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

Descrizione del servizio

SWITCH edu-ID

Versione 1.0.3
Valida dal: 15. Febbraio 2018

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

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

1 Presentazione e obiettivi

Il presente documento definisce il concetto di funzionamento e le regole per gli utenti finali che utilizzano il servizio SWITCH edu-ID per la gestione della propria identità digitale unitamente alle regole rivolte alle organizzazioni e ai gestori di servizi che fanno parte della SWITCHaai Federation.

Il presente documento è pertanto così strutturato:

Il capitolo 3 riporta le definizioni e illustra le funzioni in senso stretto.

Il capitolo 4 si rivolge specificatamente agli utenti finali.

Il capitolo 5 si rivolge specificatamente alle organizzazioni che fanno parte della SWITCHaai Federation.

Il capitolo 6 raccoglie le condizioni d'uso legali applicabili agli utenti finali e alle organizzazioni partecipanti.

Il presente documento è vincolante nella sua totalità sia per gli utenti finali, sia per le organizzazioni. Utilizzando il servizio SWITCH edu-ID, gli utenti finali, le organizzazioni e i gestori di servizi accettano le presenti condizioni e regole.

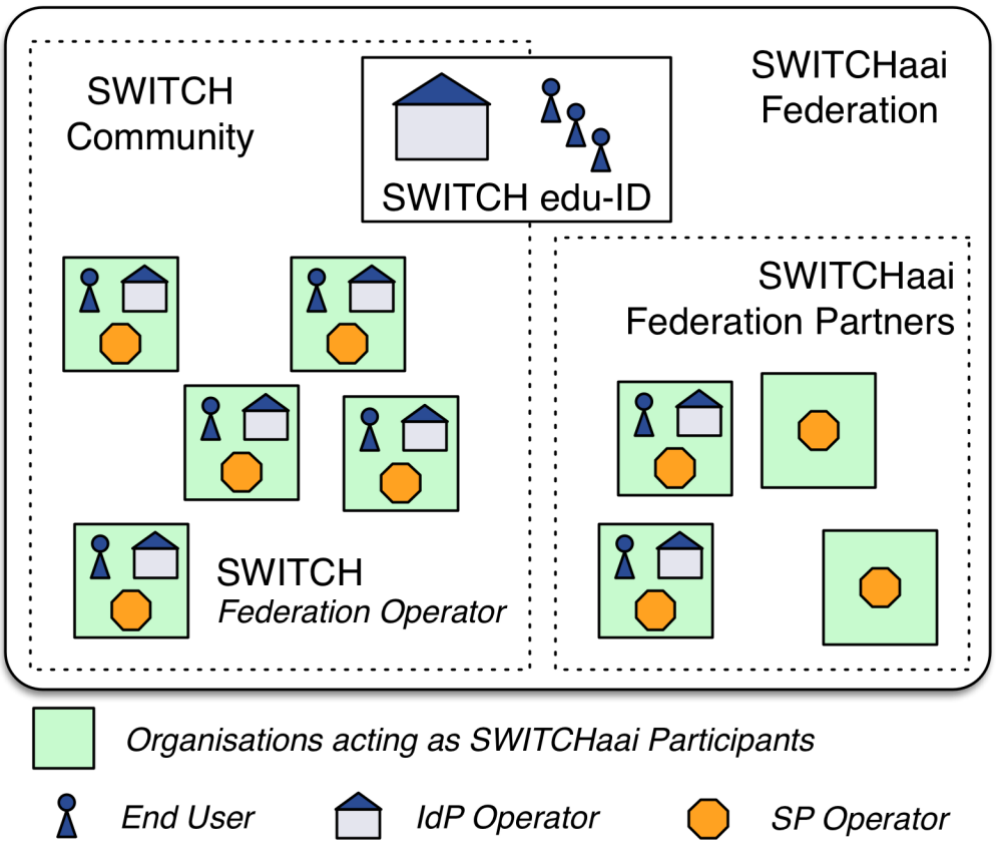
Il concetto di funzionamento alla base di SWITCH edu-ID si fonda sul concetto SWITCHaai, che sviluppa a sua volta ulteriormente. La presente descrizione del servizio sostituisce pertanto la SWITCHaai Service Description V1.0 del 15 novembre 2011.

Il servizio SWITCH edu-ID è inserito nel quadro della SWITCHaai Federation, il cui funzionamento è descritto in dettaglio nel capitolo 5.

La SWITCHaai Federation persegue l'obiettivo di semplificare e promuovere l'impiego interorganizzativo dei servizi. L'utente finale può impiegare la propria identità digitale per utilizzare i servizi registrati nella SWITCHaai Federation o in un'altra Federation federazione mediante l'Interfederation.

In qualità di Federation Operator, SWITCH coordina le necessarie attività.

Per gli SWITCHaai Participant della SWITCH Community, la partecipazione a SWITCHaai è disciplinata dal Regolamento dei servizi (RdS) e sue eventuali successive modifiche. Per Federation Partner, la partecipazione a SWITCHaai è disciplinata dalle Condizioni generali (CG) e loro eventuali successive modifiche (si veda il capitolo 6.1).



Le descrizioni di SWITCHaai e SWITCH edu-ID sono disponibili al pubblico[1]. Il link riportato[2] consente l'accesso diretto a SWITCH edu-ID.

I principi di perfezionamento di SWITCHaai sono stati definiti nell'ambito del progetto *Swiss edu-ID*, con cui è stato in parte finanziato lo sviluppo del servizio *SWITCH edu-ID*[3].

[1] https://www.switch.ch/it/services/aai/
[2] https://eduid.ch/
[3] https://www.swissuniversities.ch/it/organizzazione/progetti-e-programmi/p-5/

2 Sintesi delle informazioni fondamentali per l'utente finale

- SWITCH edu-ID è un servizio di SWITCH, che gestisce identità digitali per l'impiego permanente da parte di utenti iscritti a istituti d'istruzione superiore e altri utenti finali. In particolare, lo SWITCH edu-ID Account resta valido se l'utente finale, in qualità di titolare dell'identità digitale, abbandona un'organizzazione (a differenza di altri SWITCHaai Account).

- È possibile l'esistenza di un solo SWITCH edu-ID Account per utente finale. Gli utenti finali si impegnano a non generare duplicati e, qualora dovessero comunque venirsi a creare dei doppi Account, a informare il servizio d'assistenza SWITCH edu-ID affinché questi vengano uniti.

- Gli utenti finali si impegnano a fornire dati veritieri e a provvedere al loro aggiornamento.

- Gli utenti finali sono responsabili di tutte le attività correlate al proprio SWITCH edu-ID Account. Si impegnano pertanto anche a tutelare il proprio SWITCH edu-ID Account e a non consentirne l'utilizzo da parte di terzi. Si impegnano altresì a scegliere password sicure e a non trasmetterle a terzi.

- SWITCH[4] gestisce il servizio e tratta i dati secondo il diritto svizzero. I dati e i server si trovano in Svizzera.

- Solo i dati necessari alla fornitura del servizio SWITCH edu-ID possono essere memorizzati. Se l'utente finale decide di collegare il proprio SWITCH edu-ID Account ad altre identità, come ad esempio l'identità SWITCHaai presso un università o ORCID[5], possono essere disponibili ulteriori applicazioni.

- Al momento dell'utilizzo dei servizi, possono essere richiesti dati che sono memorizzati nello SWITCH edu-ID Account dell'utente finale, il quale può decidere se trasmetterli al servizio o negare l'accesso a tali dati.

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

3 Definizioni e descrizione delle funzioni

3.1 Definizioni

Affiliation degli utenti finali	L'*Affiliation* definisce il ruolo di un utente finale rispetto a un'organizzazione entro la SWITCHaai Federation. Essa si genera *collegando* un'identità di base all'*identità correlata all'organizzazione* dell'utente. Le identità di base possono essere collegate a una o più *Affiliation* di un utente finale o non essere collegate ad alcuna. Le Affiliation in corso di validità vengono definite *Current Affiliation* mentre le Affiliation non più attive vengono denominate *Former Affiliation*.
Assertion	Gli attributi di norma vengono rilasciati in forma di *Assertion* criptata e firmata del fornitore di IdP a uso del SP. L'Assertion è un contenitore sicuro per informazioni potenzialmente riservate. Sulla base degli attributi ricevuti in tal modo, l'SP o il Service protetto dall'SP decide se garantire all'utente finale l'accesso al Service in questione.
Attribute **Base Attribute** **Affiliation Attribute** **Complementary Attribute**	Un *attributo* è un'unità di informazione descrittiva con un nome predefinito, come ad esempio nome, e-mail, data di nascita, numero di telefono, *SWITCH edu-ID Identifier*, ecc. Gli attributi utilizzati in SWITCHaai sono documentati e specifici[6]. Gli attributi vengono spesso raccolti in categorie, ad esempio, nell'ambito di SWITCHaai, in *Core Attribute* e *Other Attribute*, oppure, nell'ambito di SWITCH edu-ID, in *Base Attributes*, *Affiliation Attributes* e *Complementary Attributes*. I *Base Attributes* sono parte integrante dell'*identità di base*. Gli *Affiliation Attributes* sono legati all'*Affiliation* dell'utente finale e vengono gestiti ed erogati da un *Attribute Provider* specifico dell'organizzazione. Gli attributi presentano le seguenti caratteristiche: • vengono rilasciati dalle organizzazioni; • vengono rilasciati solo per la durata dell'Affiliation. I *Complementary Attributes* vengono gestiti ed erogati da *Attribute Provider* integrativi.
Attribute Provider (AP)	In SWITCH edu-ID, l'*Attribute Provider (AP)* emette gli attributi di Affiliation specifici dell'organizzazione o gli attributi complementari per gli utenti definiti univocamente da uno *SWITCH edu-ID Identifier*. Nella migrazione a SWITCH edu-ID, lo *SWITCHaai Participant* sostituisce l'IdP presente attraverso un AP specifico dell'organizzazione.
AP Administrator	Il soggetto esecutivo dell'*AP Operator* viene definito *AP Administrator*.

