funetEduPerson schema

Version 2.1 21.8.2008

Contents

1. Introduction 4
2. Attributes for persons 4
   2.1. Supplement attributes in funetEduPerson 4
      2.1.1. funetEduPersonHomeOrganization (SUPERSEDED) 4
      2.1.2. funetEduPersonStudentID (SUPERSEDED) 4
      2.1.3. funetEduPersonIdentityCode (SUPERSEDED) 5
      2.1.4. funetEduPersonDateOfBirth (SUPERSEDED) 5
      2.1.5. funetEduPersonTargetDegreeUniversity (SUPERSEDED) 5
      2.1.6. funetEduPersonTargetDegreePolytech (SUPERSEDED) 5
      2.1.7. funetEduPersonTargetDegree 5
      2.1.8. funetEduPersonEducationalProgramUniv (SUPERSEDED) 6
      2.1.9. funetEduPersonEducationalProgramPolytech (SUPERSEDED) 6
      2.1.10. funetEduPersonProgram 6
      2.1.11. funetEduPersonMajorUniv (SUPERSEDED) 6
      2.1.12. funetEduPersonOrientationAlternPolytech (SUPERSEDED) 6
      2.1.13. funetEduPersonSpecialisation 7
      2.1.14. funetEduPersonStudyStart 7
      2.1.15. funetEduPersonPrimaryStudyStart 7
      2.1.16. funetEduPersonStudyToEnd 8
      2.1.17. funetEduPersonPrimaryStudyToEnd 8
      2.1.18. funetEduPersonCreditUnits 8
      2.1.19. funetEduPersonECTS 9
      2.1.20. funetEduPersonStudentCategory 9
      2.1.21. funetEduPersonStudentStatus 10
      2.1.22. funetEduPersonStudentUnion 11
      2.1.23. funetEduPersonHomeCity 11
      2.1.24. funetEduPersonEPPNTimeStamp 11
   2.2. Attributes from schac 12
      2.2.1. schacMotherTongue 12
      2.2.2. schacGender 12
      2.2.3. schacDateOfBirth (supersedes funetEduPersonDateOfBirth) 12
      2.2.4. schacPlaceOfBirth 13
      2.2.5. schacCountryOfCitizenship 13
      2.2.6. schacHomeOrganization (supersedes funetEduPersonHomeOrganization) 13
      2.2.7. schacHomeOrganizationType 13
      2.2.8. schacCountryOfResidence 14
      2.2.9. schacUserPresenceID 14
      2.2.10. schacPersonalUniqueCode (supersedes funetEduPersonStudentID) 15
      2.2.11. schacPersonalUniqueID (supersedes funetEduPersonIdentityCode) 15
      2.2.12. schacUserStatus 16
   2.3. Attributes from eduPerson 16
      2.3.1. eduPersonAffiliation 16

2.3.2. eduPersonEntitlement 19
2.3.3. eduPersonNickname 20
2.3.4. eduPersonOrgDN 20
2.3.5. eduPersonOrgUnitDN 20
2.3.6. eduPersonPrimaryAffiliation 21
2.3.7. eduPersonPrimaryOrgUnitDN 22
2.3.8. eduPersonPrincipalName 22
2.3.9. eduPersonScopedAffiliation 24
2.3.10. eduPersonTargetedID 24
2.3.11. eduPersonAssurance 25
2.4. Common attributes 26
2.4.1. cn / commonName 26
2.4.2. description 26
2.4.3. displayName 27
2.4.4. employeeNumber 27
2.4.5. facsimileTelephoneNumber 27
2.4.6. givenName 27
2.4.7. homePhone 28
2.4.8. homePostalAddress 28
2.4.9. jpegPhoto 28
2.4.10. l / localityName 28
2.4.11. labeledURI 29
2.4.12. mail 29
2.4.13. mobile 30
2.4.14. o / organizationName 30
2.4.15. ou/organizationalUnitName 30
2.4.16. postalAddress 30
2.4.17. postalCode 31
2.4.18. preferredLanguage 31
2.4.19. seeAlso 31
2.4.20. sn / surname 31
2.4.21. street 32
2.4.22. telephoneNumber 32
2.4.23. title 32
2.4.24. uid 32
2.4.25. userCertificate 33
2.4.26. userPassword 33
2.4.27. userSMIMECertificate 33
3. Attributes for organisations 33
3.1. Attributes from eduOrg 33
3.1.1. eduOrgHomePageURI 33
3.1.2. eduOrgIdentityAuthNPolicyURI 34
3.1.3. eduOrgLegalName 34
3.1.4. eduOrgSuperiorURI 34
3.1.5. eduOrgWhitePagesURI 34
3.1.6. cn /commonName 34
3.1.7. description 34
3.1.8. facsimileTelephoneNumber 35
3.1.9. l (localityName) 35

