Privacy Impact Assessment

Startarchitectuur eIDAS

6 december 2016

Auteurs: dr. J.A.G. Versmissen CIPP/E
mr. H. van der Wel
B.C. Beunders LLM

Versie: 1.1 (definitief)

PIA Startarchitectuur eIDAS

Privacy Impact Assessment op de startarchitectuur van de nationale implementatie van eIDAS met het stelsel van Elektronische Toegangsdiensten

Privacy Management Partners

Vondellaan 106
3521 GH Utrecht

Postbus 1200
3970 BE Driebergen

Telefoon: 085 401 3866
E-mail: info@pmpartners.nl
Internet: www.pmpartners.nl

Inhoudsopgave

Managementsamenvatting **5**

Inleiding **5**

Kaders **5**

Nederlandse eIDAS-implementatie **5**

Uitkomsten PIA **7**

Begrippenlijst **11**

Begrippen uit de Startarchitectuur **11**

Begrippen uit de AVG **12**

1 Inleiding **15**

2 Reikwijdte **16**

3 Verantwoording **18**

4 Kaders **19**

4.1 Wet- en regelgeving **19**

4.1.1 Bestaande regelgeving 19

4.1.2 Regelgeving in wording 19

4.2 Eerdere privacybeoordelingen **19**

4.2.1 PIA eIDAS-knooppunt 19

4.2.2 Advies AP 20

5 Beoordeling **21**

Doeleinden/doelbinding en koppeling 29

Kwaliteit 34

Profilering 34

Beveiliging 37

Bewaring/vernietiging 39

Transparantie 39

Rechten van betrokkenen 40

6 Private dienstverleners, andersoortige attributen **41**

6.1 Private dienstverleners **41**

6.2 Andersoortige attributen **42**

7 Wijzigingen in de startarchitectuur **44**

8 Conclusies **47**

9 Aanbevelingen **49**

Bijlage A Data flows 51

Bijlage B Persoonsnummers 56

Basispersoonsnummers 56

BSN 56

UID's 56

Polymorfe pseudonimisering 56

eTD-stelsel 56

Nederlandse eIDAS-implementatie 58

Opslaan UID bij BRP-koppelpunt 58

Bijlage C Aanbevelingen uit PIA eIDAS-koppelpunt 60

Bijlage D Relevante eIDAS-bepalingen 67

Gegevensverwerking, -bescherming en beveiliging 67

Toepassingsgebied 67

Aanmelding stelsel van elektronische identificatie 67

Persoonsidentificatiegegevens 68

Private dienstverleners 69

Managementsamenvatting

Inleiding

De EU heeft in 2014 de eIDAS-verordening vastgesteld. Deze verordening regelt een aantal zaken op het gebied van elektronische identificatie en vertrouwensdiensten voor elektronische transacties.

Voor deze PIA zijn de regels ten aanzien van elektronische identificatie van belang. Op dat vlak beoogt de verordening te bewerkstelligen dat ingezetenen van EU-lidstaten[1] en in de EU gevestigde rechtspersonen gebruik kunnen maken van digitale (overheids)voorzieningen in elke EU-lidstaat, door middel van verplichte wederzijdse erkenning van elektronische identiteiten tussen lidstaten. In september 2018 zal de eIDAS-verordening van kracht zijn. Dan moet het gebruik van nationale bij de EU genotificeerde elektronische authenticatiemiddelen in andere lidstaten mogelijk zijn, zodat burgers en ondernemers op eenvoudige wijze diensten kunnen afnemen en veilig transacties kunnen verrichten via de websites van overheden in alle lidstaten.

De eIDAS-verordening richt zich naast publieke dienstverleners ook op private dienstverleners. Lidstaten dienen zelfs de private sector aan te moedigen om (vrijwillig) gebruik te maken van onder eIDAS genotificeerde elektronische identificatiemiddelen.

Nederland bereidt zich hierop voor door het mogelijk te maken dat personen die de beschikking hebben over een genotificeerd EU authenticatiemiddel (en die al dan niet een rechtspersoon vertegenwoordigen) in kunnen loggen bij Nederlandse digitale overheidsvoorzieningen. Daarnaast gaat Nederland het voor natuurlijke en rechtspersonen met een Nederlands authenticatiemiddel technisch mogelijk maken om in te loggen bij overheidsvoorzieningen in andere EU-lidstaten. Door Nederland bij de EU genotificeerde authenticatiemiddelen mogen door buitenlandse overheidsdienstverleners niet geweigerd worden.

