# Factsheet eIDAS

**De EU-verordening eIDAS: wat betekent het voor u als overheidsorganisatie?**


**Auteurs** Xander van der Linde en Jonas de Graaf

**Datum** 1-7-2017

## Introductie

Mogelijk heeft u er al van gehoord. Vanaf september 2018 moeten overheidsdienstverleners EU-burgers[1] en organisaties/rechtspersonen[2] die inloggen en zich identificeren met hun eigen nationale inlogmiddel erkennen. Bijvoorbeeld een Belgische zakenman die inlogt met zijn Belgische eID om de foto van een verkeersboete te kunnen inzien. Of een Spaanse toerist die tijdens haar vakantie in Nederland slachtoffer is geworden en bij het Schadefonds Geweldsmisdrijven een aanvraag wil indienen voor een financiële tegemoetkoming.

De verordening eIDAS regelt (o.a.) de Europese acceptatie van nationale elektronische identificatiemiddelen (eIDs).[3] De Nederlandse overheid bouwt ondertussen ook aan het makkelijker en veiliger kunnen inloggen voor Nederlandse burgers bij de overheid en organisaties met een publieke taak, zoals organisaties in de zorg en pensioenfondsen. Dit beleid wordt Impuls eID genoemd. Onder Impuls eID kunnen Nederlandse burgers kiezen voor de inlogmethode die zij prettig vinden. Bijvoorbeeld DigiD, een 'selfiecheck', de App van Idensys of de inlogmethoden van de banken (iDIN). Alle inlogmethoden moeten voldoen aan strenge eisen en komen ook beschikbaar op hoge betrouwbaarheidsniveaus. Die eisen zijn gebaseerd op en  in lijn met de eIDAS-verordening. De nieuwe inlogmethoden onder de Impuls eID worden naar verwachting in 2019 verplicht voor de hele overheid en een aantal door de overheid gereguleerde sectoren, zoals zorgverzekeraars en pensioenfondsen. Dit wordt vastgelegd in de Wet Generieke Digitale Infrastructuur (wetGDI), die volgens planning waarschijnlijk vanaf januari 2019 zal gelden.

Er komen veel veranderingen aan. Dit kan een grote impact hebben op uw organisatie. Als u nu digitale dienstverlening aan Nederlandse burgers of organisaties biedt met online identificatie, is het vrijwel zeker zo dat u straks ook Europese burgers of organisaties digitaal moet kunnen identificeren middels hun eigen nationale inlogmiddel. Daarvoor moet u uw systemen aanpassen.

## Elektronische identificatie

Met een elektronisch identificatiemiddel (eID) kan een burger of vertegenwoordiger van een organisatie inloggen bij een website van de overheid, bij een (ander) bedrijf, bank, universiteit. Een eID is de digitale variant van het paspoort of de identiteitskaart. Je kunt ermee op afstand aangeven wie je bent (identificatie) en aantonen dat je het echt bent (authenticatie). Een eID is nodig voor de toegang tot persoonsgebonden online dienstverlening. In Nederland gebruiken we voor burgers DigiD voor elektronische identificatie en authenticatie; voor organisaties en rechtspersonen wordt eHerkenning gebruikt. Momenteel loopt er een aantal pilots om ook met andere middelen elektronische identificatie uit te voeren.[4]

[1] Feitelijk gaat het niet om EU-Burgers, maar om personen in het bezit van een niet-Nederlands door de EC genotificeerd Europees authenticatiemiddel uitgegeven door een van de lidstaten van de Europese Economische Ruimte (EU-lidstaten plus Noorwegen, IJsland en Liechtenstein). Om het simpel te houden, gebruiken we de term 'EU-burgers'.
[2] Voor de volledigheid gaat het om 'organisaties en rechtspersonen', maar voor de leesbaarheid gebruiken we 'organisaties'.
[3] Nederlanders moeten vanaf september 2018 ook kunnen inloggen bij dienstverleners in andere EU-lidstaten met hun eigen eID (zodra deze middelen bij de EU genotificeerd zijn), zogenaamd uitgaand verkeer. Deze factsheet gaat over
[4] Er zijn twee pilots: één bij de Belastingdienst en de andere met Idensys. Bij de Idensys-pilot kunnen burgers en organisaties inloggen via Idensys bij de overheid en het bedrijfsleven. Idensys maakt daarvoor gebruik van dezelfde afspraken als eHerkenning. In de een pilot bij de Belastingdienst loggen burgers in met hun bankpas (via iDIN).

