SWITCH
Serving Swiss Universities

AAI - Authentication and Authorization Infrastructure

Attribute Specification

7 November 2012

Version 1.4.2 / final

Table of Contents

1. Introduction

The AAI Attribute Specification is crucial for the data exchange within the SWITCHaai federation. It provides the common basis on which two communicating entities are able to share information they know to interpret identically.

This document standardizes the attributes among all organizations participating in SWITCHaai. The format of the attribute definition is close to the LDAP syntax (see chapter 3: “Attribute definitions” for further details). A schema for LDAP servers [LDAP-schema] is available.

This specification started with a basic set of attributes and is based on work of [Internet2] for the [eduPerson] specification. The set of attributes is adapted depending on requirements of consumers (the resources) and the ability of the home organizations to supply them.

Data exchange beyond the SWITCHaai federation is not within the scope of this document. For further information about that topic, see ➟ **http://www.switch.ch/aai/interfederation/** [Interfederation].

1.1. Privacy and data protection

The home organization administrator's and resource owner's first and foremost duty regarding attributes is *privacy and data protection*.

Users perceive many of the attributes specified in this document as *very sensitive information*. The persons responsible for the systems that process attributes must fully respect user privacy and the relevant data protection laws and regulations which define how to deal with personal data.

1.2. Security

Revealing attribute values can be a *security risk*.

A good example to demonstrate that aspect is the unique identifier "uid". It could provide valuable information to a malicious third party. Its intended semantics is to be a user's identifier for authentication (aka login), possibly also on the home organization. It is thus security sensitive and home organization administrators should ponder carefully the decision to release the uid attribute to any resource, even within their organization. Conversely, resource administrators should not require the uid attribute unless they have a bilateral agreement with the home organization administrators. Note that Shibboleth is designed to transfer information *about* authentication but not the credentials themselves.

2. Implementing the Attribute Specification

2.1. Responsibilities of Home Organizations

The information to be made available through attributes gets collected and maintained by the home organization. It is stored in a user directory, which can either be implemented using an LDAP compatible directory (e.g. OpenLDAP or Active Directory) or an SQL database.

The home organization is responsible for *proper identity management* and *up-to-date personal data*. In addition, it is also responsible for proper configuration of the Shibboleth attribute filter policy defining which attributes may be released to which resources in order to protect the privacy of its users.

Note

As mentioned in the "Best Current Practices" [AAI-BCP-IdP] document, each home organization participating in SWITCHaai has to implement the attributes as defined on the SWITCHaai website [Attr-Impl] on ➟ **http://www.switch.ch/aai/attributes/**. At least the attributes referred to as «core attributes» have to be implemented.

2.2. Responsibilities of Resource owners

The set of attributes needed by a resource depends on the service it offers to its users. The set may be minimal for anonymous services and rather large for highly personalized services with granular authorization. Keep in mind: according to the data protection principles, as few as possible personal data should be processed!

In addition, a resource owner should carefully consider which information to store across user sessions. The fewer information is stored, the smaller impact a potential misuse has in case of an incident.

So it is the duty of the resource owner to specify which attributes are really required to offer the service and which additional optional attributes might allow him/her to offer optional advanced services.

When defining their attribute requirements, resource owners should always check the attribute implementation status as defined on the SWITCHaai website [Attr-Impl]. If a resource requires an attribute not (yet) implemented in the home organization of its prospective users, these users will not be able to access the resource.

Note

Resource owners have to maintain the attribute requirements of their resource in the AAI Resource Registry [AAI-RR] provided by SWITCH on ➟ **https://rr.aai.switch.ch**.

2.2.1. An example for attribute requirements

A resource offers personalized access for biology students to an on-line database. Therefore, the user needs to be identified in order to allow the storage of personal search preferences.

Core Attributes

- eduPersonTargetedID to identify each user individually,
- eduPersonAffiliation to distinguish students from other AAI users,
- swissEduPersonStudyBranch3 to identify the biology students.

Other Attributes

- mobile to be able to offer an optional service for SMS notification of content changes.

3. Attribute definitions

For all attributes, the following metadata is defined:

Name	The name of the attribute
Description	A short description of the attribute
Permissible values	A list of permissible value (Where possible, the list of values is based on international or national standards.)
Typical usage	**authorization** Typically, a resource uses this attribute to make the access control decision **accounting** This attribute is used for accounting reasons **additional user information** Information which is typically not used for authorization or accounting, but may be used to offer a better service to the user (e.g. given name, surname used within a personalized portals).
References	Reference to a standard the attribute is based on (where available)
OID	Object Identifier
LDAP Syntax	The LDAP syntax of an attribute, see [RFC4517], "Directory String" and "Postal Address" are the most often used syntaxes, they both use UTF-8 encoding.
# of values	single or multi
Example values	Example values in the LDIF format, see [RFC2849]

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3.1. Unique ID

Name	swissEduPersonUniqueID
Description	A unique identifier for a person, mainly for inter-institutional user identification on personalized services
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[RFC2822]
OID	`2.16.756.1.2.5.1.1.1`
LDAP Syntax	Directory String
# of values	single

Example values	`845938727494@ethz.ch`
	`e2d8e08-248b-11dc-8314-0800200c9a66@uzh.ch`

Semantics

<unique-local-ID>@<Internet-domain>
The format used is derived from the e-mail address format.

<Internet-domain> (domain part)
It is equivalent to the registered Internet domain the home organization uses, i.e. the same value as the content of the attribute `swissEduPersonHomeOrganization`.

<unique-local-ID> (local part)
It is an ID uniquely allocated by the home organization for a user they correctly authenticated according to the local authentication policy.

It has to be unique. It MUST NOT be reassigned, also if the former user left the home organization.

Unlike the 'matriculation number' or the former 'AHV-Nummer', it should not carry semantics. However, a home organization has to be able to identify the person matching that <unique-local-ID>.

The local part can contain any characters which can be part of the local part of an e-mail address according to [RFC2822], namely: `- .` _%.

Notes

- One SHOULD NOT expose the Unique ID to end users; especially one SHOULD NOT require a user to provide his Unique ID manually!
- The <unique-local-ID> MAY be a hash value based on information about the user.
- The minimum length of the local part SHOULD be 6 and the maximum length of the whole value SHOULD be 255 characters.

3.2. Targeted ID

Name	eduPersonTargetedID
Description	A persistent, non-reassigned, opaque identifier for a principal. eduPersonTargetedID is an abstracted version of the SAML V2.0 Name Identifier format of "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent". In SAML, this is an XML construct consisting of a string value inside a <saml:NameID> element along with a number of XML attributes, of most significance NameQualifier and SPNameQualifier, which identify the source and intended audience of the value. It is left to specific profiles to define alternate syntaxes, if any, to the standard XML representation used in SAML. In abstract terms, an eduPersonTargetedID value is a tuple consisting of an opaque identifier for the principal, a name for the source of the identifier, and a name for the intended audience of the identifier. The source of the identifier is termed an identity provider and the name of the source takes the form of a SAML V2.0 entityID, which is an absolute URI. The name of the intended audience also takes the form of an absolute URI, and may refer to a single service provider or a collection of service providers.
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[eduPerson], [SAML-overview], [SAML-core], [SAML-Attr-Profiles]
OID	`1.3.6.1.4.1.5923.1.1.1.10`
LDAP Syntax	Directory String
# of values	multi

Example values	`https://aai-logon.switch.ch/idp/shibboleth!`
	`https://aai-viewer.switch.ch/shibboleth!`
	`a6c2c4d4-08b9-4ca7-8ff9-43d83e6e1d35`

Semantics

Service providers or directory-enabled applications with the need to maintain a persistent but opaque identifier for a given user for purposes of personalization or record-keeping.

Identity or service providers or directory-enabled applications with the need to link an external account to an internal account maintained within their own system. This attribute is often used to represent a long-term account linking relationship between an identity provider and service provider(s) (or other identity/attribute provider).