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

AP Operator	Il soggetto giuridico rappresentante lo *SWITCHaai Participant* e responsabile in toto della gestione di un *Attribute Provider* viene denominato *AP Operator*; si veda il capitolo 5.1.3.8.
Condizioni generali (CG)	Le Condizioni generali sono parte integrante del contratto e sono disponibili sul sito web di SWITCH[7].
Extended SWITCH Community	Organizzazioni in stretto rapporto con la SWITCH Community, in particolare organizzazioni politica universitaria, accademie, istituti di finanziamento, biblioteche e ospedali nonché istituti di ricerca privati e scuole terziarie che non fanno parte della SWITCH Community.
Federated Authentication	Si intende il processo di registrazione in cui si impiega la propria identità digitale per ottenere l'accesso ai servizi offerti dagli *SP Operators* nella Federation.
Federation (in particolare la SWITCHaai Federation)	La Federation è un'associazione di organizzazioni che accettano di collaborare sulla base di un impianto normativo comune. Tali normative riguardano in questo contesto la Federated Authentication and Authorization. La SWITCHaai Federation indica la rispettiva associazione delle organizzazioni svizzere di istruzione superiore[8]. Il servizio SWITCH edu-ID è inserito nel quadro della SWITCHaai Federation.
Federation Operator	Il Federation Operator gestisce e sviluppa la Federation, è responsabile dei componenti centrali e funge da centro di competenza. Nella SWITCHaai Federation, il Federation Operator è SWITCH.
Federation Technology Profile	Nei Technology Profile vengono definiti quali specifiche tecniche di una determinata tecnologia (ad esempio, un protocollo di comunicazione o un'interfaccia di programmazione di un'applicazione) far valere nell'ambito della Federation o come queste vadano applicate.
Identità collegata (Linked Identity, Linked Organisational Identity, Linked External Identity	Gli utenti finali possono collegare la propria identità di base ad altre identità. Se l'identità di base viene collegata all'identità dell'utente correlata a un'organizzazione della SWITCHaai Federation, si crea un'Affiliation. L'utente finale tuttavia può collegare la propria identità di base a un'identità esterna, quale ad esempio ORCID. Quindi, ad esempio, può essere aggiunto un Identifier esterno in qualità di attributo dell'identità di base.

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

Identità di base (Base Identity, Private Identity) Self-Declaration Self-Provisioning Quality Level	L'*identità di base* include informazioni specifiche dell'utente in senso stretto, quali cognome, nome, telefono cellulare privato o indirizzo e-mail personale. Nel servizio SWITCH edu-ID, l'utente finale registra autonomamente i dati per l'identità di base. Tale procedura viene denominata *Self-Declaration* e l'identità di base pertanto viene generata mediante un processo di *Self-Provisioning*. Anche i valori impiegati di frequente per il *Quality Level* delle informazioni presenti nell'identità di base sono soggetti a Self-Provisioning. L'utente finale può incrementare (o far incrementare) il Quality Level degli attributi nella propria identità digitale mediante processi di validazione.
Identità digitale (Digital Identity, identificazione digitale)	L'identità digitale è costituita da un insieme di informazioni sotto forma di attributi che può essere assegnato a un utente finale. Viene erogata e gestita da un operatore IdP, il quale può identificare l'utente finale in qualsiasi momento. L'identità digitale di base può riferirsi sia a persone, sia a cose. Tale opzione non è prevista nel presente contesto. Lo *SWITCH edu-ID Account* di un utente finale è un'identità digitale.
IdP (Identity Provider)	L'Identity Provider è il componente operativo che autentica gli utenti e rilascia le Assertion sull'utente finale per un Servizio. L'Assertion trasporta gli attributi dell'identità digitale necessari per l'accesso al Servizio. SWITCH gestisce l'IdP centrale di SWITCH edu-ID. Le organizzazioni possono gestire il proprio IdP o delegare a SWITCH tale compito. L'IdP centrale di SWITCH edu-ID si distingue dagli altri IdP poiché dispone di funzionalità aggiuntive (si veda il capitolo 3.2.3).
IdP Administrator	Il soggetto esecutivo dell'IdP Operator viene definito IdP Administrator.
IdP Operator	L'IdP Operator è uno SWITCHaai Participant che si assume la piena responsabilità della gestione di un IdP; si veda il capitolo 5.1.3.9. In particolare ciò comprende: • L'identificazione degli utenti finali; • La gestione delle identità digitali; • La definizione dei processi identificativi per gli utenti finali; • L'impiego di processi adeguati per la registrazione e la cancellazione degli utenti finali, di norma mediante l'utilizzo di un sistema di Identity Management (IdM). Tali responsabilità valgono anche per il servizio SWITCH edu-ID.
Interfederation	Attraverso l'Interfederation, gli utenti finali di una Federation ricevono l'accesso ai servizi di un'altra Federation. L'Interfederation per i membri SWITCHaai in linea di principio è aperta (si veda il capitolo 5.1.2.5).

Metadata	I Metadata comprendono dettagli tecnici e informazioni descrittive sui componenti che fanno parte della Federation, in particolare relativi a IdP, AP e SP. I Metadata di norma sono protetti da firma digitale che ne impediscono la modifica. I componenti all'interno della Federation si basano su tali Metadata per fidarsi reciprocamente sul piano tecnico. Nella SWITCHaai Federation i Metadata sono gestiti da SWITCH.
Organizzazione	Organizzazione all'interno della SWITCH Community o della Extended SWITCH Community o partner contrattuali di SWITCH. Le organizzazioni possono offrire i propri servizi ai propri utenti finali o agli utenti finali di altre organizzazioni. Di contro, le organizzazioni possono consentire ai propri utenti finali l'accesso ai servizi offerti da altre organizzazioni operando un Identity Provider (IdP) o un Attribute Provider (AP).
Partner contrattuali	Nel presente documento, i partner contrattuali sono organizzazioni che hanno stipulato un contratto per un determinato servizio con SWITCH, ma che tuttavia non appartengono né alla SWITCH Community, né all'Extended SWITCH Community.
Quality Level per Base Attributes	Un indicatore di qualità indica il Quality Level dei Base Attributes. In caso di Self-Declaration, all'inizio gli attributi quali indirizzo e-mail, numero di cellulare o indirizzo postale ricevono il Quality Level più basso, ossia il livello «self-declared». Gli attributi possono essere controllati mediante un processo di verifica attraverso il quale è possibile, in caso di esito positivo del controllo, aumentare il Quality Level.
Regolamento dei servizi (RdS)	Il regolamento dei servizi (regolamento dei servizi di SWITCH, Dienstleistungsreglement, DLR) costituisce parte integrante del contratto ed è disponibile sul sito web di SWITCH[9].
Servizio, Service Provider (SP)	Il Servizio è un'applicazione web o un altro tipo di applicazione offerta da un'organizzazione o soggetto terzo e alla quale possono accedere gli utenti finali. Il Servizio si basa sull'autenticazione dell'utente finale da parte dell'IdP di SWITCH edu-ID o di un altro IdP della Federation. Per autorizzare l'accesso dell'utente finale, il componente Service Provider (SP) valuta le informazioni relative allo stesso ricevute dall'SP nell'asserzione dell'IdP. Su tale base, il SP decide se concedere all'utente finale l'accesso al Servizio.
SP Administrator	Il soggetto esecutivo del SP Operator viene definito SP Administrator.
SP Operator	Il SP Operator è uno SWITCHaai Participant che si assume la piena responsabilità della gestione di un SP; si veda il capitolo 5.1.3.10. Il suo compito principale consiste nella definizione dei criteri di accesso al Servizio (autorizzazione).

