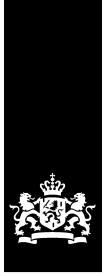


CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Toelichting LDAP datastructuur Zorg CSP

Versie 3.1

Datum 12 december 2017
Status definitief

Inhoudsopgave

Lijst van tabellen

Lijst van figuren

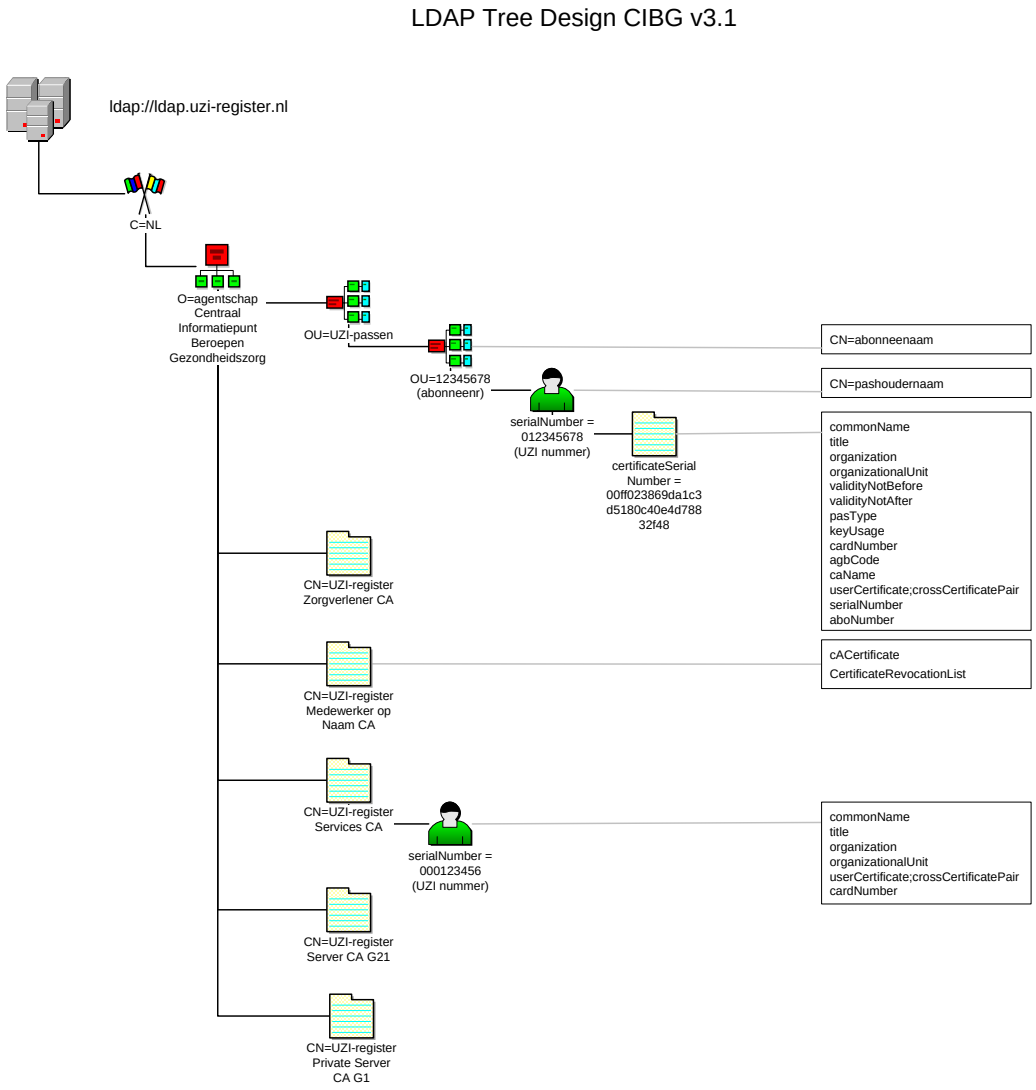
Copyright CIBG © te Den Haag
Niets uit deze uitgave mag verveelvoudigd en/of openbaar worden gemaakt (voor willekeurig welke doeleinden) door middel van druk, fotokopie, microfilm, geluidsband, elektronisch of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van CIBG.

1 LDAP datastructuur Zorg CSP

Dit document heeft als doel om de LDAP datastructuur van de Zorg CSP toe te lichten.

1.1 Overzicht directory information tree ldap.uzi-register.nl

De volgende figuur geeft een overzicht van de LDAP Directory Information Tree (DIT).



