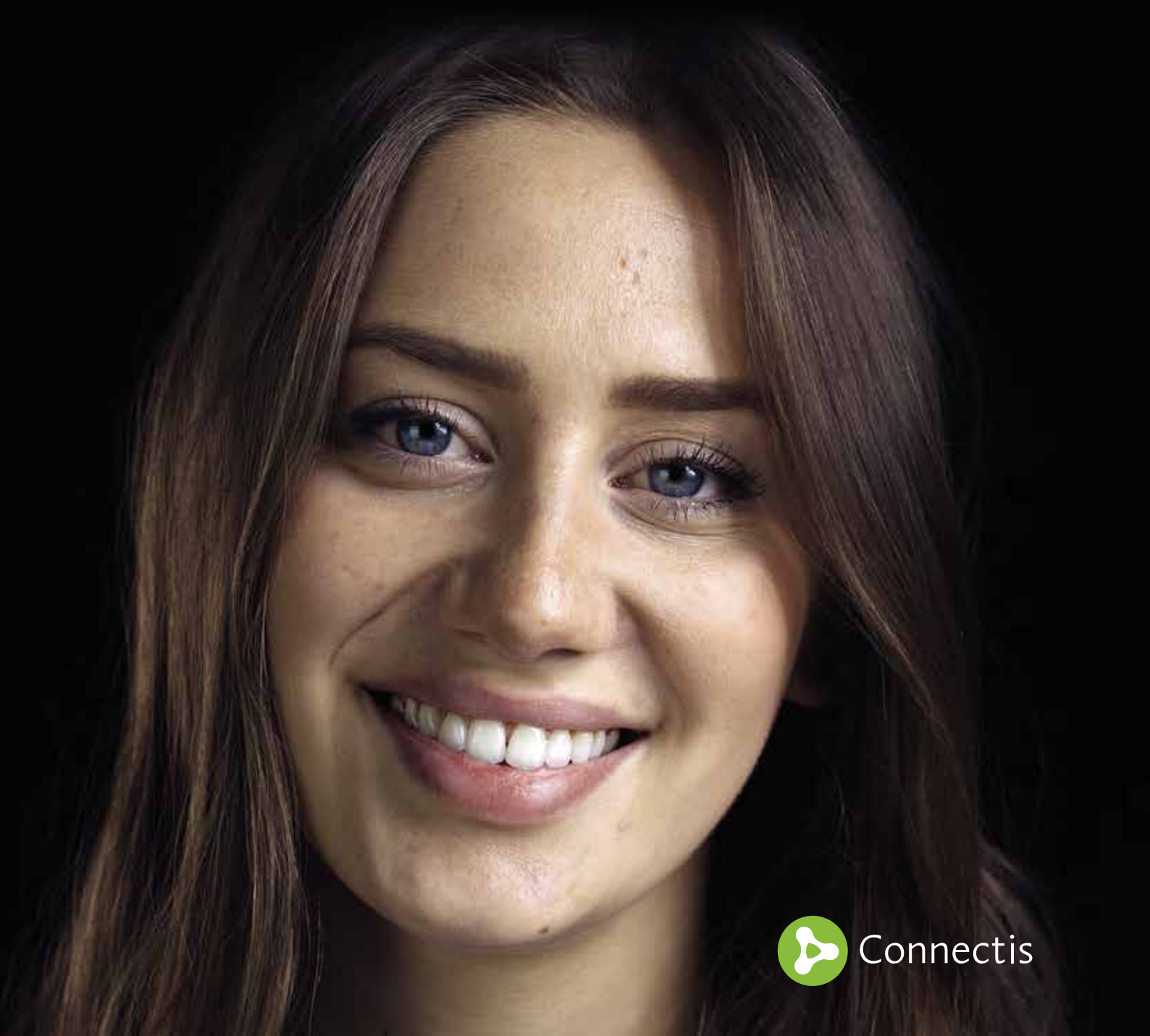
Alle online identificatiemiddelen ontsluiten

