

norEdu* Object Class Specification

September 2015

Version 1.6

UNINETT

Document History

Version	Date	Initials	Comments
1.6	September 2015	JPC, HV	Added the norEduPersonServiceAuthnLevel and norEduPersonAuthnMethod attributes.

UNINETT AS
Abels gate 5 – Teknobyen
NO-7465 Trondheim
Telephone: +47 73 55 79 00
Fax: +47 73 55 79 01
E-mail: info@uninett.no
Web: www.uninett.no

Table of Contents

1	Status of this document	1
2	Introduction	2
2.1	Relationship to other LDAP schemas.....	2
2.2	Privacy concerns and security measures.....	3
2.3	Variations in use of norEdu*	3
3	Attribute specifications (normative)	3
3.1	Attribute survey.....	3
3.2	Attribute list.....	6
3.3	norEduPerson, norEduOrg and norEduOrgUnit attributes	7
3.4	Attributes from schac.....	13
3.5	Attributes from eduPerson	13
3.6	Attributes from eduOrg	24
3.7	Common attributes.....	26
4	Document information	42
4.1	Acknowledgments	42
4.2	References.....	43
4.3	Change log.....	44
Appendix A: Object classes (normative)		
Appendix B: Attribute definitions (normative)		
Appendix C: Obsolete attributes		

I Status of this document

This document is the updated version of the norEdu* object class specification. This version of the specification is coordinated on the Nordic level, and represents the common understanding of the Nordic academic community.

The specification is appropriate for use in enterprise directory service environments in the education sector. Please monitor www.feide.no if you are using this document.

The norEdu* specification consists of Chapters 2, 3 and Appendix A, B of this document. Chapter I (this chapter), Chapter 4 and Appendix C are informative only, and are not parts of the norEdu* specification.

New versions of the norEdu* specification will be announced on www.feide.no.

2 Introduction

2.1 Relationship to other LDAP schemas

RFC 4519 “Lightweight Directory Access Protocol (LDAP): Schema for User Applications” adopts a selection of X.520 attributes for use in LDAP. The schema defines several object classes, most of them structural, with an extensive set of general attributes. Furthermore, RFC 4524, RFC 2798 and RFC 2079 define attributes that are not particularly aimed at a specific application area. These attributes are customarily referred to as “common attributes”.

eduPerson [eduPerson201203] is defined by the Object Class Specifications byUCAID's Internet2 Middleware Architecture Committee Directory Working Group (MACE-Dir). It is designed for campus directories to facilitate communication among higher education institutions. eduPerson consists of a set of data elements or attributes about individuals within higher education, along with recommendations on the syntax and semantics of the data that may be assigned to those attributes.

eduOrg [eduOrg200210] describes attributes applicable to higher education organizations.

schac [schac] is developed and maintained by a working group in REFEDS (<http://www.refeds.org>), supported by the Trans-European Research and Education Networking Association (<http://www.terena.org/>), to supplement eduPerson/eduOrg in areas where eduPerson/eduOrg definitions are considered insufficient. It is assumed that the eduPerson/eduOrg classes are used together with schac.

The norEdu* classes add further attributes supplementing eduPerson/eduOrg in order to satisfy the requirements of the environment of the Nordic educational community, such as support for National Identity Numbers (norEduPersonNIN) and for the educational numbering and identifier schemes.

The eduPerson, eduOrg, schac and norEdu object classes are all defined as auxiliary, because they will be used in conjunction with existing structural object classes, such as the “person” class of RFC 4519 (eduPerson, eduOrg and schac make references to the equivalent X.521 definitions). schac also references the RFC 2798 “inetOrgPerson” class.

It is assumed that norEdu* is used together with eduPerson/eduOrg, and consequently with the structural classes of RFC 4519.

This specification cites eduPerson/eduOrg attribute descriptions, a selection of schac attribute descriptions and relevant common attributes from RFC 4519. Although the attribute definitions are not formally part of norEdu*, norEdu* usage rules apply directly to these attributes. So as a matter of convenience, attribute descriptions are included here together with the usage rules. To some degree, the eduPerson/eduOrg attributes have a wider scope than requested by the norEdu* community. When used with norEdu*, this document makes certain restrictions/requirements specified in “usage rules”.

To cover national or regional needs, other educational communities have developed LDAP schemes similar to norEdu* and schac; examples are [auEduPerson] and [funetEduPerson]. Various supplements to eduPerson/eduOrg may be overlapping and possibly conflicting in rules of usage, syntax and semantics. It is a long-term goal to unify the various schemas used by educational institutions worldwide. The norEdu* references to schac attributes, and the Nordic cooperation for maintaining norEdu* is part of this effort.

2.2 Privacy concerns and security measures

Information in `norEduPerson`, and to a certain degree `norEduOrg/norEduOrgUnit`, is or can be related to individuals. This means that the attribute, depending on context may be regarded as personal information. Given that something is regarded as personal information, its storage and use is regulated by national and international privacy legislation.

As a part of the documentation of every attribute, there is an assessment of that attribute's need for confidentiality, integrity and availability; see the table on page 4. Some attributes contain individual comments in the usage notes.

In addition to the assessments and comments for the individual attributes one should be aware that the need for e.g. confidentiality would rise when one puts several attributes together. Revealing a person's home address is more sensitive when one at the same time reveals that persons sex, age, name and telephone number. Since there is an enormous amount of possible combinations of different attributes, it is not feasible to analyse each possible combination.

The attributes `norEduPersonNIN`, `norEduPersonAuthnMethod` and all passwords should be protected by access controls to ensure that only authorized users or applications may access this information in the LDAP directory.

2.3 Variations in use of `norEdu*`

Although `norEdu*` represents a common Nordic effort, legal regulations, established conventions and external conditions may vary between national environments. Requirements may also vary among institutions of different educational levels. Attributes considered mandatory in one environment may be irrelevant in another. E.g. university students have individual email addresses, elementary school children don't necessarily have one.

Therefore, in the `norEdu*` schema, no attributes are mandated by the schema definition. However, a given federation, such as Feide, may declare attributes as mandatory within this federation. Feide's requirements regarding each attribute are described in the document as "Feide usage". Mandatory and recommended attributes in Feide are described in the attribute documents [UH-attributter] and [GO-attributter], intended for the primary and secondary education and higher education respectively. For users to be authenticated by Feide, and for the organizations these users belong to, the attributes mandated by Feide will always be present.

If users are cross-federated, i.e. authentication is done based on information in another, trusted federation, attributes may be missing. Handling of this situation is left to the service making use of the authentication service: If missing attributes are considered essential e.g. for billing or authorization purposes, the service may reject the user, even when authentication succeeds. If missing attributes are considered non-essential by the service, the user may be accepted, possibly with functional restrictions (such as email related operations being unavailable to users without an email address).

3 Attribute specifications (normative)

3.1 Attribute survey

The table in this chapter summarizes all `norEdu*` attributes as well as the attributes of other classes that are assumed to be available. The table also provides information regarding attribute usage, such as requirements for confidentiality, data integrity and availability.

The attributes are described by the following attributes:

Application utility class:

- Core: Attribute belongs to minimally useful attribute set.
- Standard: Basic applications like white pages and some authorization data.
- Extended: Of use to some set of more specialized applications.

Confidentiality:

- None: No restrictions or requirements.
- Low: Data well known from other sources.
- Medium: Personal information.
- High: Special rules apply.

Data integrity:

- Low: Values cannot be guaranteed to be up to date.
- Medium: Values should be up to date.
- High: Values are required to be up to date, maximum 24 hours latency.

Availability:

- Low: The attribute may or may not be available for relevant objects.
- Medium: If the LDAP uses this attribute, it should normally be provided for relevant objects. Authorization may fail if no value is available.
- High: If the LDAP uses this attribute, it should as far as possible be provided for all relevant objects. Authorization will fail if no value is available.

Attribute name	Application utility class	Confidentiality	Data integrity	Availability	Description, page	Grammar, page
norEduOrgAcronym	Standard	Low	Medium	Medium	7	50
norEduOrgNIN	Standard	None	Medium	Medium	7	51
norEduOrgSchemaVersion	Standard	None	Medium	Medium	7	50
norEduOrgUniqueIdentifier	Standard	None	Medium	Medium	8	50
norEduOrgUnitUniqueIdentifier	Standard	None	Medium	Medium	8	51
norEduPersonBirthDate	Standard	Low	Low	Medium	9	50
norEduPersonLegalName	Standard	Low	Medium	Medium	10	49
norEduPersonLIN	Standard	Medium	High	Medium	10	50
norEduPersonNIN	Core	Medium	High	High	11	49
norEduPersonServiceAuthnLevel	Extended	High/Medium	High	Medium	12	51

Attribute name	Application utility class	Confidentiality	Data integrity	Availability	Description, page	Grammar, page
norEduPersonAuthnMethod	Extended	High/Medium	High	Medium	12	51
schacHomeOrganization	Standard	Low	Medium	Medium	13	52
eduOrgIdentityAuthNPolicyURI	Standard	Low	High	High	25	54
eduOrgHomePageURI	Standard	Low	Low	Low	24	54
eduOrgLegalName	Standard	Low	High	Medium	25	54
eduOrgWhitePagesURI	Standard	Low	Medium	Low	26	54
eduPersonAffiliation	Standard	Low	Medium	Medium	14	52
eduPersonAssurance	Extended	Low	Medium	Medium	23	53
eduPersonEntitlement	Extended	Low	Medium	Medium	16	52
eduPersonNickname	Standard	Low	Medium	Medium	16	52
eduPersonOrgDN	Core	Low	Medium	Medium	17	52
eduPersonOrgUnitDN	Standard	Low	Medium	Medium	17	53
eduPersonPrimaryAffiliation	Standard	Low	Medium	Medium	18	53
eduPersonPrimaryOrgUnitDN	Extended	Low	Medium	Medium	19	53
eduPersonPrincipalName	Standard	Low	High	High	19	53
eduPersonScopedAffiliation	Standard	Low	Medium	Medium	20	53
eduPersonTargetedID	Extended	Low	Medium	Medium	21	53
cn	Core	Low	Medium	Medium	26	
dc	Standard	None	Low	Low	27	
displayName	Standard	Low	Medium	Medium	28	
facsimileTelephoneNumber	Extended	Low	Medium	Medium	28	
givenName	Standard	Low	Medium	Medium	29	
homePhone	Extended	Medium	Low	Medium	29	
homePostalAddress	Extended	High	Low	Medium	30	
jpegPhoto	Extended	High	Low	Medium	30	
l (localityName)	Extended	Low	Low	Medium	31	
labeledURI	Extended	Low	Medium	Low	31	
mail	Standard	Medium	High	Medium	32	

Attribute name	Application utility class	Confidentiality	Data integrity	Availability	Description, page	Grammar, page
manager	No recommendation	Low	Medium	Low	33	
mobile	Extended	Low	Medium	Medium	33	
o	Standard	Low	High	High	34	
ou	Standard	Low	High	High	34	
postalAddress	Extended	Low	Medium	Medium	35	
postalCode	Extended	Low	Medium	Medium	35	
postOfficeBox	Extended	Low	Medium	Medium	36	
preferredLanguage	Extended	Medium	Medium	Medium	36	
sn	Core	Medium	High	High	37	
street	Extended	Low	Medium	Low	38	
telephoneNumber	Standard	Medium	Medium	Medium	38	
title	Extended	Low	Medium	Medium	39	
uid	Standard	Low	High	High	39	
userCertificate	Extended	Low	High	High	40	
userPassword	Extended	High	High	High	41	
userSMIMECertificate	Extended	Medium	High	High	42	

3.2 Attribute list

This section gives a detailed description of all norEdu* attributes as well as the attributes of other classes that are assumed to be available.

