



DigiD Gateway

DigiD: "DigiD (spreek uit: 'Diegiedee') staat voor Digitale Identificatie; het is een gemeenschappelijk systeem van en voor de overheid. Overheidsinstellingen kunnen met DigiD de identiteit verifiëren van klanten die gebruikmaken van haar elektronische diensten. Op aanvraag ontvangt de burger van DigiD hiervoor een gebruikersnaam met wachtwoord."

DigiD Gateway

Omdat in de gemeente Den Haag¹ nu authenticatie plaatsvindt voor een grotere groep dan de doelgroep van DigiD², moet voor de koppeling met DigiD in gemeente Den Haag eerst een keuze scherm worden aangeboden om de twee doelgroepen te scheiden: klanten uit de DigiD doelgroep en overige klanten. Klanten uit de DigiD doelgroep moeten gaan inloggen via DigiD, alle overige klanten moeten blijven inloggen via de bestaande Haagse voorziening. Dit is de functie van het verkeersplein. Dus de klant komt bij het verkeersplein en kiest 'DigiD' of 'niet-DigiD'. Indien gekozen wordt voor 'niet-DigiD' gaat het inloggen via de bestaande Haagse voorziening op de gebruikelijke wijze.

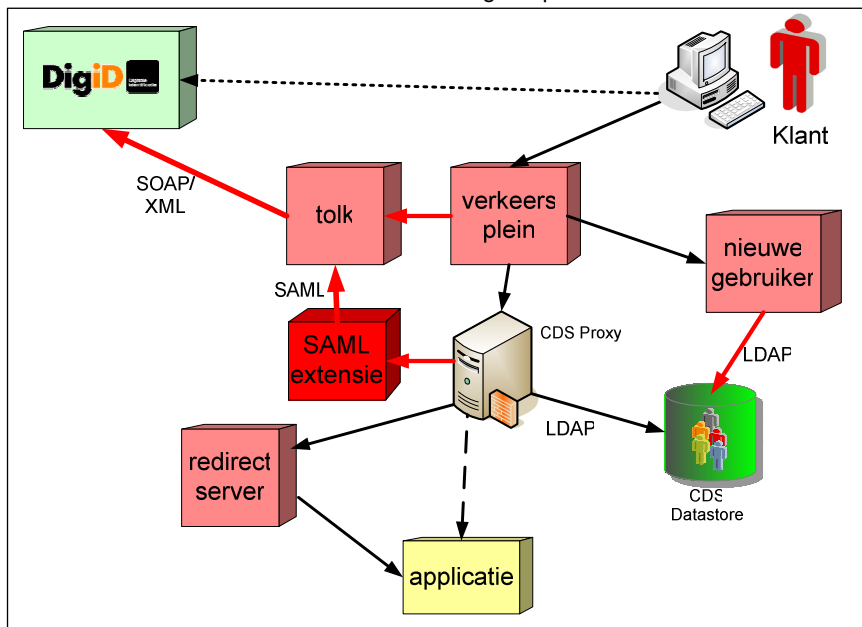
Indien gekozen wordt voor 'DigiD', dan wordt via de Tolk aan DigiD een sessie-ID gevraagd, vervolgens wordt door het verkeersplein de klant naar DigiD geredirect onder medegeven van een Haagse DigiD identiteit en het sessie-ID.

De klant logt in via de DigiD server en wordt terug gestuurd naar het verkeersplein.



Het verkeersplein vraagt via de Tolk aan DigiD of de betreffende klant inderdaad is geauthenticeerd bij DigiD. Zo nee: dan volgt een foutmelding. Zo ja: dan vraagt de Tolk aan DigiD om nadere gegevens van deze klant, waarna DigiD het Sofinumnummer (BSN)³ en Betrouwbaarheidsniveau verstrekt.

Omdat de communicatie tussen Tolk en DigiD op een niet-standaard SOAP/XML manier verloopt en de CDS



Proxy de hiervoor bedoelde SAML standaard gebruikt, wordt de hele communicatie door de Tolk omgezet naar SAML⁴. Waarna tussen de Tolk en de SAML extensie soort vraag-en-antwoord spel plaatsvindt, maar dan via het SAML protocol. Resultaat: de klant wordt ingelogd via de CDS Proxy, waarbij de op basis van het BSN opgezochte autorisatie gegevens op de gebruikelijke wijze worden doorgegeven aan de applicatie. Voor de applicatie is het transparant of iemand via DigiD of rechtstreeks via de CDS Proxy is ingelogd.

¹ De DigiD Gateway is door de gemeente Den Haag in samenwerking met de gemeente 's-Hertogenbosch ontwikkeld. Dus overal waar in dit document gemeente Den Haag wordt genoemd, wordt bedoeld: gemeente Den Haag én gemeente 's-Hertogenbosch.

