Nets DanID A/S
Lautrupbjerg 10
DK – 2750 Ballerup
T +45 87 42 45 00
F +45 70 20 66 29
www.nets.dk

CVR-nr. 30808460

Specifikationsdokument for LDAP API

Indholdsfortegnelse

Versionsfortegnelse

8. februar 2010	Version 1.0	TechniWrite
22. november 2010	Version 1.1	MTV
20. januar 2011	Version 1.2	MTV
1. februar 2011	Version 1.3	MTV
23. februar 2011	Version 1.4	CR/SEF
1. marts 2012	Version 1.5	PKRIS
3. juni 2014	Version 1.6	PHJER
5. juni 2014	Version 1.7	PHJER
19. februar 2015	Version 1.8	KMAIB
4. august 2016	Version 1.9	KMAIB

1 Formål og målgruppe

Dette dokument er en del af NemID tjenesteudbyderpakken.

Formålet med dokumentet er at give en generel introduktion til LDAP og beskrive, hvordan data er organiseret i NemIDs LDAP-servere. Dokumentet er relevant for tjenesteudbyderen, hvis Nets DanIDs Sikkerhedspakke ikke indeholder den ønskede funktionalitet på dette område.

Dokumentet henvender sig til de personer hos tjeneste-udbyderen, der er ansvarlige for implementeringen af NemID.

2 LDAP-databaser

En LDAP-database er en objektorienteret måde at opbevare data på. I modsætning til en traditionel database indeholder den ikke rækker og kolonner. I stedet er data organiseret som objekter med tilknyttede attributter i en træstruktur.

LDAP-databaser benyttes traditionelt til opbevaring af f.eks. brugerkonti på Unix-systemer eller information fra en certifikatudsteder. De lagrede informationer kan f.eks. være certifikater eller spærrelister for certifikater.

Hvert objekt i en LDAP-database har et *distinguished name* (DN), som identificerer objektet entydigt. DN fungerer som en repræsentation af en træstruktur. Objekterne i LDAP kan have underobjekter, og hvert objekt kan på den måde betragtes som et blad eller en indre knude i et træ af objekter.

Et objekt har tilknyttet én eller flere objektklasser, som indikerer, hvilke attributter der er tilknyttet objektet. En attribut kan enten være obligatorisk eller valgfri.

Som en del af NemID-infrastrukturen stiller Nets DanID to offentligt tilgængelige LDAP-databaser til rådighed:

- **Certifikat-LDAP** - Med knuder, der repræsenterer offentliggjorte slutbrugercertifikater
- **Spærreliste-LDAP -** Med knuder, der repræsenterer CA'er (Certificate Authority) og spærrelister for certifikater.

3 Eksempel på person med NemID med certifikat

En borger i Danmark, som har NemID med tilknyttet certifikat, vil også være at finde i NemIDs certifikat-LDAP, hvis personen har valgt at offentliggøre sit certifikat i adressebogen.

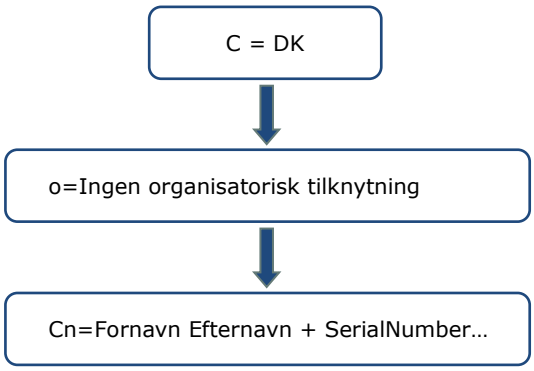
Personens DN vil da kunne se ud som følger:

```
cn=Fornavn Efternavn+SerialNumber=PID:9208-2002-2-
123456789012, o=Ingen organisatorisk tilknytning, c=DK
```

Ud af dette kan man læse:

- personens navn i feltet ***cn*** (common name)
- personens tildelte PID i feltet ***serialNumber***
- personens organisatoriske tilknytning (ingen) i feltet ***o*** (organization)
- personens land i feltet ***c*** (country).

Dette svarer til følgende træstruktur:



Bemærk, at der endvidere er mulighed for at angive ekstra information om personen i feltet **ou** (organizationalUnit), der indsættes under o-knuden. I så fald ville brugeren have følgende DN:

```
cn=Fornavn Efternavn (Ung under 18)
+SerialNumber=PID:9208-2002-2-123456789012, ou=Ung
mellem 15 og 18,o=Ingen organisatorisk tilknytning, c=DK
```

3.1 Attributter for person

For en person findes der i Certifikat-LDAP følgende ekstra attributter:

Attributnavn	Indhold
sn	Brugerens efternavn
mail	Brugerens e-mailadresse som er indeholdt i certifikatet. Hvis brugeren har valgt ikke at inkludere e-mail i certifikatet, vil denne attribut ikke være defineret
userCertificate	Brugerens certifikat. Kun brugerens nyeste certifikat er tilgængeligt.

