

Feides informasjonsmodell for grunnopplæringa

September 2015

Bruk av norEdu* Object Class Specification v.1.6 for grunnopplæringa

Attributtdokumentet



**SENTER
FOR IKT I
UTDANNINGEN**

Dokumenthistorikk

Versjon	Dato	Initialer	Kommentar
2015-09	September 2015	HV, JPC, SL	Ny versjon basert på norEdu*-spesifikasjon versjon 1.6. Nye krav knyttet til gruppeinformasjon og sterk autentisering. Se for øvrig endringslogg (s. 21).

UNINETT AS
Postboks 4769 Sluppen
NO-7465 Trondheim
Telephone: +47 73 55 79 00
Fax: +47 73 55 79 01
E-mail: info@uninett.no
Web: www.uninett.no

Innholdsfortegnelse

1	Oversikt over Feides LDAP-struktur	1
1.1	Objektklasser.....	1
1.2	Attributter.....	2
2	Person	4
2.1	Obligatorisk - person.....	4
2.2	Anbefalt - person.....	13
3	Organisasjon.....	15
3.1	Obligatorisk – organisasjon.....	15
3.2	Anbefalt – organisasjon	16
4	Organisasjonsenhet	17
4.1	Obligatorisk – organisasjonsenhet.....	17
4.2	Anbefalt – organisasjonsenhet.....	18
5	Valgfrie attributter – person og organisasjon.....	19
6	Endringslogg.....	21
6.1	Fra versjon 2012-02 til versjon 2013-10.....	21
6.2	Fra versjon 2014-01 til 2015-06.....	21
	Appendiks 1 – LDIF-eksempel	23
	Appendiks 2 – Registrering av Grep-koder i eduPersonEntitlement	25
	Appendiks 3 – Registrering av gruppeinformasjon i eduPersonEntitlement.....	28

I Oversikt over Feides LDAP-struktur

I.1 Objektklasser

Kravene Feide stiller til struktur på data i organisasjonenes LDAP-katalog er basert på [norEdu* Object Class Specification](#)¹. I tillegg til spesifikasjonen finnes dette dokumentet, som definerer hvilke av attributtene fra norEdu*-spesifikasjonen som er obligatoriske og anbefalte for organisasjoner i grunnopplæringen.

LDAP-katalogene med brukerdata hos den enkelte organisasjon er organisert i en trestruktur. I denne trestrukturen ligger noder, som er en samling av attributter og tilhørende verdier om:

- personer
- organisasjon (skoleeier)
- organisasjonsenheter (skoler)

norEdu*-spesifikasjonen definerer tre viktige objektklasser:

- norEduPerson
- norEduOrg
- norEduOrgUnit

Hver objektklasse definerer et sett med attributter. Flere objektklasser brukt sammen kan gi et større sett med attributter som utgjør all informasjon om en person, organisasjon eller organisasjonsenhet.

Et eksempel på dette er at en node med personinformasjon vil ha attributter fra objektklassene `norEduPerson`, `schac`, `eduPerson` og `inetOrgPerson`. `inetOrgPerson` vil igjen bruke attributter fra objektklassene `person`, `organizationalPerson` og `top`. Les mer om objektklasser i [norEdu*-spesifikasjonen](#).

To attributter (`eduPersonOrgDN` og `eduPersonOrgUnitDN`) forteller hvilken skoleeier og hvilke skoler en person er tilknyttet. Disse inneholder

¹ http://www.feide.no/sites/feide.no/files/documents/norEdu_spec.pdf

unik peker til noder i katalogtreet som inneholder informasjon om skoleeieren og skolene. `eduPersonPrimaryOrgUnitDN` forteller hvilken skole personen har hovedtilhørighet til. De ulike nodene for person, organisasjon og organisasjonsenheter, samt koblingene mellom dem, er vist i Figur 1 på side 3.

1.2 **Attributter**

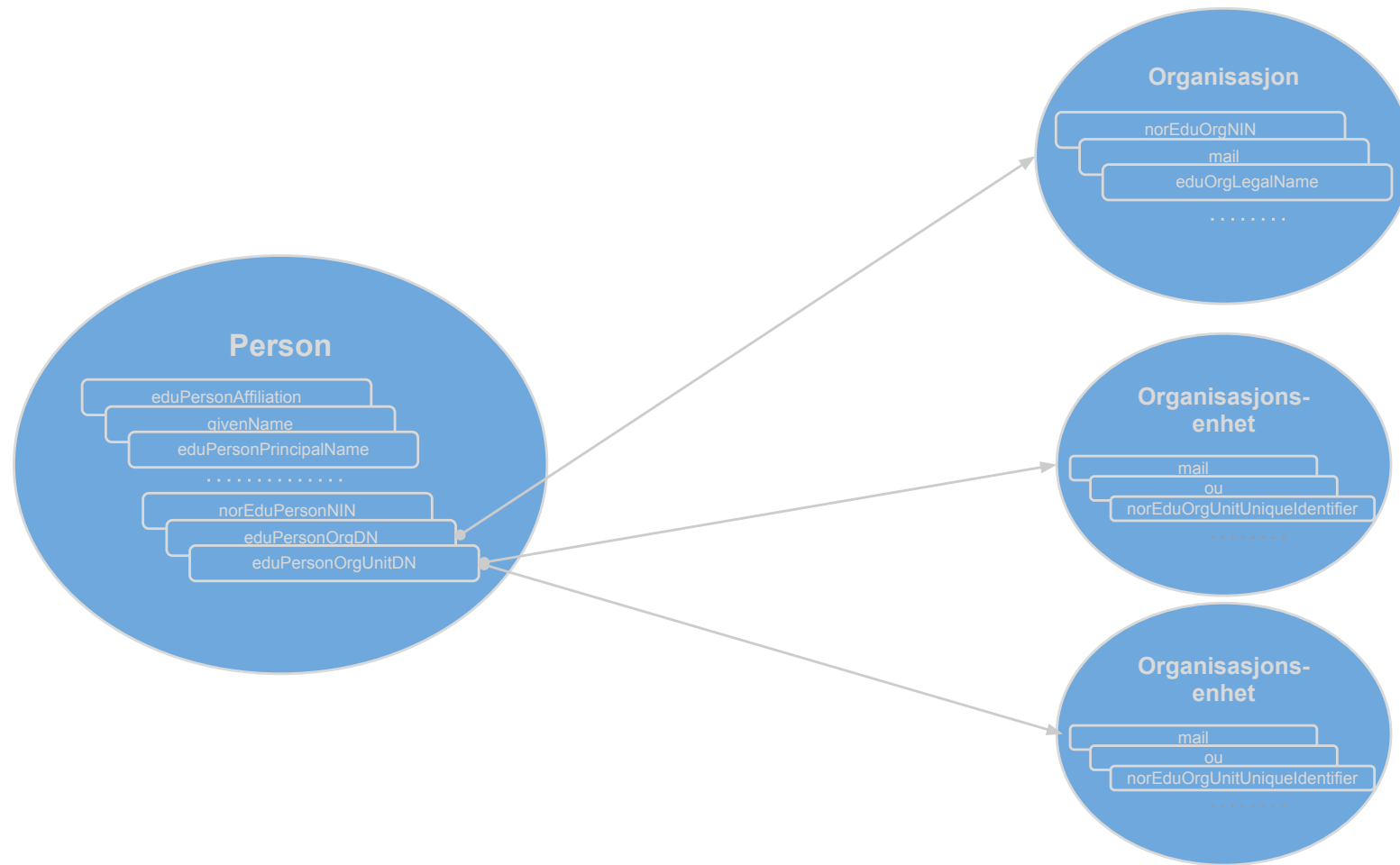
Når en bruker logger inn på en tjeneste via Feide, får tjenesten beskjed om at brukeren er autentisert samt et utvalg informasjonselementer som tilhører denne brukeren. Hvilke informasjonselementer tjenesten mottar, er begrenset gjennom en avtale mellom Feide og tjenesten. I Feide bruker vi begrepet *attributter* om de ulike informasjonselementene.