Attributes from the several non-educational object classes are listed. The purpose of listing them is primarily as a convenience to enterprise directory designers, but in some cases notes are added to clarify aspects of meaning or usage in the education community beyond what can be found in the original standards documents.

The following format for attribute description is used:

Name	<attribute name>
Description	<short description of what the attribute describes>
Format	<given in text, transcribing the RFC 4517 OID name for the attribute syntax rules>
# of values	<'single' or 'multi'>

References	<reference to standard, RFC or similar>
OID	<unique identification of the attribute>
Examples	<one or more examples of attribute definition (LDIF fragment)>

3.3 *norEduPerson, norEduOrg and norEduOrgUnit attributes*

3.3.1 *norEduOrgAcronym*

Name	norEduOrgAcronym
Description	Acronym for the educational institution or similar object.
Format	DirectoryString
# of values	Multi
OID	1.3.6.1.4.1.2428.90.1.6
Examples	norEduOrgAcronym: USIT

Usage notes

To be used with the norEduOrg and norEduOrgUnit object classes.

The system that is the source of the institutions' organizational structure should also be the source of authoritative acronyms for the institution and its parts.

3.3.2 *norEduOrgNIN*

Name	norEduOrgNIN
Description	The organization number assigned by the public authorities, prefixed with a country code
Format	DirectoryString
# of values	Single
OID	1.3.6.1.4.1.2428.90.1.12
Examples	norEduOrgNIN: NO987747323

Usage notes

Not relevant for persons.

In Norway, organization identifiers are assigned by the Norwegian Register of Business Enterprises (Brønnøysundregistrene, Foretaksregisteret). The identifier consists of an “NO” country code prefix, followed by 9 digits; the last one is a check digit.

In Sweden, the VAT number is used, consisting of an “SE” country code prefix, followed by 12 digits; the last two are check digits. No hyphens are used.

3.3.3 *norEduOrgSchemaVersion*

Name	norEduOrgSchemaVersion
------	------------------------

Description	LDAP schema information for the federation. Version number of the norEdu* specification in use.
Format	DirectoryString
# of values	Single
OID	1.3.6.1.4.1.2428.90.1.11
Examples	norEduOrgSchemaVersion: 1.6

Usage notes

Not relevant for persons, to be used at the organization directory server.

This attribute obsoletes the federationFeideSchemaVersion introduced in norEdu* 1.3.

Example applications for which this attribute would be useful:

Any application that needs to control which version of attribute definition is in use at the identity provider's directory server.

3.3.4 norEduOrgUniquelIdentifier

Name	norEduOrgUniquelIdentifier
Description	The number assigned the higher educational institution by Universities and Colleges Admission Service ("Samordna opptak", SO).
Format	DirectoryString
# of values	Single
OID	1.3.6.1.4.1.2428.90.1.7
Examples	norEduOrgUniquelIdentifier: 00000185

Usage notes

Not relevant for persons. Format is 3 digits country code (000 for Norway) and 5 digits institution number. Most Norwegian universities and colleges have 5 leading zeros in this number.

See also norEduOrgNIN.

Feide usage note

Note that this is not the organization number assigned by the public authorities such as those assigned by the Norwegian Register of Business Enterprises (Brønnøysundregistrene).

3.3.5 norEduOrgUnitUniquelIdentifier

Name	norEduOrgUnitUniquelIdentifier
Description	The identifier describing an organizational unit.
Format	DirectoryString
# of values	Single
OID	1.3.6.1.4.1.2428.90.1.8

Examples	norEduOrgUnitUniquelIdentifier: 332244
----------	--

Usage notes

Not relevant for persons.

For institutions in higher education, this is locally assigned. Local uniqueness should be assured.

Feide usage notes

For primary and secondary education, the organization number, or an underlying company number, assigned by the Norwegian Register of Business Enterprises (Brønnøysundregistrene) is used.

The institutions in higher education establish their own organizational structure and describe it using location codes (“stedkoder”). This is done as an integral part of FS, but the institutions may make corresponding definitions relating to employee registries or accounting systems. One way to use this is to contain a six-digit number of the form **XXYYZZ** where **XX** is organizational unit (“enhet”), **YY** is section (“seksjon”) and **ZZ** is group (“gruppe”).

Example applications for which this attribute would be useful:

Door locks, physical access control, web portals.

3.3.6 norEduPersonBirthDate

Name	norEduPersonBirthDate
Description	The date of birth for the subject it is associated with
Format	NumericString
# of values	Single
OID	1.3.6.1.4.1.2428.90.1.3
Examples	norEduPersonBirthDate: 19660412

Usage notes:

The string has the format **YYYYMMDD**, using 4 digits for year, 2 digits for month and 2 digits for day as described in RFC 3339 but without the dashes.

A person's birth date is not sensitive data. There are few possibilities for misuse of this data without combining with several other data, and even then the damage that can be done with a person's birth date it is very limited.

Feide usage notes:

The attribute is obtained from the institution's employee, school or student registries.

The first 6 digits of **norEduPersonNIN** and the birth date for a person may be different. This is more likely to occur with short-lived NINs.

Example applications for which this attribute would be useful:

Portals with age-relevant classes of content.

3.3.7 norEduPersonLegalName

Name	norEduPersonLegalName
Description	The legal name for the subject it is associated with
Format	DirectoryString
# of values	Single
OID	1.3.6.1.4.1.2428.90.1.10
Examples	norEduPersonLegalName: Walter Martin Tvetter norEduPersonLegalName: Jack Peter Dougherty

Usage notes

The person's full formal name as registered by public authorities.

Feide usage notes

The person's name as registered in “Det Sentrale Folkeregister” is used as norEduPersonLegalName.

The attribute is obtained from the institution's employee, school or student registries and possibly registries for non-employee affiliated persons.

Example applications for which this attribute would be useful:

For applications with high formal requirements the full formal name might be required.

3.3.8 norEduPersonLIN

Name	norEduPersonLIN
Description	Local identity number, for instance student number or employee number.
Format	DirectoryString
# of values	Multiple
OID	1.3.6.1.4.1.2428.90.1.4
Examples	norEduPersonLIN: uninett.no:employee:035016

Usage notes

This identifier may also be used for scoped identity numbers, provided that the issuer prepends the identifier with a realm for the issuing authority. Another use is similar to the attribute eduPersonTargetedID. A given value is intended only for consumption by a specific requester.

When guaranteed global uniqueness is required, eduPersonPrincipalName should be preferred over norEduPersonLIN. norEduPersonLIN is not guaranteed to be unique across several enterprise directory servers (the same locally assigned norEduPersonLIN may be issued to several persons), unless these are coordinated e.g. through use of a unique prefix.

Feide usage notes

The format consists of a prefix to ensure global uniqueness, and a string in a locally defined format.

In Feide, the realm part of the eduPersonPrincipalName (i.e. the string to the right of the '@') should be used as a prefix.

The attribute is obtained from the institution's employee, school or student registries. It is mostly added for backwards compatibility with legacy systems.

Example applications for which this attribute would be useful:

Library systems, legacy payroll systems, targets with need to maintain a persistent but opaque identifier for a given user for purposes of personalization or record-keeping.

3.3.9 norEduPersonNIN

Name	norEduPersonNIN
Description	National Identity Number, a unique, officially assigned, personal identity number.
Format	DirectoryString
# of values	Single
OID	1.3.6.1.4.1.2428.90.1.5
Examples	norEduPersonNIN: 16090211111

Usage notes

In some countries, among them Norway, the national identity number is purely numeric. Other countries may include non-numeric characters in the identifier assigned by the official authorities, so string support is needed.

Feide usage notes

The Norwegian “fødselsnummer” is used as NIN. This is assigned by “folkeregisteret” in the local municipality and registered in the central “DSF” (“Det Sentrale Folkeregister”) for all individuals living more than 3 months in Norway. The format is ddmmyynncc: The first six digits are the date, month and year of birth, the following three act as unique identifier-part including a gender indicator, and the two last digits form a checksum. However, short lived NINs (fake or real) are assigned internally in some systems, and these may indicate both wrong birth date and wrong gender. The institutions assigning NINs are responsible for ensuring uniqueness of NINs within the entire scope where these NINs are visible.

The Norwegian Data Inspectorate (“Datatilsynet”) considers the “fødselsnummer “ non-sensitive information. This is not in agreement with the views of the general public, to which we make some concessions. Accordingly, the attribute is not to be made available to parties other than those approved by the holder. Applications that need the attribute must log on to the LDAP server acting as the user. This should not be done without the user being informed.

The attribute is obtained from the institution's employee, school or student registries and possibly registries for non-employee affiliated persons.

Example applications for which this attribute would be useful:

All applications in which identification of the person is paramount: BIBSYS, Frida, StudWeb.

3.3.10 norEduPersonServiceAuthnLevel

Name	norEduPersonServiceAuthnLevel
Description	Authentication level enforcement policies related to services the subject has access to.
Format	DirectoryString
# of values	Multiple
OID	1.3.6.1.4.1.2428.90.1.13
Examples	norEduPersonServiceAuthnLevel: urn:mace:feide.no:spid:12345 urn:mace:feide.no:auth:level:fad08:3 norEduPersonServiceAuthnLevel: urn:mace:feide.no:spid:all urn:mace:feide.no:auth:level:fad08:3

Usage notes

To be used by authentication systems implementing more than one authentication level. This attribute defines the enforcement policies regarding authentication levels that should be applied to the subject. This attribute should be appropriately protected to avoid subjects being able to edit it themselves.

No controlled vocabulary, may contain anything. Formatting and contents of this attribute are therefore left to each particular implementation making use of them.

See also norEduPersonAuthnMethod.

Feide usage notes

The attribute can contain either an uri identifying the service for which a specific authentication level must be performed combined with an uri identifying the authentication level required, or the fixed string 'urn:mace:feide.no:spid:all' combined with an uri identifying the authentication level required, indicating that the specific authentication level must be enforced regardless of the service asking for authentication. See also [UH-attributter], [GO-attributter].

