

0101UZI0100REGISTER10111

Toelichting release 2.1

LDAP datastructuur

Uitgave : agentschap CIBG, UZI-register
Versie : 1.2 Definitief
Datum : 7 juli 2008

© 2008 CIBG, Den Haag

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enig andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever: CIBG, telefoon 070-3407446

Inhoudsopgave

1	Inleiding	3
1.1	Doelstelling	3
1.2	Overige documentatie LDAP directory	3
1.3	Release en Versie historie	3
1.3.1	Release LDAP	3
1.3.2	Document historie	3
2	LDAP datastructuur	4
2.1	Overzicht en algemene toelichting directory tree	4
2.2	Gedetailleerde toelichting per hiërarchisch niveau voor gebruikerscertificaten	5
2.2.1	C = NL, O = agentschap Centraal Informatiepunt Beroepen Gezondheidszorg	5
2.2.2	OU = UZI-passen	5
2.2.3	OU = [abonneenummer]	6
2.2.4	SerialNumber = [UZI-nummer]	6
2.2.5	certificateSerialNumber = [certificaat serienummer]	6
2.3	Gedetailleerde toelichting per hiërarchisch niveau overige takken	8
2.3.1	CN = [CA naam pastype]	8
2.3.2	CN = [CA naam servercertificaat]	8

Lijst van figuren

Figuur 1: Overzicht nieuwe LDAP directory information tree	4
--	---

Lijst van tabellen

Tabel 1: Toelichting attributen met certificaatgegevens.....	8
--	---

1 Inleiding

1.1 Doelstelling

Dit document heeft als doel om het nieuwe LDAP datamodel toe te lichten naar aanleiding van het zogenaamde *LDAP Redesign*. De doelgroep van dit document bestaat uit ontwikkelaars van XIS-applicaties.

De motivatie voor het LDAP redesign is tweeledig:

1. het oplossen van bestaande issues. De belangrijkste waren dat het bij één pashouder niet mogelijk was om meerdere abonneenamen of beroepstitels vast te leggen.
2. het invullen van nieuwe functionele behoeften. Dit is onder andere het vastleggen van abonneenummer en pasnummer in de directory.

1.2 Overige documentatie LDAP directory

Naar aanleiding van het LDAP redesign zijn de volgende documenten opgesteld:

- De aanleiding van het LDAP redesign is in meer detail beschreven in *20060626 Redesign LDAP en zoekpagina UZI-register (1.0).doc*. Dit interne ontwerp document is niet vereist om de werking van de LDAP directory te begrijpen. Indien gewenst, is het op te vragen via de servicedesk van het UZI-register: info@uzi-register.nl.
- In *Toelichting gebruik R2.0 LDAP directory* staat beschreven hoe de LDAP via een LDAP browser of command-line tool kan worden bevestigd.
- In *Toelichting gebruik R2.0 LDAP zoekpagina* staat beschreven hoe de LDAP via de LDAP zoekpagina kan worden bevestigd.

1.3 Release en Versie historie

1.3.1 Release LDAP

De initiële versie van de LDAP is release 1.0. De versie die operationeel is na uitvoering van het LDAP redesign is release 2.0.

