

# Handleiding eIDAS

Inzicht in de gehele keten voor het inrichten  
van grensoverschrijdende dienstverlening

Versie 1.01  
25 oktober 2018



# Inleiding

Europese burgers en vertegenwoordigers van bedrijven moeten vanaf september 2018 bij alle Nederlandse organisaties in de publieke sector kunnen inloggen met hun nationale inlogmiddel. Dat hebben de EU-lidstaten in de eIDAS verordening met elkaar afgesproken. De Europese Unie wil hiermee regelen dat het makkelijker en veiliger wordt om binnen Europa online zaken te regelen. Het is de bedoeling dat alle Nederlandse publieke organisaties vóór 29 september 2018 eIDAS-proof zijn op het gebied van online toegang.

Sinds 29 september 2018 moeten producten en diensten die de gemeente via DigiD en eHerkenning aanbiedt, ook bereikbaar zijn voor burgers en ondernemers die inloggen met een erkend (genotificeerd) identificatiemiddel van een ander Europees land. Identificatiemiddelen hebben verschillende betrouwbaarheidsniveaus. De Europese Commissie heeft technische specificaties, normen en procedures vastgesteld voor de niveaus 'laag', 'substantieel' en 'hoog'.

## Huidige stand van zaken

Op dit moment (oktober 2018) zijn Duitsland en Italië de enige landen met een genotificeerd inlogmiddel. Het Italiaanse middel is op 11 september genotificeerd en zal uiterlijk 12 september 2019 geaccepteerd moeten worden. De middelen van Spanje, Estland, Luxemburg, Kroatië, België en Portugal hebben een pre-notificatie. Naar verwachting zijn ook deze landen eind 2018 genotificeerd. De actuele stand van zaken over welke inlogmiddelen genotificeerd zijn of op de nominatie hiervoor staan ziet u in het [eIDAS magazine](#) van Logius.

## Handleiding voor dienstverleners

In deze handleiding leest u welke keuzes u kunt maken en waar u rekening mee moet houden als u diensten geschikt maakt voor inloggen met een eIDAS (genotificeerd) Europees elektronisch-identificatiemiddel (eID). Aan bod komen onder andere:

- Verschil tussen BSN diensten en diensten waarvoor geen BSN vereist is
- Hoe regel ik de aansluiting om te kunnen voldoen aan de eIDAS-verordening en wat is daarvoor nodig?
- Welke identificerende gegevens ofwel attributen zijn gewenst voor de verschillende producten en diensten?
- Hoe worden de achterliggende processen ingericht?

De technische uitvoering van implementatie staat beschreven in het [Afsprakenstelsel Elektronische Toegangsdiensden](#). In het afsprakenstelsel kunt u [specifieke informatie over eIDAS](#) vinden.

## Samenstelling

Deze handleiding is samengesteld door VNG Realisatie en tot stand gekomen met medewerking van partners uit de eIDAS-keten: Gemeente Rotterdam, Gemeente Den Haag, Digidentity, PinkRoccade Local Government en SIMgroep.

# Leeswijzer

Deze handleiding biedt zowel informatie voor gemeenten die de eIDAS implementatie voor een groot deel zelf oppakken, en voor gemeenten die het overgrote deel van de implementatie aan hun leverancier(s) uitbesteden.

Voor gemeenten die hun eigen webportaal en formulieren beheren en rechtstreeks met de Herkenningsmakelaar voor eIDAS implementatie zorgen, is het raadzaam alle hoofdstukken in dit document door te nemen.

Voor gemeenten die de eIDAS implementatie oppakken met hun leverancier, zijn de hoofdstukken 1 en 3 het meest relevant om door te nemen. Hierin wordt u geholpen afwegingen te maken over de wijze waarop u uw dienstverlening wilt inrichten voor EU-burgers.

Hoofdstuk 2 over koppelvlakken is minder relevant indien uw leverancier dit voor u regelt met de Herkenningsmakelaar.

In hoofdstuk 4 zijn de introductie en paragraaf 4.2 van belang. U leest hier waar u aan moet denken bij het maken van afspraken met uw leveranciers.

In bijlage één (ver- en ontsleuteling van de BSN) zijn de eerste drie paragrafen nuttig om door te nemen omdat u als dienstverlener zelf verantwoordelijk bent voor het ontsleutelen van pseudoniemen om een BSN te verkrijgen. De technische aspecten over pseudonimisering en ontsleuteling van pseudoniemen zijn minder relevant (paragrafen 6.1.4, 6.1.5 en 6.1.6).

In de bijlage vier vindt u ook een begrippenlijst.

# Inhoudsopgave

Inleiding .....	2
Leeswijzer .....	3
Inhoudsopgave .....	4
1. Betrouwbaarheidsniveaus .....	6
1.1. Wel of geen BSN-dienst .....	6
1.2. BSN is vereist .....	7
1.3. Inlogprocedure bij een BSN-dienst .....	7
1.4. BSN niet vereist .....	7
1.5. Fysieke verstrekking aanvraag vanuit het buitenland .....	8
2. Makelaar en koppelvlakken kiezen .....	9
2.1. Makelaar kiezen .....	9
2.1.1. Randvoorwaarden gemeente .....	10
2.1.2. Randvoorwaarden Herkenningsmakelaar .....	10
2.2. Koppelvlak kiezen .....	10
2.2.1. Koppelvlak 1.11 .....	10
2.2.2. Koppelvlak 1.12 (Servicepack eIDAS) .....	11
2.2.3. Koppelvlak 1.13 .....	11
2.3. Keuze maken voor aansluiting .....	11
2.4. Beslisboom koppelvlakken .....	12
3. Benodigde attributen identificeren .....	13
3.1. Standaard (verplichte) attributen .....	13
3.2. Optionele attributen .....	13
3.3. Attributen verplicht of optioneel uitvragen .....	14
4. Aansluiten en formulieren aanpassen .....	16
4.1. Stappenplan aansluiten eIDAS .....	16
4.2. Formulieren aanpassen .....	17
4.3. Gebruik eIDAS inlogknop .....	18

4.4. Privacyverklaring .....	18
4.5. Aansluiten op de klantreis.....	18
4.6. Online afrekenen .....	18
5. Koppeling met frontoffice/web .....	19
5.1. Afspraken met leveranciers .....	19
5.2. Afhandelen van vragen.....	19
6. Bijlagen.....	20
6.1. Bijlage: Ver- en ontsleutelen pseudoniemen .....	20
6.1.1. eIDAS-identificatie met pseudoniemen .....	20
6.1.2. Pseudoniem zonder BSN ontsleutelen .....	20
6.1.3. Pseudoniem met BSN ontsleutelen .....	20
6.1.4. Formaat versleuteling.....	21
6.1.5. Ontvangst van authenticatie.....	21
6.1.6. Software voor ontsleutelen.....	21
6.2. Bijlage 2: Voorbeelden inlogprocedure .....	22
6.3. Bijlage 3: Attributenlijst .....	27
6.4. Bijlage 4: Begrippenlijst .....	28
BSNk .....	28
eIDAS-koppelpunt .....	28
Herkenningsmakelaar .....	28
Polymorf Pseudoniem (PP).....	28
Versleuteld Pseudoniem (VP).....	28
Polymorfe Identiteit (PI) en Versleutelde Identiteit (VI) .....	28
Specifiek Pseudoniem.....	28

# 1. Betrouwbaarheidsniveaus

Gemeentelijke producten en diensten waarvoor gebruikers moeten inloggen met hun Nederlands inlogmiddel, dienen sinds 29 september 2018 ook toegankelijk te zijn voor EU-burgers met hun eigen nationale inlogmiddel. De dienstverlening achter DigiD of eHerkenning moet dus óók toegankelijk zijn voor EU-burgers en -ondernemers. Er mag géén afwijkend betrouwbaarheidsniveau voor EU-burgers gelden. Bij deze diensten moet een eIDAS-inlogknop geplaatst worden<sup>1</sup>.

De gemeente is zelf verantwoordelijk voor de keuze van het betrouwbaarheidsniveau per dienst. Om het juiste betrouwbaarheidsniveau vast te stellen, zijn er een aantal factoren om rekening mee te houden. In grote lijnen spelen een rol: de aard van de dienst, de inrichting van het proces en de risico's van misbruik. Het Forum Standaardisatie heeft een [Handreiking betrouwbaarheidsniveaus](#) gepubliceerd.

In de Uitvoeringsverordening van de Europese Commissie (paragraaf 2.1) staan de technische specificaties en procedures van de betrouwbaarheidsniveaus beschreven. De volledige beschrijvingen kunt u in verschillende formaten downloaden via de website van [publications.europa.eu](http://publications.europa.eu).

Een overzicht van veelgevraagde gemeentelijke diensten met de betrouwbaarheidsniveaus kunt u vinden op de website van VNG Realisatie.

## 1.1. Wel of geen BSN-dienst

Een belangrijk onderscheid in diensten zijn diegenen waarvoor het BSN vereist is en diegenen waarvoor dat niet nodig is. Het eIDAS koppelvlak waarvan u gebruik gaat maken om aan te sluiten op de eIDAS-infrastructuur, speelt hierbij een belangrijke rol. In hoofdstuk 2 leest u hier meer over.

Voordat u aansluit op de eIDAS-infrastructuur dient u de huidige online Product- en Dienstencatalogus in te delen op basis van twee aspecten:

1. Is het BSN vereist voor het product?
2. Is fysieke aanwezigheid in Nederland noodzakelijk ten tijde van de levering van het product?

Als voor de dienstverlening geen BSN vereist is, hoeft er in principe ook geen DigiD gebruikt te worden voor het aanbieden van de dienst binnen Nederland. De aanvrager dient dan zelf de NAW- overige vereiste gegevens in te vullen bij de aanvraag. Voorbeelden hiervan zijn (bij sommige gemeenten) het aanvragen van een ja/nee sticker en het doen van een Melding Openbare Ruimte.

Bij diensten die wel een BSN vereisen wordt nu gebruik gemaakt van DigiD. Na het inloggen met DigiD door de burger wordt een BSN geleverd aan de dienstverlener (gemeente). Ook kunnen DigiD-formulieren voorgevuld worden als voor het BSN de gegevens beschikbaar zijn. Het is dan direct duidelijk wie de aanvrager is en waar het product naartoe moet worden gestuurd.