Generelt anbefales det å legge mest mulig informasjon inn i Feide-katalogen, og i norEdu*-spesifikasjonen finnes det attributter for mange ulike typer informasjonselementer. Mange tjenester etterspør stadig flere typer informasjonselementer, og de organisasjoner som legger mye informasjon inn i Feide-katalogen vil lettere kunne ta i bruk de ulike tjenestene som er koblet til Feide.

For å gjøre det enklere for vertsansisasjonene og tjenestene, har Feide valgt å klassifisere attributter i tre kategorier:

- **Obligatorisk** – skal legges inn i Feide-katalogen
- **Anbefalt** – anbefales å legges inn i Feide-katalogen
- **Valgfrie** – disse er opp til organisasjonen selv å vurdere om de ønsker å legge i Feide-katalogen

Obligatoriske og anbefalte attributter er gjerne de som tjenestene forventer å få utlevert i dag. På tross av denne klassifiseringen vil Feide sterkt oppfordre vertsansisasjoner til å legge inn mest mulig informasjon i Feide-katalogen. I dette dokumentet får du en rask oversikt over obligatoriske, anbefalte og valgfrie attributter.



Figur 1: De ulike objektclassene i Feide-katalogen: person, organisasjon og organisasjonsenhet. Pilene viser hvordan bestemte attributter i person-noden peker på den organisasjon og organisasjonsenhet(er) personen tilhører.

2 Person

2.1 Obligatorisk - person

Attributtnavn	Kort beskrivelse	Eksempel	Multi-valued ²
cn	Generelt navn på noden med personinformasjon.	cn: Arnt Nordmann og/eller cn: olanor123	x
displayName	Personens foretrukne navn.	displayName: Ola Nordmann	
norEduPersonLegalName	Personens formelle navn, eksempelvis som registrert i Folkeregisteret.	norEduPersonLegalName: Arnt Ola Olsen Nordmann	
givenName	Personens fornavn.	givenName: Ola	x
sn	Personens etternavn.	sn: Nordmann og/eller sn: Olsen Nordmann	x
eduPersonPrincipalName	Fullt Feide-navn. (Se mer info under.)	eduPersonPrincipalName: olanor123@skotthyll.kommune.no	
norEduPersonNIN ³	Fødselsnummer. (Se mer info under.)	norEduPersonNIN: 28089533134	

² Med *multivalued* menes hvorvidt denne attributten kan ha flere verdier. Et kryss her betyr at det kan registreres flere verdier.

³ Attributten er kun obligatorisk dersom en gyldig verdi eksisterer. Se mer info på side 8.

uid	Personens lokale brukernavn hos skoleeier. (Se mer info under.)	uid: olanor123	x
userPassword	Personens passord for Feide-pålogging. (Se mer info under.)	userPassword: {SSHA}dOVBpGreCxOAj/DqQ5faXcPAEd0hIbd LTS15eA==	x
eduPersonOrgDN	Peker til LDAP-noden som inneholder informasjon om skoleeieren personen tilhører.	eduPersonOrgDN: dc=Skotthyll,dc=kommune,dc=no	
eduPersonOrgUnitDN	Peker til LDAP-nodene som inneholder informasjon om organisasjonsenheten(e) personen tilhører. (Se mer info under.)	eduPersonOrgDN: ou=Hylla skole,cn=organization,dc=Skotthyll,dc= =kommune,dc=no	x
eduPersonPrimaryOrgUnitDN	Peker til LDAP-noden som inneholder informasjon om organisasjonsenheten personen har sin hovedtilhørighet til. (Se mer info under.)	eduPersonPrimaryOrgUnitDN: ou=Hylla skole,cn=organization,dc=Skotthyll,dc= =kommune,dc=no	
eduPersonAffiliation	Rolle hos skoleeier. (Se mer info under.)	eduPersonAffiliation: member eduPersonAffiliation: student eller eduPersonAffiliation: faculty eduPersonAffiliation: employee eduPersonAffiliation: member	x

