# Attribute Specification

for the SWITCHaai Federation

14 February 2023

Version 1.7.2

SWITCH

https://www.switch.ch/aai/attributes/

# 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 the SWITCHaai federation and in chapter 2.2 the attributes specific to SWITCH edu-ID.
The format of the attribute definition is close to the LDAP syntax (see chapter 2: “Attribute definitions” for further details). A schema for LDAP servers [LDAP-schema] is available.

This specification started with a basic set of attributes 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 ➟ https://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 processing attributes must fully respect user privacy and the relevant data protection laws and regulations that 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` (User ID). It could provide valuable information to a malicious third party. Its intended semantics is to be a user's identifier for authentication (aka login). 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.

SWITCHaai is designed to transfer information *about* authentication but not the credentials themselves.

## 1.3. Protocol Support

This specification was originally designed for the SAML [SAML-core] protocol only. The fully backwards compatible and continuous evolution from a mesh based SAML only federation towards the user-centric SWITCH edu-ID service allowed the introduction of OpenID Connect [OIDC-core] as additional protocol.

Many of the attributes include OIDC specific information like the name of their claim, the scope they belong to as well as the type of the value. Only a few claims use a slightly different format or set of values compared to the attributes in SAML. Additional OIDC specific information gets added as use cases require it.

All the OIDC specific information important for SWITCH edu-ID can be found summarized on the web page:
➟ https://www.switch.ch/edu-id/docs/services/openid-connect/scopes/ [OIDC_Scopes_and_Claims].

# 2. Attribute definitions

For all attributes, the following metadata is defined:

| | |
|---|---|
| Name | The name of the attribute |
| Description | A short description of the attribute |
| Vocabulary | A list of allowed values.<br>Where applicable, the list of values is based on international or national standards. |
| References | Reference to a standard the attribute is based on (where available) |
| OIDC | Claim: name of the claim<br>Type: boolean, string or JSON Array<br>Scope: name of the scope in which the claim is included |
| OID | Object Identifier |
| LDAP Syntax | The LDAP syntax of an attribute, see[RFC4517].<br>"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 keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in[BCP14].

# 2.1. swissEduPerson Attribute Definitions

## 2.1.1. 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 |
| References | none |
| OIDC | Claim: `swissEduPersonUniqueID`<br>Type: string<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| OID | `2.16.756.1.2.5.1.1.1` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `845938727494@ethz.ch`<br>`288aac23dbf9e1460c86b1a5a04c6afb75f724ce@uzh.ch` |

### Definition

This identifier represents a specific principal in a specific identity system. Values of this attribute MUST be assigned in such a manner that no two values created by distinct identity systems could collide. This identifier is permanent, to the extent that the principal is represented in the issuing identity system. Once assigned, it MUST NOT be reassigned to another principal.

This identifier is scoped and of the form `uniqueID@scope`.

`scope` (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` .

`uniqueID` (local part)

> It is an ID uniquely allocated by the home organization for a user they correctly authenticated according to the local authentication policy.
> - The uniqueID portion MUST be unique within the context of the issuing identity system (**no reassignment** to another principal).

- It MUST contain only alphanumeric characters (a-z, A-Z, 0-9).
  Due to the `caseIgnoreMatch` matching rule from the LDAP schema one SHOULD only use uppercase OR lowercase characters to avoid potential clashes.
- The length of the uniqueID portion MUST be less than or equal to 64 characters.

### Deprecated former definition of uniqueID part

Deprecated in March 2017 (PDF document version 1.6) in favor of a definition aligned with the `eduPersonUniqueId` attribute:
~~The uniqueID part can contain any characters which can be part of the local part of an e-mail address according to [RFC5322], namely: -._%.~~

### Notes

- One SHOULD NOT expose the Unique ID to end users; especially one SHOULD NOT require a user to provide the Unique ID manually!
- The uniqueID part MAY be a Base32 [RFC4648] hash value based on unique 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.

## 2.1.2. 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` |
| References | [RFC3339] |
| OIDC | Claim: `birthdate`<br>Type: string<br>Scope: `profile`<br>Format: `YYYY-MM-DD` |
| OID | `2.16.756.1.2.5.1.1.2` |
| LDAP Syntax | Numeric String {8} |
| # of values | single |
| Example values | `19871022`<br>`20021010` |

### Definition

Based on [RFC3339] 'Date and Time on the Internet: Timestamps'. Using the `full-date` format from paragraph 5.6 but without the dashes:

`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/year

### Notes

- If a use case requires age related information but not the specific date of birth, the attribute `swissEduPersonMinimumAgeCategory` should be preferred over `swissEduPersonDateOfBirth`.

## 2.1.3. Gender

| | |
|---|---|
| Name | `swissEduPersonGender` |
| Description | The state of being male or female |
| Vocabulary | The following codes are used (see[ISO5218]):<br>`0` Not known,<br>`1` Male,<br>`2` Female,<br>`9` Not applicable |
| References | [ISO5218] |
| OIDC | Claim: `gender`<br>Type: string<br>Scope: `profile`<br>Possible values: `female`, `male`, `not applicable` |
| OID | `2.16.756.1.2.5.1.1.3` |
| LDAP Syntax | Integer {1} |
| # of values | single |
| Example values | `1`<br>`9` |

## 2.1.4. Home organization

| | |
|---|---|
| Name | `swissEduPersonHomeOrganization` |
| Description | Domain name of a home organization |
| Vocabulary | SWITCH maintains a register of organizations participating in SWITCHaai with their domain name and `swissEduPersonHomeOrganizationType` |
| References | none |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.4` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `unil.ch`<br>`ethz.ch`<br>`library.ethz.ch` |

## 2.1.5. Home organization type

| | |
|---|---|
| Name | `swissEduPersonHomeOrganizationType` |
| Description | Type of a home organization |
| Vocabulary | `university`, `uas`, `hospital`, `library`, `tertiaryb`, `uppersecondary`, `vho`, `others` |
| References | [Swiss_ENIC] |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.5` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `university`<br>`vho`<br>`hospital` |

### Definition

`university`

University or federal institute of technology recognized by [Swiss_ENIC]

`uas`

University of applied sciences or university of teacher education recognized by [Swiss_ENIC]

`hospital`

The institution is a hospital

`library`

The institution is a library

`tertiaryb`

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

`uppersecondary`

Vocational education and training school or general education school on the upper secondary level [SERI-edu]

`vho`

Virtual home organization

`others`

Institution for which none of the other values match

## 2.1.6. Study branch 1

| | |
|---|---|
| Name | `swissEduPersonStudyBranch1` |
| Description | Study branch of a student, first level of classification |
| Vocabulary | controlled, see below |
| References | [SIUS-SHIS] |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.6` |
| LDAP Syntax | Integer {6} |
| # of values | multi |
| Example values | 4<br>6 |

### Definiton

This attribute follows the catalog of study branches of the[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.

Find possible values for `swissEduPersonOrganizationType = university` in the first column of the [uniStudyBranch1] file or for `swissEduPersonOrganizationType = uas` in the first column of the [uasStudyBranch1] file. See Appendix A, *Code lists*.

### Notes

- This attribute is meaningful only if the person is a student (`eduPersonAffiliation` = `student`).
- The [uniStudyBranch1] file ([uasStudyBranch1]) 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").

## 2.1.7. Study branch 2

| | |
|---|---|
| Name | `swissEduPersonStudyBranch2` |
| Description | Study branch of a student, intermediate level of classification |
| Vocabulary | controlled, see below |
| References | [SIUS-SHIS] |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.7` |
| LDAP Syntax | Integer {6} |
| # of values | multi |
| Example values | 42<br>62 |

### Definition

This attribute follows the catalog of study branches of the[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.

Find possible values for `swissEduPersonOrganizationType = university` in the first column of the [uniStudyBranch2] file or for `swissEduPersonOrganizationType = uas` in the first column of the [uasStudyBranch2] file. See Appendix A, *Code lists*.

### Notes

- This attribute is meaningful only if the person is a student (`eduPersonAffiliation = student`).
- The [uniStudyBranch2] file ([uasStudyBranch2]) 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`.

## 2.1.8. Study branch 3

| | |
|---|---|
| Name | `swissEduPersonStudyBranch3` |
| Description | Study branch of a student |
| Vocabulary | controlled, see below |
| References | [SIUS-SHIS] |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.8` |
| LDAP Syntax | Integer {6} |
| # of values | multi |
| Example values | `4700`<br>`7450` |

### Definition

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

Find possible values for `swissEduPersonOrganizationType = university` in the first column of the [uniStudyBranch3] file or for `swissEduPersonOrganizationType = uas` in the first column of the [uasStudyBranch3] file. See Appendix A, *Code lists*.

