funetEduPersonSchema2dot2

Introduction

The main purpose of funetEduPerson schema is to serve Haka federation, the federation of Finnish higher education and research institutions, in inter-organisational exchange of attribute assertions regarding authenticated users. The schema contains also attributes of organisations and organisational units.

The schema does not preclude individual Identity and Service Providers from using also other attributes on bilateral basis. However, it is intended, that in the long run attributes with generic use in Haka federation will be included in funetEduPerson.

funetEduPerson schema has its origins in LDAP directories, and institutions may decide to use the schema in their enterprise directories as well, extended with locally defined attributes, if necessary. However, due to privacy concerns, institutions may decide not to make personal data in the enterprise directory visible outside the campus network.

Chapter 2 defines attributes describing individuals. The attributes are derived from common schemas (such as Person and InetOrgPerson) and schemas well-known in education (eduPerson, Schac) and supplemented with specialities of the Finnish higher education. Chapter 3 contains attributes for objects representing organisations and organisational units. The attributes are borrowed from the eduOrg schema of Internet2.

If the vocabulary of an attribute is not specified, the language used in attribute values can Finnish, Swedish or English.

Borrowed text is in italic.

> Haka federation's interpretation and use of international attributes is highlighted in gray background.

Changed in 2.2 colored in blue

Attributes for persons

Following attributes are mandatory:

- cn
- sn
- displayName
- givenName
- eduPersonPrincipalName

- mail
- schacHomeOrganization
- schacHomeOrganizationType

Mandatory attributes must be available for each user. However, this does not mean that they are always released to any service. In Haka federation, there are mechanisms in place to make sure that only relevant attributes are released to a service.

In addition to mandatory attributes in Haka, an organisation SHOULD make attributes defined as recommended in eduGAIN Policy Framework Attribute Profile available for each user where applicable.

Attribute Profile: https://www.geant.org/Services/Trust_identity_and_security/eduGAIN/Documents/Resources/GN3-11-012%20eduGAIN_attribute_profile.pdf

Supplement attributes in funetEduPerson

Superseded attributes

Superseded attributes from ver 1.0 listed in table.

Attribute	Defined in	Superseded by
funetEduPersonHomeOrganization	ver 1.0	SchacHomeOrganization
funetEduPersonStudentID	ver 1.0	SchacPersonalUniqueCode
funetEduPersonIdentityCode	ver 1.0	schacPersonalUniqueID
funetEduPersonDateOfBirth	ver 1.0	schacDateOfBirth
funetEduPersonTargetDegreeUniversity	ver 1.0	funetEduPersonTargetDegree
funetEduPersonTargetDegreePolytech	ver 1.0	funetEduPersonTargetDegree
funetEduPersonEducationalProgramUniv	ver 1.0	funetEduPersonProgram
funetEduPersonEducationalProgramPolytech	ver 1.0	funetEduPersonProgram
funetEduPersonMajorUniv	ver 1.0	funetEduPersonSpecialisation
funetEduPersonOrientationAlternPolytech	ver 1.0	funetEduPersonSpecialisation

funetEduPersonTargetDegree

Specifies a student's target degree (suoritettava tutkinto) using an appropriate vocabulary.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.11	DirectoryString	Multi	May

Format: URN. Currently a common namespace is defined for codes maintained by Central Statistical Office of Finland (Tilastokeskus):

- urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:stat.fi

  Vocabulary for the namespace: http://www.stat.fi/meta/luokitukset/koulutus/001-2013/index.html

Formerly two common namespaces were defined. These namespaces are deprecated.

- urn:mace:funet.fi:attribute-def:funetEduPersonProgram:university
- urn:mace:funet.fi:attribute-def:funetEduPersonProgram:polytechnic

Institutions may also use their own namespaces and locally defined vocabularies. However, to ensure cross-institutional interoperability, it is encouraged to use the common namespaces and codes whenever possible.

Examples: (Doctor of theology, a code defined by Central Statistical Office)

```
funetEduPersonTargetDegree: urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:stat.fi:827101
```

Examples: (Bachelor of Health Care (Polytechnic) Physiotherapist, a code defined by Central Statistical Office)

```
funetEduPersonTargetDegree: urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:stat.fi:671112
```

Examples: (Erasmus exchange student, a code defined locally by Tampere University of Technology)

```
funetEduPersonTargetDegree: urn:mace:funet.fi:tut.fi:schema:targetDegrees:915
```

funetEduPersonProgram

The educational degree program (tutkinto-ohjelma) using an appropriate vocabulary.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.12	DirectoryString	Multi	May

Format: URN. Currently a common namespace is defined for codes maintained by Central Statistical Office of Finland (Tilastokeskus):

- urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:stat.fi

  Vocabulary for the namespace: http://www.stat.fi/meta/luokitukset/koulutus/001-2013/index.html

Formerly two common namespaces were defined. These namespaces are deprecated.

- urn:mace:funet.fi:attribute-def:funetEduPersonProgram:university
- urn:mace:funet.fi:attribute-def:funetEduPersonProgram:polytechnic

Institutions may also use their own namespaces and locally defined vocabularies. However, to ensure cross-institutional interoperability, it is encouraged to use the common namespaces and codes whenever possible.

Examples: (Education in Social Sciences, a code defined by Central Statistical Office)

```
funetEduPersonProgram: urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:stat.fi:733
```

funetEduPersonSpecialisation

The specialisation option (opintosuunta) of a student using an appropriate vocabulary.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.13	DirectoryString	Multi	May

Format: URN. Currently a common namespace is defined for codes maintained by Central Statistical Office of Finland (Tilastokeskus):

- urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:stat.fi

  Vocabulary for the namespace: http://www.stat.fi/meta/luokitukset/koulutus/001-2013/index.html

Formerly two common namespaces were defined. These namespaces are deprecated.

- urn:mace:funet.fi:attribute-def:funetEduPersonProgram:university
- urn:mace:funet.fi:attribute-def:funetEduPersonProgram:polytechnic

Institutions may also use their own namespaces and locally defined vocabularies. However, to ensure cross-institutional interoperability, it is encouraged to use the common namespaces and codes whenever possible.

Examples: (Specialist Degree in Medicine, a code defined by Central Statistical Office)

```
funetEduPersonSpecialisation: urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:stat.fi:7751
```

Examples: (Bachelor of Engineering (Polytechnic), Industrial Management, a code defined by Central Statistical Office)

```
funetEduPersonSpecialisation: urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:stat.fi:6516
```

funetEduPersonStudyStart

The date when a student started his/her studies (opintojen aloittamispäivä).

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.14	DirectoryString	Multi	May

Format: YYYYMMDD

Examples:

```
funetEduPersonStudyStart: 20050826
```

funetEduPersonPrimaryStudyStart

The date when a student started his/her primary studies (ensisijaisten opintojen aloittamispäivä).

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.15	DirectoryString	Single	May

Format: YYYYMMDD

Single-valued version of funetEduPersonStudyStart. If a student has several rights to study, one can be expressed as the primary one.

Examples:

```
funetEduPersonPrimaryStudyStart: 20050826
```

funetEduPersonStudyToEnd

The date when a student is expected to finish his/her studies, e.g. graduate (arvioitu opintojen päättymispäivä/valmistumispäivä).

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.16	DirectoryString	Multi	May

Format: YYYYMMDD

It is up to the institution to decide how to derive the value of this attribute.

Examples:

```
funetEduPersonStudyToEnd: 20070531
```

funetEduPersonPrimaryStudyToEnd

The date when a student is expected to finish his/her primary studies, e.g. graduate (arvioitu ensisijaisen opinto-oikeuden päättymispäivä /valmistumispäivä).

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.17	DirectoryString	Single	May

Format: YYYYMMDD

Single-valued version of funetEduPersonStudyToEnd. If a student has several rights to study, one can be expressed as the primary one.

It is up to the institution to decide how to derive the value of this attribute.

Examples:

```
funetEduPersonPrimaryStudyToEnd: 20070531
```

funetEduPersonCreditUnits

Number of credit units (opintoviikko) a student has.
In Finland, national credit units (1 cu equals to 40 hours of work) were used before ECTS credit units were adopted in 2005.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.18	DirectoryString	Single	May

The number of credit units a student has.

Notice: this attribute represents the total number of credit units a student has in the institution, not the credit units in a particular degree program. A student may be a degree student in several parallel degree programs at a time, and the credits are assigned to a degree at the time of graduation.