Het Ministerie van Economische Zaken (hierna: “EZ”) is niet alleen de dossierhouder van de verordening elektronische identiteiten, maar ook beleidsverantwoordelijk. In opdracht van EZ wordt een architectuur opgesteld voor de zaken die Nederland moet regelen om te kunnen voldoen aan de eIDAS-verordening. Momenteel bevindt het project zich nog in de ontwerpfase, waarbij de doelarchitectuur en de overkoepelende (project)startarchitectuur van eIDAS reeds gereed zijn. In de startarchitectuur worden de beleidskeuzes en architectuurprincipes beschreven, maar ook de technische specificaties van de koppelvlakken tussen de componenten die nodig zijn om het hele stelsel te laten werken. De startarchitectuur is het evaluatieobject van deze PIA.

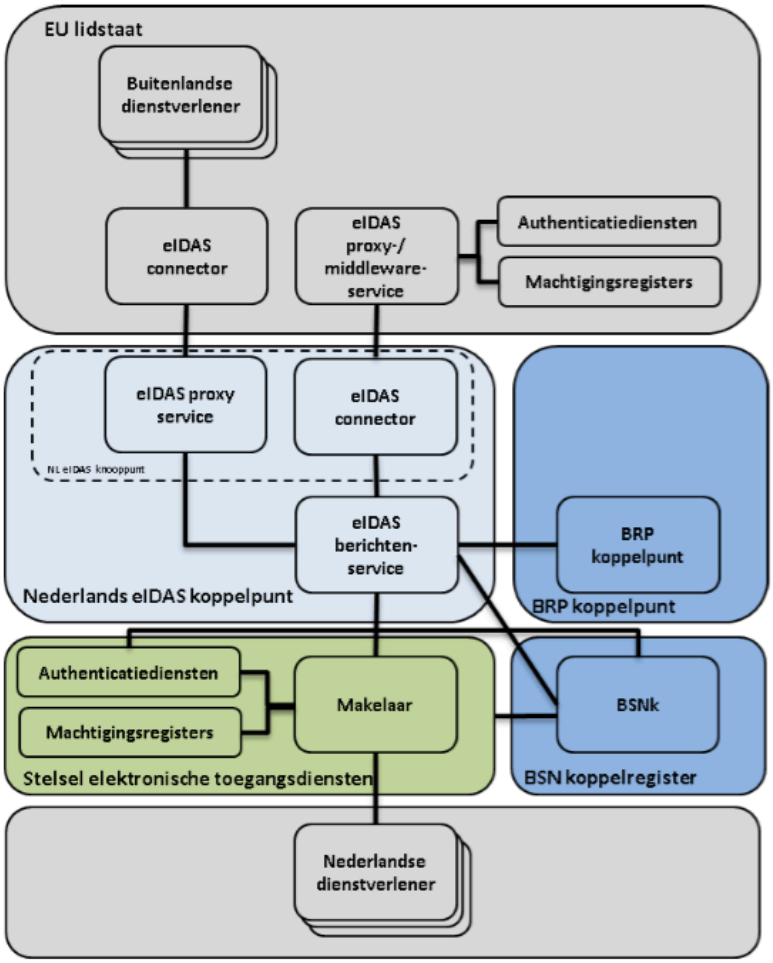
Kaders

De belangrijkste kaders voor de beoordeling in deze PIA zijn de eIDAS-regelgeving en de Algemene Verordening Gegevensbescherming. Ook is rekening gehouden met de eerdere PIA op het eIDAS-knooppunt en het advies van de Autoriteit Persoonsgegevens over de eIDAS-uitvoeringswet.

Nederlandse eIDAS-implementatie

Bijgaande figuur uit de startarchitectuur schetst de Nederlandse eIDAS-implementatie in haar context. Evaluatieobject van deze PIA zijn de eIDAS-berichtenservice, het BRP-koppelpunt en (de toegevoegde functionaliteit van) het BSNk, hun onderlinge samenhang en de verbindingen naar buiten. Deze onderdelen worden hieronder beschreven.

[1] En ook Noorwegen, Liechtenstein en IJsland.