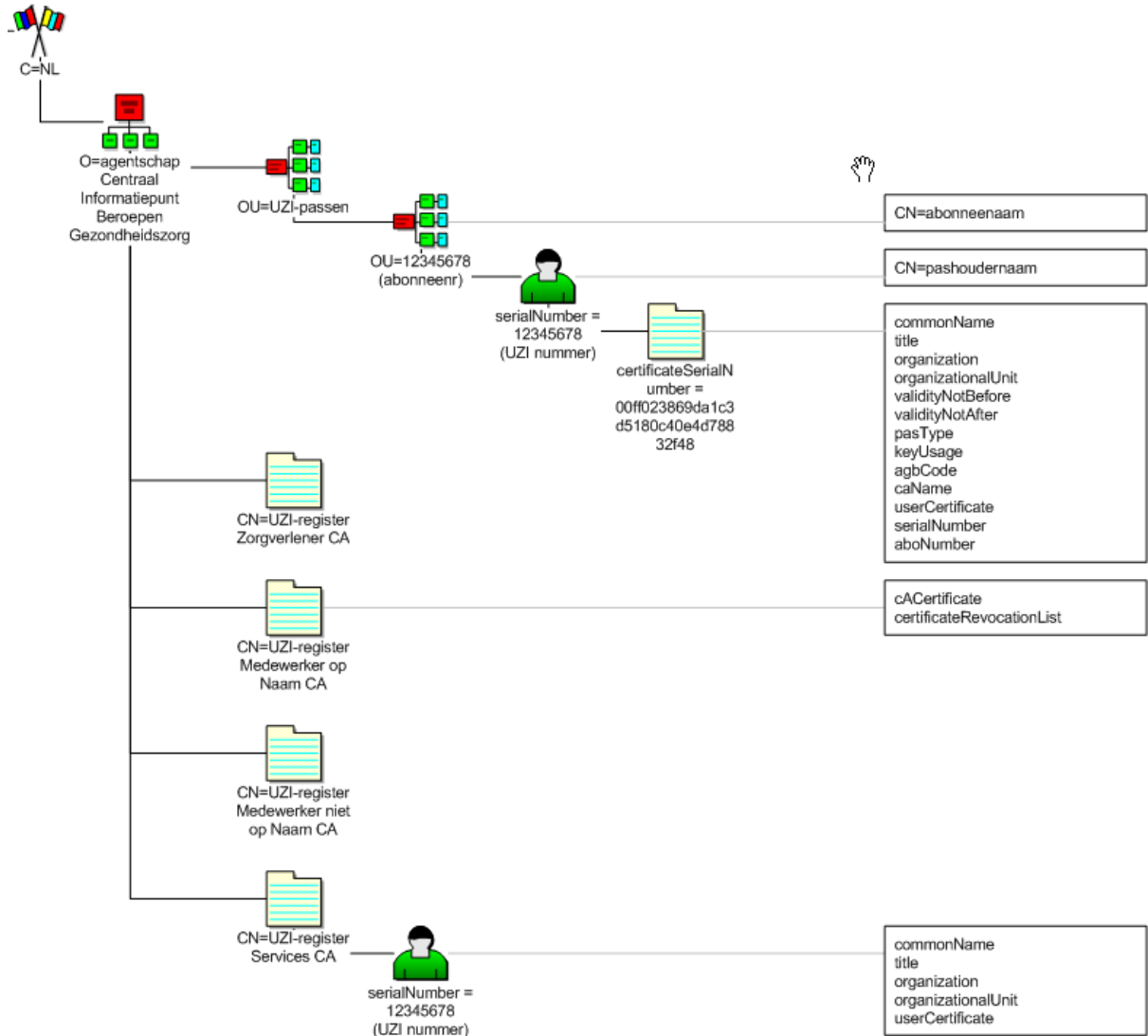
1.3.2 Document historie

Versie	Datum	Status	Omschrijving
1.0	27-04-2007	Definitief	Gepubliceerd als <i>20070427 Toelichting release 2.0 LDAP en zoekpagina UZI-register v1.0.pdf</i>
1.1	14-03-2008	Definitief	Er zijn geen wijzigingen in de LDAP datastructuur. Wijziging t.o.v. originele document: Hoofdstuk 3 LDAP zoekpagina is verwijderd. Hiervoor is een apart document opgesteld.

2 LDAP datastructuur

2.1 Overzicht en algemene toelichting directory tree

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



Figuur 1: Overzicht nieuwe LDAP directory information tree

De belangrijkste wijzigingen en kenmerken van versie 2.0 van het LDAP ontwerp zijn hieronder weergegeven:

1. De eindgebruikerscertificaten worden niet meer onder het CA-object geplaatst, maar onder een nieuw 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 makkelijker om alle passen van één abonnee te tonen.
2. Er is een apart hiërarchisch niveau gecreëerd voor abonnees. Eindgebruikers worden niet direct onder het nieuwe OU-object 'UZI-passen' gepubliceerd. Onder de OU 'UZI-passen' worden

objecten uit de class uzi-registerOrganisation geplaatst (abonnees), waaronder vervolgens de pashouders van die abonnee worden geplaatst. Motivatie is dat hierdoor sneller pashouders van een bepaalde abonnee gevonden kunnen worden.

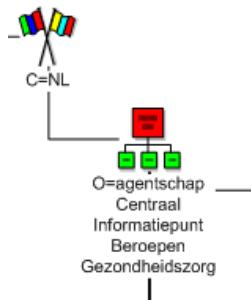
3. Het gebruikersobject bevat alleen een unieke identifier (het UZI-nummer) én de naam van de pashouder. Verder dient het als container voor certificaatobjecten. Gebleken is dat er gegevens zijn die per samenhangende groep certificaten (UZI-pas) kunnen veranderen, zoals beroepstitel. In de oude datastructuur werden deze gegevens nog op het niveau van de gebruiker opgeslagen. In de nieuwe structuur op het niveau van het certificaat.
4. Eindgebruikerscertificaten zijn samen met een aantal gegevens 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 vergemakkelijken.
5. Per certificaat wordt ook het pasnummer opgeslagen van de UZI-pas waarop het certificaat staat. Dit pasnummer maakt het mogelijk om met zekerheid certificaten van één pas te combineren en om op het pasnummer te kunnen zoeken.
6. Vanaf versie 2.0 van de LDAP directory wordt er onderscheid gemaakt tussen servercertificaten en eindgebruikerscertificaten van UZI-passen. De opslag van servercertificaten in de LDAP is niet gewijzigd in versie 2.0 van de LDAP directory.
7. De opslag van de CRL's en CA certificaten is niet gewijzigd.