## Wat is de Europese verordening eIDAS?

De Europese eIDAS-verordening stelt dat het vanaf september 2018 voor burgers en organisaties mogelijk moet zijn om met de nationale, genotificeerde (door Europa erkende), middelen in te loggen bij alle overheidsorganisaties binnen de Europese Unie. De (Nederlandse) overheidsdiensten moeten ervoor zorgen dat alle EU-ingezetenen zo toegang hebben tot hun dienstverlening. De verordening bestaat uit twee delen:

- *Inkomend verkeer (verplicht)*
  Europese burgers die met hun nationale inlogmiddel inloggen bij Nederlandse dienstverleners. Zo kunnen bijvoorbeeld expats bij de gemeente Wassenaar met hun eigen nationale eID inloggen op het gemeenteportaal om daar hun persoonsgegevens op te vragen. Dit deel van de verordening is verplicht voor de betreffende Nederlandse organisaties, voor alle door de EU erkende (genotificeerde) eID's.

- *Uitgaand verkeer (niet verplicht)*
  Nederlanders die met een genotificeerd (door Europa erkend) Nederlands inlogmiddel bij andere Europese dienstverleners inloggen. Dit deel van de verordening is niet verplicht. Wel zijn DigiD, eHerkenning en Idensys van plan hun inlogmiddelen te notificeren. Deze worden dan geschikt om in te loggen bij alle Europese overheidsdienstverleners.

In deze factsheet gaat het alleen om het inkomende verkeer!

## Verplichting versus ambities

De verordening verplicht dienstverleners EU-burgers en organisaties te identificeren die inloggen met hun eigen nationale inlogmiddel. Het aanpassen van bestaande dienstverlening aan een nieuwe doelgroep - bijvoorbeeld door Engelstalige of meertalige formulieren - is optioneel. Het advies is om eerst te zorgen voor het verplichte onderdeel en de afweging om de dienstverlening wel of niet aan te passen expliciet te agenderen.

## Wie kunnen zich straks identificeren?

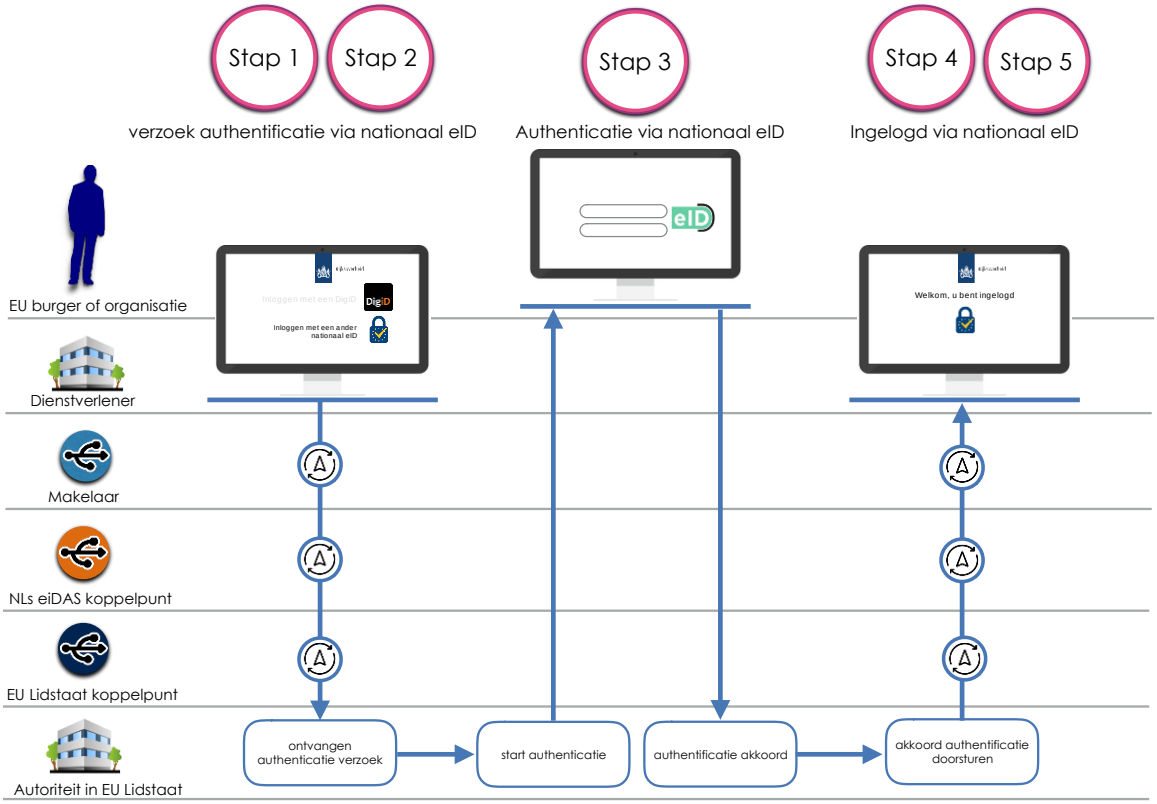
Enkele voorbeelden:

- Een Poolse seizoensarbeider die te veel betaalde belasting terugvraagt.
- Een Belgische zakenman die inlogt met zijn Belgische eID om de foto van een verkeersboete (bij het CJIB) te kunnen inzien.

- Een Duitse student die aan de TU Delft wil studeren en een vergunning nodig heeft;
- In Rotterdam wonende Fransman die een parkeervergunning wil aanvragen.
- Een Nederlandse gepensioneerde die met zijn Spaanse bankkaart zijn SVB-pensioenoverzicht bekijkt.
- Een Nederlander in Nederland die Belastingaangifte doet met een Ests authenticatiemiddel.
- Een Spaanse toerist die tijdens haar vakantie in Nederland slachtoffer is geworden en bij het Schadefonds Geweldsmisdrijven een aanvraag wil indienen.

## Het toekomstig proces

Als straks een EU-burger of organisatie zich digitaal meldt, ziet het proces er in grote lijnen als volgt uit:




**Stap 1**
EU-burger of organisatie gaat naar het portaal.

**Stap 2**
EU-burger of organisatie kiest de eigen nationale eID uit het keuzemenu.

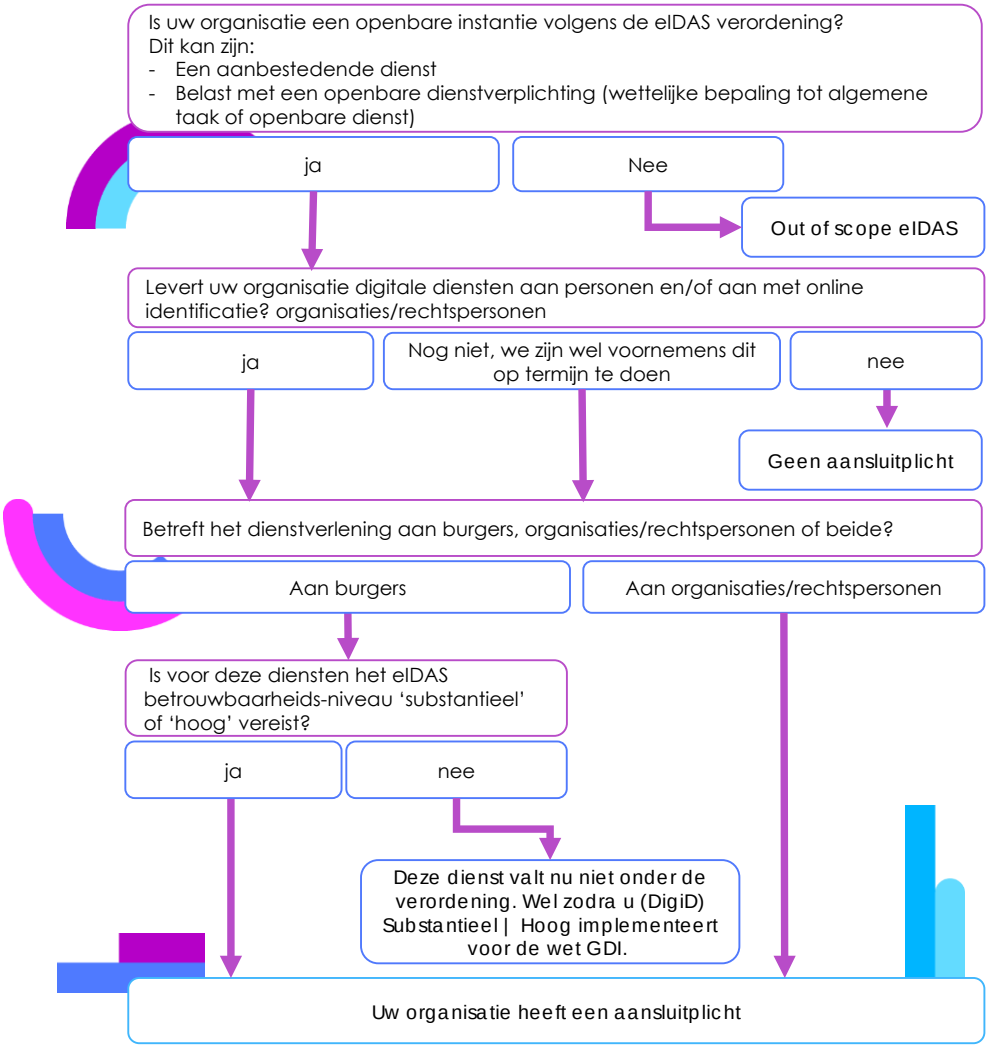
**Stap 3**
Achter de schermen wordt (via de Nederlandse makelaar en het knooppunt) een identiteitscontrole gedaan op het eigen eID-systeem.