via de Connectis Identity Broker

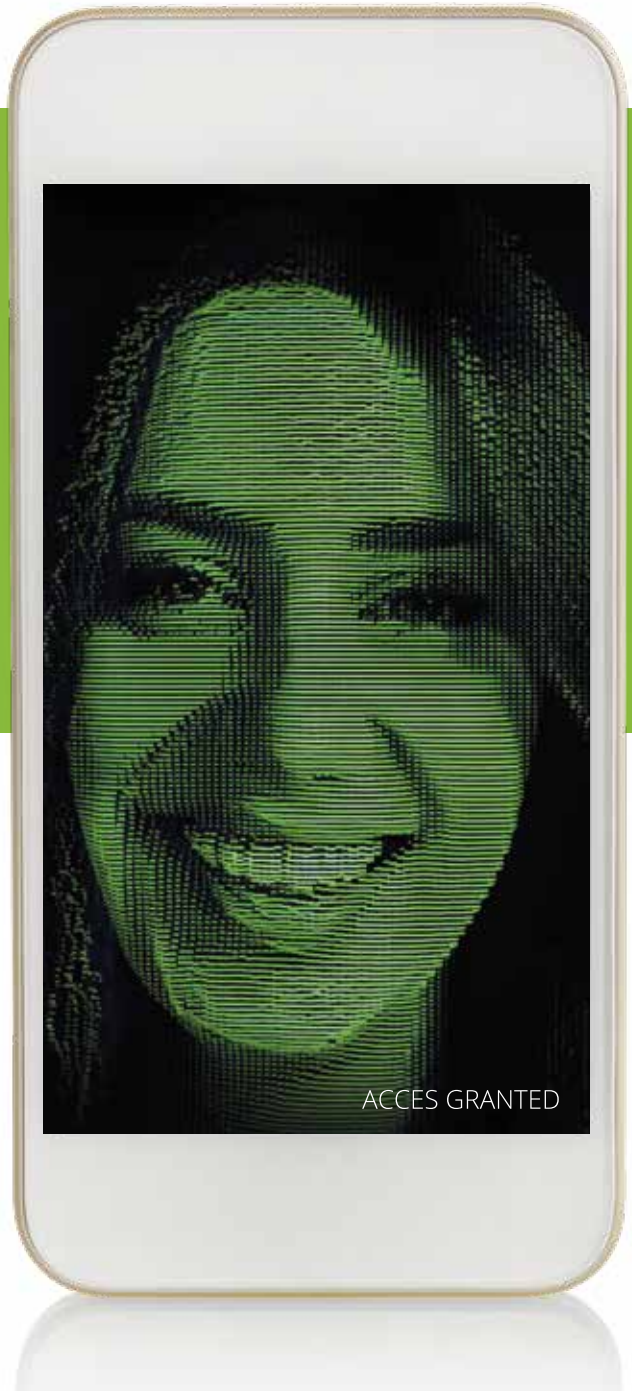


Connectis

Alle inlogmiddelen ontsluiten via de Connectis Identity Broker

eID's: voor ieder wat wils

Er zijn diverse inlogmiddelen beschikbaar die u naar keuze kunt ontsluiten, met ieder hun eigen voordelen en gebruiksscenario's. Daarnaast is het mogelijk om Multi Factor Authenticatie (MFA) toe te voegen. Met de Connectis Identity Broker beheert u een keur van deze systemen vanuit een enkel beheerportaal. Deze brochure geeft een overzicht van enkele door ons ondersteunde eID's.



Protocollen
De laatste jaren is het aantal beschikbare eID's behoorlijk uitgebreid. Aan de 'achterkant' werken deze inlogmiddelen met speciale protocollen. Deze bepalen onder andere de manier waarop de verbinding met de authenticatieserver plaatsvindt, welke versleuteling wordt toegepast, en welke extra functionaliteiten beschikbaar zijn.

De Connectis Identity Broker ondersteunt drie veelgebruikte varianten:
- SAML 2.0 (Security Assertion Markup Language)
- OAuth (Open Authorization)
- OpenID

DigiD

DigiD is een eID waarmee de Nederlandse overheid en zorginstanties zoals zorgverzekeraars burgers toegang verlenen tot hun diensten. DigiD kent drie betrouwbaarheidsniveaus: Basis, Midden en Substantieel. In 2019 wordt daar een hoogste niveau aan toegevoegd: DigiD Hoog. Hoe meer zekerheid er is over de identiteit van de gebruiker, hoe meer diensten beschikbaar zijn. Niveau Basis vereist enkel een combinatie van een gebruikersnaam en wachtwoord. Midden voegt daar een controlecode via sms of DigiD-app aan toe. Bij Substantieel moeten gebruikers eenmalig de DigiD-app koppelen met hun identiteitsbewijs. Bij DigiD Hoog blijft dit ook de volgende keren noodzakelijk.