4 Eksempel på medarbejder med NemID medarbejdersignatur

En medarbejder i en virksomhed i Danmark, som har NemID medarbejdersignatur, findes i NemIDs certifikat-LDAP, hvis medarbejderen har valgt at offentliggøre sit certifikat i adressebogen.

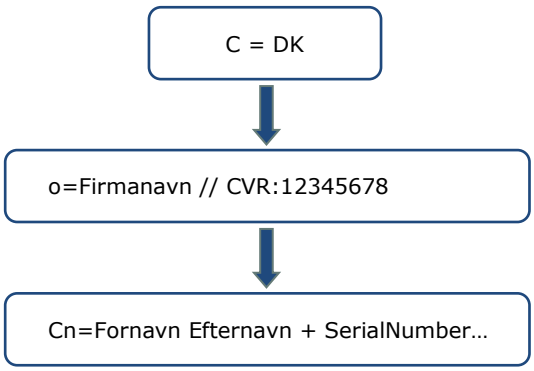
Medarbejderens DN vil da kunne se ud som følger:

```
cn=Fornavn Efternavn+serialNumber=CVR:12345678-
RID:123456789012, o=Firmanavn // CVR:12345678, c=DK
```

Ud fra DN kan man læse:

- medarbejderens navn i feltet ***cn*** (common name)
- medarbejderens tildelte serienummer (som indeholder CVR-nummer for hans virksomhed samt et løbenummer) i feltet ***serialNumber***
- medarbejderens organisatoriske tilknytning i feltet ***o*** (organization)
- medarbejderens land i feltet ***c*** (country).

Dette svarer til nedenstående træstruktur:



Bemærk, at der også er mulighed for at angive hvilken organisatorisk enhed, medarbejderen er tilknyttet. Dette sker vha. feltet *ou* (organizationalUnit), der indsættes under *o*-knuden, således at medarbejderen kunne have følgende DN:

```
cn=Fornavn Efternavn+serialNumber=CVR:12345678-
RID:123456789012, OU=Testafdelingen, o=Firmanavn
// CVR:12345678, c=DK
```

Af mulige attributter er der for en medarbejder de samme som for en borger.

5 Eksempel på Virksomhedssignatur

LDAP-egenskaberne for Virksomhedssignatur er de samme som for NemID medarbejdersignatur. Eneste forskel er at *serialNumber* indeholder UID i stedet for RID som i en medarbejdersignatur.

6 Eksempel: NemID-udstedende CA

NemID fungerer ved hjælp af en rod-CA, der udelukkende udsteder certifikater til en række udstedende CA'er. Hver af disse CA'er udsteder et (stort) antal certifikater, hvorefter den overgår til en inaktiv tilstand, hvor den ikke længere udsteder certifikater, men udelukkende administrerer (f.eks. hvad angår revokering) de allerede udstedte certifikater.

Et NemID-certifikat er altså altid udstedt af én udstedende CA, aldrig af rod-CA'en. Både rod-CA'en og de udstedende CA'er er repræsenteret som knuder i Spærreliste-LDAP.

Rod-CA'en har følgende DN:

```
cn=TRUST2408 OCES Primary CA, o=TRUST2408, c=DK
```

De udstedende CA'er har DN'er på følgende form:

```
cn=TRUST2408 OCES CA n, o=TRUST2408, c=DK
```

6.1 Attributter for CA

CA-knuderne har b.la. følgende attributter:

Attributnavn	Indhold
caCertificate	CA'ens certifikat. For rod CA'en er certifikatet selvsigneret, for en udstedende CA er det signeret af rod-CA'en
certificateRevocationList	Den fulde spærreliste for de certifikater, der er udstedt af denne CA. For rod-CA'en er disse certifikater for udstedende CA'er, for en udstedende CA er det certifikater for borgere

7 Partielle spærrelister

Under hver knude, der repræsenterer en udstedende CA, findes en række knuder, der hver indeholder en del af den fulde spærreliste. Disse kaldes for *partielle spærrelister*. En partiel spærreliste indeholder information om op til 750 certifikater, men er til gengæld hurtigere og mindre pladskrævende at hente end den fulde spærreliste for en CA.

Knuderne har DN på formen:

```
cn=CRL1,cn=TRUST2408 OCES CA n, o=TRUST2408, c=DK
```

Selve spærrelisten opbevares ligesom den fulde spærreliste i attributten *certificateRevocationList* under knuden.

For at finde den partielle spærreliste, et givent borgercertifikat vil stå opført på, hvis certifikatet er spærret, skal man først bruge det DN på den udstedende CA, der står i certifikatet som issuerDN, til at lokalisere den udstedende CA i LDAP.

Når man har lokaliseret denne, kan man bruge X509 extension point *crlDistributionPoint* i certifikatet til at finde DN for den underknude under den udstedende CA, der indeholder den partielle spærreliste – og hermed kan man udføre en søgning, der finder den rigtige knude.