3.1.10. o / organizationName 35
3.1.11. postalAddress 35
3.1.12. postalCode 35
3.1.13. postOfficeBox 35
3.1.14. seeAlso 36
3.1.15. street 36
3.1.16. telephoneNumber 36
3.2. Supplement attributes 36
3.2.1. mail 36
4. Other object classes 36
4.1. Attributes for courses and course memberships 36
4.2. Attributes for groups and group memberships 36
5. References 37
Appendix A: Collection of attributes for intra-organisational use 38
Appendix B: Changelog 40

1. 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.

2. Attributes for persons

Following attributes are mandatory:

cn
sn
displayName
eduPersonPrincipalName
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.

A separate document will be published on attributes that are recommended.

2.1. Supplement attributes in funetEduPerson

2.1.1. funetEduPersonHomeOrganization (SUPERSEDED)

Superseded by SchacHomeOrganization. See funetEduPerson ver 1.0 for details.

2.1.2. funetEduPersonStudentID (SUPERSEDED)

Superseded by SchacPersonalUniqueCode. See funetEduPerson ver 1.0 for details.

2.1.3. funetEduPersonIdentityCode (SUPERSEDED)

Superseded by schacPersonalUniqueID. See funetEduPerson ver 1.0 for details.

2.1.4. funetEduPersonDateOfBirth (SUPERSEDED)

Superseded by schacDateOfBirth. See funetEduPerson ver 1.0 for details.

2.1.5. funetEduPersonTargetDegreeUniversity (SUPERSEDED)

Superseded by funetEduPersonTargetDegree. See funetEduPerson ver 1.0 for details.

2.1.6. funetEduPersonTargetDegreePolytech (SUPERSEDED)

Superseded by funetEduPersonTargetDegree. See funetEduPerson ver 1.0 for details.

2.1.7. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.11			

Format: URN. Currently two common namespaces are defined for codes maintained by Central Statistical Office of Finland (tilastokeskus):

For universities:

Namespace urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:university

Vocabulary for the namespace (yliopistotutkintojen koodit):
http://www.tilastokeskus.fi/keruu/ylio/koodistot.html

For polytechnics:

Namespace urn:mace:funet.fi:attribute-def:funetEduPersonTargetDegree:polytechnic

Vocabulary for the namespace (amk-tutkinto):
http://www.tilastokeskus.fi/keruu/amkt/ammattikorkeakoulutunnukset.html

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.

Supersedes funetEduPersonTargetDegreePolytech and funetEduPersonTargetDegreeUniversity (change in syntax).

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

```
funetEduPersonTargetDegree: urn:mace:funet.fi
 :attribute-def:funetEduPersonTargetDegree:university:311
```

Examples: (polytechnic physiotherapist, a code defined by Central Statistical Office)

```
funetEduPersonTargetDegree : urn:mace:funet.fi
 :attribute-def:funetEduPersonTargetDegree:polytechnic:513
```

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

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

2.1.8. funetEduPersonEducationalProgramUniv (SUPERSEDED)

Superseded by funetEduPersonProgram. See funetEduPerson ver 1.0 for details.

2.1.9. funetEduPersonEducationalProgramPolytech (SUPERSEDED)

Superseded by funetEduPersonProgram. See funetEduPerson ver 1.0 for details.

2.1.10. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonProgram			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.12			

Format: URN. Currently two common namespaces are defined for codes maintained by Central Statistical Office of Finland (tilastokeskus):

For universities:

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

Vocabulary for the namespace (yliopistojen koulutusohjelmakoodit): http://www.tilastokeskus.fi/keruu/ylio/koodistot.html

For polytechnics:

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

Vocabulary for the namespace (amk-koulutusohjelma): http://www.tilastokeskus.fi/keruu/amkt/ammattikorkeakoulutunnukset.html

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.