eduPersonEntitlement	Informasjon om rettigheter, roller og grupper personen har. (Se mer info under.)	<p>Eksempel på trinn: eduPersonEntitlement: urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn6</p> <p>Eksempel på utdanningsprogram: eduPersonEntitlement: urn:mace:feide.no:go:grep:http://psi.udir.no/ontologi/utdanningsprogram/studiespesialisering</p> <p>Eksempel på basisgruppe: eduPersonEntitlement: urn:mace:feide.no:go:group:b::NO975278964:6A:2014-08-01:2015-06-15:student:Klasse%206A</p> <p>Eksempel på undervisningsgruppe: eduPersonEntitlement: urn:mace:feide.no:go:group:u:NOR1211:NO974558386:3aaa%2F3nh:2014-08-01:2015-06-15:student:Norsk%20hovedm%C3%A5l%20VG3</p> <p>Eksempel på annen gruppe: eduPersonEntitlement: urn:mace:feide.no:go:group:a::NO974558386:3fysa%2F1b3:2014-08-01:2014-12-31:student:Labgruppe%203%20Fysikk%20VG3</p>	x
norEduPersonAuthnMethod (kun obligatorisk ved bruk av sterk autentisering)	Liste over metoder for sterk autentisering som er tilgjengelig for personen. (Se mer info under.)	norEduPersonAuthnMethod: urn:mace:feide.no:auth:method:sms+4712345678 label=Work%20phone	x

norEduPersonServiceAuthnLevel <i>(kan brukes ved sterk autentisering, er ikke obligatorisk)</i>	Spesifiserer for hvilke tjenester sterk autentisering kreves. (Se mer info under.)	norEduPersonServiceAuthnLevel: urn:mace:feide.no:spid:12345 urn:mace:feide.no:auth:level:fad08:3 og/eller norEduPersonServiceAuthnLevel: urn:mace:feide.no:spid:all urn:mace:feide.no:auth:level:fad08:3	x
---	--	--	----------

eduPersonPrincipalName

`eduPersonPrincipalName` er per definisjon ikke case-sensitive. `OlaNor123@uin.no` er altså det samme Feide-navnet som `olanor123@uin.no`. For å sikre kompatibilitet med andre systemer, skal likevel `eduPersonPrincipalName` legges inn i katalogen med kun små bokstaver.

`eduPersonPrincipalName` bør aldri gjenbrukes av en ny person. Organisasjonen må sikre at `eduPersonPrincipalName` er unik. Dersom organisasjonen velger å gjenbruke et `eduPersonPrincipalName` som ikke er i aktiv bruk, er organisasjonen ansvarlig for at dette ikke fører til problemer. Det må for eksempel tas i betraktning at `eduPersonPrincipalName` kan ha blitt brukt som identifikator i eksterne systemer/tjenester.

`eduPersonPrincipalName` består av to deler: `<bruker>@<realm>`. Merk at når domenenavn benyttes som realm, skal dette være (underlagt) et domene som vertsorganisasjonen er registrert eier av.

Første del av `eduPersonPrincipalName` (før "@") skal være lik `uid`.

norEduPersonNIN

`norEduPersonNIN` skal være et unikt identifikasjonsnummer utstedt av Folkeregisteret eller Utlendingsdirektoratet (UDI):

- Fødselsnummer
- D-nummer
- DUF-nummer

Dersom en person ikke har noen av disse numrene, skal det ikke registreres noen verdi i `norEduPersonNIN` for denne personen.

uid

Selv om `uid` i utgangspunktet er multivalued, skal man bare registrere én verdi i dette feltet. `uid` er ikke case-sensitive, men skal på samme måte som `eduPersonPrincipalName` legges inn i katalogen med kun små bokstaver. `uid` skal utgjøre den første delen av `eduPersonPrincipalName`, før "@".

userPassword

Selv om `userPassword` i utgangspunktet er multivalued, er det vanlig å bare registrere én verdi i dette feltet.

I dette dokumentet er `userPassword` satt som en obligatorisk attributt fordi alle brukere må ha passord ved pålogging. Vær oppmerksom på at passord kan bli håndtert automatisk av katalogsystemet, slik at det ikke nødvendigvis må bli håndtert direkte. Det viktige er at den enkelte person kan autentisere seg ovenfor katalogsystemet (og dermed Feide) med bruk av et passord.

eduPersonOrgUnitDN

`eduPersonOrgUnitDN` er obligatorisk for personer som er tilknyttet en skole. For de personer som ikke er tilknyttet en skole, men likevel har behov for en Feide-bruker i sitt daglige virke, skal det ikke registreres noen verdi i `eduPersonOrgUnitDN`.

eduPersonPrimaryOrgUnitDN

Det presiseres at verdien som benyttes i `eduPersonPrimaryOrgUnitDN` også må være satt i `eduPersonOrgUnitDN`.

eduPersonAffiliation

eduPersonAffiliation inneholder informasjon om personens generelle rolle ved organisasjonen. Det er definert et lite sett generelle roller, ordnet i et hierarki som vist i figur 2 til høyre.

En elev vil ha alle verdiene:

```
eduPersonAffiliation: student
eduPersonAffiliation: member
```

En pedagogisk ansatt vil ha alle verdiene:

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

En ansatt som ikke er pedagogisk ansatt vil ha alle verdiene:

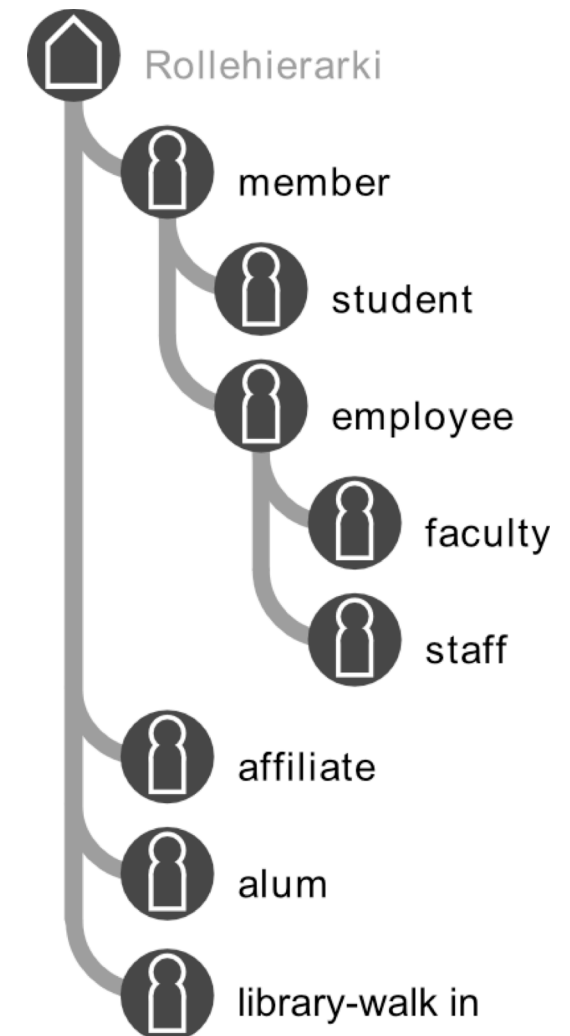
```
eduPersonAffiliation: staff
eduPersonAffiliation: employee
eduPersonAffiliation: member
```

Verdien "affiliate" brukes for å tydeliggjøre at personen er tilknyttet organisasjonen, men uten formelle kontrakter for et ansettelsesforhold eller en skoleplass (for eksempel privatister):

```
eduPersonAffiliation: affiliate
```

En person kan ha flere roller, for eksempel både være ansatt og elev:

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



Figur 2: Rollehierarki

eduPersonEntitlement

`eduPersonEntitlement` inneholder spesifikke rettigheter eller roller som personen har. Dette kan f.eks. være uttrykt ved en stillingskode eller spesifikke rettigheter knyttet til en bestemt tjeneste. Så fremt det finnes slik informasjon om en person, anbefales det at dette blir registrert i `eduPersonEntitlement`.

Verdier som benyttes i `eduPersonEntitlement`-feltet skal være gyldige URler (Uniform Resource Identifier). Vi anbefaler bruk av URNer. Dersom det opprettes nye URN-verdier for `eduPersonEntitlement`, skal disse registreres i et [register som administreres av Feide](#)⁴. Forespørsler om tildeling av navnerom sendes på e-post til support@feide.no.

For grunnopplæringen skal informasjon om personens trinn, utdanningsprogram, programområde og fag være registrert i attributtet `eduPersonEntitlement`, uttrykt ved koder fra Utdanningsdirektoratets [Grep-rammeverk](#)⁵. Trinn, utdanningsprogram og programområde er obligatorisk å fylle ut, det vil si at attributtet skal være tilstede og det skal ha et innhold. Elever i grunnskolen er ikke assosiert med utdanningsprogram og programområde, og skal følgelig ikke ha disse utfyllt. Grep-koder skal prefikses med strengen "urn:mace:feide.no:go:grep:". Se "Appendiks 2 – Registrering av Grep-koder i `eduPersonEntitlement`" for detaljert informasjon.

Informasjon om personers tilhørighet til grupper skal også registreres i attributtet `eduPersonEntitlement`. Elever og læreres tilhørighet til basisgrupper/klasser og undervisningsgrupper er obligatorisk å fylle ut. Tilhørighet til andre typer grupper kan fylles ut. Gruppeinformasjon skal prefikses med strengen "urn:mace:feide.no:go:group:". Se "Appendiks 3 – Registrering av gruppeinformasjon i `eduPersonEntitlement`" for detaljert informasjon.

norEduPersonAuthnMethod

Denne attributten er obligatorisk for personer som skal logge inn på tjenester med sterk autentisering. Gyldige verdier bygges opp slik:

```
<identifikator for metoden> <metodedata spesifikt for personen> <valgfri "merkelapp">
```

Identifikator for SMS: urn:mace:feide.no:auth:method:sms

Identifikator for Godkjenner/ Authenticator: urn:mace:feide.no:auth:method:ga

⁴ <http://www.feide.no/urn>

⁵ http://grewiki.udir.no/index.php?title=Kom_i_gang

Eksempler:

Ved bruk av metoden engangspassord på sms:

- `norEduPersonAuthnMethod: urn:mace:feide.no:auth:method:sms +4712345678 label=Work%20phone`

Ved bruk av metoden Godkjenner/ Authenticator:

- `urn:mace:feide.no:auth:method:ga ABCDEFGHIJ234567 label=Authenticator%20(Feide)`

norEduPersonServiceAuthnLevel

Denne attributten gir muligheten til å liste opp hvilke tjenester én enkelt person skal bruke sterk autentisering til. Dette kan for eksempel være nyttig for personer som har utvidede rettigheter til en eller flere tjenester. Gyldige verdier er her:

- `urn:mace:feide.no:spid:<Feide-id for tjeneste> <autentiseringsnivå>`: Settes for de enkelttjenester personen skal logge inn med sterk autentisering. Feide-id for tjeneste fås ved å ta kontakt med support@feide.no.
- `urn:mace:feide.no:spid:all <autentiseringsnivå>`: Settes dersom personen skal logge inn med sterk autentisering til alle tjenester.