---

<sup>1</sup> Volgens de verordening moet de deur naar de dienstverlening geopend worden, maar hoeft de dienst niet daadwerkelijk verleend te worden

Voor een EU-burger die met een eIDAS middel inlogt is niet altijd een BSN beschikbaar. Voor de dienst die u aanbiedt wordt in de Dienstencatalogus aangegeven of hierbij een BSN noodzakelijk is. Uw Herkenningmakelaar stelt dit naar uw wensen voor u in. Dit houdt in dat een EU-burger zonder BSN geen gebruik kan maken van diensten waarvoor een BSN verplicht is. Voor die diensten waarvoor een BSN niet verplicht is, geldt deze beperking uiteraard niet. U zult dus onderscheid moeten maken tussen een kanaal mét BSN en één zonder BSN.

## 1.2. BSN is vereist

Als een BSN vereist is voor het product of de dienst, dan moet de EU-burger beschikken over een BSN. eIDAS kan dan voorzien in identificatie van de aanvrager.

### **Voorbeeld: aanvraag uittreksel burgerlijke stand**

Emma D. is geëmigreerd en vraagt een uittreksel burgerlijke stand aan door in te loggen met haar buitenlandse inlogmiddel. Ze wordt via eIDAS geïdentificeerd en kan meteen online betalen. Aanvragen per post en identificatie met een kopie van het paspoort is niet meer nodig.

## 1.3. Inlogprocedure bij een BSN-dienst

Als een Europese burger voor het eerst met een buitenlands identificatiemiddel op een Nederlandse website inlogt voor een BSN-dienst, controleert de RvIG op basis van de attributen die meegestuurd worden of de persoon geregistreerd staat in de Registratie Niet Ingezetenen van de Basisregistratie Personen (BRP). Als controlemiddel wordt degene die inlogt gevraagd zijn BSN in te vullen. Deze procedure vindt alléén plaats als iemand voor de eerste keer inlogt. Bij de tweede keer inloggen is de persoon al gekoppeld aan de BRP.

### **Geen match gevonden. Wat dan?**

Wordt er geen match gevonden in de BRP, dan volgt handmatige controle door de RvIG. Als de burger aangeeft een BSN te hebben, volgt er handmatige matching in de BRP. Na een aantal dagen kan de burger alsnog digitaal inloggen. Zijn er te weinig of te veel conflicterende gegevens en kan dit niet geautomatiseerd of handmatig uitgezocht worden, dan moet de persoon in kwestie persoonlijk langskomen bij een RNI-balie.

Heeft een EU-burger geen BSN, dan moet hij dit eerst aanvragen door zich in te schrijven in het Register van niet-ingezetenen (RNI). Om ingeschreven te worden in de RNI is het verplicht om fysiek te verschijnen bij één van de 19 [RNI-loketten](#). Er is géén mogelijkheid voor online inschrijving in de RNI.

## 1.4. BSN niet vereist

Als het product of de dienst verstrekt kan worden zonder BSN moet u bij uw Herkenningmakelaar aangeven welke eIDAS-identificerende gegevens ofwel attributen u nodig heeft om de dienst te kunnen verlenen. In bijlage 7.2 staat beschreven welke attributen er geleverd kunnen worden. Indien de door u vereiste gegevens niet geleverd kunnen worden via het eIDAS-koppelvlak, kunt u deze gegevens door de aanvrager handmatig toe laten voegen of in een uiterst geval overwegen te dienst niet te leveren. Meer hierover leest u in hoofdstuk drie.

## 1.5. Fysieke verstrekking aanvraag vanuit het buitenland

Een groot deel van de gemeentelijke APV-producten en diensten zijn locatie gebonden. Denk bijvoorbeeld aan het aanvragen van een container. Als de aanvrager niet in Nederland verblijft ten tijde van de levering van het product of de dienst, dan kunt u besluiten de dienst niet te verlenen. U bent bijvoorbeeld niet verplicht een afvalcontainer buiten de gemeentegrenzen te leveren. Uw gemeente mag hierbij zelf de afweging maken in hoeverre fysieke aanwezigheid en vestiging op voorhand vereist is voor aanvragen en leveren van het product of de dienst. Hierbij dient u wel te beseffen dat aanvragers in uw gemeente ook kunnen beschikken over een eIDAS-inlogmiddel en dat u dit middel wel toegang dient te verlenen. Bijvoorbeeld: Een Duitse burger kan in uw gemeente wonen en met zijn eigen Duitse middel bij u inloggen.



## 2. Makelaar en koppelvlakken kiezen

Om te voldoen aan de eIDAS verordening, dient uw organisatie toegang te krijgen tot het eIDAS-netwerk. In Nederland is ervoor gekozen aan te sluiten via het reeds bestaande eHerkennings-afsprakenstelsel. Via een van de bestaande Herkenningmakelaars kan uw organisatie worden aangesloten op het eIDAS-netwerk via de nieuwste versie van het koppelvlak (op dit moment is dat versie 1.11, volgende versies bieden meer en/of andere functionaliteit). De keuze voor Herkenningmakelaar en koppelvlak wordt in dit hoofdstuk beschreven.

### 2.1. Makelaar kiezen

Om aan te kunnen sluiten op de eIDAS-infrastructuur heeft u een Herkenningmakelaar nodig. U kunt een overzicht van de Herkenningmakelaars vinden op de [website van eHerkenning](#).

Herkenningmakelaars voldoen allemaal aan dezelfde beveiligings- en functionele eisen die door de eIDAS-verordening worden gesteld. Zij concurreren op verschillende fronten en onderscheiden zich op:

1. Prijs (eenmalig/terugkerend)
2. Standaardoplossing versus maatwerk
3. Inhoudelijke ondersteuning
4. Service Level Agreement (SLA)
5. Serviceniveau

De prijs van de aansluiting op het eIDAS-netwerk hangt af van uw wensen. Het is aan te raden om bij meerdere Herkenningmakelaars een offerte aan te vragen en in deze aanvraag zo specifiek mogelijk te zijn over uw wensen. Houd bij de selectie van een Herkenningmakelaar rekening met:

1. De eigen wensen, zoals standaardoplossing versus maatwerk en overstapmogelijkheid naar een andere Herkenningmakelaar zonder aanpassingen;
2. De prijs: eenmalige en terugkerende kosten;
3. De Service Level Agreement;
4. Het kunnen leveren van de gewenste inhoudelijke ondersteuning;
5. Bestaande relaties: direct of via een ICT-leverancier.

**TIP....**

**Ga na of uw ICT-leveranciers die betrokken zijn bij dienstverleningsprocessen ervaring hebben met een of meerdere Herkenningmakelaars. Betrek uw leveranciers bij de ontwikkeling van de online dienstverlening.**

De doorlooptijd om aan te sluiten op een koppelvlak verschilt per situatie en per makelaar. Houd in ieder geval rekening met een maand doorlooptijd voor een aansluiting.

### 2.1.1. Randvoorwaarden gemeente

Voor het aansluiten op eIDAS zijn organisatorische en technische randvoorwaarden nodig bij de gemeente.

1. Een ontwikkelaar met voldoende kennis om een SAML-verbinding tot stand te brengen.
2. Een beheerder die na implementatie de volgende acties kan uitvoeren:
  - o Certificaatwissels
  - o Aanpassen metadata
  - o Aanpassen AuthnRequests: de feitelijke inhoud van de berichten die tussen u als dienstverlener en de herkenningmakelaar worden uitgewisseld.
3. Een applicatie en/of connector die SAML-berichten kan versturen en ontvangen volgens de eIDAS-specificaties. De applicatie kan van de gemeente zelf zijn (als zij applicaties ontwikkelt), maar is vaak van een leverancier. Een connector kan geleverd worden door een Herkenningmakelaar of een derde partij.
4. Een testomgeving én een productieomgeving. Een testomgeving is echter geen verplichting voor dienstverleners vanuit het stelsel. Afhankelijk van het aansluitproces bij de makelaar kan dit wellicht wel een vereiste zijn. Een mogelijk scenario is dat de Herkenningmakelaar u aansluit op een pre-productie/acceptatie/test omgeving, welke zoveel mogelijk identiek is aan de productieomgeving. Testen kan dan plaatsvinden tijdens aansluitproces met niet-productie testmiddelen die de Herkenningmakelaar beschikbaar stelt.
5. PKI Overheid certificaten (bij koppelvak 1.12 (ServicePack eIDAS) is een certificaat met daarin het OIN van de dienstverlener vereist voor het verkrijgen van sleutels voor ontsluiting van pseudoniemen).

Het stappenplan aansluiten eIDAS in hoofdstuk 4 gaat verder op in op de stappen die u en de Herkenningmakelaar nemen tijdens het aansluitproces.

### 2.1.2. Randvoorwaarden Herkenningmakelaar

De Herkenningmakelaar levert vaak een implementatiemanager, met eventueel ondersteuning door development-specialisten.

## 2.2. Koppelvak kiezen

De ontwikkelde doelarchitectuur voor aansluiting op de eIDAS-infrastructuur is in beginsel gebaseerd op koppelvak versie 1.11. De koppelvakken 1.12 (ServicePack eIDAS) en 1.13 bieden nieuwe functionaliteit. U kunt vanaf nu uw aansluiting op het ServicePack eIDAS inregelen. Koppelvak 1.13 staat gepland om medio maart 2019 in productie te zijn. Houd de website van Logius in de gaten om te kijken wanneer welke versie in productie komt of vraag uw Herkenningmakelaar u op de hoogte te houden.

Deze nieuw ontwikkelde koppelvakken zijn doorontwikkelingen van het bestaande koppelvak voor eHerkenning dat al in gebruik is (versie 1.9). Heeft u al een aansluiting op eHerkenning? Ga dan in gesprek met uw Herkenningmakelaar. Bespreek het gewenste technische en economisch haalbare scenario om een keuze te kunnen maken voor een koppelvak dat in uw situatie het beste past.