Supersedes funetEduPersonEducationalProgramUniv and funetEduPersonEducationalProgramPolytech (change in syntax).

Examples: (Educational program of Political History, a code defined by Central Statistical Office)

```
funetEduPersonProgram: urn:mace:funet.fi
 :attribute-def:funetEduPersonProgram:university:1096
```

Examples: (degree programme in Environmental Management, a code defined by Central Statistical Office)

```
funetEduPersonProgram: urn:mace:funet.fi
 :attribute-def:funetEduPersonProgram:polytechnic:1001
```

2.1.11. funetEduPersonMajorUniv (SUPERSEDED)

Superseded by funetEduPersonSpecialisation. See funetEduPerson ver 1.0 for details.

2.1.12. funetEduPersonOrientationAlternPolytech (SUPERSEDED)

Superseded by funetEduPersonSpecialisation. See funetEduPerson ver 1.0 for details.

2.1.13. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonSpecialisation			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.13			

Format: URN. Currently two common namespaces are defined for codes maintained by Central Statistical Office of Finland (tilastokeskus):

For universities:

Namespace urn:mace:funet.fi:attribute-def:funetEduPersonSpecialisation:university

Vocabulary for the namespace (yliopistojen pääainekoodit):
http://www.tilastokeskus.fi/keruu/ylio/koodistot.html

For polytechnics:

Namespace urn:mace:funet.fi:attribute-def:funetEduPersonSpecialisation:polytechnic

Vocabulary for the namespace (amk-suuntautumisvaihtoehto):
http://www.tilastokeskus.fi/keruu/amkt/ammattikorkeakoulutunnukset.html

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.

Supersedes funetEduPersonMajorUniv and funetEduPersonOrientationAlternPolytech (change in syntax).

Examples: (gerontology, a code defined by Central Statistical Office)

```
funetEduPersonSpecialisation: urn:mace:funet.fi
 :attribute-def:funetEduPersonSpecialisation:university:0891
```

Examples: (Management of Built Environment, a code defined by Central Statistical Office)

```
funetEduPersonSpecialisation: urn:mace:funet.fi
 :attribute-def:funetEduPersonSpecialisation:polytechnic: 10042
```

2.1.14. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonStudyStart			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.14			

Format: YYYYMMDD

Examples:

```
funetEduPersonStudyStart: 20050826
```

2.1.15. 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

Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonPrimaryStudyStart
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.15

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
```

2.1.16. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonStudyToEnd			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.16			

Format: YYYYMMDD

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

Examples:

```
funetEduPersonStudyToEnd: 20070531
```

2.1.17. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonPrimaryStudyToEnd			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.17			

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
```

2.1.18. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonCreditUnits			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.18			

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
```

2.1.19. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonECTS			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.19			

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
```

2.1.20. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonStudentCategory			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.20			

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
```

2.1.21. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonStudentStatus			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.21			

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
```

2.1.22. 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
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonStudentUnion			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.22			

Examples:

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

2.1.23. funetEduPersonHomeCity

Home City (kotikunta) of the user.

OID	Syntax	# values	relevance
1.3.6.1.4.1.16161.1.1.23	DirectoryString	Single	May
Shibboleth 1.x name: urn:mace:funet.fi:attribute-def:funetEduPersonHomeCity			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.23			

Syntax: NNN

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

Examples: (Hauho)

```
funetEduPersonHomeCity: 083
```

2.1.24. 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
Shibboleth 1.x name: urn: urn:mace:funet.fi:attribute-def:funetEduPersonEPPNTimeStamp			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.16161.1.1.24			

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
```

2.2. Attributes from schac

2.2.1. schacMotherTongue

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacMotherTongue			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.1			

(schac 1.3.0) Format: See RFC 3066 Tags for the Identification of Languages

Examples:

```
schacMotherTongue: fr
schacMotherTongue: es-ES
schacMotherTongue: fi
```

2.2.2. schacGender

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacGender			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.2			

(schac 1.3.0) Format:

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

Examples:

```
schacGender: 2
```

2.2.3. schacDateOfBirth (supersedes funetEduPersonDateOfBirth)

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacDateOfBirth			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.3			

(schac 1.3.0) 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
```

2.2.4. schacPlaceOfBirth

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacPlaceOfBirth			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.4			

Examples:

```
schacPlaceOfBirth: Turku, Suomi
```

2.2.5. schacCountryOfCitizenship

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacCountryOfCitizenship			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.5			

(schac 1.3.0) Format: Two-letter country acronym in accordance with ISO 3166.