Notes

This attribute may or may not be stored in a typical Directory Service because of its potential variance by relying party, but it is defined here for use in other service contexts such as Security Assertion Markup Language (SAML) assertions. It is typically used in federated scenarios in which more typical opaque identifiers lack appropriate uniqueness guarantees across multiple identity providers.

In SAML, a service provider is an abstract designation and may or may not refer to a single application or physical system. As a result, and because service providers may be grouped arbitrarily into "Affiliations" for policy purposes, the intended audience of an eduPersonTargetedID may be (and often is) limited to a single "target" application, or may consist of a large number of related applications. This is at the discretion of the identity provider. The value of the principal identifier SHOULD be different for different "audience" values, but this is also at the discretion of the identity provider.

Per the SAML format definition, the identifier portion MUST NOT exceed 256 characters, and the source and audience URI values MUST NOT exceed 1024 characters.

Persistence

As defined by SAML, eduPersonTargetedID values are not required to have a specific lifetime, but the association SHOULD be maintained longer than a single user interaction and long enough to be useful as a key for consuming services. Protocols might also be used to refresh (or "roll-over") an identifier by communicating such changes to service providers to avoid a loss of service. (SAML V2.0 includes one such example.) This may be needed in the event that the association between the principal and the identifier becomes public, if privacy requirements are involved.

Privacy

This attribute is designed in part to aid in the preservation of user privacy. It is therefore REQUIRED to be opaque, having no particular relationship to the principal's other identifiers, such as a local username. It MAY be a pseudorandom value generated and stored by the identity provider, or MAY be derived from some function over the audience's identity and other principal-specific input(s), such as a serial number or UUID assigned by the identity provider.

This attribute is also designed to inhibit, when appropriate, the ability of multiple unrelated services to correlate user activity by comparing values. This is achieved when desired by varying the identifier based on the intended audience.

In other words, there is no guarantee of non-correlation, but there is an assumption of non-correlation from the relying party's perspective outside of explicitly arranged "Affiliations" of relying parties and cooperating identity providers prepared to recognize them.

Uniqueness

A value of this attribute is intended only for consumption by a specific audience of services (often a single one). Values of this attribute therefore MUST be unique within the namespace of the identity provider and the namespace of the service provider(s) for whom the value is created. The value is "qualified" by these two namespaces and need not be unique outside them; the uniqueness of the identifier therefore depends on all three pieces of information.

Reassignment

A distinguishing feature of this attribute is that it prohibits re-assignment. Since the values are opaque, there is no meaning attached to any particular value beyond its identification of the principal. Therefore particular values created by an identity provider MUST NOT be re-assigned such that the same value given to a particular service provider refers to two different principals at different points in time.

3.3. User ID

Name	uid
Description	A unique identifier for a person, mainly used for user identification within the user's home organization
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[RFC4519], [eduPerson]
OID	`0.9.2342.19200300.100.1.1`
LDAP Syntax	Directory String
# of values	single (multi in [RFC4519], see notes)
Example values	`pmuster` `stud_05999123`

Semantics

The User ID attribute type specifies a computer system login name. `uid` is the short name for User Identifier. It should not be confused with the Unix uid (a user's unique numerical ID) nor with the ‘Unique ID’ (`swissEduPersonUniqueID`). Unlike the ‘Unique ID’, the `uid` is well known by the user, may carry visible semantics and may be presented to the user. It may be reassigned, if the former user left the home organization.

Notes

- `uid`, contrary to common belief, is multi-valued. Within SWITCHaai, home organizations MUST provide a *single value only*: the value most convenient for the user (e.g. well known or most meaningful).

- `uid` is case insensitive; provisioning this attribute with case sensitive values that otherwise fit the intended semantics might cause unexpected results (e.g. non-uniqueness within an organization).

- `uid` is security sensitive since it is used for authentication (login) at the home organization. This attribute SHOULD NOT be provided to resources outside the issuing home organization. It is mostly anyhow not unique across organizations.

3.4. Surname

Name	surname
Description	Surname or family name
Vocabulary	not applicable, no controlled vocabulary
Usage	additional user information
References	[RFC4519], [eduPerson]
OID	`2.5.4.4`
LDAP Syntax	Directory String
# of values	single (multi in [RFC4519], see notes)

Example values	`Meier-Müller`
	`Bauchière`
	`von Roten`

Semantics

This is the X.500 surname attribute, which contains the family name of a person. The [eduPerson] specification says: If the person has a multi-part surname (whether hyphenated or not), store the multi-part name as one value and each component as separate values in this multi-valued attribute. That yields the best results for the broadest range of clients doing name searches.

Notes

– Within SWITCHaai, home organizations MUST provide a *single value only*: the surname which is used for official communication with that person.

3.5. Given name

Name	givenName
Description	Given name of a person
Vocabulary	not applicable, no controlled vocabulary
Usage	additional user information
References	[RFC4519], [eduPerson]
OID	`2.5.4.42`
LDAP Syntax	Directory String
# of values	single (multi in [RFC4519], see notes)

Example values	`Hans-Peter`
	`Hans Jürg`
	`René`

Semantics

The givenName attribute is used to hold the part of a person's name which is not their surname. The [eduPerson] specification says: If the person has a multi-part given name (whether hyphenated or not), store the multi-part name as one value and each component as separate values in this multi-valued attribute. That yields the best results for the broadest range of clients doing name searches.

Notes

- Within SWITCHaai, home organizations MUST provide a *single value only*: the given name which is used for official communication with that person.

3.6. Principal name

Name	eduPersonPrincipalName
Description	A scoped identifier for a person. It should be represented in the form "user@scope" where 'user' is a name-based identifier for the person and where 'scope' defines a local security domain. Each value of 'scope' defines a namespace within which the assigned identifiers MUST be unique. Given this rule, if two eduPersonPrincipalName (ePPN) values are the same at a given point in time, they refer to the same person.
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.6`
LDAP Syntax	Directory String
# of values	single
Example values	`hputter@hsww.wiz`

Semantics

Each institution decides the criteria for membership in each affiliation classification.

A reasonable person should find the listed relationships commonsensical.

Notes

- For SWITCHaai, this attribute SHOULD NOT be used. Use `eduPersonTargetedID` or `swissEduPersonUniqueID` instead.

Syntactically, ePPN looks like an email address but is not intended to be a person's published email address or be used as an email address. In general, name-based identifiers tend to be subject to some degree of expected change and/or reassignment.

Values of eduPersonPrincipalName are often, but not required to be, human-friendly, and may change as a result of various business processes. They may also be reassigned after a locally-defined period of dormancy. Applications that require a guarantee of non-reassignment and more stability, but can tolerate values unfriendly (and unknown) to humans should refer to the eduPersonTargetedID attribute.

3.7. Matriculation number

Name	swissEduPersonMatriculationNumber
Description	Matriculation number of a student
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[SIUS-SHIS]
OID	`2.16.756.1.2.5.1.1.11`
LDAP Syntax	Numeric String {8}
# of values	single

Example values	`04911506`
	`72836596`

Semantics

The matriculation number is a unique number assigned to each student when he/she matriculates the first time to a Swiss University or University of Applied Sciences. It is defined by the [SIUS-SHIS]. The number has eight digits. The first two digits represent the year of the first matriculation. The next five digits are number blocks reserved for each of the universities. The last digit is a check digit.

3.8. Employee number

Name	employeeNumber
Description	Identifies an employee within an organization
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[RFC2798]
OID	`2.16.840.1.113730.3.1.3`
LDAP Syntax	Directory String
# of values	single

Example values	`400345`
	`74622225`

Semantics

Numeric or alphanumeric identifier assigned to a person, typically based on order of hire or association with an organization. The use case for this attribute is internal to the issuing home organization, mainly for internal administrative purposes. It MUST to be unique within the issuing home organization but will not be unique across organizations.