**Stap 4**
Na een positieve identificatie en authenticatie krijgt de EU-burger / organisatie toegang tot het portaal.

**Stap 5**
EU-burger of organisatie kan een of meer diensten afnemen (optioneel).

## Aansluiten op eIDAS wel of niet vereist?

Als u digitale dienstverlening levert aan burgers of organisaties waarbij authenticatie vereist is - of als u van plan bent dit te gaan doen - dan heeft u waarschijnlijk de verplichting om aan de eIDAS-verordening te voldoen. De onderstaande beslisboom helpt om te bepalen of uw organisatie wel of niet moet voldoen.




## eIDAS en de wet GDI

In deze factsheet is het uitgangspunt 'het wetsvoorstel voor de Wet Generieke Digitale Infrastructuur' zoals die recent is geconsulteerd. In die consultatie werd onder andere op het punt van de verplichting het nodige aan terugkoppeling gegeven; dit kan ertoe leiden dat het uitgangspunt (de plicht) uiteindelijk anders wordt ingevuld - en dat de situatie voor uw organisatie alsnog wijzigt. Na de zomer van 2017 wordt meer duidelijkheid verwacht over de impact van de consultatie op het wetsvoorstel voor de wet GDI en de betekenis daarvoor op de eIDAS-verordening.

## Niveaus van betrouwbaarheid

eIDAS legt criteria vast voor de betrouwbaarheidsniveaus van authenticatiemiddelen. Er zijn drie niveaus: laag, substantieel en hoog. Voor de classificatie van digitale overheidsdiensten zijn er verschillende criteria, die zijn gekoppeld aan de betrouwbaarheidsniveaus. Sommige criteria die van toepassing zijn op een dienst kunnen laag scoren en andere substantieel. De hoogste score bepaalt het gewenste betrouwbaarheidsniveau voor de gehele dienst. Om de juiste hoogte van het betrouwbaarheidsniveau te bepalen, kunt u gebruik maken van de Handreiking Betrouwbaarheidsniveaus[5] van het Forum Standaardisatie.

## eIDAS en het BSN

Wanneer een burger met een buitenlands authenticatiemiddel voor de eerste keer een dienst van een Nederlandse dienstverlener af wil nemen waarvoor het BSN vereist is, wordt er straks centraal in het zogenaamde BRP-koppelpunt bij de Rijksdienst voor Identiteitsgegevens (RvIG) een koppeling met de BRP gemaakt. Het BRP-koppelpunt zorgt voor de matching van buitenlandse identiteitsgegevens met een BSN wanneer dit mogelijk is. En het koppelpunt verstrekt het BSN aan de dienstverlener, die daartoe gemachtigd is. De verificatie vindt plaats op basis van de eIDAS attributen; er is daarbij geen sprake van 'melden in persoon'. Het BRP-koppelpunt wordt momenteel ontwikkeld door het ministerie van BZK.

Als een de aanvragende EU-burger geen BSN heeft, moet de dienstleverancier kiezen tussen of geen dienst leveren, of de dienst aanbieden op basis van de beschikbare attributen. Voor welke van de twee u kiest, is afhankelijk van hoe uw processen zijn ingericht. Het kan dus zijn dat u straks een EU-burger identificeert (de verplichting) en vervolgens verwijst naar een alternatief kanaal (zoals fysieke verschijning) voor de werkelijke dienstverlening.