Geleverde compatibiliteit tussen koppelvakken kunnen verschillen per Herkenningmakelaar. Denk bijvoorbeeld aan het wel of niet mogelijk maken om het eIDAS proces los te trekken van eHerkenning. Een scheiding tussen eHerkenning en eIDAS is niet in alle gevallen noodzakelijk, maar als uw Herkenningmakelaar de mogelijkheid tot ontkoppeling aanbiedt, kunt u bijvoorbeeld (tijdelijk) voor twee koppelvakaansluitingen kiezen. Dit brengt voor een korte periode extra kosten en beheer met zich mee.

### 2.2.1. Koppelvak 1.11

Bij dit koppelvak kunt u attributen vanuit Europa geleverd krijgen (zie hoofdstuk 3) en een specifiek pseudoniem van de gebruiker. eHerkenning kent voor koppelvak 1.11 géén authenticatiedienst en géén

machtigingenregister van eHerkenning en is daarmee alléén bruikbaar voor eIDAS en dan alléén voor diensten die geen BSN vereisen. In deze versie kan géén BSN meegeleverd worden. Het technisch ontwerp is zo opgezet dat een aansluiting voor eIDAS een nieuwe aansluiting voor gemeente zou betekenen. In de praktijk is er echter aanbod met de technische scheiding van eIDAS en eHerkenning en zonder deze scheiding.

### **2.2.2. Koppelvlak 1.12 (Servicepack eIDAS)**

Bij dit koppelvlak krijgt u als dienstverlener vanuit Europa de door u gevraagde attributen geleverd, plus een (specifiek of versleuteld) pseudoniem óf het BSN, indien dit beschikbaar is. Het bevat géén authenticatiedienst en géén machtigingenregister van eHerkenning en is daarmee alléén bruikbaar voor eIDAS. Kiest u voor levering van het BSN, maar wordt dit niet in de BRP of het RNI gevonden, dan wordt de authenticatie afgebroken en krijgt de gebruiker het bericht dat er geen BSN gevonden kon worden. Het koppelvlak is volgens de huidige planning beschikbaar vanaf november 2019.

### **2.2.3. Koppelvlak 1.13**

Bij dit koppelvlak kan aangegeven worden dat voor de dienst een BSN vereist is, maar u kunt ook aangeven dat u het BSN of een specifiek pseudoniem of versleuteld pseudoniem (zie hoofdstuk 6) optioneel geleverd wilt krijgen. Is het BSN bekend, dan wordt dit via het BSNK<sup>2</sup> en het BRP-koppelpunt geleverd. Als er in de BRP of het RNI geen BSN-match wordt gevonden, ontvangt u in ieder geval de gevraagde Europese attributen. Dienstverlening aan een (vertegenwoordiger van een) eenmanszaak op basis van het BSN wordt dan via dezelfde interface mogelijk. Het koppelvlak is volgens de huidige planning beschikbaar vanaf medio maart 2019.

## **2.3. Keuze maken voor aansluiting**

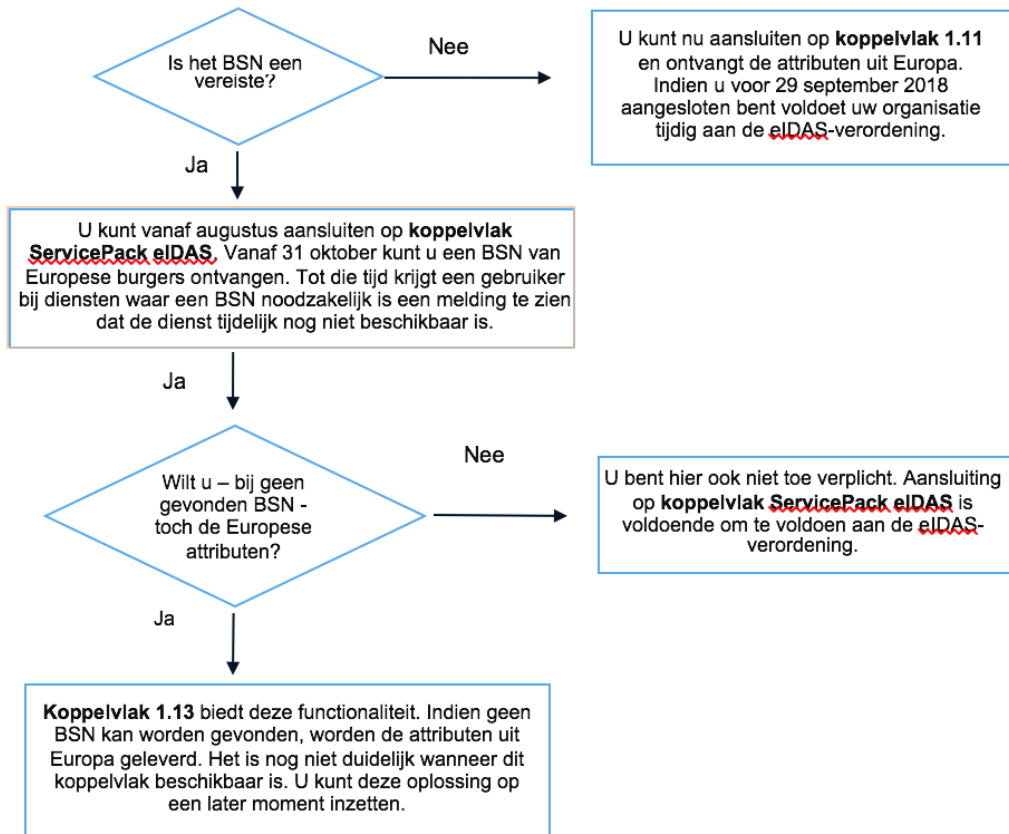
Of het voor u wenselijk is om direct aan te sluiten op de eIDAS-infrastructuur, hangt van een aantal factoren af:

1. U voldoet op de ingangsdatum van de eIDAS-verordening. U bent dan aangesloten via koppelvlak 1.11
2. Er zijn ook gemeenten die wachten op de komst van het koppelvlak 1.13 om zo in één keer aan te sluiten mét de mogelijkheid BSN's te ontvangen. Bijvoorbeeld omdat u nu (nog) geen of nauwelijks diensten aanbiedt waarvoor ingelogd hoeft te worden, of omdat er geen of nauwelijks sprake is van Europese burgers die gebruik (willen) maken van uw diensten. U dient zich wel te realiseren dat u dan niet aan de eIDAS-verordening voldoet.

---

<sup>2</sup> Een publieke voorziening die authenticatiemiddelen aan het BSN koppelt en pseudoniemen en sleutel materiaal verstrekt

## 2.4. Beslisboom koppelvlakken



	1.11	1.12 (Servicepack eIDAS)	1.13
BSN geen vereiste	Ja	Ja	Ja
BSN wel vereiste	Nee	Ja	Ja
BSN wel vereiste + Europese attributen	Nee	Nee	Ja

## 3. Benodigde attributen identificeren

Voor het leveren van diensten heeft u gegevens nodig van de EU-burger die inlogt. Via het eIDAS-koppelpunt krijgt u de door u gevraagde attributen geleverd. Heeft u geen attributen nodig, dan moet de standaard set weliswaar verplicht vanuit eIDAS aan Nederland geleverd worden, maar het eIDAS-koppelpunt geeft ze niet door aan de dienstverlener (de gemeente). Misschien heeft u voor bepaalde diensten méér gegevens nodig, een adres bijvoorbeeld. In dat geval kunt u optionele attributen uitvragen.

### 3.1. Standaard (verplichte) attributen

In alle gevallen levert het eIDAS-koppelpunt 4 attributen aan Nederland (zie bijlage 7.2) voor diensten die geleverd worden aan inwoners (natuurlijke personen) binnen de EU. Dat is een verplichting:

1. Huidige familienaam of familienamen
2. Huidige voornaam of voornamen
3. Geboortedatum
4. Uniek identificatienummer (let op: geen BSN)

Inlogmiddelen voor ondernemers zijn nog niet beschikbaar. Het Italiaanse inlogmiddel kan gebruikt worden voor zowel burgeridentificatie als inlogmiddel voor ondernemers. Dat betekent in de praktijk dat gemeenten die digitale diensten aanbieden aan bedrijven via bijvoorbeeld eHerkenning, uiterlijk 12 september 2019 ook Italiaanse inlogmiddelen toegang moeten verlenen. De standaard set attributen voor ondernemers (rechtspersonen) die vanuit eIDAS verplicht aan Nederland geleverd worden:

1. Huidige wettelijke naam
2. Pseudoniem van het unieke identificatienummer burger (vertegenwoordiger van het bedrijf)
3. Pseudoniem van het unieke identificatienummer bedrijf

### 3.2. Optionele attributen

Welke optionele attributen u kunt uitvragen, kunt u nakijken in bijlage 7.2. Het is afhankelijk van het land van herkomst welke attributen meegestuurd worden. Ook bij optionele attributen moet de burger zélf toestemming geven aan de gemeente om deze te gebruiken.

**Let op!**

- U vraagt optionele attributen altijd uit via uw Herkenningsmakelaar
- De burger bepaalt zélf of de gemeente optionele attributen mag gebruiken
- Het is mogelijk dat het land de gevraagde attributen niet kan leveren

Per dienst is het nodig te bepalen welke attributen u wilt uitvragen. Het is mede afhankelijk van het land van herkomst welke attributen meegestuurd kunnen worden.

Nadat u eIDAS-attributen geleverd krijgt bij een dienst, kunt u aanvullend het RNI bevragen. Dit is een optie als u extra validatie wilt of attributen niet geleverd kunnen worden via eIDAS, maar wel in het RNI beschikbaar zijn. Dit is echter alleen mogelijk bij een beschikbaar BSN.

### 3.3. Attributen verplicht of optioneel uitvragen

De gemeente kan een attribuut op twee manieren opvragen: verplicht of optioneel. Zijn attributen noodzakelijk om de dienst te kunnen verlenen, dan vraagt u deze uit als verplichte attributen. Zijn attributen niet noodzakelijk, maar wel gewenst voor de dienstverlening, dan vraagt u de attributen optioneel uit.