Er zijn vier kernprocessen ('Use Cases'):

- Use case IIA: een persoon met een EU-middel logt in bij een dienstverlener in Nederland; de dienstafnemer is een natuurlijke persoon.
- Use case IIB: een persoon met een EU-middel logt in bij een dienstverlener in Nederland; de dienstafnemer is een niet-natuurlijke persoon
- Use case IIIA: een persoon met een Nederlands middel logt in bij een dienstverlener in een andere lidstaat; de dienstafnemer is een natuurlijke persoon
- Use case IIIB: een persoon met een Nederlands middel logt in bij een dienstverlener in een andere lidstaat; de dienstafnemer is een niet-natuurlijke persoon

Deze worden in detail beschreven in hoofdstuk 4 van de startarchitectuur.

eIDAS-berichtenservice

Om de berichtenservice goed te kunnen beschrijven gaan we hier ook in op het Nederlandse eIDAS-koppelpunt als geheel. Dit koppelpunt faciliteert de interoperabiliteit tussen het Nederlandse stelsel voor elektronische toegangsdiensten (eTD-stelsel) en buitenlandse eIDAS-koppelpunten. Richting de buitenlandse eIDAS-knooppunten voldoet het Nederlandse 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 c.q. machtigingregister (voor authenticatie van personen met een buitenlands middel) en dienstverlener (voor authenticatie van personen met een Nederlands middel).

Het eIDAS-koppelpunt bestaat uit de componenten:
- het *eIDAS-knooppunt*, bestaande uit eIDAS-connector en eIDAS-proxy service.
- de *eIDAS-berichtenservice*: de brugfunctie tussen het eIDAS-knooppunt en het eTD-stelsel. De berichtenservice bevat onder meer functionaliteit voor het omvormen van eIDAS-berichten tot eTD-berichten en omgekeerd.

BRP-koppelpunt
Het BRP-koppelpunt zorgt voor het vaststellen of een persoon die met een buitenlands middel inlogt al in de BRP bekend is. Het wordt ingeschakeld door de eIDAS-berichtenservice op het moment dat een natuurlijk persoon met een buitenlands authenticatiemiddel voor de eerste keer een dienst van een Nederlandse dienstverlener af wil nemen waarvoor het BSN vereist is. Het BRP-koppelpunt wordt alleen ingeschakeld indien een burger een dienst in het BSN-domein af wil nemen. Een dienst behoort tot het BSN-domein als de dienstverlener voor de dienstverlening ter identificatie van de natuurlijke persoon gebruik mag of moet maken van het BSN. Het BRP-koppelpunt registreert de koppeling tussen de eIDAS-*uniqueness id* en het BSN. Het heeft geen rol in dienstverlening aan buitenlandse bedrijven en dienstverlening door buitenlandse dienstverleners aan personen met een Nederlands middel.

BSNk
Het BSNk zorgt voor de koppeling van een authenticatiemiddel aan het BSN en het genereren van de pseudoniemen die in het stelsel nodig zijn. Het eTD-stelsel biedt authenticatiediensten voor burgers en bedrijven tot zowel publieke diensten als private diensten. Private authenticatiediensten zijn doorgaans niet gerechtigd om het BSN te gebruiken. Om private authenticatiemiddelen in het publieke domein te kunnen gebruiken is het BSNk ontwikkeld. Het BSNk koppelt de authenticatiemiddelen aan het BSN en geeft het BSN – indien de dienstverlener daar recht toe heeft – vrij. Om de privacy te borgen, maakt het BSNk gebruik van pseudonimisering.

Uitkomsten PIA

In de PIA is allereerst de privacy impact van de startarchitectuur beoordeeld. Op grond hiervan zijn conclusies getrokken, die waar relevant aanleiding gaven tot privacyrisico mitigerende aanbevelingen. Hieronder zijn de belangrijkste beoordelingen, conclusies en aanbevelingen thematisch gerangschikt. Wij hechten er belang aan om op te merken dat diverse (mogelijke) privacyrisico's in deze PIA nog niet of slechts marginaal beoordeeld konden worden. Het betreft dan met name componenten in de architectuur die nu nog niet zijn uitgewerkt en zoals te doen gebruikelijk in een volgende architectuurfase aan de orde zullen komen. Gedacht kan worden aan privacyrisico's die inherent zijn aan dit soort stelsels, zoals logging van (meta)data uit het oogpunt van onder meer beheer, beveiliging, incidentmanagement, fraudebestrijding en om te kunnen voldoen aan verzoeken van betrokkenen in verband met hun privacyrechten. Andere privacyrisico's kunnen pas goed beoordeeld worden wanneer ze concreet aan de orde zijn, zoals het gebruik van eIDAS door private dienstverleners en het werken met andersoortige attributen dan de verplichte en aanvullende attributen. Alsdan zal een aanvullende beoordeling van de privacyrisico's moeten plaatsvinden, waarvan de uitkomsten aanleiding kunnen zijn tot privacyrisico mitigerende maatregelen in onder meer de architectuur, governance, regelgeving en stelselafspraken. Tot slot besteedt de startarchitectuur naar haar aard slechts beperkt aandacht aan bestuurlijke aspecten, zoals governance.