Hvis man udelukkende har behov for at undersøge, om ét givet certifikat for en borger er spærret, vil det som regel være mere hensigtsmæssigt at benytte OCSP-protokollen. Læse mere i dokumentet **Specifikationsdokument for OCSP**, der er en del af NemID tjenesteudbyderpakken.

8 Søgninger

Når man skal lave en søgning, er der et antal nødvendige parametre:

1. Hvilken LDAP-server skal der søges i:
    a. NemIDs certifikat-LDAP findes på *crtdir.certifikat.dk*.
    b. Spærreliste-LDAP findes på *crldir.certifikat.dk*.

    I begge tilfælde skal der oprettes en TCP-forbindelse til port 389.
2. Hvilken søgebase, søgningen skal starte i, dvs., hvilken knude i træet der skal fungere som rodknude for søgningen.
3. Hvor dybt man vil søge: 1) i søgebase-knuden, 2) ét niveau ned eller 3) i hele undertræet for søgebase-knuden.
4. Hvilket søgefilter, der skal matches mod.
5. Hvilke attributter, der ønskes returneret for matchende knuder.
6. Endvidere skal det angives, om man ønsker at logge på for at udføre søgningen. Kun anonym søgning i NemID LDAP-databaserne understøttes. Det er endvidere ikke muligt at foretage wildcard-søgninger via LDAP-protokollen.

Ovenstående parametre skal angives, uanset hvilken LDAP-klient der benyttes, men mekanismen til at angive dem kan selvfølgelig variere.

8.1 Søgning efter en person med NemID med certifikat

Hvis du vil finde de certifikater, der tilhører en person med navnet Jens Hansen, skal du angive følgende søgeparametre:

Søgebase	o=Ingen organisatorisk tilknytning, c=DK
Søgedybde	Sub
Søgefilter	cn=Jens Hansen
Attribut	userCertificate

I dette tilfælde er en personens navn dog et dårligt filter, da der er mange personer, der hedder Jens Hansen. I stedet kan du bruge personens email-adresse som filter. Hvis den Jens Hansen, der ledes efter, har email-adressen **jens@hansen.dk**, kan det gøres med følgende søgeparametre:

Søgebase	o=Ingen organisatorisk tilknytning, c=DK
Søgedybde	Sub
Søgefilter	mail=jens@hansen.dk
Attribut	userCertificate

Der returneres et begrænset antal søgeresultater. Grænsen er fem fra OCES II.

8.2 Søgning efter spærreliste for en udstedende CA

For at hente den fulde spærreliste for f.eks. udstedende CA nummer I, kan man lave en søgning med følgende parametre:

Søgebase	o=TRUST2408, c=DK
Søgedybde	One
Søgefilter	cn=TRUST2408 OCES CA I, o=TRUST2408, c=DK
Attribut	certificateRevocationList

Herved vil den fulde spærreliste returneres.

9 LDAP-klienter

Der findes mange forskellige klienter til LDAP. Ofte vil mailklienter have indbygget LDAP i deres adressebogsfunktionalitet – det gælder f.eks. mailklienter fra Mozilla og Microsoft.

På *http://www.openldap.org* finder du LDAP-klienten ***ldapsearch***, som er et kommandolinjeværktøj.

http://www.ldapadministrator.com har en GUI-baseret LDAP browser-klient.

9.1 Eksempel på søgning med ldapsearch

De tre ovennævnte eksempelsøgninger kunne foretages med nedenstående parametre til **ldapsearch**:

> ldapsearch -x -h crtdir.certifikat.dk -b "o=Ingen organisatorisk tilknytning, c=DK" "cn=Jens Hansen" userCertificate

> ldapsearch -x -h crtdir.certifikat.dk -b "o=Ingen organisatorisk tilknytning, c=DK" "mail=jens@hansen.dk" userCertificate

> ldapsearch -x -h crldir.certifikat.dk -b "o=TRUST2408, c=DK" –s one "cn=TRUST2408 OCES CA I" certificateRevocationList

Det er også muligt at fremsøge en CA's certifikat med nedenstående parametre til **ldapsearch**:

> ldapsearch -x -h crldir.certifikat.dk -s one -b 'o=TRUST2408,c=DK' '(cn=TRUST2408 OCES CA I)' cACertificate

Med tilføjelse af AIA i certifikater er det dog muligt direkte at finde den udstedende CA's certifikat ved at følge den angivne HTTP reference i brugerens certifikat.

9.2 Eksempel på søgning med Internet Explorer

Udover adressebogens GUI-søgning understøtter Internet Explorer også LDAP-søgninger via URL-enkodning af søgestrengen. Dette er beskrevet nærmere i RFC 2255 (http://www.ietf.org/rfc/rfc2255.txt).
Resultaterne vises i adressebogen med henblik på sikker e-mail.