**Registeren als niet-ingezetene**
De Wet BRP beschrijft drie manieren hoe een niet-ingezetene geregistreerd wordt:

- De ingezetene doet aangifte van emigratie (of ambtshalve te worden geëmigreerd bij gebrek aan een aangifte).
- Door als burger bij een Inschrijfvoorziening (RNI-loket) zich te melden om in te schrijven.
- Door op verzoek van een zogenaamd Aangewezen Bestuursorgaan (ABO) te worden ingeschreven. De ABO's fungeren niet als loket, dus doen dit uitsluitend als ze daar zelf ook behoefte aan hebben voor de aangewezen taak.

**Het proces binnen het BRP-koppelpunt**
Het proces zoals dat binnen het BRP-koppelpunt plaatsvindt:

- Gebruiker kan optioneel zijn/haar BSN opgeven.
- BRP-koppelpunt stelt een Verificatievraag aan de Beheervoorziening BSN met attributen Geslachtsnaam, Geboortedatum en Geslacht.
- Indien de gebruiker een BSN heeft opgegeven, en
  - Één van de gevonden resultaten komt overeen: de koppeling wordt gelegd;
  - Geen van de gevonden resultaten komt overeen: geen koppeling.
- Indien de gebruiker geen BSN heeft opgegeven, en
  - Er wordt één resultaat gevonden: koppeling wordt gelegd als gebruiker instemt met koppeling met BSN ******123;
  - Er wordt geen resultaat gevonden: geen koppeling;
  - Er worden meerdere resultaten gevonden: handmatige actie.

[5] https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

## Dataset(s)

De eIDAS verordening definieert de attributen van de natuurlijke en niet-natuurlijke persoon die uitgewisseld worden: de minimale dataset. De minimale dataset bestaat naast een unieke identificatiecode - de zogenaamde Uniqueness Identifier - uit een aantal verplichte en een aantal vrijwillige attributen. Daarnaast mogen lidstaten ervoor kiezen om nog extra aanvullende attributen uit te wisselen. Deze zijn niet in de verordening uitgewerkt.

De eIDAS dataset ziet er als volgt uit:

| | Natuurlijke persoon | Organisatie/Rechtspersoon |
|---|---|---|
| Verplicht | - huidige familienaam of familienamen<br>- huidige voornaam of voornamen<br>- geboortedatum<br>- unieke identificatiecode | - huidige wettelijke naam<br>- unieke identificatiecode |
| Vrijwillig | - voornaam of voornamen en familienaam of familienamen bij geboorte<br>- geboorteplaats<br>- huidig adres<br>- geslacht | - huidig adres<br>- btw-nummer<br>- fiscaal referentienummer<br>- vennootschapsnummer<br>- identificatienummer voor juridische entiteiten<br>- EORI-nummer<br>- accijnsnummer<br>- bedrijfsindelingscode |

Wij adviseren uw software gereed te maken om minimaal deze attributen te kunnen ontvangen of op termijn te werken met het BSN via het BRP-koppelpunt.

## Aansluiten via een makelaar

Het aansluiten via de makelaar bestaat uit diverse stappen. Wij adviseren dit te bespreken met een makelaar. Men moet in ieder geval rekening houden met de volgende zaken:

- Minimaal met het netwerk aansluiten op een ETD-makelaar.
- Beschikken over een keuzescherm met het eIDAS-logo (als u geen eigen keuzescherm hebt, kunt u dit overlaten aan de makelaar).
- Onderhoud plegen op deze eigen voorziening.
- Afdoende kennis van protocollen en afspraken in huis hebben.
- Een eigen OTAP-omgeving inrichten specifiek voor de koppeling met eIDAS.
- Aanvragen en onderhouden van verschillende (PKI)-certificaten.
- Bijhouden van wijzigingen in protocollen en afspraken met betrekking tot eIDAS.
- Doen van een volledige end-to-end PENtest van de opgezette verbinding.

Deze eerste selectie van aandachtspunten is alleen voor de verplichte eIDAS-koppeling.

## Impactanalyse

ICTU heeft voor VenJ een impactanalyse uitgevoerd (Q1 en Q2 2017). Hierbij is onderzocht wat de impact is van de verordening op VenJ-organisaties. Daarbij hebben we de organisaties geïnformeerd wat de verordening voor hen mogelijk kan betekenen zodat zij tijdig maatregelen kunnen nemen (zoals het reserveren van budget). Meer informatie is bij ICTU (en via ICTU bij VenJ) op te vragen.