Algemeen
Bij het opstellen van de startarchitectuur is invulling gegeven aan het uitgangspunt van privacy-by-design. Hoofdstuk 6 van de startarchitectuur beschrijft een aantal maatregelen op dat gebied, waaronder pseudonimisering en andere vormen van dataminimalisatie. Deze leiden er onder meer toe dat op geen enkele manier ooit een BSN wordt verstrekt aan een andere lidstaat.

Verantwoordelijkheden en governance

- De verdeling van verantwoordelijkheden binnen eIDAS is van groot belang (en een verplichting uit hoofde van de Algemene Verordening Gegevensbescherming, AVG). Onduidelijkheden met betrekking tot deze verantwoordelijkheidsverdeling brengen privacyrisico's met zich mee. Gezien de relatie van het eIDAS-koppelpunt met het eTD-stelsel kunnen ook op dit vlak ten aanzien van het eTD-stelsel door eerdere PIA's en de Autoriteit Persoonsgegevens gesignaleerde privacyrisico's spelen.
- De ministers van EZ en BZK zijn gezamenlijk verwerkingsverantwoordelijke de Nederlandse eIDAS-implementatie. Dit moet goed geregeld worden.
- Met een duidelijke verdeling van verantwoordelijkheden, zoals beschreven in het antwoord op vraag 1 in hoofdstuk 5, tussen met name de Ministers van EZ en BZK, zijn deze privacyrisico's niet zonder meer in voldoende mate gemitigeerd.[2] Ook een goede en effectieve governance binnen de organisaties van de verantwoordelijken en tussen eIDAS en het eTD-stelsel is noodzakelijk. De wet GDI en/of de daarbij behorende lagere regelgeving zal deze duidelijkheid wel moeten bieden.

Aanbevelingen

- Regel de gezamenlijke verantwoordelijkheid van de beide ministers ten aanzien van eIDAS en het eTD-stelsel, zoals bedoeld in artikel 26 AVG.
- Ga als Ministerie van EZ en Ministerie van BZK door met het gezamenlijk en integraal uitwerken van verantwoordelijkheidsvraagstukken.
- Maak duidelijke afspraken over wie waarvoor verantwoordelijk is. Regel de verantwoordelijkheden en voeg deze zoveel mogelijk toe aan bestaande afsprakenstelsels, wetten en ministeriële besluiten. Doe dit zo integraal en consistent mogelijk.
- Beleg verantwoordelijkheden bij concreet benoemde onderdelen van de ministeries. Benoem wie binnen welk ministerie de ambtelijke verantwoordelijkheid draagt.
- Aandachtspunten hierbij zijn onder meer:
  - Wie is binnen het Ministerie van BZK verantwoordelijk voor het BSNk en respectievelijk het BRP-koppelpunt?
  - Wie neemt de uiteindelijke beslissing als men het oneens is met elkaar?
  - Hoe scheidt het Ministerie van EZ zijn rol en verantwoordelijkheden ten aanzien van eIDAS enerzijds en het eTD-stelsel anderzijds?
- Haak, uit het oogpunt van convergentie, met het eIDAS-koppelpunt zo veel mogelijk aan bij c.q. stem af op het verbeterproces van de governance en het toezicht op het eID-stelsel (voor zover dit het eTD-stelsel raakt).

Bewerkers

- Bij het inschakelen van (private of publieke) bewerkers gelden er soortgelijke risico's als zijn gesignaleerd in de eerder uitgevoerde PIA's op het eID-stelsel. Deze hangen met name samen met ongewenste samenloop van rollen en het doorbreken van functiescheidingen. Dergelijke risico's zullen zich met name voordoen wanneer door eIDAS ingeschakelde bewerkers ook rollen vervullen binnen het eTD-stelsel.

