



IT- og Telestyrelsen

Ministeriet for Videnskab
Teknologi og Udvikling

Anbefaling til Kerneattributter for Bruger

Kolofon:

OIO Referencemodel for tværgående brugerstyring

Denne anbefaling kan frit anvendes af alle. Citeres fra anbefalingen i andre publikationer til offentligheden skal angives korrekt kildehenvisning.

Forslag til anbefalinger for tværgående brugerstyring udarbejdes af IT- og Telestyrelsen, IT-strategisk kontor, som sekretariat for OIO It-Arkitekturkomiteen.

Kontaktperson:

It-Arkitekt Søren Peter Nielsen, email: spn@itst.dk

Telefon 25 67 07 83 (direkte)

It-Arkitekt Anders Dalsgaard, email: ada@itst.dk

Telefon 25 65 32 08 (direkte)

Ministeriet for Videnskab, Teknologi og Udvikling

IT- og Telestyrelsen

IT-strategisk kontor

Holsteinsgade 63

DK-2100 København Ø

Telf. +45 35 45 00 00

Fax. +45 35 45 00 10

<http://www.itst.dk>

itst@itst.dk

Indholdsfortegnelse

1	Indledning.....	4
1.1	Opsummering.....	4
1.2	Formål.....	4
1.3	Overblik / Baggrund for anbefaling.....	4
1.4	Anvendelsesområde.....	4
2	Anbefaling.....	5
3	Kerneattributter for bruger.....	6
3.1	Baggrund for de foreslåede attributter.....	6
4	Appendiks A.....	8
5	Appendiks B - Yderligere information.....	11

1 Indledning

Ved lagring af brugerattributter i kataloger som f.eks. et LDAP Directory samt ved overdragelse af brugerattributter fra et it-system til et andet, er der behov for at lagre og overføre attributter via anvendelse af standardattributter. Dette sikrer en fælles begrebsforståelse og simplificerer integrationen på tværs af systemer både lokalt og globalt. Ved anvendelse af internationale standarder vil man endvidere kunne udveksle attributter på tværs af landegrænser.

1.1 Opsummering

Der anbefales anvendelse af

- En navngivning, der følger LDAP schemaet inetOrgPerson, indenfor digital forvaltning med hensyn til registrering af brugerattributter.
- Et minimumssæt af attributter til overførsel af information om en it-bruger i forbindelse med tværgående autenticitetssikring (på tværs af organisatoriske skel, domæner etc.).

1.2 Formål

Formålet med denne anbefaling er at sikre en konsistent og præcis navngivning af brugerattributter. Endvidere defineres en bruger ud fra et minimum sæt af attributter. Dette skal sikre, at man i forbindelse med tværgående brugerstyring har et fælles sæt af attributter til at matche forskellige konti for den samme bruger eller som basis for oprettelse af en konto for brugeren i en ekstern organisation.

Definitionen af en bruger kan bl.a. anvendes i SAML 2.0 konvolutten, der anvendes ved autenticitetssikring af brugere.

1.3 Overblik / Baggrund for anbefaling

Hvis man anvender en fælles begrebsmodel for brugerattributter bliver samkøring af brugerkataloger samt overlevering af attributter mellem it-systemer simplificeret. Endvidere danner dette udgangspunkt for en fælles autenticitetssikringservice, der kan benyttes og genbruges af nye services.

1.4 Anvendelsesområde

Ved oprettelse af brugere i brugerkataloger kan denne anbefaling benyttes som udgangspunkt for en fælles begrebsmodel. Listen af attributter er ikke udtømmende, men skal betragtes som en delmængde, der som minimum skal med for at beskrive en bruger. Det er op til den enkelte ejer af et brugerkatalog at definere et udtømmende sæt, der opfylder de krav, der lokalt er til attributter, der skal kobles på en bruger.

Specielt ved anvendelse af regelbaseret adgangskontrol vil der opstå behov for en differentiering af attributter fra katalog til katalog i forbindelse med behov for yderligere oplysninger om brugerne.

2 Anbefaling

I forbindelse med lagring af brugerattributter i lokale brugerkataloger anbefales det, at der tages udgangspunkt i LDAP¹ objektclassen 'inetOrgPerson'². Dette er et objekt, der indeholder LDAP attributter til beskrivelse af en person, der hører til en organisation. 'inetOrgPerson' er en veldokumenteret objektclass, der understøttes af de fleste leverandører af katalogservices og anvendes internationalt.