#### AANDACHTSPUNT...

**Houd rekening met het principe van data-minimalisatie uit de AVG: vraag geen onnodige attributen uit. Volstaat het op basis van geboortedatum iemands leeftijd te weten? Vraag dan bijvoorbeeld het attribuut 'ouder dan 65' uit.**

Als de burger niet instemt met het gebruik door de gemeente van attributen die u als optioneel uitvraagt, of als het land deze attributen niet kan leveren, dan slaagt de authenticatie voor de dienst toch. Bij attributen die u opvraagt als verplicht voor die dienst die u wilt leveren, wordt de authenticatie afgebroken als de burger geen consent verleent of het land de attributen niet kan leveren.

#### LET OP...

- » **Als de lidstaat een attribuut niet heeft en/of de burger geen consent verstrekt bij de door u als 'optioneel' gevraagde attributen, blijft het veld in het formulier leeg.**
- » **Vraag aan uw leverancier of deze 'vooringevulde'-velden zo geïmplementeerd zijn dat het voor de gebruiker mogelijk is hier zelf iets in te vullen, of:**
- » **Vraag om implementatie van een verplicht veld dat niet gevuld wordt vanuit het eIDAS-koppelpunt, maar dat de burger altijd zelf moet invullen. Let hierbij wel op dat dit een onbetrouwbaar gegeven is. Als "18+" van groot belang is voor een dienst, is het niet raadzaam slechts op invoer van de gebruiker te vertrouwen.**

### **Voorbeeld dienstverlening met optioneel attribuut**

#### **Wens**

De gemeente wil fysieke uittreksels toe kunnen sturen en heeft hiervoor adresgegevens nodig.

#### **Opdracht Herkenningsmakelaar**

De gemeente geeft de Herkenningsmakelaar opdracht om bij deze dienst de optionele attributen "Postcode" "Huisnummer" "Huisnummer toevoeging" "Straat" "Woonplaats" en "Provincie of staat" uit te vragen bij het eIDAS koppelpunt.

#### **Opdracht leverancier online formulier**

De gemeente geeft de leverancier van online formulieren opdracht om:

1. de eIDAS-inlogknop te plaatsen bij het de formulier van de betreffende diensten (zie hoofdstuk 4);
2. een duidelijke link bij de formulieren te plaatsen naar de privacyverklaring van de gemeente zodat de burger weet hoe de gemeente met zijn gegevens omgaat (zie hoofdstuk 4);
3. te voorzien in velden met voldoende karakters voor buitenlandse adresnotaties.

## 4. Aansluiten en formulieren aanpassen

Afhankelijk van de service die uw leverancier biedt, loopt deze alle stappen met u door en denkt met u mee over de te maken keuzes bij het aansluiten op eIDAS. Houdt in elk geval rekening met de volgende zaken:

1. Indien uw formulieren extern gehost worden: Zorg dat er een [verwerkersovereenkomst](#) is overeengekomen in het kader van de AVG.
2. Regel dat uw Herkenningsmakelaar of leverancier van portaal diensten een PKI Overheidscertificaat aanvraagt met daarin het OIN (Overheids Identificatienummer) van de organisatie. Uw bestaande PKI Overheidscertificaat is alléén geschikt voor eIDAS als er een OIN in is opgenomen. Dit certificaat heeft u nodig om pseudoniemen te kunnen ontsleutelen.
3. Vraag naar de implicaties van het aansluiten op het koppelvlak van uw keuze: wat zijn de kosten en welke gevolgen heeft implementatie voor de workflow?
4. Maak afspraken over het testen van de aansluiting met de Herkenningsmakelaar en de eIDAS-berichtenservice. Testen met inlogmiddelen is geen verplichting. Elke Herkenningsmakelaar of marktpartij heeft een eigen testprocedure. Een van de mogelijkheden is testen via een pre-productieomgeving, eventueel met testmiddelen. Op het afsprakenstelsel elektronische toegang zijn de [testen](#) te vinden die van toepassing zijn.

### 4.1. Stappenplan aansluiten eIDAS

U of uw leverancier doorloopt met uw Herkenningsmakelaar een aantal stappen om aan te sluiten op eIDAS. De werkwijze en volgorde kan per Herkenningsmakelaar verschillen. Onderstaande stappen zijn een voorbeeld van wat u kunt verwachten.

1. U gebruikt een SAML-protocol, volgens de specificatie voor koppelvlak 1.11 en/of een nieuwere release.
2. U stuurt test-metadata door naar de Herkenningsmakelaar.
3. Uw Herkenningsmakelaar controleert de metadata en geeft aan u door of er veranderingen nodig zijn. Voldoen de metadata aan de specificatie, dan wordt deze ingeladen. De Herkenningsmakelaar stuurt dan de eigen test-metadata naar u toe en publiceert een test-dienst.
4. Nadat zowel u als de Herkenningsmakelaar de metadata hebben ingeladen, kunt u een Authentication Request (AuthnRequest) naar de Herkenningsmakelaar sturen.
  - a) Voldoet deze niet aan de specificatie, dan wordt er een foutmelding getoond. Neem dan contact op met de Herkenningsmakelaar om de oorzaak van de foutmelding te krijgen.
  - b) Voldoet deze wel aan de specificatie, dan wordt de eIDAS Berichtenservice getoond. De flow voor inloggen kan doorgelopen worden en er kan een response ontvangen worden. Is de AuthnRequest succesvol, dan ontvangt u na het doorlopen van de flow een response met de benodigde (gevraagde) attributen.
5. Kan uw applicatie de response verwerken, dan kunt u testen uitvoeren.
6. Na de testperiode wordt de koppeling in productie tot stand gebracht. Dit is ook het moment waarop u de wensen voor de naamgeving van de dienst kunt doorgeven zoals die gebruikt wordt in de Dienstencatalogus. Hier moet een passende naam voor worden gekozen. Deze kan voor eIDAS generiek zijn zoals bijvoorbeeld 'eIDAS for the Municipality of The Hague'.
7. U levert de productie-metadata aan bij de makelaar. Deze levert op zijn beurt de eigen productie-metadata bij u aan zodat u op fouten kunt controleren. De metadata worden dan door beide partijen ingeladen.



8. U stuurt nu een AuthnRequest in de productieomgeving om de koppeling te testen. Bij een succesvolle flow is de implementatie compleet. De beheerders kunnen het nu overnemen.

Belangrijke specificaties zijn:

1. [Interface-specificaties](#) Dienstverlener - Herkenningsmakelaar – specificatie voor de request en response
2. [Dienstverlener metadata voor Herkenningsmakelaar](#) – specificatie voor de metadata
3. [Service catalog](#) – specificatie voor diensten

## 4.2. Formulieren aanpassen

Afhankelijk van wie uw website beheert (uzelf of een leverancier) kunt u ervoor kiezen om uw portaal- of formulierenleverancier contact op te laten nemen met uw Herkenningsmakelaar zodat zij in samenspraak uw formulieren geschikt maken voor eIDAS. Houdt in ieder geval rekening met het volgende:

1. Denk er over na of u de formulieren wilt (laten) vertalen. Dat is nu nog geen verplichting, maar kan een overweging voor de klantvriendelijkheid zijn. Het Afsprakenstelsel Elektronische Dienstverlening ondersteunt een aanbod van diensten in meerdere talen (naam en beschrijving van de dienst, URL van de privacyverklaring etc.). De attributen bevatten bij alle eIDAS koppelvlakken ook een landcode waarmee bij inloggen herkend kan worden uit welk land het inlogmiddel afkomstig is. Het is uiteraard niet aantoonbaar dat degene die inlogt de nationaliteit van dit land heeft. Iedereen kan immers inloggen met een identificatiemiddel van een land naar keuze (mits dit gefaciliteerd wordt door het betreffende land).
2. Er moeten standaardattributen van het Afsprakenstelsel gebruikt worden.
3. Het authenticatiemiddel dient aan het formulier toegevoegd te worden.
4. Bij elk formulier dient de eIDAS-knop toegevoegd te worden (of bij ruimtegebrek eventueel een teksthyperlink).
5. Digitale formulieren moeten aangepast worden aan de verschillende adresnotaties van EU-lidstaten.
6. Adresgegevens moeten aanpasbaar zijn door de aanvrager.

### Voorbeeld aanpassing adresgegevens in het formulier

Via inloggen met DigiD worden alle velden voorgevuld met gegevens uit de BRP. Maar wat nu in de volgende situatie: Heinrich H. heeft een internationaal bewijs nodig van in leven zijn (een attestatie de vita). De gemeente heeft zijn adres nodig om het toe te kunnen sturen. Heinrich is echter onlangs verhuisd binnen Duitsland maar heeft dat niet in Nederland doorgegeven. Hij logt in met zijn Duitse inlogmiddel, en omdat zijn BSN in dit geval bekend is binnen de RNI wordt het adres meegeleverd. Het oude adres van Heinrich verschijnt nu voorgevuld op het formulier. De leverancier heeft er in dit voorbeeld voor gekozen de voorgevulde velden niet aanpasbaar te maken. Heinrich moet nu dus zélf zijn nieuwe adres door kunnen geven aan de gemeente. Een extra veld *'Kloppen uw adresgegevens niet? Vul dan hier uw huidige adres in'*, is nodig om de dienst goed te kunnen verlenen.

### 4.3. Gebruik eIDAS inlogknop

Europese burgers die van uw online dienst gebruik willen maken, kunnen niet inloggen via de DigiD-knop of de eHerkenning-knop. Bij diensten waarvoor ingelogd moet worden door een EU-burger, zult u naast de gebruikelijke inlogknoppen ook een eIDAS-knop moeten plaatsen. Als u gebruik maakt van een knop dan is de vormgeving van deze knop gestandaardiseerd door Logius. Gebruik van deze standaard is niet verplicht gesteld, maar bij zoveel mogelijk eenheid heeft de Europese burger wel meer duidelijkheid. Bij ruimtegebrek behoort een tekst-hyperlink tot de mogelijkheden.



De eIDAS login-knop kunt u in verschillende formaten downloaden via de [eIDAS communicatietoolkit](#) van Logius. Deze communicatietoolkit bevat het beeldmerk in verschillende formaten (150, 300, 500 px) en indelingen (CMYK en RGB, PNG, EPS, AI).

