Recommendation for the schema of the Funet directories in Finland

v. 1.0 / 16.06.2003

Table of Contents

Introduction

The main purpose of this document is to present object classes and attributes available for the cross-organizational user administration in Finland.

Chapter 2 describes the set of mandatory attributes of various standardized object classes and the new object class funetEduPerson that *has to be used* when participating in cross-organizational actions. For example, if a person´s uid -attribute is not populated, he can not have access to the services provided by the target site of another organization.

The new funetEduPerson object class has been specified for the needs that will occur when identifying and authorizing users for network services.

There are also optional attributes that can be used both for cross-organizational authentication and white pages –type purposes according to the decisions and needs of the home organization. These attributes are introduced briefly in the *chapter 3*.

Chapter 4 is an informal collection of attributes used in the intra-organizational user administration of Finnish universities. They have been introduced for special needs by a single Finnish university or a Polytechnic. The list is purely advisory and optional.

If the vocabulary of an attribute is not specified, the language used in attribute values can be selected from Finnish, Swedish and English

2. Mandatory attributes for cross-organizational use

These attributes are relevant for objects in the People –branch of the directory.

2.1 cn / commonName OID 2.5.4.3 (object class person)

RFC 2256: 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.

funetEduPerson relevance: **MUST**

Notes: object class person requires that the cn is defined.

2.2 sn / surname OID 2.5.4.4 (object class person)

RFC 2256: "This is the X.500 surname attribute, which contains the family name of a person."

funetEduPerson relevance: **MUST**

Notes: object class person requires that the sn is defined.

2.3 uid OID 0.9.2342.19200300.100.1.1 (inetOrgPerson)

RFC 2798: "Identifies the entry´s userid (usually the logon ID)."

funetEduPerson relevance: **MUST**

2.4 givenName OID 2.5.4.42 (organizationalPerson)

RFC 2256: "The givenName attribute is used to hold the part of a person's name which is not their surname nor middle name."

funetEduPerson relevance: **MUST**

Notes: There is no other standardized attribute to describe a person´s forename or first name, therefore this is recommended to be used for all Finnish given names, for example Mikko Matinpoika Johannes.

2.5 funetEduPersonHomeOrganization OID 1.3.6.1.4.1.16161.1.1.9 (funetEduPerson)

Specifies a person´s home organization using the domain name of the organization, in Finland for example tut.fi, pspt.fi.

funetEduPerson relevance: **MUST**
Notes: This is the only mandatory attribute of the funetEduPerson object class. Domain name of the organization as a value is more informative than for example a numeric code.

2.6 Optional attributes both for intra- and cross-organizational use

----

In addition with those attributes mentioned in the chapter 2 earlier, the following attributes can be used both in intra-organization directories and in cross-organizational use. For funetEduPerson the relevance of them is optional.

Objectclass person (RFC 2256)

telephoneNumber OID 2.5.4.20

RFC 2256: Office/campus phone number. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567."

funetEduPerson relevance: **MAY**

description OID 2.5.4.13

RFC 2256: “This attribute contains a human-readable description of the object”

funetEduPerson relevance: **MAY**

seeAlso OID 2.5.4.34

RFC 2256: Follow person object class definition: Identifies (by DN) another directory server entry that may contain information related to this entry. According to X.520 (2000), "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."

funetEduPerson relevance: **MAY**

userPassword OID 2.5.4.35

EduPerson 200210: “This attribute identifies the entry’s password and encryption method in the following format: {encryption method}encrypted password.
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. ”

Notes: The entry´s password has to be encrypted. This attribute must deploy MD5, SHA-1 or Unix encryption methods and identify it in the format {method}encrypted password.

funetEduPerson relevance: **MAY**

Objectclass organizationalPerson (RFC 2256)

title OID 2.5.4.12

RFC 2256: "This attribute contains the title, such as "Vice President", of a person in their organizational context. The "personal-Title" attribute would be used for a person's title independent of their job function."

