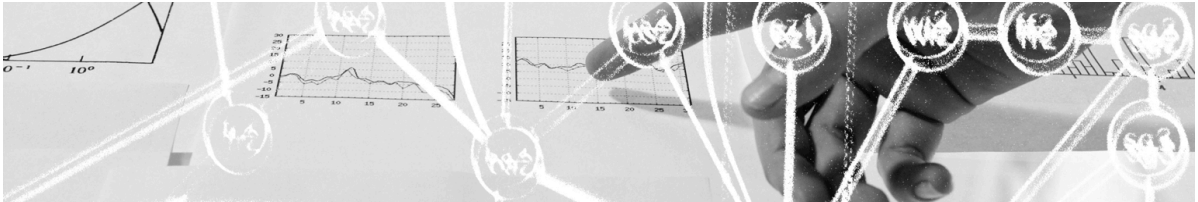


# Swiss edu-ID Unique Identifier

## Specification



**Rolf Brugger (SWITCH), Lars Händler (ETH-Bibliothek Zürich), Gerhard Hassenstein (Berner Fachhochschule), Thomas Selzam (Berner Fachhochschule)**

<b>Document Type:</b>	Specification
<b>Version:</b>	V1.1
<b>Created:</b>	10.07.14
<b>Last changes:</b>	19.08.14
<b>Classification:</b>	Public

## Content

1	Context and Scope of this Document	3
2	Usage	3
3	Issuing	3
4	Requirements	3
4.1	Boundary Conditions	3
5	Specification	5
5.1	Format	5
5.2	Generation	5
5.2.1	SwissEduIDs for persons	5
5.2.2	SwissEduID Test Range	5
6	Appendix: Examples of existing Identifiers	7

## 1 Context and Scope of this Document

The Swiss edu-ID is an extension of the identity management solution SWICHaaI. With Swiss edu-ID students, alumni, researchers and other individuals who get in contact with Swiss higher education organizations are getting a permanent digital identification. The identification gives its users unique access to resources provided by Swiss higher education organizations and their partners.

The purpose of this document is to specify the inner structure of the Swiss edu-ID unique identifier (swissEduID) and its generation.

We do not describe business processes of any organization here.

## 2 Usage

The swissEduID uniquely identifies a person within the Swiss edu-ID framework. Its goal is to provide a way to link personal data of different services and applications, and to assign it to a person.

The Swiss edu-ID has two main goals:

1. Link personal data over a long period of time (e.g. decades) between services/applications and across institutional boundaries. To achieve this goal, the swissEduID is used.
2. Authenticate users and issue personal data for services and applications provided by institutions of the SWITCH community and their partners. To achieve this goal, the swissEduID is *not* used.

## 3 Issuing

A swissEduID is issued when a person requests it. The creation of a Swiss edu-ID Account together with the associated swissEduID can be initiated

- by self-registration and filling-in a form on a web site, or
- by deriving a Swiss edu-ID account from an active digital identity like AAI.

For the time being it is planned to generate and issue the swissEduID by a single, central organization. In the future, however, it could be necessary to issue swissEduIDs at multiple, loosely connected organizations.

Automated or batch generation of Swiss edu-ID accounts is currently not planned. Yet, the design of the swissEduID should still allow for automated processing.

## 4 Requirements

### 4.1 Boundary Conditions

- The swissEduID will be used over a period of multiple decades.
- The Swiss edu-ID can basically be requested by any entity involved – be it persons, organizations or service providers. However, it will be designed to comply with the requirements of universities and their members (the SWITCH community). In terms of users these are primarily persons, who get in contact with a Swiss higher education organization. The estimated

number of new users per year is about 40'000<sup>1</sup>. The total number of students in 2013 is about 229'461, the number of staff is 45'000.

- The swissEduID is used to link personal data across applications, services and organizations. To protect the privacy of users, only federation partners like Swiss universities (and other trustworthy organizations) get access to the swissEduID, may store it and use it to link with data of other organizations. The usage of the swissEduID is subject to regulations.
- Whenever possible, standards or widely used existing specifications should be used.