Aanbevelingen

- Regel de rol van bewerkers, inclusief eisen op het gebied van privacy en informatiebeveiliging in de Regeling EBV, de Wet GDI en het afsprakenstelsel.

[2] Wij verwijzen hiervoor naar de samenhang tussen dit onderwerp en de bevindingen in par. 4.2 van deze PIA en de beantwoording van vraag 15

– Draag daarbij zorg voor nadere regulering en toetsing van de scheiding van meerdere vormen van dienstverlening binnen één organisatie en systeem (ook wel 'Chinese muren' genaamd).

Wettelijk kader

– Naast de eIDAS-verordening en de uitvoeringsverordeningen 1501 en 1502 is er vanuit Europa geen aanvullende wetgeving gemaakt. Deze zijn vrijwel uitsluitend gericht op de interactie tussen lidstaten, en zeggen nauwelijks iets over de nationale eIDAS-implementaties. Mede gelet op de opmerkingen hierboven, over het belang van goede governance en een duidelijke verdeling van verantwoordelijkheden, treden er risico's op als deze zaken niet goed worden uitgewerkt in Nederlandse wet- en regelgeving.
– Het gebruik van het BSN binnen het eIDAS berichtenverkeer leidt gemakkelijk tot juridische discussies. Een concreet risico is dat een situatie ontstaat waarin, althans volgens de letter van de wet, het BSN 'onnodig' verplicht moet worden meegezonden bij veel eIDAS-berichtenverkeer.

Aanbevelingen

– Leg in aanvulling op de eIDAS-verordening en de uitvoeringswet eIDAS de contouren van de Nederlandse eIDAS-implementatie, zoals de componenten, rollen, taken, bevoegdheden en verantwoordelijkheden vast in de Wet GDI.
– Tref een zeer duidelijke regeling voor het gebruik van het BSN, het UID en de polymorfe pseudoniemen aanvullend in de Wet GDI en de Ministeriële regeling inzake elektronisch berichtenverkeer (Regeling EBV).

Kwaliteit

– De veronderstelde unieke koppeling tussen individuen enerzijds en persoonsnummers als het BSN en de UID anderzijds kan in de praktijk minder eenduidig zijn.

Aanbeveling

– Ga na of er nog extra maatregelen nodig zijn voor het mitigeren van risico's die kunnen optreden wanneer persoonsnummers niet uniek aan individuen gekoppeld blijken te zijn.

Private dienstverleners

– Het gebruik van de eIDAS-infrastructuur door private dienstverleners brengt mogelijk privacyrisico's met zich mee, doordat met (de privacyaspecten van) dit gebruik in de EU-regelgeving en in de Nederlandse eIDAS-implementatie nog slechts beperkt rekening is gehouden.

Aanbevelingen

– Voer een aanvullende PIA uit, bijvoorbeeld op sector- of domeinniveau, bij gebruik van eIDAS door private dienstverleners.
– Hanteer ten aanzien van het gebruik van eIDAS door private dienstverleners de volgende uitgangspunten:
  - Aan het gebruik van buitenlandse persoonsidentificatiegegevens door Nederlandse private dienstverleners worden ten minste dezelfde eisen gesteld als het eTD-stelsel aan hen stelt m.b.t. het gebruik van Nederlandse authenticatie-informatie.
  - Aan buitenlandse private dienstverleners en het gebruik dat zij maken van Nederlandse authenticatie-informatie worden ten minste dezelfde eisen gesteld als het Nederlandse eTD-stelsel stelt aan (Nederlandse) private dienstverleners.

Andersoortige attributen

– Het is niet duidelijk hoe andersoortige attributen buiten de minimale dataset precies aan de eIDAS-infrastructuur toegevoegd worden, en aan welke voorwaarden dan moet worden voldaan.

De inhoud van deze andersoortige attributen kan veel privacygevoeliger zijn dan de minimale dataset van eIDAS. De bestaande maatregelen mitigeren slechts beperkt de specifieke risico's die gebruik van bepaalde (combinaties van) andersoortige attributen met zich mee kan brengen.