'Hvis der er yderligere behov for attributter, som ikke er dækket af 'inetOrgPerson', anbefales det, at man som udgangspunkt anvender internationale LDAP attributter fra andre LDAP schemaer i størst mulig udstrækning, givet de semantisk og værdimæssigt kan rumme den ønskede information.' Hvis der er behov for egne attributter, skal attributter fra OIO InfoStructureBase'n i videst muligt omfang bruges.

I forbindelse med overførsel af brugerattributter fra et it-system til et andet, ved f.eks. autenticitetssikring og anvendelse af SAML 2.0 protokollen, anbefales det, at man bibeholder navngivningen af attributter fra LDAP, således at entydigheden overføres til denne protokol og dermed også til modtagersystemet.

Se Appendix A for en nærmere beskrivelse af 'inetOrgPerson'.

Såfremt der eksisterer sektorspecifikke schemaer, der er nedarvet efter inetOrgPerson, kan disse også anvendes.

¹ LDAP, version 3.0.

² InetOrgPerson er defineret i RFC2798. Se <http://www.faqs.org/rfcs/rfc2798.html> for en komplet inetOrgPerson LDAP klasse definition.

3 Kerneattributter for bruger

Kerneattributter dækker over de attributter, man som udgangspunkt skal have med i sin brugerprofil for med rimelig sikkerhed at kunne identificere en bruger. De kan betragtes som kernen i beskrivelse af en bruger. Attributnavnene er taget fra LDAP-schemaet 'inetOrgPerson', hvor det har været muligt.

Basisattributter (fra inetOrgPerson):

- sn Efternavn
- cn Navn – det som personen omtaler sig som.
- uid Brugerid
- mail Mailadresse (e-post adresse)

Nye attributter, som ikke er defineret i eksisterende LDAP, ver. 3.0 objektklasser, men som det anbefales at anvende ved overførsel af information om en bruger, der skal kunne identificeres:

- uniqueAccountKey³ Id-nøgle til matchning og synkronisering af brugerinformation på tværs af systemer.
- cvrNumberIdentifier⁴ CVR nummer. Angiver brugerens ansættelsesmæssige tilknytningsforhold⁵.

'uniqueAccountKey' og 'cvrNumberIdentifier' er ikke obligatoriske. 'uniqueAccountKey' skal kun angives i de tilfælde, hvor man har valgt at implementere en unik XRI-nøgle i sit system. Dokumentet 'Anbefaling til unik Id-nøgle' anbefaler, hvorledes den enkelte organisation kan oprette en id-nøgle, der med høj sandsynlighed er unik på tværs af organisationer.

BEMÆRK: Denne anbefaling retter sig kun mod situationer, hvor det er nødvendigt at kende den specifikke bruger. I situationer hvor det fx er aftalt, at det er nok at kende brugerens rolle og tilhørsforhold, er det ikke relevant at overføre de anbefalede kerneattributter.

3.1 Baggrund for de foreslåede attributter

Formålet med anbefalingen om kerneattributter er at kunne sikre, at man i forbindelse med tværgående brugerstyring har et fælles sæt af attributter til at matche forskellige konti for den samme bruger eller som basis for oprettelse af en konto for brugeren i en ekstern organisation.

De anbefalede attributter består af kerneattributter om en bruger. En delmængde af disse er normalt angivet i forskellige brugerkonti. Med det foreslåede udvalg af attributter er der således forskellige muligheder for at matche forskellige brugerkonti på med krav om, at mere end én attribut skal være fælles.

³ LDAP, version 3.0: SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256}

⁴ LDAP, version 3.0: SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{8}

⁵ Bemærk, at dokumentet 'Anbefaling til unik Id-nøgle' også anvender CVR-nummer, men dette ikke nødvendigvis er det samme CVR nummer som her. I den anbefalede id-nøgle anvendes et CVR-nummer, som hører til den institution, der oprettede brugeren i brugerkataloget. Her er der tale om det nuværende tilhørsforhold, som kan være ændret f.eks. efter en opgaveflytning mellem myndigheder.