Examples:

```
schacCountryOfCitizenship: fi
```

2.2.6. schacHomeOrganization (supersedes funetEduPersonHomeOrganization)

(schac 1.3.0) Specifies a person´s home organization using the domain name of the organization.

OID	Syntax	# values	relevance
1.3.6.1.4.1.25178.1.2.9	directoryString	Single	MUST
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacHomeOrganization			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.9			

(schac 1.3.0) Format: Domain name acording to RFC 1035

Examples:

```
schacHomeOrganization: tut.fi
```

2.2.7. schacHomeOrganizationType

(schac 1.3.0) Type of a Home Organization.

OID	Syntax	# values	relevance
1.3.6.1.4.1.25178.1.2.10	DirectoryString	Single	MUST
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacHomeOrganizationType			

SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.10

(schac 1.3.0) Format: urn:mace:terena.org: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 http://www.terena.org/registry/terena.org/schac/homeOrganizationType/*
- *<string> from a nationally controlled vocabulary, published through the URI identified at the above mentioned TERENA URN registry.*

Examples:

```
schacHomeOrganizationType:
urn:mace:terena.org:schac:homeOrganizationType:fi:university

schacHomeOrganizationType:
 urn:mace:terena.org:schac:homeOrganizationType:fi:polytechnic

schacHomeOrganizationType:
 urn:mace:terena.org:schac:homeOrganizationType:fi:researchInstitution

schacHomeOrganizationType:
 urn:mace:terena.org:schac:homeOrganizationType:fi:other

schacHomeOrganizationType:
 urn:mace:terena.org:schac:homeOrganizationType:es:opi
```

2.2.8. schacCountryOfResidence

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacCountryOfResidence			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.11			

(schac 1.3.0) Format: Two-letter country acronym in accordance with ISO 3166 country code identifier.

Examples:

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

2.2.9. schacUserPresenceID

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacUserPresenceID			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.12			

(schac 1.3.0) 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
```

2.2.10. schacPersonalUniqueCode (supersedes funetEduPersonStudentID)

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacPersonalUniqueCode			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.14			

(schac 1.3.0) Format: urn:mace:terena.org: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 http://www.terena.org/registry/terena.org/schac/personalUniqueCode*
- *<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:mace:terena.org:schac
 :personalUniqueCode:int:studentID:tut.fi:165934
```

Examples:

```
schacPersonalUniqueCode: urn:mace:terena.org:schac
 :personalUniqueCode:se:LIN:87654321
```

2.2.11. schacPersonalUniqueID (supersedes funetEduPersonIdentityCode)

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacPersonalUniqueID			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.15			

(schac 1.3.0) Format: urn:mace:terena.org: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 http://www.terena.org/registry/terena.org/schac/personalUniqueID*
- *<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:mace:terena.org: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.

Examples:

```
schacPersonalUniqueID:
 urn:mace:terena.org:schac:personalUniqueID:fi:FIC:260667-123F

schacPersonalUniqueID:
 urn:mace:terena.org:schac:personalUniqueID:es:NIF:31241312L

schacPersonalUniqueID:
 urn:mace:terena.org:schac:personalUniquelD:se:NIN:12345678
```

2.2.12. schacUserStatus

(schac 1.3.0) 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
Shibboleth 1.x name: urn:mace:terena.org:schac:attribute-def:schacUserStatus			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.25178.1.2.19			

(schac 1.3.0) Format: urn:mace:terena.org: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 http://www.terena.nl/registry/terena.org/schac/userStatus/*
- *<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)):

```
schacUserStaus:
 urn:mace:terena.org:schac:userStatus:es:uma.es:affiliation:expired
schacUserStaus:
 urn:mace:terena.org:schac:userStatus:es:uma.es:sendMail:expired
schacUserStaus: urn:mace:terena.org: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:mace:terena.org:schac:userStatus:si:ujl.si:webmail:active+ttl=200605312359
59
```

2.3. Attributes from eduPerson

2.3.1. eduPersonAffiliation

(eduPerson200806) Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc.