3.3.11 norEduPersonAuthnMethod

Name	norEduPersonAuthnMethod
Description	Authentication methods that can be used by the subject to enable multi-factor authentication.
Format	DirectoryString
# of values	Multiple
OID	1.3.6.1.4.1.2428.90.1.14
Examples	norEduPersonAuthnMethod: urn:mace:wayf.dk:two-factor:method:yubikey 0123456789 norEduPersonAuthnMethod: urn:mace:feide.no:auth:method:sms +4712345678 label=Work%20phone

Usage notes

To be used by authentication systems implementing multiple authentication levels. This attribute defines the list of authentication methods available for the subject that can be used to perform multi-factor authentication, plus the information required for that purpose. Its value should be appropriately protected to avoid subjects being able to edit it themselves.

This attribute contains three parts separated by a single space. The first part must contain a method identifier, which takes the form of a URN. Valid identifiers should be univocally linked to a particular implementation of the multi-factor method they refer to. The second part of the attribute contains a string of data whose semantics are specific to the indicated method, with all spaces as well as percent and equal signs being percent encoded according to [RFC3986]. Finally, an optional third part might be available, including parameters separated by single spaces, where the name and the value of each parameter are separated by an equal sign and any spaces, percent or equal signs are also percent encoded.

See also `norEduPersonServiceAuthnLevel`.

Feide usage notes

The attribute contains as many values as different authentication methods that can be used to authenticate the subject. Its values consist of the prefix 'urn:mace:feide.no:auth:method:' concatenated with an identifier of the method, a method-specific value whose semantics depend on the method itself, and optional parameters also depending on the method. See also [UH-attributter], [GO-attributter].

3.4 Attributes from *schac*

3.4.1 `schacHomeOrganization`

Name	<code>schacHomeOrganization</code>
Description	Specifies a person's home organization using the domain name of the organization.
Format	Domain name according to RFC 1035
# of values	Single
References	RFC 1035 - Domain names - implementation and specification
OID	1.3.6.1.4.1.25178.1.2.9
Examples	<code>schacHomeOrganization: uio.no</code>

Usage notes:

This attribute applies to the person entry. Other organization attributes are found in the organization entry.

3.5 Attributes from *eduPerson*

Description and Usage notes for `eduPerson` attributes are, for the most part, direct citation of text in [eduPerson201203, eduPerson200210, eduPerson200312, eduPerson200604, eduPerson200712 and eduPerson200806]. There may be some stylistic differences between the `eduPerson` and `norEdu*` descriptions.

Note that some usage restrictions may apply when eduPerson/eduOrg is used with norEdu*, in particular when used in the Feide federation. Such restrictions are noted following the general Usage notes below.

3.5.1 eduPersonAffiliation

Name	eduPersonAffiliation
Description	Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).
Format	DirectoryString
Permissible values	faculty, student, staff, alum, member, affiliate, employee, library walk-in
# of values	Multi
OID	1.3.6.1.4.1.5923.1.1.1.1
Examples	eduPersonAffiliation: faculty

Usage notes

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

The primary intended purpose of eduPersonAffiliation is to convey broad-category affiliation assertions between members of an identity federation. Given this inter-institutional context, only values of eduPersonAffiliation with broad consensus in definition and practice will have any practical value. The list of allowed values in the current version of the object class is certainly incomplete, especially in terms of local institutional use. The editors felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included in later versions of eduPerson.

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

The "member" affiliation **MUST** be asserted for people carrying one or more of the following affiliations:

- faculty or
- staff or
- student or
- employee

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

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

The "affiliate" value for eduPersonAffiliation indicates that the holder has some definable affiliation

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

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

"Library-walk-in:" This term was created to cover the case where physical presence in a library facility grants someone access to electronic resources typically licensed for faculty, staff and students. In recent years the library walk-in provision has been extended to cover other cases such as library users on the campus network, or those using on-campus workstations. Licensed resource providers have often been willing to interpret their contracts with licensees to accept this broader definition of "library-walk-in," though specific terms may vary. For a more direct way of using eduPerson attributes to express library privilege information, see the eduPersonEntitlement value "urn:mace:dir:entitlement:common-lib-terms" as defined in the MACE-Dir Registry of eduPersonEntitlement values <http://middleware.internet2.edu/urn-mace/urn-mace-dir-entitlement.html>.

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

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

Semantics

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

A reasonable person should find the listed relationships plausible.

Feide usage notes

The following values are used for affiliation:

- Student – The person is an active pupil or student. He or she is entitled to a school place or to participate in a study program in which he or she attends courses. All students have the additional value of member.
- Faculty – The person is employed with a job code that belongs to the main category 'Faculty' ("Vitenskapelig") (according to Norwegian legislation ("Universitetslovens elector gruppe vitenskapelig tilsatte")). For primary and secondary education, this value should be used for all educational employees. All faculty has the additional values of employee and member.
- Staff – The person is employed with a job code, which does not belong to the main category 'Faculty'. All staff has the additional values of employee and member.
- Employee – The union of 'Faculty', 'Staff' and other persons on the institution's payroll.
- Alum – Persons that are included in the organization's alumni arrangements.

Affiliation is extracted from information contained in the institution's employee, school or student registries and access control system (where available).

Example applications for which this attribute would be useful:

White pages, controlling access to resources.

3.5.2 eduPersonEntitlement

Name	eduPersonEntitlement
Description	URI (either URN or URL) that indicates a set of rights to specific resources.
Format	DirectoryString
# of values	Multi
OID	1.3.6.1.4.1.5923.1.1.1.7
Examples	eduPersonEntitlement: http://xstor.com/contracts/HEd123 eduPersonEntitlement: urn:mace:feide.no:go:grep: http://psi.udir.no/laereplan/aarstrinn/aarstrinn6

Usage notes

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

URN values 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.

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/>.

Feide usage notes

Trust between parties is established by contractual relationships.

The name space urn:mace:feide.no has been delegated to Feide, see <http://www.feide.no/urn/>.

Example applications for which this attribute would be useful:

Controlling access to resources.

3.5.3 eduPersonNickname

Name	eduPersonNickname
Description	Person's nickname, or the informal name by which they are accustomed to be hailed
Format	DirectoryString

# of values	Multi
OID	1.3.6.1.4.1.5923.1.1.1.2
Examples	eduPersonNickname: Spike

Usage notes

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

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

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

Example applications for which this attribute would be useful:

White pages.

3.5.4 eduPersonOrgDN

Name	eduPersonOrgDN
Description	The distinguished name (DN) of the directory entry representing the institution with which the person is associated.
Format	DistinguishedName
# of values	Single
OID	1.3.6.1.4.1.5923.1.1.1.3
Examples	eduPersonOrgDN: o=Hogwarts, dc=hsww, dc=wiz

Usage notes

With a distinguished name, the client can do an efficient lookup in the institution's directory to find out more about the organization with which the person is associated.

`cn` (common name), `sn` (surname, family name) and this attribute, `eduPersonOrgDN`, are the three attributes satisfying the "core" application utility class of `eduPerson`.

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

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.5.5 eduPersonOrgUnitDN

Name	eduPersonOrgUnitDN
------	--------------------

Description	The distinguished name(s) (DN) of the directory entries representing the person's Organizational Unit(s).
Format	DistinguishedName
# of values	Multi
OID	1.3.6.1.4.1.5923.1.1.1.4
Examples	eduPersonOrgUnitDN: ou=Potions, o=Hogwarts, dc=hsww, dc=wiz

Usage notes

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.

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).

The directory entry pointed to by this dn should be represented in the X.521(2001) "organizational unit" object class. In addition to organizationalUnitName, this object class has the same optional attribute set as the organization object class.

Feide usage notes

Source is the institution's employee and student management systems. The attribute may contain a listing of DNs to the locations to which a person has some relation independent of "affiliation".

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.5.6 eduPersonPrimaryAffiliation

Name	eduPersonPrimaryAffiliation
Description	Specifies the person's primary relationship to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).
Format	DirectoryString
Permissible values	faculty, student, staff, alum, member, affiliate, employee, library walk-in
# of values	Single
OID	1.3.6.1.4.1.5923.1.1.1.5
Examples	eduPersonPrimaryAffiliation: student

Usage notes

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

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

See [eduPersonAffiliation](#) for further details.

Feide usage notes

The source is the institution's employee and student management systems. It is not readily apparent that it will be possible to agree on an algorithm to determine which of a person's affiliations is the primary affiliation. This raises little or no dangers from a privacy viewpoint.

Example applications for which this attribute would be useful:

Controlling access to resources.

3.5.7 eduPersonPrimaryOrgUnitDN

Name	eduPersonPrimaryOrgUnitDN
Description	The distinguished name (DN) of the directory entry representing the person's primary Organizational Unit.
Format	DistinguishedName
# of values	Single
OID	1.3.6.1.4.1.5923.1.1.1.8
Examples	eduPersonPrimaryOrgUnitDN: ou=Music Department, o=Notre Dame, dc=nd, dc=edu

Usage notes

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.

The source is the institution's employee and student management systems. It is not readily apparent that it will be possible to agree on an algorithm to decide which OU is the primary one for a given person.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.5.8 eduPersonPrincipalName

Name	eduPersonPrincipalName
Description	A scoped identifier for a person. It should be represented in the form "user@scope" where 'user' is a name-based identifier for the person and where 'scope' defines a local security domain. Each value of 'scope' defines a namespace within which the assigned identifiers MUST be unique. Given this rule, if two eduPersonPrincipalName (ePPN) values are the same at a given point in time, they refer to the same person.
Format	DirectoryString
# of values	Single

OID	1.3.6.1.4.1.5923.1.1.1.6
Examples	eduPersonPrincipalName: hputter@hsw.wiz

Usage notes

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

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

Feide usage notes

An eduPersonPrincipalName should never be reassigned to another person; lifelong learning must be kept in mind. The organization assigning principal names must ensure uniqueness among active values. If the organization chooses to reassign a principal name, which is not in active use, it is responsible for doing this in a way that will not cause problems. E.g. it should be considered that when a principal name has been exposed externally, it might have been used as a database primary key by others.

A person may be assigned a new principal name.

It is worth noting that this id, being related to the national identity number (NIN), ought to have the same confidentiality as the NIN. This should be taken into consideration, however, eduPersonPrincipalName has to be accessible to applications that want to grant a person certain rights connected to the person.

The values to the right of the “@” sign should be a dotted string which is the Feide realm of the organization with which the user is affiliated.

The value to the left of the “@” sign should be identical to the “uid” value.

By definition eduPersonPrincipalName is not case sensitive. Because of differences in LDAP implementations, it is still recommended to use only lower case letters in this attribute.