Examples:

```
funetEduPersonCreditUnits: 80
```

funetEduPersonECTS

Number of ECTS (European Credit Transfer System) credit units (opintopiste) a student has.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.19	DirectoryString	Single	May

The number of ECTS credit units a student has.

Notice: this attribute represents the total number of ECTS credit units the student has in the institution, not the credit units in a particular degree program. A student may be a degree student in several parallel degree programs at a time, and the credits are assigned to a degree at the time of graduation.

Examples:

```
funetEduPersonECTS: 140
```

funetEduPersonStudentCategory

Category of a student, based on the target of the studies.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.20	DirectoryString	Multi	May

Vocabulary: bachelor, master, licentiate, doctor, other-degree, visiting-student, exchange-student, qualifying-studies, further-education, open-university, other

- **bachelor:** bachelor's students in universities (yliopistojen alempi korkeakoulututkinto), degree students in polytechnics (ammattikorkeakoulujen ammattikorkeakoulututkinto)
- **master:** master's students in universities (yliopistojen ylempi korkeakoulututkinto), postgraduate students in polytechnics (ammattikorkeakoulujen ylempi ammattikorkeakoulututkinto)
- **licentiate:** licentiate students in universities (yliopistojen tieteelliset jatkotutkinnot: lisensisaatti)
- **doctor:** doctoral students in universities (yliopistojen tieteelliset jatkotutkinnot: tohtori)
- **other-degree:** other students that aim at a degree as laid down by a decree (muut opiskelijat, jotka tähtäävät asetuksella annettuun tutkintoon)
- **visiting-student:** students taking courses in the institution in order to have them included in a degree in another Finnish institution (opiskelija suorittaa korkeakoulussa kursseja sisällyttääkseen ne tutkintoonsa toisessa suomalaisessa korkeakoulussa, mm. JOO)
- **exchange-student:** students taking courses in the institution in order to have them included in a degree in an institution abroad (opiskelija suorittaa korkeakoulussa kursseja sisällyttääkseen ne tutkintoonsa ulkomaisessa yliopistossa)
- **qualifying-studies:** the student has a degree and is taking courses in order to acquire further qualifications (pätevöityminen: opiskelija täydentää tässä tai jossain muussa korkeakoulussa suorittamaansa tutkintoa)
- **further-education:** the student has a degree and is taking further education courses without aiming at acquiring further qualifications (opiskelija täydentää tässä tai jossain muussa korkeakoulussa suorittamaansa tutkintoa)
- **open-university:** students in open university (avoin yliopisto), open polytechnic (avoin amk), further education center (täydennyskoulutuskeskus)
- **other:** the person is a student in the institution in some other sense.

This is a more fine-grained attribute for student categories than eduPersonAffiliation. Following mapping is expected:

- eduPersonAffiliation="student": bachelor, master, licentiate, doctor, other-degree, visiting-student, exchange-student
- eduPersonAffiliation="member": qualifying-studies, further-education
- eduPersonAffiliation="affiliate": open-university, other

Being registered as present or absent does not affect on this attribute.

Examples:

```
funetEduPersonStudentCategory: master
```

funetEduPersonStudentStatus

Status of a student (läsnäolotieto); present or absent.

According to the Universities act (yliopistolaki) and Polytechnics act (ammattikorkeakoululaki), each academic year the student must register as being present (läsnäoleva) or absent (poissaoleva).

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.21	DirectoryString	Single	May

Vocabulary: present, absent.

The value carried by the attribute should be considered as the current status of a student. A student may graduate, terminate his/her studies or otherwise change the status at any time.

Examples:

```
funetEduPersonStudentStatus: present
```

funetEduPersonStudentUnion

Name of the student union the student is a member of, if any.

According to the Universities act (yliopistolaki), all the university students who have been admitted to programs leading to the lower or higher university degree shall belong to the student union (ylioppilaskunta). The student union may also accept other students of the university as members.

In polytechnics, belonging to the student union (amk-opiskelijayhdistys) is voluntary.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.22	DirectoryString	Single	May

Examples:

```
funetEduPersonStudentUnion: Tampereen teknillisen yliopiston ylioppilaskunta
```

funetEduPersonHomeCity

Home City (kotikunta) of the user.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.23	DirectoryString	Single	May

Syntax: NNN

Vocabulary: the 3-number codes assigned by the Population Register Center (Väestörekisterikeskus) of Finland ("Kunta- ja rekisterinpitäjäluettelo").

Examples: (Hauho)

```
funetEduPersonHomeCity: 083
```

funetEduPersonEPPNTimeStamp

The date when eduPersonPrincipalName was issued to this individual.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.24	DirectoryString	Single	May

Over time, some institutions reassign eduPersonPrincipalName values to new individuals. On the other hand, in services, eduPersonPrincipalName is commonly used for binding profiles to individuals. This attribute is intended for assisting services to deduce if eduPersonPrincipalName has been reassigned to a new person.

> In Haka Federation, there is a requirement for the Identity Providers to freeze revoked eduPersonPrincipalName values for certain period of time (at the time of publication: 24 months) before reassignment, and a requirement for Service Providers to expect reassignment if the EPPN holder has not used the service for respective time. See Haka federation policy documents for details.

This attribute is to complement these requirements by enabling services with extended user lifecycle to maintain user profiles longer.

Format: YYYYMMDD.

Examples:

```
funetEduPersonEPPNTimeStamp: 20040826
```

funetEduPersonGivenNames

The funetEduPersonGivenNames attribute type contains name strings that are the part of a person's name that is not their surname.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.25	DirectoryString	Single	May

The funetEduPersonGivenName attribute type is parallel to Haka interpretation of globally defined givenName attribute type with different semantics. In schema version 2.2. interpretation of globally defined givenName attribute changed to follow RFC 2256. The funetEduPersonGivenNames attribute follows RFC 4519 definition with difference that the funetEduPersonGivenNames is single valued attribute with one catenated string of defined name parts delimited by space where the delimiter is not part of the official name (e.g. multipart name delimited with hyphen).

> See commonName for conventions for attributes carrying the name of an individual. This attribute SHOULD not be mixed with givenName attribute.

funetEduPersonFullName

Space delimited catenated string of all official name strings of a person.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.26	DirectoryString	Single	May

The funetEduPersonFullName attribute type is parallel to globally defined cn attribute type with different semantics. While in Haka cn is interpretated to hold the name the individual has registered as the one (s)he uses + sn, the funetEduPersonFullName holds the person's official name in its entirety as one string. Name parts are delimited by space where the delimiter is not part of the official name (e.g. multipart name delimited with hyphen). All name parts in the funetEduPersonFullName are transcribed as they are registered to official census (in Finland The Finnish Population Information System held by Population Register Centre).

> See commonName for conventions for attributes carrying the name of an individual. This attribute SHOULD not be mixed with givenName attribute.

funetEduPersonLearnerId

11-digit identifier to identify a person.

OID	Syntax	values	relevance
1.3.6.1.4.1.16161.1.1.27	DirectoryString	Single	May

LearnerId is an 11-digit identifier, which may be used to identify a person while storing, managing or transferring personal data. LearnerId is issued when personal data is initially stored to student selection registry. schacPersonalUniqueID (identity number) or corresponding unique identifier is used when issuing LearnerId first time. LearnerId is permanent.

LearnerId complies with finnish law 18.12.1998/1058 of student selection registry, data warehouse for higher education and registry for matriculation examination [1].

LearnerId doesn't include any information about a person [2]. Random number starting from 1000000000 is used to issue the identifier. Colissions are prevented by checking from central database that given identifier has not yet been issued to another person. The identifier is presented as an OID on branch 1.2.246.562.24 according to JHS 159 specification [3]. Eleventh digit of the identifier is a IBM-1-3-7 checksum of the first ten digits.

[1] http://www.finlex.fi/fi/laki/ajantasa/1998/19981058
[2] https://confluence.csc.fi/download/attachments/8127300/Oppijanumero+ja+OID.pdf
[3] http://www.jhs-suositukset.fi/suomi/jhs159

Format: 1.2.246.562.24.x

Examples:

funeteduPersonLearnerId: 1.2.246.562.24.10000000008
funeteduPersonLearnerId: 1.2.246.562.24.99999999990

Attributes from Finnish public sector attribute profile

electronicIdentificationNumber (satu)

(Fin Attr Profile 1.1) The electronic identification number (sähköinen asiointitunnus, satu) issued to an individual by Population Registry Center (Väestörekisterikeskus).