DigiD is in beheer van Logius, het overheidsorgaan dat verantwoordelijk is voor producten en diensten voor de digitale overheid.

Veel diensten vereisen op dit moment het veiligheidsniveau Midden. De sms-controle werpt met name voor minder digivaardige gebruikers een drempel op. Connectis kan die drempel wegnemen, dankzij de zogeheten 'Dynamic LoA'-technologie. Hierbij vervangt de Connectis Identity Broker de sms als tweede factor authenticatie met een cookie op het systeem van de gebruiker. De gebruiker kan zo de sms-controle overslaan, wat de toegankelijkheid vergroot.

DigiD ondersteunt dankzij het SAML-protocol single sign-on (SSO). Gebruikers krijgen na een enkele inlog toegang tot alle diensten die gebruikmaken van DigiD. Een voorwaarde is dat de omgeving ook single sign-out ondersteunt. DigiD stuurt hiervoor een signout-signaal naar de verschillende diensten. Sommige enterprisesystemen (waaronder ADFS) zijn echter ongevoelig voor dit signaal. Connectis maakt een single sign-on ondanks die beperking toch mogelijk.

eHerkenning

eHerkenning wordt ook wel gezien als de 'DigiD voor het bedrijfsleven'. eHerkenning is met name geschikt voor publieke organisaties die online diensten veilig toegankelijk willen maken voor ondernemers. Ook zelfstandigen die zijn ingeschreven bij de Kamer van Koophandel (KvK) kunnen gebruikmaken van eHerkenning.

Net zoals DigiD kent ook eHerkenning meerdere betrouwbaarheidsniveaus. Bij eHerkenning gaat het om de niveaus EH1, EH2, EH2+, EH3 en EH4, waarvan EH1 zal worden uitgefaseerd. Deze niveaus zeggen bijvoorbeeld iets over de betrouwbaarheid, de registratie en de uitgifte van het eHerkenningsmiddel. Een gebruikersnaam-wachtwoordcombinatie is bijvoorbeeld minder betrouwbaar dan een certificaat dat persoonlijk is uitgereikt.

eHerkenning maakt in bepaalde situaties gebruik van encryptie van attributen, en bepaalde attributen zijn polymorf ge-encrypt. Connectis kan de dienstverlener ontzorgen met de decryptie van deze attributen, via de Identity Broker of door middel van onze adapter.

eIDAS

Uw organisatie heeft een publieke taak? Of laat Nederlandse burgers en bedrijven inloggen met een inlogmiddel op substantieel of hoog niveau? Dan valt uw organisatie sinds 29 september 2018 onder de Europese eIDAS (Electronic Identities And Trust Services)-verordening. Dit is bijvoorbeeld het geval als u een dienstverlening aanbiedt via DigiD of eHerkenning op een substantieel of hoog niveau (zoals EH3 en EH4).

Alle burgers en bedrijven binnen de EU moeten vanaf september 2018 met een 'eIDAS-erkend' nationaal inlogmiddel kunnen inloggen bij organisaties uit de publieke sector. Hiermee wil de Europese Unie (EU) het grensoverschrijdend regelen van online zaken gemakkelijker en veiliger maken. Zo moet een Duitse verkeersovertreder met zijn nationale inlogmiddel gemakkelijk kunnen inloggen bij het Nederlandse CJIB om daar zijn boete af te handelen. Omgekeerd moet een Nederlander met een eIDAS-erkend inlogmiddel kunnen inloggen bij bijvoorbeeld de Belgische belastingdienst.

ADFS

Met ADFS (Active Directory Federation Services) als eID kunnen gebruikers die lid zijn van een Active Directory, onderdeel van Windows Server-omgevingen, zich aanmelden bij diensten van derden. Een groot voordeel van dit inlogmiddel is het gebruiksgemak. Na het inloggen op een Windows-omgeving met Active Directory is bij systemen die ADFS ondersteunen geen verdere aanmeldprocedure vereist.