Example applications for which this attribute would be useful:

Controlling access to resources and other cases where a human friendly identifier is needed.

3.5.9 eduPersonScopedAffiliation

Name	eduPersonScopedAffiliation
Description	Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc.
Format	DirectoryString
Permissible values	See controlled vocabulary for eduPersonAffiliation; only these values are allowed to the left of the @ sign.

# of values	Multi
OID	1.3.6.1.4.1.5923.1.1.1.9
Examples	eduPersonScopedAffiliation: member@uninett.no eduPersonScopedAffiliation: employee@I12233.ntnu.no

Usage notes

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. The right-hand side syntax of eduPersonScopedAffiliation intentionally matches that used for the right-hand side values for eduPersonPrincipalName since both identify a security domain.

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."

Feide usage notes

The values to the right of the "@" should either be the realm part of the user's eduPersonPrincipalName, or this value prefixed with the norEduOrgUnitUniquelIdentifier to which the affiliation applies, separated by a full stop. The second example above illustrates the use of a norEduOrgUnitUniquelIdentifier part for a Feide user at ntnu.no who is an employee in the unit with the (locally) unique identifier I12233.

Example applications for which this attribute would be useful:

White pages, controlling access to resources.

3.5.10 eduPersonTargetedID

Name	eduPersonTargetedID
Description	A persistent, non-reassigned, privacy-preserving identifier for a principal.
Format	DirectoryString
# of values	Multi
OID	1.3.6.1.4.1.5923.1.1.1.10
Examples	eduPersonTargetedID: 24d66f51ac1c0b140e617af335b9abb4b8d88a5b

Usage notes

eduPersonTargetedID is an abstracted version of the SAML V2.0 Name Identifier format of "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" (see <http://www.oasis-open.org/committees/download.php/35711>). In SAML, this is an XML construct consisting of a string value inside a <saml:NameID> element along with a number of XML attributes, of most significance NameQualifier and SPNameQualifier, which identify the source and intended audience of the value. It is left to specific profiles to define alternate syntaxes, if any, to the standard XML

representation used in SAML.

In abstract terms, an eduPersonTargetedID value is a tuple consisting of an opaque identifier for the principal, a name for the source of the identifier, and a name for the intended audience of the identifier. The source of the identifier is termed an identity provider and the name of the source takes the form of a SAML V2.0 entityID, which is an absolute URI. The name of the intended audience also takes the form of an absolute URI, and may refer to a single service provider or a collection of service providers (for which SAML V2.0 uses the term "Affiliation", not to be confused with the ordinary eduPerson use of the term).

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

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

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

More specific requirements and guidance follows.

Persistence

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

Privacy

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

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

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

Uniqueness

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

Reassignment

A distinguishing feature of this attribute inherited from SAML is that it prohibits re-assignment. Since the values are opaque, there is no meaning attached to any particular value beyond its identification of the principal. Therefore particular values created by an identity provider **MUST NOT** be re-assigned such that the same value given to a particular service provider refers to two different principals at different points in time. It is allowable (though perhaps confusing) for a given value to refer to two or more different principals when scoped to different audiences.

Human Palatability

This attribute does not meet requirements for human palatability or readability. It is ill-suited for display to end users or administrators, and is not useful for provisioning accounts ahead of initial access by users since the value will rarely be known by users or administrators. It may be accompanied by other attributes more suited to such purposes, in which case its privacy properties are presumably of no interest, but the lack of reassignment often is.

Feide usage notes

This attribute is defined for use with Shibboleth, but may be used in other contexts as well.

Note that the attribute is not stored in the LDAPs of host organizations, but in the login service.

Example applications for which this attribute would be useful

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

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

3.5.11 eduPersonAssurance

Name	eduPersonAssurance
Description	Set of URIs that asserts compliance with specific standards for identity assurance.
Format	DirectoryString
# of values	Multi
OID	1.3.6.1.4.1.5923.1.1.1.11
Examples	eduPersonAssurance: urn:mace:incommon:IAQ:sample eduPersonAssurance: http://idm.example.org/LOA#sample

Usage notes

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

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

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

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

Example applications for which this attribute would be useful

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

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

3.6 Attributes from eduOrg

The attributes in the following section are copied from eduOrg with minor compatibility changes.

Description and Usage notes for eduOrg attributes are, for the most part, direct citation of text in [eduOrg200210]. Rather than rewriting the text to incorporate norEdu*/Feide considerations, separate norEdu*/Feide usage notes have been added as separate paragraphs. There may be some stylistic differences between the eduPerson and norEdu* descriptions.

3.6.1 eduOrgHomePageURI

Name	eduOrgHomePageURI
Description	The URL for the organization's top level home page.
Format	DirectoryString
# of values	Multi
OID	1.3.6.1.4.1.5923.1.2.1.2
Examples	eduOrgHomePageURI: http://www.uio.edu

Usage notes

Most useful in a search by name of institutions in a directory of directories. Among other things, a way to remove the guesswork around the institution's second-level domain name: www.???.edu.

Note that this is the root of the information tree, not a pointer to a student union or similar.

It is recommended that this value be copied to labeledURI for the organization.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.6.2 eduOrgIdentityAuthNPolicyURI

Name	eduOrgIdentityAuthNPolicyURI
Description	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.
Format	DirectoryString
# of values	Multi
OID	1.3.6.1.4.1.5923.1.2.1.3
Examples	eduOrgIdentificationAuthNPolicyURI: http://www.uchicago.edu/security/IA-Policy.html

Usage notes

Primarily useful as a pointer to information relevant to judgment of risks in participating in inter-institutional resource sharing arrangements.

Used in connection with certificates. Obtained from the certification policy of the relevant CA (CP).

Example applications for which this attribute would be useful:

Digital signatures, smart cards.

3.6.3 eduOrgLegalName

Name	eduOrgLegalName
Description	The organization's legal corporate name.
Format	DirectoryString
# of values	Multi
OID	1.3.6.1.4.1.5923.1.2.1.4
Examples	eduOrgLegalName: Georgia Institute of Technology

Usage notes

Directory implementers should check with the institution's legal counsel to determine the proper value for this attribute.

This value should be copied to the “o” attribute, to facilitate searches.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.6.4 eduOrgWhitePagesURI

Name	eduOrgWhitePagesURI
Description	The URL of the open white pages directory service for the university, predominantly LDAP these days.
Format	DirectoryString
# of values	Multi
OID	1.3.6.1.4.1.5923.1.2.1.6
Examples	eduOrgWhitePagesURI: ldap://wpage1.uwrf.edu

Usage notes

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

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7 Common attributes

The attributes in the following section are from other standard object classes or attribute definitions; most of them originated in the X.520 recommendation, later adopted by RFC 4519, or from the RFC 4524schema. This specification does not include descriptions of all RFC 4519 or RFC 4524attributes, but in any case where the eduPerson working group or norEdu* editors considered that some comment was needed to clarify the meaning or utility of an attribute, it can be found here.

For details on the syntax and other aspects of these attributes, see the appropriate standards documents.

Note that for several attributes adopted from X.520, the attribute syntax is described using the same name as in X.520, but the formal RFC 4519 grammar specifies an OID defined by RFC 4517. In most cases, this will be of minor concern except possibly if schema definitions are ported between X.500 (DAP) and LDAP directories, if the software involved makes consistency checks based on OIDs.

3.7.1 cn

Name	cn
Description	Common name
Format	DirectoryString
# of values	Multi
References	X.520, RFC 4519
OID	2.5.4.3

Examples	cn: Universitetet i Oslo cn: Universitas Osloensis cn: University of Oslo cn: UiO cn: Walter Martin Tveter cn: Walter M. Tveter cn: Walter Tveter
----------	---

Usage notes

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

Organization:

All the names that identify the institution, including acronyms.

Person:

Full name as obtained from the employee or student management system. May contain variants of the person's name.

Required. One of the two required attributes in the person object class (the other is sn). As such it is one of three recommended "core application utility" attributes. The third is eduPersonOrgDN. With eduPersonOrgDN and cn, the client knows the person's name and the distinguished name of the organization with which he/she is associated. The latter could help them find a directory entry for the person's organization.

Feide usage notes

This attribute will not be a problem as long as the person does not have special needs for anonymity. In such cases all name related attributes must be protected or pseudonyms used.

Example applications for which this attribute would be useful:

All.

3.7.2 dc

Name	dc
Description	A string holding one component, a label, of a DNS domain name naming a host.
Format	IA5 String
# of values	Single
References	RFC 4519, RFC 1123, RFC 2181
OID	2.16.840.1.113730.3.1.241
Examples	dc: uninett

Usage notes

Valid values include "example" and "com" but not "example.com". The latter is invalid as it contains multiple domain components.

It is noted that the directory service will not ensure that values of this attribute conform to the host label restrictions. It is the client's responsibility to ensure that the labels it stores this attribute are appropriately restricted.

Directory applications supporting International Domain Names SHALL use the ToASCII method [RFC3490] to produce the domain component label. The special considerations discussed in Section 4 of RFC3490 should be taken, depending on whether the domain component is used for "stored" or "query" purposes.

Example applications for which this attribute would be useful:

Directory of directories, white pages, email client.

3.7.3 displayName

Name	displayName
Description	The name(s) that should appear in white-pages-like applications for this person; preferred name of a person to be used when displaying entries
Format	DirectoryString
# of values	Single
References	RFC 2798
OID	2.16.840.1.113730.3.1.241
Examples	displayName: Jack Dougherty displayName: Walter Tveter

Usage notes

Since other attribute types such as cn (commonName) are multi-valued, displayName is a better candidate for use in white pages and configurable email clients.

If the institution's employee and student management systems support this, the attribute may be used.

Example applications for which this attribute would be useful:

Directory of directories, white pages, email client.

3.7.4 facsimileTelephoneNumber

Name	facsimileTelephoneNumber
Description	A fax number for the directory entry. Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."
Format	FacsimileTelephoneNumber
# of values	Multi
References	RFC 4519
OID	2.5.4.23
Examples	facsimileTelephoneNumber: +47 73557901

Usage notes

According to 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.

Normally used for employees only, where the value is stored in the employee payroll system.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.5 givenName

Name	givenName
Description	Contains name strings that are the part of a person's name that is not their surname.
Format	DirectoryString
# of values	Multi
References	RFC 4519
OID	2.5.4.42
Examples	givenName: Walter Martin givenName: Walter

Usage notes

The given name of the person, obtained from the employee management system or the student registry. The attribute may have multiple values. If it does have multiple values they represent the alternative renderings of the given name.

Feide usage

All questions regarding the use of given names, middle names and surnames, are to be referred to the Norwegian naming legislation [navneloven].