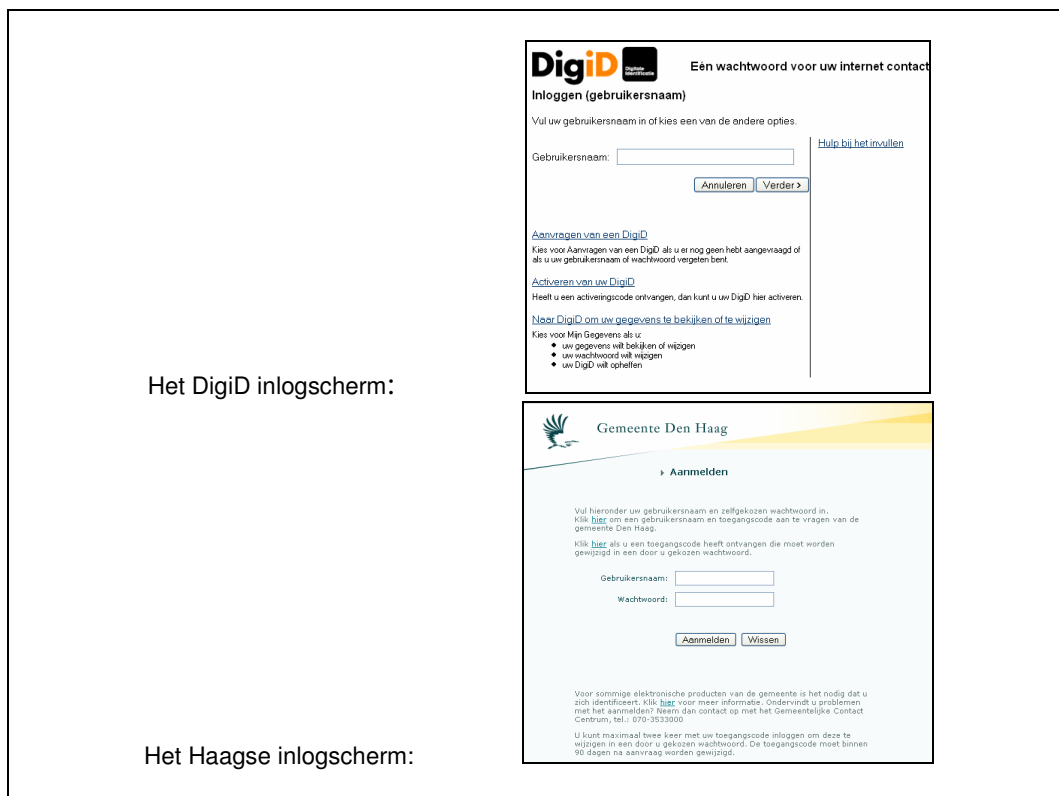
² DigiD richt zich op dit moment uitsluitend op natuurlijke personen, die zijn ingeschreven als inwoner van een Nederlandse gemeente.

³ Begin 2006 wordt het Sofinumnummer vervangen door het Burgerservicenummer (BSN)

⁴ Vandaar de naam DigiD Gateway.

Nieuwe gebruiker

Bovenbeschreven methode werkt uitsluitend indien het Sofinummer (BSN) van de burger voorkomt in de Haagse CDS Datastore, met andere woorden: indien deze burger een bestaande klant is van de gemeente Den Haag. Indien een gebruiker wel een DigiD inlogcode heeft, maar (nog) niet bekend is bij de gemeente Den Haag (zijn/haar BSN komt niet voor in de CDS Datastore) dan betreft het een zogenaamde 'nieuwe gebruiker'. In dit geval krijgt de gebruiker de keuze om als tijdelijke klant te worden toegevoegd aan de Haagse CDS Datastore. Indien de gebruiker hiervoor kiest, wordt zijn/haar BSN opgenomen in de CDS Datastore. Regelmatig worden deze tijdelijke gebruikers gewist (huidige planning is om dit elke nacht te doen). Omdat deze nieuwe gebruikers in een speciale separate container van de CDS Datastore worden aangemaakt, krijgen de applicaties de mogelijkheid om al of niet diensten te verlenen aan deze nieuwe gebruikers.



Technische realisatie

De DigiD gateway is ontworpen en gebouwd om op diverse platformen te kunnen werken. Inmiddels zijn implementaties gedaan op Windows 2003 en Suse linux.

Er is uitsluitend gebruik gemaakt van open standaarden, zoals SAML, LDAP, SOAP, XML en http, en open source producten, zoals Apache, Tomcat en Open SAML. Als resultaat hiervan is de gehele DigiD Gateway als open source beschikbaar via het OSOSS uitwisselplatform.

Vanzelfsprekend is alle output van de DigiD gateway browser onafhankelijk en voldoet deze volledig aan de W3C eisen.

Componenten

De DigiD Gateway bestaat uit de volgende componenten:

- DigiD Gateway Verkeersplein
- DigiD Gateway Tolk
- DigiD Gateway Nieuwe Gebruiker aanmaken
- DigiD Gateway Nieuwe Gebruiker verwijderen
- DigiD Gateway Redirect applicatie
- HaagiD Gebruikersnaam aanvragen
- HaagiD Toegangscode aanvragen
- HaagiD Toegangscode wijzigen
- HaagiD Gebruikersnaam opvraag service