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 for the data they regularly send to SIUS/SHIS.

### Notes

- This attribute is meaningful only if the person is a student (`eduPersonAffiliation = student`).
- The [uniStudyBranch3] file ([uasStudyBranch3]) 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 `swissEduPersonStudy-Branch1 = 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).

## 2.1.9. Study level

| | |
|---|---|
| Name | swissEduPersonStudyLevel |
| Description | Study level of a student in a particular study branch |
| Vocabulary | controlled, see bleow |
| References | [SIUS-SHIS] |
| OIDC | n/a |
| OID | 2.16.756.1.2.5.1.1.9 |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | 4700-15<br>7450-20 |

### Definition

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 2.1.8, “Study branch 3”.

For <study level>, find possible values for swissEduPersonOrganizationType = university in the first column of the [uniStudyLevel] file or for swissEduPersonOrganizationType = uas in the first column of the [uasStudyLevel] file. See Appendix A, *Code lists*.

### 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 of the swissEduPersonStudyBranch3 values.
- The content of the attributes swissEduPersonStudyBranch3 and swissEduPersonStudyLevel must be consistent: swissEduPersonStudyBranch3 should contain at least the study branch part of each swissEduPersonStudyLevel value.

## 2.1.10. Staff category

| | |
|---|---|
| Name | swissEduPersonStaffCategory |
| Description | Workbranch of a staff member |
| Vocabulary | controlled, see below |
| References | [SIUS-SHIS] |
| OIDC | n/a |
| OID | 2.16.756.1.2.5.1.1.10 |
| LDAP Syntax | Integer {3} |
| # of values | multi |
| Example values | 101<br>305 |

### Definition

The classification is based on the staff categories of the [SIUS-SHIS] documents.

Find possible values for swissEduPersonOrganizationType = university in the first column of the [uniStaffCategory] file or for swissEduPersonOrganizationType = uas in the first column of the [uasStaffCategory] file. See Appendix A, *Code lists*.

## 2.1.11. Matriculation number

| | |
|---|---|
| Name | `swissEduPersonMatriculationNumber` |
| Description | Matriculation number of a student |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [SIUS-SHIS] |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.11` |
| LDAP Syntax | Numeric String {8} |
| # of values | single |
| Example values | `04911506`<br>`72836596` |

### Definition

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 or teacher education university. 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.

## 2.1.12. Card UID

| | |
|---|---|
| Name | `swissEduPersonCardUID` |
| Description | Card unique identifier |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [ISO15693] |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.12` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `E002219C5298303B@ISO15693`<br>`0298450109348@unil.ch` |

### Definition

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

For RFID Cards with the UID format defined in the ISO standard[ISO15693], the identifier for the card type is `ISO15693`. The value is formatted as specified in the ISO 15693 standard, a 64-bit unique identifier with the most significant bytes first. The value is represented as a hexadecimal string.

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

## 2.1.13. Minimum age category

| | |
|---|---|
| Name | `swissEduPersonMinimumAgeCategory` |
| Description | The minimum age category of the person |
| Vocabulary | `0`, `6`, `8`, `12`, `14`, `16`, `18` |
| References | none |
| OIDC | Claim: `swissEduPersonMinimumAgeCategory`<br>Type: string<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| OID | `2.16.756.1.2.5.1.1.19` |
| LDAP Syntax | Numeric String {2} |
| # of values | single |
| Example values | `14`<br>`18` |

### Definition

`max(x) WHERE x ∈ {0, 6, 8, 12, 14, 16, 18} AND x ≤ age`

### Notes

- If a use case requires age related information but not the specific date of birth, the attribute `swissEduPersonMinimumAgeCategory` should be preferred over `swissEduPersonDateOfBirth` .

## 2.1.14. Organizational e-mail

| | |
|---|---|
| Name | `swissEduPersonOrganizationalMail` |
| Description | Organizational e-mail addresses of a person |
| Vocabulary | not applicable, no controlled vocabulary |
| References | none |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.20` |
| LDAP Syntax | IA5 String {256} |
| # of values | multi |
| Example values | `mary.francis-xavier@example.edu` |

## 2.1.15. Private e-mail

| | |
|---|---|
| Name | `swissEduPersonPrivateMail` |
| Description | Private e-mail addresses of a person |
| Vocabulary | not applicable, no controlled vocabulary |
| References | none |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.18` |
| LDAP Syntax | IA5 String {256} |
| # of values | multi |
| Example values | `aiesh12@example.org` |

# 2.2. SWITCH edu-ID Attribute Definitions

The prefix `swissEduID` for the following SWITCH edu-ID specific attributes was derived from the original project name "Swiss edu-ID", whereas the service is now named "SWITCH edu-ID".

## 2.2.1. Swiss edu-ID internal identifier

| | |
|---|---|
| Name | `swissEduID` |
| Description | The Swiss edu-ID persistent identifier for Swiss Higher Education users |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [RFC4122], [eduIDSpec] |
| OIDC | Claim: `swissEduID`<br>Type: string<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| OID | `2.16.756.1.2.5.1.1.13` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `0000bdaf-da5c-4851-ae02-26416dfda1c2`<br>`0000a1a1-b2f8-42fa-852b-d768f8261e20` |

### Definition

The identifier is associated to a user for her/his entire life. The `swissEduID` should only be used internally to link personal data over a long period of time between services or applications and across institutional boundaries.

- The `swissEduID` SHOULD NOT be exposed to users.

- The `swissEduID` is a UUID version 4 string according to[RFC4122], where the hex digits MUST be lower case, despite the standard would allow lower or upper case.

A `swissEduID` issued to a real person has not the value 0 in all the first 16 bits (the first 4 hex digits).

A `swissEduID` that has the value 0 in all the 16 leading bits (in the first 4 hex digits) is reserved for examples, developments, tests, debugging etc.

## 2.2.2. SWITCH edu-ID associated e-mail

| | |
|---|---|
| Name | `swissEduIDAssociatedMail` |
| Description | All currently associated e-mail addresses of the private identity |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [RFC4524] |
| OIDC | Claim: `swissEduIDAssociatedMail`<br>Type: JSON array<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| OID | `2.16.756.1.2.5.1.1.17` |
| LDAP Syntax | IA5 String {256} |
| # of values | multi |
| Example values | `john.doe@unia.ch jdoe@unib.ch`<br>`john@unic.ch` |

### Definition

The attribute contains all `mail` values of the private identity without the mail values of the current affiliations of an edu-ID account.

The order of the values in the attribute is not defined.

## 2.2.3. SWITCH edu-ID assurance level

| | |
|---|---|
| Name | `swissEduIDAssuranceLevel` |
| Description | Attribute Quality Assurance |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduIDAttributeQuality] |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.1027` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `mail:https://eduid.ch/def/loa2`<br>`homePhone:https://eduid.ch/def/loa1` |

### Definition

Quality statements are made on attribute level. Multivalued attributes have only a single verification status. The SWITCH edu-ID attribute quality model is inspired by the [eCH-0171] specification.

The following verification levels are supported by edu-ID:

1 - low, with loa-string: `https://eduid.ch/def/loa1`

Self-declared attributes by the user, on an online form of the SWITCH edu-ID web site.

2 - medium, with loa-string: `https://eduid.ch/def/loa2`

Requires an automated validation process. The user triggers a validation process that is programmatically executed on the SWITCH edu-ID IdP.

`swissEduIDAssuranceLevel` values are a concatenation of:
`<attribute-name> ":" <loa-string>`

where `<atrribute-name>` is one of the attribute names listed in [eduIDAttributeQuality]

and <loa-string> is one of the values listed above.

## 2.2.4. SWITCH edu-ID linked affiliation

| | |
|---|---|
| Name | swissEduIDLinkedAffiliation |
| Description | List of eduPersonScopedAffiliation values of all current affiliations |
| Vocabulary | see controlled vocabulary for eduPersonAffiliation |
| References | eduPersonScopedAffiliation |
| OIDC | Claim: swissEduIDLinkedAffiliation<br>Type: JSON array<br>Scope: https://login.eduid.ch/authz/User.Read |
| OID | 2.16.756.1.2.5.1.1.1029 |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | student@unia.ch member@unia.ch staff@unib.ch member@unib.ch affiliate@unic.ch |

### Definition

The attribute contains all eduPersonScopedAffiliation values of all current affiliations of an edu-ID account.