2.2 Gedetailleerde toelichting per hiërarchisch niveau voor gebruikerscertificaten

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

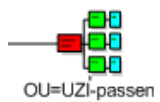
2.2.1 C=NL, O=agentschap Centraal Informatiepunt Beroepen Gezondheidszorg

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



2.2.2 OU=UZI-passen

De eerste OrganizationalUnit wordt gebruikt om een onderscheid te maken tussen een tak waaronder alle eindgebruikerscertificaten zijn opgeslagen en de overige takken in de LDAP structuur.



2.2.3 *OU=[abonneenummer]*

De tweede OrganizationalUnit (Objectclass uzi-registerOrganization) wordt gebruikt om het abonneenummer te publiceren en pashouders te organiseren per abonnee. Omdat de naam van een abonnee niet uniek hoeft te zijn, bestaat het naamgevende attribuut van dit OU object uit het abonneenummer. Abonnees fungeren als container voor pashouders, gedefinieerd in de objectclass uzi-registerUser.



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.

2.2.4 *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.

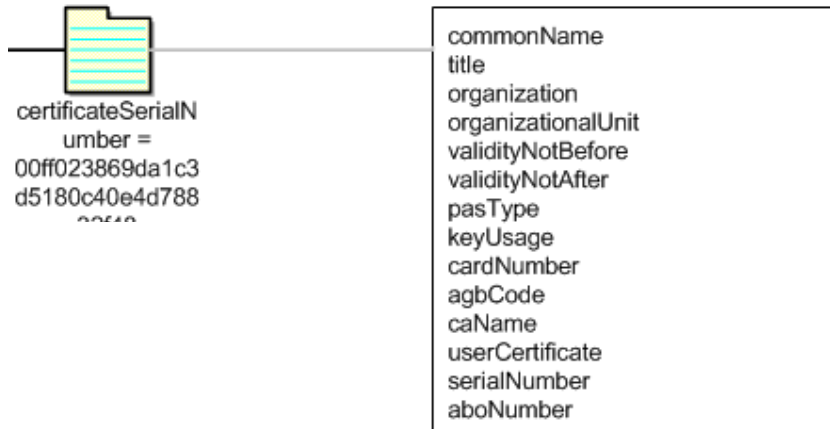


Behalve het UZI-nummer is uit efficiency overwegingen de naam van de pashouder opgenomen in een CommonName attribuut.

Door deze ontwerpkeuze is het mogelijk om op basis van UZI-nummer (en abonneenummer) de naam van de pashouder op te vragen.

2.2.5 *certificateSerialNumber=[certificaat serienummer]*

Certificaten van eindgebruikers en een aantal verwante attributen worden opgeslagen in objecten van de objectclass uzi-registerCertificateData. Hieronder is aangegeven welke gegevens per certificaat worden opgeslagen.



Naast het binaire certificaat bestaat deze objectclass dus uit attributen die gevuld worden uit het geparseerde 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: <ul style="list-style-type: none"> • 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 nieuwe 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
agbCode	Uit subject.AltName van certificaat (8NUM).

Attribuut	Toelichting
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	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

2.3 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 Gezondheidszorg. Dit betreft één node per CA.

2.3.1 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.

2.3.2 CN=[CA naam servercertificaat]

Door het LDAP redesign ontstaat er een verschil tussen servercertificaten en eindgebruikercertificaten. De servercertificaten worden direct onder het CA object gepubliceerd. Hierin is niets gewijzigd ten opzichte van LDAP release 1.0.



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.

De redenen om de servercertificaten ongewijzigd te laten bij het LDAP redesign zijn:

- De servercertificaten worden rechtstreeks gepubliceerd vanuit het CA systeem, waardoor de oplossing die gerealiseerd is voor de certificaten van de UZI-passen niet toepasbaar is;
- De beperkingen van het LDAP datamodel release 1.0 zijn niet van toepassing op servercertificaten;
- De functionele behoefte om uitgebreider te kunnen zoeken op servercertificaten is niet bekend.