Vanuit beheeroogpunt is dat centrale rechtensysteem een groot pluspunt. De rechten van een ADFS-gebruiker zijn direct gekoppeld aan de rechten toegekend in Active Directory. Wijzigt of vervalt een functie of rol van een medewerker in Active Directory, dan veranderen zijn of haar rechten in applicaties die ADFS ondersteunen automatisch mee. Het beheer van ADFS is in handen van Windows Server-systeembeheerders.

SALESFORCE

Deze eID is met name populair in zakelijke omgevingen die gebruikmaken van de bedrijfssoftware van Salesforce. Via Salesforce SSO (single sign-on) kunnen gebruikers inloggen op eigen bedrijfsapplicaties en cloudomgevingen. Salesforce beschikt over verschillende functies die de veiligheid vergroten. Zo ondersteunt de eID het gebruik van tokens in plaats van wachtwoorden. Beheerders kunnen de loginpagina toegankelijk stellen binnen de firewall van het bedrijfsnetwerk. Via Single Logout kunnen gebruikers in een keer uitloggen bij verschillende bedrijfsapplicaties. Het beheer en uitgifte van de eID is in handen van Salesforce.

GOOGLE

Ook Google stelt zijn inlogsysteem beschikbaar aan derden. Net zoals andere identityproviders biedt ook Google diverse extra mogelijkheden, zoals een herstel van een vergeten wachtwoord. Zijn gebruikers ingelogd via een apparaat, dan zijn ze automatisch via hun andere apparaten ook ingelogd. Ook maakt het systeem directe koppelingen mogelijk met Google-applicaties zoals YouTube, Gmail en Google Drive. Het systeem wordt met name gebruikt door webapplicaties gericht op consumenten, waarbij laagdrempelig inloggen prioriteit heeft. Het beheer en onderhoud van het inlogsysteem is volledig in handen van Google.

SURFCONEXT

Via de SURFconext-infrastructuur loggen studenten, docenten en onderzoekers in bij clouddiensten van derden. SURFnet heeft zijn inlogsysteem inmiddels beschikbaar gesteld voor ruim 170 clouddiensten. Ook commerciële aanbieders kunnen van het systeem gebruikmaken. SURFconext kent ruim 1,3 miljoen gebruikers. Het beheer en de uitgifte van deze eID is in handen van SURFnet.

