

Dokumentation

Nets Rettighedsstyring (Attributtjeneste)

Indholdsfortegnelse

1	Introduktion	4
1.1	Hvad er Attributtjeneste?.....	4
1.2	Et eksempel på brugen af attributter	4
1.3	Hvem laver attributter?	4
1.4	Hvem kan bruge attributter?	5
1.5	Hvem skal bruge attributterne?	5
1.6	Forespørgsel på attribut	5
1.7	Validering af attributindhold	5
2	Udveksling af attributter	6
3	Oprette/nedlægge attributter	6
3.1	Hvem kan oprette/nedlægge attributter?	6
3.2	Bestilling af nye attributter	6
3.3	Nedlægning af eksisterende attributter.....	7
4	Attribut webservice	7
4.1	Operationer og input parametre	7
4.1.1	publishAttribute	7
4.1.2	endPublishAttribute	7
4.1.3	getAttribute.....	7
4.1.4	getAttributes	8
4.1.5	verifyAttribute	8
4.2	WSDL.....	Error! Bookmark not defined.
4.3	Returværdier	10
5	Kontaktinformation	10

Figurliste

Figur 1: Attributopslag	6
-------------------------------	---

Versionsfortegnelse

19-12-2008	Første udkast	KNS
11-11-2011	Opdateringer	PKRIS
02-05-2012	Issuer og WSDL for test og prod tilføjet	KNS
11-11-2014	WSDL og Service endpoint samt kontaktinfo	KMAIB

Bilagsfortegnelse

Bilag 1	Bestillingsformular
---------	---------------------

1 Introduktion

1.1 *Hvad er Attributtjeneste?*

Attributtjenesten – også kaldet Nets Rettighedsstyring - gør det muligt for virksomheder at tildele attributter (roller eller rettigheder) til ansatte med medarbejdercertifikater.

Tildelingen af attributter sker i administratorens selvbetjeningssystem – det system, hvor oprettelse og administration af medarbejdersignaturer finder sted¹. Rent praktisk foregår det ved, at administratoren fremsøger medarbejderen og tilknytter de relevante attributter til medarbejderens medarbejdercertifikat. Tilknytningen finder sted i et særligt område i selvbetjeningssystemet.

Det er Tjenesteudbyderen der definerer:

- hvilke attributter, der skal være tilgængelige, og
- hvilke virksomheder (CVR-numre) der skal kunne se og vælge attributten i selvbetjeningssystemet.

Det er gratis for virksomhederne at tildele attributter og anvende dem. Tjenesteudbyderen betaler for etablering og drift af Attributtjenesten.

1.2 *Et eksempel på brugen af attributter*

En medarbejder skal indberette pension til jeres pensionsselskab på vegne af virksomheden.

Pensionsselskabet stiller via Attributtjenesten en attribut til rådighed der f.eks. hedder "Pensionsindberetter". Virksomhedens administrator (LRA) tildeler denne attribut til en af virksomhedens medarbejdere, ved at tilknytte attributten til medarbejderens medarbejdersignatur. Når medarbejderen forsøger at tilgå pensionsselskabets onlineservice for at indberette pension med sin medarbejdersignatur, vil pensionsselskabet kunne kontrollere om den fornødne attribut er sat for den pågældende medarbejder. Er dette tilfældet gives adgang til at indberette pension på den pågældende virksomheds vegne.

En anden medarbejder uden denne attribut vil pensionsselskabet afvise.

1.3 *Hvem laver attributter?*

Det er forskellige virksomheder og offentlige myndigheder der, efter aftale med Nets DanID, stiller attributter til rådighed for andre.

¹¹ NemID selvbetjening til erhverv (MOCES2) og LRA administration (MOCES).

1.4 Hvem kan bruge attributter?

Nogen attributter stilles kun til rådighed for udvalgte CVR-numre mens andre attributter er synlige og kan vælges af alle CVR-numre med medarbejdersignaturer. Hvis attributten er synlig for administratoren i selvbetjeningen, har virksomheden mulighed for at benytte den. Man kan normalt tilknytte de samme attributter til én eller flere medarbejdere.

1.5 Hvem skal bruge attributterne?

Om man skal bruge attributter er afhængig af hvilke services, tjenester m.v. virksomhedens medarbejdere skal bruge. Normalt vil tjenesteudbyderen (f.eks. pensionselskabet i ovenstående eksempel) gøre kunden opmærksom på, at de skal tilknytte en given attribut til deres medarbejdersignatur for at kunne bruge servicen.