Notes

– `employeeNumber` is security sensitive since it might be used for authentication at the home organization. This attribute SHOULD NOT be provided to resources outside the issuing home organization.

3.9. Card UID

Name	swissEduPersonCardUID
Description	Card unique identifier
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[ISO15963]
OID	`2.16.756.1.2.5.1.1.12`
LDAP Syntax	Directory String
# of values	single

Example values	`E002219C5298303B@ISO15693`
	`0298450109348@unil.ch`

Semantics

The value of the attribute is composed of the card identifier followed by a seperator (the '@' sign) and an identifier for the type of card ID which is used.

For RFID Cards with the UID format defined in the ISO standard ISO 15693, the identifier for the card type is "ISO15963". The value is formatted as specified in the ISO 15963 standard, a 64-bit unique identifier with the most significant bytes first. The value is represented as a hexadecimal string.

For card identifiers which are not defined in a widely accepted standard, the identifier for the type can be set to the domain name of the home institution who generated the number (local identifier).

3.10. Nick name

Name	eduPersonNickname
Description	Person's nickname, or the informal name by which they are accustomed to be hailed.
Vocabulary	not applicable, no controlled vocabulary
Usage	additional user information
References	[RFC4512], [eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.2`
LDAP Syntax	Directory String
# of values	multi
Example values	`Spike`

Notes

Most often a single name as opposed to displayName which often consists of a full name. Useful for user-friendly search by name. As distinct from the cn (common name) attribute, the eduPersonNickname attribute is intended primarily to carry the person's preferred nickname(s). E.g., Jack for John, Woody for Durwood, JR for Joseph Robert.

Carrying this in a separate attribute makes it relatively easy to make this a self-maintained attribute. If it were merely one of the multiple values of the cn attribute, this would be harder to do. A review step by a responsible adult is advisable to help avoid institutionally embarrasing values being assigned to this attribute by would-be malefactors!

Application developers can use this attribute to make directory search functions more "user friendly."

3.11. Date of birth

Name	swissEduPersonDateOfBirth
Description	The date of birth of the person
Vocabulary	`date-mday` MUST be within the proper range depending on the values of `date-month` and `date-fullyear`
Usage	additional user information
References	[RFC3339]
OID	`2.16.756.1.2.5.1.1.2`
LDAP Syntax	Numeric String {8}
# of values	single

Example values	`19871022`
	`20021010`

Semantics

Based on [RFC3339] 'Date and Time on the Internet: Timestamps'. Using the 'full-date' format from paragraph 5.6:

```
full-date      = date-fullyear date-month date-mday
date-fullyear  = 4DIGIT
date-month     = 2DIGIT ; 01-12
date-mday      = 2DIGIT ; 01-28, 01-29, 01-30, 01-31 based on month
```

3.12. Gender

Name	swissEduPersonGender
Description	The state of being male or female
Vocabulary	The following codes are used (see [ISO5218]): `0` Not known, `1` Male, `2` Female, `9` Not specified
Usage	additional user information
References	[ISO5218]
OID	`2.16.756.1.2.5.1.1.3`
LDAP Syntax	Integer {1}
# of values	single

Example values	`1`
	`9`

3.13. Preferred language

Name	preferredLanguage
Description	Preferred language of a user

Vocabulary	The syntax and registry of language tags is the same as that defined by [RFC 4646]. In summary, a language tag is composed of 1 or more parts: A primary language tag and a possibly empty region subtags:
	`language-tag = language *( "-" region )`
	`language = 2ALPHA`
	`region = 2ALPHA`
	Whitespace is NOT allowed within the tag and all tags are case-insensitive. The name space of language tags is administered by the [IANA]. Example tags are: `en`, `en-us`, `de`, `de-ch` where any two-letter `language` is an ISO 639 language abbreviation and any two-letter `region` is an ISO 3166 country code.

Usage	additional user information
References	[RFC2798]
OID	`2.16.840.1.113730.3.1.39`
LDAP Syntax	Integer {1}
# of values	single

Example values	`en`
	`de-ch`
	`it`
	`fr-ch`

3.14. E-mail address

Name	mail
Description	Preferred address for the "To:" field of e-mail to be sent to this person
Vocabulary	not applicable, no controlled vocabulary
Usage	not applicable, no controlled vocabulary
References	[RFC2821]
OID	`0.9.2342.19200300.100.1.3`
LDAP Syntax	IA5 String {256}
# of values	multi
Example values	`peter.meier@uzh.ch` `dumbledore@hsww.wiz`

Semantics

The 'mail' (rfc822mailbox) attribute type holds Internet mail addresses in Mailbox [RFC2821] form.

```
Mailbox = Local-part "@" Domain
```

Notes

- For SWITCHaai, the correctness of this attribute can *not* be guaranteed by the home organization since mailboxes may be changed by the user without informing the home organization (private mailboxes). If a person has more than one e-mail address, it is *recommended* to provide a single address only (the address used by the home organization itself when sending e-mails to that person).

3.15. Home postal address

Name	homePostalAddress
Description	Home address of the user
Vocabulary	not applicable, no controlled vocabulary
Usage	additional user information
References	[RFC4524]
OID	`0.9.2342.19200300.100.1.39`
LDAP Syntax	Postal Address
# of values	multi

Example values	`Bernerstrasse 45$CH-8048 Zürich`
	`ch. des Vignes 59$CH-1260 Nyon`

Semantics

The 'homePostalAddress' attribute specifies home postal addresses for an object. Each value should be limited to up to 6 directory strings of 30 characters each.

Notes

- Within SWITCHaai, the limitation to up to 6 lines of 30 characters is *not* relevant.

3.16. Business postal address

Name	postalAddress
Description	Campus or office address
Vocabulary	not applicable, no controlled vocabulary
Usage	additional user information
References	[RFC4519]
OID	`2.5.4.16`
LDAP Syntax	Postal Address
# of values	multi

Example values	`ETH Zentrum$CH-8092 Zürich`
	`Quartier UNIL-Sorge$Bâtiment Amphimax$CH-1015 Lausanne`

Semantics

The 'postalAddress' attribute type contains addresses used by a postal service to perform services for the object.

Notes

– Within SWITCHaai, the limitation to up to 6 lines of 30 characters is *not* relevant.

3.17. Private phone number

Name	homePhone
Description	Private phone number
Vocabulary	not applicable, no controlled vocabulary
Usage	additional user information
References	[RFC4524]
OID	`0.9.2342.19200300.100.1.20`
LDAP Syntax	Telephone Number
# of values	multi

Example values	`+41 44 345 6789`
	`+44 71 123 4567`

Semantics

Private phone number of the user. Attribute values should follow the agreed format for international telephone numbers as specified in [E.123].

3.18. Business phone number

Name	telephoneNumber
Description	Office/campus phone number
Vocabulary	not applicable, no controlled vocabulary
Usage	additional user information
References	[RFC4519]
OID	`2.5.4.20`
LDAP Syntax	Telephone Number
# of values	multi

Example values	`+41 44 345 6789`
	`+44 71 123 4567`

Semantics

Office/campus phone number of the user. Attribute values should follow the agreed format for international telephone numbers as specified in [E.123].

3.19. Mobile phone number

Name	mobile
Description	Mobile phone number
Vocabulary	not applicable, no controlled vocabulary
Usage	additional user information
References	[RFC4524]
OID	`0.9.2342.19200300.100.1.41`
LDAP Syntax	Telephone Number
# of values	multi

Example values	`+41 79 345 6789`
	`+44 71 123 4567`

Semantics

The 'mobile' attribute type specifies a mobile telephone number associated with a person. Attribute values should follow the agreed format for international telephone numbers as specified in [E.123].

Notes

– This attribute may be useful if a resource has the ability to send SMS (short message service).