3.7.6 homePhone

Name	homePhone
Description	A home telephone number associated with a person. Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."
Format	TelephoneNumber
# of values	Multi
References	RFC 2798, RFC 4524
OID	0.9.2342.19200300.100.1.20
Examples	homePhone: +47 23456789

Usage notes

The home phone number is not really different from the office phone number, in as much as it is not listed with a (home) address. If this is the case then it will reveal a personal (and unprotected) location where one can reach such individuals. Therefore such telephone numbers should probably be listed only with the billing address - that of the university.

Feide usage notes

The value is obtained from the institution's employee management system. It should be used only when the institution pays for the telephone subscription or the telephone is used for purposes related to the person's employment.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.7 homePostalAddress

Name	homePostalAddress
Description	A home postal address for an object.
Format	PostalAddress
# of values	Multi
References	RFC 4524
OID	0.9.2342.19200300.100.1.39
Examples	homePostalAddress: 1212 Como Ave. \$ Midton, SD 45621

Usage notes

eduPerson has a PostalAddress that complements this attribute.

homePostalAddress should only be used by institutions that know this is needed.

The PostalAddress syntax [RFC 4517] allows the value to be a list of strings, separated by dollar signs. Each element in the list is usually interpreted as one address line. A dollar sign or backslash, which is part of the proper address string, must be escaped using backslash as an escape character (“\\”, “\\$”).

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.8 jpegPhoto

Name	jpegPhoto
Description	An image of a person using the JPEG File Interchange Format [JFIF].
Format	jpegPhoto
# of values	Multi
References	RFC 2798

OID	0.9.2342.19200300.100.1.60
Examples	(Attribute value is in binary format)

Usage notes

A smallish photo in jpeg format.

Example applications for which this attribute would be useful:

Student cards, physical entrance cards, white pages.

3.7.9 l (localityName)

Name	l
Description	The name of a locality, such as a city, county or other geographic region (localityName).
Format	DirectoryString
# of values	Multi
References	X.520, RFC 4519
OID	2.5.4.7
Examples	l: Oslo

Usage notes

When used as a component of a directory name, the locality name 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.

If used, it should hold names of locations to which the person is affiliated. For institutions with more than one campus this is relevant.

Location names as used by the postal service. The source of this attribute should be the employee or student management systems, and maintaining consistency with the localization used in each organization is a goal.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.10 labeledURI

Name	labeledURI
Description	Uniform Resource Identifier with optional label
Format	CaseExactString
# of values	Multi
References	RFC 2079
OID	1.3.6.1.4.1.250.1.57

Examples	labeledURI: ftp://ds.internic.net/rfc/rfc822.txt labeledURI: http://www.umich.edu/%7Ersug/ldap/ LDAP Home Page labeledURI: http://champagne.inria.fr/Unites/rennes.gif Rennes [photo]
----------	---

Usage notes

Commonly a URL for a web site associated with this person or entity. The vocabulary for the label portion of the value is not standardized.

For persons this is typically a private home page, or at least a privately maintained home page, as opposed to an institution-maintained page or a page representing an institution. As such it will probably be voluntary to have one, and even if this is not so it will probably be up to each individual to decide its content. This does not represent any special problems in a privacy perspective as long as the individuals who have home pages are made aware that their URLs are listed.

Examples of labeledURI Attribute Values:

The first example is of a labeledURI attribute value that does not include a label

The second example is of a labeledURI attribute value that contains a tilde character in the URL (special characters in a URL must be encoded). The label is "LDAP Home Page"

The third example includes a hint in the label to help the user realize that the URL points to a photo image. The label is "Rennes [photo]".

Example applications for which this attribute would be useful:

Directory of directories, local search engines, white pages.

3.7.11 mail

Name	mail
Description	The 'mail' (rfc822mailbox) attribute type holds Internet mail addresses in Mailbox [RFC2821] form (e.g., user@example.com).
Format	IA5 String
# of values	Multi
References	RFC 4524
OID	0.9.2342.19200300.100.1.3
Examples	mail: sophus.lie@student.hia.no

Usage notes

Preferred address for the "to:" field of email to be sent to this person or entity. Usually of the form firstname.lastname@univ.domain. 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. [ldaprecipe].

Feide usage notes

Personal email address for a person. Obtained from the organization's email system or another

authoritative source.

There is a rising problem with spam/UCE and other unwanted incoming email communication. In the educational institutions (at least in Norway), one has not made any clear decisions as to who owns e-mail addresses and if the users whose name they point to can use them for personal use. If one chooses to view an e-mail address, as a resource that the institution owns, then the listing of it, and the risks that follow with this - unwanted incoming communications, is more of an efficiency problem for the institution than an infringement of the users personal sphere.

One could say this is more of a mixed situation in as much as any communication that is aimed at the individual as a private person and not as a representative of an institution is as much an infringement of this individual's personal sphere as if he or she owned this e-mail address themselves. This argument however, is not valid for an institutions ability to prescribe that its employees (or students) should have accessible e-mail addresses. It is valid towards the senders of the unwanted communications in questions about whether or not one can bring charge against them as individuals, consumers etc.

Example applications for which this attribute would be useful:

Directory of directories, white pages, email client.

3.7.12 manager

Name	manager
Description	The manager of an object represented by an entry
Format	DistinguishedName
# of values	Multi
References	RFC 4524
OID	0.9.2342.19200300.100.1.10
Examples	manager: uid=twilliams,ou=people,dc=hobart,dc=edu

Usage notes

This attribute carries the DN of the manager of the person represented in this entry.

For employees only. Taken from the employee management systems if used at all. Restricted to the person that is the immediate manager for the employee's job position.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.13 mobile

Name	mobile
Description	A mobile telephone number associated with a person. Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."
Format	TelephoneNumber
# of values	Multi

References	RFC 4524
OID	0.9.2342.19200300.100.1.41
Examples	mobile: +47 40404040

Example applications for which this attribute would be useful.

Directory of directories, white pages, SMS message with one-time password.

3.7.14 o

Name	o
Description	Standard name of the top-level organization (institution) with which this person is associated.
Format	DirectoryString
# of values	Multi
References	RFC 4519
OID	2.5.4.10
Examples	o: St. Cloud State

Usage notes

Meant to carry the TOP-LEVEL organization name. Do not use this attribute to carry names of organizational sub-units.

The o attribute may list all the names of the institution, including the one found in eduOrgLegalName. Each name is one value of this multi-valued attribute.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.15 ou

Name	ou
Description	The names of an organizational unit name.
Format	DirectoryString
# of values	Multi
References	RFC 4519
OID	2.5.4.11
Examples	ou: Faculty Senate

Usage notes

When used as a component of a directory name it identifies an organizational unit with which the named object is affiliated.

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.

Administratively determined. Located in the employee and student directories.

Example applications for which this attribute would be useful:

Directory of directories, white pages, learning management systems.

3.7.16 postalAddress

Name	postalAddress
Description	Campus or office address, specifying the address information required for the physical postal delivery to an object.
Format	PostalAddress
# of values	Multi
References	X.520, RFC 4519
OID	2.5.4.16
Examples	postalAddress: P.O. Box 333 \$ Whoville, WH 99999

Usage notes

The PostalAddress syntax [RFC 4517] allows the value to be a list of strings, separated by dollar signs. Each element in the list is usually interpreted as one address line. A dollar sign or backslash, which is part of the proper address string, must be escaped using backslash as an escape character (“\\”, “\\$”).

The postalAddress is, with exception for individuals with a qualified requirement for anonymity, not considered a problematic piece of personal information.

Feide usage notes

Not assigned for students. Contains both mailbox address and postal number, even if these are separate attributes. Taken from the employee management system.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.17 postalCode

Name	postalCode
Description	Codes used by a Postal Service to identify postal service zones.
Format	DirectoryString
# of values	Multi
References	X.520, RFC 4519

OID	2.5.4.17
Examples	NO-7465

Usage notes

ZIP code in USA, postal code for other countries. If not prefaced by country code, assume local. If this attribute value is present, it will be part of the object's postal address. Regarded as unproblematic in a privacy perspective.

Feide usage notes

Campus postal code is taken from the employee management system.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.18 postOfficeBox

Name	postOfficeBox
Description	The Postal Office Box by which the object will receive physical postal delivery.
Format	DirectoryString
# of values	Multi
References	X.520, RFC 4519
OID	2.5.4.18
Examples	postOfficeBox: 109260

Usage notes

Each postal box identifier is a single value of this multi-valued attribute. If present, the attribute value is part of the object's postal address. Regarded as unproblematic in a privacy perspective.

Feide usage notes

postOfficeBox attributes are campus address taken from the employee management system.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.19 preferredLanguage

Name	preferredLanguage
Description	Preferred written or spoken language for a person.
Format	ISO 639
# of values	Single

References	RFC 2798, BCP 47, ISO 639, ISO 3166
OID	2.16.840.1.113730.3.1.39
Examples	preferredLanguage: nn

Usage notes

In a privacy perspective, language preference may in certain contexts be sensitive information: Any value other than the national language or English may possibly indicate the registered individuals ethnic origin. A given language preference may lead to an assumption of the individual's specific ethnic origin, or may indicate a non-specific, but non-native origin. It should therefore be held as confidential as possible without removing its practical use.

Feide usage notes

The attribute originates in student registry system.

Attribute values are restricted to two or three letter codes according to BCP 47: nn (Norwegian, nynorsk), nb (Norwegian, bokmål), no (Norwegian), en (English), se (Northern Sami), sma (Southern Sami) or smj (Lule Sami), used in accordance with recommendation in [BCP 47] based on [ISO 639] and [ISO 3166] country codes. If languages that indicate ethnicity are used, requirements for confidentiality rise to high.

Example applications for which this attribute would be useful:

Presentation of web pages in correct language, directory of directories, white pages.

3.7.20 sn

Name	sn
Description	Surname or family name.
Format	DirectoryString
# of values	Multi
References	X.520, RFC 4519
OID	2.5.4.4
Examples	sn: Carson-Smith sn: Carson sn: Smith

Usage notes

In X.520, this attribute is called surname.

Required. One of the two required attributes in the person object class from which eduPerson derives (the other is cn). As such it is one of eduPerson's three "core application utility" attributes. The third is eduPersonOrgDN.

If the person has a multi-part surname (whether hyphenated or not), store both 1) the whole surname including hyphens if present and 2) each component of a hyphenated surname as a separate value in this multi-valued attribute. That yields the best results for the broadest range of clients doing name searches. Beware of applications sorting persons by sn-cn, they may need

access controls added to protect them from multivalued surnames.

Feide usage notes

Source is a student registry or human resource system.

All questions regarding the use of given names, middle names and surnames, are to be referred to the Norwegian naming legislation [navneloven].

Example applications for which this attribute would be useful:

All.

3.7.21 street

Name	street
Description	The physical address of the object to which the entry corresponds, such as an address for package delivery.
Format	DirectoryString
# of values	Multi
References	X.520, RFC 4519
OID	2.5.4.9
Examples	street: 303 Mulberry St.