## Contact

Stichting ICTU
T (070) 7000 900
E info@ictu.nl (algemeen)

## Colofon

Deze informatiebrochure is opgesteld door Stichting ICTU

# Vragen en antwoorden

## Wie moet je straks kunnen identificeren?

Personen in het bezit van een niet-Nederlands door de EC genotificeerd Europees authenticatiemiddel. Aangezien de EC uitsluitend middelen zal notificeren op betrouwbaarheidsniveau substantieel of hoog, impliceert dit dat het middel tenminste betrouwbaarheidsniveau substantieel heeft. Uiteraard moeten ook Nederlandse middelen worden geaccepteerd, maar dat is *niet* in het kader eIDAS. Overigens blijft de naam DigiD gehandhaafd voor door de overheid uitgegeven middelen, dus ook die op niveau substantieel of hoog, dus het is beter om te spreken over DigiD laag (huidig DigiD), DigiD substantieel (binnenkort be schikbaar) en DigiD hoog (vanaf eind 2018 beschikbaar op het rijbewijs en de eNIK).

## Is het aanpassen van de dienstverlening verplicht?

Nee, de eIDAS verordening verplicht alleen EU-burgers en organisaties/rechtspersonen te identificeren. Men hoeft dus niet de dienstverlening aan te passen (bijv. in een andere taal aan te bieden). Het kan dus zijn dat je straks een EU-burger identificeert (de verplichting) en vervolgens verwijst naar een alternatief kanaal (zoals fysieke verschijning) voor de werkelijke dienstverlening. Het advies is eerst te zorgen voor het verplichte deel – de authenticatie – en vervolgens de dienstverlening aan te passen.

## Is het gebruik van het BRP-koppelpunt noodzakelijk?

Nee, het BRP-Koppelpunt wil ontzorgen voor een deel van de dienstverleners in de publieke sector. De keuze of een dienstverlener gebruik maakt van het BRP-koppelpunt wordt vastgelegd in het dienstenregister. Er zijn drie mogelijkheden:

- Dienstverlener gebruikt nooit een BSN bij het verlenen van de dienst (NB: dit geldt voor alle private dienstverlening [die mogen immers het BSN niet gebruiken] en een beperkt aantal publieke dienstverleners). Het BRP-Koppelpunt wordt niet gebruikt en de dienstverlener krijgt de attributen die noodzakelijk zijn voor de dienstverlener, waarbij de verplichte attributen (UniquenessID, voornaam, geslachtsnaam, geboortedatum) altijd kunnen worden geleverd en de optionele attributen (geboortevoornaam, geboortegeslachtsnaam, geboorteplaats, geslacht, postcode, huisnummer, huisnummertoevoeging) indien die door het betreffende EU-land beschikbaar worden gesteld.
- Dienstverlener heeft voorkeur voor een BSN, maar kan de dienst ook leveren zonder (denk: DUO/Studielink die een nieuwe student inschrijft). BRP-Koppelpunt wordt gebruikt en – indien aanwezig – wordt het BSN geleverd. Als er geen BSN is worden de uit Europa aangeleverde attributen geleverd (vgl met geen BSN hierboven).
- Dienstverlener heeft een BSN nodig voor de dienstverlening. BRP-Koppelpunt wordt gebruikt en indien beschikbaar wordt het BSN geleverd. Als er geen BSN beschikbaar is, wijst het BRP-Koppelpunt op de noodzaak van het bezit van een BSN en hoe dit kan worden verkregen. De dienstverlener krijgt in dit geval dus GEEN gegevens aangeleverd. Merk op dat deze optie op gespannen voet kan staan met het idee achter de verordening dat eigen middelen niet mogen worden bevoordeeld. Dus de noodzaak van het BSN moet wel hard te maken zijn. (denk: Belastingdienst. Het terugvragen van teveel betaalde belasting of het aanvragen van een toeslag zal altijd gebeuren op basis van gegevens die in de BRP zijn opgenomen, en opname in de BRP impliceert het hebben van een BSN).

Merk op dat het BRP-Koppelpunt uitsluitend de eerste keer wordt gebruikt als een EU-middel voor een Nederlandse publieke dienst wordt ingezet. Het eIDAS-Koppelpunt (EZ) onthoudt daarna het eerder verkregen Polymorfe Pseudoniem van het BSN en gebruikt indien de EU-burger zich voor dezelfde of een andere publieke dienst meldt.