Aanbeveling

– Tref waarborgen, bijvoorbeeld op sector- of domeinniveau, rondom het proces van het toelaten van een specifieke uitwisseling van andersoortige attributen buiten de minimale dataset die eDIAS definieert, waaronder de verplichting om eerst de privacyrisico's te beoordelen, voordat doorzetting van die gegevens door het eIDAS-knooppunt kan plaatsvinden.

Begrippenlijst

Begrippen uit de Startarchitectuur

– Authenticatiebericht	Het authenticatiebericht vormt het antwoord op het authenticatie-verzoek (zie 'Authenticatieverzoek').
– Authenticatiemiddel	Het middel waarmee een persoon zijn of haar identiteit (online) kan aantonen.
– Authenticatieverzoek	Het verzoek tot authenticatie, afkomstig van een online dienstverlener uit een EU/EER-lidstaat, met het oog op toegang tot een online dienst.
– BRP-koppelpunt	Een voorziening die personen met een buitenlands authenticatiemiddel die om een BSN-dienst verzoeken probeert te matchen met een bestaande registratie in de BRP.
– BSNk	BSNk staat voor "BSN-koppelregister". Dit register zorgt zowel voor het koppelen van authenticatiemiddelen aan het BSN, als voor het uitgeven van Polymorfe Pseudoniemen ter identificatie van natuurlijke personen.
– Dataset	Een verzameling attributen behorend bij een identiteit. De startarchitectuur spreekt enerzijds over een 'minimale dataset', bestaande uit verplichte en aanvullende attributen en benoemt anderzijds de mogelijkheid van andersoortige attributen.
– eIDAS-berichtenservice	de brugfunctie tussen het eIDAS-knooppunt en het eTD-stelsel. De berichtenservice bevat onder meer functionaliteit voor het omvormen van eIDAS-berichten tot eTD-berichten en omgekeerd.
– eIDAS-knooppunt	De door de eIDAS-verordening voorgeschreven voorziening voor het routeren van eIDAS-berichtenverkeer tussen lidstaten. Het eIDAS-knooppunt bestaat uit een eIDAS-connector en een eIDAS-proxy service. De EU stelt hiervoor een referentie-implementatie beschikbaar. Ook andere lidstaten zijn verplicht om een eIDAS-knooppunt in te richten. De communicatie tussen de eIDAS-knooppunten is geüniformeerd.
– eIDAS-koppelpunt	Deze voorziening zorgt ervoor dat Nederland is gekoppeld aan de andere Europese lidstaten. Het eIDAS-koppelpunt bestaat uit het eIDAS-knooppunt en de eIDAS-berichtenservice. Enerzijds faciliteert het koppelpunt het inloggen door personen die beschikken over een authenticatiemiddel uit een andere lidstaat bij Nederlandse dienst-verleners, anderzijds het inloggen van personen die beschikken over een Nederlands authenticatiemiddel bij dienstverleners in andere lidstaten. Om deze reden onderhoudt het koppelpunt koppelingen

	naar elk van de buitenlandse eIDAS-koppelpunten en naar het stelsel eTD.
– eIDAS-verordening	Een Europese verordening die onder meer bepaalt dat als een lidstaat voor het afnemen van een overheidsdienst elektronische authenticatie toestaat, die authenticatie ook mogelijk moet zijn met genotificeerde authenticatiemiddelen die zijn uitgegeven in andere lidstaten.
– Genotificeerd authenticatiemiddel	Een authenticatiemiddel binnen een door een lidstaat bij de EU genotificeerd stelsel van elektronische identificatie.
– (Polymorfe) Pseudoniemen	Van persoonsnummers afgeleide codes die gebonden zijn aan een specifiek persoon. Deze pseudoniemen zijn bedoeld om binnen het stelsel eTD de privacy van de gebruikers te borgen. Gebruikers hebben voor iedere dienstverlener waarmee ze een relatie hebben een apart pseudoniem. De pseudoniemen voor verschillende sites zijn niet onderling te koppelen of te herleiden tot één en dezelfde gebruiker. Dit helpt voorkomen dat dienstverleners gegevens gaan combineren om profielen over gebruikers samen te stellen.
– Private dienstverleners	Partijen uit de private sector die voor de toegang tot hun elektronische dienstverlening gebruik maken van de elektronische middelen die zijn genotificeerd bij de Europese Commissie.
– Stelsel eTD	Het afsprakenstelsel elektronische toegangsdiensten voor identificatie, authenticatie en machtigingen van Nederlandse (natuurlijke- en rechts)personen en online toegangsdiensten voor Nederlandse dienst-verleners. Onder het stelsel eTD vallen Idensys (voor personen) en eHerkenning (voor organisaties).
– Uniqueness ID	Een persoonsnummer waarvan het gebruik is voorgeschreven voor eIDAS-berichtenverkeer tussen lidstaten, en dat voor iedere persoon uniek en zo persistent mogelijk moet zijn.