For sterk autentisering gjennom Feide er uri for autentiseringsnivå: `urn:mace:feide.no:auth:level:fad08:3`

2.2 Anbefalt - person

Attributtnavn	Kort beskrivelse	Eksempel	Multi-valued
mail	Personens e-postadresse. Skal være en personlig adresse. (Se mer info under.)	mail: ola.nordmann@elev.skotthyll.kommune.no og/eller mail: arnt1990@gmail.com	x
mobile	Mobilnummer knyttet til personen. (Se mer info under.)	mobile: +47 40404040	x
preferredLanguage	Personens foretrukne språkform etter ISO 639-3 og BCP 47.	preferredLanguage: nn eller preferredLanguage: nb	
schacHomeOrganization	Realm til organisasjonen som personen tilhører.	schacHomeOrganization: skotthyll.kommune.no	
eduPersonPrimaryAffiliation	Primærrolle hos skoleeier. (Se mer info under.)	eduPersonPrimaryAffiliation: student eller eduPersonPrimaryAffiliation: employee	
eduPersonScopedAffiliation	Personens rolle og institusjon. (Se mer info under.)	eduPersonScopedAffiliation: employee@NO179530458.skotthyll.kommune.no og eduPersonScopedAffiliation: employee@skotthyll.kommune.no	x

mail

mail skal være en personlig e-postadresse som bare brukeren har tilgang til.

mobile

`mobile` skal være et personlig mobilnummer som bare brukeren benytter.

eduPersonPrimaryAffiliation

`eduPersonPrimaryAffiliation` angir personens primærrolle ved organisasjonen. Dette kan eksempelvis være ekstra verdifullt om en person både opptrer som student og ansatt ved organisasjonen. For gyldige verdier, se mer info på side 10 (`eduPersonAffiliation`). Det presiseres at alle verdiene i Figur 2 kan brukes, men merk at verdien som benyttes også må være satt i `eduPersonAffiliation`.

eduPersonScopedAffiliation

For personer tilknyttet en skole, angir `eduPersonScopedAffiliation` personens rolle ved skolen, samt hvilken skole det gjelder. Syntaks for `eduPersonScopedAffiliation` er:

```
<rolle>@<norEduOrgUnitUniqueIdentifier>.<realm>
```

og

```
<rolle>@<realm>
```

Rolle må være en av verdiene i `eduPersonAffiliation`, mens `realm` tilsvarer den høyre delen (etter @) i `eduPersonPrincipalName`.

3 Organisasjon

Organisasjon er i Feide-sammenheng skoleeier – dette kan for eksempel være en kommune, fylkeskommune eller en privatskoleeier.

3.1 Obligatorisk – organisasjon

Attributtnavn	Kort beskrivelse	Eksempel	Multi-valued
eduOrgLegalName	Det offisielle navnet til organisasjonen.	eduOrgLegalName: Skotthyll kommune og/eller eduOrgLegalName: Skotthyll gielda	x
o	Navnet til organisasjonen.	o: Skotthyll kommune og/eller o: Skotthyll gielda	x
norEduOrgNIN	Organisasjonsnummer fra Brønnøysundregistrene. (Se mer info under.)	norEduOrgNIN: NO179530458	
mail	E-postadresse til organisasjonen.	mail: info@skotthyll.kommune.no	x
norEduOrgSchemaVersion	Hvilken versjon av norEdu* Object Class Specification organisasjonen benytter.	norEduOrgSchemaVersion: 1.5.1	

norEduOrgNIN

Merk at `norEduOrgNIN` skal være organisasjonsnummeret fra Brønnøysundregisteret som er registrert som skoleeier i Nasjonalt skoleregister⁶. Det skal bestå av ni siffer som prefikses med NO, og det skal ikke inneholde bindestrek eller mellomrom.

⁶ <http://nsr.udir.no>

3.2 Anbefalt – organisasjon

Attributtnavn	Kort beskrivelse	Eksempel	Multi-valued
telephoneNumber	Telefonnummer til organisasjonen.	telephoneNumber: +47 73557900	x
postalAddress	Postadressen til organisasjonen. (Se mer info under.)	postalAddress: Postboks 340\$7640 Skotthyll og/eller postalAddress: Kongens gate 12\$7640 Skotthyll	x

postalAddress

Merk at linjeskift i postadresser typisk oppgis som et \$-tegn (se eksempelet i tabellen over). Dette er noe som ofte håndteres automatisk av systemet som importerer data til katalogen.

4 Organisasjonsenhet

Hver skole tilknyttet skoleeieren er i utgangspunktet en egen organisasjonsenhet.

4.1 Obligatorisk – organisasjonsenhet

Attributtnavn	Kort beskrivelse	Eksempel	Multi-valued
ou	Det offisielle navnet til skolen.	ou: Hylla skole og/eller ou: Hylla	x
norEduOrgUnitUniqueIdentifiser	En unik identifikator for skolen. Enten et organisasjonsnummer eller underliggende bedriftsnummer fra Brønnøysundregistrene.	norEduOrgUnitUniqueIdentifiser: NO179530458	
mail	E-postadresse til skolen.	mail: hylla@skotthyll.kommune.no og/eller mail: post@hylla.skotthyll.kommune.no	x

norEduOrgUnitUniqueIdentifiser

`norEduOrgUnitUniqueIdentifiser` skal inneholde skolens organisasjonsnummer eller underliggende bedriftsnummer fra Brønnøysundregistrene, som registrert i Nasjonalt skolerregister⁷. Det skal bestå av ni siffer som prefikses med NO, og det skal ikke inneholde bindestrek eller mellomrom. Dersom skoleeier og skole er én og samme organisasjon skal `norEduOrgUnitUniqueIdentifiser` være lik `norEduOrgNIN`.

⁷ <http://nsr.udir.no>

4.2 Anbefalt – organisasjonsenhet

Attributtnavn	Kort beskrivelse	Eksempel	Multi-valued
telephoneNumber	Telefonnummer til skolen.	telephoneNumber: +47 73557900	x
postalAddress	Postadressen til skolen. (Se mer info under.)	postalAddress: Postboks 340\$7640 Skotthyll og/eller postalAddress: Nordveien 5\$7640 Skotthyll	x

postalAddress

Merk at linjeskift i postadresser typisk oppgis som et \$-tegn (se eksempelet i tabellen over). Dette er noe som ofte håndteres automatisk av systemet som importerer data til katalogen.