## 2.2.5. SWITCH edu-ID linked affiliation e-mail

| | |
|---|---|
| Name | swissEduIDLinkedAffiliationMail |
| Description | List of e-mail values of all current affiliations |
| Vocabulary | not applicable, no controlled vocabulary |
| References | mail |
| OIDC | Claim: swissEduIDLinkedAffiliationMail<br>Type: JSON array<br>Scope: https://login.eduid.ch/authz/User.Read |
| OID | 2.16.756.1.2.5.1.1.1031 |
| LDAP Syntax | IA5 String {256} |
| # of values | multi |
| Example values | john.doe@unia.ch jdoe@unib.ch john@unic.ch |

### Definition

The attribute contains all mail values of all current affiliations of an edu-ID account.

The order of the values in the attribute is not defined.

### Notes

To associate e-Mail addresses from affiliations to their corresponding swissEduPersonUniqueID the extended attribute model with requests to the SWITCH edu-ID affiliation API [eduIDAffiliationAPI] needs to be implemented.

## 2.2.6. SWITCH edu-ID linked affiliation unique ID

| | |
|---|---|
| Name | swissEduIDLinkedAffiliationUniqueID |
| Description | List of swissEduPersonUniqueID values of all current affiliations |
| Vocabulary | not applicable, no controlled vocabulary |
| References | swissEduPersonUniqueID |
| OIDC | Claim: swissEduIDLinkedAffiliationUniqueID<br>Type: JSON array<br>Scope: https://login.eduid.ch/authz/User.Read |
| OID | 2.16.756.1.2.5.1.1.1032 |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | 123456789@unia.ch 987654321@unib.ch 5487433b2aa643198edf45f2cb609e34@unic.ch |

### Definition

The attribute contains all `swissEduPersonUniqueID` values of all current affiliations of an edu-ID account.

### Notes

For each of the `swissEduPersonUniqueID` values the associated affiliation attributes can be accessed by issuing a `GET` request via the SWITCH edu-ID affiliation API[eduIDAffiliationAPI].

## 2.2.7. SWITCH edu-ID active user

| | |
|---|---|
| Name | `swissEduIDUsage1y` |
| Description | Did the user authenticate at least once with the SWITCH edu-ID credentials during the past 12 months? |
| Vocabulary | TRUE, FALSE |
| References | none |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.1026` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `TRUE` |

### Definition

The attribute returns `TRUE` if the user authenticated at least once with the SWITCH edu-ID credentials during the past 12 months, `FALSE` otherwise.

# 2.3. swissLibraryPerson Attribute Definitions

## 2.3.1. Library patron affiliation

| | |
|---|---|
| Name | `swissLibraryPersonAffiliation` |
| Description | Type of library affiliation |
| Vocabulary | `private`, `company`, `guest` |
| References | none |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.1023` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `company` |

### Definition

This attribute specifies the library affiliation of a patron who is neither a student nor an employee of the institution the library is related with. Patrons who make use of `swissLibraryPersonAffiliation` MUST have the value `affiliate` set in `eduPersonAffiliation` .
There are three possible values for this attribute:

`private`

: Patron is registered as a private person. Patron visits the library physically on a regular basis and/or uses digital resources the library offers.

`company`

: Patron is registered with an employer relationship. Patron uses library services and/or use digital resources the library offers.

`guest`

: Patron visits the library physically and uses on-site services like Internet terminals.

### Notes

- When using `swissLibraryPersonAffiliation`, the use of the `eduPersonAffiliation` value `library-walk-in` is not recommended, unless there is a specific reason.

## 2.3.2. Library patron residence

| | |
|---|---|
| Name | `swissLibraryPersonResidence` |
| Description | Defines the current residence of the patron |
| Vocabulary | Two letter country codes specified in ISO 3166-1 alpha-2 |
| References | [ISO3166-1_alpha-2] |
| OIDC | n/a |
| OID | `2.16.756.1.2.5.1.1.1025` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `CH`<br>`LI` |

### Definition

This attribute allows to authorize access to e-resource licenses that are only available to legal or current residents in a specific country. Licenses of ebooks or ejournals are commonly bound to residency in one specific country.

## 2.3.3. Canton of residence

| | |
|---|---|
| Name | `swissLibraryPersonResidenceCanton` |
| Description | The current canton of residence of the patron |
| Vocabulary | Two letter canton code specified in Swiss VZV Art. 84 |
| References | [VZV_Art84] |
| OIDC | Claim: `swissLibraryPersonResidenceCanton`<br>Type: string<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| OID | `2.16.756.1.2.5.1.1.1033` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `FR`<br>`LU` |

### Definition

This attribute, likely derived from the postal address of the patron, allows to authorize access to e-resource licenses restricted to legal or current residents in a specific Swiss canton. Namely cantonal libraries license access to ebooks or ejournals bound to residency in their canton.

# 2.4. eduPerson Attribute Definitions

## 2.4.1. Affiliation

| | |
|---|---|
| Name | `eduPersonAffiliation` |
| Description | Type of affiliation |
| Vocabulary | `faculty`, `student`, `staff`, `alum`, `member`, `affiliate`, ~~`employee`~~ , `library-walk-in` |
| References | [eduPerson] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.5923.1.1.1.1` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `student`<br>`affiliate` |

## Definition

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

The primary intended purpose of `eduPersonAffiliation` is to convey broad-category affiliation assertions between members of an identity federation. Given this inter-institutional context, only values of `eduPersonAffiliation` with broad consensus in definition and practice will have any practical value. 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.

`member` is intended to include faculty, staff, student, and other persons with a full set of basic 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`
- `staff`
- `student`
- `employee`

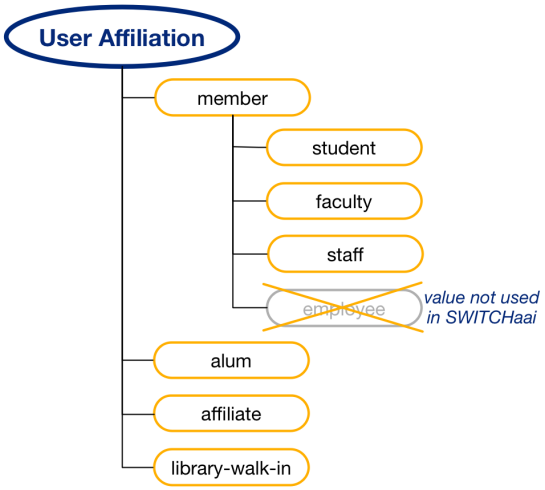
`affiliate` for `eduPersonAffiliation` indicates that the holder has some definable affiliation to the university NOT captured by any of `faculty`, `staff`, `student`, `employee`, `alum` and/or `member`. Typical examples might include event volunteers, parents of students, guests and external auditors. 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] ➟ **https://www.switch.ch/aai/common-lib-terms** .

The presence of other affiliation values neither implies nor precludes the affiliation `library-walk-in`.

It is not feasible to attempt to reach broad-scale, precise and binding inter-institutional definitions of affiliations such as faculty and students. Organizations have a variety of business practices and institutional specific uses of common terms. Therefore each institution will decide the criteria for membership in each affiliation classification. What is desirable is that a reasonable person should find an institution's definition of the affiliation plausible.

## Important




Role hierarchy of the `eduPersonAffiliation` values

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

## Notes

- If there is a value in `eduPersonPrimaryAffiliation` , that value MUST be asserted here as well.

- Holders of the affiliation a `lum` are not typically "members" since they are not eligible for the full set of basic institutional privileges enjoyed by faculty, staff and students.
- 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.

## 2.4.2. 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 |
| References | [eduPerson], [RFC3986] |
| OIDC | Claim: `eduPersonEntitlement`<br>Type: JSON array<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| 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`<br>`urn:mace:dir:entitlement:common-lib-terms` |

### Definition

URI (either URN or URL) that indicates a set of rights to specific resources.

### Notes

- A simple example would be a URL 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.
- URN values would correspond to a set of rights to resources based on an agreement across the relevant community. MACE (Middleware Architecture Committee for Education) affiliates may opt to register with MACE as a naming authority, enabling them to create their own URN values.
  ➟ https://www.switch.ch/aai/mace/

## 2.4.3. Nick name

| | |
|---|---|
| Name | `eduPersonNickname` |
| Description | Person's nickname |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.5923.1.1.1.2` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `Spike` |

### Definition

Person's nickname, or the informal name by which they are accustomed to be hailed.