1.6 Forespørgsel på attribut

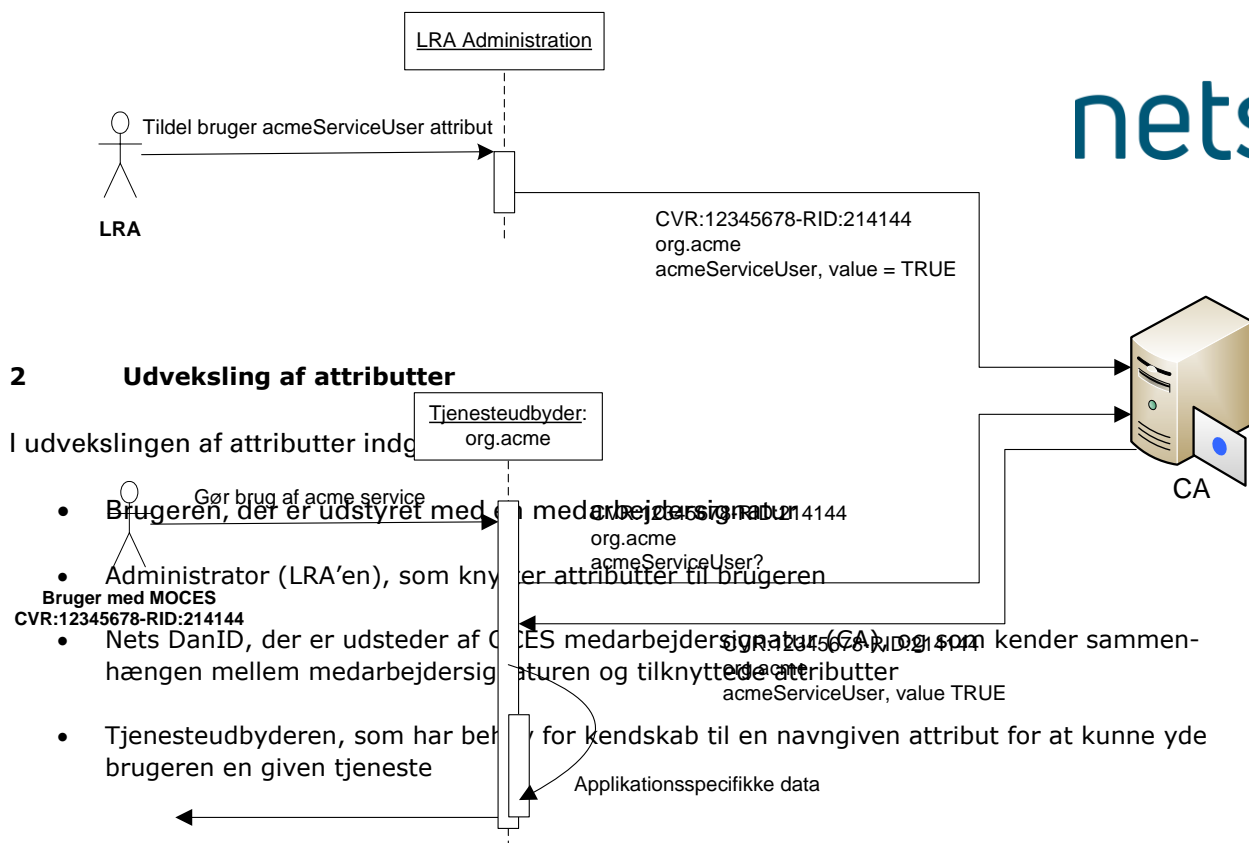
Nets DanID beskytter en given navngiven attribut (namespace, navn) mod udlevering til uønskede serviceudbydere på følgende måder:

- En attribut kan være tilgængelig for opslag for alle serviceudbydere
- En attribut kan være tilgængelig for opslag af navngiven serviceudbyder efter aftale mellem Nets DanID og attributejer
- En attribut kan være tilgængelig for verifikation for alle applikationsserviceudbydere
- En attribut kan være tilgængelig for verifikation af navngiven serviceudbyder efter aftale mellem Nets DanID og attributejer

1.7 Validering af attributindhold

Nets DanID validerer attributsyntaks, men kontrollerer i øvrigt ikke indhold og værdien af tilknyttede attributter.

Det er op til virksomheden/LRA og serviceudbyderen at etablere den nødvendige tillid til indhold af attributter.



figur 1: Eksempel, attributopslag

3 Oprette/nedlægge attributter

3.1 Hvem kan oprette/nedlægge attributter?

Nets DanID vedligeholder en "liste" over personer der må administrere attributter på vegne af den pågældende organisation. Listen indeholder, som udgangspunkt, alle der er registreret som administrator (LRA) for den pågældende organisation. Ved aftaleindgåelse kan yderligere navne tilføjes listen.