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

SWITCH Community	Tutte le organizzazioni del settore dell'istruzione e della ricerca collegate a SWITCH (secondo quanto indicato nell'allegato del RdS).
SWITCH edu-ID Advisory Board	Quest'organo[10] è costituito dai rappresentanti dei principali gruppi di stakeholder della SWITCHaai Federation. Offre consulenza a SWITCH per questioni strategiche riguardo al servizio SWITCH edu-ID e alla SWITCHaai Federation.
SWITCH edu-ID (servizio)	SWITCH edu-ID è un servizio di identità digitale sviluppato da SWITCH per l'impiego permanente da parte di utenti iscritti a istituti d'istruzione superiore. Il servizio SWITCH edu-ID è descritto in dettaglio al capitolo 3.2.
SWITCH edu-ID (Identifier)	Lo SWITCH edu-ID Identifier è descritto in dettaglio al capitolo 3.2.2.2.
SWITCH edu-ID (Identity e concetto)	La SWITCH edu-ID Identity è l'analogo digitale di un documento d'identità e garantisce al titolare, ossia l'utente finale, l'accesso a diversi servizi. Il principio alla base di SWITCH edu-ID è descritto in dettaglio al capitolo 3.2.1.
SWITCHaai Participant	Un'organizzazione che prende parte a SWITCHaai (persona giuridica) viene definita SWITCHaai Participant.
SWITCHaai Federation Partner	Le organizzazioni non appartenenti alla SWITCH Community ma che prendono parte a SWITCHaai vengono definite SWITCHaai Federation Partner.
Trust & Identity WG (gruppo di lavoro fiducia e identità)	Questo gruppo di lavoro è formato dai rappresentanti di tutte le organizzazioni della SWITCH Community e dell'Extended SWITCH Community parte di SWITCHaai e di SWITCHpki. Da un lato, il gruppo costituisce un canale informativo e, dall'altro, una piattaforma di scambio per fornire un riscontro a domande di carattere operativo o tecnico.
Utente finale (utente, User)	Un *utente finale* è una persona fisica (uomo o donna) che utilizza il servizio. L'utilizzo ha inizio con la creazione di un SWITCH edu-ID Account personale da parte dell'utente finale. Il servizio SWITCH edu-ID si rivolge in particolare a tutti gli utenti finali collegati a organizzazioni della SWITCH Community.

3.2 Funzionamento di SWITCH edu-ID

3.2.1 Il concetto di SWITCH edu-ID

SWITCH edu-ID è un'identità digitale sviluppata da SWITCH destinata all'impiego permanente da parte di utenti iscritti a istituti d'istruzione superiore e altri utenti finali. Deve essere sicura e riconosciuta in tutto il mondo. Il servizio SWITCH edu-ID è basato su SWITCHaai, un'efficace soluzione federata di Identity Management che semplifica la gestione delle identità degli istituti d'istruzione superiore e consente di attivare ulteriori servizi all'identità digitale. Rispetto a SWITCHaai, SWITCH edu-ID introduce le seguenti novità:

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

- Centralità dell'utente (user-centric) e persistenza (persistency): l'identità digitale appartiene all'utente finale, il quale può controllare autonomamente le informazioni di base del proprio SWITCH edu-ID in qualsiasi momento. L'identità digitale è indipendente dall'appartenenza a un'organizzazione e resta pertanto valida anche quando l'utente finale abbandona un'organizzazione.
- Self-Provisioning: ogni persona fisica può crearsi la propria identità di base elettronica, divenendo così utente finale di SWITCH edu-ID. In tal modo riceve il pieno controllo su una serie di attributi personali (Base Attributes), quali cognome, nome, indirizzo e-mail o numero di cellulare.
- Quality Level degli attributi: il sistema di Self-Provisioning porta a priori e per sua natura a un livello qualitativo iniziale degli attributi più basso. Gli attributi pertanto non contengono solo un valore, bensì anche indicatori qualitativi che completano il valore. I Quality Level possono essere incrementati attraverso procedimenti di validazione o ridotti, ad esempio al raggiungimento di un termine (avanzare dell'età) o mediante modifica manuale del valore.
- Multiple Affiliation (Affiliation multiple): un utente finale può appartenere a una o più organizzazioni o a nessuna. Di conseguenza, la sua identità di base può contenere una o più Affiliation o nessuna a seconda che l'identità di base sia stata collegata con le identità correlate a organizzazioni parte della SWITCHaai Federation. Le informazioni appartenenti alle Affiliation vengono fornite dalle organizzazioni partecipanti, di norma attraverso i propri Attribute Provider (AP).

3.2.2 Come funziona il servizio SWITCH edu-ID?

Se l'utente finale dispone di un'identità di base, in linea di principio può impiegarla per accedere a una serie di servizi all'interno della SWITCHaai Federation. Il servizio può richiedere determinati Quality Level di specifici attributi di base al fine di consentire l'accesso o attributi complementari, che in particolare forniscono dati in merito alle Affiliations esistenti. Affinché tali dati vengano resi accessibili al Servizio, l'utente finale fornisce prima il proprio consenso (user consent).

Al momento della registrazione al servizio, l'IdP di SWITCH edu-ID raccoglie tutti gli attributi rilasciati necessari dell'utente finale all'interno di un'Assertion e li trasmette attraverso una modalità sicura al servizio, che li verifica e decide se consentire l'accesso in base alla rispettiva configurazione.

In tal senso, l'IdP di SWITCH edu-ID soddisfa i requisiti di un IdP all'interno della SWITCHaai Federation. Il servizio SWITCH edu-ID è caratterizzato dai seguenti principi:

3.2.2.1 Classic ed Extended Attribute Model (modello classico ed esteso degli attributi)

I servizi che possono gestire Affiliations multiple supportano l'*Extended Attribute Model*, ossia possono essere loro trasmesse tutte le informazioni di Affiliation disponibili e rilasciate dall'utente finale. Il servizio decide quindi come gestire le diverse Affiliation. Nel documento strutturale di Swiss edu-ID (capitolo 2.1) sono disponibili ulteriori dettagli in merito[11].

Tutti gli altri servizi richiedono un'Affiliation specifica e supportano pertanto il *Classic Attribute Model*. Nel caso in cui un utente finale possegga più Affiliation in corso di validità, deve

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

comunicare all'IdP mediante l'Affiliation Chooser (si veda il capitolo 3.2.3.6) quale Affiliation desidera impiegare per il servizio in questione. Solo gli Affiliation Attributes richiesti per l'Affiliation selezionata vengono trasmessi al servizio.

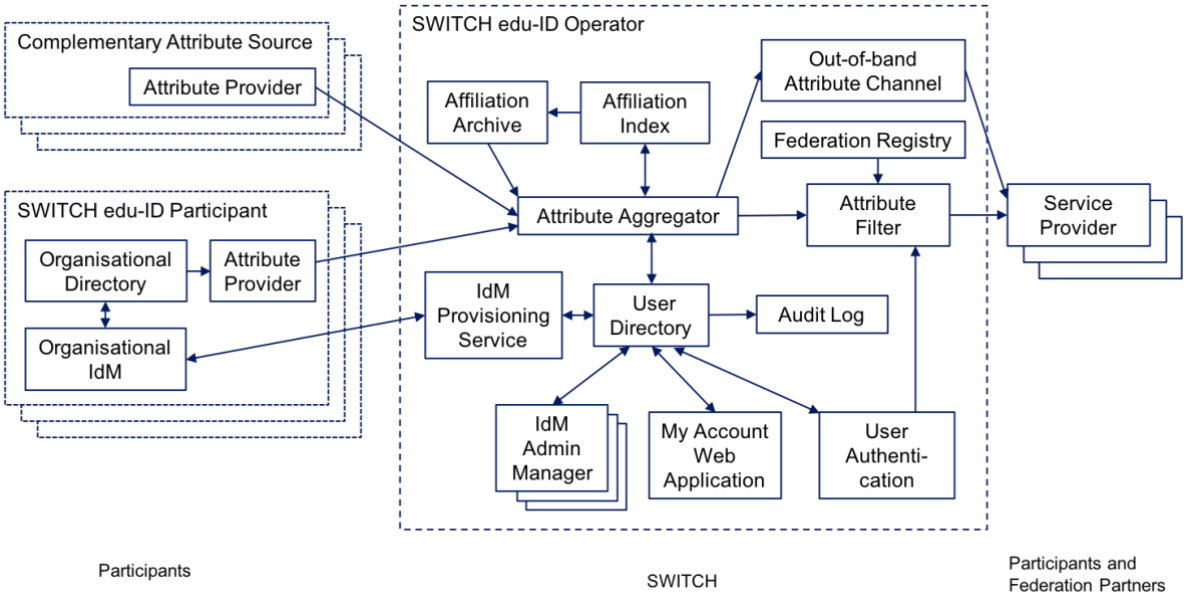
3.2.2.2 Lo SWITCH edu-ID Identifier

Lo SWITCH edu-ID Identifier[12] [13] identifica in maniera univoca e permanente ciascun utente finale. Esso costituisce l'identificativo primario di settore per la comunità accademica svizzera impiegato per il collegamento univoco di ulteriori dati personali.

Lo SWITCH edu-ID Identifier costituisce il presupposto per la raccolta di dati che possono essere visualizzati come profilo personale ai sensi della Legge federale sulla protezione dei dati del 19 giugno 1992 (LPD; RS 235.1)[14] e come tale deve essere pertanto trattato (si veda il capitolo 5.1.3.12).

Dove possibile, i servizi devono impiegare un altro identificativo (ad esempio un pairwise identifier o lo swissEduPersonUniqueID) salvo siano costretti da un motivo urgente a utilizzare lo SWITCH edu-ID Identifier. Se un servizio necessita dello SWITCH edu-ID Identifier, allo SP Operator vengono trasmessi i relativi obblighi di dovuta diligenza.