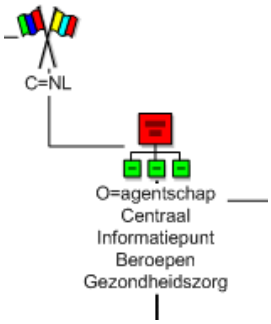
Figuur 1: Overzicht LDAP directory information tree

1.2 Toelichting per hiërarchisch niveau voor gebruikerscertificaten

Hieronder is de LDAP tree toegelicht vanaf het hoogste niveau. Deze paragraaf beschrijft alleen de tak voor certificaten van de UZI-passen.

1.2.1 C=NL, O=agentschap Centraal Informatiepunt Beroepen Gezondheidzorg

De eerste 2 nodes in de hiërarchie zijn standaard en identiek voor alle certificaten.

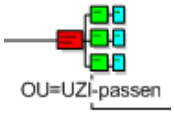


Bij de overgang naar de Public G3/Private G1 generatie zal de officiële organisatienaam -die ook opgenomen is in de issuer.organizationName van de certificaten- wijzigen in CIBG. Desondanks is besloten om de certificaten van de Public G3/Private G1 generatie te publiceren onder dezelfde nodes: C=NL, O=agentschap Centraal Informatiepunt Beroepen Gezondheidzorg. Motivatie:

- De LDAP structuur en naamgeving van de nodes is volledig intern en nergens zichtbaar voor gebruikers. Gebruikers zoeken alleen in de LDAP via de zoekpagina.
- Een volledig nieuwe structuur naast de bestaande (O=agentschap Centraal Informatiepunt Beroepen Gezondheidzorg) levert veel extra complexiteit op in de zoekpagina en ook in het Landelijke Schakelpunt van VZVZ waar een replica van de LDAP in gebruik is.

1.2.2 OU=UZI-passen

De eerste OrganizationalUnit wordt gebruikt om een onderscheid te maken tussen een tak waaronder alle eindgebruikerscertificaten van UZI-passen zijn opgeslagen en de overige takken in de LDAP structuur. De eindgebruikerscertificaten worden niet direct onder het CA-object geplaatst, maar onder een OU-object ‘UZI-passen’. Motivatie hiervoor is dat de locatie van eindgebruikerscertificaten niet wijzigt als de CA hiërarchie vernieuwd wordt. Daarnaast maakt het samenvoegen van alle pastypen in één generieke structuur het eenvoudiger om alle passen van één abonnee te tonen.



1.2.3 OU=[abonneenummer]

Eindgebruikers (en hun certificaten) worden niet direct onder het OU-object ‘UZI-passen’ gepubliceerd. Onder de ‘OU=UZI-passen’ worden objecten (type OrganizationalUnit) uit de class uzi-registerOrganisation aangemaakt. Dit object wordt gebruikt om het abonneenummer te publiceren en pashouders te organiseren per abonnee. Abonnees fungeren als container voor pashouders, gedefinieerd in de objectclass uzi-registerUser. Motivatie is dat hierdoor sneller alle pashouders van een bepaalde abonnee gevonden kunnen worden. Omdat de naam van een abonnee niet uniek hoeft te zijn, bestaat het naamgevende attribuut van dit OU object uit het abonneenummer.

Behalve het abonneenummer is uit efficiency overwegingen ook de naam van de organisatie opgenomen in een CommonName attribuut.

Door deze ontwerpkeuze is het mogelijk om op basis het abonneenummer de abonneenaam op te vragen.