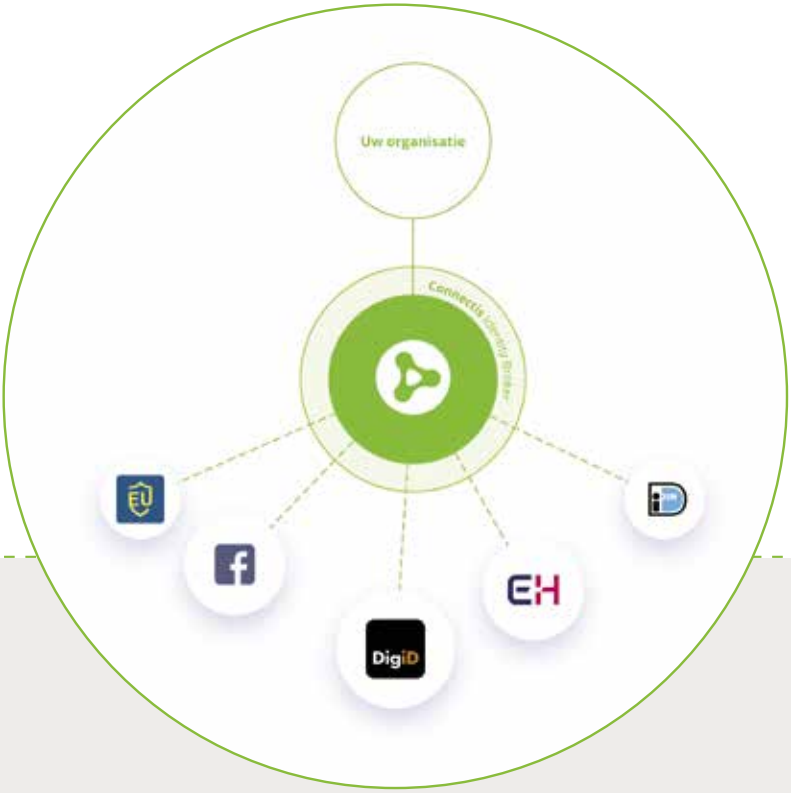
FACEBOOK

Gebruikers kunnen zich via hun Facebook-account aanmelden bij sites van derden. Het systeem wordt meestal gebruikt voor consumentenwebsites. Een voordeel is dat de website toegang krijgt tot het Facebookprofiel van de gebruiker. Dat is vaak verrijkt met demografische gegevens, zoals woonplaats en leeftijd.
Een socialmedialogin als die van Facebook is niet geschikt voor de bescherming van privacygevoelige informatie, zoals bij mijn-omgevingen in de gezondheidszorg, bij verzekeringsmaatschappijen of in het bankwezen.
Gebruik van de Facebook-login kan daarnaast problemen veroorzaken in omgevingen waarin het gebruik van social media aan banden is gelegd.

UZI-pas

Het Unieke Zorgverlener Identificatienummer (UZI) is een nummer dat gebruikt wordt om een bij het zorgproces betrokken persoon te identificeren. De gegevens van de uitgegeven passen worden opgeslagen in het UZI-register. Het UZI-register wordt beheerd door het CIBG (een uitvoeringsorganisatie van het ministerie van VWS).

Het nummer is gekoppeld aan de UZI-pas, een chipkaart die tot doel heeft om een veilige uitwisseling van patiëntgegevens te garanderen. De chipkaart wordt gebruikt voor de identificatie en authenticatie van in het BIG-register opgenomen zorgverleners en hun medewerkers. De UZI-pas wordt bijvoorbeeld gebruikt bij het elektronisch ondertekenen van een elektronisch geneesmiddelenrecept of een elektronisch verslag van een ziekenhuisopname. Naast de UZI-pas in de vorm van een smartcard geeft het UZI-register ook servercertificaten uit voor de identificatie en authenticatie van systemen.



iDIN

iDIN is een dienst van de banken waarmee consumenten zich online kunnen identificeren, inloggen en leeftijd bevestigen. In de praktijk doet het vaak dienst als identificator voor consumenten. Via iDIN kunnen zij inloggen met de vertrouwde inlogmiddelen van hun eigen bank, bij bijvoorbeeld verzekeringsmaatschappijen en webwinkels.

Met iDIN kan een klant zijn identiteit online bevestigen omdat hij zich al heeft gelegitimeerd bij het openen van een bankrekening. Het betrouwbaarheidsniveau van IDIN is substantieel. Dat komt omdat banken vanwege hun zorgvuldige aanmeldingsproces beschikken over betrouwbare identiteitsgegevens. De methode is voor een breed publiek geschikt. Vrijwel iedereen heeft wel een account voor onlinebankieren.

De iDIN simulator van Connectis maakt het mogelijk om verschillende attributen en foutcodes uit te vragen zonder dat u de connectie per test hoeft aan te passen. Dit zorgt ervoor dat het testen eenvoudiger, sneller en goedkoper wordt.