funetEduPerson relevance: **MAY**

street OID 2.5.4.9

RFC 2256: "This attribute contains the physical address of the object to which the entry corresponds, such as an address for package delivery (streetAddress)."

funetEduPerson relevance: **MAY**

facsimileTelephoneNumber OID 2.5.4.23

RFC 2256: "Fax number"

funetEduPerson relevance: **MAY**

o / organizationName OID 2.5.4.10

RFC 2256: "This attribute contains the name of an organization."

funetEduPerson relevance: **MAY**

postalAddress OID 2.5.4.16

RFC 2256: "Campus or office address. X.520 (2000) reads: "The Postal Address attribute type specifies the address information required for the physical postal delivery to an object."

funetEduPerson relevance: **MAY**

postalCode OID 2.5.4.17

RFC 2256: "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." Zip code in USA, postal code for other countries."

funetEduPerson relevance: **MAY**

ou/organizationalUnitName OID 2.5.4.11

RFC 2256: "This attribute contains the name of an organizational unit."

funetEduPerson relevance: **MAY**

l / localityName OID 2.5.4.7

RFC 2256: "This attribute contains the name of a locality, such as a city, county or other geographic region."

funetEduPerson relevance: **MAY**

Objectclass inetOrgPerson (RFC 2798)

displayName OID 16.840.1.113730.3.1.241

RFC 2798: "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 multi-valued, an additional attribute type is needed. Display name is defined for this purpose."

funetEduPerson relevance: **MAY**

jpegPhoto OID 0.9.2342.19200300.100.1.60

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

funetEduPerson relevance: **MAY**

labeledURI OID 1.3.6.1.4.1.250.1.57

RFC 2798: "Follow inetOrgPerson definition of RFC 2079: "Uniform Resource Identifier with optional label. Commonly a URL for a web site associated with this person. Good candidate for a self-maintained attribute. Note, however, that the vocabulary for the label portion of the value is not standardized.

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").

An example of a labeledURI attribute value that does not include a label:
ftp://ds.internic.net/rfc/rfc822.txt

An example of a labeledURI attribute value that contains a tilde character in the URL (special characters in a URL must be encoded as specified by the URL document [1]). The label is "LDAP Home Page": http://www.umich.edu/%7Ersug/ldap/ LDAP Home Page

Another example. This one includes a hint in the label to help the user realize that the URL points to a photo image. http://champagne.inria.fr/Unites/rennes.gif Rennes [photo]

Semantics: Most commonly a URL for a web site associated with this person."

funetEduPerson relevance: **MAY**

userCertificate OID 2.5.4.36

RFC 2798: "PKCS #12 [PKCS12] provides a format for exchange of personal identity information. When such information is stored in a directory service, the userPKCS12 attribute should be used. This attribute is to be stored and requested in binary form, as 'userPKCS12;binary'. The attribute values are PFX PDUs stored as binary data."

funetEduPerson relevance: **MAY**

preferredLanguage OID 2.16.840.1.113730.3.1.39

RFC 2798: "Used to indicate an individual's preferred written or spoken language. This is useful for inter-national correspondence or human-computer interaction. Values for this attribute type MUST conform to the definition of the Accept-Language header field defined in RFC 2068 with one exception: the sequence "Accept-Language" ":" should be omitted."
vocabulary: ISO 639-1 -standard (Codes for the representation of names of languages)

funetEduPerson relevance: **MAY**

homePhone OID 0.9.2342.19200300.100.1.20

RFC 2798: "The Home Telephone Number attribute type specifies a home telephone number associated with a person. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567". (RFC 1274)

funetEduPerson relevance: **MAY**

homePostalAddress OID 0.9.2342.19200300.100.1.39

RFC 2798: "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. (RFC1274)"

funetEduPerson relevance: **MAY**

mail OID 0.9.2342.19200300.100.1.3

RFC 2798: "email address"

funetEduPerson relevance: **MAY**

mobile OID 0.9.2342.19200300.100.1.41

RFC 2798: "This attribute contains the number of a cellular or mobile phone"

funetEduPerson relevance: **MAY**

Objectclass eduPerson (v200210 / mace)
http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduPerson-200210.pdf

eduPersonAffiliation OID 1.3.6.1.4.1.5923.1.1.1.1 (eduPerson)

The quotation from the eduPerson standard: "Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (*Permissible values (if controlled)* **faculty, student, staff, alum, member, affiliate, employee**)."

funetEduPerson relevance: **MAY**

Notes: It is vital to specify how these values should be used in Finnish organizations to avoid contradictions.