5 Valgfrie attributter – person og organisasjon

Her er en oversikt over attributter fra norEdu*-spesifikasjonen som ikke er obligatorisk eller anbefalt i Feide. For mer informasjon om hvert enkelt attributt, se norEdu*-spesifikasjonen. Det er opp til hver enkelt skoleeier å vurdere om denne informasjonen skal legges inn i Feide-katalogen, men det er en fordel hvis det som er tilgjengelig fylles ut.

Attributtnavn	Kort beskrivelse	Eksempel	Multi-valued
norEduOrgAcronym	Akronym for organisasjonen eller organisasjonsenheten.	norEduOrgAcronym: USIT	x
norEduPersonBirthDate	Fødselsdato for personen.	norEduPersonBirthDate: 19890828	
norEduPersonLIN	Lokalt ID-nummer, for eksempel student- eller ansattnummer.	norEduPersonLIN: skotthyll.kommune.no:employee:035016	x
eduOrgIdentityAuthNPolicyURI	URI som peker på organisasjonens policy for identitetshåndtering.	eduOrgIdentityAuthNPolicyURI: http://www.skotthyll.kommune.no/security/IA-policy.html	x
eduOrgHomePageURI	URL til organisasjonens toppnivå hjemmeside.	eduOrgHomePageURI: http://www.skotthyll.kommune.no	x
eduOrgWhitePagesURI	URL til organisasjonens åpne katalogtjeneste.	eduOrgWhitePagesURI: ldap://wpage.skotthyll.kommune.no	x
eduPersonAssurance	URI som gir informasjon om hvilke tillitsnivå for identitetshåndtering og autentisering organisasjonen oppfyller.	eduPersonAssurance: urn:mace:incommon:IAQ:sample	x

eduPersonNickname	Navn personen kalles til daglig.	eduPersonNickname: Ola	x
facsimileTelephoneNumber	Faksnummer.	facsimileTelephoneNumber: +47 73557901	x
homePhone	Hjemmenummeret til personen.	homePhone: +47 23456789	x
homePostalAddress	Hjemmepostadresse til personen.	homePostalAddress: Jordbærgata 14c\$7640 Skotthyll	x
jpegPhoto	Et bilde av personen i jpeg-format (opptil 250*250 px, rundt 30 kB).	(attributtverdi er i binær-format)	x
manager	LDAP-peker til leder for personen.	manager: uid=ojohnsen,ou=people,dc=skotthyll,dc=kommune,dc=no	x
postalCode	Postnummer for organisasjonen.	postalCode: NO-7640	x
postOfficeBox	Postboks.	postOfficeBox: 109260	x
street	Gateadresse.	street: Nordveien 5	x
title	Personens tittel.	title: Rektor	x
userCertificate	Personens X.509-sertifikat.	(attributtverdi er i binær-format)	x
userSMIMECertificate	Et X.509-sertifikat spesielt beregnet på bruk i S/MIME-applikasjoner, for eksempel signering og kryptering av e-post.	(attributtverdi er i binær-format)	x

6 Endringslogg

6.1 Fra versjon 2012-02 til versjon 2013-10

- `norEduPersonNIN` er endret fra "obligatorisk" til "obligatorisk dersom en gyldig verdi eksisterer". Retningslinjer for hvilke numre som kan legges inn i `norEduPersonNIN` er endret (s. 8).
- `eduPersonPrimaryAffiliation` er endret fra å være obligatorisk til å bli anbefalt (s. 13).
- Informasjon om organisasjonsenhet er nå kun obligatorisk for personer som er tilknyttet en skole (s. 9).
- To nye attributter er blitt anbefalte (s. 13):
 - `eduPersonScopedAffiliation`
 - `schacHomeOrganization`
- Presiserer at `uid` skal være lik første del av `eduPersonPrincipalName` (før "@") (s. 8).
- Informasjon om `eduPersonPrincipalName` og hvilket realm som kan brukes er endret (s. 8).
- Dokumentet refererer nå til `norEdu*`-spesifikasjonen versjon 1.5.1 (s. 1).
- Nytt kapittel med mer informasjon om obligatoriske, anbefalte og valgfrie attributter lagt til (kap. 1.2).
- Figur 1 oppdatert til å være mer generell når det gjelder hvilke attributter som er obligatoriske, anbefalte og valgfrie (s. 3).
- Dokumentet har gjennomgått språklige endringer slik at det i større grad er tilpasset privatskoleeiere.
- Nytt kapittel med oversikt over valgfrie attributter lagt til (kap. 5).
- Endringslogg lagt til (kap. 6).

6.2 Fra versjon 2014-01 til 2015-09

- Det er nå obligatorisk å registrere informasjon om elevers og læreres tilhørighet i basisgrupper/klasser og undervisningsgrupper i `eduPersonEntitlement`.

- Ett nytt attributt er obligatorisk for personer som skal benytte sterk autentisering (s. 11):
 - `norEduPersonAuthnMethod`
- Ett nytt attributt kan brukes for å liste opp hvilke tjenester én enkelt person skal bruke sterk autentisering til (dette er ikke obligatorisk):
 - `norEduPersonServiceAuthnLevel`
- Det er spesifisert at privatister kan ha verdien "affiliate" i attributtet `eduPersonAffiliation` for å tydeliggjøre tilknytning til organisasjonen.