3.2.3 Componenti del servizio SWITCH edu-ID



3.2.3.1 Indice degli utenti finali (User Directory)

La SWITCH edu-ID Identity (identità di base) viene salvata nel database centrale di SWITCH edu-ID. A ogni autenticazione di un utente finale, si accede a tali dati. Ogni dato è attribuito specificatamente a un utente finale. Ogni utente finale è responsabile della correttezza dei propri dati.

[12] https://www.switch.ch/aai/support/documents/attributes/swisseduid/
[13] https://swit.ch/eduidspec
[14] https://www.admin.ch/ch/i/sr/c235_1.html

3.2.3.2 Attribute Aggregator

L'Attribute Aggregator (aggregatore di attributi) verifica che l'Affiliation Index (si veda il grafico) sia aggiornato tenendosi in contatto con i vari Attribute Provider specifici delle organizzazioni.

3.2.3.3 SP Notification

Previo accordo, il modulo SP Notification può informare gli SP di eventuali modifiche ai valori degli attributi. Gli SP hanno così la possibilità di aggiornare il proprio database di utenti.

3.2.3.4 Applicazione web «Account personale» (My Account)

Questa applicazione web consente all'utente finale di controllare tutti i propri dati personali, di aggiornarli ed eventualmente integrarli o farli verificare. Tutte le transazioni vengono registrate ai fini della tracciabilità.

3.2.3.5 Identity Provider (IdP)

L'Identity Provider è responsabile dell'autenticazione degli utenti finali (user authentication). Inoltre raccoglie gli attributi necessari per il SP che ha avviato l'autenticazione, richiede se necessario il consenso dell'utente finale alla trasmissione dei dati (user consent) e inoltre le informazioni in forma di Assertion a uso del SP.

3.2.3.6 Affiliation Chooser

Se necessario, dopo l'autenticazione l'Affiliation Chooser consente all'utente finale di selezionare una delle Affiliation esistenti con cui quindi iscriversi al servizio. L'Affiliation Chooser viene impiegato dai servizi che utilizzano il Classic Attribute Model. L'Affiliation Chooser ricava le Affiliations dall'Affiliation Index.

3.2.3.7 Affiliation Archive

Se l'Attribute Aggregator nota che un'Affiliation non viene più rinnovata dall'Attribute Provider, sposta le informazioni ancora presenti nell'Affiliation Archive delle Affiliations precedenti non più attive. In tal modo si conserva l'informazione che l'utente finale un tempo è stato affiliato all'organizzazione. I futuri servizi, ad esempio le organizzazioni di alumni, previa raccolta di relativa autorizzazione, possono rivolgersi specificatamente a tali gruppi di utenti.

3.2.3.8 Altri sistemi di supporto: Test Federation e Demo Sites

SWITCH gestisce una Test Federation[15] per provare nuovi componenti e configurazioni. Questa raccoglie i componenti necessari a fini dimostrativi, quali ad esempio un IdP, un AP o un SP, i quali illustrano in dettaglio le modalità di funzionamento di SWITCHaai e le possibili configurazioni.

3.2.3.9 Altri sistemi di supporto: Attribute Viewer

Con il nome di Attribute Viewer[16], SWITCH mette a disposizione un SP che richiede all'IdP tanti attributi quanti possibili e li visualizza su un sito web a uso dell'utente finale.

---

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

- Un IdP può impiegare l'Attribute Viewer per verificare se i propri attributi siano stati rilasciati correttamente.
- Gli utenti finali possono visualizzare quali attributi ha emesso l'IdP su di loro.
- In caso di dubbio, gli SP Administrator o gli utenti finali con le opportune competenze possono verificare la correttezza del proprio SP, controllare se l'IdP opera correttamente con l'AAI Attribute Viewer e contenere così eventuali problemi.

L'Attribute Viewer supporta il *Classic Attribute Model* ma, se necessario, può anche essere modificato in seguito per supportare l'*Extended Attribute Model*.

3.3 Disponibilità e supporto

Il servizio di base è disponibile 24 ore su 24, 7 giorni la settimana. SWITCH esegue interventi di manutenzione programmati solitamente al di fuori dei normali orari di ufficio annunciandoli almeno una settimana prima alla pagina di accesso dell'IdP di SWITCH edu-ID. SWITCH mira a garantire una disponibilità del servizio e di ogni sua sottocomponente pari ad almeno il 99,99%. Viene fatta riserva di eventuali guasti che possono compromettere il servizio.

SWITCH si impegna ad adottare e implementare misure volte all'eliminazione di guasti e malfunzionamenti del servizio entro i consueti orari d'ufficio.

Il supporto per gli utenti finali[17] è operativo durante i consueti orari d'ufficio.

I consueti orari d'ufficio sono definiti nelle disposizioni del Regolamento dei servizi (RdS) e delle Condizioni generali (CG) e loro rispettive eventuali modifiche.

SWITCH adotta inoltre le necessarie precauzioni per garantire anche al di fuori degli orari d'ufficio un'ottima qualità del servizio in funzione dell'urgenza e a propria discrezione.

3.4 Monitoraggio e conservazione dei dati (logging)

Le condizioni di funzionamento del servizio SWITCH edu-ID vengono descritte su base continuativa sul sito web pubblico di SWITCH[18].

Ulteriori informazioni sulle condizioni di funzionamento vengono fornite regolarmente agli SWITCHaai Participant sul portale dei clienti[19].

In coordinamento con le organizzazioni, SWITCH può monitorarne i componenti (in particolare gli IdP e gli AP) e renderne accessibili i risultati ad altre organizzazioni in forma appropriata. A tal fine SWITCH opera Account tecnici dedicati.

In caso di interruzione del servizio, SWITCH attiva il processo interno di Incident Management (gestione degli inconvenienti), che comprende anche azioni di comunicazione esterna.

SWITCH può salvare le modifiche alle condizioni di servizio o eventuali transazioni sui dati degli utenti finali ai fini della tracciabilità. Possono essere registrati in particolare i processi di validazione. I resoconti disponibili vengono messi a disposizione degli utenti finali in forma appropriata.

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

SWITCH conserva i dati riguardanti l'utilizzo del servizio da parte degli utenti finali o delle organizzazioni. Dove possibile, tale azione viene eseguita in maniera distinta per ciascuna organizzazione. SWITCH fornisce alle organizzazioni statistiche anonime sull'utilizzo di SWITCH edu-ID.

4 Informazioni specifiche dell'utente finale

4.1 Creazione e accesso

a) Tutti gli utenti finali interessati alla creazione di un'identità digitale durevole per l'accesso ai servizi possono usufruire del servizio SWITCH edu-ID.

b) Per utilizzare il servizio SWITCH edu-ID è necessario un apposito Account. A tal fine devono essere forniti almeno i seguenti dati:

- nome per esteso
- un indirizzo e-mail valido
- una password sicura

c) L'utente finale può modificare il nome fornito, l'indirizzo (o gli indirizzi) e-mail e la password del proprio SWITCH edu-ID Account in qualsiasi momento.

d) Per servizi specifici possono essere richiesti ulteriori attributi personali, come data di nascita, indirizzo, numero di telefono cellulare ecc. Una biblioteca, ad esempio, può spedire i libri all'utente solo nel caso sia stato fornito un indirizzo.

e) I Service Provider possono richiedere le informazioni sui *Quality Level* degli attributi di base. Gli attributi possono essere controllati mediante un processo di verifica attraverso il quale è possibile, in caso di esito positivo del controllo, aumentare il Quality Level. Ad esempio, per un numero di telefono cellulare può ad esempio essere richiesto che l'utente finale sia raggiungibile su tale numero.

La verifica può essere condotta dall'utente finale, da SWITCH o da un'organizzazione e può essere effettuata una o più volte. I Quality Level sono visibili nel applicazione web «Account personale».

f) Gli utenti finali possono creare un nuovo SWITCH edu-ID Account o utilizzare un SWITCHaai Account esistente. Il secondo procedimento offre il vantaggio di collegare da subito lo SWITCH edu-ID Account (in una sola direzione, ossia all'identità SWITCHaai) e di trasferire già gli attributi di base esistenti nell'Account. Al momento della creazione delle SWITCH edu-ID Account questi dati sono già visualizzati come campi non modificabili.

g) L'utente finale può collegare anche in seguito il proprio SWITCH edu-ID Account con uno o più SWITCHaai Account e aggiungerli quindi come Affiliations. Allo stesso modo è possibile effettuare un collegamento con identità esterne, quali ad esempio ORCID. Tali collegamenti possono essere necessari nel caso in cui l'utente finale volesse utilizzare lo SWITCH edu-ID Account per l'accesso a servizi per cui sono necessari gli identificativi delle identità collegate.

h) Le organizzazioni nella SWITCHaai Federation stabiliscono autonomamente quali dei propri servizi intendono mettere a disposizione dei singoli utenti finali e quali condizioni debbano essere soddisfatte per il loro utilizzo. L'utente finale non ha alcun diritto intrinseco all'accesso ai servizi.

4.2 Informazioni di contatto e pagina di supporto SWITCH edu-ID

In caso di domande relative alle SWITCH edu-ID Account è possibile consultare la pagina di supporto[20].