Usage notes

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.

As long as the individual that the information relates to does not have any special need for anonymity, then this information is not problematic from a privacy point of view.

Feide usage notes

Sources are student registry or employee payroll system.

Example applications for which this attribute would be useful:

Directory of directories, white pages, door locks.

3.7.22 telephoneNumber

Name	telephoneNumber
Description	Office/campus phone number. Attribute values should comply with the ITU Recommendation E.123 [E.123]: i.e., "+44 71 123 4567."
Format	TelephoneNumber
# of values	Multi
References	X.520, RFC 4519

OID	2.5.4.20
Examples	telephoneNumber: +47 73593000

Usage notes

Telephone number confidentiality is not a problem in itself. If someone has a special need to be anonymous, then it will have to be possible to hide this. In addition one should be aware that if the phone number is listed with an address in a phone directory, then the number will have to be treated at least as carefully as the address that is listed.

Feide usage notes

Sources are employee payroll system or PABX or switchboard.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.23 title

Name	title
Description	The title of a person in their organizational context. Each title is one value of this multi-valued attribute.
Format	DirectoryString
# of values	Multi
References	X.520, RFC 4519
OID	2.5.4.12
Examples	title: Assistant Vice-Deputy for Redundancy Reduction

Usage notes

No controlled vocabulary, may contain anything. Student is not considered a title. Both academic titles and functions are covered in this attribute.

Feide usage notes

Source is an employee payroll system or student registry.

To encode employee category (“stillingskode”), the eduPersonEntitlement attribute (see page 16) is preferred over the title attribute, to ensure that unambiguous codes (represented by registered URNs) are used. Note that URNs registered by Feide currently does not include employee categories, but organizations owning a URN namespace may define their own values if needed.

Example applications for which this attribute would be useful:

Directory of directories, white pages.

3.7.24 uid

Name	uid
------	-----

Description	A computer system login name associated with the object
Format	DirectoryString
# of values	Multi
References	RFC 4519
OID	0.9.2342.19200300.100.1.1
Examples	uid: gmettes

Usage notes

A uid must be restricted to ASCII excluding space; avoiding punctuation is recommended. A common (stronger) restriction is a maximum length of 8 letters, restricted to [a-z, 0-9, -] must start with a letter. Likely only one value. See the extensive discussion in the "LDAP Recipe" [ldaprecipe].

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

A uid in itself is just an identifier. If mapping from uid to other identifications, such as the NIN, can be done by others, then the uid will require the same level of confidentiality as the NIN.

This attribute is reused in eduPersonPrincipalName and the restrictions on reallocation defined for eduPersonPrincipalName apply.

Feide usage notes

Source is user management system or another authoritative system. A person should have a single uid per organization.

Notice that uid is not case sensitive. uid should be used as the first part of eduPersonPrincipalName (before "@"), hence only lower case letters is to be used in uid. See also eduPersonPrincipalName.

Example applications for which this attribute would be useful:

Controlling access to resources.

3.7.25 userCertificate

Name	userCertificate
Description	A user's X.509 certificate
Format	Certificate
# of values	Multi
References	RFC 4523
OID	62.5.4.36
Examples	

Usage notes

RFC 4523 states that this attribute is to be requested and transferred using the attribute

description 'userCertificate;binary.' Incompatible implementations exist, see the IETF PKI work for details.

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).

The confidentiality of a certificate in itself is not problematic, depending on what information one chooses to include in the certificate. It is probable that the information included will be a combination of different fields of information described in this document. The certificate will then be an accumulation of all the different fields' combined features.

Assigned by a CA (Certificate Authority). Each CA has a contract with the higher education institution.

The userCertificate attribute was defined in RFC 2256, but was moved to RFC 4523.

Example applications for which this attribute would be useful:

Email clients, controlling access to resources, validation of electronic signatures.

3.7.26 userPassword

Name	userPassword
Description	The entry's password and encryption method in the following format: {encryption method}encrypted password
Format	OctetString
# of values	Multi
References	RFC 4519
OID	2.5.4.35
Examples	{SSHA}XtfcuWTPnI96jkPDEZfgIEzQ/39J8d9UGUbmNQ==

Usage notes

The server must support the LDAP Simple Bind method over TLS (Transport Layer Security). Applications that use LDAP Bind methods that transmit plain text passwords, such as Simple Bind, must use TLS or SSL (Secure Sockets Layer) to protect the password.

The person entries must be associated with a password, so that people can bind to the server. Servers may support various ways to achieve this. Typically the person entry will contain an attribute like userPassword.

Even if the password stored in this attribute is hashed, the attribute should be protected by access controls so that nobody can read the attribute and it only can be used to authenticate. Preferably, Bind methods that transmit plain text passwords should also be disabled when TLS or SSL is not established on the connection, in order to teach users not to send plain text passwords.

Feide usage notes

Source is user management system or another authoritative system. All passwords must be hashed/encrypted using a strong encryption method, such as SSHA, to make it unreadable to an intruder. See [sechash] for approved hashing algorithms. See RFC 2307 for format information.

It is recommended that passwords consist of a combination of upper and lowercase letters, digits and punctuation, have a length of at least 8 characters, and are not a word that can be found in an ordinary dictionary. For legacy reasons, national letters, such as æøå, should be avoided as they may cause interoperability problems with systems and browsers that do not support international character sets.

Example applications for which this attribute would be useful:

Controlling access to resources.

3.7.27 userSMIMECertificate

Name	userSMIMECertificate
Description	An X.509 certificate specifically for use in S/MIME applications (see RFCs 2632, 2633 and 2634).
Format	Binary
# of values	Multi
References	RFC 2798
OID	2.16.840.1.113730.3.1.40
Examples	

Usage notes

According to RFC 2798, "If available, this attribute is preferred over the userCertificate attribute for S/MIME applications." See also RFCs 2632, 2633 and 2634. RFC 2798 states that this attribute is to be stored and requested in the binary form, as 'userSMIMECertificate;binary.'

Semantic follow userSMIMECertificate in RFC 2798, "A PKCS#7 [RFC 2315] SignedData."

4 Document information

This chapter is informative only, and does not form part of the norEdu* specification.

4.1 Acknowledgments

Editing team: Ingrid Melve, Jon Strømme, Bård Henry Moum Jakobsen, Anders Lund, Walter Tvester, Ketil Albertsen, Snorre Løvås, Annette Grande, Hildegunn Vada and Jaime Pérez. Contact address is aktive@feide.no

Thanks to Keith Hazelton and Internet2/NMI for allowing us to reuse the eduPerson and eduOrg documentation. Without your example and your kind help, this document would have been much harder to write.

Thanks to Peter Green for giving access to auEduPerson and answering questions. Thanks to the SWITCH AAI team for publishing switchEduPerson and documenting choices made.

Thanks to the GNOMIS community for feedback and support. Discussions on funetEduPerson attributes proved helpful.

Among other persons who provided valuable help and feedback are Steinar Hamre, Hallvard Furuseth, Per-Steinar Iversen and Tor Gjerde.

4.2 References

- [auEduPerson] "auEduPerson Schema", <http://www.aaf.edu.au/wp-content/uploads/2012/05/aueduperson-200812.txt>
- [BCP47] A. Phillips, "Tags for Identifying Languages", BCP 47, Sep. 2009
- [eduOrg200210] "EduOrg Object Class Specification (200210)" Internet2 Middleware Architecture Committee (MACE-Dir), <http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduOrg-200210.pdf>
- [eduPerson201203] "eduPerson Object Class Specification (201203)" Internet2 Middleware Architecture Committee (MACE-Dir), <http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html>
- [funetEduPerson] "FunetEduPerson schema", http://www.csc.fi/hallinto/haka/maaritykset/funeteduperson-skeema/fep_2.1.pdf
- [GO-attributter] "Feides informasjonsmodell for grunnopplæringa", http://www.feide.no/sites/feide.no/files/documents/go_attributter.pdf
- [ISO639] ISO639-1 and ISO639-2, "Codes for the Representation of Names of Languages", <http://www.loc.gov/standards/iso639-2/>
- [ISO3166] "ISO 3166 code lists", http://www.iso.org/iso/home/standards/country_codes.htm
- [ldaprecipe] "A Recipe for Configuring and Operating LDAP Directories", <http://middleware.internet2.edu/dir/docs/ldap-recipe.htm>
- [navneloven] "Lov om personnavn (navneloven)", Norwegian naming legislation, <http://www.lovdatab.no/all/nl-20020607-019.html>
- [RFC2079] Smith, M., "Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs)", RFC 2079, Jan. 1997.
- [RFC2798] M Smith, "Definition of the inetOrgPerson LDAP Object Class", RFC 2798, Apr. 2002
- [RFC2849] Goode, G., "The LDAP Data Interchange Format (LDIF) - Technical Specification" RFC 2849, Jun. 2000.
- [RFC3986] T. Berners-Lee, "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986, Jan. 2005
- [RFC4510] K. Zeilenga, "LDAP: Technical Specification Road Map", RFC 4510, Jun. 2006

[RFC4511]	J. Sermersheim, "LDAP: The Protocol", RFC 4511, Jun. 2006
[RFC4512]	J. Sermersheim, "LDAP: Directory Information Models", RFC 4512, Jun. 2006
[RFC4513]	R. Harrison, "LDAP: Authentication Methods and Security Mechanisms", RFC 4513, Jun. 2006
[RFC4514]	K. Zeilenga, "LDAP: String Representation of Distinguished Names", RFC 4514, Jun. 2006
[RFC4515]	M. Smith, "LDAP: String Representation of Search Filters", RFC 4515, Jun. 2006
[RFC4516]	M. Smith, "LDAP: Uniform Resource Locator", RFC 4516, Jun. 2006
[RFC4517]	S. Legg, "LDAP: Syntaxes and Matching Rules", RFC 4517, Jun. 2006
[RFC4518]	K. Zeilenga, "LDAP: Internationalized String Preparation", RFC 4518, Jun. 2006
[RFC4519]	A. Sciberras, "LDAP: Schema for User Applications", RFC 4519, Jun. 2006
[RFC4520]	K. Zeilenga, "Internet Assigned Numbers Authority (IANA) Considerations for LDAP", RFC 4520, Jun. 2006
[RFC4524]	K. Zeilenga, "COSINE LDAP/X.500 Schema", RFC 4524, Jun. 2006
[saml]	"Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip
[schac]	"SCHema for ACademia", TERENA, 2011, https://wiki.refeds.org/display/STAN/SCHAC
[sechash]	"Secure hashing - approved algorithms", NIST, http://csrc.nsl.nist.gov/groups/ST/toolkit/secure_hashing.html
[UH-attributter]	"Feides informasjonsmodell for høgere utdanning", http://www.feide.no/sites/feide.no/files/documents/uh_attributter.pdf