OID	Syntax	values	relevance
1.2.246.22	DirectoryString	Single	May

(Fin Attr Profile 1.1) Inteded use: Identification of an end user

Examples:

```
electronicIdentificationNumber: 012345678N
```

nationalIdentificationNumber (hetu)

(Fin Attr Profile 1.1) The national identification number (henkilötunnus, hetu) issued to an individual by Population Registry Center (Väestörekisterikeskus).

OID	Syntax	values	relevance
1.2.246.21	DirectoryString	Single	May

(Fin Attr Profile 1.1) Inteded use: Identification of an end user

> NationalIdentificationNumber is a paraller attribute to schacPersonalUniqueId. Note that the format is different.

Examples:

`nationalIdentificationNumber:` 010191-123A

Attributes from schac

schacMotherTongue

(schac 1.5.0) Is the language a person learns first. Correspondingly, the person is called a native speaker of the language. Usually a child learns the basics of their first language from their family.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.1	DirectoryString	Single	May

(schac 1.5.0) Format: See RFC 3066 Tags for the Identification of Languages

Examples:

```
schacMotherTongue: fr
```

```
schacMotherTongue: es-ES
```

```
schacMotherTongue: fi
```

schacGender

(schac 1.5.0) The state of being male or female. The gender attribute specifies the legal gender the subject it is associated with.

"Either of the two groups that people, animals and plants are divided into according their function of producing young" (Oxford Advanced Learner's Dictionary).

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.2	Integer	Single	May

(schac 1.5.0) Format:

- *0 Not known*
- *1 Male*
- *2 Female*
- *9 Not specified*

Examples:

```
schacGender: 2
```

schacDateOfBirth

(schac 1.5.0) The date of birth for the subject it is associated with

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.3	Numeric string	Single	May

(schac 1.5.0) Format: Numeric value YYYYMMDD, using 4 digits for year, 2 digits for month and 2 digits for day as described in RFC 3339 'Date and Time on the Internet: Timestamps' as reference using the 'full-date' format from paragraph 5.6 but without the dashes.

Examples:

```
schacDateOfBirth: 19660412
```

schacYearOfBirth

(schac 1.5.0) The year of birth for the subject is associated with.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.0.2.3	Numeric string	Single	May

(schac 1.5.0) Format: Numeric value YYYY, using 4 digits for the year, as described in RFC 3339 'Date and Time on the Internet: Timestamps' as reference using the 'full-date' format from paragraph 5.6 but without the dashes.

Examples:

```
schacYearOfBirth = 1966
```

schacPlaceOfBirth

(schac 1.5.0) The schacPlaceOfBirth attribute specifies the place of birth for the subject it is associated with.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.4	DirectoryString	Single	May

(schac 1.5.0) Format: Free string

Examples:

```
schacPlaceOfBirth: Turku, Suomi
```

schacCountryOfCitizenship

(schac 1.5.0) The schacCountryOfCitizenship attribute specifies the (claimed) countries of citizenship for the subject it is associated with.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.5	DirectoryString	Multi	May

(schac 1.5.0) Format: Two-letter country acronym in accordance with ISO 3166.

Examples:

```
schacCountryOfCitizenship: fi
```

schacHomeOrganization

(schac 1.5.0) Specifies a person´s home organization using the domain name of the organization. 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.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.9	DirectoryString	Single	MUST

(schac 1.5.0) Format: Domain name acording to RFC 1035

> According to the interpretation of Haka Advisory Commitee*:*
>
> *Home organization shall populate the same value to all it's users. E.g. all users either tkk.fi or hut.fi .*

Examples:

```
schacHomeOrganization: tut.fi
```

schacHomeOrganizationType

(schac 1.5.0) Type of a Home Organization.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.10	DirectoryString	Multi	MUST

(schac 1.5.0) Format: urn:schac:homeOrganizationType:<country-code>:<string>

- *The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at* https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry
- *<string> from a nationally controlled vocabulary, published through the URI identified at the above mentioned TERENA URN registry.*

Examples:

```
schacHomeOrganizationType: urn:schac:homeOrganizationType:fi:university
```

```
schacHomeOrganizationType: urn:schac:homeOrganizationType:fi:polytechnic
schacHomeOrganizationType: urn:schac:homeOrganizationType:fi:researchInstitution
schacHomeOrganizationType: urn:schac:homeOrganizationType:fi:other
schacHomeOrganizationType: urn:schac:homeOrganizationType:es:opi
```

schacCountryOfResidence

(schac 1.5.0) The schacCountryOfResidence attribute specifies the (claimed) country of residence for the subject is associated with.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.11	DirectoryString	Multi	May

(schac 1.5.0) Format: Two-letter country acronym in accordance with ISO 3166 country code identifier.

Examples:

```
schacCountryOfResidence: es
schacCountryOfResidence: fi
```

schacUserPresenceID

(schac 1.5.0) To store a set of values related to network presence protocols.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.12	DirectoryString	Multi	May

(schac 1.5.0) Format: URI

```
Examples:
schacUserPresenceID: xmpp:pepe@im.univx.es
schacUserPresenceID: sip:pepe@myweb.com
schacUserPresenceID: sip:+34-95-505-6600@univx.es;transport=TCP;user=phone
schacUserPresenceID: sips:alice@atlanta.com?subject=project%20x&priority=urgent
schacUserPresenceID: h323:pepe@myweb.fi:808;params
```

schacPersonalPosition

(schac 1.5.0) The Personal Position attribute type specifies a personal position inside an institution.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.13	DirectoryString	Multi	May

(schac 1.5.0) Format: urn:schac:personalPosition:<country-code>:<domain>:<iNSS>

- The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+Registry
- <domain> is the institution domain name according to RFC 1035
- <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insenstitive. Valid components for it are those specified (or explicitly delegated) by the TERENA URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+Registry

Examples:

```
schacPersonalPosition: urn:schac:personalPosition:pl:umk.pl:programmer
```

schacPersonalUniqueCode

(schac 1.5.0) 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,...

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.14	DirectoryString	Multi	May

(schac 1.5.0) Format: urn:schac:personalUniqueCode:<country-code>:<iNSS>

- *The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at* https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry
- *<iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive, from a nationally controlled vocabulary, published through the URI identified at the above mentioned TERENA URN registry.*

See also: employeeNumber

Examples: (opiskelijanumero)

```
schacPersonalUniqueCode: urn:schac:personalUniqueCode:int:studentID:tut.fi:165934
```

Examples:

```
schacPersonalUniqueCode: urn:schac:personalUniqueCode:se:LIN:87654321
```

schacPersonalUniqueID

(schac 1.5.0) Specifies a "legal unique identifier" for the subject it is associated with. This might be DNI in Spain, FIC (henkilötunnus) in Finland, NIN in Sweden,...

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.15	DirectoryString	Multi	May

(schac 1.5.0) Format: urn:schac:personalUniqueID:<country-code>:<idType>:<idValue>

- *The <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry*
- *<idType>. Acceptable values must be declared per each country code through the URI identified at the above mentioned TERENA URN registry.*
- *<idValue>*

In Finland, use urn:schac:personalUniqueID:fi:FIC:<hetu> for the Finnish Identification Code (henkilötunnus) assigned by the Population Registry Center (Väestörekisterikeskus).

This attribute is not for locally assigned Finnish Identification Codes (ie codes that look like FICs but are generated locally by the organisation), since nothing guarantees that they are unique. For locally assigned FIC, use schacPersonalUniqueCode instead.

See also nationalIdentificationNumber.

Examples:

```
schacPersonalUniqueID: urn:schac:personalUniqueID:fi:FIC:260667-123F
```

```
schacPersonalUniqueID: urn:schac:personalUniqueID:es:NIF:31241312L
```

```
schacPersonalUniqueID: urn:schac:personalUniquelD:se:NIN:12345678
```

schacExpiryDate

(schac 1.5.0) The date from which the set of data is to be considered invalid (specifically, in what refers to rights and entitlements). This date applies to the entry as a whole.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.17	Generalized Time	Single	May

(*schac 1.5.0*) Format: Values must be expressed in UTC and must include seconds (i.e., times are YYYYMMDDhhmmssZ), even where the number of seconds is zero. GeneralizedTime values must not include fractional seconds.