### 4.4. Privacyverklaring

Bij het aanbieden van diensten dient u ook een privacyverklaring te publiceren. Op de website van VNG Realisatie vindt u een [Handreiking privacyverklaring voor gemeentelijke websites](#).

### 4.5. Aansluiten op de klantreis

Het geschikt maken van diensten en formulieren voor eIDAS-inlogmiddelen, is een goede aanleiding de gebruiksvriendelijkheid en toegankelijkheid van de website onder de loep te nemen. Biedt u elke dienst tweetalig aan?<sup>3</sup> Staat de eIDAS-inlogknop op een logische plek voor bezoekers? Is voor de bezoeker duidelijk wat de mogelijkheden zijn na inloggen? Zijn de diensten beschreven in begrijpelijke taal? In de [database klantreizen](#) vindt u voorbeelden van gemeenten die voor uiteenlopende diensten klantreizen gemaakt hebben met een inventarisatie van de pijn- en verbeterpunten. Daarnaast vindt u in het [eIDAS Magazine](#) van Logius praktische ondersteuningsmiddelen rond de communicatie over eIDAS voor gebruikers.

### 4.6. Online afrekenen

Als er voor een online dienst betaald moet worden, houdt er dan rekening mee dat de Europese burger deze dienst óók bij u moet kunnen afrekenen. Dit betekent dat u naast bijvoorbeeld een iDeal-betaling ook betaling met bijvoorbeeld creditcard of PayPal aan moet bieden. Zorg er dan voor dat uw backoffice hierop ingericht is en dat u de betreffende betaalmiddelen activeert in uw internetkassa. Een voorbeeld van een inlogprocedure vindt u in bijlage 7.1 van dit document.

---

<sup>3</sup> Tweetalig aanbieden van online diensten is niet verplicht vanuit de eIDAS verordening, maar straks wel bij invoering van een andere EU-verordening: Single Digital Gateway.

## 5. Koppeling met frontoffice/web

Implementatie van eIDAS heeft gevolgen voor de inrichting van uw webportaal en systemen. Denk aan het onderscheid in diensten met en zonder BSN en de categorisering naar hun betrouwbaarheidsniveau. Daarnaast moeten formulieren voor EU-burgers geschikt gemaakt worden voor eIDAS-authenticatie.

### 5.1. Afspraken met leveranciers

Leveranciers van uw online formulieren en zaaksystemen krijgen allemaal te maken met de invoering van eIDAS en de koppeling met de eIDAS-infrastructuur. Inventariseer daarom tijdig met welke leveranciers u hierover afspraken moet maken.

#### **Voorbeeldcasus aanpassingen in de keten**

Stel, u wilt dienstverlening bieden die zonder BSN kan worden afgenomen. In dat geval wilt u Europese attributen uitvragen, zoals buitenlandse adresgegevens. Het eerste waar u dan voor moet zorgen is dat de pre-fill functie van het formulier de attributen toont. De volgende stap is dat u de gegevens kan verwerken in uw zaakstelsel en zakenmagazijn. Werkt uw stelsel volgens de RGBZ en RSGB standaarden, dan zal dit weinig problemen opleveren. U moet dit echter wel valideren bij uw leveranciers. Ook de verdere uitwisseling van gegevens na het zakenmagazijn, (denk bijvoorbeeld aan een CRM) kan leiden tot aanpassingen in de keten.

Onderstaande punten bieden een handvat om het gesprek met uw leveranciers aan te gaan.

1. Vraagt u aanvullende attributen uit? Dan worden de formulieren daarmee uitgebreid en moet het zaakstelsel deze kunnen accepteren, inclusief afwijkende notaties (denk aan adresvelden).
2. Worden in de huidige situatie alleen formulieren geaccepteerd als het BSN bekend is? Of kunnen ook formulieren voor diensten zonder BSN geregistreerd worden?
3. Is de inrichting van het gegevensmodel gebaseerd op StUF-koppelingen? Dan moet er hoogstwaarschijnlijk ruimte komen voor nieuwe attributen. Hiervoor past –waar nodig– VNG Realisatie het Referentiemodel Stelsel van Gemeentelijke Basisgegevens (RSGB) en bijbehorende standaarden binnen de GEMMA aan.
4. Houd er rekening mee dat ook in uw gegevensmagazijn aanpassingen doorgevoerd moeten worden.
5. Aansluiting op het eIDAS-koppelvlak vereist SAML (Security Assertion Markup Language). Dit is een randvoorwaarde om aanpassingen conform de eIDAS-infrastructuur door te kunnen voeren. Veel gemeenten maken nu gebruik van het CGI-koppelvlak. Voor DigiD kan dit worden gehandhaafd. Voor eIDAS is ontwikkeling van een SAML-implementatie nodig, voor gemeenten die dit nog niet hebben.

### 5.2. Afhandelen van vragen

Er zijn veel dienstverleners die op eIDAS aan moeten sluiten, er zijn verschillende Herkenningmakelaars die daarbij helpen en er zijn diverse organisaties die componenten leveren in de eIDAS keten. Dat maakt dat ook gebruikersondersteuning in een keten van organisaties georganiseerd moet worden. In het [eIDAS Magazine](#) van Logius vindt u praktische tips en ondersteuning rond communicatie over eIDAS.

## 6. Bijlagen

### 6.1. Bijlage: Ver- en ontsleutelen pseudoniemen

Bij de startarchitectuur van eIDAS is uitgegaan van privacy by design. Dat betekent dat op geen enkele manier een BSN verstrekt wordt aan een andere lidstaat. Als u diensten aanbiedt waarvoor u authenticatie of het BSN nodig heeft, krijgt u te maken met (polymorfe) pseudoniemen en het ontsleutelen daarvan. Het ontsleutelen moet in het domein van de dienstverlener (de gemeente) gedaan worden. De Herkenningmakelaar kan u helpen met coderen of met een applicatie waarmee u pseudoniemen kunt ontsleutelen.

#### 6.1.1. eIDAS-identificatie met pseudoniemen

Elke EU-burger krijgt van het land waar hij woont een pseudoniem op basis van zijn identiteit toegewezen. De eIDAS berichtenservice ontvangt dit pseudoniem. Zodra een bezoeker een dienst afneemt waarvoor BSN vereist is, koppelt de RvIG (Rijksdienst voor Identiteitsgegevens) dit pseudoniem aan het BSN. Hierdoor ontstaat een pseudoniem binnen het Register voor Niet Ingezetenen (RNI) waarmee de persoon altijd juist geïdentificeerd kan worden.

Het matchen van identiteitsgegevens aan het BSN gebeurt vanaf 31 oktober 2018 automatisch via een speciaal daarvoor ingericht BRP-koppelpunt.

Op dit moment is hierop één uitzondering: een Duits burger die in Duitsland een nieuw identiteitsbewijs ontvangt, krijgt een nieuw persistent pseudoniem toegewezen (zie bijlage 7.2). Met dit nieuwe, persistente pseudoniem is deze burger wel te koppelen aan een BSN maar als hij geen BSN heeft, kan de gemeente dit nieuwe pseudoniem niet relateren aan het vorige dat bij zijn vorige identiteitsbewijs hoorde. Deze burger komt dus twee keer voor met twee verschillende persistente pseudoniemen in de registratie van de gemeente. Voor de gemeente hoeft dit geen probleem te zijn. De burger kan echter niet meer zien welke zaken hij met zijn vorige persistente pseudoniem heeft gedaan.

#### 6.1.2. Pseudoniem zonder BSN ontsleutelen

De ontsleuteling van een pseudoniem kan weliswaar technisch plaatsvinden bij een derde partij, maar verantwoordelijkheid hiervan ligt bij de dienstverlener. In geval van uitbesteding is een sluitende juridische overeenkomst dan ook een voorwaarde. Een pseudoniem ontsleutelen gaat in een aantal stappen:

1. U heeft allereerst een PKlo (overheidscertificaat) nodig met daarin opgenomen het Overheids Identificatienummer (OIN). Een bestaand certificaat is alleen bruikbaar voor eIDAS als het OIN hierin is opgenomen. Het OIN is gebonden aan de dienstverlener, niet aan een leverancier.
2. Uw Herkenningmakelaar vraagt met het certificaat de (decryptie)sleutels op bij het BSNk.
3. Via uw PKlo-certificaat krijgt u vervolgens twee sleutels versleuteld aangeleverd.
4. U kunt deze sleutels ontsleutelen met de private key die bij uw PKlo-certificaat hoort.
5. Nu heeft u de sleutels om het pseudoniem te ontsleutelen. Dit pseudoniem is uniek voor uw organisatie. Het is een zogeheten *Versleuteld Pseudoniem* waaruit u géén BSN kunt afleiden.
6. U kunt uit het *Versleuteld Pseudoniem* wel een *Persistent Pseudoniem*. Derden kunnen de identiteit nooit afleiden uit de kenmerken van een Persistent Pseudoniem.

#### 6.1.3. Pseudoniem met BSN ontsleutelen

Heeft u het BSN van de gebruiker nodig voor de dienst, dan moet uw OIN voorkomen op de Autorisatielijst BSN. Deze lijst wordt onder verantwoordelijkheid van het ministerie van BZK opgesteld. Het pseudoniem ontvangt u dan in de vorm van een *Versleutelde Identiteit* waaruit u het BSN kunt afleiden. Voor het

ontsleutelen van een Versleutelde Identiteit ontvangt u naast de decryptiesleutel nóg een sleutel om het BSN te ontsleutelen.

#### 6.1.4. Formaat versleuteling

De versleuteling van pseudoniemen heeft een standaard vorm: het [Elgamal-encryptiesysteem](#). Voor ontsleuteling zijn generieke libraries en tools beschikbaar.

#### 6.1.5. Ontvangst van authenticatie

Bij ontvangst van een pseudoniem of identiteit, bevat de ontvangen SAML Assertion een of meer 'EncryptedID' elementen. Na afhandeling van het SAML-bericht bevat deze verklaring een Versleuteld Pseudoniem (VP) of een Versleutelde Identiteit (VI). Deze VI of VP moet ontsleuteld (decrypted) worden, om respectievelijk het persistent pseudoniem of BSN of van de gebruiker te verkrijgen.