### 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."

## 2.4.4. 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 |
| References | [eduPerson] |
| OIDC | n/a |
| 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`<br>`o=Hogwarts,dc=hsww,dc=wiz` |

### Definition

The distinguished name (DN) of the directory entry representing the institution with which the person is associated.

### Semantics

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

#### Important

- In SWITCHaai, the value of `swissEduPersonHomeOrganization` attribute is better suited for authorization based on the organization the person is associated with.

### 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.

## 2.4.5. 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 |
| References | [eduPerson] |
| OIDC | n/a |
| 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`<br>`ou=Potions,o=Hogwarts,dc=hsww,dc=wiz` |

### Definition

The distinguished name(s) (DN) of the directory entries representing the person's Organizational Unit(s). May be multivalued, as for example, in the case of a faculty member with appointments in multiple departments or a person who is a student in one department and an employee in another.

### 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).

## 2.4.6. Primary affiliation

| | |
|---|---|
| Name | `eduPersonPrimaryAffiliation` |
| Description | The person's primary relationship to the institution |
| Vocabulary | see controlled vocabulary for `eduPersonAffiliation` |
| References | [eduPerson] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.5923.1.1.1.5` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `student` |

### Definition

Specifies the person's primary relationship to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).

#### Important

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

### 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.

## 2.4.7. 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 |
| References | [eduPerson] |
| OIDC | n/a |
| 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` |

### Definition

The distinguished name (DN) of the directory entry representing the person's primary Organizational Unit(s).

### 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.

## 2.4.8. Principal name

| | |
|---|---|
| Name | `eduPersonPrincipalName` |
| Description | A scoped identifier for a person |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.5923.1.1.1.6` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `hputter@hsww.wiz` |

### Definition

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 the `scope` portion MUST be the administrative domain of the identity system where the identifier was created and assigned. 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. There must be one and only one `@` sign in valid values of `eduPersonPrincipalName`.

#### Important

- In SWITCHaai, this attribute SHOULD NOT be used. Use `swissEduPersonUniqueID` if a non-targeted identifier is required.
- For interfederation use, `eduPersonPrincipalName` might be suitable, however, `subject-id` would be better.

### Notes

- Values of `eduPersonPrincipalName` are often, but not required to be, human-friendly, and may change as a result of various business processes.
  Possibilities of changes and reassignments make this identifier unsuitable for many purposes. As a result, `eduPersonPrincipalName` is NOT RECOMMENDED for use by applications that provide separation between low-level identification and more presentation-oriented data such as name and email address.
  Common identity protocols provide for a standardized and more stable identifier for such applications, and these protocol-specific identifiers should be used whenever possible; where using a protocol-specific identifier is not possible, the `eduPersonUniqueId` attribute may be an appropriate "neutral" form.
- Syntactically, `ePPN` looks like an email address but is not intended to be a person's published email address, or to be used as an email address. Consumers must not assume this is a valid email address for the individual.

### Syntax

In general Unicode characters are allowed. In LDAP, this data type implies UTF-8 encoding, and such characters are permitted. However, to reduce the risk of application errors, it is recommended that values contain only characters that could occur in account or login user names.
While the UTF-8 encoding will often be appropriate, the specific encoding depends on the technology involved, and may not be limited to UTF-8 when more than LDAP is involved.

## 2.4.9. Scoped affiliation

| | |
|---|---|
| Name | `eduPersonScopedAffiliation` |
| Description | The person's affiliation within a particular security domain |
| Vocabulary | see controlled vocabulary for `eduPersonAffiliation` |
| References | [eduPerson] |
| OIDC | n/a |
| 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` |

### Definition

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` .
- The `scope` portion MUST be the administrative domain to which the affiliation applies. 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 regular expression processing.

### Permissible values

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.

### 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.

#### Important

- In SWITCHaai, the value for the `scope` portion MUST be the same as the user's `swissEduPersonHomeOrganization` attribute value.

### 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.

## 2.4.10. Targeted ID

| Name | `eduPersonTargetedID` |
|---|---|
| Description | A persistent, non-reassigned, opaque identifier for a principal |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [SAML-core] |
| OIDC | n/a |
| 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` |

### Note

"`eduPersonTargetedID` is DEPRECATED in [eduPerson] 2020-01 and will be marked as obsolete in a future version of this specification.
Its equivalent definition in SAML 2.0 has been replaced by a new specification for standard Subject Identifier attributes[SAML-subject-id], one of which ( `pairwise-id` ) is a direct replacement for this identifier with a simpler syntax and safer comparison rules.
Existing use of this attribute in SAML 1.1 or SAML 2.0 should be phased out in favor of the new Subject Identifier attributes."

### Definition

`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 (for which SAML V2.0 uses the term "Affiliation", not to be confused with the ordinary eduPerson use of the term).

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.

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.

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.

More specific requirements and guidance follows.

**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.

**Human Palatability**

> This attribute does not meet requirements for human palatability or readability. It is ill-suited for display to end users or administrators, and is not useful for provisioning accounts ahead of initial access by users since the value will rarely

be known by users or administrators. It may be accompanied by other attributes more suited to such purposes, in which case its privacy properties are presumably of no interest, but the lack of reassignment often is.

### *Example applications*

- 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).

## 2.4.11. Assurance profile

| | |
|---|---|
| Name | `eduPersonAssurance` |
| Description | Set of URIs that assert compliance with specific standards for identity assurance |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson] |
| OIDC | n/a |
| 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`<br>`http://idm.example.org/LOA#sample` |

### Definition

Set of URIs that assert compliance with specific standards for identity assurance.

### Notes

- This multivalued 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 multivalued 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*

- 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.

## 2.4.12. eduPerson unique ID

| | |
|---|---|
| Name | `eduPersonUniqueId` |
| Description | A long-lived, non re-assignable, omnidirectional identifier<br>The international version of the `swissEduPersonUniqueID` |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.5923.1.1.1.13` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `28c5353b8bb34984a8bd4169ba94c606@foo.edu` |

### Definition

A long-lived, non re-assignable, omnidirectional identifier suitable for use as a principal identifier by authentication providers or as a unique external key by applications.

This identifier represents a specific principal in a specific identity system. Values of this attribute MUST be assigned in such a manner that no two values created by distinct identity systems could collide. This identifier is permanent, to the extent that the principal is represented in the issuing identity system.
Once assigned, it MUST NOT be reassigned to another principal. This identifier is meant to be freely sharable, is public, opaque, and SHOULD remain stable over time regardless of the nature of association, interruptions in association, or complexity of association by the principal with the issuing identity system. When possible, the issuing identity system SHOULD associate any number of principals associated with a single person with a single value of this attribute.

This identifier is scoped and of the form `uniqueID@scope`.
The `uniqueID` portion MUST be unique within the context of the issuing identity system and MUST contain only alphanumeric characters (`a-z`, `A-Z`, `0-9`). The length of the `uniqueID` portion MUST be less than or equal to 64 characters.
The `scope` portion MUST be the administrative domain of the identity system where the identifier was created and assigned. The `scope` portion MAY contain any Unicode character. The length of the `scope` portion MUST be less than or equal to 256 characters. Note that the use of characters outside the seven-bit ASCII set or extremely long values in the `scope` portion may cause issues with interoperability.

Relying parties SHOULD NOT treat this identifier as an email address for the principal as it is unlikely (though not precluded) for it to be valid for that purpose. Most organizations will find that existing email address values will not serve well as values for this identifier.

### Important

- In SWITCHaai use `swissEduPersonUniqueID` if a non-targeted identifier is required.
- For interfederation use, `eduPersonUniqueId` might be suitable, however, `subject-id` would be better.
- Due to the `caseIgnoreMatch` matching rule from the LDAP schema one SHOULD only use uppercase OR lowercase characters to avoid potential clashes.

### *Example applications*

- Controlling access to resources where it is important to ensure a unique stable identifier for a principal that will be unique across time.