Examples:

```
schacExpiryDate: 20051231125959Z
```

schacUserPrivateAttribute

(schac 1.5.0) Used to model privacy requirements, as expressed by the user and/or organizational policies. The values are intended to be attribute type names and applies to the attribute and any subtypes of it for a given entity. In what respects to data exchange, it applies to the expression of privacy requirements. This attribute can also have specific operational semantics (one has already been applied to LDAP servers: see references below), that will be defined in a separate document.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.18	DirectoryString	Multi	May

(schac 1.5.0) Format: An attribute type identifier. Operational semantics may imply specific values as wildcards.

Examples:

Attributes mail and telephoneNumber are considered private

```
schacUserPrivateAttribute = mail;telephoneNumber
```

schacUserStatus

(schac 1.5.0) Used to store a set of status of a person as user of services.

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.19	DirectoryString	Multi	May

(schac 1.5.0) Format: urn:schac:userStatus:<country-code>:<domain>:<iNSS>

- *the <country-code> must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN registry for this attribute at* https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry
- *<domain> is the institution domain name according to RFC1035*
- *<iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive*

Examples (To store different user activity states at University of Málaga (uma.es)):

```
schacUserStatus:
 urn:schac:userStatus:es:uma.es:affiliation:expired
schacUserStatus:
 urn:schac:userStatus:es:uma.es:sendMail:expired
schacUserStatus:
 urn:schac:userStatus:es:uma.es:getMail:active
```

Examples (a parameter in the URN can be used to represent the temporal validity of the status):

```
schacUserStatus:
 urn:schac:userStatus:si:ujl.si:webmail:active?+ttl=20060531235959
```

schacProjectMembership

(schac 1.5.0) The name of the project the user belongs to

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.20	DirectoryString	Multi	May

(*schac 1.5.0*) Format: The <project-name> must be a name assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry

Examples:

```
schacProjectMemberShip: perfsonar
```

schacProjectSpecificRole

(schac 1.5.0) Used to store a set of roles inside specific projects

OID	Syntax	values	relevance
1.3.6.1.4.1.25178.1.2.21	DirectoryString	Multi	May

(schac 1.5.0) Format: urn:schac:projectSpecificRole:<project-name>:<iNSS>

- The <project-name> must be a name assigned by the SCHAC URN Registry for this attribute at https://wiki.refeds.org/display/STAN/SCHAC+URN+Registry .
- <iNSS> is a Namespace Specific String as defined in RFC 2141 but case insensitive

Examples:

```
schacProjectSpecificRole: urn:schac:projectSpecificRole:perfsonar:developer
```

Attributes from eduPerson

eduPersonAffiliation

(eduPerson201310) Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc.

OID	Syntax	1. values	relevance
1.3.6.1.4.1.5923.1.1.1.1	DirectoryString	Multi	SHOULD

(eduPerson201310) Permissible values

faculty, student, staff, alum, member, affiliate, employee, library-walk-in.

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

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 or
staff or
student or
employee

Note: Holders of the affiliation "alum" are not typically "members" since they are not eligible for the full set of basic institutional privileges enjoyed by faculty, staff and students.

Cautionary note: 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.

The "affiliate" value 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.

For the sake of completeness, if for some reason the institution carries digital identity information for people with whom it has no affiliation according to the above definitions, the recommendation is simply not to assert eduPersonAffiliation values for those individuals.

"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 the eduPersonEntitlement value " urn:mace:dir:entitlement:common-lib-terms " as defined in the MACE-Dir Registry of eduPersonEntitlement values http://middleware.internet2.edu/urn-mace/urn-mace-dir-entitlement.html .

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.

Semantics

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

A reasonable person should find the listed relationships plausible.

Example applications for which this attribute would be useful

white pages, controlling access to resources

In order to harmonize semantics of this attribute and ease its use for authorization, following convention is used in Haka federation:

- **Student** = a student who has registered as being present (läsnäoleva) and
  1. who aims at a degree that is laid down by a decree (opiskelija, joka tähtää asetuksella annettuun tutkintoon); e.g. bachelor, master, licentiate, doctor; or
  2. who is going to include the studies in his/her degree in another Finnish or foreign university; e.g. exchange/visiting student (vaihto-opiskelija, JOO-opiskelija).
- **Faculty**= research and education workers at laboratories and institutes; e.g. professors, researchers, lecturers, assistants, whether employed by the institution or some other organisation (such as Academy of Finland). Docents may be affiliated as faculty, if they are actively involved in research or education in an institute.
  - Mapping to categories of the KOTA database for universities:
    - educational workers (opetushenkilökunta)
    - research workers (tutkimushenkilökunta)
  - Mapping to categories of the AMKOTA database for polytechnics:
    - teachers (opettajat)
    - R&D workers (901, 902, 903 tutkimushenkilökunta)
  - In Haka federation the value faculty of eduPersonAffiliation attribute is **RECOMMENDED** to be available when it is appropriate for the person in question providing the coupling between base registry (eg student registry) and user database is functional.
- **Staff** = administrational workers at the institution, whether employed by the institution or some other organisation (like a subcontractor such as campus restaurant or cleaning firm).
  - Mapping to categories of the KOTA database for universities:
    - supportive staff for research and education (opetuksen ja tutkimuksen apuhenkilöstö)
    - library staff (kirjastohenkilökunta)- IT staff (ATK-henkilökunta)
    - administrational and office staff (hallinto- ja toimistohenkilökunta)
    - property maintenance staff (huolto- ja kiinteistönhuoltohenkilökunta)
  - Mapping to categories of the AMKOTA database for polytechnics:
    - teaching administration (201 Opetuksen hallinto: opetuksen järjestämiseen liittyvän hallinnon henkilöstö, esim. apulaisrehtori, koulutusohjelmajohtaja, opintoasiainpäällikkö, opintoasiainsihteeri, opintotukisihteeri)
    - library staff (301 Kirjasto- ja tietopalvelut)
    - other supportive staff for teaching (401 Muu opetuksen tukitoiminta, esim. harjoittelu- ja laboratorioinsinöörit)
    - general and IT administration (701 Yleishallinto, esim. rehtori, johdon sihteeri, tiedottaja, tietohallinto- ja tietotekniikka henkilöstö)
    - financial administration (702 Taloushallinto, esim. talouspäällikkö, -johtaja, -sihteeri, taloudenhoitaja, kirjanpitäjä)
    - human resources administration (703 Henkilöstöhallinto, esim. palkanlaskija, henkilöstöpäällikkö, henkilöstöasiain sihteeri)
    - other staff (850 Muu henkilökunta, kaikki muut, jotka eivät sisälly edellisiin)
- **Employee** = a person actually employed by the institution (työ/virkasuhteessa).
- **Member** = This value covers all categories mentioned above plus students taking qualifying education courses or further education courses (pätevöitymiseen tähtäävä täydennyskoulutus, muu täydennyskoulutus).
- **Affiliate** = a person that for some reason has to be granted a user identity in the organization, but who does not receive any other benefits. E. g. an open university and further education center students (avoin yliopisto/korkeakoulu, täydennyskoulutuskeskuksen opiskelijat), a degree student with an absent status (poissaolevaksi kirjoittautunut tutkinto-opiskelija), a library walk-in (kirjaston kadunmies-asiakas), an outside member of a research group etc.
- **Alum** = a graduated student of the institution
- **Library-walk-in** = a library walk-in (kirjaston kadunmies-asiakas)

In the absence of coupling between base registry (eg student registry) and the user database, role based attributes like eduPersonAffiliation **SHALL NOT** be made available in Haka federation.

See also: funetEduPersonStudentCategory

Examples (professor of a university):

```
eduPersonAffiliation: faculty
eduPersonAffiliation: employee
eduPersonAffiliation: member
```

Examples (researcher employed by Academy of Finland):

```
eduPersonAffiliation: faculty
eduPersonAffiliation: member
```

Examples (docent who is not actively involved in research and education):

```
eduPersonAffiliation: affiliate
```

Examples (civilian servant serving in the university library):

```
eduPersonAffiliation: staff
eduPersonAffiliation: member
```

Examples (student that has been hired as a research assistant in a laboratory):

```
eduPersonAffiliation: staff
eduPersonAffiliation: employee
eduPersonAffiliation: student
eduPersonAffiliation: member
```

Examples (library walk-in):

```
eduPersonAffiliation: library-walk-in
```

eduPersonEntitlement

(eduPerson201310) URI (either URN or URL) that indicates a set of rights to specific resources.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.7	DirectoryString	Multi	May

(eduPerson201310) 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. See the first example below.

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. See the second example below.

The driving force behind the definition of this attribute has been the MACE Shibboleth project. Shibboleth defines an architecture for inter-institutional sharing of web resources subject to access controls. For further details, see the project's web pages at http://shibboleth.internet2.edu/ .

