Templates for SWITCHaai*[37].

6.3.4 Responsabilité de l'utilisateur final

Toute donnée que l'utilisateur final enregistre, par exemple le nom, l'adresse e-mail ou l'adresse postale etc., doit correspondre à la réalité. Le service SWITCH edu-ID peut envoyer des rappels à l'utilisateur final en guise d'aide.

L'utilisateur final doit choisir un mot de passe sûr et le protéger de sorte que son SWITCH edu-ID Account ne puisse pas être utilisé par des tiers.

L'utilisateur final n'a pas le droit de posséder plus d'un SWITCH edu-ID Account. Tout doublon créé par erreur doit être signalé à l'assistance[38] qui se charge ensuite de fusionner les Accounts dupliqués. D'éventuelles pertes de données causées par la fusion des Accounts, par exemple pour les services utilisés précédemment, doivent être corrigées par l'utilisateur final.

Une utilisation non conforme ou abusive d'un SWITCH edu-ID Account ou du service SWITCH edu-ID ou une infraction aux présentes conditions d'utilisation peut entraîner le blocage ou la suppression du SWITCH edu-ID Account concerné (cf. chapitre 6.7).

6.3.5 Traitement des données par le Service

Lors de chaque accès d'un utilisateur final à un Service, le SP peut demander certaines données relatives à l'utilisateur final. Dans ce cas, l'autorisation de l'utilisateur final est nécessaire pour transmettre ses données de l'IdP au SP. Cette fonction d'approbation indique à l'utilisateur final les données à transmettre et l'aide à protéger ses données personnelles.

Les données personnelles de l'utilisateur final, telles que le nom, l'adresse e-mail ou la date de naissance, peuvent être utilisées et transmises par les Service Providers exclusivement aux fins suivantes:

- Fourniture des services proposés par des Service Providers
- Authentification et autorisation

[37] https://www.switch.ch/aai/legaltemplates/
[38] eduid-support@switch.ch

- Pour contacter l'utilisateur final
- Afin de détecter les doublons et les Affiliations qui ne sont plus actives et de régler ces situations.

Des conditions d'utilisation spécifiques relatives à la protection des données peuvent s'appliquer à des Services qui ont recours à SWITCH edu-ID pour leur authentification.

6.3.6 Audits

Le service SWITCH edu-ID est régulièrement audité dans le cadre d'un processus ISMS[39]. Ceci implique la définition et l'ajustement régulier des mesures techniques et organisationnelles nécessaires au fonctionnement du service.

La SWITCHaai Federation Policy (cf. chapitre 5) ne prévoit a priori pas d'audit auprès des SWITCHaai Participants (y compris SWITCH). Certaines circonstances peuvent toutefois rendre un audit nécessaire. Le droit de réaliser un audit demeure donc réservé.

6.4 Collaboration avec des tiers situés dans le pays ou à l'étranger

Si les organisations et les utilisateurs finaux participants y consentent, des données personnelles peuvent être transmises à un SP (en Suisse ou à l'étranger) afin d'effectuer l'authentification décrite au chapitre 3.2.3.5 et l'émission des attributs qui y est liée.

Les SWITCHaai Participants acceptent qu'une partie des informations qu'ils saisissent lorsqu'ils inscrivent leurs ressources dans le Resource Registry soient rendues accessibles à d'autres participants de la SWITCHaai Federation et qu'elles servent de description librement accessible sur le web ou dans les Metadata. Si de telles informations sont accompagnées de conditions d'utilisation, de mentions de copyright ou d'autres déclarations de propriété intellectuelle, le consommateur de ces informations doit se conformer auxdites restrictions ou contacter SWITCH pour clarifier la situation relative à l'utilisation.

6.5 Accès aux données par les collaborateurs

Si des données sont transférées à SWITCH à des fins de traitement, il est possible qu'une organisation/un partenaire contractuel requière, pour des raisons d'exploitation, l'accès à des données qui ont été stockées sur demande de l'organisation/du partenaire contractuel par un employé qui est alors injoignable.

Dans un tel cas, l'organisation/le partenaire contractuel doit prouver de manière claire et détaillée qu'elle/il est en droit d'accéder aux données en question. Si cette preuve ne peut pas être fournie de manière incontestable ou s'il subsiste un risque de responsabilité non supportable pour SWITCH, SWITCH est en droit de refuser ledit accès.

6.6 Utilisation autorisée du service

L'utilisation du service n'est autorisée que si elle n'entraîne aucune violation des présentes conditions d'utilisation, des droits de tiers ou des lois applicables.

[39] ISMS: Information Security Management System

6.7 Utilisation inappropriée du service

Une utilisation inappropriée du service est définie par les dispositions du RRP ou les CG dans leur version en vigueur.