Een VI of VP is ondertekend om de integriteit te waarborgen. Deze ondertekening hoort bij ontvangst gevalideerd te worden. Deze validatie kan met een algemene publieke sleutel die in de BSNk metadata wordt gepubliceerd en met de eigen, specifieke sleutels van de dienstverlener worden gevalideerd.

De ontsleuteling van een Versleuteld Pseudoniem en Versleutelde Identiteit staat formeel beschreven in het Polymorphic Encryption and Pseudonymisation (*PEP*) paper. Op een VP is algoritme 22 van toepassing. Op een VI is algoritme 21 (pag. 43) van toepassing.

In het afsprakenstelsel elektronische toegang staat de technische structuur van een [Versleuteld Pseudoniem en een Versleutelde Identiteit](#) beschreven.

Veel cryptografische software ondersteunt tegenwoordig de benodigde Elliptische Curve Cryptografie met de *BrainpoolP320r1 curve* en het verwerken van zogeheten *ASN.1 notatie*. Met behulp van dergelijke software zijn de hierboven genoemde algoritmen en structuren vrij eenvoudig te implementeren.

#### 6.1.6. Software voor ontsleutelen

Om pseudoniemen te kunnen ontsleutelen heeft u software nodig. Uw Herkenningsmakelaar kan deze eventueel leveren. U zult zelf voor ontsleuteling moeten zorgen, de Herkenningsmakelaar is niet gerechtigd BSN's in te zien. Op dit moment zijn er op basis van de beschikbare algoritmes (zie 6.5), twee voorbeeldimplementaties in open source beschikbaar:

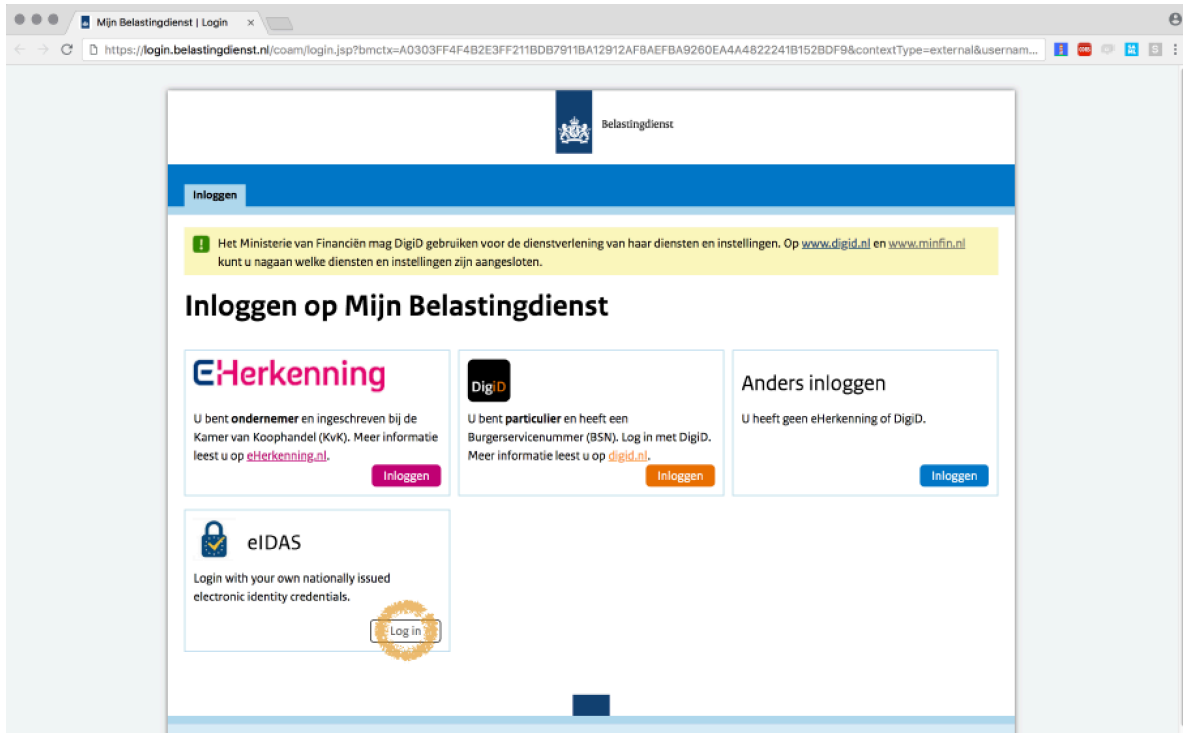
1. Java – maakt gebruik van de [BouncyCastle library](#) voor de onderliggende cryptografie
2. Ruby – maakt gebruik van de [openssl library](#) voor de onderliggende cryptografie

VNG heeft het verzoek ingediend bij het ministerie van BZK om de ontsleutelssoftware in de meest gangbare talen beschikbaar te stellen, te onderhouden en beheren. Houdt voor de stand van zaken de [eIDAS-pagina](#) op de website van VNG in de gaten.

## 6.2. Bijlage 2: Voorbeelden inlogprocedure

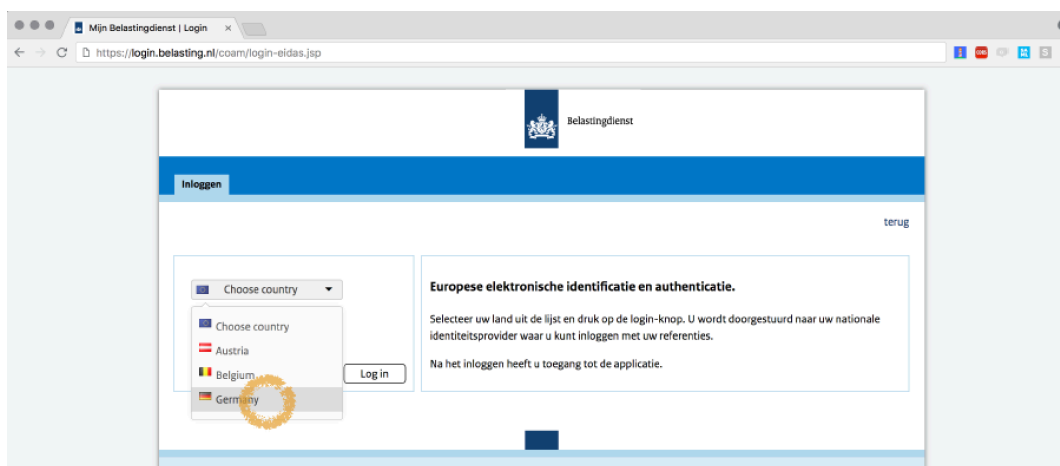
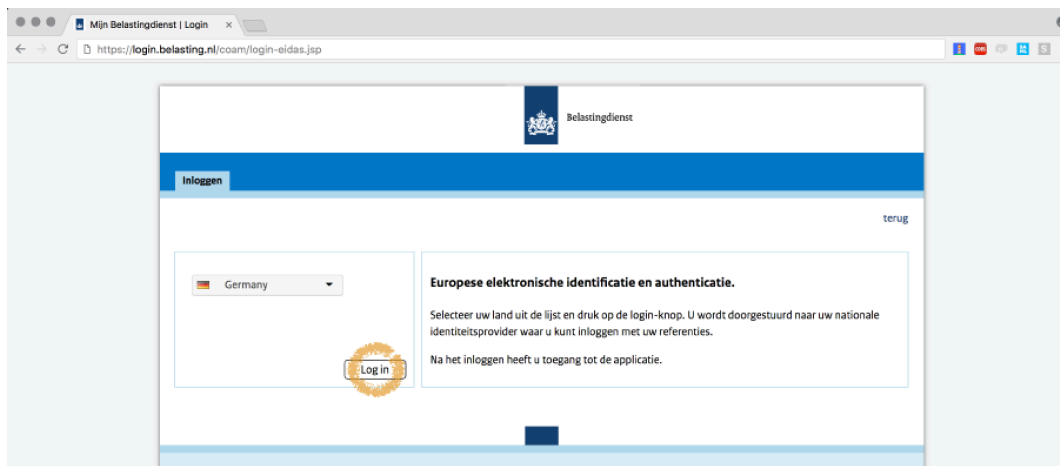
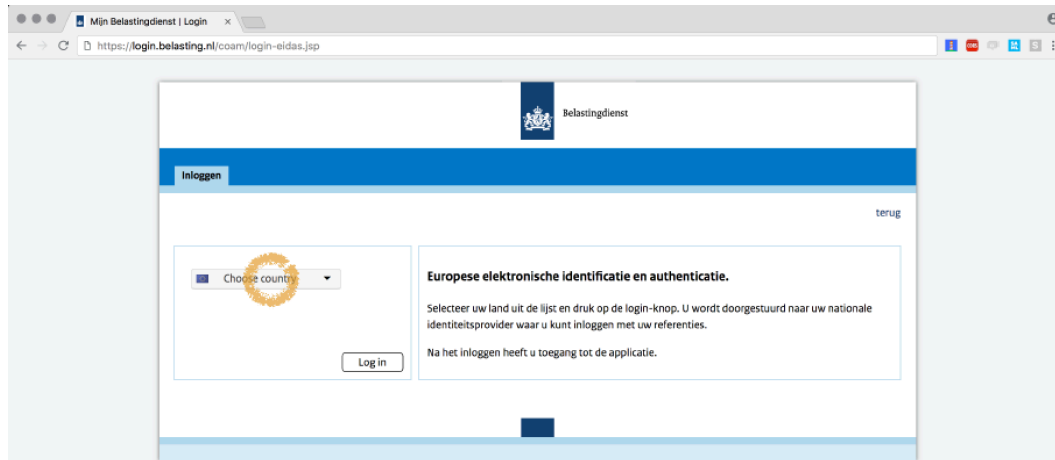
Voorbeeld van de inlogprocedure van een Duitse burger bij de Belastingdienst.