Examples (the user is entitled to access licensed library content):

```
eduPersonEntitlement: urn:mace:dir:entitlement:common-lib-terms
```

Examples:

```
eduPersonEntitlement: http://xstor.com/contracts/HEd123
eduPersonEntitlement: urn:mace:washington.edu:confocalMicroscope
eduPersonEntitlement: http://www.joopas.fi/virkailijaroolit/jooHakemuksenPuoltaja
```

eduPersonNickname

(eduPerson201310) Person's nickname, or the informal name by which they are accustomed to be hailed.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.2	DirectoryString	Multi	May

(eduPerson201310) 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."

> See commonName for conventions for attributes carrying the name of an individual.

Examples:

```
eduPersonNickname: Sepi
```

eduPersonOrcid

(orcid-draft-01) An eduPersonOrcid attribute carries values of the ORCID-assigned researcher identifiers for the associated entry.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.16	Directory String	Multi	May

Permissible values

Values MUST be valid ORCID identifiers in the ORCID-preferred URL representation (see Example given below)

Semantics

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

Examples:

```
eduPersonOrcid: http://orcid.org/0000-0102-9134-699X
```

eduPersonOrgDN

(eduPerson201310) The distinguished name (DN) of the of the directory entry representing the institution with which the person is associated.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.3	DistinguishedName	single	May

(eduPerson201310) 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.

Examples:

```
eduPersonOrgDN: o=Hogwarts, dc=hsww, dc=wiz
```

eduPersonOrgUnitDN

(eduPerson201310) 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.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.4	DistinguishedName	multi	May

(eduPerson201310) 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).

Examples:

```
eduPersonOrgUnitDN: ou=Potions, o=Hogwarts, dc=hsww, dc=wiz
```

eduPersonPrimaryAffiliation

(eduPerson201310) Specifies the person's PRIMARY relationship to the institution in broad categories such as student, faculty, staff, alum, etc.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.5	DirectoryString	Single	May

(eduPerson201310) Permissible values

faculty, student, staff, alum, member, affiliate, employee, library-walk-in

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.

> See eduPersonAffiliation for a more specific Finnish interpretation.
>
> In Haka federation, following priorities are recommended: 1) faculty, 2) staff, 3) employee, 4) student, 5) member, 6) affiliate, 7) library-walk-in.

eduPersonPrimaryOrgUnitDN

(eduPerson201310) The distinguished name (DN) of the directory entry representing the person's primary Organizational Unit(s).

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.8	DistinguishedName	single	May

(eduPerson201310) Appropriate if the person carries at least one of the defined eduPersonOrgUnitDN. The choices of values are the same as for that attribute.

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

eduPersonPrincipalName

(eduPerson201310) 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.

OID	Syntax	1. values	relevance
1.3.6.1.4.1.5923.1.1.1.6	DirectoryString	single	MUST

(eduPerson201310) *Syntactically, ePPN looks like an email address but is not intended to be a person's published email address or be used as an email address. In general, name-based identifiers tend to be subject to some degree of expected change and/or reassignment.*

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

In Haka Federation, there is a requirement for the Identity Providers to freeze revoked eduPersonPrincipalName values for certain period of time (at the time of publication: 24 months) before reassignment, and a requirement for Service Providers to expect reassignment if the EPPN holder has not used the service for respective time. See Haka federation policy documents for details.
See also: funetEduPersonEPPNTimeStamp

Examples:

```
mvirtane@hut.fi
mkorhone@students.oamk.fi
```

eduPersonPrincipalNamePrior (defined in eduPerson 201211)

(eduPerson201312) Each value of this multi-valued attribute represents an ePPN (eduPersonPrincipalName) value that was previously associated with the entry. The values MUST NOT include the currently valid ePPN value. There is no implied or assumed order to the values. This attribute MUST NOT be populated if ePPN values are ever reassigned to a different entry (after, for example, a period of dormancy). That is, they MUST be unique in space and over time.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.12	DirectoryString	multi	May

(eduPerson201312) This attribute provides a historical record of ePPN values associated with an entry, provided the values are not subject to reassignment. It is permissible to reassign ePPN values, but doing so precludes the use of this attribute; consumers must be able to assume that a historical ePPN value is associated with exactly one entry for all time. As an identifier that may be based on a user's name, values of ePPN may change over time, and this creates problems for applications that are limited in their capacity to accommodate less friendly identifiers. To improve the user experience in such cases, applications may be enhanced to leverage this attribute to identify renamed accounts. Applications that support automated renaming can be enhanced to do so, while those that do not could be enhanced with logging or exception reporting that identifies the problem. It is strongly preferable to enhance, or build new, applications to support more stable/persistent (and necessarily opaque) identifiers, but this attribute may be useful as a transitional aid. It is permissible, though likely unusual, for a subject with no current eduPersonPrincipalName value to have eduPersonPrincipalNamePrior values. This could reflect, for example, a deprovisioning scenario.

Example

eduPersonPrincipalName: baz@hsww.wiz
eduPersonPrincipalNamePrior: foo@hsww.wiz
eduPersonPrincipalNamePrior: bar@hsww.wiz

eduPersonScopedAffiliation

(eduPerson201310) Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc. The values consist of a left and right component separated by an "@" sign. The left component is one of the values from the eduPersonAffiliation controlled vocabulary. This right-hand side syntax of eduPersonScopedAffiliation intentionally matches that used for the right-hand side values for eduPersonPrincipalName since both identify a security domain. Multiple "@" signs are not recommended, but in any case, the first occurrence of the "@" sign starting from the left is to be taken as the delimiter between components. Thus, user identifier is to the left, security domain to the right of the first "@". This parsing rule conforms to the POSIX "greedy" disambiguation method in regluar expression processing.

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.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.9	DirectoryString	multi	SHOULD

(eduPerson201310) 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.

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."

Example:

```
eduPersonScopedAffiliation: faculty@tut.fi
eduPersonScopedAffiliation: student@students.oamk.fi
```

eduPersonTargetedID

(eduPerson201310) A persistent, non-reassigned, opaque identifier for a principal.

eduPersonTargetedID is an abstracted version of the SAML V2.0 Name Identifier format of "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" (see http://www.oasis-open.org/committees/download.php/35711). 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.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.10	DirectoryString	Multi	May

(eduPerson201310) 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 inherited from SAML 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 reassigned such that the same value given to a particular relying party refers to two different principals at different points in time. It is allowable (though perhaps confusing) for a given value to refer to two or more different principals when scoped to different audiences.

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).

eduPersonAssurance

(eduPerson201310) Set of URIs that assert compliance with specific standards for identity assurance.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.11	DirectoryString	Multi	May

(eduPerson201310) This multi-valued attribute represents identity assurance profiles (IAPs), which are the set of standards that are met by an identity assertion, based on the Identity Provider's identity management processes, the type of authentication credential used, the strength of its binding, etc. An example of such a standard is the InCommon Federation's proposed IAPs.

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

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

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

Example:

```
eduPersonAssurance: urn:mace:incommon:IAQ:sample
```

```
eduPersonAssurance: http://idm.example.org/LOA#sample
```

eduPersonUniqueId

(eduPerson201310) 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.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.1.1.13	DirectoryString	Single	May

(eduPerson201310) 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 (see section 1.3) 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.

Example:

```
  eduPersonUniqueId: 28c5353b8bb34984a8bd4169ba94c606@foo.edu
```

Common attributes

cn / commonName

(RFC 4519) The 'cn' ('commonName' in X.500) attribute type contains names of an object. Each name is one value of this multi-valued attribute. If the object corresponds to a person, it is typically the person's full name. (RFC2256) This is the X.500 commonName attribute, which contains a name of an object. If the object corresponds to a person, it is typically the person's full name.

OID	Syntax	values	relevance
2.5.4.3	DirectoryString	multi	MUST

(eduPerson201310) One of the two required attributes in the person object class (the other is sn).

In Finland, people have one family name and at most three first names, for example Seppo Matinpoika Johannes Virtanen.
In order to harmonize practices in Finland,

- sn = family name
- givenName = the preferred given name the person has indicated to be used (in Finland: "kutsumanimi")
- funetEduPersonGivenNames = all official given names of a person.
- funetEduPersonFullName = official full name of a person
- cn = the name the individual has indicated as the one (s)he uses + sn
- displayName = the name the individual has indicated as the one (s)he uses + sn
- eduPersonNickname = the informal name by which the individual is accustomed to be hailed

Examples:

```
sn: Virtanen
givenName: Seppo
funetEduPersonGivenNames: Seppo Matinpoika Johannes
funetEduPersonFullName: Seppo Matinpoika Johannes Virtanen
cn: Seppo Virtanen
displayName: Seppo Virtanen
eduPersonNickname: Sepi
```

description

(RFC 2256) This attribute contains a human-readable description of the object. (RFC 4519) The 'description' attribute type contains human-readable descriptive phrases about the object. Each description is one value of this multi-valued attribute.