1.2.4 *SerialNumber=[UZI-nummer]*

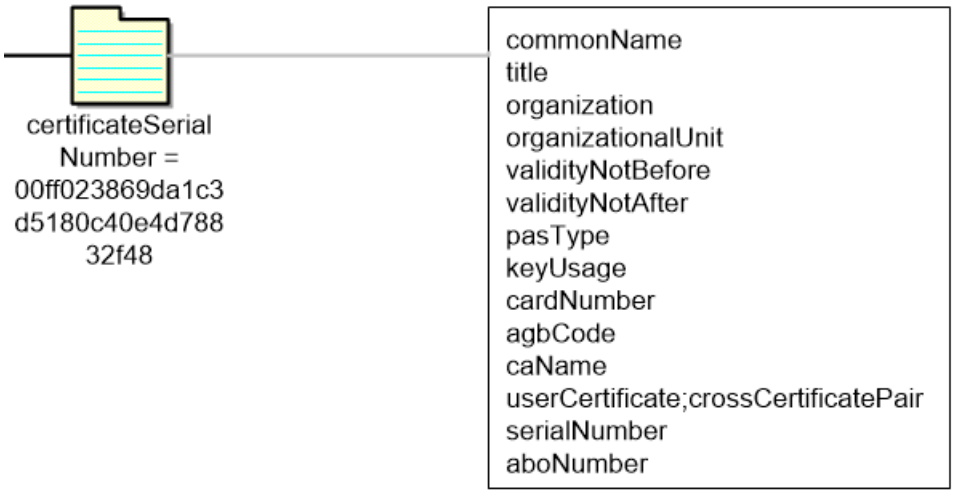
Pashouders worden gedefinieerd in objecten van de objectclass uzi-registerUser. Op dit niveau wordt het gegarandeerd unieke attribuut van een pashouder opgeslagen, te weten het subject.serialNumber waarin het UZI-nummer is opgeslagen.
Pashouders fungeren als container voor certificaten, gedefinieerd in de objectclass uzi-registerCertificateData.

Behalve het UZI-nummer is uit efficiency overwegingen de naam van de pashouder opgenomen in een CommonName attribuut. Door deze ontwerpkeuze is het mogelijk om op basis van UZI-nummer (en abonneenummer) de naam van de pashouder op te vragen.

1.2.5 *certificateSerialNumber=[certificaat serienummer]*

Eindgebruikerscertificaten zijn samen met een aantal attributen in een aparte objectclass gedefinieerd. Dit betreft -met uitzondering van het pasnummer- gegevens die uit het certificaat zijn overgenomen. Deze gegevens worden in attributen opgeslagen om het zoeken erop te vereenvoudigen. Dit betreft objecten van de objectclass uzi-registerCertificateData.

Hieronder is aangegeven welke gegevens per certificaat zijn opgeslagen.



Naast het binaire certificaat bestaat deze objectclass dus uit attributen die gevuld worden uit het geparste certificaat, maar ook metadata. Deze extra attributen zijn toegevoegd voor de leesbaarheid en om het zoekproces op certificaatattributen te optimaliseren, met name vanuit de LDAP zoekpagina.
Deze objecten worden onder pashouders (uzi-registerUser) geplaatst en worden uniek geïdentificeerd aan de hand van het certificate.serialnumber.

Onderstaande tabel geeft per attribuut een toelichting.

Attribuut	Toelichting
commonName	Bevat de naam van de pashouder uit de Subject.commonName van het certificaat. Strikt genomen is de CN redundant met de commonName die in het uzi-registerUser object is opgenomen. Er is gekozen om dit toch op 2 plaatsen op te nemen vanwege de volgende redenen: • Als een gebruiker alleen de naam nodig heeft bij een UZI-nummer, kan eenvoudig het uzi-registerUser object opgevraagd worden. Om dit efficiënt te doen is in de structuur ook een abonneenummer nodig; • Als rechtstreeks het certificaat wordt opgevraagd, staat alle informatie uit het certificaat in de attributen van het uzi-registerCertificateData object; • Toekomstvastheid bij mogelijke naamswijzigingen.
title	Beroepstitel overgenomen uit subject.title van het certificaat.
organization	Bevat de naam van de abonnee uit de Subject.organizationName van het certificaat. Strikt genomen is dit redundant met de abonneenaam die in het abonnee object is opgenomen. Er is gekozen om dit toch op 2 plaatsen op te nemen vanwege de volgende redenen: • Als een gebruiker alleen de abonneenaam nodig heeft bij een abonneenummer (en geen UZI-nummer beschikbaar heeft), hoeft alleen het uzi-registerOrganization object opgevraagd te worden; • Als rechtstreeks het certificaat wordt opgevraagd, staat alle informatie uit het certificaat in de attributen van het uzi-registerCertificateData object; • Toekomstvastheid bij mogelijke naamswijziging.
organizationalUnit	Optionele OU attribuut in bepaalde pastypen. Overgenomen uit subject.OrganizationalUnitName.
validityNotAfter validityNotBefore	Geldigheidsduur van certificaat, zodat eenvoudig is vast te stellen of een certificaat nog geldig is.
pasType	Gecodeerde pastype uit subject.AltName van certificaat (Z, I, M, N)
keyUsage	Weergave van het keyUsage attribuut uit het certificaat. Dit maakt het mogelijk om te zoeken op authenticatie-, vertrouwelijkheid, of handtekeningcertificaat. Het is als volgt gevuld: • Als keyUsage=digitalSignature dan 'Authenticatie' • Als keyUsage=NonRepudiation dan 'Elektronische handtekening' • Als keyUsage=keyEncipherment, dataEncipherment, keyAgreement dan 'Vertrouwelijkheid'
cardNumber	Pasnummer (8NUM) van de UZI-pas. Dit pasnummer van de UZI-pas waar de certificaten op staan, maakt het mogelijk om met zekerheid certificaten van één pas te combineren en om op het pasnummer te kunnen zoeken.
agbCode	Uit subject.AltName van certificaat (8NUM).
caName	Is gelijk aan Issuer.CommonName van het certificaat. De caName is nodig omdat de CA naam niet meer in de hiërarchie zit van de eindgebruikerscertificaten en waarschijnlijk wijzigt bij vernieuwing van de CA hiërarchie.
userCertificate; crossCertificatePair[1]	DER encoded certificaat.
serialNumber	UZI-nummer uit certificaat (9NUM).
aboNumber	UZI-register Abonneenummer (URA) uit de subject.AltName van certificaat (8NUM).