- Student = a student aiming at an academic or polytechnic degree; e.g. bachelor, master, doctor. A person *has to have* the *attending*-status to be able to receive this attribute value.
- Faculty = academic workers at laboratories and institutes; e.g. professors, researchers, lecturers, assistants, also Finnish Academy researchers and docents (although not employed by org.)
- Staff = administrational workers employed by the organization, e.g. staff in the library, staff in the IT center, secretaries, staff in the administration
- Employee = a person employed by the organization, covers both Faculty and Staff
- Member = This value covers all categories mentioned above and also students not aiming at an academic degree (Students of open university, people attending updating education courses etc.).
- 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 outside member of a research group who has to be allowed to access a certain resource.
- Alumn = a graduated student of a university

The quotation from the eduPerson standard: "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."

eduPersonEntitlement OID: 1.3.6.1.4.1.5923.1.1.1.7

The quote from eduPerson 200210: "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:
eduPersonEntitlement: http://xstor.com/contracts/HEd123
eduPersonEntitlement: urn:mace:washington.edu:confocalMicroscope"

funetEduPerson relevance: **MAY**

eduPersonPrincipalName OID 1.3.6.1.4.1.5923.1.1.1.6 (eduPerson)

eduPerson 1.0: "The "NetID" of the person for the purposes of cross-organizational authentication. Should be stored in the form of user@univ.edu, where univ.edu is the name of the local security domain."

funetEduPerson relevance: **MAY**

Notes: **username@domain** name of the organization can be used as EPPN, although it may change, e.g. virtanen@tut.fi. If the username can be reassigned to another person, it is strongly recommended that there will be a break of 2 years before.

The quotation from A receipe for Configuring and Operating LDAP Directories by Michael R Gettes:

To provide some perspective on the use of this attribute, Paul Hill (MIT) has contributed the following:

> "The EPPN is intended to be an expedient attribute, useful for building some inter-institutional applications. It is intended that this attribute will be useful to create some applications that are based on currently deployed technologies and code that do not currently use LDAP or require a PKI. This attribute should help to create a framework to create interesting inter-institutional collaborations between sites that use different technologies. In short, this attribute provides a foundation for yet another abstraction layer.
>
> It is also expected that this attribute may become deprecated in the future. This would occur as LDAP enabled infrastructures and applications become more mature. One metric of this maturity will be the convergence of best practices and their consistent deployments."

The quotation from the eduPerson standard: "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. Over time, many sites are expected to be using PKI for authentication; however, they may still be specifying identity in EPPN format.

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.

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.

It is expected that this attribute may become deprecated in some future version of eduPerson. This would occur as LDAP enabled infrastructures and applications become more mature. One metric of this maturity will be the convergence on best practices and their widespread adoption."

eduPersonOrgDN OID 1.3.6.1.4.1.5923.1.1.1.3

eduPerson 1.0: "The distinguished name (DN) of the directory entry representing the institution with which the person is associated."

funetEduPerson relevance: **MAY**

eduPersonOrgUnitDN OID 1.3.6.1.4.1.5923.1.1.1.4

eduPerson 1.0: "The distinguished name (DN) of the directory entries representing the person's Organizational Unit(s)."

funetEduPerson relevance: **MAY**

eduPersonPrimaryAffiliation OID 1.3.6.1.4.1.5923.1.1.1.5

eduPerson 1.0: "Specifies the person's PRIMARY relationship to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).

Permissible values (if controlled): faculty, student, staff, alum, member, affiliate, employee

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.