OID	Syntax	values	relevance
2.5.4.13	DirectoryString	Multi	May

(eduPerson201310) Open-ended; whatever the person or the directory manager puts here.

displayName

(RFC 2798) Preferred name of a person to be used when displaying entries. (RFC2798) When displaying an entry, especially within a one-line summary list, it is useful to be able to identify a name to be used. Since other attribute types such as 'cn' are multivalued, an additional attribute type is needed. Display name is defined for this purpose.

OID	Syntax	values	relevance
2.16.840.1.113730.3.1.241	DirectoryString	Single	MUST

(eduPerson201310) The name(s) that should appear in white-pages-like applications for this person.

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

See commonName for conventions for attributes carrying the name of an individual.

employeeNumber

(RFC 2798) Numeric or alphanumeric identifier assigned to a person, typically based on order of hire or association with an organization. Single valued.

OID	Syntax	values	relevance
2.16.840.1.113730.3.1.3	DirectoryString	Single	May

Locally unique.

Examples:

```
employeeNumber: 1054
```

facsimileTelephoneNumber

(RFC 2256 RFC 4519) The 'facsimileTelephoneNumber' attribute type contains telephone numbers (and, optionally, the parameters) for facsimile terminals. Each telephone number is one value of this multi-valued attribute.

OID	Syntax	values	relevance
2.5.4.23	FacsimileTelephoneNumber	Multi	May

(eduPerson201310) Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."

givenName

(RFC 2256) The givenName attribute is used to hold the part of a person's name which is not their surname nor middle name. (RFC 4519) 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 multi-valued attribute.

OID	Syntax	values	relevance
2.5.4.42	DirectoryString	Multi	MUST

As from version 2.2 of the schema, in Haka, the givenName attribute type is interpretated as defined in RFC 2256 with special complements below.

See commonName for conventions for attributes carrying the name of an individual. If the object corresponds to a person, following rules should be considered. Since displayName seems to be widely used as full name of a person in addition to cn, Haka interpretation of the givenName attribute is the preferred given name the person has indicated to be used (in Finland: "kutsumanimi"). In Finland, only one name can be registered as preferred. For this reason and to avoid confusion, only one value SHOULD be made available when describing a person.

Traditionally both givenName (displayname in FEP 2.1 and before) and sn have been made available for each user in Haka as mandatory attributes. After the change in semantics in version 2.2 of the schema, givenName needs to be specified as mandatory for the same set of personal data to be available as before in FEP 2.1.

homePhone

(RFC 1274) The Home Telephone Number attribute type specifies a home telephonenumber associated with a person. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567".

OID	Syntax	values	relevance
0.9.2342.19200300.100.1.20	TelephoneNumber	Multi	May

Examples:

```
homePhone: +358 3 317 7059
```

homePostalAddress

(RFC 1274) The Home postal address attribute type specifies a home postal address for an object. This should be limited to up to 6 lines of 30 characters each.

OID	Syntax	values	relevance
0.9.2342.19200300.100.1.39	PostalAddress	Multi	May

$ is used as a line separator

Examples:

```
homePostalAddress: Kotikatu 4$00100 Helsinki
```

jpegPhoto

(RFC 2798) Used to store one or more images of a person using the JPEG File Interchange Format [JFIF].

OID	Syntax	values	relevance
0.9.2342.19200300.100.1.60	JPEG	Multi	May

l / localityName

(RFC 2256 / RFC 4519) The 'l' ('localityName' in X.500) attribute type contains names of a locality or place, such as a city, county, or other geographic region. Each name is one value of this multi-valued attribute."This attribute contains the name of a locality, such as a city, county or other geographic region (localityName).

OID	Syntax	values	relevance
2.5.4.7	DirectoryString	Multi	May

Examples:

```
l: Viikki
```

labeledURI

(eduPerson201310) Follow inetOrgPerson definition of RFC 2079: "Uniform Resource Identifier with optional label."
Commonly a URL for a web site associated with this person.

OID	Syntax	values	relevance
1.3.6.1.4.1.250.1.57	DirectoryString	Multi	May

(eduPerson201310) Good candidate for a self-maintained attribute. Note, however, that the vocabulary for the label portion of the value is not standardized.

Note from RFC 2079: "The labeledURI attribute type has the caseExactString syntax (since URIs are case-sensitive) and it is multivalued. Values placed in the attribute should consist of a URI (at the present time, a URL) optionally followed by one or more space characters and a label. Since space characters are not allowed to appear un-encoded in URIs, there is no ambiguity about where the label begins. At the present time, the URI portion must comply with the URL specification.

Multiple labeledURI values will generally indicate different resources that are all related to the X.500 object, but may indicate different locations for the same resource.

The label is used to describe the resource to which the URI points, and is intended as a friendly name fit for human consumption. This document does not propose any specific syntax for the label part. In some cases it may be helpful to include in the label some indication of the kind and/or size of the resource referenced by the URI.

Note that the label may include any characters allowed by the caseExactString syntax, but that the use of non-IA5 (non-ASCII) characters is discouraged as not all directory clients may handle them in the same manner. If non-IA5 characters are included, they should be represented using the X.500 conventions, not the HTML conventions (e.g., the character that is an "a" with a ring above it should be encoded using the T.61 sequence 0xCA followed by an "a" character; do not use the HTML escape sequence "&aring").

Examples:

```
labeledURI: http://students.tut.fi/%7Eteemu Teemu Teekkari's home page
labeledURI: http://champagne.inria.fr/Unites/rennes.gif Rennes [photo]
```

mail

(RFC 4524) The 'mail' (rfc822mailbox) attribute type holds Internet mail addresses in Mailbox [RFC2821] form (e.g., user@example.com).

OID	Syntax	values	relevance
0.9.2342.19200300.100.1.3	IA5String	Multi	SHOULD

(eduPerson201310) Preferred address for the "to:" field of email to be sent to this person. Usually of the form localid@univ.edu. Though multi-valued, there is often only one value.

Some mail clients will not display entries unless the mail attribute is populated. See the LDAP Recipe for further guidance on email addresses, routing, etc. (https://www.internet2.edu/media/medialibrary/2013/09/09/ldap-recipe.htm#E-MailRouting *).*

Examples:

```
mail: esko.esimerkki@oulu.fi
```

mobile

(RFC 4524) The 'mobile' (mobileTelephoneNumber) attribute specifies mobile telephone numbers (e.g., "+1 775 555 6789") associated with a person (or entity). (RFC1274) The Mobile Telephone Number attribute type specifies a mobile telephone number associated with a person. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567".

OID	Syntax	values	relevance
0.9.2342.19200300.100.1.41	TelephoneNumber	Multi	May

(eduPerson201310) cellular or mobile phone number. Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."

Examples:

```
mobile: +358 40 345 6789
```

o / organizationName

(eduPerson201310) Standard name of the top-level organization (institution) with which this person is associated. (RFC2256) This attribute contains the name of an organization (organizationName).

OID	Syntax	values	relevance
2.5.4.10	DirectoryString	Multi	May

Examples:

```
 o: University of Tampere
```

ou/organizationalUnitName

(RFC2256) This attribute contains the name of an organizational unit (organizationalUnitName). (eduPerson201310) Organizational unit(s). 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."

OID	Syntax	values	relevance
2.5.4.11	DirectoryString	Multi	May

(eduPerson201310) The designated organizational unit is understood to be part of an organization designated by an OrganizationName [o] attribute. It follows that if an Organizational Unit Name attribute is used in a directory name, it must be associated with an OrganizationName [o] attribute.

An attribute value for Organizational Unit Name is a string chosen by the organization of which it is a part.

Examples:

```
ou: Faculty of Humanities
ou: Department of History
```

postalAddress

(eduPerson201310) Campus or office address. inetOrgPerson has a homePostalAddress that complements this attribute. X.520(2000) reads: "The Postal Address attribute type specifies the address information required for the physical postal delivery to an object."