3.20. Home organization

Name	swissEduPersonHomeOrganization
Description	Domain name of a home organization
Vocabulary	SWITCH maintains a register of organizations participating in SWITCHaai with their domain names and `swissEduPersonHomeOrganizationType`.
Usage	authorization, accounting
References	none
OID	`2.16.756.1.2.5.1.1.4`
LDAP Syntax	Directory String
# of values	single

Example values	`unil.ch`
	`ethz.ch`
	`library.ethz.ch`

3.21. Home organization type

Name	swissEduPersonHomeOrganizationType
Description	Type of a home organization
Vocabulary	`university`, `uas`, `hospital`, `library`, `tertiaryb`, `uppersecondary`, `vho`, `others`
Usage	authorization
References	[Swiss_ENIC]
OID	`2.16.756.1.2.5.1.1.5`
LDAP Syntax	Directory String
# of values	single

Example values	`university`
	`vho`
	`hospital`

Notes

- tertiaryb = professional education and training (PET) college (Höhere Fachschule, école supérieure), which is an institution on the tertiary B level [SER-edu]

- university = university or federal institute of technology recognized by Swiss ENIC [Swiss_ENIC]

- uas = university of applied sciences or university of teacher education recognized by Swiss ENIC [Swiss_ENIC]

- uppersecondary = institution on the upper secondary level: baccalaureate school, upper secondary specialized school, vocational education and training (VET) (apprenticeship)

- vho = virtual home organization

- others = institution for which none of the other values match

3.22. Affiliation

Name	eduPersonAffiliation
Description	Type of affiliation
Vocabulary	`faculty`, `student`, `staff`, `alum`, `member`, `affiliate`, ~~`employee`~~, `library-walk-in`
Usage	authorization
References	[eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.1`
LDAP Syntax	Directory String
# of values	multi
Example values	`student` `affiliate`

Semantics

Specifies the user's relationship(s) to the home organization in broad categories such as student, faculty, employee, etc. (see controlled vocabulary).

The eduPerson specification (201203) says: The list of allowed values in the current version of the object class is certainly incomplete, especially in terms of local institutional use. The editors felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included in later versions of eduPerson.

We also deliberately avoided including a value such as "other" or "misc" because it would be semantically equivalent to "none of the above." To indicate "none of the above," for a specific person, *leave the attribute empty*.

`member` is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., they are given institutional calendar privileges, library privileges and/or vpn accounts). It could be glossed as "member in good standing of the university community." The `member` affiliation MUST be asserted for people carrying one or more of the following affiliations: faculty or staff or student or employee.

`affiliate` for eduPersonAffiliation indicates that the holder has some definable affiliation to the university not captured by any of faculty, staff, student, employee, alum and/or member. Typical examples might include event volunteers, parents of students, guests and external auditors. There are likely to be widely varying definitions of `affiliate` across institutions. Given that, `affiliate` is of dubious value in federated, inter-institutional use cases.

`Library-walk-in`: This term was created to cover the case where physical presence in a library facility grants someone access to electronic resources typically licensed for faculty, staff and students. In recent years the library walk-in provision has been extended to cover other cases such as library users on the campus network, or those using on-campus workstations. Licensed resource providers have often been willing to interpret their contracts with licensees to accept this broader definition of `library-walk-in`, though specific terms may vary. For a more direct way of using eduPerson attributes to express library privilege information, see [commonlibterms] ➟ **http://www.switch.ch/aai/common-lib-terms** [commonlibterms].

Notes

- For SWITCHaai, the value `employee` MUST NOT be used. Use `staff` instead.

- There are significant differences in practice between identity providers in the way they define faculty, staff and employee and the logical relationships between the three. In particular there are conflicting definitions of "staff" and "employee" from country to country that make those values particularly unreliable in any international context.

3.23. Scoped affiliation

Name	eduPersonScopedAffiliation
Description	Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc. The values consist of a left and right component separated by an "@" sign. The left component is one of the values from the eduPersonAffiliation controlled vocabulary. This right-hand side syntax of eduPersonScopedAffiliation intentionally matches that used for the right-hand side values for eduPersonPrincipalName since both identify a security domain. Multiple "@" signs are not recommended, but in any case, the first occurrence of the "@" sign starting from the left is to be taken as the delimiter between components. Thus, user identifier is to the left, security domain to the right of the first "@". This parsing rule conforms to the POSIX "greedy" disambiguation method in regluar expression processing.
Vocabulary	See controlled vocabulary for eduPersonAffiliation. Only these values are allowed to the left of the "@" sign. The values to the right of the "@" sign should indicate a security domain.
Usage	authorization, accounting
References	[eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.9`
LDAP Syntax	Directory String
# of values	multi
Example values	`faculty@cs.berkeley.edu`

Semantics

An eduPersonScopedAffiliation value of "x@y" is to be interpreted as an assertion that the person in whose entry this value occurs holds an affiliation of type "x" within the security domain "y."

Notes

Consumers of eduPersonScopedAffiliation will have to decide whether or not they trust values of this attribute. In the general case, the directory carrying the eduPersonScopedAffiliation is not the ultimate authoritative speaker for the truth of the assertion. Trust must be established out of band with respect to exchanges of this attribute value.

3.24. Primary affiliation

Name	eduPersonPrimaryAffiliation
Description	Specifies the person's primary relationship to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).
Vocabulary	`faculty`, `student`, `staff`, `alum`, `member`, `affiliate`, ~~`employee`~~, `library-walk-in`
Usage	authorization, accounting
References	[eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.5`
LDAP Syntax	Directory String
# of values	single
Example values	`student`

Semantics

Each institution decides the criteria for membership in each affiliation classification.

A reasonable person should find the listed relationships commonsensical.

Notes

Appropriate if the person carries at least one of the defined eduPersonAffiliations. The choices of values are the same as for that attribute.

Think of this as the affiliation one might put on the name tag if this person were to attend a general institutional social gathering. Note that the single-valued eduPersonPrimaryAffiliation attribute assigns each person in the directory into one and only one category of affiliation. There are application scenarios where this would be useful.

See eduPersonAffiliation for further details.

3.25. Study branch 1

Name	swissEduPersonStudyBranch1
Description	Study branch of a student, first level of classification
Vocabulary	For `swissEduPersonOrganizationType = university`, possible values can be found in the first column of the uniStudyBranch1.csv file (see also Appendix A, *Study branches for Swiss universities*). For `swissEduPersonOrganizationType = uas`, possible values can be found in the first column of the uasStudyBranch1.csv file (see also Appendix B, *Study branches for Swiss universities of applied sciences*).
Usage	authorization
References	[SIUS-SHIS]
OID	`2.16.756.1.2.5.1.1.6`
LDAP Syntax	Integer {6}
# of values	multi
Example values	4 6

Semantics

This attribute follows the catalog of study branches of the SIUS/SHIS [SIUS-SHIS]. It is classified in branch, domain of branch and group of domain. This attribute is a code corresponding to the group of domain.

Notes

- This attribute is meaningful only if the person is a student (`eduPersonAffiliation` = `student`).

- The uniStudyBranch1.csv file (uasStudyBranch1.csv) lists possible values of this attribute and the corresponding meaning in German and French.

- Example: the value 1 means that the student is studying in a branch belonging to "Geistes + Sozialwiss." ("Sciences humaines + sociales").

3.26. Study branch 2

Name	swissEduPersonStudyBranch2
Description	Study branch of a student, intermediate level of classification
Vocabulary	For `swissEduPersonOrganizationType = university`, possible values can be found in the first column of the uniStudyBranch2.csv file (see also Appendix A, *Study branches for Swiss universities*). For `swissEduPersonOrganizationType = uas`, possible values can be found in the first column of the uasStudyBranch2.csv file (see also Appendix B, *Study branches for Swiss universities of applied sciences*).
Usage	authorization
References	[SIUS-SHIS]
OID	`2.16.756.1.2.5.1.1.7`
LDAP Syntax	Integer {6}
# of values	multi

Example values	`42`
	`62`

Semantics

This attribute follows the catalog of study branches of the SIUS/SHIS [SIUS-SHIS]. It is classified in branch, domain of branch and group of domain. This attribute is a code corresponding to the domain of branch.