## 2.4.13. ORCID identifier

| | |
|---|---|
| Name | `eduPersonOrcid` |
| Description | ORCID iDs are persistent digital identifiers for individual researchers |
| Vocabulary | see permissible values below |
| References | [eduPerson], [ORCID] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.5923.1.1.1.16` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `https://orcid.org/0000-0002-1825-0097`<br>`https://orcid.org/0000-0002-1694-233X` |

### Definition

ORCID iDs are persistent digital identifiers for individual researchers. Their primary purpose is to unambiguously and definitively link them with their scholarly work products. ORCID iDs are assigned, managed and maintained by the ORCID organization: ➟ https://orcid.org

### Permissible values

Values MUST be valid ORCID identifiers in the ORCID-preferred URL representation.

### Semantics

Each value represents an ORCID identifier registered with ORCID.org as belonging to the principal.

## 2.4.14. Member of

| | |
|---|---|
| Name | `isMemberOf` |
| Description | The values of `isMemberOf` are identifiers for groups to which the containing entity belongs |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduMember] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.5923.1.5.1.1` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `https://toolbox.switch.ch/sig-mobile-wg`<br>`Stanford:faculty:emeritus` |

### Definition

The values of `isMemberOf` are identifiers for groups to which the containing entity belongs.

### Permissible values

If the context requires global uniqueness, well-formed URIs are recommended.

### Semantics

The presence of a group identifier as a value of `isMemberOf` implies that the containing entity is a member of the identified group.

#### *Example applications*

Controlling access to resources

# 2.5. SCHAC Attributes

## 2.5.1. SCHAC home organization

| | |
|---|---|
| Name | `schacHomeOrganization` |
| Description | A person's home organization using the domain name of the organization |
| Vocabulary | Domain name according to RFC 1035 |
| References | [SCHAC] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.25178.1.2.9` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `tut.fi` |

### Definition

Issuers of `schacHomeOrganization` attribute values via SAML are strongly encouraged to publish matching `<shibmd:Scope>` elements as part of their IdP's SAML metadata.

Relaying Parties recieving `schacHomeOrganization` values via SAML are strongly encouraged to check attribute values against the Issuer's published `<shibmd:Scope>` elements in SAML metadata, and may discard any non-matching values.

### Important

- In SWITCHaai, use only `swissEduPersonHomeOrganization` .
- For interfederation use, `schacHomeOrganization` is suitable.

## 2.5.2. SCHAC home organization type

| | |
|---|---|
| Name | `schacHomeOrganizationType` |
| Description | Type of a home organization |
| Vocabulary | see permissible values below |
| References | [SCHAC] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.25178.1.2.10` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `urn:schac:homeOrganizationType:ch:university`<br>`urn:schac:homeOrganizationType:eu:educationalInstitution`<br>`urn:schac:homeOrganizationType:int:other` |

### Permissible values

Format:

`urn:schac:homeOrganizationType:<country-code>:<string>`

`<country-code>` = `int`

`<string>` MUST be registered in the [SCHAC-URN-Registry]

`<country-code>` = valid two-letter [ISO3166-1_alpha-2] country code

`<string>` from a nationally controlled vocabulary, published through the URI identified at the [SCHAC-URN-Registry]

#### Important

- In SWITCHaai, use only `swissEduPersonHomeOrganizationType` .
- For interfederation use, `schacHomeOrganizationType` is suitable.

## 2.5.3. SCHAC country of citizenship

| | |
|---|---|
| Name | `schacCountryOfCitizenship` |
| Description | The (claimed) countries of citizenship for the subject it is associated with |
| Vocabulary | Two letter country codes specified in ISO 3166-1 |
| References | [SCHAC], [ISO3166-1_alpha-2] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.25178.1.2.5` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `es` |

## 2.5.4. SCHAC personal unique code

| | |
|---|---|
| Name | `schacPersonalUniqueCode` |
| Description | Specifies a “unique code” for the subject it is associated with |
| Vocabulary | see permissible values below |
| References | [SCHAC], [ISO3166-1_alpha-2] |
| OIDC | Claim: `schacPersonalUniqueCode`<br>Type: JSON array<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| OID | `1.3.6.1.4.1.25178.1.2.14` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `urn:schac:personalUniqueCode:int:esi:HR:xxxxxxxxxx`<br>`urn:schac:personalUniqueCode:int:esi:example.edu:xxxxxxxxxx`<br>`urn:schac:personalUniqueCode:fi:tut.fi:hetu:010161-995A` |

### Definition

Specifies a “unique code” for the subject it is associated with. Its value does not necessarily correspond to any identifier outside the scope of the directories using this schema.

This might be Student number, Employee number,...

### Permissible values

Format:

`urn:schac:personalUniqueCode:<country-code>:<string>`

`<country-code>` = valid two-letter [ISO3166-1_alpha-2] country code

`<string>` a namespace specific string as defined in [RFC8141] but case-insensitive, from a nationally controlled vocabulary, published through the URI identified at the [SCHAC-URN-Registry].

`<country-code>` = `int`

`<string>` MUST be registered in the [SCHAC-URN-Registry]

### Notes

- The European Student Identifier [ESI] uses `schacPersonalUniqueCode` as container.

# 2.6. Other Common Person Attributes

## 2.6.1. Common name

| Name | `commonName` (`cn`) |
|---|---|
| Description | The names of an object |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4519] |
| OIDC | n/a |
| OID | `2.5.4.3` |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | `Mary Francis Xavier` |

### Definition

From[RFC4519]: "The `cn` (`commonName` in X.500) attribute type contains names of an object. Each name is one value of this multivalued attribute. If the object corresponds to a person, it is typically the person's full name."

### Notes

- This attribute is often overloaded in the sense that many applications act as if this were "their" attribute, and therefore add values to this attribute as they see fit. Because of that it is impossible to give a precise and accurate definition of what this field means.

## 2.6.2. Display name

| Name | `displayName` |
|---|---|
| Description | The name(s) that should appear in white-pages-like applications |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC2798] |
| OIDC | Claim: `name`<br>Type: string<br>Scope: `profile` |
| OID | `2.16.840.1.113730.3.1.241` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `Jack Dougherty` |

### Definition

The name(s) that should appear in white-pages-like applications for this person.

From [RFC2798] description: "preferred name of a person to be used when displaying entries."

### Notes

- Cn (common name) is multivalued and overloaded to meet the needs of multiple applications. displayName is a better candidate for use in DoD white pages and configurable email clients.

## 2.6.3. Employee number

| | |
|---|---|
| Name | `employeeNumber` |
| Description | Numerically identifies an employee within an organization |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [RFC2798] |
| OIDC | n/a |
| OID | `2.16.840.1.113730.3.1.3` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `400345`<br>`74622225` |

### Definiton

Numeric or alphanumeric identifier assigned to a person, typically based on order of hire or association with an organization. Single valued.

#### Important

- The use case for this attribute is internal to the issuing home organization, mainly for internal administrative purposes.
  It MUST be unique within the issuing home organization but will not be unique across organizations.
- `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.

## 2.6.4. Given name

| | |
|---|---|
| Name | `givenName` |
| Description | Given name of a person |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4519] |
| OIDC | Claim: `given_name`<br>Type: string<br>Scope: `profile` |
| OID | `2.5.4.42` |
| LDAP Syntax | Directory String |
| # of values | single (multi in[RFC4519], see 'Important') |
| Example values | `Hans-Peter`<br>`Hans Jürg`<br>`René` |

### Definition

From [RFC4519] description: "The 'givenName' attribute type contains name strings that are the part of a person's name that is not their surname. Each string is one value of this multivalued attribute."

#### Important

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

## 2.6.5. Private phone number

| Name | homePhone |
|---|---|
| Description | Private phone number |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4524] |
| OIDC | Claim: swissEduPersonHomePhone<br>Type: JSON array<br>Scope: https://login.eduid.ch/authz/User.Read |
| OID | 0.9.2342.19200300.100.1.20 |
| LDAP Syntax | Telephone Number |
| # of values | multi |
| Example values | +41 44 345 6789<br>+44 71 123 4567 |

### Definition

From[RFC4524]: "The homePhone attribute specifies home telephone numbers associated with a person."

### Notes

- Attribute values should comply with the international format specified in ITU Recommendation [E.123] e.g., +44 71 123 4567.

## 2.6.6. Home postal address

| Name | homePostalAddress |
|---|---|
| Description | Home address of the user |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4524] |
| OIDC | n/a |
| OID | 0.9.2342.19200300.100.1.39 |
| LDAP Syntax | Postal Address |
| # of values | multi |
| Example values | Bernerstrasse 45$8048 Zürich$Switzerland<br>ch. des Vignes 59$1260 Nyon$Switzerland |

### Definition

From[RFC4524]: "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. (Note: It is not intended that the directory service enforce these limits.)"