Appendiks I – LDIF-eksempel

Person

```
dn: uid=olanor123,cn=people,dc=Skotthyll,dc=kommune,dc=no
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
objectClass: eduPerson
objectClass: schac
objectClass: norEduPerson
cn: Arnt Ola Nordmann
cn: olanor123
displayName: Ola Nordmann
eduPersonAffiliation: member
eduPersonAffiliation: student
eduPersonPrimaryAffiliation: student
eduPersonOrgDN: dc=Skotthyll,dc=kommune,dc=no
eduPersonOrgUnitDN: ou=Hylla skole,cn=organization,dc=Skotthyll,dc=kommune,dc=no
eduPersonPrimaryOrgUnitDN: ou=Hylla skole,cn=organization,dc=Skotthyll,dc=kommune,dc=no
eduPersonPrincipalName: olanor123@skotthyll.kommune.no
eduPersonScopedAffiliation: student@NO179530458.skotthyll.kommune.no
givenName: Ola
norEduPersonLegalName: Arnt Ola Olsen Nordmann
norEduPersonNIN: 28088933134
norEduPersonAuthnMethod: urn:mace:feide.no:auth:method:sms +4740404040 label=Work%20phone
schacHomeOrganization: skotthyll.kommune.no
sn: Nordmann
sn: Olsen Nordmann
uid: olanor123
userPassword: {SSHA}dOVBpGreCxOAJ/DqQ5faXcPAEd0hIbdLTS15eA==
```

```
eduPersonEntitlement: urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn6
mail: ola.nordmann@elev.skotthyll.kommune.no
mobile: +47 40404040
preferredLanguage: nb
```

Organisasjon (skoleeier)

```
dn: dc=Skotthyll,dc=kommune,dc=no
objectClass: eduOrg
objectClass: norEduOrg
objectClass: organization
objectClass: top
dc: Skotthyll kommune
eduOrgLegalName: Skotthyll kommune
norEduOrgNIN: NO179530458
norEduOrgSchemaVersion: 1.5.1
o: Skotthyll kommune
mail: info@skotthyll.kommune.no
telephoneNumber: +47 73557900
postalAddress: Postboks 340$NO-7640 Skotthyll
```

Organisasjonsenhet (skole)

```
dn: ou=Hylla skole,cn=organization,dc=Skotthyll,dc=kommune,dc=no
objectClass: norEduOrgUnit
objectClass: organizationalUnit
objectClass: top
norEduOrgUnitUniqueIdentifier: NO179530458
ou: Hylla skole
mail: hylla@skotthyll.kommune.no
telephoneNumber: +47 73557900
postalAddress: Postboks 340$NO-7640 Skotthyll
postalAddress: Nordveien 5$NO-7640 Skotthyll
```

Appendiks 2 – Registrering av Grep-koder i eduPersonEntitlement

Tjenester har økende behov for informasjon om brukernes årstrinn, fag o.l. På grunn av dette skal Grep-koder registreres for elever i grunnopplæringen. I Feide er det valgt å bruke feltet `eduPersonEntitlement` for Grep-koder.

Lærere/ansatte

Det er ikke obligatorisk å registrere Grep-koder for lærere eller andre ansatte, kun for elever. Lærere kan registreres med Grep-koder for fag de underviser i og grupperinger (trinn, utdanningsprogram, programområde og fag) de er ansvarlige for. Andre ansatte skal ikke ha Grep-koder registrert.

Elever i 1.-10.trinn

For elever i grunnskolen (1.-10. trinn) skal kun trinn registreres. Denne tabellen viser hvilke verdier trinn kan ha i grunnskolen:

Trinn	Grep-kode
1. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn1
2. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn2
3. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn3
4. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn4
5. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn5
6. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn6
7. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn7

8. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn8
9. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn9
10. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/aarstrinn10

Elever i videregående skole

For elever i videregående skole skal følgende registreres:

- trinn
- utdanningsprogram
- programområde

Denne tabellen viser hvilke verdier trinn kan ha i videregående skole:

Trinn	Grep-kode
1. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/vg1
2. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/vg2
3. trinn	urn:mace:feide.no:go:grep:http://psi.udir.no/laereplan/aarstrinn/vg3

For utdanningsprogram og programområde er antallet Grep-koder både stort og dynamisk, og det vil være u hensiktsmessig å liste det opp i tabeller. Vi anbefaler derfor at disse Grep-kodene hentes fra de skoleadministrative systemene og prefikses med "urn:mace:feide.no:go:grep:".

Grep-koder registrert i skoleadministrative system

Flere skoleadministrative systemer har Grep-kodeverket implementert i sine løsninger. Samtidig inneholder disse systemene også andre koder som

gir informasjon om årstrinn og fag o.l. Vær oppmerksom på at Grep-kodene som registreres i Feide-katalogen må være den unike identifikatoren til trinnet, utdanningsprogrammet, programområdet eller faget.

Under er noen eksempler som viser forskjellene mellom Grep-koder og andre koder.

Et eksempel på trinn:

- *8. årstrinn* er et navn (på kortform) og skal ikke brukes om identifikator i Feide.
- <http://psi.udir.no/laereplan/aarstrinn/aarstrinn8> er årstrinnets identifikator og skal benyttes i Feide.

Et eksempel på utdanningsprogram:

- *ST* er koden til *studiespesialisering*, men dette er ikke identifikatoren.
- <http://psi.udir.no/ontologi/utdanningsprogram/studiespesialisering> er programmets identifikator og skal benyttes i Feide.

Et eksempel på programområde:

- *STREA2*— er områdets kode.
- `uuid:81d3b889-16c8-4b0a-81af-d0832fbc219` er områdets identifikator i kodeverket og skal benyttes i Feide.

Et eksempel på et fag:

- *REA3005* er koden til faget Fysikk 2.
- `uuid:7a0fa1f7-f6f9-4a5e-93a4-78f59ad57166` er fagets identifikator i kodeverket og skal benyttes i Feide.

Appendiks 3 – Registrering av gruppeinformasjon i eduPersonEntitlement

Tjenester har økende behov for informasjon om brukernes basisgrupper/klasser, undervisningsgrupper og andre grupper. På grunn av dette skal elever og læreres gruppeinformasjon registreres. I Feide er det valgt å bruke feltet `eduPersonEntitlement` for gruppeinformasjon.

Alle som er tilknyttet gruppen skal ha informasjonen registrert

Alle personer som er tilknyttet en gruppe skal ha informasjonen registrert på sitt personobjekt. Dette vil som regel være elever og lærere, men kan også være andre personer som har en formell knytning til det daglige arbeidet i gruppen.

Gruppetyper

Det er definert tre gruppetyper som kan uttrykkes:

- Basisgruppe/klasse
- Undervisningsgruppe
- Andre grupper

Basisgruppe/klasse og undervisningsgruppe er obligatoriske å registrere for en person, mens andre grupperinger kan registreres.