OID	Syntax	# values	relevance
1.3.6.1.4.1.5923.1.1.1.1	DirectoryString	Multi	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonAffiliation			

SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.1

(eduPerson200806) Controlled vocabulary: faculty, student, staff, alum, member, affiliate, employee, library-walk-in.

If there is a value in eduPersonPrimary Affiliation, that value should be stored here as well.

The list of allowed values in the current version of the object class is CERTAINLY incomplete. We felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included as part of the later versions of eduPerson.

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

"Member" is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., they are given institutional email and calendar accounts). It could be glossed as "member in good standing of the university community."

"Affiliate" is intended to apply to people with whom the university has dealings, but to whom no general set of "community membership" privileges are extended.

"Library-walk-in:" This value is intended to facilitate the handling of a fairly widely encountered agreement between an institution and licensed resource providers that e-resources may be made accessible to students, faculty, staff and library walk-ins. This term originally indicated people who were physically present in a library facility. 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. Under appropriate licensing terms, it is valid to assert an affiliation of "library-walk-in" for members of this broader class of users. The affiliation "library-walk-in" is independent of any other affiliation value. In other words, having the affiliation "library-walk-in" has no effect, positive or negative, on any of the other defined affiliation values. Similarly, no other affiliation value implies or precludes the affiliation "library-walk-in."

Each institution decides the criteria for membership in each affiliation classification. A reasonable person should find the listed relationships commonsensical.

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)

- **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), 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)

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
```

2.3.2. eduPersonEntitlement

(eduPerson200806) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonEntitlement			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.7			

(eduPerson200806) 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
```

2.3.3. eduPersonNickname

(eduPerson200806) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonNickname			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.2			

(eduPerson200806) 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 2.4.1 for conventions for attributes carrying the name of an individual.

Examples:

```
eduPersonNickname: Sepi
```

2.3.4. eduPersonOrgDN

(eduPerson200806) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonOrgDN			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.3			

(eduPerson200806) 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
```

2.3.5. eduPersonOrgUnitDN

(eduPerson200806) 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

Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonOrgUnitDN
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.4

(eduPerson200806) 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
```

2.3.6. eduPersonPrimaryAffiliation

(eduPerson200806) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.5			

(eduPerson200806) Controlled vocabulary: 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.

The list of allowed values in the current version of the object class is CERTAINLY incomplete. We felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included as part of future versions of eduPerson.

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

"Member" is intended to include faculty, staff, student, and other persons granted a basic set of privileges that go with membership in the university community (e.g., library privileges). It could be glossed as "member in good standing of the university community."

"Affiliate" is intended to apply to people with whom the university has dealings, but to whom no general set of "community membership" privileges are extended.

"Library-walk-in:" This value is intended to facilitate the handling of a fairly widely encountered agreement between an institution and licensed resource providers that e-resources may be made accessible to students, faculty, staff and library walk-ins. This term originally indicated people who were physically present in a library facility. 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. Under appropriate licensing terms, it is valid to assert an affiliation of "library-walk-in" for members of this broader class of users. The affiliation "library-walk-in" is independent of any other affiliation value. In other words, having the

affiliation "library-walk-in" has no effect, positive or negative, on any of the other defined affiliation values. Similarly, no other affiliation value implies or precludes the affiliation "library-walk-in."

See 2.3.1 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.

2.3.7. eduPersonPrimaryOrgUnitDN

(eduPerson200806) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonPrimaryOrgUnitDN			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.8			

(eduPerson200806) 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.

2.3.8. eduPersonPrincipalName

(eduPerson200806) The "NetID" of the person for the purposes of inter-institutional authentication. It should be represented in the form "user@scope" where scope defines a local security domain.

OID	Syntax	# values	relevance
1.3.6.1.4.1.5923.1.1.1.6	DirectoryString	single	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonPrincipalName			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.6			

(eduPerson200806) *Multiple "@" signs are not recommended, but in any case, the first occurrence of the "@" sign starting from the left is to be taken as the delimiter between components. Thus, user identifier is to the left, security domain to the right of the first "@". This parsing rule conforms to the POSIX "greedy" disambiguation method in regular expression processing. When the scope is a registered domain name, the corresponding registrant organization is to be taken as the scope. For example, francis@trinity.edu would imply that the identity behind the ePPN has the "NetID" "francis" at the instituion of higher education that registered itself with the domain name "trinity.edu." If other value styles are used, their semantics will have to be profiled by the parties involved. Each value of scope defines a namespace within which the assigned principal names are unique. Given this rule, no pair of eduPersonPrincipalName values should clash. If they are the same, they refer to the same principal within the same administrative domain.*

If populated, the user should be able to authenticate with this identifier, using locally operated services. Local authentication systems should be able to adequately affirm (to both local and remote applications) that the authenticated principal is the person to whom this identifier was issued.