Tabel 1: Toelichting attributen met certificaatgegevens

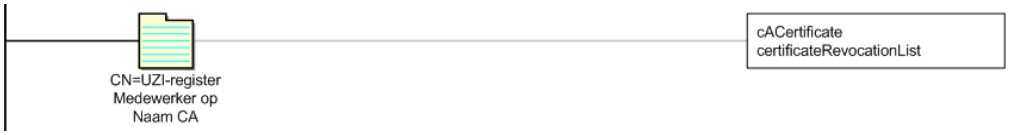
1 In de G3 Public/G1 Private omgeving is in de TSP CA certificaten een subject.organisationIdentifier opgenomen. Die komt als issuer.organisationIdentifier terug in de eindgebruikerscertificaten. Dit leverde problemen op bij publicatie met het standaard attribuut userCertificate en bleek wel te werken met type crossCertificatePair.

1.3 Gedetailleerde toelichting per hiërarchisch niveau overige takken

Deze paragraaf beschrijft de overige nodes van de directory structuur die aangemaakt zijn onder O=agentschap Centraal Informatiepunt Beroepen Gezondheidzorg. Dit betreft één node per CA.

1.3.1 CN=[CA naam pastype]

De CA-gegevens (CA-certificaat en de CRL) worden in objecten van de bestaande objectclass pkiCA gepubliceerd. Dit is identiek aan de huidige situatie.



Bij het ontstaan van nieuwe CA's -bijvoorbeeld bij de vernieuwing van de CA-hiërarchie- ontstaan er een nieuwe CA-objecten voor de publicatie van CRL's en het CA certificaat.

De publicatie van CRL's in de LDAP stopt voor de uitfasering van G2. Voor de Public G3/Private G1 hiërarchie zal geen CRL publicatie in de LDAP worden ingericht.

1.3.2 CN=[CA naam servercertificaat]

In het LDAP ontwerp is er een verschil tussen servercertificaten en eindgebruikercertificaten van UZI-passen. De servercertificaten worden direct onder het CA object gepubliceerd.

Consequentie hiervan is dat bij een vernieuwing van de CA voor servercertificaten het nieuwe CA object niet alleen gebruikt wordt voor publicatie van CRL en CA certificaat, maar ook voor publicatie van de servercertificaten die vanaf dat moment gepubliceerd worden.

Met de invoering van Generatie 2 is er een tak bijgekomen die verder geen verandering op de werking van de LDAP met zich meebrengt. Dit is: CN=UZI-register Server CA G2.

Met de invoering van SHA-2 is er een tak bijgekomen die verder geen verandering op de werking van de LDAP met zich meebrengt. Dit is: CN=UZI-register Server CA G21.

Met de invoering van Private G1 hiërarchie voor servercertificaten komt er een tak bij die verder geen verandering op de werking van de LDAP met zich meebrengt. Dit is: CN=UZI-register Private Server CA G1. Wel is het schema uitgebreid met crossCertificatePair, zie voetnoot 1.

Voor ZOVAR servercertificaten is een vergelijkbare structuur aanwezig. Ook hier geldt dat de invoering van Private G1 hiërarchie voor servercertificaten een nieuwe tak oplevert waaronder de ZOVAR Private G1 servercertificaten worden gepubliceerd.