Notes

- This attribute is meaningful only if the person is a student (`eduPersonAffiliation = student`).
- The uniStudyBranch2.csv file (uasStudyBranch2.csv) lists possible values of this attribute and the corresponding meaning in German and French. Example: the value 42 means that the student is studying in a branch belonging to "Naturwissenschaften" ("Sciences naturelles").
- If a value of this attribute is set, it always implies a value of `swissEduPersonStudyBranch1` even if it is not explicitly defined; it is the value given on the fourth column of the csv file. Example: `swissEduPersonStudyBranch2 = 42` means that `swissEduPersonStudyBranch1 = 4`.

3.27. Study branch 3

Name	swissEduPersonStudyBranch3
Description	Study branch of a student
Vocabulary	For `swissEduPersonOrganizationType = university`, possible values can be found in the first column of the uniStudyBranch3.csv file (see also Appendix A, *Study branches for Swiss universities*). For `swissEduPersonOrganizationType = uas`, possible values can be found in the first column of the uasStudyBranch3.csv file (see also Appendix B, *Study branches for Swiss universities of applied sciences*). The possible values of this attribute and their meaning correspond exactly to the coding used by the SIUS/SHIS; this coding is already used by every university and ETH for the data that is regularly sent to SIUS/SHIS.
Usage	authorization
References	[SIUS-SHIS]
OID	`2.16.756.1.2.5.1.1.8`
LDAP Syntax	Integer {6}
# of values	multi

Example values	`4700`
	`7450`

Semantics

This attribute is the SIUS/SHIS code of the study branch. It is classified in branch, domain of branch and group of domain.

Notes

- This attribute is meaningful only if the person is a student (`eduPersonAffiliation = student`).
- The uniStudyBranch3.csv file (uasStudyBranch3.csv) lists possible values of this attribute and the corresponding meaning in German and French.

  Example: the value 7450 means that the student is studying in the branch "Mikrotechnik" ("Microtechnique").
- If a value of this attribute is set, it implies always a value of `swissEduPersonStudyBranch1` even if it is not explicitly defined; it is the value given on the seventh column of the csv file. It also implies (not always) a value of `swissEduPersonStudyBranch2`.
- Example: `swissEduPersonStudyBranch3 = 7450` means that `swissEduPersonStudyBranch2 = 62` and `swissEduPersonStudyBranch1 = 6`.

- Change process: SHIS/SIUS may add new study branches, but will not delete or modify existing ones. Home organizations are obliged to implement new branches until the statistical data records have to be delivered to SHIS/SIUS (i.e. every year on Nov 15).

3.28. Study level

Name	swissEduPersonStudyLevel
Description	Study level of a student in a particular study branch
Vocabulary	This attribute follows the definition of study branch and study level of the SIUS/SHIS. The format is `<swissEduPersonStudyBranch3> - <study level>`. For `<swissEduPersonStudyBranch3>`, see Section 3.27, “Study branch 3”. For `<study level>`, the permissible values are listed in Appendix C, *Study levels of Swiss universities* and Appendix D, *Study levels of Swiss universities of applied sciences*.
Usage	authorization
References	[SIUS-SHIS]
OID	`2.16.756.1.2.5.1.1.9`
LDAP Syntax	Directory String
# of values	multi

Example values	`4700-15`
	`7450-20`

Notes

- This attribute is meaningful only if the person is a student (`eduPersonAffiliation = student`).

- A student may study in more than one study branch and may have reached a different study level in each of these study branches. Therefore, this attribute may have multiple values, defining the study level for each study branches 3.

- Make sure that the content of the attribute `swissEduPersonStudyBranch3` and `swissEduPersonStudyLevel` are consistent (`swissEduPersonStudyBranch3` should contain at least the study branch part of each study level).

3.29. Staff category

Name	swissEduPersonStaffCategory
Description	Workbranch of a staff member
Vocabulary	There are three main categories: `1xx` Teachers `2xx` Researchers `3xx` Others (Support, Admin and technical staff) The last two digits indicate a subcategory, as explained in Appendix E, *Staff categories*.
Usage	authorization, accounting
References	[SIUS-SHIS]
OID	`2.16.756.1.2.5.1.1.10`
LDAP Syntax	Integer {3}
# of values	multi

Example values	`101`
	`305`

Semantics

The classification is based on the staff categories of the SIUS/SHIS documents, suitably expanded to include non-school categories.

3.30. Organization path

Name	eduPersonOrgDN
Description	The distinguished name (DN) of the directory entry representing the organization with which the person is associated
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization
References	[eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.3`
LDAP Syntax	Directory String
# of values	single

Example values	`o=Universite de Lausanne,c=CH`
	`o=Hogwarts,dc=hsww,dc=wiz`

Semantics

The directory entry pointed to by this DN should be represented in the X.521(2001) "organization" object class.

Notes

- With a distinguished name, the client can do an efficient lookup in the institution's directory to find out more about the organization with which the person is associated.
- The value of `swissEduPersonHomeOrganization` attribute is better suited for authorization based on the organization the person is associated with.

3.31. Organizational unit path

Name	eduPersonOrgUnitDN
Description	The distinguished name (DN) of the directory entries representing the person's Organizational Unit(s)
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization
References	[eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.4`
LDAP Syntax	Directory String
# of values	multi

Example values	`ou=Faculte des sciences,o=Universite de Lausanne,c=CH`
	`ou=Potions,o=Hogwarts,dc=hsww,dc=wiz`

Semantics

The directory entry pointed to by this DN should be represented in the X.521(2001) "organizational unit" object class.

Notes

- With a distinguished name, the client can do an efficient lookup in the institution's directory for information about the person's organizational unit(s).
- It also possible to use this attribute to give some authorization to persons that belong to a known organizational unit.

3.32. Primary organizational unit

Name	eduPersonPrimaryOrgUnitDN
Description	The distinguished name (DN) of the directory entry representing the person's primary Organizational Unit(s).
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.8`
LDAP Syntax	Directory String
# of values	single
Example values	`ou=Music Department,o=Notre Dame,dc=nd,dc=edu`

Semantics

Each institution populating this attribute decides the criteria for determining which organization unit entry is the primary one for a given individual.

Notes

Appropriate if the person carries at least one of the defined eduPersonOrgUnitDN. The choices of values are the same as for that attribute.

3.33. Entitlement

Name	eduPersonEntitlement
Description	URI (either URL or URN) that indicates a set of rights to specific resources
Vocabulary	URIs only, i.e. a URL or URN
Usage	authorization, accounting
References	[eduPerson], [RFC3986]
OID	`1.3.6.1.4.1.5923.1.1.1.7`
LDAP Syntax	Directory String
# of values	multi
Example values	`http://unil.ch/resources/biblio92` `urn:mace:dir:entitlement:common-lib-terms`

Semantics

A simple example would be a URI for a contract with a licensed resource provider. When a principal's home institutional directory is allowed to assert such entitlements, the business rules that evaluate a person's attributes to determine eligibility are evaluated there. The target resource provider does not learn characteristics of the person beyond their entitlement. The trust between the two parties must be established out of band. One check would be for the target resource provider to maintain a list of subscribing institutions. Assertions of entitlement from institutions not on this list would not be honored.

Notes

– This attribute is suitable when a home organization knows to which resources a certain set of their students, staff etc. should have access to. The home organization knows their users and can therefore add a specific entitlement value to the entries of entitled users.

3.34. Assurance level

Name	eduPersonAssurance
Description	Set of URIs that assert compliance with specific standards for identity assurance.
Vocabulary	not applicable, no controlled vocabulary
Usage	authorization, accounting
References	[eduPerson]
OID	`1.3.6.1.4.1.5923.1.1.1.11`
LDAP Syntax	Directory String
# of values	multi
Example values	`urn:mace:incommon:IAQ:sample` `http://idm.example.org/LOA#sample`

Semantics

Notes

This multi-valued attribute represents identity assurance profiles (IAPs), which are the set of standards that are met by an identity assertion, based on the Identity Provider's identity management processes, the type of authentication credential used, the strength of its binding, etc. An example of such a standard is the InCommon Federation's proposed IAPs.

