

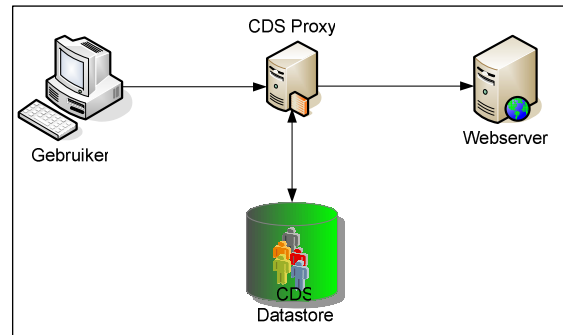


## Centrale Directory Server

Sinds februari 2001 heeft de Gemeente Den Haag een Centrale Directory Server operationeel. Deze Centrale Directory Server verzorgt voor alle medewerkers en klanten van de gemeente Den Haag (zowel inwoners als niet-natuurlijke personen) de centrale authenticatie voor de Internet omgeving. Deze Centrale Directory Server bestaat in feite uit twee delen: de CDS authenticatie Proxy en de CDS Datastore. De CDS Datastore bevat ongeveer 700.000 identiteiten.

De centrale authenticatie kan worden gedaan met behulp van gebruikersnaam en wachtwoord of op basis van gebruikersnaam en een tokenwachtwoord (zogenaamde twee-factoren authenticatie: "kennis en bezit"). Voor het opvragen van de gebruikersnaam en het aanvragen van een initieel wachtwoord voor natuurlijke personen, ingeschreven in een Nederlandse gemeente, is DigiD beschikbaar en voor de overigen is de applicatie HaagiD beschikbaar.

Eind 2005 is de Centrale Directory Server ook gekoppeld aan DigiD (de landelijke identiteits provider), zodat klanten met een DigiD account ook kunnen inloggen bij Den Haag.

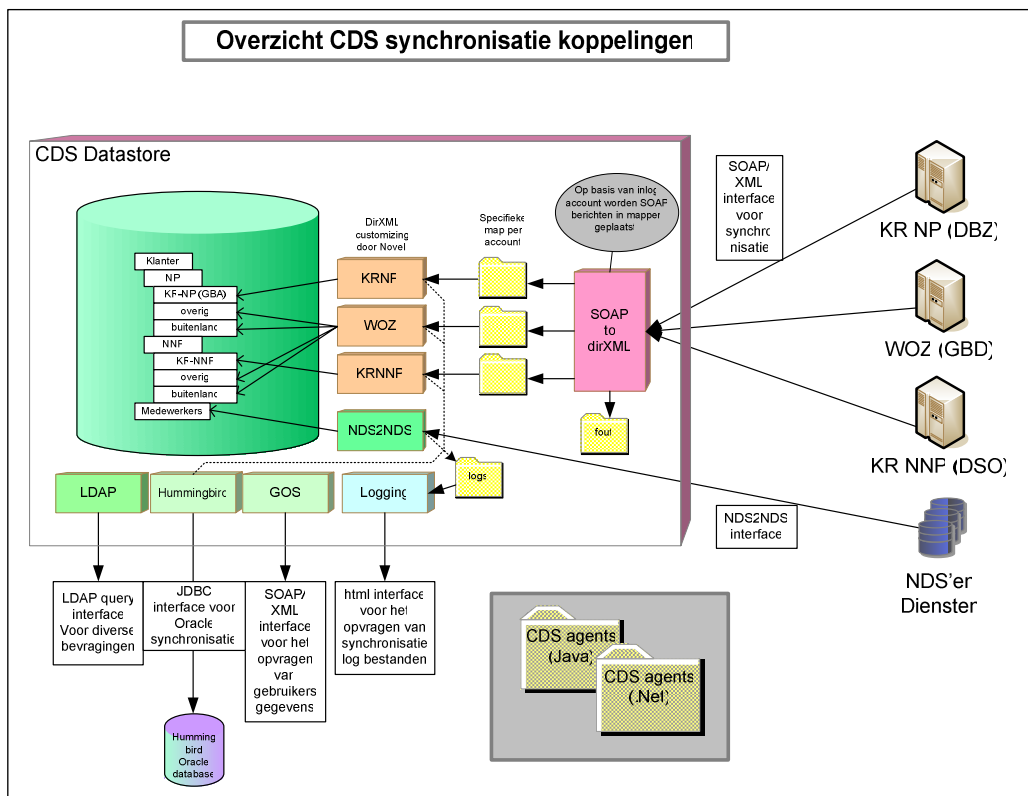


Naast de authenticatie voorziet de centrale directory server ook in het opslaan en verstrekken van autorisatie gegevens aan de achterliggende applicaties.