#### Important

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

## 2.6.7. E-mail

| Name | `mail` |
|---|---|
| Description | Preferred address for the "To:" field of e-mail to be sent to this person |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4524] |
| OIDC | Two claims get derived from `mail`:<br>Claim: `email`<br>Type: string<br>Scope: `email`<br>Claim: `email_verified`, its value is always `true`.<br>Type: boolean<br>Scope: `email` |
| OID | `0.9.2342.19200300.100.1.3` |
| LDAP Syntax | IA5 String {256} |
| # of values | multi |
| Example values | `peter.meier@uzh.ch`<br>`dumbledore@hsww.wiz` |

### Definition

From[RFC4524]: "The `mail` (rfc822mailbox) attribute type holds Internet mail addresses in Mailbox [RFC5321] form (e.g., `user@example.com`)."

### Important

- In 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.
  More e-mail addresses might be provided in `swissEduPersonOrganizationalMail` `swissEduPersonPrivateMail`

## 2.6.8. Mobile phone number

| Name | `mobile` |
|---|---|
| Description | Mobile phone number |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4524] |
| OIDC | Claim: `swissEduPersonMobilePhone`<br>Type: JSON array<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| OID | `0.9.2342.19200300.100.1.41` |
| LDAP Syntax | Telephone Number |
| # of values | multi |
| Example values | `+41 79 345 6789`<br>`+44 71 123 4567` |

### Definition

From RFC4524: "The `mobile` attribute type specifies a mobile telephone number associated with a person."

### Notes

- Attribute values should comply with the international format specified in ITU Recommendation[E.123]: e.g., `+44 71 123 4567`.

## 2.6.9. Organizational unit

| Name | ou |
|---|---|
| Description | Organizational unit(s) |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4519] |
| OIDC | n/a |
| OID | 2.5.4.11 |
| LDAP Syntax | Directory String |
| # of values | multi |
| Example values | Faculty Senate |

### Definition

According to X.520(2000): "The Organizational Unit Name attribute type specifies an organizational unit. When used as a component of a directory name it identifies an organizational unit with which the named object is affiliated."

## 2.6.10. Business postal address

| Name | postalAddress |
|---|---|
| Description | Campus or office address |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4519] |
| OIDC | n/a |
| OID | 2.5.4.16 |
| LDAP Syntax | Postal Address |
| # of values | multi |
| Example values | ETH Zentrum$8092 Zürich$Switzerland<br>Quartier UNIL-Sorge$Bâtiment Amphimax$1015 Lausanne$Switzerland |

### Definition

From[RFC4519]: "The postalAddress attribute type contains addresses used by a Postal Service to perform services for the object. Each address is one value of this multivalued attribute."

### Important

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

## 2.6.11. Preferred language

| Name | preferredLanguage |
|---|---|
| Description | Preferred written or spoken language for a person |
| Vocabulary | see permissible values below |
| References | [eduPerson], [RFC2798] |
| OIDC | Claim: locale<br>Type: string<br>Scope: profile |
| OID | 2.16.840.1.113730.3.1.39 |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | de-CH<br>en<br>it<br>fr-CH |

### Definition

From[RFC2798]: "Used to indicate an individual's preferred written or spoken language."

### Permissible values

The syntax for `preferredLanguage` is derived from[BCP47]:

```
langtag  = language ["-" region]
language = 2*3ALPHA ; shortest ISO 639 code
region   = 2ALPHA ; ISO 3166 code
```

The language tag is composed of a primary language (two-letter [ISO639] language code) and an optional region (two-letter [ISO3166-1_alpha-2] country code).

## 2.6.12. Surname

| Name | `surname (sn)` |
|---|---|
| Description | Surname or family name |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4519] |
| OIDC | Claim: `family_name`<br>Type: string<br>Scope: `profile` |
| OID | `2.5.4.4` |
| LDAP Syntax | Directory String |
| # of values | single (multi in[RFC4519], see 'Important') |
| Example values | `Meier-Müller`<br>`Bauchière`<br>`von Roten` |

### Definition

From[RFC4519]: "The `sn` (`surname` in X.500) attribute type contains name strings for the family names of a person."

From[eduPerson]: "If the person has a multi-part surname (whether hyphenated or not), store both 1) the whole surname including hyphens if present and 2) each component of a hyphenated surname as a separate value in this multivalued attribute. That yields the best results for the broadest range of clients doing name searches."

### Important

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

## 2.6.13. Business phone number

| Name | `telephoneNumber` |
|---|---|
| Description | Office/campus phone number |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [eduPerson], [RFC4519] |
| OIDC | Claim: `swissEduPersonBusinessPhone`<br>Type: JSON array<br>Scope: `https://login.eduid.ch/authz/User.Read` |
| OID | `2.5.4.20` |
| LDAP Syntax | Telephone Number |
| # of values | multi |
| Example values | `+41 44 345 6789`<br>`+44 71 123 4567` |

### Definition

Office/campus phone number of the user.

### Notes

- Attribute values should comply with the international format specified in ITU Recommendation[E.123]: e.g., `+44 71 123 4567`.

## 2.6.14. 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 |
| References | [eduPerson], [RFC4519] |
| OIDC | n/a |
| OID | `0.9.2342.19200300.100.1.1` |
| LDAP Syntax | Directory String |
| # of values | single (multi in[RFC4519], see 'Important') |
| Example values | `pmuster`<br>`stud_05999123` |

### Definition

From[RFC4519]: "The `uid` attribute type contains computer system login names associated with the object."

`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' attribute `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.

### Important

- `uid`, contrary to common belief, is multivalued.
  In 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.

## 2.6.15. User ID number

| Name | `uidNumber` |
|---|---|
| Description | An integer uniquely identifying a user in an administrative domain |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [RFC2307], [nis-schema] |
| OIDC | n/a |
| OID | `1.3.6.1.1.1.1.0` |
| LDAP Syntax | Integer |
| # of values | single |
| Example values | `912`<br>`41032` |

### Definition

The `uidNumber` is the user's integer identification number, associated with the user's login name in the `uid` attribute."

### Important

- `uidNumber` is security sensitive. This attribute SHOULD NOT be provided to resources outside the issuing home organization. It is mostly anyhow not unique across organizations.

## 2.6.16. User principal name

| Name | `userPrincipalName` |
|---|---|
| Description | An Internet-style login name for a user |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [MSUPN] |
| OIDC | n/a |
| OID | `1.2.840.113556.1.4.656` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `peter.meier@uzh.ch`<br>`dumbledore@hsww.wiz` |

### Definition

The `UserPrincipalName` is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than the distinguished name and easier to remember. By convention, this should map to the user email name."

## 2.6.17. SSH public key

| Name | `sshPublicKey` |
|---|---|
| Description | A ssh public key |
| Vocabulary | OpenSSH public key file format |
| References | [LDAP-OpenSSH], [OpenSSH_Public_Key_File_Format] |
| OIDC | n/a |
| OID | `1.3.6.1.4.1.24552.500.1.1.1.13` |
| LDAP Syntax | Octet String |
| # of values | multi |
| Example values | `ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAv45J[...]BOFus=` |

### Definition

A `sshPublicKey` value needs to be encoded in the OpenSSH public key file format as documented in [OpenSSH_Public_Key_File_Format] in section 'Authorized Keys File Format'.

## 2.6.18. Pairwise subject ID

| Name | `pairwise-id` |
|---|---|
| Description | This is a long-lived, non-reassignable, uni-directional identifier suitable for use as a unique external key specific to a particular relying party. Its value for a given subject depends upon the relying party to whom it is given, thus preventing unrelated systems from using it as a basis for correlation. |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [SAML-subject-id] |
| OIDC | n/a |
| OID | n/a |
| URN | `urn:oasis:names:tc:SAML:attribute:pairwise-id` |
| LDAP Syntax | Directory String |
| # of v alues | single |
| Example values | `HATINBZGYZDOZBZMZRGKNZTME3TMNBXGYYTIOBYGMYWKNLFMYYDAYY=@example.edu` |

### Definition

The value consists of two substrings (termed a `unique ID` and a `scope` in the remainder of this definition) separated by an @ symbol (ASCII 64) as an inline delimiter. The `unique ID` consists of 1 to 127 ASCII characters, each of which is either an alphanumeric ASCII character, an equals sign (ASCII 61), or a hyphen (ASCII 45). The first character MUST be alphanumeric.
The `scope` consists of 1 to 127 ASCII characters, each of which is either an alphanumeric ASCII character, a hyphen (ASCII 45), or a period (ASCII 46). The first character MUST be alphanumeric.
The scope deliberately resembles, and often is, a DNS domain name, but is drawn from a more limited character set due to case folding considerations, and no attempt is made to limit the allowable grammar to legal domain names (e.g., it allows consecutive periods).