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

Notes: It is vital to specify how these values should be used in Finnish organizations to avoid contradictions.

- Student = a student aiming at an academic or polytechnic degree; e.g. bachelor, master, doctor. A person *has to have* the *attending*-status to be able to receive this attribute value.
- Faculty = academic workers at laboratories and institutes; e.g. professors, researchers, lecturers, assistants, also Finnish Academy researchers and docents (although not employed by org.)
- Staff = administrational workers employed by the organization, e.g. staff in the library, staff in the IT center, secretaries, staff in the administration
- Employee = a person employed by the organization, covers both Faculty and Staff
- Member = tThis value covers all categories mentioned above and also students not aiming at an academic degree (Students of open university, people attending updating education courses etc.).
- 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 outside member of a research group who has to be allowed to access a certain resource.
- Alumn = a graduated student of a university

eduPersonPrimaryOrgUnitDN OID 1.3.6.1.4.1.5923.1.1.1.8

eduPerson 200210: “The distinguished name (DN) of the directory entry representing the person's primary Organizational Unit(s).”

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.”

funetEduPerson relevance: **MAY**

Objectclass EduOrg (v. 200210 / mace) (Objectclass Organization standard X.521/2001) http://www.nmi-edit.org/eduOrg/internet2-mace-dir-eduOrg-200210.pdf

These attributes are relevant for objects in the Org –branch of the directory.

o / organizationName OID 2.5.4.10 (eduOrg)

v. 200210 / mace: "Standard name of the top-level organization (institution)." Required.

funetEduPerson relevance: **MAY**

eduOrgHomePageURI OID 1.3.6.1.4.1.5923.1.2.1.2

v. 200210 / mace: "The URL for the organization's top level home page."

funetEduPerson relevance: **MAY**

eduOrgIdentityAuthNPolicyURI OID 1.3.6.1.4.1.5923.1.2.1.3

v. 200210 / mace: "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."

funetEduPerson relevance: **MAY**

eduOrgLegalName OID 1.3.6.1.4.1.5923.1.2.1.4

v. 200210 / mace: "The organization´s legal corporate name."

funetEduPerson relevance: **MAY**

eduOrgSuperiorURI OID 1.3.6.1.4.1.5923.1.2.1.5

v. 200210 / mace: "LDAP URL for the organization object one level superior to this entry."

funetEduPerson relevance: **MAY**

eduOrgWhitePagesURI OID 1.3.6.1.4.1.5923.1.2.1.6

v. 200210 / mace: "The URL of the open white pages directory service for the university, predominantly LDAP these days."

funetEduPerson relevance: **MAY**

cn /commonName OID 2.5.4.3

v. 200210 / mace: "X.520 (2001) "commonName." Name or names by which this organization is commonly known."

funetEduPerson relevance: **MAY**

description OID 2.5.4.13

v. 200210 / mace: "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"."

funetEduPerson relevance: **MAY**

facsimileTelephoneNumber OID 2.5.4.23

v. 200210 / mace: "A fax number for the directory entry. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567."

funetEduPerson relevance: **MAY**

l (localityName) OID 2.5.4.7

v. 200210 / mace: "This attribute contains the name of the locality, such as a city, county or other geographic region."

funetEduPerson relevance: **MAY**

mail OID 0.9.2342.19200300.100.1.3

v. 200210 / mace: "email address (of the organization)"

funetEduPerson relevance: **MAY**

postalAddress OID 2.5.4.16

v. 200210 / mace: "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."

funetEduPerson relevance: **MAY**

postalCode OID 2.5.4.17

v. 200210 / mace: "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."

funetEduPerson relevance: **MAY**

postOfficeBox OID 2.5.4.18

v. 200210 / mace: "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."

funetEduPerson relevance: MAY

seeAlso OID 2.5.4.34

v. 200210 / mace: "Identifies (by DN) another directory server entry that may contain information related to this entry."

funetEduPerson relevance: **MAY**

street OID 2.5.4.9

v. 200210 / mace: "Street address of the primary campus offices."