The initial intent is to use this attribute within the Shibboleth project, http://shibboleth.internet2.edu/. However, it has quickly become clear that a number of other applications could also make good use of this attribute (e.g. H.323 video, chat

software, etc). eduPersonPrincipalName (EPPN) would be used as follows: A resource owner, A, would look at B's directory entry to discover B's EPPN. A would then tell the local authorization system that B's EPPN is allowed to use the resource. When B tries to access the resource, the application (or access control infrastructure) would validate B's identity, check with the local authorization system to ensure that B has been granted the appropriate access privileges, and then either grant or deny access.

EPPN looks like a Kerberos identifier (principal@realm). A site might choose to locally implement EPPN as Kerberos principals. However, this is not a requirement. A site can choose to do authentication in any way that is locally acceptable.

Likewise, EPPN should NOT be confused with the user's published email address, although the two values may be the same. Some sites have chosen to make the user portion of email addresses and security principals the same character string; other sites have chosen not to do this. Even when they appear to be the same, they are used in different subsystems and for different purposes, and there is no requirement that they have to remain the same.

The uid attribute of the user's object within the local white pages directory may also contain a login id, a security principal; some systems (eg NDS) may put a login id in the cn attribute. These attributes are defined within objectclasses that are universal. Unfortunately, their use is not prescribed in a sufficiently precise and consistent manner for use with cross domain authorization. A variety of systems already make conflicting use of these attributes; consequently, we have defined this new attribute.

An assumption is that EPPNs are managed on an enterprise basis by the univ of univ.edu. A particular EPPN is assigned solely to the associated user; it is not a security principal identifier shared by more than one person. Lastly, each EPPN is unique within the local security domain.

How long, if ever, before a formerly assigned EPPN is reassigned to a differrent individual is an institutional decision. Some institutions will choose never to reassign EPPNs. Others may opt for a relatively short hiatus before reassignment. While this complicates the work of the relying parties, it is unavoidable given institutional autonomy. See MACE best practice documents on identifiers for further discussion of these issues.

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

This attribute should prove useful in creating some applications that are based on currently deployed technologies and on code that does not currently use LDAP or require a PKI. This attribute should help to create a framework to foster interesting inter-institutional collaborations between sites that use different technologies. In short, this attribute provides a foundation for yet another abstraction layer.

Examples:

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

2.3.9. eduPersonScopedAffiliation

(eduPerson200806) 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	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonScopedAffiliation			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.9			

(eduPerson200806) 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
```

2.3.10. eduPersonTargetedID

(eduPerson200806) A persistent, non-reassigned, privacy-preserving identifier for a principal shared between a pair of coordinating entities, denoted by the SAML 2 architectural overview [1] as identity provider and service provider (or a group of service providers). An identity provider uses the appropriate value of this attribute when communicating with a particular service provider or group of service providers, and does not reveal that value to any other service provider except in limited circumstances.

OID	Syntax	# values	relevance
1.3.6.1.4.1.5923.1.1.1.10	DirectoryString	Multi	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:eduPersonTargetedID			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.10			

(eduPerson200806) While this attribute might not be stored as such in a typical Directory Service, it may be produced by a Directory Service. In any case, it is defined here for potential use in other service contexts such as Security Assertion Markup Language (SAML) assertions.

EduPersonTargetedID values should not be reassigned.

Persistence

eduPersonTargetedID does not require 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 a particular service that is consuming it. Protocols might also be used to refresh (or "roll-over") an identifier to maintain the user's privacy by communicating such changes to service providers to avoid a loss of service. See [2] for an example of such a protocol.

Privacy

This attribute is designed to preserve the principal's privacy and inhibit the ability of multiple unrelated services from correlating principal activity by comparing values. It is therefore REQUIRED to be opaque, having no particular relationship to the principal's other identifiers, such as a username or eduPersonPrincipalName. It SHOULD be considerably difficult for an observer to guess the value that would be returned to a given service provider.

It MAY be a pseudorandom value generated and stored by the identity provider, or MAY be derived from some function over the service provider's identity and other principal-specific input(s), such as a serial number or UUID assigned by the identity provider.

It MUST NOT exceed 256 characters in length.

Uniqueness

A value of this attribute is intended only for consumption by a specific audience of applications (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. Logically, the attribute value is made up of the triple of an identifier, the identity provider, and the service provider(s). [2] suggests a possible naming scheme for such qualifiers based on URIs.

Reassignment

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

[1] http://www.oasis-open.org/committees/download.php/7521/

[2] http://www.oasis-open.org/committees/download.php/10627/

2.3.11. eduPersonAssurance

(eduPerson200806) 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
SAML 2.0 name: urn:oid:1.3.6.1.4.1.5923.1.1.1.11			

(eduPerson200806) 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
```