4.3 Amministrazione dell'utente finale

a) Un SWITCH edu-ID Account può essere creato dall'utente finale o con l'intermediazione di un'organizzazione.

b) Nel caso in cui l'utente finale dovesse abbandonare un'organizzazione, ad esempio un'università o un istituto di ricerca, il suo SWITCH edu-ID Account resta attivo, a differenza del SWITCHaai Account, che di norma viene disattivato una volta abbandonata un'organizzazione.

c) Per la revoca dello SWITCH edu-ID Account l'utente finale deve contattare l'assistenza SWITCH edu-ID[21] per e-mail. L'utente finale deve sapere che l'eliminazione della propria identità permanente contraddice il suo stesso scopo. Al momento della revoca dello SWITCH edu-ID Account tutti i dati dell'utente finale vengono eliminati definitivamente.

Determinate Affiliations esistenti con organizzazioni della SWITCHaai Federation possono impedire la revoca delle SWITCH edu-ID Account.

d) In caso di decesso, i familiari dell'utente finale possono contattare l'assistenza SWITCH edu-ID e chiederne il blocco e/o l'eliminazione presentando i necessari documenti ufficiali.

4.4 Archiviazione automatica e sospensione della fornitura degli SWITCH edu-ID Account

Gli SWITCH edu-ID Account non utilizzati per un periodo prolungato di tempo vengono inseriti nel processo automatico di archiviazione e sospensione della fornitura. La sospensione può essere operata anche su richiesta dell'utente finale (si veda il capitolo 4.3) e a seguito di utilizzo improprio (si veda il capitolo 6.7).

In una prima fase, l'utente finale viene contattato attraverso gli indirizzi e collegamenti registrati, in particolare attraverso le Affiliation presenti, per segnalargli l'inattività dello SWITCH edu-ID Account ed esortarlo a riprenderne l'utilizzo. I termini sono descritti alla pagina delle FAQ[22].

Nella fase successiva, lo SWITCH edu-ID Account viene bloccato, laddove l'utente finale non dia seguito all'invito a riprendere l'attività entro il termine indicato (si veda sopra). La riapertura dell'Account è possibile solo attraverso l'assistenza SWITCH edu-ID e solo a seguito di identificazione positiva del titolare.

Nella terza fase lo SWITCH edu-ID Account viene eliminato e gli attributi tecnici permanenti (in particolare lo SWITCH edu-ID Identifier e lo swissEduPersonUniqueID) vengono archiviati per evitare possibili riassegnazioni. I dati personali vengono cancellati nel rispetto della normativa vigente secondo la finalità d'uso di SWITCH edu-ID.

---

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

5 La SWITCHaai Federation Policy

5.1 Governance e ruoli

5.1.1 Governance

In qualità di Federation Operator, SWITCH gestisce la SWITCHaai Federation consultando sia lo SWITCH edu-ID Advisory Board[23], sia il Trust & Identity WG.

Nello SWITCH edu-ID Advisory Board siedono i rappresentanti dei principali gruppi di stakeholder delle organizzazioni partecipanti, tra cui i rappresentanti della SWITCH Community, di organi politici nel settore dell'istruzione e SP Operator. Lo SWITCH edu-ID Advisory Board opera in qualità di organo consultivo per la strategia a lungo termine del servizio SWITCH edu-ID.

SWITCH si consulta con lo SWITCH edu-ID Advisory Board su argomenti quali ad esempio:

- Quali categorie di Federation Partner accettare
- Quali categorie di Federation Partner possono gestire un IdP o un AP
- Accordo Interfederation
- Pianificazione dello sviluppo futuro di SWITCH edu-ID e della SWITCHaai Federation e ottimizzazione amministrativa e tecnica
- Modifiche nella gestione della SWITCHaai Federation o della presente descrizione del servizio, nonché di altri documenti specifici relativi alla Federation

Lo SWITCH edu-ID Advisory Board non ha alcun potere decisionale. SWITCH decide la composizione dello SWITCH edu-ID Advisory Board.

Il Trust & Identity WG è formato dai rappresentanti di tutte le organizzazioni della SWITCH Community e dell'Extended SWITCH Community parte di SWITCHaai e di SWITCHpki. Il gruppo viene coinvolto su base informale e può fornire un riscontro in caso di domande o modifiche.

SWITCH intrattiene solide relazioni con gli SWITCHaai Participant. SWITCH organizza eventi dove gli SWITCHaai Participant, in particolare gli AP, IdP e SP Administrator, ricevono informazioni e si confrontano sui nuovi sviluppi riguardo la *Federated Authentication and Authorization*.

SWITCH fornisce informazioni sulle idee e sui principi introdotti in SWITCH edu-ID e nella SWITCHaai Federation a gruppi interessati e organizzazioni che potrebbero adottare concept analoghi. A tal proposito, particolare attenzione viene dedicata ai gruppi che mostrano il massimo potenziale di sfruttamento della SWITCH Community.

SWITCH funge da centro di competenza per la *Federated Authentication and Authorization* nell'ambito della formazione accademica. SWITCH esegue il test del software e suggerisce e documenta soluzioni. SWITCH fornisce indicazioni sull'installazione e/o configurazione di pacchetti software specifici per determinati sistemi operativi da impiegare nella SWITCHaai

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

Federation. L'integrazione di altri prodotti è agevolata attraverso configurazioni esemplificative.

Laddove non siano altrimenti disponibili sottofunzioni, SWITCH ha la facoltà di sviluppare autonomamente i componenti mancanti o di incaricare soggetti terzi del loro sviluppo.

5.1.2 Diritti e obblighi del Federation Operator

5.1.2.1 Generale

SWITCH è responsabile del funzionamento della Federation e dell'inclusione standard delle organizzazioni nazionali e internazionali rilevanti.

SWITCH elabora e pubblica un elenco dei SWITCHaai Participant[24].

5.1.2.2 Resource Registry (RR)

Per l'amministrazione della Federation, SWITCH gestisce il Resource Registry[25]. Nell'ambito del Resource Registry, gli AP, IdP e SP vengono definiti come risorse.

Gli AP, IdP e SP Administrator degli SWITCHaai Participant mantengono aggiornate tutte le informazioni rilevanti sulle rispettive risorse, tra cui le informazioni di contatto e di assistenza, informazioni specifiche di configurazione tecnica, Attribute Requirement, Attribute Release Policy, Intended Audience, ecc.

Tutti questi dati vengono archiviati in un database, sulla base del quale SWITCH produce diversi tipi di ulteriori file utilizzati in altro ambito, quali ad esempio file di Metadata o configurazioni per l'Attribute Release per gli AP e IdP, ecc.

Per inserire nuovi SP nel Resource Registry e apportare modifiche a quelli già presenti è necessaria un'autorizzazione affinché essi siano attivati e compaiano nei Metadata. Tale funzione è responsabilità degli «AAI Resource Registration Authority Administrator» dello SWITCHaai Participant di competenza del SP. A seguito di opportuna verifica della correttezza e conformità dei dati, essi autorizzano il nuovo inserimento o la modifica. Si veda la documentazione sul Resource Registry[26].

5.1.2.3 Metadata Service

SWITCH gestisce il Metadata Service[27], il quale firma digitalmente e pubblica le proprietà degli SWITCHaai Participant. Per la firma, SWITCH impiega una SWITCHaai Root Certification Authority (CA)[28] offline apposita i cui certificati fungono da Trust Anchor per la verifica dei Metadata.

5.1.2.4 Discovery Service (DS)

SWITCH gestisce un Discovery Service centrale (anche denominato «Where Are You From» (WAYF) Service). Gli SP possono utilizzare tale Discovery Service centrale o configurare un

[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/

Discovery Service locale. SWITCH mette a disposizione degli SP Administrator le necessarie informazioni in merito.

5.1.2.5 Interfederation

SWITCH è responsabile della cura dei rapporti con i rappresentanti di interesse nazionali e internazionali nell'ambito della *Federated Authentication and Authorization*, per lo più nel settore dell'istruzione superiore. Ciò riguarda in particolare i contatti riguardanti le attività dell'Interfederation[29].

Purché di utilità per la SWITCH Community, SWITCH può stipulare accordi a nome della SWITCHaai Federation, ad esempio può condividere Metadata con altre Federation e/o con Interfederation Services.

Attraverso la partecipazione all'Interfederation, le organizzazioni da un lato possono offrire i propri servizi agli utenti finali di altre Federation e, dall'altro, consentire ai propri utenti finali di accedere ai servizi di altre Federation. Partecipando all' Interfederation, le organizzazioni contribuiscono alla riduzione degli Account di utenti finali locali.

5.1.2.6 Virtual Home Organisation (VHO)

La Virtual Home Organisation[30] costituisce l'IdP di ultima istanza per una piccola parte di utenti finali che devono ottenere l'accesso a singoli servizi protetti da SWITCHaai ma che non hanno ricevuto alcuna identità digitale dalla rispettiva organizzazione.

SWITCH gestisce l'IdP Virtual Home Organisation in associazione con un'applicazione web per l'amministrazione degli VHO Account fino a quando necessario.

Gli SP Administrator possono fare richiesta a SWITCH per l'amministrazione di un proprio gruppo di utenti finali di questo tipo. Per far ciò, devono seguire la SWITCHaai VHO Policy[31].

Ogni SWITCHaai Participant può inoltre richiedere per sé un VHO Account ai fini di prova.