OID	Syntax	values	relevance
2.5.4.16	PostalAddress	Multi	May

Examples:

```
postalAddress: P.O. Box 405$02101 Espoo
```

postalCode

(eduPerson201310) Follow X.500(2001): "The postal code attribute type specifies the postal code of the named object. If this attribute value is present, it will be part of the object's postal address."

OID	Syntax	values	relevance
2.5.4.17	DirectoryString	Multi	May

(eduPerson201310) ZIP code in USA, postal code for other countries.

Examples:

```
postalCode: 02101
```

preferredLanguage

(RFC 2798) Preferred written or spoken language for a person.

OID	Syntax	values	relevance
2.16.840.1.113730.3.1.39	DirectoryString	Single	May

(eduPerson201310) See RFC 2068 and ISO 639 for allowable values in this field. Esperanto, for example is EO in ISO 639, and RFC 2068 would allow a value of en-US for US English.

Examples:

```
preferredLanguage: fi
```

seeAlso

(RFC 4519) The 'seeAlso' attribute type contains the distinguished names of objects that are related to the subject object. Each related object name is one value of this multi-valued attribute.

OID	Syntax	values	relevance
2.5.4.34	DistinguishedName	Multi	May

Examples:

```
seeAlso: cn=Department Chair, ou=physics, o=University of Technology, dc=utech, dc=ac, dc=uk
```

sn / surname

(RFC 4519) The 'sn' ('surname' in X.500) attribute type contains name strings for the family names of a person. Each string is one value of this multi-valued attribute." (RFC2256) This is the X.500 surname attribute, which contains the family name of a person.

OID	Syntax	values	relevance
2.5.4.4	DirectoryString	Multi	MUST

Object class person requires that the sn is defined.

> See commonName for conventions for attributes carrying the name of an individual.

street

(RFC 4519) The 'street' ('streetAddress' in X.500) attribute type contains site information from a postal address (i.e., the street name, place, avenue, and the house number). Each street is one value of this multi-valued attribute.

OID	Syntax	values	relevance
2.5.4.9	DirectoryString	Multi	May

Examples:

```
street: Korkeakoulunkatu 1
```

telephoneNumber

(eduPerson201310) Office/campus phone number. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567."

OID	Syntax	values	relevance
2.5.4.20	TelephoneNumber	Multi	May

title

(RFC 4519) The 'title' attribute type contains the title of a person in their organizational context. Each title is one value of this multi-valued attribute.

OID	Syntax	values	relevance
2.5.4.12	DirectoryString	Multi	May

Examples:

```
Title: professor
```

uid

(RFC 4519) The 'uid' ('userid' in RFC 1274) attribute type contains computer system login names associated with the object. Each name is one value of this multi-valued attribute.

OID	Syntax	values	relevance
0.9.2342.19200300.100.1.1	DirectoryString	Multi	May

(eduPerson201310) Likely only one value. See the extensive discussion in the "LDAP Recipe" (https://www.internet2.edu/media/medialibrary/2013/09/09/ldap-recipe.htm).

A number of off-the-shelf directory-enabled applications make use of this inetOrgPerson attribute, not always consistently.

userCertificate

(eduPerson201310) A user's X.509 certificate

(RFC 2256) This attribute is to be stored and requested in the binary form, as 'userCertificate;binary'.

OID	Syntax	values	relevance
2.5.4.36	Certificate	Multi	May

(eduPerson201310) Note that userSMIMECertificate is in binary syntax (1.3.6.1.4.1.1466.115.121.1.5) whereas the userCertificate attribute is in certificate syntax (1.3.6.1.4.1.1466.115.121.1.8).

userPassword

(eduPerson200312eduPerson200806) This attribute identifies the entry's password and encryption method in the following format: {encryption method}encrypted password.

OID	Syntax	1. values	relevance
2.5.4.35	DirectoryString	Multi	May

(eduPerson200312eduPerson200806) The user pw is hidden, and is used in the bind operation in LDAP. The bind operation must be done over SSL to avoid sending clear text passwords over the wire or through the air.

userSMIMECertificate

(eduPerson200806) An X.509 certificate specifically for use in S/MIME applications (see RFCs 2632, 2633 and 2634).

OID	Syntax	values	relevance
2.16.840.1.113730.3.1.40	Binary	Multi	May

(RFC 2798) If available, this attribute is preferred over the userCertificate attribute for S/MIME applications. This attribute is to be stored and requested in the binary form, as 'userSMIMECertificate;binary.'

Attributes for organisations

These are attributes for an object representing an organisation or organisational unit. The attributes are expected to be used in the organisation branch of an enterprise directory.

Attributes from eduOrg

eduOrgHomePageURI

(eduOrg200210) The URL for the organization's top level home page.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.2.1.2	DirectoryString	Multi	May

Example:

```
eduOrgHomePageURI: http://www.helsinki.fi/
```

eduOrgIdentityAuthNPolicyURI

(eduOrg200210) A URI pointing to the location of the organization´s policy regarding identification and authentication (the issuance and use of digital credentials). Most often a URL, but with appropriate resolution mechanisms in place, could be a URN.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.2.1.3	DirectoryString	Multi	May

Haka federation requires each identity provider to disclose description of its identity management procedures.

Example:

```
eduOrgIdentficationAuthNPolicyURI: http://www.tut.fi/public/it/idm/TTY-idm-kuvaus.html
```

eduOrgLegalName

(eduOrg200210) The organization´s legal corporate name.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.2.1.4	DirectoryString	Multi	May

Example:

```
eduOrgLegalName: Päijät-Hämeen koulutuskonserni
```

eduOrgSuperiorURI

(eduOrg200210) LDAP URL for the organization object one level superior to this entry.

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.2.1.5	DirectoryString	multi	May

eduOrgWhitePagesURI

(eduOrg200210) The URL of the open white pages directory service for the university, predominantly LDAP these days

OID	Syntax	values	relevance
1.3.6.1.4.1.5923.1.2.1.6	DirectoryString	multi	May

cn /commonName

(eduOrg200210) X.520 (2001) "commonName." Name or names by which this organization is commonly known.

OID	Syntax	1. values	relevance
2.5.4.3	DirectoryString	multi	May

Example:

```
cn: University of Lapland
```

description

(eduOrg200210) Open-ended; whatever the person or the directory manager puts here. According to RFC 2256, "This attribute contains a human-readable description of the object.

OID	Syntax	values	relevance
2.5.4.13	DirectoryString	multi	May

facsimileTelephoneNumber

(eduOrg200210) A fax number for the directory entry. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567.

OID	Syntax	values	relevance
2.5.4.23	FacsimileTelephoneNumber	multi	May

l (localityName)

(eduOrg200210) According to RFC 2256, "This attribute contains the name of a locality, such as a city, county or other geographic region."
X.520 (2001) reads: "The Locality Name attribute type specifies a locality. When used as a component of a directory name, it identifies a geographical area or locality in which the named object is physically located or with which it is associated in some other important way."

OID	Syntax	values	relevance
2.5.4.7	DirectoryString	multi	May

o / organizationName

(eduOrg200210) Standard name of the top-level organization (institution).

OID	Syntax	values	relevance
2.5.4.10	DirectoryString	multi	May

postalAddress

(eduOrg200210) Main office address. X.520 (2001) reads: "The Postal Address attribute type specifies the address information required for the physical postal delivery to an object."

OID	Syntax	values	relevance
2.5.4.16	PostalAddress	multi	May

postalCode

(eduOrg200210) Follow X.520 (2001): "The postal code attribute type specifies the postal code of the named object. If this attribute value is present, it will be part of the object's postal address." Zip code in USA, postal code for other countries.

OID	Syntax	values	relevance
2.5.4.17	DirectoryString	multi	May

postOfficeBox

(eduOrg200210) Follow X.520 (2001): "The Post Office Box attribute type specifies the Postal Office Box by which the object will receive physical postal delivery. If present, the attribute value is part of the object's postal address.

OID	Syntax	values	relevance
2.5.4.18	DirectoryString	multi	May

seeAlso

(eduOrg200210) The distinguished name of another directory entry. According to X.520 (2001), "The See Also attribute type specifies names of other Directory objects which may be other aspects (in some sense) of the same real world object."

OID	Syntax	values	relevance
2.5.4.34	DistinguishedName	multi	May

street

(eduOrg200210) Street address of the primary campus offices. According to RFC 2256, "This attribute contains the physical address of the object to which the entry corresponds, such as an address for package delivery (streetAddress)."