2.4. Common attributes

2.4.1. 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.

OID	Syntax	# values	relevance
2.5.4.3	DirectoryString	multi	MUST
Shibboleth 1.x name: urn:mace:dir:attribute-def:cn			
SAML 2.0 name: urn:oid:2.5.4.3			

(eduPerson200806) 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 = all given names
- cn = the name the individual has registered as the one (s)he uses + sn
- displayName = the name the individual has registered as the one (s)he uses
- eduPersonNickname = the informal name by which the individual is accustomed to be hailed

Examples:

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

2.4.2. description

(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
Shibboleth 1.x name: urn:mace:dir:attribute-def:description			
SAML 2.0 name: urn:oid:2.5.4.13			

(eduPerson200806) Open-ended; whatever the person or the directory manager puts here.

2.4.3. displayName

(RFC 2798) Preferred name of a person to be used when displaying entries.

OID	Syntax	# values	relevance
2.16.840.1.113730.3.1.241	DirectoryString	Single	MUST
Shibboleth 1.x name: urn:mace:dir:attribute-def:displayName			
SAML 2.0 name: urn:oid:2.16.840.1.113730.3.1.241			

(eduPerson200806) 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 2.4.1 for conventions for attributes carrying the name of an individual.

2.4.4. 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:employeeNumber			
SAML 2.0 name: urn:oid:2.16.840.1.113730.3.1.3			

Locally unique.

Examples:

```
employeeNumber: 1054
```

2.4.5. facsimileTelephoneNumber

(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
Shibboleth 1.x name: urn:mace:dir:attribute-def:facsimileTelephoneNumber			
SAML 2.0 name: urn:oid:2.5.4.23			

(eduPerson200806) Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."

2.4.6. givenName

(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	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:givenName			
SAML 2.0 name: urn:oid:2.5.4.42			

See 2.4.1 for conventions for attributes carrying the name of an individual.

2.4.7. 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:homePhone			
SAML 2.0 name: urn:oid:0.9.2342.19200300.100.1.20			

Examples:

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

2.4.8. 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:homePostalAddress			
SAML 2.0 name: urn:oid:0.9.2342.19200300.100.1.39			

$ is used as a line separator

Examples:

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

2.4.9. 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
SAML 2.0 name: urn:oid:0.9.2342.19200300.100.1.60			

2.4.10. l / localityName

(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."

OID	Syntax	# values	relevance
2.5.4.7	DirectoryString	Multi	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:l			
SAML 2.0 name: urn:oid:2.5.4.7			

Examples:

```
l: Viikki
```

2.4.11. labeledURI

(eduPerson200806) Follow inetOrgPerson definition of RFC 2079: "Uniform Resource Identifier with optional label."

Most 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:labeledURI			
SAML 2.0 name: urn:oid:1.3.6.1.4.1.250.1.57			

(eduPerson200806) 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]
```

2.4.12. 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	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:mail			
SAML 2.0 name: urn:oid:0.9.2342.19200300.100.1.3			

(eduPerson200806)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. (http://middleware.internet2.edu/dir/docs/ldap-recipe.htm).

Examples:

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

2.4.13. mobile

(RFC 4524) The 'mobile' (mobileTelephoneNumber) attribute specifies mobile telephone numbers (e.g., "+1 775 555 6789") associated with a person (or entity).

OID	Syntax	# values	relevance
0.9.2342.19200300.100.1.41	TelephoneNumber	Multi	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:mobile			
SAML 2.0 name: urn:oid:0.9.2342.19200300.100.1.41			

(eduPerson200806) 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
```

2.4.14. o / organizationName

(eduPerson200806) Standard name of the top-level organization (institution) with which this person is associated.