Informasjonselementer om gruppen og personens relasjon til gruppen

Hver gruppetilhørighet som registreres for en person inneholder 8 informasjonselementer:

Informasjonselement	Beskrivelse
Gruppetype	Viser hvilken type gruppe dette er. Gyldige verdier er 'b', 'u' og 'a' for henholdsvis basisgruppe/klasse, undervisningsgruppe og annen gruppe.
Grepkode	For undervisningsgrupper er det fagkoden til faget undervisningsgruppen tilhører fra Grepkodeverket. For basisgrupper og andre grupper skal det være en tom verdi.

Organisasjonsnummer/ bedriftsnummer	Organisasjonsnummer/bedriftsnummer til skolen/skoleeieren gruppen tilhører. For de aller fleste grupper vil den være knyttet til skolen, men det kan være grupper som er knyttet direkte til skoleeieren.
Gruppeidentifikator	En identifikator på gruppen der navnestandard er definert ved skolen/skoleeieren. Skal være unik innenfor skolen/skoleeieren gruppen tilhører.
Starttidspunkt	Starttidspunkt gruppen blir aktiv/gyldig. ISO 8601 extended format for date, YYYY-MM-DD
Sluttidspunkt	Sluttidspunkt når gruppen ikke lenger er aktiv/gyldig. ISO 8601 extended format for date, YYYY-MM-DD
Rolle	Personens rolle i gruppen. Gyldige verdier er de samme som i <code>eduPersonAffiliation</code> . En person skal bare et innslag for rolle i gruppen, for eksempel <code>faculty</code> , og ikke hele hierarkiet som i <code>eduPersonAffiliation</code> .
Beskrivende gruppenavn	Gruppens menneskelesbare navn som kan vises frem i tjenester

Formatering av gruppeinformasjon

Hver gruppetilhørighet registreres som en egen linje i `eduPersonEntitlement`.

Linjen skal starte med prefikset 'urn:mace:feide.no:go:group:' etterfulgt av hver av informasjonselementene i samme rekkefølge som tabellen over. Hvert informasjonselement skilles fra hverandre med et kolon, ':'.
'

For å kunne overføre verdiene fra en system til et annet definerer RFC 2141 og RFC 3986 hvilke verdier som er gyldige, hvilke som benyttes direkte og hvilke som må prosent-kodes. URNer er begrenset til ASCII så de fleste spesialtegn og særnorske tegn må prosent-kodes i overføringen. Man benytter UTF-8 oversetting først og så til US-ASCII (RFC 2141 2. Syntax). Dette gjøres ved å oversette disse tegnene til %<hex><hex>. For eksempel vil det særnorske tegnet 'å' oversettes fra UTF-8 til to oktetter som så kodes og blir %C3%A5.

<Space> er et spesialtilfelle. Mange funksjoner for prosent-koding koder dette om til + som bryter med RFC 3986. Det korrekte for URNer er %20. Vertsorganisasjoner bør påse at dette blir riktig, mens tjenesteleverandører bør ta høyde for begge formateringsene av <space>.

For gruppeinformasjon benyttes kolon (:) som separator mellom informasjonselementer. Om dette tegnet benyttes inne i informasjonselementene, for eksempel i det beskrivende navnet eller gruppeidentifikatoren, må dette kodes, som %3A.

Case-sensitivitet

Informasjonselementene for gruppeinformasjonen skal behandles **case-insensitiv**, etter RFC 2141 åpning for funksjonell sammenligning av verdiene.

Eksempler på gruppeinformasjon i eduPersonEntitlement

Elev i basisgruppe/klasse 6A ved Berg skole (Trondheim kommune)

Gruppetype: b

Grepkode: <tom verdi>

Organisasjonsnummer: NO975278964

Gruppeidentifikator: 6A

Rolle: Elev – 'student' i Feide.

Starttidspunkt: 1. aug 2014

Sluttidspunkt: 15. juni 2015

Beskrivende navn: Klasse 6A

eduPersonEntitlement:

urn:mace:feide.no:go:group:b::NO975278964:6A:2014-08-01:2015-06-15:student:Klasse%206A

Lærer i undervisningsgruppe 2kja ved Tiller vgs

Gruppetype: u

Grepkode: REA3012

Organisasjonsnummer: NO974558386

Gruppeidentifikator: 2kja – Her brukes små bokstaver, men verdien er case-insensitive

Rolle: Lærer – 'faculty' i Feide

Starttidspunkt: 1. aug 2014

Sluttidspunkt: 15. juni 2015

Beskrivende navn: Kjemi 2A

eduPersonEntitlement:

urn:mace:feide.no:go:group:u:REA3012:NO974558386:3kja:2014-08-01:2015-06-15:faculty:Kjemi%202A

Elev i undervisningsgruppe Norsk hovedmål VG3 ved Tiller vgs

Gruppetype: u

Grepkode: NOR1211

Organisasjonsnummer: NO974558386

Gruppeidentifikator: 3aaa/3nh

Rolle: Elev

Starttidspunkt: 1. aug 2014

Sluttidspunkt: 15. juni 2015

Beskrivende navn: Norsk hovedmål VG3

eduPersonEntitlement:

urn:mace:feide.no:go:group:u:NOR1211:NO974558386:3aaa%2F3nh:2014-08-01:2015-06-15:student:Norsk%20hovedm%3%A51%20VG3

Elev i labgruppe 3 Fysikk VG3 ved Tiller vgs

Gruppetype: a – andre grupper

Grepkode: <tom verdi>

Organisasjonsnummer: NO974558386

Gruppeidentifikator: 3fysa/lb3

Rolle: Elev

Starttidspunkt: 1. aug 2014

Sluttidspunkt: 31. des 2014

Beskrivende navn: Labgruppe 3 Fysikk VG3

eduPersonEntitlement:

urn:mace:feide.no:go:group:a::NO974558386:3fysa%2F1b3:2014-08-01:2014-12-31:student:Labgruppe%203%20Fysikk%20VG3