Ønskes personer tilføjet eller fjernet fra listen, skal det gøres af en person der allerede er på listen. Meddelelser om dette skal sendes via e-mail. E-mailen skal være digitalt underskrevet med den pågældende medarbejders medarbejdersignatur.

3.2 Bestilling af nye attributter

Ved bestilling af nye attributter benyttes bestillingsformular, som kan rekvireres hos Nets DanIDs support.

Nets DanID kontakter bestillingen, hvis attributten er kompleks, og dens funktionalitet skal bekræftes.

3.3 Nedlægning af eksisterende attributter

Eksisterende attributter nedlægges ved henvendelse via e-mail til Nets DanID.

4 Attribut webservicen

Attribut webservicen stilles til rådighed af Nets DanID for tjenesteudbyderne.

Følgende beskriver kort de tilgængelige operationer.

4.1 Operationer og input parametre

4.1.1 *publishAttribute*

Med operationen *publishAttribute* kan tjenesteudbyderen gøre en attribut synlig for LRA'er i en given virksomhed.

Inputværdier: Attributtens ID, virksomhedens CVR-nummer.

4.1.2 *endPublishAttribute*

Med operationen *endPublishAttribute* kan tjenesteudbyderen gøre en attribut usynlig for LRA'er i en given virksomhed.

Inputværdier: Attributtens ID, virksomhedens CVR-nummer.

4.1.3 *getAttribute*

Med operationen *getAttribute* kan tjenesteudbyderen spørge på værdien af en given attribut for en given medarbejder.

Input: Attributten id, medarbejderens certifikats `subjectSerialNumber`.

4.1.4 *getAttributes*

Med operationen *getAttributes* kan tjenesteudbyderen foretage multiple kald af *getAttribute* i ét kald.

Input: liste af inputtet til *getAttribute*

4.1.5 *verifyAttribute*

Med operationen *verifyAttribute* kan tjenesteudbyderen verificere værdien af en given attribut for en given medarbejder.

Input: attributtens ID, attributtens værdi, medarbejderens certifikats `subjectSerialNumber`.

4.2 WSDL

Testmiljø:

WSDL: https://ws-erhverv.pp.certifikat.dk/attributeservice_serviceprovider_server/?WSDL

Service endpoint: https://ws-erhverv.pp.certifikat.dk/attributeservice_serviceprovider_server

Produktionsmiljø:

WSDL: https://ws-erhverv.certifikat.dk/attributeservice_serviceprovider_server/?WSDL

Service endpoint: https://ws-erhverv.certifikat.dk/attributeservice_serviceprovider_server

Issuer er "TRUST 2408"

WS-kald	Inputparametre	Beskrivelse
publishAttribute	Attributtens ID Virksomhedens CVR-nummer	Med operationen <i>publishAttribute</i> kan tjenesteudbyderen gøre en attribut synlig for LRA'er i en given virksomhed.
endPublishAttribute	Attributtens ID Virksomhedens CVR-nummer	Med operationen <i>endPublishAttribute</i> kan tjenesteudbyderen gøre en attribut usynlig for LRA'er i en given virksomhed.
getAttribute	Attributtens ID Medarbejderens certifikats subjectSerialNumber, fx CVR:30808460-RID:1256293651992	Med operationen <i>getAttribute</i> kan tjenesteudbyderen spørge på værdien af en given attribut for en given medarbejder.
getAttributes	Liste af inputtet til <i>getAttribute</i>	Med operationen <i>getAttributes</i> kan tjenesteudbyderen foretage multiple kald af <i>getAttribute</i> i ét kald.
verifyAttribute	Attributtens ID Attributtens værdi Medarbejderens certifikats subjectSerialNumber	Med operationen <i>verifyAttribute</i> kan tjenesteudbyderen verificere værdien af en given attribut for en given medarbejder.

4.3 Returværdier

For hvert kald til webservicen understøttes følgende selvforklarende returværdier:

STATUS_OK = 0

UNKNOWN_ATTRIBUTE = 101

REFERRAL_ATTRIBUTE = 102

LOOKUP_NOT_ALLOWED = 103

VERIFICATION_NOT_ALLOWED = 104

ISSUER_NOT_SUPPORTED = 105

UNKNOWN_USER = 106

ATTRIBUTE_NOT_CONFIGURED_FOR_USER = 107

STATUS_ERROR = 108

VALUE_NOT_VERIFIED = 109

5 Kontaktinformation

Kontakt til Nets DanID vedrørende attributter kan ske via kontaktformularen:

<http://www.nets.eu/dk-da/Service/kundeservice/nemid-tu/Pages/Skriv-til-NemID-tjenesteudby-der-support.aspx>