Voor de vulling en actualisatie van de CDS Datastore worden SOAP/XML koppelingen gebruikt, via welke de gegevens in de Datastore kunnen worden beheerd.

Voor de raadpleging van de gegevens in de CDS Datastore staat naast LDAP ook een webservice ter beschikking.

Alle gebruikte software is gebaseerd op open standaarden en voor zover mogelijk open source. Via DigiD en OSOSS is de programmatuur ook beschikbaar voor andere gemeenten en overheids-instellingen.



## Technische details:

De CDS bestaat uit twee delen:

- CDS Datastore, hierin zitten alle gegevens. De gebruikers zijn onderverdeeld in medewerkers en Klanten.
- CDS Proxy, dit is een authenticatie Proxy welke de feitelijke authenticatie verzorgd.

In feite biedt de CDS twee functies: authenticatie en autorisatie

## Authenticatie

Via de CDS Proxy wordt aan http/https applicaties authenticatie aangeboden. Alle netwerkverkeer loopt fysiek door de CDS Proxy en wordt alleen doorgegeven aan de applicatie na een succesvolle authenticatie.

Hoe en onder welke condities wordt geauthenticeerd wordt in de CDS ingesteld in overleg met de applicatie eigenaar.

Omdat alle netwerkverkeer via de CDS Proxy blijft lopen kan deze ook single-signon bieden tussen verschillende applicaties.

**Eisen aan applicatie:** Geen, uitsluitend geauthenticeerde gebruikers komen bij de applicatie. Inloggen gebeurt dus niet op de applicatie, maar op de CDS Proxy.

## Autorisatie

Naast de hiervoor beschreven authenticatie voorziet de CDS ook in het aanreiken van autorisatie gegevens aan de applicatie, op basis waarvan de applicatie de juiste autorisatie kan bepalen.

Deze autorisatie gegevens komen altijd uit de CDS datastore en kunnen fysiek op twee verschillende manieren (query string of http header) aan de applicatie worden doorgegeven.

Default worden gebruikersnaam en wachtwoord meegegeven in de http authorisation header

**Eisen aan de applicatie:** om de meegezonden autorisatie gegevens te kunnen gebruiken, dient de applicatie deze uit de query string of http header uit te lezen. Dit zal in veel gevallen een (eenvoudige) aanpassing aan de applicatie vergen.

## CDS Agents

Om applicatie bouwers te ondersteunen bij het uitlezen van de gegevens uit de query string en authorisation header zijn zogenaamde CDS Agents beschikbaar in een .Net en Java uitvoering. Dit is een stukje code die in de applicatie kan worden gebruikt. Deze CDS Agents voorzien ook in een functie om via (S)LDAP de autorisatie gegevens van een gebruiker te controleren of op te halen tegen de CDS Datastore.

## DigiD en HaagiD

Zoals voor de natuurlijke personen, ingeschreven in een Nederlandse gemeente, nu DigiD beschikbaar is voor het verstrekken van een gebruikersnaam en inlogcode, is in Den Haag voor de overige klanten HaagiD beschikbaar. HaagiD is een separate webapplicatie voor het aanvragen van de gebruikersnaam en een initieel wachtwoord. Zowel gebruikersnaam als initieel wachtwoord worden via een zogenaamde pin-mailer per post aan de gebruiker toegezonden. Om na ontvangst van het initiële wachtwoord in te kunnen loggen dient de gebruiker eerst dit initiële wachtwoord te wijzigen in een zelfgekozen wachtwoord. Dit loopt ook via de HaagiD applicatie.

## Componenten

De basis van de CDS wordt gevormd door de CDS Datastore en CDS Proxy. Daaromheen zijn een aantal componenten gebouwd, welke gebaseerd zijn op open standaarden (LDAP, SOAP, XML en http) en open source software (Apache, Tomcat).