SWITCH può fornire le funzionalità necessarie per la gestione di tali identità esterne all'organizzazione, di associazione a gruppo o Affiliation di organizzazioni senza proprio AP anche per mezzo di altri componenti.

5.1.3 Diritti e obblighi degli SWITCHaai Participant

5.1.3.1 Collaborazione

Lo SWITCHaai Participant collabora con SWITCH e adotta tutte le misure necessarie per il corretto funzionamento della SWITCHaai Federation. Questo include mettere a disposizione le informazioni necessarie, dati, risorse, diritti (d'accesso) e altri servizi. Lo SWITCHaai Participant in particolare si impegna a non alterare i servizi e i sistemi gestiti dalla SWITCHaai Federation o a non utilizzarli per scopi diversi da quelli previsti.

In qualità di AP Operator, l'organizzazione è responsabile della corretta trasmissione degli Affiliation Attributes per le identità di base SWITCH edu-ID esistenti. Si veda il capitolo 5.1.3.8.

---

[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

In qualità di IdP Operator, l'organizzazione è responsabile del corretto svolgimento dell'autenticazione e della corretta emissione dei Base Attributes. Si veda il capitolo 5.1.3.9.

Gli SWITCHaai Participant sono tenuti a segnalare tempestivamente a SWITCH eventuali modifiche personali ai propri AP, IdP e SP Administrator. Qualora ciò non avvenisse, SWITCH non può garantire l'accesso ai dati operativi dello SWITCHaai Participant.

5.1.3.2 Compliance

Lo SWITCHaai Participant garantisce di:

- installare, gestire e utilizzare i componenti AP, IdP e SP di propria responsabilità nel rispetto dei Federation Technology Profile;
- fornire a SWITCH i necessari contatti tecnici e amministrativi;
- non consentire l'accesso a terzi alla SWITCHaai Federation (fatta eccezione per i propri utenti finali) in assenza di autorizzazione scritta di SWITCH;
- fornire alla SWITCHaai Federation esclusivamente dati veritieri sui propri utenti finali.

5.1.3.3 Collaborazione con gli Administrator delle organizzazioni

SWITCH mette a disposizione degli AP e IdP Administrator inseriti nel Resource Registry un Service Desk di terzo livello, raggiungibile per e-mail o telefonicamente nei consueti orari d'ufficio[32].

5.1.3.4 Assistenza

Lo SWITCHaai Participant offre agli utenti finali un'assistenza di primo livello (ad esempio, il Service Desk) per rispondere direttamente alle loro domande durante gli orari d'ufficio locali. Il SWITCHaai Participant mette a disposizione dei propri SP Administrator un'assistenza di secondo livello.

5.1.3.5 Design Guideline

Gli SWITCHaai Participant si impegnano a rispettare le SWITCHaai Design Guideline[33] per gli elementi dell'interfaccia utenti finali.

I loghi di SWITCH possono essere impiegati solo come indicato nelle Design Guideline. I loghi di SWITCH sono marchi tutelati. Viene fatta riserva di qualsiasi utilizzo da parte di terzi al di fuori delle Design Guideline dietro autorizzazione scritta di SWITCH.

5.1.3.6 Accordi bilaterali entro la SWITCHaai Federation

Gli SWITCHaai Participant possono stipulare accordi riguardo l'erogazione e/o l'accesso ai servizi. A tal proposito, gli SWITCHaai Participant sono responsabili delle possibili conseguenze, per cui SWITCH non si assume alcuna responsabilità.

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

5.1.3.7 Account tecnici e Account di prova di SWITCH edu-ID

Gli AP Operator possono creare un numero limitato di Account tecnici o di prova per scopi specifici e dotarli di una delle proprie Affiliation. L'AP Operator si assume in tal caso la responsabilità di ciascuno dei propri Account. Egli può delegare internamente la responsabilità a uno dei propri AP Administrator assicurandosi inoltre che gli indirizzi di posta elettronica registrati possano effettivamente ricevere e-mail. In caso di inattività, l'AP Operator farà eliminare immediatamente l'Account tecnico o di prova. Con cadenza regolare, SWITCH invia promemoria agli AP Operator riguardo tali Account.

5.1.3.8 Obblighi dell'AP Operator

L'AP Operator si attiene alla presente descrizione del servizio e ne garantisce il rispetto anche da parte dei propri utenti finali. Eventuali usi impropri dei valori degli attributi originati da un AP vengono imputati al relativo AP Operator.

L'AP Operator

- garantisce la correttezza dei valori degli attributi da lui assegnati agli utenti finali;
- su richiesta di un altro SWITCHaai Participant trasmette i processi IdM (in particolare l'assegnazione e la revoca degli Affiliation Attributes);
- segnala tempestivamente a SWITCH la presenza di duplicati rilevati e/o eventuali usi impropri individuati degli Account degli utenti finali;
- consente al servizio SWITCH edu-ID l'aggiornamento delle proprie informazioni in cache purché riguardanti l'Affiliation.

5.1.3.9 Obblighi dell'IdP Operator

L'IdP Operator si attiene alla presente descrizione del servizio e ne garantisce il rispetto anche da parte dei propri utenti finali. All'IdP Operator viene imputato l'eventuale uso improprio delle identità digitali sul cui IdP si è autenticato il relativo utente finale.

L'IdP Operator

- si assicura di poter identificare i propri utenti finali;
- su richiesta di un altro SWITCHaai Participant trasmette i processi IdM (inclusi l'identificazione, l'autenticazione e i processi di On-Boarding [inclusione] e Off-Boarding [uscita]);
- si impegna ad attivare lo User Consent Dialog[34] per la partecipazione all'Interfederation con l'IdP.

5.1.3.10 Obblighi del SP Operator

Per l'assegnazione degli accessi, l'erogazione del servizio e la rettifica dei dati, gli SP si affidano all'autenticazione efficace con l'IdP e agli attributi ricevuti. Gli SP Operator si impegnano a utilizzare i dati ricevuti, inclusi i dati personali, esclusivamente a tal fine.

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

5.1.3.11 Aggiornamento dei dati presso i Service Provider

Ogni volta che un utente finale accede a un servizio, quest'ultimo riceve dati personali sull'utente, e può archiviarli presso di sé laddove necessario nell'ambito dell'utilizzo del servizio. Tali dati possono divenire obsoleti e il servizio ha la facoltà di richiederne la validità all'IdP di SWITCH edu-ID ai fini dell'aggiornamento dati. L'IdP di SWITCH edu-ID a sua volta può assicurarsi mediante interventi tecnici che il servizio possa presentare tale richiesta solo per le identità che già conosce (ad esempio, consentendo la richiesta solo attraverso un pairwise identifier quale l'eduPersonTargetedId[35]).

5.1.3.12 Sicurezza dello SWITCH edu-ID Identifier

Ai fini del collegamento univoco con l'identità locale correlata a un'organizzazione, gli AP Operator possono ricevere lo SWITCH edu-ID Identifier[36] dei propri utenti finali. A tal proposito, essi si impegnano a

1. mantenere sempre riservato tale Identifier e gestirlo di conseguenza e, in particolare, a non renderlo accessibile a terzi;
2. utilizzare tale Identifier esclusivamente ai fini della ricerca di altri attributi personali a uso dell'IdP di SWITCH edu-ID o per processi di gestione delle identità, in particolare a prevenzione della creazione di duplicati. Per tutti gli altri scopi devono essere impiegati altri Identifier;
3. salvare tale Identifier solo nei sistemi appositamente necessari e a
4. non rendere accessibile tale Identifier agli utenti finali in assenza di esplicita richiesta.

SWITCH supporta le organizzazioni nella formazione dei propri collaboratori in merito alla gestione dello SWITCH edu-ID Identifier e altri dati personali.

5.1.3.13 Introduzione di SWITCH edu-ID in un'organizzazione

SWITCH offre la propria consulenza alle organizzazioni per l'introduzione di SWITCH edu-ID. Di norma a tal fine l'organizzazione tramuta il proprio IdP in un AP e una parte dei processi all'interno dell'organizzazione (in particolare i processi di On-Boarding/Off-Boarding) viene modificata.

Fino all'introduzione di SWITCH edu-ID, l'IdP dell'organizzazione è responsabile della corretta autenticazione degli utenti (User Authentication), a seguire tale responsabilità passa all'IdP di SWITCH edu-ID.

Fino all'introduzione di SWITCH edu-ID, l'IdP dell'organizzazione mette a disposizione del SP il set completo di attributi necessari; a seguire tale responsabilità passa all'IdP di SWITCH edu-ID, il quale raccoglie a tal fine una parte delle informazioni presso l'AP dell'organizzazione.

Per l'introduzione di SWITCH edu-ID, l'organizzazione definisce e implementa i propri processi di On-Boarding ex novo così che non possano essere più prodotte nuove identità digitali per nuovi utenti, ma che venga collegata invece una nuova Affiliation con un'identità di base SWITCH edu-ID esistente. L'AP assegna i relativi Affiliation Attributes. In maniera analoga, anche la procedura di Off-Boarding viene semplificata eliminando solo l'Affiliation.

---

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

Con l'introduzione di SWITCH edu-ID, l'organizzazione accetta le disposizioni della presente descrizione del servizio.