*Stap 1: Inlogmiddel kiezen. (NB. De inlogknop wordt straks vervangen door de officiële eIDAS-inlogknop (hoofdstuk 4.3))*

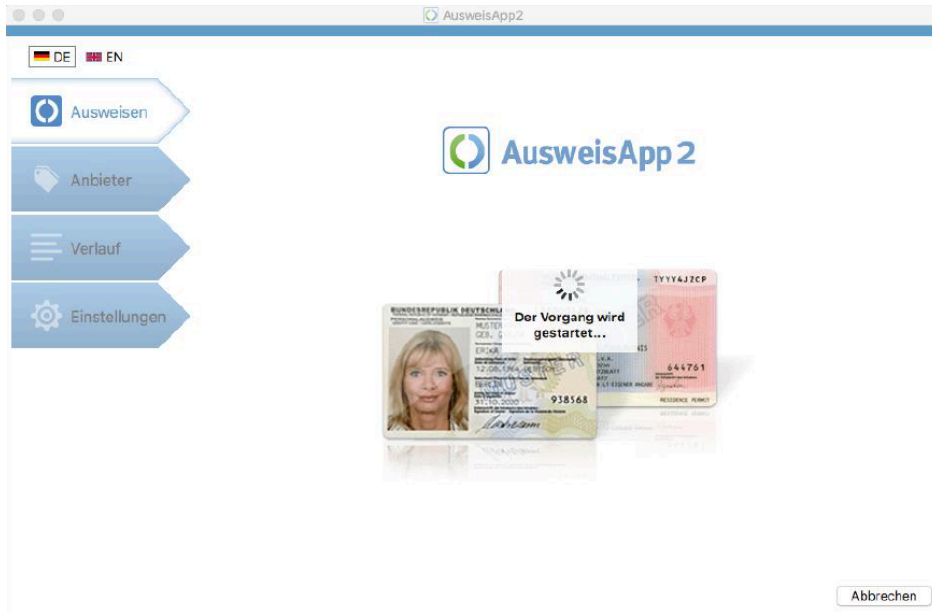


The screenshot shows the login page of the Dutch tax authority (Belastingdienst). The page title is "Mijn Belastingdienst | Login". The URL in the browser address bar is <https://login.belastingdienst.nl/coam/login.jsp?bmctx=A0303FF4F4B2E3FF211BDB7911BA12912AF8AEFBA9260EA4A4622241B152BDF9&contextType=external&usernam...>. The page features a blue header with the "Belastingdienst" logo and the word "Inloggen". A yellow banner at the top contains a message: "Het Ministerie van Financiën mag DigiD gebruiken voor de dienstverlening van haar diensten en instellingen. Op [www.digid.nl](http://www.digid.nl) en [www.minfin.nl](http://www.minfin.nl) kunt u nagaan welke diensten en instellingen zijn aangesloten." Below this, the main heading is "Inloggen op Mijn Belastingdienst". There are three main login options: 1. "eHerkenning" (e-Recognition) for entrepreneurs, with a pink "Inloggen" button. 2. "DigiD" for individuals, with an orange "Inloggen" button. 3. "Anders inloggen" (Other login), with a blue "Inloggen" button. At the bottom, there is an "eIDAS" section with a "Log in" button.

Stap 2: Selecteren van het land waarvan het inlogmiddel afkomstig is

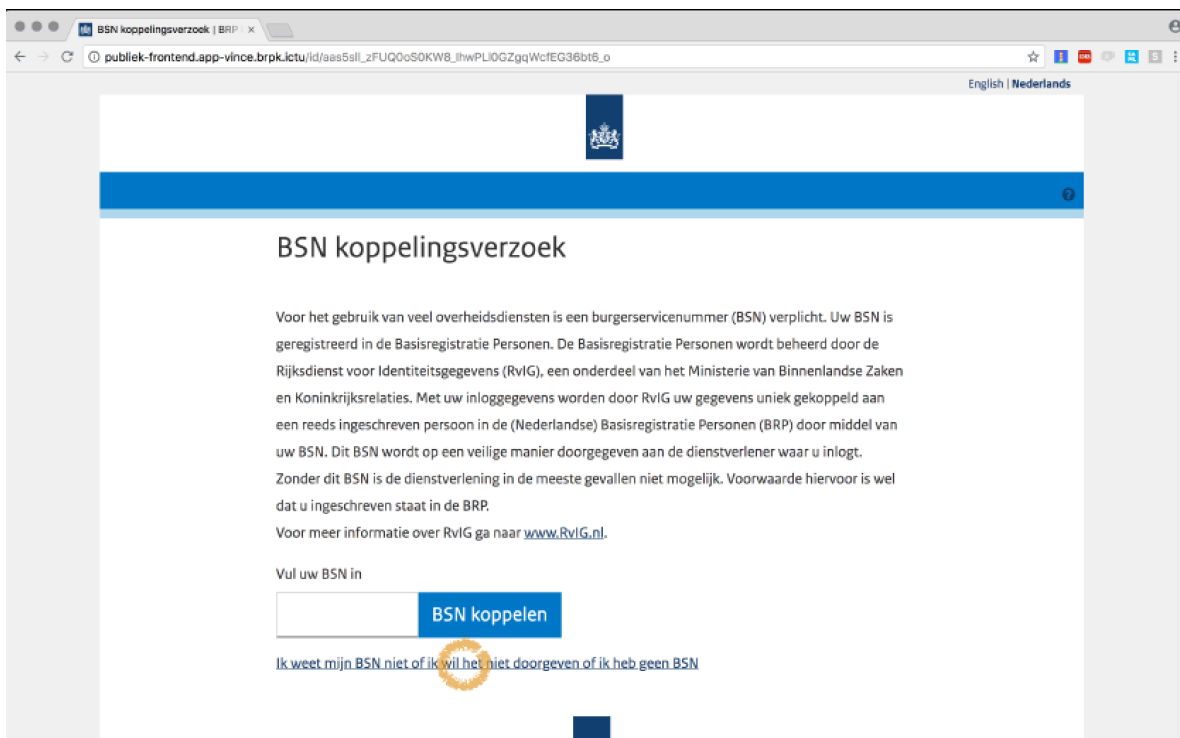
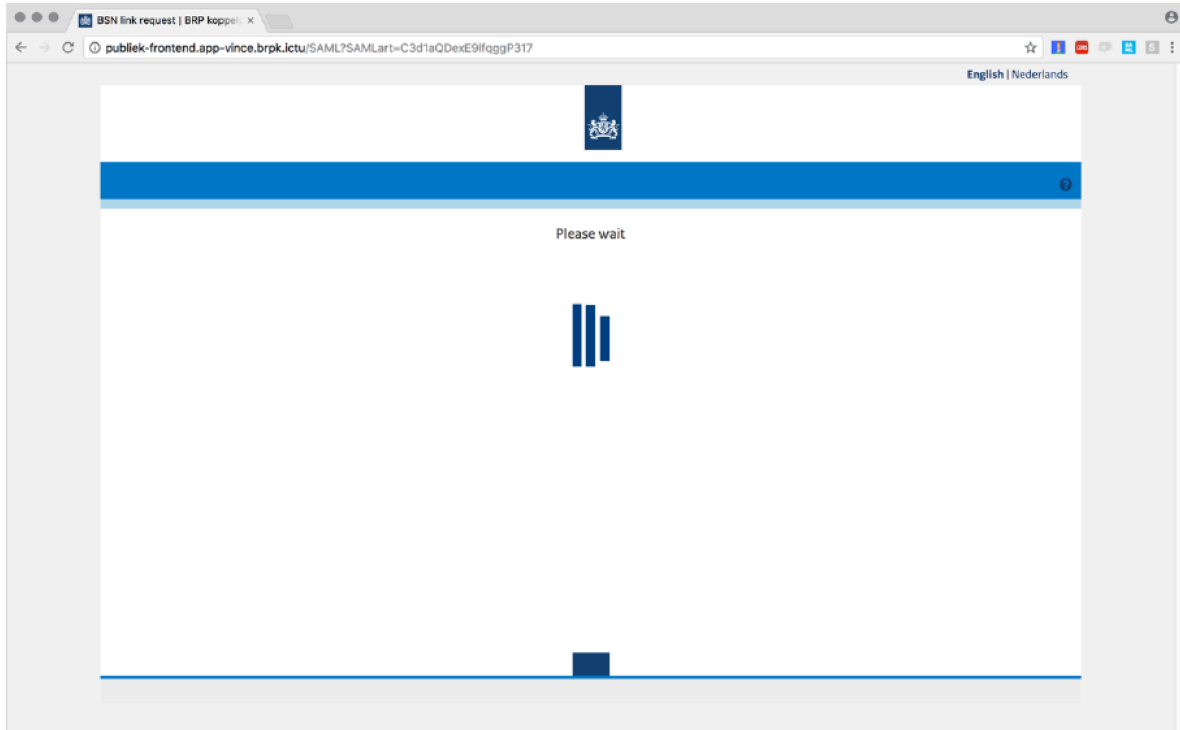