Requirement	Rating <sup>2</sup>	Comment
Low setup and operation costs.	K	
The swissEduID is uniquely assigned to one person. It is never issued more than once.	K	
The swissEduID is visible to its owner.	N	
The swissEduID is human readable	N	Only necessary in exceptional cases.
The swissEduID is machine readable. The swissEduID is printed e.g. on a student card. The series of digits or the QR-code is optically readable.	N	Machine-readable student cards should use their own identifiers, which are linked to the swissEduID.
The swissEduID is independent of personal features.	K	
Protection against guessing or enumeration to find valid swissEduIDs (brute-force attack)	I	Attributes must be protected even if the swissEduID of a person is known or has been leaked.
The swissEduID can be manually processed: e.g. typed-in in an online form, sent by email or spelled by phone. Students who register at a university might be asked for their swissEduID. In a transitional period an automated transfer process might be missing and the swissEduID would have to be handed over manually.	N	Manually handing over stating the swissEduID should be limited to exceptional cases like recovery processes, software debugging etc.
The swissEduID should be interchangeable for a person. Example: a person requests a new swissEduID to interrupt traceability.	N	Processes and policies to re-issue a swissEduID are to be defined.
The swissEduID should contain a checksum or parity to check its consistency and prevent from small typing or transmission errors.	I	
The swissEduID can be issued decentralized. Multiple authorities are entitled to issue	I	Central issuing is planned. However, the design of the swissEduID should

<sup>1</sup> Basis: about 40'000 bachelor and master graduates per year at universities and universities of applied science. (BFS 2012: <http://www.bfs.admin.ch/bfs/portal/de/index/themen/15/01/key/blank/03.html>)

<sup>2</sup> K: killer criterion, I: important, N: nice-to-have

swissEduID, and measures must be taken to avoid collisions.		allow for future decentral issuing.
---	--	-------------------------------------

## 5 Specification

### 5.1 Format

The swissEduID is a 128-bit number, represented as 32-digit, hexadecimal encoded number including leading zeroes and with four separators.

Examples:

- 6c17b073-3e37-4c4a-83c8-be85ee353d23
- f5b0c371-115c-4a84-ac8f-2cfe24b1aff5
- 4c09e224-8fb3-4984-ba72-75dba7d98e03

Remarks:

- The swissEduID is represented according to the UUID Standard RFC 4122<sup>3</sup>
- The swissEduID does not have a checksum<sup>4</sup>

### 5.2 Generation

#### 5.2.1 SwissEduIDs for persons

A swissEduID issued to a real person is a

1. UUID version 4 according to RFC 4122 (<http://tools.ietf.org/html/rfc4122>)
2. Not all of the first 16 bits (the first 4 hex digits) are 0

Examples:

- 6c17b073-3e37-4c4a-83c8-be85ee353d23
- f5b0c371-115c-4a84-ac8f-2cfe24b1aff5

#### 5.2.2 SwissEduID Test Range

swissEduIDs that have the value 0 in the 16 leading bits (in the first 4 hex digits) are reserved for examples, developments, tests, debugging etc.

Examples:

- 0000b073-3e37-4c4a-83c8-be85ee353d23
- 0000c371-115c-4a84-ac8f-2cfe24b1aff5

<sup>3</sup> <http://tools.ietf.org/html/rfc4122>

<sup>4</sup> UUID are usually encoded as hexadecimal text digits, but other encodings are occasionally used as well (base64, Ascii85, binary). None of these encoding standards includes a checksum. The only base64-encoding specification that includes a checksum is the 'Radix-64' encoding for OpenPGP, which is considered too exotic to be used here.



## 6 Appendix: Examples of Other Existing Identifiers

ID	Example
AHVN13	756.0271.4792.62 (3-digit country code, 9-digit number, 1 digit checksum)
ORCID	<a href="http://orcid.org/0000-0002-1825-0097">http://orcid.org/0000-0002-1825-0097</a> (ISO 27729 compatible)
ISNI	0000 0001 2096 4892 (ISO 27729; last digit is checksum)
VIAF ID	79167493
Google+ user ID	108174485180354048197
Twitter ID	15156194
CH identity card	IDCHEC6947312
CH drivers license	FACHE007416589002
eduid.se	(ID not disclosed to its owner)
AAI UUID	550e8400-e29b-41d4-a716-446655440000
AAI swissEduPersonUniqueID	550e8400-e29b-41d4-a716-446655440000@uzh.ch