Those establishing values for this attribute should provide documentation explaining the semantics of the values.

As a multi-valued attribute, relying parties may receive multiple values and should ignore unrecognized values.

The driving force behind the definition of this attribute is to enable applications to understand the various strengths of different identity management systems and authentication events and the processes and procedures governing their operation and to be able to assess whether or not a given transaction meets the requirements for access. Example applications for which this attribute would be useful

Determining strength of asserted identity for on-line transactions, especially those involving more than minimal institutional risk resulting from errors in authentication.

A system supporting access to grants management in order to provide assurance for financial transactions.

References

[AAI-BCP-IdP] *Best current practices for operating a SWITCHaai Identity Provider*. http://www.switch.ch/aai/bcp/ .

[AAI-RR] *SWITCHaai Resource Registry*. http://www.switch.ch/aai/resourceregistry/ .

[Attr-Impl] *SWITCHaai Attributes Implementation*. http://www.switch.ch/aai/attributes/ .

[commonlibterms] *The common-lib-terms Entitlement*. http://www.switch.ch/aai/common-lib-terms/ .

[E.123] *Notation for national and international telephone numbers, e-mail addresses and Web addresses*. ITU. February 2001. http://www.itu.int/rec/T-REC-E.123/en .

[eduPerson] *EduPerson Object Class Specification (201203)*. EduPerson. Internet2 Middleware Architecture Committee for Education, Directory Working Group. 03.2012. http://middleware.internet2.edu/eduperson/ .

[IANA] *Internet Assigned Numbers Authority*. IANA. http://www.iana.org .

[Interfederation] *SWITCHaai Inter-federation activities*. http://www.switch.ch/aai/interfederation/ .

[Internet2] *Internet2*. Internet2. http://www.internet2.edu .

[ISO5218] *Information Interchange - Representation of Human Sexes*. ISO5218-2004. http://standards.iso.org/ittf/PubliclyAvailableStandards/, http://en.wikipedia.org/wiki/ISO_5218 .

[ISO9834] *Information Technology - Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components*. ISO9834-8:2005. http://standards.iso.org/ittf/PubliclyAvailableStandards/ .

[ISO15963] *Information technology -- Radio frequency identification for item management -- Unique identification for RF tags* . ISO/IEC. August 2009. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52124 .

[LDAP-schema] *LDAP Schema for AAI Attributes*. LDAP-schema. http://www.switch.ch/aai/docs/LDAP-schemas/ .

[RFC2119] *Key words for use in RFCs to Indicate Requirement Levels*. RFC 2119. IETF. March 1997. http://www.ietf.org/rfc/rfc2119.txt .

[RFC2798] *Definition of the inetOrgPerson LDAP Object Class*. RFC 2798. IETF. April 2000. http://www.ietf.org/rfc/rfc2798.txt .

[RFC2821] *Simple Mail Transfer Protocol*. RFC 2821. IETF. April 2001. http://www.ietf.org/rfc/rfc2821.txt .

[RFC2822] *Internet Message Format*. RFC 2822. IETF. April 2001. http://www.ietf.org/rfc/rfc2822.txt .

[RFC2849] *The LDAP Data Interchange Format (LDIF) - Technical Specification*. RFC 2849. IETF. June 2000. http://www.ietf.org/rfc/rfc2849.txt .

[RFC3339] *Date and Time on the Internet: Timestamps*. RFC 3339. IETF. July 2002. http://www.ietf.org/rfc/rfc3339.txt .

[RFC3986] *Uniform Resource Identifier (URI): Generic Syntax* . RFC 3986. IETF. January 2005. http://www.ietf.org/rfc/rfc3986.txt .

[RFC4512] *Lightweight Directory Access Protocol (LDAP): Directory Information Models*. RFC 4512. IETF. June 2006. http://www.ietf.org/rfc/rfc4512.txt .

[RFC4517] *Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules*. RFC 4517. IETF. June 2006. http://www.ietf.org/rfc/rfc4517.txt .

[RFC4519] *Lightweight Directory Access Protocol (LDAP): Schema for User Applications*. RFC 4519. IETF. June 2006. http://www.ietf.org/rfc/rfc4519.txt .

[RFC4524] *COSINE LDAP/X.500 Schema*. RFC 4524. IETF. June 2006. http://www.ietf.org/rfc/rfc4524.txt .

[RFC4646] *Tags for Identifying Languages*. RFC 4646. IETF. September 2006. http://www.ietf.org/rfc/rfc4646.txt .

[SAML-Attr-Profiles] *MACE-Dir SAML Attribute Profiles*. SAML Attribute Profiles. http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200804.pdf .

[SAML-core] *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 - Errata Composite*. SAML Core. OASIS. December 2009. http://www.oasis-open.org/committees/download.php/35711/ .

[SAML-overview] *Executive Overview of the Security Assertions Markup Language (SAML) v2.0*. SAML Exec Overview. OASIS. June 2004. http://www.oasis-open.org/committees/download.php/7521/ .

[SER-edu] *State secretariat for Education and Research, Switzerland's education system*. SER, Switzerland's Education System. http://www.sbf.admin.ch/htm/themen/bildung_en.html .

[Shib] *Shibboleth Internet2*. http://shibboleth.internet2.edu .

[SIUS-SHIS] *Service d'Information Universitaire Suisse, Schweizerisches Hochschulinformationssystem*. SIUS/SHIS. http://www.bfs.admin.ch, http://www.shs.bfs.admin.ch, http://www.shs.bfs.admin.ch .

[Swiss_ENIC] *Swiss European Network of National Information Centres on Academic Recognition and Mobility (ENIC)*. Swiss ENIC. http://www.crus.ch/information-programmes/reconnaissance-swiss-enic.html .

A. Study branches for Swiss universities

1. Permissible values for study branch 1

For the entire list see http://www.switch.ch/aai/docs/uniStudyBranch1.csv.

Study branch 1	German	French
1	Geistes- + Sozialwiss.	Sciences humaines + sociales
2	Wirtschaftswissenschaften	Sciences économiques
3	Recht	Droit
...	...	...

2. Permissible values for study branch 2

For the entire list see http://www.switch.ch/aai/docs/uniStudyBranch2.csv.

Study branch 2	German	French	Study branch 1
11	Theologie	Théologie	1
12	Sprach- + Literaturw. (SLW)	Langues + Littérature (LL)	1
13	Historische + Kulturw.	Sciences historiques + culture	1
...	...	...	...

3. Permissible values for study branch 3

For the entire list see http://www.switch.ch/aai/docs/uniStudyBranch3.csv.

Study branch 3	German	French	Study branch 1	Study branch 2
1201	Theologie fächerübergr./übrige	Théologie pluridisc./autres	1	12
1205	Protestantische Theologie	Théologie protestante	1	12
1210	Römisch-katholische Theologie	Théologie catholique-romaine	1	12
1215	Christkatholische Theologie	Théologie catholique-chrétienne	1	12
...	...	...	...	...

B. Study branches for Swiss universities of applied sciences

1. Permissible values for study branch 1

For the entire list see http://www.switch.ch/aai/docs/uasStudyBranch1.csv.

Study branch 1	German	French
10000	Architektur, Bau- und Planungswesen	Architecture, construction et planification
20000	Technik und IT	Technique et IT
30000	Chemie und Life Sciences	Chimie et sciences de la vie
40000	Land- und Forstwirtschaft	Agriculture et économie forestière
...	...	...

2. Permissible values for study branch 2

For the entire list see http://www.switch.ch/aai/docs/uasStudyBranch2.csv.