4.3 Change log

4.3.1 From version 1.0 to 1.1

- Changed OIDs for the Feide attributes that are not inherited from eduPerson or eduOrg.
- Changed names of Feide attributes (norEduPersonBirthDate, norEduPersonNIN, norEduPersonLIN, norEduOrgAcronym, norEduOrgUniqueNumber, norEduOrgUnitUniqueNumber).
- Changed norEduPersonNIN type from Integer to DirectoryString

- Changed givenName to MANDATORY, due to popular demand.
- Indexing information for eduOrg200210 updated and changed as result of testing
- Changed matching rules from caseExactIA5Match to caseExactMatch

4.3.2 From version 1.1 to 1.2

- Changed givenName back to OPTIONAL, after discussions with service providers
- userSMIMECertificate and userCertificate both have the same confidentiality level of medium
- Fixed typos and removed warning about beta

4.3.3 From version 1.2 to 1.3

- Changed object classes to Auxiliary to minimize interoperability problems.
- Removed all unused attributes from the document
- Feide realm specification, added feideSchema for versioning information of AT
- Restrictions on Feide name (eduPersonPrincipalName) changed to prevent reuse
- Added definitions for jpegPhoto, mobile, eduPersonEntitlement, eduPersonScopedAffiliation
- Changed data type from Integer to NumericString for norEduPersonBirthDate and norEduPersonNIN
- norEduPersonLIN is defined to include all scoped identifiers. The attribute must be parsed to separate the issuer from the value of the identifier.
- labeledURI may be part of norEduOrg, duplicates eduOrgHomePageURI and eduOrgWhitePageURI
- Added norEduOrgUniqueIdentifier (replaces norEduOrgUniqueNumber) and norEduOrgUnitUniqueIdentifier (replaces norEduOrgUnitUniqueNumber), and moved the two deprecated attributes to a new object class norEduObsolete
- Added federationFeideSchemaVersion attribute in the new object class federationFeideSchema

4.3.4 From version 1.3 to 1.4

Schema related changes:

- norEdu* objects now has no MUST attributes. In the Norwegian Feide federation, a number of attributes are defined as mandatory, as a federation defined restriction on use of the schema.
- Added attributes norEduOrgNIN and norEduOrgSchemaVersion.
- User password encryption method is no longer required to be MD5. However, a strong encryption method should be used.
- Included description of schac attributes schacHomeOrganization and schacUserPrivateAttribute, eduPerson attributes eduPersonNickname and eduPersonTargetedID, and common attribute dc.
- Obsoleted attribute federationFeideSchemaVersion and object class feideFederationSchema in favor of norEduOrgSchemaVersion, norEduOrgUniqueNumber in favor of norEduOrgUniqueIdentifier and norEduOrgUnitUniqueNumber in favor of norEduOrgUnitUniqueIdentifier.
- The norEdu* grammar definitions in Appendix A and B is cleaned up and is now formally correct.

Editorial changes:

- Removed search type info from individual attribute description. This information is found in the formal grammar in the appendix.
- References to eduPerson updated to include reference to 2004 version. Several citations of eduPerson descriptions updated to the 2004 version of eduPerson. All eduPerson attributes are now incorporated into the norEdu* description.
- Moved obsolete attributes to appendix.
- Complete rewrite of introductory chapters, format of attribute descriptions etc. norEdu attributes are now described in alphabetical order (similar to schac and eduPerson/eduOrg schema descriptions). For the electronic document version, the majority of external references have been made clickable links (where such have been found).
- Added index of attributes, with clickable (intra document) links to the description and grammar.
- References to RFC 2251 to 2256 updated to refer to the revised LDAP RFCs 4510 to 4519.

Feide specific changes:

- Changed Feide relevance from Mandatory to Optional for the ou attribute.
- Added definition of Feide urn:mace:feide.no:value-def:foresatt for use in eduPersonEntitlement.
- In Feide, norEduOrgNIN (the “foretaksnummer”, assigned by Brønnøysundregistrene) replaces norEduOrgUniqueIdentifier (assigned by SO) as a mandatory attribute.

4.3.5 From version 1.4 to 1.4.1

- In the norEduOrg and norEduOrgUnit object classes, those common attributes which are neither specified in the MAY parts of the eduOrg/eduOrgUnit classes nor the X.521 organization object class. The affected attributes are,
norEduOrg: dc, mail, labeledURI
norEduOrgUnit: cn, mail, labeledURI
(These were specified in norEdu 1.3, but the 1.4 class definitions included norEdu attributes only in the MAY part of the Appendix B definitions).
- The description of norEduOrgAcronym in chapter 3.1.1 stated that the attribute is to be used with the norEduOgr and norEduOrgUnit class, while it was omitted from the norEduOrgUnit class description in Appendix A. It is now included in both class definitions.
- The documentation now states explicitly that Appendix A and B are considered normative, i.e. part of the norEdu specification. Appendix C is informative, i.e. it is not a formal part of the specification.
- Chapter 1 now describes how information about new versions and revisions of the specification shall be distributed.

4.3.6 From version 1.4.1 to 1.5

- Removed the column “Feide relevance” in the Attribute Survey table in 3.1. All information regarding Feide relevance is now found in the two documents "GO-attributter" and "UH-attributter", for the primary and secondary school and higher education respectively.
- Added attribute description and definition for new attribute norEduPersonLegalName.
- Removed references to and information about the schac attributes.
- Updated information about userPassword. Changed the example from using MD5 to using

the SSHA hashing algorithm. Also included a reference to a NIST recommendation for approved algorithms.

- Updated the document according to eduPerson200712 and eduPerson200806.
- Updated the Feide usage notes and the norEdu attribute descriptions with regard to the increasing use of this specification in primary and secondary education.

4.3.7 From version 1.5 to 1.5.1

- Added one attribute definition from the schac schema (schacHomeOrganization).
- Updated the document according to eduPerson201203.
- Updated references.

4.3.8 From version 1.5.1 to 1.6

- Added two attribute definitions to the norEdu schema for multi-factor authentication.
- Updated description of the schac schema as well as its reference.
- Updated links to the TERENA website.
- Updated references pointing to the attribute table.
- Those using this document should from now on monitor www.feide.no for new versions and changes of this document, and not aktive@feide.no, forum@feide.no or gnomis@uninett.no.

Appendix A: Object classes (normative)

This appendix is normative, to be considered an integral part of the norEdu* specification.

norEdu

norEdu* has adopted the eduPerson and eduOrg object classes, but with some adaptations to the Nordic academic environment. Support for National Identity Numbers (norEduPersonNIN) and support for the numbering scheme for academic institutions have been added.

Note that when the norEdu* schema is used in the Feide federation, several attributes which are optional (MAY) according to the schema definition, are mandatory by the Feide usage rules (equivalent to a schema MUST requirement).

norEduOrg

```
objectclass ( 1.3.6.1.4.1.2428.90.2.1
  NAME 'norEduOrg'
  AUXILIARY
  DESC 'Supplementary attributes for an educational organization'
  MAY ( norEduOrgUniqueIdentifier $ norEduOrgNIN $
    norEduOrgAcronym $ norEduOrgSchemaVersion $
    dc $ mail $ labeledURI ) )
```

norEduOrgUnit

```
objectclass ( 1.3.6.1.4.1.2428.90.2.2
  NAME 'norEduOrgUnit'
  AUXILIARY
  DESC 'Supplementary attributes for a unit of an educational organization'
  MAY ( norEduOrgUnitUniqueIdentifier $ norEduOrgAcronym $
    cn $ mail $ labeledURI ) )
```

norEduPerson

```
objectclass ( 1.3.6.1.4.1.2428.90.2.3
  NAME 'norEduPerson'
  AUXILIARY
  DESC 'Supplementary attributes for a person affiliated with an educational organization'
  MAY ( norEduPersonNIN $ norEduPersonLIN $ norEduPersonBirthDate $
    norEduPersonLegalName $ norEduPersonServiceAuthnLevel $
    norEduPersonAuthnMethod ) )
```

norEduObsolete

```
objectclass ( 1.3.6.1.4.1.2428.90.2.4
  NAME 'norEduObsolete'
  AUXILIARY
  DESC 'Attributes obsoleted in norEdu 1.4 or later'
  MAY ( norEduOrgUniqueNumber $ norEduOrgUnitUniqueNumber $
    federationFeideSchemaVersion ) )
```

eduPerson

eduPerson is an auxiliary object class for campus directories designed to facilitate communication among higher education institutions. It consists of a set of data elements or attributes about individuals within higher education, along with recommendations on the syntax and semantics of the data that may be assigned to those attributes. The eduPerson attributes are found in the next

section. All these attribute names are prefaced with eduPerson. The eduPerson auxiliary object class contains all of them as "MAY" attributes:

```
objectclass ( 1.3.6.1.4.1.5923.1.1.2
  NAME 'eduPerson'
  AUXILIARY
  MAY ( eduPersonAffiliation $ eduPersonNickname $ eduPersonOrgDN $
    eduPersonOrgUnitDN $ eduPersonPrimaryAffiliation $
    eduPersonPrincipalName $ eduPersonEntitlement $
    eduPersonPrimaryOrgUnitDN $ eduPersonScopedAffiliation $
    eduPersonTargetedID $ eduPersonAssurance ) )
```

It is recommended that person entries have the person, organizationalPerson and inetOrgPerson object classes defined. The former two are defined in X.521 (2001) and inetOrgPerson is defined in RFC 2798 and based in part on RFC 2256 (now obsoleted by RFC 4519). EduPerson attributes would be brought in to the person entry as appropriate from the auxiliary eduPerson object class.

Attributes from the person, organizationalPerson and inetOrgPerson classes are listed. The purpose of listing them is primarily as a convenience to enterprise directory designers, but in some cases notes were added to clarify aspects of meaning or usage in the education community beyond what can be found in the original standards documents.

Additional information on eduPerson including LDIF for implementing the object class and attributes, is available at its home on the web: <http://middleware.internet2.edu/eduperson/>.

eduOrg

eduOrg describes attributes for higher education organizations.

```
objectclass ( 1.3.6.1.4.1.5923.1.2.2
  NAME 'eduOrg'
  AUXILIARY
  MAY ( eduOrgHomePageURI $ eduOrgIdentityAuthNPolicyURI $
    eduOrgLegalName $ eduOrgSuperiorURI $
    eduOrgWhitePagesURI $ cn ) )
```

Appendix B: Attribute definitions (normative)

This appendix is normative, to be considered an integral part of the norEdu* specification.