funetEduPerson relevance: **MAY**

telephoneNumber OID 2.5.4.20

v. 200210 / mace: "Main campus phone number. Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567."

funetEduPerson relevance: **MAY**

3. funetEduPerson –object class

There are certain needs that standardized object classes can not satisfy. Therefore the new object class funetEduPerson, attributes and vocabularies must have been specified.

funetEduPerson –object class (OID 1.3.6.1.4.1.16161.1.1):

funetEduPersonIdentityCode

funetEduPersonDateOfBirth

funetEduPersonTargetDegreeUniversity

funetEduPersonTargetDegreePolytech

funetEduPersonEducationalProgramUniv

funetEduPersonEducationalProgramPolytech

funetEduPersonOrientationAlternPolytech

funetEduPersonMajorUniv

funetEduPersonHomeOrganization

funetEduPersonStudentID

---

funetEduPersonIdentityCode OID 1.3.6.1.4.1.16161.1.1.1

Desc	Finnish Identity Code (earlier social security number) (Väestörekisterikeskuksen myöntämä suomalainen henkilötunnus)
Semantics	Specifies the person´s Finnish Identity Code. The code is assigned by Population Registration Centre (Väestörekisterikeskus). (For foreign people some information systems are able to create artificial identity codes.)
LDAP Syntax	1.3.6.1.4.1.1466.115.121.1.15
Number of values	Single
Classification	Optional, MAY
Examples	260667-123F

Usage	Identification
Notes	Foreign students and employees seldom have Finnish Identity Code or the code part of it is artificial and made by the home organization. Therefore the classification is optional.

funetEduPersonDateOfBirth OID 1.3.6.1.4.1.16161.1.1.2

Desc	Person´s date of birth
Semantics	Specifies a person´s date of birth
LDAP Syntax	1.3.6.1.4.1.1466.115.121.1.15
Number of values	Single
Classification	Optional, MAY
Examples	26.06.1967
Usage	Identification
Notes	There are educational organizations in Finland that do not or can not identify people using the Finnish Identity Code. For identification purposes this attribute is weak.

funetEduPersonTargetDegreeUniversity OID 1.3.6.1.4.1.16161.1.1.3

Desc	Person´s academic target degree
Semantics	Specifies the person´s target degree in his home university using the classification of Central Statistical Office of Finland: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/yliopistot_tutkinnot.xls
LDAP Syntax	1.3.6.1.4.1.1466.115.121.1.27
Number of values	Multi
Classification	Optional, MAY
Examples	311 (doctor of Theology)
Usage	Can be used when authorizing students for personified services according to their academic target degree.

Notes This attribute is for a university student only, there is another for polytechnics. This is due to the fact that the codes are different for university and polytechnic.

funetEduPersonTargetDegreePolytech OID 1.3.6.1.4.1.161.1.1.4

Desc Person´s polytechnical target degree

Semantics Specifies the person´s target degree in his home polytechnic using the classification of Central Statistical Office of Finland: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/amk_tutkintokoodit.xls

LDAP Syntax 1.3.6.1.4.1.1466.115.121.1.27

Number of values Multi

Classification Optional, MAY

Examples 513 (physiotherapist)

Usage Can be used when authorizing students for personified services

Notes This attribute is for a student in polytechnics only, there is another for a university student.

funetEduPersonEducationalProgramUniv OID 1.3.6.1.4.1.16161.1.1.5

Desc The educational program of a student

Semantics Specifies a student´s educational program using the classification of Central Statistical Office of Finland: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/yliopistot_kokoodit.xls

LDAP Syntax 1.3.6.1.4.1.1466.115.121.1.27

Number of values Multi

Classification Optional, MAY

Examples 1096 (Educational program of Political History)

Usage Can be used when authorizing students for personified services according to their academic educational program.

funetEduPersonEducationalProgramPolytech OID 1.3.6.1.4.1.16161.1.1.6

Desc Student´s educational program in his home polytechnic

Semantics Specifies a student´s educational program using the classification of Central Statistical Office of Finland: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/amk_kokoodit.xls

LDAP Syntax 1.3.6.1.4.1.1466.115.121.1.27

Number of values Multi

Classification Optional, MAY

Examples 1001 (degree programme in Environmental Management)

Usage Can be used when authorizing students for personified services according to their polytechnical educational program.