The ABNF [RFC5234] grammar is therefore:

```
<value> = <uniqueID> "@" <scope>

<uniqueID> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "=" / "-")

<scope> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "-" / ".")
```

Value comparison MUST be performed case-insensitively (that is, values that differ only by case are the same, and MUST refer to the same subject).
In the grammar above, the ALPHA production contains characters that can be expressed in both upper and lower case. It is RECOMMENDED that the unique ID be exclusively upper- or lower-case when expressed or stored to facilitate ease of comparison.
Further, it is RECOMMENDED that scopes be expressed in lower case, since they are generally chosen independently of more “entrenched” decisions and are frequently, though not required to be, in the form of DNS domains.

### Important

- The `pairwise-id` is the replacement for the deprecated `eduPersonTargetedID` .

## 2.6.19. Subject ID

| Name | `subject-id` |
|---|---|
| Description | This is a long-lived, non-reassignable, omni-directional identifier suitable for use as a globally-unique external key. Its value for a given subject is independent of the relying party to whom it is given. |
| Vocabulary | not applicable, no controlled vocabulary |
| References | [SAML-subject-id] |
| OIDC | n/a |
| OID | n/a |
| URN | `urn:oasis:names:tc:SAML:attribute:subject-id` |
| LDAP Syntax | Directory String |
| # of values | single |
| Example values | `idm123456789@example.com` |

### Definition

The value consists of two substrings (termed a `unique ID` and a `scope` in the remainder of this definition) separated by an `@` symbol (ASCII 64) as an inline delimiter. The `unique ID` consists of 1 to 127 ASCII characters, each of which is either an alphanumeric ASCII character, an equals sign (ASCII 61), or a hyphen (ASCII 45). The first character MUST be alphanumeric.
The `scope` consists of 1 to 127 ASCII characters, each of which is either an alphanumeric ASCII character, a hyphen (ASCII 45), or a period (ASCII 46). The first character MUST be alphanumeric.
The scope deliberately resembles, and often is, a DNS domain name, but is drawn from a more limited character set due to case folding considerations, and no attempt is made to limit the allowable grammar to legal domain names (e.g., it allows consecutive periods).

The ABNF [RFC5234] grammar is therefore:

```
<value> = <uniqueID> "@" <scope>

<uniqueID> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "=" / "-")

<scope> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "-" / ".")
```

Value comparison MUST be performed case-insensitively (that is, values that differ only by case are the same, and MUST refer to the same subject).
In the grammar above, the ALPHA production contains characters that can be expressed in both upper and lower case. It is RECOMMENDED that the unique ID be exclusively upper- or lower-case when expressed or stored to facilitate ease of comparison.
Further, it is RECOMMENDED that scopes be expressed in lower case, since they are generally chosen independently of more “entrenched” decisions and are frequently, though not required to be, in the form of DNS domains.

### Important

- In SWITCHaai, home organizations MUST provide the same value as for `swissEduPersonUniqueID` .

# References


[BCP14] *Key words for use in RFCs to Indicate Requirement Levels* IETF Mar 1997 https://www.rfc-editor.org/info/bcp14

[BCP47] *Tags for Identifying Languages* IETF Sep 2009 https://www.rfc-editor.org/info/bcp47

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

[E.123] *Notation for national and international telephone numbers, e-mail addresses and Web addresses* Feb 2001 https://en.wikipedia.org/wiki/E.123

[eCH-0171] *eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID* 04 April 2014 https://www.ech.ch/standards/60603

[eduIDAffiliationAPI] *SWITCH edu-ID Affiliation API* https://swit.ch/eduIDAffiliationAPI

[eduIDAttributeQuality] *SWITCH edu-ID Attribute Quality* https://swit.ch/eduIDAttributeQuality

[eduIDExtendedAttributeModel] *SWITCH edu-ID Extenced Attribute Model* https://swit.ch/eduIDExtendedAttributeModel

[eduIDServiceDesc] *Service Description SWITCH edu-ID* https://www.switch.ch/edu-id/terms/

[eduIDSpec] *Swiss edu-ID Unique Identifier Specification* https://swit.ch/eduidspec

[eduMember] *eduMember* http://doi.org/10.26869/TI.111.1

[eduPerson] *eduPerson Object Class Specification (202111)* REFEDS Schema Board Mar 2020 https://wiki.refeds.org/display/STAN/eduPerson

[ESI] *European Student Identifier* https://wiki.geant.org/display/SM/European+Student+Identifier

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

[Internet2] *Internet2* https://internet2.edu/

[ISO639] *Codes for the representation of names of languages* https://en.wikipedia.org/wiki/ISO_639

[ISO3166-1_alpha-2] *Two-letter Country Codes* https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2

[ISO5218] *Information Interchange - Representation of Human Sexes* https://en.wikipedia.org/wiki/ISO/IEC_5218

[ISO15693] *Information technology -- Radio frequency identification for item management -- Unique identification for RF tags* Aug 2009 https://en.wikipedia.org/wiki/ISO/IEC_15693

[LDAP-OpenSSH] *SSH Public Keys in OpenLDAP* http://pig.made-it.com/ldap-openssh.html

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

[MSUPN] *User-Principal-Name attribute* https://docs.microsoft.com/en-us/windows/win32/adschema/a-userprincipalname

[nis-schema] *OpenLDAP distributed nis.schema File* https://www.openldap.org/doc/admin25/schema.html https://git.openldap.org/openldap/openldap/-/blob/e1c90d0977d389db05803c127d45b39c89a5ac2f/servers/slapd/schema/nis.schema

[OIDC-core] *OpenID Connect Core 1.0* OpenID Foundation Nov 2014 https://openid.net/specs/openid-connect-core-1_0.html

[OIDC_Scopes_and_Claims] *OIDC Scopes and Claims for SWITCH edu-ID* SWITCH https://www.switch.ch/edu-id/docs/services/openid-connect/scopes/

[OpenSSH_Public_Key_File_Format] *OpenSSH Public Keys File Format* OpenSSH Jun 2021 https://man.openbsd.org/sshd.8#AUTHORIZED_KEYS_FILE_FORMAT

[ORCID] *Structure of the ORCID Identifier* https://support.orcid.org/hc/en-us/articles/360006897674

[RFC2307] *An Approach for Using LDAP as a Network Information Service* IETF Mar 1998 https://www.rfc-editor.org/info/rfc2307

[RFC2798] *Definition of the inetOrgPerson LDAP Object Class* IETF Apr 2000 https://www.rfc-editor.org/info/rfc2798

[RFC2849] *The LDAP Data Interchange Format (LDIF) - Technical Specification* IETF Jun 2000 https://www.rfc-editor.org/info/rfc2849

[RFC3339] *Date and Time on the Internet: Timestamps* IETF Jul 2002 https://www.rfc-editor.org/info/rfc3339

[RFC3986] *Uniform Resource Identifier (URI): Generic Syntax* IETF Jan 2005 https://www.rfc-editor.org/info/rfc3986

[RFC4122] *A Universally Unique IDentifier (UUID) URN Namespace* IETF Jul 2005 https://www.rfc-editor.org/info/rfc4122

[RFC4512] *Lightweight Directory Access Protocol (LDAP): Directory Information Models* IETF Jun 2006 https://www.rfc-editor.org/info/rfc4512

[RFC4517] *Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules* IETF Jun 2006 https://www.rfc-editor.org/info/rfc4517

[RFC4519] *Lightweight Directory Access Protocol (LDAP): Schema for User Applications* IETF Jun 2006 https://www.rfc-editor.org/info/rfc4519

[RFC4524] *COSINE LDAP/X.500 Schema* IETF Jun 2006 https://www.rfc-editor.org/info/rfc4524

[RFC4648] *The Base16, Base32, and Base64 Data Encodings* IETF Oct 2006 https://www.rfc-editor.org/info/rfc4648

[RFC5234] *Augmented BNF for Syntax Specifications: ABNF* IETF Jan 2008 https://www.rfc-editor.org/info/rfc5234