Les organisations dont font partie les utilisateurs finaux fautifs peuvent, en plus des utilisateurs finaux, être tenues responsables de tous les dommages encourus par SWITCH ou par des tiers en raison d'une utilisation inappropriée du service par lesdits utilisateurs finaux.

Sur première demande de SWITCH, l'organisation dont l'utilisateur final fautif fait partie est tenue de défendre à ses frais les demandes déposées par des tiers à l'encontre de SWITCH en relation avec l'utilisation inappropriée du service. Cette organisation est tenue d'assumer conjointement et solidairement les frais juridiques et les coûts assimilés, les droits de licence et/ou les obligations de dommages-intérêts encourus par SWITCH, dans la mesure où SWITCH a notifié par écrit l'organisation concernée et s'il l'a autorisée à mener et à résoudre le litige, notamment par une transaction judiciaire ou extrajudiciaire.

En cas de suspicion fondée d'une utilisation illégale ou non-contractuelle du service, SWITCH se réserve le droit de supprimer immédiatement les Accounts concernés et/ou de bloquer temporairement ou définitivement les utilisateurs finaux enregistrés concernés sans en informer au préalable les utilisateurs finaux ou les organisations concernés, ceci sans que les utilisateurs finaux ou les organisations concernés ne puissent faire valoir de droit à une réparation.

Afin de garantir un bon fonctionnement, SWITCH peut en outre demander, à tout moment et sans suspicion d'une utilisation inappropriée, que les utilisateurs finaux enregistrés réinitialisent leur mot de passe ou exécutent à nouveau une procédure d'authentification.

Les utilisateurs finaux et les organisations sont tenus d'assister SWITCH dans la clarification d'incidents en cas d'utilisation inappropriée, d'infractions et d'autres faits dommageables.

En outre, SWITCH se réserve le droit, dans tous les cas où ceci est requis par la loi ou approprié, de collaborer avec les autorités publiques compétentes et de fournir toutes les informations nécessaires à la poursuite des infractions juridiques.

6.8 Garantie

La garantie est soumise aux dispositions du RRP et des CG dans leur version en vigueur en relation avec la disponibilité garantie au chapitre 3.3.

SWITCH ne garantit pas de résultat particulier en rapport avec un service fourni par une organisation lorsque l'authentification se base sur le service SWITCH edu-ID.

6.9 Responsabilité

6.9.1 Responsabilité de SWITCH

La responsabilité de SWITCH à l'égard des organisations de la SWITCH Community est régie par les dispositions du RRP dans sa version en vigueur. SWITCH décline toute responsabilité quant à l'utilisation légale du service.

La responsabilité de SWITCH à l'égard des organisations de l'Extended SWITCH Community est régie par les dispositions des CG dans leur version en vigueur.

La responsabilité de SWITCH à l'égard des utilisateurs finaux et des tiers qui utilisent le service de SWITCH sans contrat conclu séparément avec SWITCH mais avec le consentement de l'organisation est exclue, dans la mesure autorisée par la loi. Notamment, SWITCH ne peut être tenue responsable des violations de la protection des données par des organisations ou des prestataires de service si l'authentification est traitée via le service SWITCH edu-ID.

6.9.2 Responsabilité des organisations

Les organisations sont conjointement et solidairement responsables à l'égard de SWITCH, dans le cadre légal, au titre des dommages encourus par SWITCH du fait d'une utilisation inappropriée des services et au titre d'autres dommages indirects. Cette responsabilité continue d'exister même si les SWITCHaai ou SWITCH edu-ID Accounts ont déjà été supprimés.

La responsabilité comprend en particulier les comptes techniques et de test dans SWITCH edu-ID, cf. paragraphe 5.1.3.7.

6.9.3 Responsabilité de l'utilisateur final

L'utilisateur final est responsable de toutes les activités réalisées en rapport avec son SWITCH edu-ID Account et sa responsabilité peut être engagée à ce titre par les AP Operators, IdP Operators, SP Operators et SWITCH.

L'utilisateur final est responsable à l'égard de SWITCH, dans le cadre légal, au titre des dommages encourus par SWITCH du fait d'une utilisation inappropriée de son SWITCHaai ou SWITCH edu-ID Account ainsi qu'au titre d'autres dommages indirects. Cette responsabilité continue d'exister même si le SWITCHaai ou SWITCH edu-ID Account a déjà été supprimé.

Dans le cas d'un abus relatif à son identité numérique, l'utilisateur final ne peut demander de réparation à l'encontre des AP Operators, IdP Operators, SP Operators ou SWITCH.

6.10 Droit applicable et for juridique

L'utilisation du SWITCH edu-ID Account est soumise au droit suisse.

Le droit applicable et le for juridique sont définis par les dispositions du RRP ou les CG dans leur version en vigueur.

6.11 Versions linguistiques

La présente description du service existe en versions allemande, française, italienne et anglaise. Toutes les versions linguistiques ont la même valeur.

6.12 Révisions

La présente version est la première.