Notes This attribute is for a polytechnical student only.

funetEduPersonOrientationAlternPolytech OID 1.3.6.1.4.1.16161.1.1.7

Desc Student´s orientation alternative in his home polytechnic

Semantics Specifies a student´s orientation alternative using the classification of Central Statistical Office of Finland: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/amk_svkoodit.xls

LDAP Syntax 1.3.6.1.4.1.1466.115.121.1.27

Number of values Multi

Classification Optional, MAY

Examples 10042 (Management of Built Environment)

Usage Can be used when authorizing students for personified services according to their polytechnical orientation alternative.

funetEduPersonMajorUniv OID 1.3.6.1.4.1.16161.1.1.8

Desc Student´s main subjects in a university

Semantics Specifies a student´s main subject(s) using the classification of Central Statistical Office of Finland: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/yliopistot_pakoodit.xls

LDAP Syntax 1.3.6.1.4.1.1466.115.121.1.27

Number of values Multi

Classification Optional, MAY

Examples 0891 (gerontology)

Usage Can be used when authorizing students for personified services according to their main subject(s).

Notes This attribute is for a university student only (because of the vocabulary used)

funetEduPersonHomeOrganization OID 1.3.6.1.4.1.16161.1.1.9

Desc Person´s home organization

Semantics Specifies a person´s home organization using the domain name of the organization

LDAP Syntax 1.3.6.1.4.1.1466.115.121.1.15

Number of values Single

Classification Mandatory, MUST

Examples tut.fi, pspt.fi

Usage Authorization

Notes This is the only MUST-attribute of the funetEduPerson objectclass. Domain name of the organization as a value is more informative than for example a numeric code.

If a person is studying in two different universities at the same time, he has two different identities and two different Home Organizations.

funetEduPersonStudentID OID 1.3.6.1.4.1.16161.1.1.10

Desc a person´s student number

Semantics Specifies a person´s student number in his university or polytechnic

LDAP Syntax 1.3.6.1.4.1.1466.115.121.1.15

Number of values Multi

Classification Optional, MAY

Examples	A123456
Usage	Identification
Notes	At the moment this attribute is common for both university and polytechnic students. It is also multi-valued and alphanumeric, a lot of different syntaxes are used. funetEduPersonStudentID is locally, but not globally, unique.

4. List of attributes used for intra-organizational directories

----

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

This part of the recommendation is purely advisory and does not require any actions by a university or a polytechnic.

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

- persons, e.g. People
- user accounts, e.g. Accounts or Posixaccounts
- department information, e.g. Departments
- groups

Useful attributes relevant for a person:

(own)PersonPrimaryAffiliation # primary affiliation for a person within own organization, vocabylary local
(own)PersonAffiliation # other affiliation for a person within own organization
(own)PersonStudentNoInfo # single-valued (0/1), a student may allow or refuse to give 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

```
# funetEduPerson LDAP-schema v. 1.0
#____________________________________________________________________________
#
# attributes:
#
# funetEduPersonIdentityCode
# Finnish Identity Code
# alphanumeric
# single-valued
attributetype (1.3.6.1.4.1.16161.1.1.1
        NAME 'funetEduPersonIdentityCode'
        DESC 'Finnish Identity Code, earlier social security number'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )


# funetEduPersonDateOfBirth
# specifies a person's date of birth
# alphanumeric
# single-valued
attributetype (1.3.6.1.4.1.16161.1.1.2
        NAME 'funetEduPersonDateOfBirth'
        DESC 'date of birth'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )


# funetEduPersonTargetDegreeUniversity
# specifies the person´s target degree in a University
# numeric
# multi-valued
# values: Central Statistical Office of Finland:
# http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/yliopistot_tutkinnot.xls
attributetype ( 1.3.6.1.4.1.16161.1.1.3
        NAME 'funetEduPersonTargetDegreeUniversity'
        DESC 'university target degree'
        EQUALITY numericStringMatch
        SUBSTR numericStringSubstringsMatch
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.36' )


# funetEduPersonTargetDegreePolytech
# specifies the person´s target degree in a Polytechnic
# numeric
# multi-valued
# values: Central Statistical Office of Finland:
# http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/amk_tutkintokoodit.xls
```

```
attributetype (1.3.6.1.4.1.16161.1.1.4
        NAME 'funetEduPersonTargetDegreePolytech'
        DESC 'polytechnical target degree'
        EQUALITY numericStringMatch
        SUBSTR numericStringSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )

# funetEduPersonEducationalProgramUniv
# specifies a student´s educational program (using Stat classification, koulutusohjelma)
# numeric
# multi-valued
# values: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/yliopistot_kokoodit.xls
attributetype (1.3.6.1.4.1.16161.1.1.5
        NAME 'funetEduPersonEducationalProgramUniv'
        DESC 'educational program'
        EQUALITY numericStringMatch
        SUBSTR numericStringSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )


# funetEduPersonEducationalProgramPolytech
# specifies a student´s educational program (using Stat classification, koulutusohjelma)
# numeric
# multi-valued
# values: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/amk_kokoodit.xls
attributetype (1.3.6.1.4.1.16161.1.1.6
        NAME 'funetEduPersonEducationalProgramPolytech'
        DESC 'educational program'
        EQUALITY numericStringMatch
        SUBSTR numericStringSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )


# funetEduPersonOrientationAlternPolytech
# specifies the orientation alternative of a student (using Stat classification, suunt.vaihtoehto)
# numeric
# multi-valued
# values: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/amk_svkoodit.xls
attributetype (1.3.6.1.4.1.16161.1.1.7
        NAME 'funetEduPersonOrientationAlternPolytech'
        DESC 'orientation alternative'
        EQUALITY numericStringMatch
        SUBSTR numericStringSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )


# funetEduPersonMajorUniv
# specifies the main academic subjects of a student (using Stat classification, pääaine), only for a
# university student
# numeric
# multi-valued
# values: http://www.tilastokeskus.fi/tk/he/tiedonkeruu_oppilaitokset/yliopistot_pakoodit.xls
```

```
attributetype (1.3.6.1.4.1.16161.1.1.8
        NAME 'funetEduPersonMajorUniv'
        DESC 'main subject(s)'
        EQUALITY numericStringMatch
        SUBSTR numericStringSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.36 )

# funetEduPersonHomeOrganization
# specifies a person´s home university = domain name of the Organization
# alphanumeric
# single-valued
# values: domain name of a home organization (e.g. tut.fi)
attributetype (1.3.6.1.4.1.16161.1.1.9
        NAME 'funetEduPersonHomeOrganization'
        DESC 'domain name of the person´s home organization'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )

# funetEduPersonStudentID OID 1.3.6.1.4.1.16161.1.1.10
# specifies a person´s student number or code
# alphanumeric
# multi-valued
# values:
attributetype (1.3.6.1.4.1.16161.1.1.10
        NAME 'funetEduPersonStudentID'
        DESC 'student number or code'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

#-------------------------------------------------------
# funetEduPerson Object Class:
#
objectclass ( 1.3.6.1.4.1.16161.1.1
        NAME 'funetEduPerson'
        DESC 'members of Funet community'
        AUXILIARY
        MUST funetEduPersonHomeOrganization
        MAY ( funetEduPersonIdentityCode $
                funetEduPersonDateOfBirth $
                funetEduPersonTargetDegreePolytech $
                funetEduPersonTargetDegreeUniversity $
                funetEduPersonEducationalProgramUniv $
                funetEduPersonEducationalProgramPolytech $
                funetEduPersonOrientationAlternPolytech $
                funetEduPersonMajorUniv $
                funetEduPersonStudentID )
        )
# end
```