My Own IdP

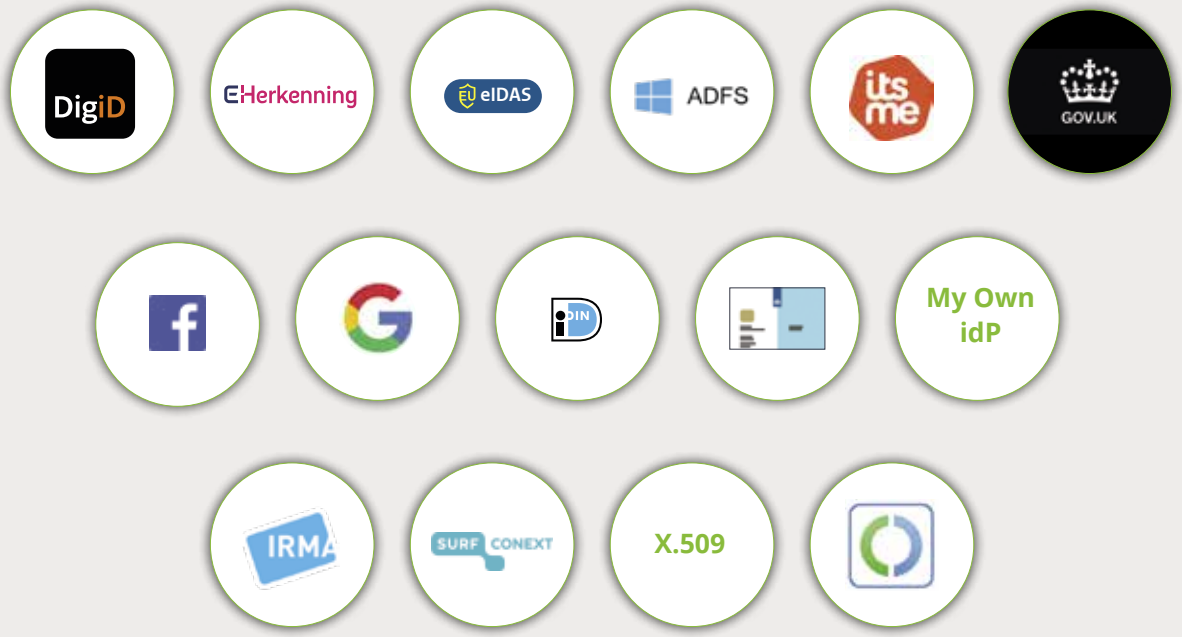
Dienstverleners kunnen kiezen voor My Own IdP wanneer zij hun eigen inlogsysteem met username-wachtwoord willen blijven gebruiken in plaats van -of naast- de eerder genoemde eID's. Met My Own IdP kunnen attributen opgeslagen worden in de Connectis attribute provider en het wachtwoord in de wachtwoorddatabase zonder afhankelijk te zijn van een externe identity provider. Een voordeel van My Own IdP via de Connectis Identity Broker is dat de (beveiligings)beheerslast die hoort bij het verwerken en opslaan van gebruikersnamen en wachtwoorden voor u tot een minimum beperkt wordt.

X.509

Een X.509-certificaat is een digitaal certificaat dat gebruikmaakt van de algemeen geaccepteerde internationale X.509-infrastructuur voor openbare-sleutelinfrastructuur (PKI). Een X.509-certificaat bevat informatie over de identiteit van de gebruiker, computer of service waaraan een certificaat is toegekend en de identiteit die het heeft uitgegeven. Een openbare sleutel die deel uitmaakt van het certificaat wordt gebruikt voor de authenticatie.

My Own IdP kan ook gecombineerd worden met een X.509 certificaat. Gebruikers kunnen dan inloggen op uw diensten met username-wachtwoord, aangevuld met een geldig geïnstalleerd X.509 certificaat.

Ontsluit ieder elektronisch identificatiemiddel (eID) via de
Connectis Identity Broker.



Vragen of interesse?

Heeft u vragen over het aansluiten van eID's via de Connectis Identity Broker, wilt u een ander eID ontsluiten of bent u geïnteresseerd in een vrijblijvend gesprek? Neem dan contact op via sales@connectis.com of bel ons op 088-012 02 80.

Connectis Online identification.
Secure. Smart. Easy.

Connectis verbindt organisaties, sectoren en landen via online identificatie-infrastructuur. Onze oplossingen maken het mogelijk dat uw klanten inloggen met DigiD, eHerkenning, Facebook, Google, eIDAS, iDIN en vele andere inlogmiddelen. Met een centrale verbinding zorgen wij ervoor dat uw klanten zo gemakkelijk en veilig mogelijk toegang krijgen tot uw online diensten. Connectis is opgericht in 2008 en sinds 2017 onderdeel van SIDN, de beheerder van het .nl-domein. Het hoofdkantoor is gevestigd in Rotterdam, en beschikt daarnaast over een vestiging in Boekarest, Roemenië en een klantenservice in Lelystad. Inmiddels maken meer dan 350 organisaties gebruik van de eHerkenningsmakelaar voor het online identificeren van meer dan 14 miljoen gebruikers. Ruim 50.000 organisaties maken gebruik van onze software en eHerkenningsmiddelen voor het veilig inloggen bij publieke en private diensten. 70% van alle transacties binnen eHerkenning lopen via de software en infrastructuur van Connectis.

Telefoon
088-012 02 22

Website
Connectis.com

Postadres
Postbus 975
3000 AZ Rotterdam

Bezoekadres
Weena 327-329
Rotterdam

1901EID1.0