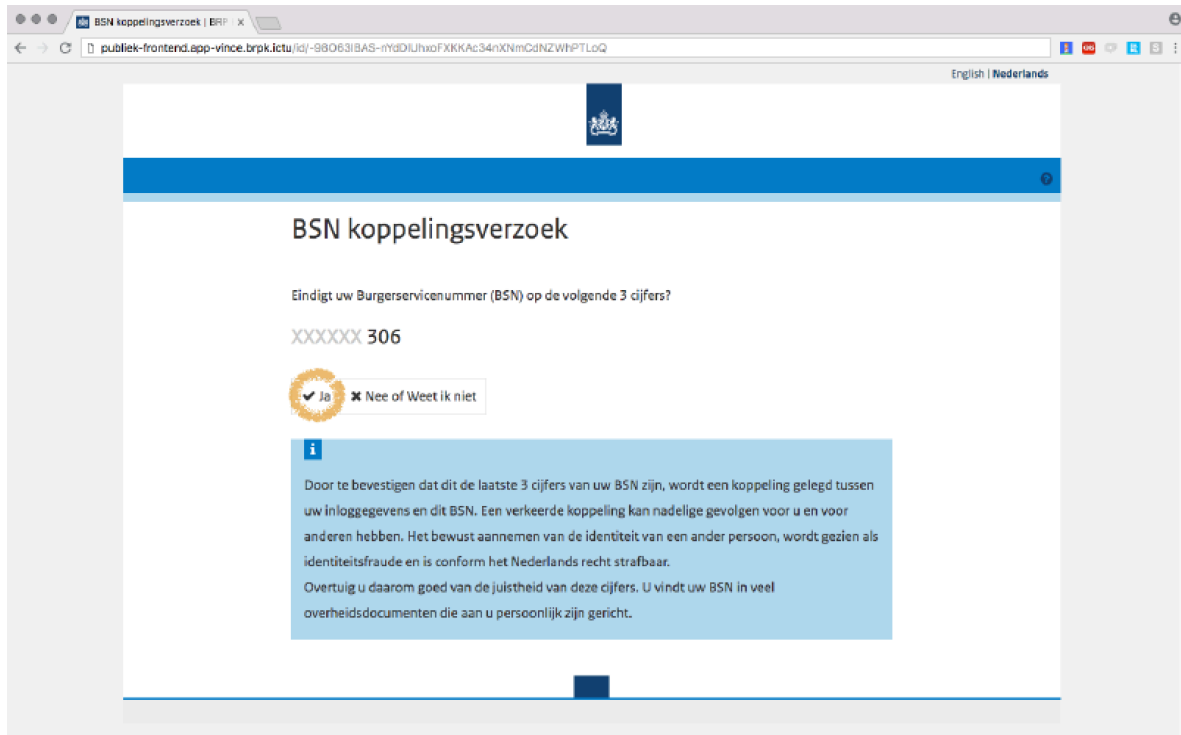
Stap 3: De burger wordt doorgestuurd naar de Nationale inlogprovider. Hier wordt vermeld dat de instantie waarbij hij inlogt (Belastingdienst) moet voldoen aan regelgeving inzake gegevensbescherming. Ook staan de gegevens vermeld die de Belastingdienst nodig heeft om de dienst te kunnen verlenen en dat de burger optionele gegevens kan deselecteren (uitvinken).



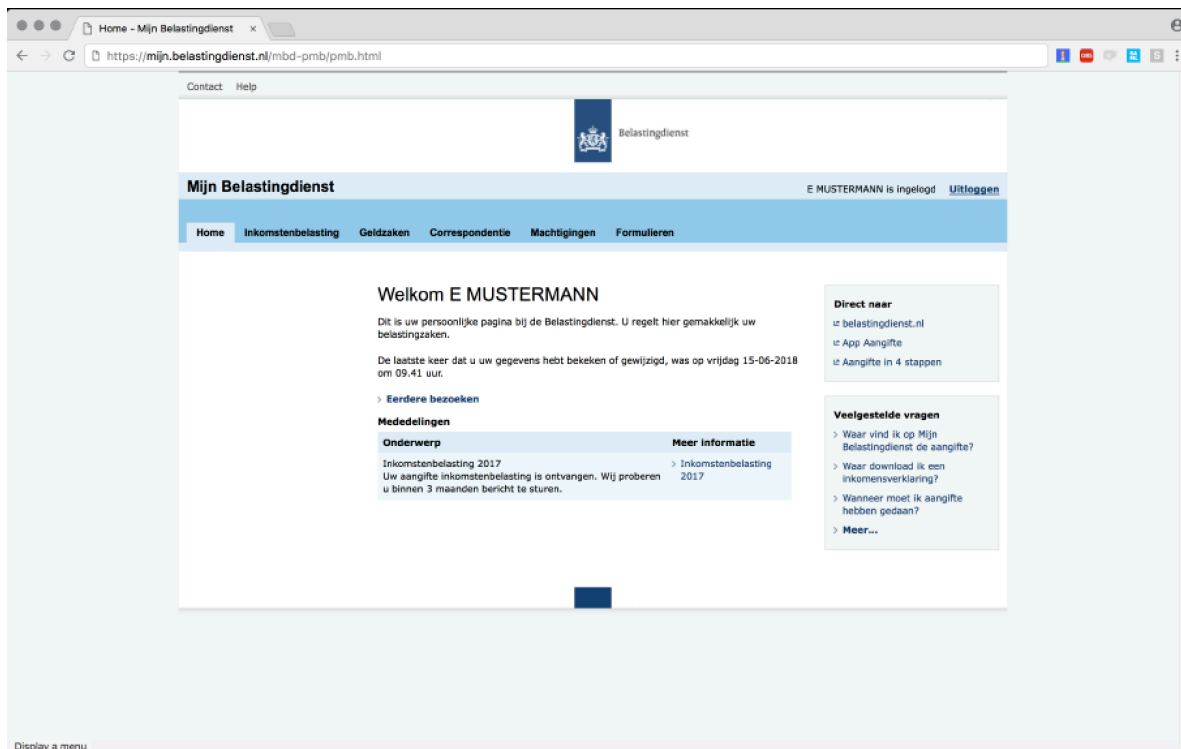


Stap 4: Als voor de dienst een BSN vereist is, wordt na een akkoord bij de Nationale inlogprovider, de burger verbonden met een portaal van de Rijksoverheid (RvIG). Hier wordt gevraagd om ter controle het BSN in te vullen. (Zie hoofdstuk 1.3). Is er geen BSN nodig voor de dienst, dan wordt deze stap overgeslagen.





Stap 5: De burger belandt op de persoonlijke pagina van de Belastingdienst.



### 6.3. Bijlage 3: Attributenlijst

Attributen met de toevoeging *verplicht* worden altijd vanuit eIDAS aan Nederland geleverd, maar ze worden alleen aan u als gemeente geleverd als u zelf aangeeft deze attributen vanuit Europa te willen ontvangen.

<b>Natuurlijke personen</b>
<b>PseudoID</b> (verplicht)
<b>Voorna(a)men</b> (verplicht)
Initialen
<b>Voorvoegsel</b> (verplicht indien van toepassing)
<b>Achternaam</b> (verplicht)
Naam bij geboorte
Voornaam in ander alfabet
Achternaam in ander alfabet
Voornaam bij geboorte in ander alfabet
Achternaam bij geboorte in ander alfabet
<b>Geboortedatum</b> (verplicht)
Ouder dan 18
Ouder dan 16
Ouder dan 12
Ouder dan 65
Geboorteplaats
Geslacht
<b>Niet natuurlijke personen</b>
<b>PseudoID</b> (verplicht)
<b>Bedrijfsnaam</b> (verplicht)
Bedrijfsnaam intermediair
Bedrijfsnaam in ander alfabet
BTW-nummer
Fiscaal referentienummer
KvK code
<b>Legal Entity Identifier</b> (verplicht)
Economic Operator Registration and Identification nr.

System for Exchange of Excise Data nummer
Standard Industrial Classification nummer
<b>Generiek</b>
Postcode
Huisnummer
Huisnummer toevoeging
Postbus
Straat
Huisnummer of identificatie
Naam van gebouw
Wijk
Woonplaats
Provincie of staat
Landcode
Postcode van de vertegenwoordigde
Huisnummer van de vertegenwoordigde
Huisnummer toevoeging van de vertegenwoordigde
Postbus van de vertegenwoordigde
Straat van de vertegenwoordigde
Huisnummer of andere identificatie van de vertegenwoordigde
Naam van het gebouw van de vertegenwoordigde
Wijk van de vertegenwoordigde
Woonplaats van de vertegenwoordigde
Provincie of staat van de vertegenwoordigde
Landcode van de vertegenwoordigde

## 6.4. Bijlage 4: Begrippenlijst

**BRP- koppelpunt** – een centrale voorziening die ervoor zorgt dat als een Europese burger, die al geregistreerd staat in de BRP, met zijn genotificeerde inlogmiddel inlogt bij een Nederlandse publieke organisatie, zijn BSN wordt gekoppeld aan de reeds geleverde attributen.

**BSNk** – publieke voorziening, onder verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, die pseudoniemen en sleutelmaterialen verstrekt voor polymorfe pseudonimisering.

**eIDAS-koppelpunt** – Iedere Europese lidstaat heeft een nationaal eIDAS-koppelpunt hebben. Deze koppelpunten maken de toegang mogelijk tot de digitale dienstverlening van alle Europese lidstaten. Het koppelpunt fungeert als authenticatiedienst ofwel machtigingenregister (voor authenticatie van personen). De Rijksdienst voor Ondernemend Nederland ontwikkelt en beheert het eIDAS koppelpunt.

**Herkenningsmakelaar** - Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die het single point of contact vormt waarlangs dienstverleners Herkenningsdiensten afnemen, die de verantwoordelijkheid heeft om het berichtenverkeer van en naar de dienstverleners te ontkoppelen van de interne berichten binnen het netwerk en die optreedt als routeerder naar alle deelnemende authenticatiediensten, machtigingenregisters en ondertekendiensten.

**Polymorf Pseudoniem (PP)** – een polymorf pseudoniem is een cryptografisch element dat wordt afgeleid van de identiteit van de gebruiker. Een authenticatiedienst gebruikt dit om een gebruiker te authenticeren. Het BSNk verstrekt het PP aan de middelenuitgever die dit aanvraagt. Dit PP wordt vervolgens voor de ontvangende partij getransformeerd naar een Versleuteld Pseudoniem waaruit géén BSN kan worden afgeleid.

**Versleuteld Pseudoniem (VP)** – een versleuteld pseudoniem is gebaseerd op polymorfe pseudonimisering. Na decryptie leidt dit tot een persistent pseudoniem.

**Polymorfe Identiteit (PI) en Versleutelde Identiteit (VI)** – een polymorfe identiteit is technisch gelijk aan een polymorf pseudoniem met dit verschil dat een PI voor de ontvanger wordt omgezet in een versleutelde identiteit (VI) waaruit wél een BSN kan worden afgeleid.

**Specifiek Pseudoniem** – een pseudoniem dat gedurende een langere periode toegepast wordt in een specifiek werkingsdomein. Een dienstverlener-specifiek pseudoniem is steeds hetzelfde voor dezelfde dienstverlener in wiens context het gebruikt wordt, een dienstafnemer-specifiek pseudoniem is steeds hetzelfde voor de context van één dienstafnemer etc.

Voor een uitgebreide begrippenlijst zie: <https://afsprakenstelsel.etoegang.nl/display/as/Begrippenlijst>

### VNG Realisatie

Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag  
070 373 8008 | realisatie@vng.nl