[RFC5321] *Simple Mail Transfer Protocol* IETF Oct 2008 https://www.rfc-editor.org/info/rfc5321

[RFC5322] *Internet Message Format* IETF Oct 2008 https://www.rfc-editor.org/info/rfc5322

[RFC8141] *URN Syntax* IETF Apr 2017 https://www.rfc-editor.org/info/rfc8141

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

[SAML-subject-id] *SAML V2.0 Subject Identifier Attributes Profile Version 1.0* OASIS Jan 2019 https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html

[SCHAC] *SCHema for ACademia: Specification* SCHAC Specification REFEDS May 2022 https://wiki.refeds.org/display/STAN/SCHAC+Releases

[SCHAC-URN-Registry] *SCHema for ACademia: URN Registry* REFEDS https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry

[SERI-edu] *State Secretariat for Education, Research and Innovation: Swiss education system* SERI - Swiss Education System https://www.sbfi.admin.ch/sbfi/en/home/education/swiss-education-area/swiss-education-system.html

[SIUS-SHIS] *Service d'Information Universitaire Suisse, Schweizerisches Hochschulinformationssystem* SIUS/SHIS https://www.bfs.admin.ch/bfs/en/home/statistics/education-science/surveys/sahs.html

[Swiss_ENIC] *Swiss ENIC (European Network of National Information Centres on Academic Recognition and Mobility)* https://www.swissuniversities.ch/en/service/recognition/swiss-enic

[uasStaffCategory] *uasStaffCategory.csv* https://www.switch.ch/aai/docs/uasStaffCategory.csv

[uasStudyBranch1] *uasStudyBranch1.csv* https://www.switch.ch/aai/docs/uasStudyBranch1.csv

[uasStudyBranch2] *uasStudyBranch2.csv* https://www.switch.ch/aai/docs/uasStudyBranch2.csv

[uasStudyBranch3] *uasStudyBranch3.csv* https://www.switch.ch/aai/docs/uasStudyBranch3.csv

[uasStudyLevel] *uasStudyLevel.csv* https://www.switch.ch/aai/docs/uasStudyLevel.csv

[uniStaffCategory] *uniStaffCategory.csv* https://www.switch.ch/aai/docs/uniStaffCategory.csv

[uniStudyBranch1] *uniStudyBranch1.csv* https://www.switch.ch/aai/docs/uniStudyBranch1.csv

[uniStudyBranch2] *uniStudyBranch2.csv* https://www.switch.ch/aai/docs/uniStudyBranch2.csv

[uniStudyBranch3] *uniStudyBranch3.csv* https://www.switch.ch/aai/docs/uniStudyBranch3.csv

[uniStudyLevel] *uniStudyLevel.csv* https://www.switch.ch/aai/docs/uniStudyLevel.csv

[VZV_Art84] *Verkehrszulassungsverordnung VZV Art. 84 Nummerierungssystem* https://www.fedlex.admin.ch/eli/cc/1976/2423_2423_2423/de#art_84

# A. Code lists

Changes to earlier versions of the code lists are documented in the https://www.switch.ch/aai/docs/code_list_changes.txt file.

## A.1. staffCategory code lists

`swisseduPersonstaffCategory`

- Universities: https://www.switch.ch/aai/docs/unistaffCategory.csv
- Universities of applied sciences: https://www.switch.ch/aai/docs/uasstaffCategory.csv

## A.2. studyBranch code lists

`swisseduPersonStudyBranch1`

- Universities: https://www.switch.ch/aai/docs/uniStudyBranch1.csv
- Universities of applied sciences: https://www.switch.ch/aai/docs/uasStudyBranch1.csv

`swisseduPersonStudyBranch2`

- Universities: https://www.switch.ch/aai/docs/uniStudyBranch2.csv
- Universities of applied sciences: https://www.switch.ch/aai/docs/uasStudyBranch2.csv

`swisseduPersonStudyBranch3`

- Universities: https://www.switch.ch/aai/docs/uniStudyBranch3.csv
- Universities of applied sciences: https://www.switch.ch/aai/docs/uasStudyBranch3.csv

## A.3. studyLevel code lists

`swisseduPersonStudyLevel`

- Universities: https://www.switch.ch/aai/docs/uniStudyLevel.csv
- Universities of applied sciences: https://www.switch.ch/aai/docs/uasStudyLevel.csv

# B. Changelog

## Revision History

Revision 1.7.2 2023-02-14

- add chapter 1.3: “Protocol Support” as well as OIDC specific details like claim names, types and scopes for the attributes that can be released via OIDC protocol.

Revision 1.7.1 2022-09-21

- correct a copy & paste error in the `schacPersonalUniqueCode` examples

Revision 1.7 2022-08-17

- document title modified: 'SWITCHaai Attribute Specification' instead of 'Attribute Specification'
- new swissEduPerson & swissLibraryPerson attributes added: `swissEduPersonMinimumAgeCategory`, `swissEduPersonOrganizationalMail`, `swissEduPersonPrivateMail`, `swissLibraryPersonResidenceCanton`
- new SWITCH edu-ID attributes added: `swissEduIDAssociatedMail`, `swissEduIDAssuranceLevel`, `swissEduIDLinkedAffiliation`, `swissEduIDLinkedAffiliationMail`, `swissEduIDLinkedAffiliationUniqueID`, `swissEduIDUsage1y`
- new SCHAC & other attributes added: `schacCountryOfCitizenship`, `schacPersonalUniqueCode`, `pairwise-id`, `subject-id`, `sshPublicKey`, `uidNumber`, `userPrincipalName`
- update `mail` with references to `swissEduPersonOrganizationalMail` and `swissEduPersonPrivateMail`
- update `swissEduPersonDateOfBirth` to clarify the use of `full-date` format without the dashes and a reference to `swissEduPersonMinimumAgeCategory`
- update `swissEduPersonUniqueID` with reference to `caseIgnoreMatch` and use of only upper or lower case characters, or to use a Base32 hash
- update `swissEduID` with MUST for lower case hex digits only
- adopts the changes from eduPerson(201602) v4.1.0 to eduPerson(202208) v4.4.0
- update `eduPersonOrcid` example values and reference link
- deprecate `eduPersonTargetedID` in favor of `pairwise-id`
- correct `schacHomeOrganizationType` example value `urn:schac:homeOrganizationType:eu:educationalInstitution`. It was corrected in the SCHAC URN registry in April 2018.
- drop former chapter 2 "Implementing the Attribute Specification". The SWITCHaai Federation Policy covers the obligations. The policy is part of the "Service Description SWITCH edu-ID" [eduIDServiceDesc]
- new Appendix A, *Code lists* replaces the former appendices A to D

Revision 1.6 2017-04-11

- list of attributes sorted by origin
- more consistent format for the attribute descriptions
- `swissEduPersonUniqueID` : recommends to use only alphanumeric characters for the local part for compatibility with `eduPersonUniqueId`, use only upper OR lower case characters
- `swissLibraryPersonAffiliation` : sets friendly name to 'Library Patron Affiliation'
- `swissLibraryPersonResidence` : corrects the vocabulary to ISO 3166-1, sets friendly name to 'Library Patron Residence'
- adopts the changes from eduPerson(201310) to eduPerson(201602)
- `eduPersonAssurance` : renames the friendly name from 'Assurance level' to 'Assurance profile'
- `eduPersonNickname` : corrects the '# of values' from 'single' to 'multi'
- adds attributes: `eduPersonOrcid`, `isMemberOf`, `ou`, `schacHomeOrganization`, `schacHomeOrganizationType`
- `postalAddress`, `homePostalAddress` : updates the examples to current recommomendations (no ISO country codes)
- `preferredLanguage` : corrects the syntax from 'Integer {1}' to 'Directory String' and fixes the examples where the region codes were in lower case

Revision 1.5.0 2015-09-01

- dropped the 'Usage' from all attribute descriptions
- new attributes: `swissLibraryPersonAffiliation`, `swissLibraryPersonResidence`, `eduPersonUniqueId`, `swissEduID`
- adopts the changes from eduPerson(201203) to eduPerson(201310)

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`, `swissEduPerseoneEntitlement`, `mobileTelephoneNumber`: attributename changed
- `swissEduPersonDateOfBirth`, `swissEduPersonGender`: format changed
- code lists for UAS study branches added (appendix B)

Revision 0.6 2002-11-07

Initial version