Study branch 2	German	French	Study branch 1
10101	Architektur	Architecture	1
10102	Bauingenieurwesen	Génie civil	10000
10104	Raumplanung	Aménagement du territoire	10000
10106	Geomatik	Géomatique	10000
...	...	...	...

3. Permissible values for study branch 3

For the entire list see http://www.switch.ch/aai/docs/uasStudyBranch3.csv.

Study branch 3	German	French	Study branch 1	Study branch 2
3801	Architektur	Architecture	10000	10101
3802	Bauingenieurwesen	Génie civil	10000	10102
3804	Raumplanung	Aménagement du territoire	10000	10104
...	...	...	...	...

C. Study levels of Swiss universities

00	de	Vorbereitungs- oder Fortbildungskurs, Gaststudierende
	en	Preparatory or continuing education course, guest students
	fr	Cours préparatoire, perfectionnement, auditeurs libre
	it	Corso preparatorio, perfezionamento, uditori
10	de	Lizentiats- oder Diplomstudium
	en	Licentiate or diploma study
	fr	Etudes conduisant à une licence ou un diplôme
	it	Studi che portano ad una licenza o un diploma
15	de	Bachelor-Studium
	en	Bachelor study
	fr	Etudes conduisant au Bachelor
	it	Studi che portano al bachelor
20	de	Zweite Studienhälfte
	en	2nd cycle of the study
	fr	Etudes 2e cycle
	it	Studi di 2ndo ciclo
25	de	Master-Studium mit Bachelor
	en	Master study with Bachelor’s degree
	fr	Etudes conduisant au Master avec un Bachelor
	it	Studi che portano al master con un bachelor
31	de	Doktoratsstudium
	en	Doctorate study
	fr	Etudes conduisant au doctorat
	it	Studi che portano ad un dottorato
33	de	Universitäre Weiterbildung
	en	University continuing education
	fr	Formations continues universitaires
	it	Formazione post universitaria
35	de	Universitäre Aufbau- und Vertiefungsstudien
	en	Advanced studies
	fr	Etudes universitaires spécialisées et approfondies
	it	Studi universitari specializzati ed approfonditi
39	de	Individuelles Nachdiplomstudium, Weiterbildung
	en	Individual postgraduate study, continuing education
	fr	Postdiplôme, formation continue
	it	Postdiploma, formazione permanente

1. Studienstufe

00 Studierende, die nur vorübergehend an der betreffenden Hochschule immatrikuliert sind (Fremdsprachenaufenthalt, Fortbildung) und hier *keine* Abschlussprüfungen ablegen werden (Gaststudierende).

Studierende, die im Rahmen eines von der Hochschule durchgeführten Vorbereitungskurses auf die Zulassung zu einem Studium hinarbeiten (z.B. Cours de mathématiques spéciales EPFL; *Zusatzqualifikationen für die Zulassung zu Master-Studiengängen*).

10 Studierende in der Studienphase, die zu einem der folgenden Abschlüsse führt: Lizentiat, Diplom, Gymnasial-, Sekundar- oder Primarlehrpatent, Abschlussprüfung bei Kurzstudiengängen.

Studierende der Medizin und der Eidg. Technischen Hochschulen: Hier werden nur die Vorkliniker/innen bzw. die Studierenden vor dem 2. Vordiplom mit der Studienstufe 10 bezeichnet.

15 Studierende in der Studienphase, die zum Bachelor führt.

20 Medizinstudierende in den klinischen Semestern, d.h. Medizinstudierende, die das 2. Propädeutikum bestanden haben.

Studierende der Eidg. Technischen Hochschulen, die das 2. Vordiplom absolviert haben.

25 Studierende, die den Bachelortitel erworben haben und einen Master anstreben.

31 Studien, die auf das Doktorat vorbereiten und einen akademischen Titel (Master, Lizentiat, Diplom) oder einen gleichwertigen Abschluss voraussetzen.

33 Angebote der universitären Weiterbildung mit *mindestens* 60 ECTS-Kreditpunkten, z.B. Master of Advanced Studies.

35 universitäre Aufbau- und Vertiefungsstudien mit *mindestens* 60 ECTS-Kreditpunkten: Diplôme d'études approfondies (DEA), Diplômes d'études supérieures spécialisées (DESS), "3e Cycle", zukünftig auch Master of Advanced Studies. Im Unterschied zur universitären Weiterbildung erfolgt der Besuch von Aufbau- und Vertiefungsstudien in der Regel direkt im Anschluss an den Erwerb eines universitären Abschlusses der zweiten Stufe (Master, Lizenziat/Diplom). Die Studien sind entweder auf eine zukünftige Forschungstätigkeit orientiert (z.B. DEA) oder bereiten die Studierenden auf die Berufspraxis vor (z.B. DESS).

39 Universitäre Weiterbildung von individuellem Charakter, mit oder ohne Abschlussdiplom, insbesondere:

– Immatrikulation im selben Fach nach einem Erstabschluss (Lizenziat, Diplom) ohne bestimmtes Studienziel

– Studien nach dem Doktorat.

2. Niveau d'études

00 Étudiants au niveau d'études diplôme qui sont immatriculés temporairement à la haute école concernée (séjour linguistique, perfectionnement) et qui n'y subiront *pas d'examen* (auditeurs libres).

Étudiants fréquentant des cours organisés par la haute école préparant aux études (par ex. cours de mathématiques spéciales EPFL; *qualifications supplémentaires pour l'admission aux études de master*).

10 Étudiants réguliers se trouvant dans une phase d'études qui les conduit à un des examens finals suivants: licence, diplôme, titre de maître ou maîtresse de gymnase ou de maître ou maîtresse primaire ou secondaire, examen final pour des filières de cycle court (p.ex. notaire).

Étudiants en médecine et des écoles polytechniques fédérales: seuls les précliniciens, c'est-à-dire les étudiants n'ayant pas subi le deuxième examen propédeutique sont recensés sous le niveau 10 (en voie de disparition).

15 étudiants réguliers se trouvant dans une phase d'études qui les conduit au titre de bachelor et les étudiants en médecine dans les filières MH, MD, MV et chiropratique en semestres précliniques ($1^{ère}$ et $2^{ème}$ années de programme).

16 Etudiants en médecine dans les filières MH, MD, MV et chiropratique en semestres cliniques ($3^{ème}$ année de programme).

20 Étudiants en médecine en semestres d'études cliniques.

Etudiants des écoles polytechniques fédérales qui ont passé le deuxième examen propédeutique.

25 Étudiants réguliers, ayant obtenu le titre de bachelor et qui aspirent au titre de master.

31 Études préparant au doctorat, après avoir obtenu un diplôme académique (master, licence, diplôme) ou un titre équivalent.

33 Formations continues universitaires d'*au moins* 60 points ECTS, p. ex. Master of Advanced Studies.

35 Études universitaires spécialisées et approfondies d'*au moins* 60 points ECTS: diplômes d'études supérieures spécialisées (DESS), diplôme d'études approfondies (DEA), «3e cycle», et désormais aussi Master of Advanced Studies. A la différence des formations continues, les études spécialisées et approfondies font en règle générale directement suite à l'acquisition d'un titre universitaire du 2e cycle (master, licence/ diplôme). Il s'agit soit d'études préparant à une activité professionnelle (p. ex. DESS), soit d'études préparant à une activité de recherche (p. ex. DEA).

39 Autres études post-diplôme, à caractère individuel, avec ou sans diplôme final, notamment:

- inscription dans la même filière après un premier titre universitaire (licence, diplôme) sans but défini

- études postdoctorat.