OID	Syntax	# values	relevance
2.5.4.10	DirectoryString	Multi	May
Shibboleth 1.x name: urn:mace:dir:attribute-def:o			
SAML 2.0 name: urn:oid:2.5.4.10			

Examples:

```
o: University of Tampere
```

2.4.15. ou/organizationalUnitName

(eduPerson200806) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:ou			
SAML 2.0 name: urn:oid:2.5.4.11			

(eduPerson200806) 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
```

2.4.16. postalAddress

(eduPerson200806) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:postalAddress			
SAML 2.0 name: urn:oid:2.5.4.16			

Examples:

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

2.4.17. postalCode

(eduPerson20080006) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:postalCode			
SAML 2.0 name: urn:oid:2.5.4.17			

(eduPerson20080006) ZIP code in USA, postal code for other countries.

Examples:

```
postalCode: 02101
```

2.4.18. 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:preferredLanguage			
SAML 2.0 name: urn:oid:2.16.840.1.113730.3.1.39			

(eduPerson200806) 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
```

2.4.19. 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:seeAlso			
SAML 2.0 name: urn:oid:2.5.4.34			

Examples:

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

2.4.20. 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."

OID	Syntax	# values	relevance
2.5.4.4	DirectoryString	Multi	MUST
Shibboleth 1.x name: urn:mace:dir:attribute-def:sn			
SAML 2.0 name: urn:oid:2.5.4.4			

Object class person requires that the sn is defined.

See 2.4.1 for conventions for attributes carrying the name of an individual.

2.4.21. 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:street			
SAML 2.0 name: urn:oid:2.5.4.9			

Examples:

```
street: Korkeakoulunkatu 1
```

2.4.22. telephoneNumber

(eduPerson200806) 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:telephoneNumber			
SAML 2.0 name: urn:oid:2.5.4.20			

2.4.23. 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:title			
SAML 2.0 name: urn:oid:2.5.4.12			

Examples:

```
Title: professor
```

2.4.24. 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
Shibboleth 1.x name: urn:mace:dir:attribute-def:uid			
SAML 2.0 name: urn:oid:0.9.2342.19200300.100.1.1			

(eduPerson200806) Likely only one value. See the extensive discussion in the "LDAP Recipe" (http://middleware.internet2.edu/dir/docs/ldap-recipe.htm).

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

2.4.25. userCertificate

(eduPerson200806) 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
SAML 2.0 name: urn:oid:2.5.4.36			

(eduPerson200806) 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).

2.4.26. userPassword

(eduPerson200806) This attribute identifies the entry's password and encryption method in the following format:

{encryption method}encrypted password.

OID	Syntax	# values	relevance
2.5.4.35	DirectoryString	Multi	May

(eduPerson200806) 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.

2.4.27. 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
SAML 2.0 name: urn:oid:2.16.840.1.113730.3.1.40			

(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.'

3. 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.

3.1. Attributes from eduOrg

3.1.1. 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/
```

3.1.2. 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
```

3.1.3. 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
```

3.1.4. 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

3.1.5. 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

3.1.6. cn /commonName

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

OID	Syntax	# values	relevance
2.5.4.3	DirectoryString	multi	May

Example:

```
cn: University of Lapland
```

3.1.7. 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

3.1.8. 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

3.1.9. 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

3.1.10. o / organizationName

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

OID	Syntax	# values	relevance
2.5.4.10	DirectoryString	multi	May

3.1.11. 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

3.1.12. 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

3.1.13. 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

3.1.14. 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

3.1.15. 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

3.1.16. 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

3.2. Supplement attributes

3.2.1. 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
```

4. Other object classes

4.1. Attributes for courses and course memberships

Institutions are advised to follow development of the eduCourse schema of Internet2.

http://middleware.internet2.edu/courseid

4.2. Attributes for groups and group memberships

Institutions are advised to follow development of the eduMember schema of Internet2.

http://middleware.internet2.edu/dir/groups

5. References

eduOrg200210

Internet2 Middleware Architecture Committee, Directory Working Group. “EduOrg Object Class Specification (200210).” October, 2002. http://www.educause.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.

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

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 2.0:

- 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