OID	Syntax	values	relevance
2.5.4.9	DirectoryString	multi	May

telephoneNumber

(eduOrg200210) Main campus phone number. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567."

OID	Syntax	values	relevance
2.5.4.20	TelephoneNumber	multi	May

Supplement attributes

mail

Mail address of the organisation, as defined in the Act on Electronic Services and Communication in the Public Sector (Laki sähköisestä asioinnista viranomaistoiminnassa).

OID	Syntax	values	Relevance
0.9.2342.19200300.100.1.3	IA5String	multi	May

Example:

```
mail: kirjaamo@uta.fi
```

Acknowledgements

Haka-IAM -verkosto is a network of specialists working on the access and identity management on Finnish higher education institutions facilitated by Haka identity federation. The network has participated actively on the update to version 2.2.

References

- eduOrg200210
  - Internet2 Middleware Architecture Committee, Directory Working Group. "EduOrg Object Class Specification (200210)." October, 2002. http://middleware.internet2.edu/eduperson/ , cited with the permission of Internet2.
- eduPerson200806
  - Internet2 Middleware Architecture Committee for Education, Directory Working Group. "EduPerson Object Class Specification (200806)." June, 2008. http://www.educause.edu/eduperson , cited with the permission of Internet2.
- RFC1274
  - Barker, P., Kille, S. "RFC 1274: The COSINE and Internet X.500 Schema." November, 1991
- RFC 2256
  - Wahl, M. "RFC2256: A Summary of the X.500(96) User Schema for use with LDAPv3". December, 1997.
- RFC2798
  - Smith, M. "RFC 2798: Definition of the inetOrgPerson LDAP Object Class". April, 2000.
- RFC 3066
  - Alvestrand, H. "RFC 3066: Tags for the Identification of Languages". January, 2001.
- Schac ver 1.2.0
  - Schac, Schema for Academia. "Attribute Definitions for Individual Data", 4 May 2006
- RFC 4519
  - Sciberras, A. "RFC 4519: Lightweight Directory Access Protocol (LDAP): Schema for User Applications." June, 2006.
- RFC 4524
  - Zeilenga, K. "RFC 4524: COSINE LDAP/X.500 Schema". June, 2006.
- Schac ver 1.3.0
  - Schac, Schema for Academia. "Attribute Definitions for Individual Data", 12 December 2006
- eduOrg201203
  - Internet2 Middleware Architecture Committee for Education, Directory Working Group (MACE-Dir).
- SCHAC schema IAD 1.5.0.c
  - The SCHema for ACademia, TERENA Task Force on Middleware, TF-EMC2
- Fin Attr Profile 1.1
  - Approved by Ministry of Finance and Ministry of Employment and the Economy, SAML 2.0 Attribute Profile specification for the Finnish public sector identity federation services, version 1.1, 21.2.2011
- eduGAIN Policy Framework, Attribute Profile

Appendix A: Collection of attributes for intra-organisational use

These attributes are used in intra-organizational user administration by some Finnish universities and polytechnics. The list has been collected from several directory schemas and is published to help organizations to create their organizational user directories.

This part of the recommendation is advisory only and does not require making the attributes available for inter-organisational use.

Typically in the LDAP-tree there are separate branches for:

- persons, e.g. people
- user accounts, e.g. accounts or posixaccounts
- organisational information, e.g. organization
- groups

Some useful attributes relevant for a person:
(own)PersonAffiliation # other affiliation for a person within own organization
(own)PersonPrimaryAffiliation # primary affiliation for a person within own organization, vocabylary local
(own)PersonStudentNoInfo # single-valued (0/1), a student may allow or refuse to release information outside his own university
(own)PersonPrivate # personal hidden attributes
(own)PersonExpDate # the date a person will be removed from the directory
(own)PersonStudentInactiveDate # the date when no longer student
(own)PersonEmployeeInactiveDate # the date when no longer employed
(own)PersonExpertArea # area of expertise
(own)PersonAccountDN # accounts owned by the person
(own)PersonAliases # (mail)aliases for the person
(own)PersonEmployeeOu # OU where employed
(own)PersonStudentOu # OU where studying
(own)PersonTeachingSubject # subject a person is teaching
(own)PersonIntranetRole # the role of the person in the own intranet
(own)PersonConsultingHours # consulting hours for students
(own)PersonMemberOf # association with projects and groups within own organization
(own)PersonRole # personnel, graduate student, post-graduate student, exchange student
(own)PersonStudentGroup # studying program & class number
(own)PersonUniqueNumber # unique id, does not change, cannot be reassigned
(own)PersonEid # electronic ID, value: CA_eid

Attributes relevant for a user account:
(own)AccountOwnerID # DirIDNumber of an account owner
(own)AccountHost # win, unix
(own)AccountWinStatus # shows status of Windows account
(own)AccountUnixStatus # shows status of Unix account
(own)AccountWinExpirDate # the date when the account expires

Appendix B: Changelog

Changes from funetEduPerson ver 2.1

- Superseded attributes from ver 1.0 listed in table
- added schacHomeOrganization interpretation from Advisory Commitee
- new supplementary attributes:
  - funetEduPersonLearnerId
  - funetEduPersonGivenNames
  - funetEduPersonFullName
- new attributes from the Finnish Public Sector attribute profile
  - electronicIdentificationNumber
  - nationalIdentificationNumber
- corrections regarding to the referenced schema: schac, eduOrg eduPerson
- changes in mandatory and recommended attributes
  - eduPersonAffiliation value faculty set to RECOMMENDED
  - givenName set as mandatory
  - added recommendation to follow eduGAIN Attribute profile
- new attribute eduPersonOrcid from eduOrg draft
- new attributes from schac:
  - schacYearOfBirth
  - schacUserPrivateAttribute
  - schacExpiryDate
  - schacProjectMembership
  - schacProjectSpecificRole
- removed sub-category Other object Classes (course membership, group membershib)
- removed Shibboleth 1.0 attribute names
- new namespace for funetEduPersonTargetDegree
- deprecated namespaces for funetEduPersonTargetDegree, funetEduPersonProgram and funetEduPersonSpecialisation

Changes from funetEduPerson ver 2.0

- introduced SAML 2.0 attribute names (urn:oid:…)
- corrected broken URLs in the document
- corrected discrepancy in the relevance of funetEduPersonEPPNTimeStamp. The correct relevance is May
- adopted eduPerson 200806 and 200712:

    - new attribute eduPersonAssurance
    - new vocabulary value "library-walk-in" for eduPersonAffiliation/ScopedAffiliation/PrimaryAffiliation
    - updated "Common attributes" section according to eduPerson 200806 (references to new RFCs 4519 and 4524)
    - new attribute userSMIMECertificate
- adopted schac 1.3.0
    - changed schacHomeOrganization syntax to directory string
    - changed schacUserStatus syntax and examples
    - introduced "int" as an alternative to country codes

Changes from funetEduPerson ver 1.0

- reformatting, rearranging and adding examples to make the document easier to read
- mandatory attributes revised
- adopted eduPerson 200604
- only one occurrence of '@' in eduPersonScopedAffiliation and Eppn
- eduPersonTargetedID definitions
- added new attributes: eduPersonScopeedAffiliation, eduPersonTargetedID and eduPersonNickname
- introduced schac and replaced overlapping national attributes
- the replaced attributes: funetEduPersonHomeOrganization (replaced by schacHomeOrganization), funetEduPersonStudentID (schacPersonalUniqueCode), funetEduPersonIdentityCode (schacPersonalUniqueID), funetEduPersonDateOfBirth (schacDateOfBirth)
- added/clarified Haka federation interpretation for
- attributes carrying the name of an individual
- eduPersonAffiliation, eduPersonPrimaryAffiliation and eduPersonScopedAffiliation
- reassignment of eduPersonPrincipalName
- added new attributes funetEduPersonStudyStart, funetEduPersonPrimaryStudyStart, funetEduPersonStudyToEnd, funetEduPersonPrimaryStudyToEnd, funetEduPersonCreditUnits, funetEduPersonECTS, funetEduPersonEPPNTimeStamp, funetEduPersonHomeCity, funetEduPersonStudentCategory, funetEduPersonStudentStatus, funetEduPersonStudentUnion
- added new attributes for target degree, study program and specialisation with hierarchical syntax, adopted the terminology and translations (educational degree programme, specialication option) of Finnish Virtual University.
- added employeeNumber
- attribute LDAP syntax fix: codes by tilastokeskus changed: Integer-> DirectoryString and name length cut to max 32 chars
- added references to eduCourse and eduMember