D. Study levels of Swiss universities of applied sciences

10	de	Diplom
	en	Diploma
	fr	Diplôme
	it	Diploma
15	de	Bachelor
	en	Bachelor
	fr	Bachelor
	it	Bachelor
20	de	Master
	en	Master
	fr	Master
	it	Master
33	de	Weiterbildung
	en	Continuing education
	fr	Formations continues
	it	Formazione
34	de	Modulare Weiterbildung
	en	Modular continuing education
	fr	Formations continues modulaire
	it	Formazione modulare

1. Studienstufe

10 *Diplom:* Studien im Hinblick auf ein FH-Diplom

15 *Bachelor:* Studien im Hinblick auf ein Bachelordiplom FH

25 *Master:* Studien im Hinblick auf ein Masterdiplom FH (*ohne* Masterstudien im *Bereich Weiterbildung*; siehe unten)

33 *Weiterbildung:* Vertiefungs- und Spezialisierungsstudiengänge

- Master of Advanced Studies MAS (mindestens 60 ECTS)
- Executive Master of Business Administration EMBA (mindestens 60 ECTS)
- Nachdiplomstudien NDS (gemäss bisheriger Definition 600 + 200 Stunden; Start noch bis Oktober 2007 möglich)

34 *Modulare Weiterbildung:* Modular aufgebaute Vertiefungs- und Spezialisierungsstudien (Definitionen wie oben unter Code 33 beschrieben)

2. Niveau d'études

00 Étudiants au niveau d’études diplôme qui sont immatriculés temporairement à la haute école concernée (séjour linguistique, perfectionnement) et qui n'y subiront *pas d'examen* (auditeurs libres).

Etudiants fréquentant des cours organisés par la haute école préparant aux études (par ex. cours de mathématiques spéciales EPFL; *qualifications supplémentaires pour l’admission aux études de master*).

10 *Diplôme:* études vers le diplôme HES

15 *Bachelor:* études vers un diplôme de bachelor HES

25 *Master:* études vers un diplôme de master HES (*sans* les études de master dans le domaine de *la formation continue*; voir ci-dessous)

33 *Formation continue:* Études postgrades visant une spécialisation / approfondissement

- Master of Advanced Studies MAS (60 ECTS au minimum)
- Executive Master of Business Administration EMBA (60 ECTS au minimum)
- Études postgrades EPG (selon la définition de 600 + 200 heures; ces EPG peuvent débuter encore jusqu'en octobre 2007)

34 *Formation continue modulaire:* Etudes postgrades modulaires visant une spécialisation ou un approfondissement (mêmes définitions comme pour le code 33; voir ci-dessus)

E. Staff categories

The permissible values of the `swissEduPersonStaffCategory` attribute are, where possible, obtained from the SIUS/SHIS documents:

– [1] Technisches Handbuch für universitäre Hochschulen

– [2] Technisches Handbuch für die Erhebung des Personals der FH und der PH.

1. Teaching

Designates staff with teaching duties (including physicians working at university hospitals). Completely based on the SIUS/SHIS documents.

Staff category	Name	Example	Remark
101	Professors	Ordinary Professors	[1] Cat I-II, [2] Cat 10
102	Oberer Mittelbau / Corps intermediaire superieur	Lecturers	[1] Cat III-IV, [2] Cat 20
103	Unterer Mittelbau / Corps intermediaire inferieur	Assistants	[1] Cat V-VI, [2] Cat 30

2. Research

Designates staff with research duties. Similar to the Teaching category, but for researchers only.

Staff category	Name	Example	Remark
201	Permanent Researchers	Ordinary Professors	[1] Cat I-II, [2] Cat 10
202	Oberer Mittelbau / Corps intermediaire superieur	Lecturers	[1] Cat III-VI, [2] Cat 20
203	Unterer Mittelbau / Corps intermediaire inferieur	Assistants	[1] Cat VII-X, [2] Cat 30

3. Admin, support, technical

This section has no direct correspondence to the SIUS/SHIS documents. Though, it's based on the categories XI-XVII of [1].

Staff category	Name	Example	Remark
301	Administrative Personnel	Members of HR	[1] Cat XI, [2] Cat 40
302	Administrative Personnel: Apprentices and Interns		[1] Cat XII, [2] Cat 40
303	Technical Personnel	System administrators	[1] Cat XII, [2] Cat 40
304	Technical Personnel: Apprentices and Interns		[1] Cat XIII, [2] Cat 40
305	Janitors, Building Managers		[1] Cat XIV, [2] Cat 40
306	Social and Wellness Personnel		[1] Cat XVI, [2] Cat 40
307	Library Personnel		[1] Cat XVII, [2] Cat 40
308	Safety Personnel	Radiation, Firefighters, Guards	

F. Changelog

Revision History

Revision 1.4.2 2012-10-25

- updated Notes and Semantics according the changes from eduPerson(200806) to eduPerson(201203)

Revision 1.4.1 2012-07-26

- corrected the links to the cvs files in Appendix B and updated the example values for study branch 2 and 3

Revision 1.4 2011-01-05

- added new values 'tertiaryb' and 'uppersecondary' in swissEduPersonHomeOrganizationType attribute

Revision 1.3 2010-06-23

- document title modified: 'AAI Attribute Specification' replaced by 'Attribute Specification'
- Added new chapter “Implementing the Attribute Specification” and removed implementation status from attribute definitions, now having the master information on the website for the implementation status
- new swissEduPerson attribute added: 'Card UID'
- added complete set of attributes from eduPerson specification to this document (eduPersonTargetedID, eduPersonPrincipalName, eduPersonNickname, eduPersonScopedAffiliation, eduPersonPrimaryAffiliation, eduPersonPrimaryOrgUnitDN, eduPersonAssurance)
- added new value 'library-walk-in' in eduPersonAffiliation attribute
- new layout of the document

Revision 1.2 2007-09-05

- document title modified: 'Authorization' replaced by 'AAI'
- new introduction text
- new attributes added: 'User ID', 'Matriculation number', 'Employee number'

- E-mail is mandatory instead of recommended only
- maximum length of swissEduPersonUniqueID 255 characters
- eduPerson attributes updated accordingly to eduPerson specification (200604)
- references to obsoleted RFCs adapted
- format of attribute description changed, Origin and OID added
- short descriptions of study levels added
- UAS: study branches updated, study levels added

Revision 1.1 2004-01-15

- example of swissEduPersonUniqueID
- value of swissEduPersonOrganizationType in chap. 4.16-4.18
- references added
- eduPerson attributes updated accordingly to eduPerson specification (200312)
- chapter "5. Group membership ..." removed

Revision 1.0 2002-12-11

- surname, givenname, mail, homePostalAddress, postalAddress: usage within AAI changed
- swissEduPersonOrgDN, swissEduPersonOrgUnitDN, swissEduPersoneEntitlement, mobileTelephoneNumber: attributename changed
- swissEduPersonDateOfBirth, swissEduPersonGender: format changed
- code lists for UAS study branches added (appendix B)

Revision 0.6 2002-11-07

Initial version

G. Contributors

Version 1.4	
Thomas Lenggenhager	SWITCH
Patrik Schnellmann	SWITCH
Version 1.3	
Michael Hausherr	Fachhochschule Nordwestschweiz
Thomas Lenggenhager	SWITCH
Roberto Mazzoni	Universität Zürich
Alexandre Roy	Université de Lausanne
Patrik Schnellmann	SWITCH
Thomas Staub	Universität Bern
Version 1.2	
Roland Dietlicher	ETH Zürich
Peter Geiser	Universität Bern
Thomas Lenggenhager	SWITCH
Beat Müller	ETH Zürich
Dominique Petitpierre	Université de Genève
Pascal Py	Universität Zürich
Alexandre Roy	Université de Lausanne
Luzian Scherrer	Universität Zürich
Patrik Schnellmann	SWITCH
Version 1.1	
Thomas Lenggenhager	SWITCH
André Redard	at rete ag
Version 1.0	
Serge Droz	PSI
Pascal Jacot-Guillarmod	Université de Lausanne
Thomas Lenggenhager	SWITCH
Christian Heim	Universität Bern
David McLaughlin	ETH Zürich
Pascal Py	Universität Zürich
André Redard	at rete ag
Alexandre Roy	Université de Lausanne
Marc-Alain Steinemann	Universität Bern