Dal momento dell'introduzione di SWITCH edu-ID per il primo SWITCHaai Participant ha luogo una gestione mista in cui alcune organizzazioni creano ancora autonomamente le identità digitali, altre invece collegano solo le proprie Affiliation all'identità SWITCH edu-ID.

L'introduzione di SWITCH edu-ID di per sé non può portare alla creazione di duplicati.

5.2 Condizioni di partecipazione

5.2.1 Destinatari

Possono prendere parte a SWITCHaai le organizzazioni della SWITCH Community, dell'Extended SWITCH Community e altre organizzazioni purché di utilità per la SWITCH Community.

5.2.2 Commissioni

SWITCH si riserva il diritto di applicare commissioni agli SWITCHaai Federation Partner per la partecipazione a SWITCHaai e per l'utilizzo di altri servizi.

In particolare, SWITCH può richiedere ai Federation Partner una quota di partecipazione per l'opzione Interfederation.

Le commissioni sono da saldare rispettivamente entro 30 giorni. Oltre tale scadenza, si considerano decaduti gli accordi stipulati.

5.3 Procedure

5.3.1 Procedura di adesione

Le nuove organizzazioni possono gestire gli SP e, alle condizioni richieste, un AP oppure, per casi debitamente motivati, un IdP.

Di base qualsiasi organizzazione che attraverso la gestione di servizi contribuisca alla SWITCHaai Federation può presentare debita richiesta a SWITCH per rendere così accessibili i propri servizi agli SWITCHaai Participant.

Un'organizzazione non appartenente alla SWITCH Community presenta una richiesta formale di adesione per l'accettazione entro la SWITCHaai Federation. A tal fine, SWITCH valuta in particolare il vantaggio per la SWITCH Community rappresentato da tale inclusione. SWITCH decide infine se confermare l'adesione.

L'accettazione di un'organizzazione come SWITCHaai Federation Partner è soggetta alla sottoscrizione dello SWITCHaai Federation Partner Agreement.

Un'organizzazione dell'Extended SWITCH Community che entra a far parte della SWITCHaai Federation diventa un *Federation Partner Basic* se offre solo servizi senza gestire alcun AP o IdP. A determinate condizioni, l'organizzazione può anche essere autorizzata a gestire un AP o un IdP entro la SWITCHaai Federation. A tal fine riceve il ruolo di AP Operator o di un IdP Operator divenendo così un *Federation Partner Plus*.

Agli SWITCHaai Federation Partner si applicano le disposizioni del listino prezzi, del presente documento e delle Condizioni generali (CG).

5.3.2 Procedura in caso di ritiro

La disdetta dei servizi è disciplinata dalle disposizioni del Regolamento dei servizi (RdS) e delle Condizioni generali (CG) e loro rispettive eventuali modifiche.

6 Condizioni d'uso legali

6.1 Disposizioni applicabili

Creando il proprio SWITCH edu-ID o utilizzando per la prima volta il servizio SWITCH edu-ID, l'utente finale accetta la presente descrizione del servizio.

L'utilizzo dei servizi da parte delle organizzazioni e degli utenti finali sono soggetti alle seguenti disposizioni e loro eventuali successive modifiche:

- Alle organizzazioni della SWITCH Community e agli utenti finali appartenenti a un'organizzazione della SWITCH Community si applicano:
  - la presente descrizione del servizio
  - la rispettiva tariffa in vigore
  - il RdS

  In caso di incongruenze, la presente descrizione del servizio ha precedenza sul tariffario e il tariffario ha precedenza sul RdS.
- Alle organizzazioni dell'Extended SWITCH Community, agli utenti finali appartenenti a un'organizzazione dell'Extended SWITCH Community, ai partner contrattuali e agli utenti finali appartenenti a un partner contrattuale si applicano:
  - la presente descrizione del servizio
  - lo SWITCHaai Federation Partner Agreement
  - le CG

  In caso di incongruenze, la presente descrizione del servizio ha precedenza sul Federation Partner Agreement e il Federation Partner Agreement ha precedenza sulle CG.
- Agli utenti finali che non appartengono ad alcuna organizzazione della SWITCH Community o dell'Extended SWITCH Community, né a un partner contrattuale si applicano:
  - la presente descrizione del servizio
  - le CG

  In caso di incongruenze, la presente descrizione del servizio ha precedenza sulle CG.

6.2 Procedura in caso di modifiche

SWITCH può modificare la presente descrizione del servizio in qualsiasi momento e senza preavviso agli utenti finali; si veda il capitolo 5.1.1 Governance. In base all'entità delle modifiche, SWITCH può informare gli utenti finali o richiederne l'accettazione affinché essi possano continuare a utilizzare il proprio Account SWITCH edu-ID.

Entità e gestione delle modifiche:

a) **Marginale:** in caso di modifiche o correzioni di minima entità senza conseguenze sostanziali sugli accordi, è possibile apportare e pubblicare una modifica senza informare gli utenti finali. Se del caso, le modifiche possono essere segnalate agli utenti finali (ad esempio per e-mail o nel applicazione web «Account personale»).

b) Sostanziale: le modifiche con effetto diretto sugli accordi sono considerate sostanziali. Le modifiche sostanziali vengono discusse preliminarmente con lo SWITCH edu-ID Advisory Board e il Trust & Identity WG come descritto nel capitolo 5.1.1. Le modifiche vengono infine comunicate alle organizzazioni in modalità appropriate. In assenza di segnalazione di dissenso entro 30 giorni dalla comunicazione della modifica, questa entra in vigore. Il dissenso da parte di un'organizzazione porta alla risoluzione del contratto. In caso di modifiche sostanziali, gli utenti finali devono accettare di nuovo le condizioni di utilizzo dopo segnalazione delle modifiche alla successiva registrazione a un Servizio.

L'entità delle modifiche viene stabilita di volta in volta dal dipartimento legale di SWITCH.

6.3 Tutela e sicurezza dei dati

6.3.1 Trattamento dei dati da parte di SWITCH

Per quanto riguarda il trattamento dei dati personali, SWITCH si orienta alle disposizioni del RdS e delle CG e rispettive eventuali modifiche.

SWITCH inoltre elabora statistiche anonime a uso delle organizzazioni e dei partner contrattuali. Viene fatta riserva di eventuali casi di uso improprio.

Il servizio SWITCH edu-ID archivia e aggiorna dati risultanti dalle identità collegate.

I servizi cui l'utente finale ha acceduto almeno una volta possono richiedere al servizio SWITCH edu-ID i valori aggiornati delle rispettive informazioni presenti per aggiornare così il proprio database di utenti.

Attraverso l'adozione di opportune misure, SWITCH garantisce la riservatezza, l'integrità e la disponibilità dei dati ricevuti. Tra tali misure sono incluse:

- interventi strutturali e limitazioni d'accesso all'infrastruttura del server
- norme di accesso (user concept, firewall e simili)
- interventi periodici di manutenzione del server
- monitoraggio automatico del servizio
- principio operativo ridondante e creazione di back-up a prevenzione della perdita di dati
- cifratura dei dati e firma per la trasmissione delle informazioni
- promozione di una cultura del rispetto della privacy, che deve essere sempre considerata sin dalla progettazione in modo automatico, per lo scambio dei dati entro la Federation
- coinvolgimento dell'utente finale in processi relativi ai suoi dati
- sensibilizzazione del personale per questioni di tutela dei dati attraverso workshop
- regolamenti e direttive
- contratti

6.3.2 Luogo di archiviazione dei dati

I server per tutti i dati salvati su SWITCH si trovano nell'infrastruttura SWITCH in Svizzera.

6.3.3 Responsabilità dello SWITCHaai Participant

Lo SWITCHaai Participant rispetta in ogni momento le disposizioni dell'ordinamento giuridico svizzero in materia di protezione dei dati e le disposizioni cantonali nella misura in cui esse riguardano lo SWITCHaai Participant e il trattamento dei dati personali entro la SWITCHaai Federation. Inoltre si attiene alle clausole contrattuali standard UE (o interpretazioni più rigorose in determinate giurisdizioni) e si accerta dell'inclusione nei vari contratti dei paragrafi pertinenti il trasferimento dei dati personali.

A tal fine, lo SWITCHaai Participant adotta appropriate misure tecniche e organizzative a prevenzione del trattamento non autorizzato e illecito dei dati e dell'eliminazione o perdita accidentali di detti dati. Su tale aspetto, l'utente finale si attiene alle eventuali raccomandazioni di SWITCH.

Ogni AP Operator e ogni IdP Operator è tenuto a rispettare le indicazioni relative i *Legal Templates for SWITCHaai*[37] (standard legali SWITCHaai).

6.3.4 Responsabilità dell'utente finale

Tutti i dati registrati dall'utente finale, ad esempio nome, indirizzo e-mail, indirizzo postale, ecc., devono corrispondere a verità. A titolo di supporto, il servizio SWITCH edu-ID può inviare dei promemoria all'utente finale.

L'utente finale deve scegliere una password sicura e tutelarla in modo da prevenire accessi da parte di terzi al proprio SWITCH edu-ID Account.

All'utente finale è consentito possedere un solo SWITCH edu-ID Account. Eventuali duplicati creati per errore devono essere segnalati all'assistenza[38] che provvederà alla loro unione. L'utente finale deve rimediare a eventuali perdite di dati causate dall'unione degli Account, ad esempio per servizi utilizzati in precedenza.