- **sn** Efternavn – Er obligatorisk felt i LDAP objektklassen 'inetOrgPerson'. Det er således en forudsætning for, at en ekstern organisation kan oprette brugeren i sit eget LDAP brugerkatalog
- **cn** Navn – det som personen omtaler sig som. Er obligatorisk i LDAP objektklassen inetOrgPerson. Derudover giver det også mulighed for brugervenlig repræsentation af brugeren i de løsninger vedkommende anvender.
- **uid** Bruger-id tillader mapping i mellem systemer hvor brugeren er registreret med samme brugerid.
- **mail** Mailadresse giver umiddelbart de løsninger, som brugeren anvender, mulighed for at sende e-mail til vedkommende.
- **uniqueAccountKey** Id-nøgle giver mulighed for at matche og synkronisere brugerkonti, der findes i forskellige systemer/organisationer. Id-nøglen knytter sig til den kontekst, som brugeren optræder i, og kan ikke anvendes til matching af information om brugeren uden for denne kontekst. Eksempelvis vil det ikke være samme uniqueAccountKey, der anvendes, når brugeren er privatperson, som når brugeren optræder som ansat i en organisation
- **cvrNumberIdentifier** CVR nummer giver mulighed for at identificere brugerens tilknytningsforhold. Dette kan f.eks. anvendes i situationer, hvor der normalt er krav om, at eksterne brugere skal identificeres, men der er en speciel aftale med organisation om, at man blot behøver sikkerhed for brugerens tilknytning til organisationen. En anden anvendelse er til simpel autorisation, hvor alle brugere med tilknytning til et givet CVR nummer må tilgå en given service.

4 Appendiks A

inetOrgPerson er en generel objektklasse, der indeholder attributter til beskrivelse af en person. Objektclassen er designet til protokoller baseret på LDAP (RFC2251) samt X.500 afledte protokoller.

inetOrgPerson indgår i følgende LDAP-hierarki:

top (RFC2256) ->

person (RFC2256) ->

organizationalPerson (RFC2256) ->

inetOrgPerson (RFC2798)

inetOrgPerson er beskrevet ved følgende attributter:

Attribut	Påkrævet/Valgfrit	Schema
ObjectClass	P	top
sn	P	person
cn	P	person
description	V	person
seeAlso	V	person
telephoneNumber	V	person
userPassword	V	person
title	V	organizationalPerson
ou	V	organizationalPerson
preferredDeliveryMethod	V	organizationalPerson
st	V	organizationalPerson
telexNumber	V	organizationalPerson
l	V	organizationalPerson
physicalDeliveryOfficeName	V	organizationalPerson
postalCode	V	organizationalPerson
internationalISDNNumber	V	organizationalPerson
x121Address	V	organizationalPerson

registeredAddress	V	organizationalPerson
street	V	organizationalPerson
postalAddress	V	organizationalPerson
facsimileTelephoneNumber	V	organizationalPerson
teletexTerminalIdentifier	V	organizationalPerson
postOfficeBox	V	organizationalPerson
destinationIndicator	V	organizationalPerson
userCertificate	V	inetOrgPerson
uid	V	inetOrgPerson
homePostalAddress	V	inetOrgPerson
employeeType	V	inetOrgPerson
preferredLanguage	V	inetOrgPerson
mail	V	inetOrgPerson
homePhone	V	inetOrgPerson
roomNumber	V	inetOrgPerson
x500UniqueIdentifier	V	inetOrgPerson
employeeNumber	V	inetOrgPerson
photo	V	inetOrgPerson
businessCategory	V	inetOrgPerson
pager	V	inetOrgPerson
o	V	inetOrgPerson
jpegPhoto	V	inetOrgPerson
secretary	V	inetOrgPerson
audio	V	inetOrgPerson
userPKCS12	V	inetOrgPerson
displayName	V	inetOrgPerson
mobile	V	inetOrgPerson
labeledURI	V	inetOrgPerson

carLicense	V	inetOrgPerson
givenName	V	inetOrgPerson
manager	V	inetOrgPerson
userSMIMECertificate	V	inetOrgPerson
initials	V	inetOrgPerson
departmentNumber	V	inetOrgPerson

Ved behov for yderligere attributter anbefales det at nedarve fra inetOrgPerson.

Hvis man ønsker at gemme oplysninger om organisationen i sit katalog og evt. anvende disse oplysninger til at lave et hierarki, anbefales det at benytte objektklasserne 'organization' og evt. 'organizationalUnit' (begge defineret i RFC2256).

5 Appendiks B - Yderligere information

Dette fællesoffentlige arbejde i forbindelse med tværgående brugerstyring er beskrevet på

<http://www.oio.dk/arkitektur/brugerstyring>

Information om nogle af de aktiviteter inden for it-sikkerhed, som Videnskabsministeriet varetager findes på

<http://www.oio.dk/sikkerhed>

Information vedrørende arbejdet med at implementere en fælles standard for styring af it-sikkerhedsprocesser i staten findes på

<http://www.oio.dk/itsikkerhed/isis>