## Is de nationaliteit van de gebruiker onderdeel van de dataset?

Nee, de verordening schrijft voor welke attributen minimaal en maximaal kunnen worden geleverd en daar hoort de nationaliteit niet bij. Overigens is er in de verordening ruimte voor aanvullende – thans nog niet in de verordening geregelde – attributen, maar dat gaat pas werken als daarover (bilaterale?) afspraken worden gemaakt tussen landen.
Dit is overigens geen specifiek eIDAS-issue. Het Nederlandse rijbewijs wordt ook voorzien van DigiD-hoog en dat document bevat geen gegevens over de nationaliteit. Omdat wonen in Nederland een voorwaarde is voor het verkrijgen ervan, zullen in praktijk alle rijbewijsbezitters in de BRP zijn ingeschreven en kan de dienstverlener (als nationaliteit noodzakelijk is voor de dienstverlener, dan zal die dienstverlener geautoriseerd zijn om dit gegeven uit de BRP te ontvangen) de nationaliteit op deze manier achterhalen. De BRP bevat echter ook gegevens over niet-ingezetenen (RNI) en van de 3,7 miljoen als niet-ingezetene ingeschreven personen zijn er ongeveer 1 miljoen waarbij de nationaliteit niet is geregistreerd. Dit is het gevolg van het feit dat het naast door emigratie en door inschrijving van een burger aan het RNI-loket ook mogelijk is een persoon op te voeren door een Aangewezen Bestuursorgaan (ABO, thans: Belastingdienst, SVB, UWV, CAK en minBZ) voor de daarvoor aangewezen taken. Aangezien ABO's uitsluitend gegevens mogen aanleveren die worden gebruikt voor die aangewezen taak en nationaliteit daar vaak niet bij hoort, worden personen opgevoerd zonder nationaliteitsgegevens. (denk: een in het kader van de ZVW meeverzekerd gezinsland in het buitenland). Dus zelfs met BSN is nationaliteit niet altijd leverbaar.

## Wat betekenen de begrippen identificatie, authenticatie en autorisatie?

- Identificatie: identificatie is het bekend maken van de identiteit van personen, bedrijven en IT-systemen.
- Authenticatie: het aantonen dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft. Authenticatie noemt men ook wel verificatie. eIDAS gaat over authenticatie van Europese burgers en organisaties/rechtspersonen.
- Autorisatie: het proces van het toekennen van rechten voor de toegang tot geautomatiseerde functies en/of gegevens in ICT-voorzieningen van de identiteit.

## Wat is het Nederlandse eIDAS Koppelpunt?

Het Nederlandse eIDAS Koppelpunt faciliteert de interoperabiliteit tussen het Nederlandse stelsel eTD en buitenlandse eIDAS koppelpunten. Richting de buitenlandse eIDAS koppelpunten voldoet het NL koppelpunt aan de eIDAS-standaard en richting het eTD aan de daar geldende eTD-standaard. Het eIDAS koppelpunt onderhoudt de koppelingen naar elk van de andere aangesloten lidstaten en gedraagt zich naar het stelsel eTD als authenticatiedienst/ machtigingregister (voor authenticatie van personen met een buitenlands middel) en dienstverlener (voor authenticatie van personen met en Nederlands middel). Het eIDAS koppelpunt valt onder de departementale verantwoordelijkheid van het ministerie van EZ.

## Hoe weet ik dat de authenticatie die in het buitenland plaatsvindt betrouwbaar is?

Met het instemmen met de verordening hebben lidstaten aangegeven dat zij elkaars digitale authenticatiemiddelen accepteren en daarmee ook de onderliggende uitgifteprocessen. Dat betekent niet dat direct elk authenticatiemiddel geaccepteerd is. Lidstaten moeten notificeren dat zij hun authenticatiemiddel(len) goedgekeurd willen hebben. Dit vindt plaats middels een review waarbij lidstaten controleren of het middel en de onderliggende uitgifteprocessen voldoen aan de gestelde eisen. Nederland (via minEZ) neemt deel aan het reviewen van de processen. Daarnaast is het zo dat alleen authenticatiemiddelen met het niveau substantieel of hoog kunnen worden genotificeerd i.h.k.v. eIDAS.