L'utilizzo improprio o non autorizzato di un SWITCH edu-ID Account o del servizio SWITCH edu-ID o violazioni alle presenti condizioni di utilizzo possono portare al blocco o all'eliminazione delle SWITCH edu-ID Account in questione (si veda il capitolo 6.7).

6.3.5 Trattamento dei dati da parte del Servizio

A ogni accesso dell'utente finale a un determinato servizio, il SP può richiedere specifici dati sull'utente finale stesso. A tal fine è necessaria l'approvazione dell'utente affinché i suoi dati vengano trasmessi dall'IdP a uso del SP. Tale funzione di approvazione mostra all'utente finale i dati da trasmettere e lo aiuta a tutelare i propri dati personali.

I dati personali dell'utente finale, come nome, indirizzo e-mail o data di nascita, possono essere utilizzati e inoltrati dai SP esclusivamente per i seguenti scopi:

- per l'erogazione dei servizi offerti dagli SP
- ai fini dell'autenticazione e autorizzazione
- per contattare l'utente finale
- per rintracciare e rimuovere i duplicati e le Affiliations scadute

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

Ai servizi il cui processo di autenticazione si svolge attraverso SWITCH edu-ID possono applicarsi condizioni di utilizzo specifiche in materia di tutela dei dati.

6.3.6 Ispezioni

Il servizio SWITCH edu-ID viene controllato periodicamente nell'ambito di un processo ISMS[39], attraverso il quale vengono definite e aggiornate con regolarità le necessarie misure tecniche e organizzative per il funzionamento del servizio.

La SWITCHaai Federation Policy (si veda il capitolo 5) non prevede a priori alcuna ispezione dei SWITCHaai Participant (SWITCH inclusa). Tali ispezioni possono rendersi necessarie in determinate circostanze e vengono pertanto fatte salve.

6.4 Collaborazione con terzi in territorio nazionale o all'estero

Previo consenso delle organizzazioni e degli utenti finali partecipanti, i dati personali possono essere trasmessi a un SP (in Svizzera o all'estero) ai fini dell'autenticazione descritta al capitolo 3.2.3.5 e della relativa emissione di attributi.

Gli SWITCHaai Participant accettano che parte delle informazioni che registrano all'atto dell'inserimento delle proprie risorse nel Resource Registry sia resa accessibile ad altri partecipanti della SWITCHaai Federation sul web o nei Metadata come descrizione pubblicamente accessibile. Qualora tali informazioni siano corredate da condizioni di utilizzo, dichiarazioni di copyright o altre diciture di proprietà intellettuale, il fruitore di tali informazioni deve rispettare tali limitazioni o contattare SWITCH al fine di chiarirne l'utilizzo.

6.5 Accesso ai dati dei collaboratori

Laddove vengano trasmessi a SWITCH dei dati affinché vengano gestiti, può succedere che un'organizzazione/un partner commerciale necessiti di accedere per motivi operativi a dati registrati da un collaboratore non raggiungibile su incarico dell'organizzazione/del partner contrattuale.

L'organizzazione/il partner contrattuale deve comunque dimostrare in maniera chiara ed esaustiva di essere intitolata/o ad accedere ai rispettivi dati. Laddove non venga prodotta chiaramente tale prova o sussista un rischio di responsabilità non accettabile per SWITCH, quest'ultima ha il diritto a negare tale accesso.

6.6 Uso consentito del servizio

Qualsiasi uso del servizio è consentito purché esso non porti a violazioni delle presenti condizioni di utilizzo, dei diritti di soggetti terzi o di altre leggi vigenti.

6.7 Uso improprio del servizio

L'utilizzo illecito dei servizi è disciplinato dalle disposizioni del RdS e delle CG e loro rispettive eventuali modifiche.

[39] ISMS: Information Security Management System

Le organizzazioni di appartenenza degli utenti finali colpevoli di uso improprio possono essere ritenute responsabili in solido o insieme agli utenti finali di tutti gli eventuali danni subiti da SWITCH o da terzi a causa dell'utilizzo illecito del servizio da parte di detti utenti finali.

Su primo sollecito da parte di SWITCH, l'organizzazione di appartenenza degli utenti finali colpevoli di uso improprio è tenuta a proprie spese a contestare le richieste di risarcimento avanzate da terzi nei confronti di SWITCH in relazione all'utilizzo improprio del servizio. L'organizzazione di appartenenza degli utenti finali colpevoli di uso improprio deve assumersi in solido le spese legali o altrimenti sostenute da SWITCH, royalty e/o oneri di risarcimento danni, purché SWITCH abbia informato l'organizzazione in questione della richiesta di risarcimento avanzata e l'abbia autorizzata della gestione e risoluzione della controversia legale entro i limiti del diritto processuale applicabile, in particolare anche mediante accordo giudiziario o extragiudiziale.

In caso di fondato sospetto di utilizzo illecito o improprio del servizio, SWITCH si riserva il diritto di eliminare immediatamente gli Account in questione senza preavviso all'utente o organizzazioni coinvolti e/o di bloccare a titolo provvisorio o permanente gli utenti finali registrati coinvolti senza essere tenuta a risarcire gli utenti finali e le organizzazioni in questione.

Inoltre, al fine di garantire il corretto funzionamento del servizio e anche in assenza di un sospetto di uso improprio, SWITCH può richiedere in qualsiasi momento agli utenti finali registrati di reimpostare la propria password o di ripetere il processo di autenticazione.

Gli utenti finali e le organizzazioni sono tenute a supportare SWITCH per la risoluzione dei casi di uso improprio, reati e altri danni.

Inoltre SWITCH si riserva in tutti in casi in cui la legge lo preveda o sia ritenuto opportuno ai fini legali il diritto di collaborare con le autorità statali competenti e di trasmettere loro in tale contesto tutte le informazioni necessarie alla persecuzione delle violazioni di legge.

6.8 Garanzia

La garanzia è disciplinata dalle disposizioni del RdS e delle CG e loro rispettive eventuali modifiche in concomitanza con la disponibilità garantita nel capitolo 3.3.

SWITCH non si assume alcuna responsabilità in merito ad alcun esito specifico in relazione a un servizio nel caso di organizzazioni il cui processo di autenticazione viene svolto mediante il servizio SWITCH edu-ID.

6.9 Responsabilità

6.9.1 Responsabilità di SWITCH

La responsabilità di SWITCH nei confronti delle organizzazioni della SWITCH Community è definita in base alle disposizioni del RdS e delle sue eventuali successive modifiche. SWITCH non si assume alcuna responsabilità relativamente all'utilizzo corretto del servizio.

La responsabilità di SWITCH nei confronti delle organizzazioni della Extended SWITCH Community è definita in base alle disposizioni delle CG e delle loro eventuali successive modifiche.

È esclusa ogni responsabilità di SWITCH nei confronti degli utenti finali e di soggetti terzi che utilizzano i servizi di SWITCH senza un contratto proprio stipulato con quest'ultima ma con l'autorizzazione dell'organizzazione. In particolare, SWITCH non si assume alcuna responsabilità per eventuali violazioni in materia di protezione dei dati perpetrate dalle organizzazioni o dai fornitori dei servizi la cui autenticazione si effettua mediante il servizio SWITCH edu-ID.

6.9.2 Responsabilità delle organizzazioni

Le organizzazioni sono responsabili in solido entro i limiti di legge nei confronti di SWITCH per eventuali danni subiti da quest'ultima causati dall'uso non autorizzato del servizio e per altri danni indiretti. Tale responsabilità permane anche nel caso in cui gli SWITCHaai Account o SWITCH edu-ID Account coinvolti siano già stati eventualmente eliminati.

La responsabilità comprende in particolare gli Account tecnici e Account di prova di SWITCH edu-ID; si veda il paragrafo 5.1.3.7.

6.9.3 Responsabilità dell'utente finale

L'utente finale è responsabile di tutte le attività svoltesi in relazione al proprio SWITCH edu-ID Account e può per tanto essere ritenuto responsabile a tal fine dagli AP Operator, IdP Operator, SP Operator o SWITCH.

L'utente finale è responsabile entro i limiti di legge nei confronti di SWITCH per eventuali danni subiti da quest'ultima causati dall'uso non autorizzato del proprio SWITCHaai Account o SWITCH edu-ID e per altri danni indiretti. Tale responsabilità permane anche nel caso in cui lo SWITCHaai Account o SWITCH edu-ID Account sia già stato eventualmente eliminato.

In caso di uso improprio della propria identità digitale, l'utente finale non può far valere alcuna richiesta di risarcimento nei confronti degli AP Operator, IdP Operator, SP Operator o SWITCH.

6.10 Diritto applicabile e foro competente

L'utilizzo delle SWITCH edu-ID Account è disciplinato dalla legge svizzera.

Il diritto applicabile e il foro competente sono definiti nelle disposizioni del RdS e delle CG e loro rispettive eventuali modifiche.

6.11 Versioni linguistiche

La presente descrizione del servizio è redatta in lingua tedesca, francese, italiana e inglese. Tutte le versioni linguistiche sono equivalenti.

6.12 Revisioni

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