Attributes defined by norEdu*

norEduPersonNIN

```
attributetype ( 1.3.6.1.4.1.2428.90.1.5
  NAME 'norEduPersonNIN'
  DESC 'National Identity Number, assigned by public authorities'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  EQUALITY caseIgnoreMatch
  USAGE userApplications
  SINGLE-VALUE )
```

norEduPersonLegalName

```
attributetype ( 1.3.6.1.4.1.2428.90.1.10
  NAME 'norEduPersonLegalName'
```

DESC 'The legal name for the subject it is associated with'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SUBSTR caseIgnoreSubstringsMatch
EQUALITY caseIgnoreMatch
USAGE userApplications
SINGLE-VALUE)

norEduPersonLIN

attributetype (1.3.6.1.4.1.2428.90.1.4
NAME 'norEduPersonLIN'
DESC 'Locally defined unique identifier for a person'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SUBSTR caseIgnoreSubstringsMatch
EQUALITY caseIgnoreMatch
USAGE userApplications)

norEduOrgAcronym

attributetype (1.3.6.1.4.1.2428.90.1.6
NAME 'norEduOrgAcronym'
DESC 'Acronym for the organization.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
EQUALITY caseIgnoreMatch
USAGE userApplications)

norEduPersonBirthDate

attributetype (1.3.6.1.4.1.2428.90.1.3
NAME 'norEduPersonBirthDate'
DESC 'Birth date for a person.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
EQUALITY integerMatch
USAGE userApplications
SINGLE-VALUE)

norEduOrgSchemaVersion

attributetype (1.3.6.1.4.1.2428.90.1.11
NAME 'norEduOrgSchemaVersion'
DESC 'Version number of the norEdu schema used by the organization'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
EQUALITY caseIgnoreMatch
USAGE userApplications)

norEduOrgUniqueIdentifier

attributetype (1.3.6.1.4.1.2428.90.1.7
NAME 'norEduOrgUniqueIdentifier'
DESC 'Unique identifier describing the organization.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
EQUALITY caseIgnoreMatch
USAGE userApplications
SINGLE-VALUE)

norEduOrgUnitUniquelIdentifier

attributetype (1.3.6.1.4.1.2428.90.1.8
 NAME 'norEduOrgUnitUniquelIdentifier'
 DESC 'Unique identifier describing the organizational unit.'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 EQUALITY caseIgnoreMatch
 USAGE userApplications
 SINGLE-VALUE)

norEduOrgNIN

attributetype (1.3.6.1.4.1.2428.90.1.12
 NAME 'norEduOrgNIN'
 DESC 'Identifier assigned to the organization by public authorities'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 EQUALITY caseIgnoreMatch
 USAGE userApplications
 SINGLE-VALUE)

norEduPersonServiceAuthnLevel

attributetype (1.3.6.1.4.1.2428.90.1.13
 NAME 'norEduPersonServiceAuthnLevel'
 DESC 'Authentication level enforcement policies.'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 EQUALITY caseIgnoreMatch
 USAGE userApplications)

norEduPersonAuthnMethod

attributetype (1.3.6.1.4.1.2428.90.1.14
 NAME 'norEduPersonAuthnMethod'
 DESC 'List of authentication methods that can be used by the subject.'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 EQUALITY caseIgnoreMatch
 USAGE userApplications)

Obsolete norEdu* attributes**norEduOrgUniqueNumber**

attributetype (1.3.6.1.4.1.2428.90.1.1
 NAME 'norEduOrgUniqueNumber'
 DESC 'The number describing the institution.'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
 EQUALITY integerMatch
 USAGE userApplications
 SINGLE-VALUE)

norEduOrgUnitUniqueNumber

attributetype (1.3.6.1.4.1.2428.90.1.2
 NAME 'norEduOrgUnitUniqueNumber'
 DESC 'The number describing the organizational unit.'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27

EQUALITY integerMatch
USAGE userApplications
SINGLE-VALUE)

federationFeideSchemaVersion

attributetype (1.3.6.1.4.1.2428.90.1.9
NAME 'federationFeideSchemaVersion'
DESC 'The norEdu scheme version used by the LDAP of the organization.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
EQUALITY caseIgnoreMatch
USAGE userApplications
SINGLE-VALUE)

Attributes from schac

schacHomeOrganization

attributetype (1.3.6.1.4.1.25178.1.2.9
NAME 'schacHomeOrganization'
DESC ' Domain name of the home organization.'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
EQUALITY caseIgnoreMatch
SINGLE-VALUE)

Attributes from eduPerson

eduPersonAffiliation

attributetype (1.3.6.1.4.1.5923.1.1.1.1
NAME 'eduPersonAffiliation'
DESC 'eduPerson per Internet2 and EDUCAUSE'
EQUALITY caseIgnoreMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

eduPersonEntitlement

attributetype (1.3.6.1.4.1.5923.1.1.1.7
NAME 'eduPersonEntitlement'
DESC 'eduPerson per Internet2 and EDUCAUSE'
EQUALITY caseExactMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

eduPersonNickname

attributetype (1.3.6.1.4.1.5923.1.1.1.2
NAME 'eduPersonNickname'
DESC 'eduPerson per Internet2 and EDUCAUSE'
EQUALITY caseIgnoreMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

eduPersonOrgDN

attributetype (1.3.6.1.4.1.5923.1.1.1.3
NAME 'eduPersonOrgDN'
DESC 'eduPerson per Internet2 and EDUCAUSE'
EQUALITY distinguishedNameMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.12' SINGLE-VALUE)

eduPersonOrgUnitDN

attributetype (1.3.6.1.4.1.5923.1.1.1.4
 NAME 'eduPersonOrgUnitDN'
 DESC 'eduPerson per Internet2 and EDUCAUSE'
 EQUALITY distinguishedNameMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.12')

eduPersonPrimaryAffiliation

attributetype (1.3.6.1.4.1.5923.1.1.1.5
 NAME 'eduPersonPrimaryAffiliation'
 DESC 'eduPerson per Internet2 and EDUCAUSE'
 EQUALITY caseIgnoreMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE)

eduPersonPrimaryOrgUnitDN

attributetype (1.3.6.1.4.1.5923.1.1.1.8
 NAME 'eduPersonPrimaryOrgUnitDN'
 DESC 'eduPerson per Internet2 and EDUCAUSE'
 EQUALITY distinguishedNameMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.12' SINGLE-VALUE)

eduPersonPrincipalName

attributetype (1.3.6.1.4.1.5923.1.1.1.6
 NAME 'eduPersonPrincipalName'
 DESC 'eduPerson per Internet2 and EDUCAUSE'
 EQUALITY caseIgnoreMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE)

eduPersonScopedAffiliation

attributetype (1.3.6.1.4.1.5923.1.1.1.9
 NAME 'eduPersonScopedAffiliation'
 DESC 'eduPerson per Internet2 and EDUCAUSE'
 EQUALITY caseIgnoreMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

eduPersonTargetedID

attributetype (1.3.6.1.4.1.5923.1.1.1.10
 NAME ' eduPersonTargetedID'
 DESC 'eduPerson per Internet2 and EDUCAUSE'
 EQUALITY caseExactMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

eduPersonAssurance

attributetype (1.3.6.1.4.1.5923.1.1.1.11
 NAME 'eduPersonAssurance'
 DESC 'eduPerson per Internet2 and EDUCAUSE'
 EQUALITY caseExactMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

Attributes from eduOrg

eduOrgHomePageURI

attributetype (1.3.6.1.4.1.5923.1.2.1.2
NAME 'eduOrgHomePageURI'
DESC 'eduOrg per Internet2 and EDUCAUSE'
EQUALITY caseExactMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

eduOrgIdentityAuthNPolicyURI

attributetype (1.3.6.1.4.1.5923.1.2.1.3
NAME 'eduOrgIdentityAuthNPolicyURI'
DESC 'eduOrg per Internet2 and EDUCAUSE'
EQUALITY caseExactMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

eduOrgLegalName

attributetype (1.3.6.1.4.1.5923.1.2.1.4
NAME 'eduOrgLegalName'
DESC 'eduOrg per Internet2 and EDUCAUSE'
EQUALITY caseIgnoreMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

eduOrgWhitePagesURI

attributetype (1.3.6.1.4.1.5923.1.2.1.6
NAME 'eduOrgWhitePagesURI'
DESC 'eduOrg per Internet2 and EDUCAUSE'
EQUALITY caseExactMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

Appendix C: Obsolete attributes

This appendix is informative only, and does not form part of the norEdu* specification.

Attributes obsoleted from norEdu*1.3 to norEdu*1.4

norEduOrgUniqueNumber

Obsoleted by norEduOrgNIN, norEduOrgUniquelIdentifier.

Definition

The number assigned the higher educational institution by Universities and Colleges Admission Service (SO).

Application utility class	# values	Syntax	Search type	OID
Standard	Single	Integer	Eq	1.3.6.1.4.1.2428.90.1.1

Notes

Not relevant for persons. Format is 3 digits country code (000 for Norway) and 5 digits institution number. To contain the number obtained from FS/SUAF/USIT/UiO.

Confidentiality	Data integrity	Availability	Feide relevance
None	Medium	Medium	DEPRECATED

SO and FS/SUA/USIT/UiO define institution numbers for institutions. The institution number is not an organization number as defined by the Norwegian Brønnøysund registry (Register of Business Enterprises) or a number identifying the institution as a legal entity. If those numbers are to be used they must be contained in separate attributes to be defined later.

Example (LDIF Fragment):

norEduOrgUniqueNumber: 00000185

norEduOrgUnitUniqueNumber

Obsoleted by norEduOrgUnitUniquelIdentifier

Definition

The number describing the organizational unit.

Application utility class	# values	Syntax	Search type	OID
Standard	Single	Integer	Pres, Eq	I.3.6.1.4.1.2428.90.1.2

Notes:

Not relevant for persons

Confidentiality	Data integrity	Availability	Feide relevance
None	Medium	Medium	DEPRECATED

The institutions establish their own organizational structure and describe it using location codes (“stedkoder”). This is done as an integral part of FS, but the institutions may make corresponding definitions relating to employee registries or accounting systems. One way to use this is to contain a six-digit number of the form XXYYZZ where XX is organizational unit (“ENHET”), YY is section (“seksjon”) and ZZ is group (“gruppe”).

Example applications for which this attribute would be useful:

Door locks, physical access control, web portals.

Example (LDIF Fragment):

norEduOrgUnitUniqueNumber: 332244

federationFeideSchemaVersion

Obsoleted by norEduSchemaVersion.

Definition

Attribute containing the schema information for the federation. Version number of the norEdu* specification in use.

Application utility class	# values	Syntax	Search type	OID
Standard	Single	DirectoryString	Eq	I.3.6.1.4.1.2428.90.1.9

Notes

To be used with the norEduOrg object class.

Confidentiality	Data integrity	Availability	FEIDE relevance
Low	High	High	MANDATORY

The version number should be included in the description of the schema specification for the federation.

Example (LDIF Fragment)

federationFeideSchemaVersion: 1.3