Begrippen uit de AVG[3]

– Beveiliging	Door het nemen van passende technische of organisatorische maatregelen ervoor zorgen dat persoonsgegevens beschermd zijn tegen onder meer ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (“integriteit en vertrouwelijkheid”). (Artikel 5 lid 1 onder f AVG)
– Bewerker	De huidige benaming voor wat onder de AVG de ‘verwerker’ gaat heten (zie aldaar).

[3] Algemene Verordening Gegevensbescherming.

– Persoonsgegeven	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”). (Artikel 4 lid 1 AVG)
– Pseudonimisering	Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. (Artikel 4 lid 5 AVG)
– Toestemming	Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt. (Artikel 4 lid 11 AVG)
– Verantwoordelijke	De huidige benaming voor wat onder de AVG de ‘verwerkingsverantwoordelijke gaat heten (zie aldaar).
– Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. (Artikel 4 lid 2 AVG)
– Verwerkings-verantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. (Artikel 4 lid 7 AVG)
– Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkings-verantwoordelijke persoonsgegevens verwerkt. (Artikel 4 lid 8 AVG)

Afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BRP	Basisregistratie Personen
BSN	Burgerservicenummer
BZK	(Ministerie van) Binnenlandse Zaken en Koninkrijksrelaties
DV	Dienstverlener
EBV	Elektronisch berichtenverkeer
eTD	Elektronische toegangsdiensten
EZ	(Ministerie van) Economische Zaken
MvT	Memorie van Toelichting
PIA	Privacy Impact Assessment
PP	Polymorf pseudoniem
PP-BSN, PP-EU, PP-PS	Specifieke polymorfe pseudoniemen (zie bijlage B)
RFC	Request for Change
RNI	Registratie Niet-Ingezetenen
RvIG	Rijksdienst voor Identiteitsgegevens
UID	Uniqueness Identifier
Wabb	Wet algemene bepalingen burgerservicenummer
Wbp	Wet bescherming persoonsgegevens
WGDI	Wet Generieke Digitale Infrastructuur

1 Inleiding

Het Europees Parlement en de Raad hebben op 23 juli 2014 de EU-verordening (nr. 910/2014) betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt vastgesteld (hierna: “eIDAS-verordening” of kortweg “de verordening”). Deze verordening regelt een aantal zaken op het gebied van elektronische identificatie en vertrouwensdiensten voor elektronische transacties.

Voor deze Privacy Impact Assessment (PIA)[4] zijn de regels ten aanzien van elektronische identificatie van belang. Op dat vlak bewerkstelligt de verordening dat een in de Europese Unie gevestigde natuurlijke of rechtspersoon gebruik kan maken van digitale (overheids)voorzieningen in elke EU-lidstaat, door middel van verplichte wederzijdse erkenning van elektronische identiteiten tussen lidstaten. In september 2018 zal de eIDAS-verordening van kracht zijn. Dan moet het gebruik van nationale elektronische identiteiten in het buitenland mogelijk zijn, zodat burgers en ondernemers op eenvoudige wijze diensten kunnen afnemen en veilig transacties kunnen verrichten via de websites van buitenlandse overheden.

De eIDAS-verordening richt zich naast publieke dienstverleners ook op private dienstverleners. Lidstaten dienen zelfs de private sector aan te moedigen om (vrijwillig) gebruik te maken van onder eIDAS genotificeerde elektronische identificatiemiddelen. Mogelijkheden voor authenticatie moeten door lidstaten onder dezelfde voorwaarden beschikbaar worden gesteld aan private vertrouwende partijen in andere lidstaten als aan vertrouwende partijen in de eigen lidstaat.

Nederland bereidt zich hierop voor door het mogelijk te maken dat natuurlijke en rechtspersonen die de beschikking hebben over een genotificeerd EU authenticatiemiddel in kunnen loggen bij Nederlandse digitale overheidsvoorzieningen. Daarnaast gaat Nederland het voor natuurlijke en rechtspersonen met een Nederlands authenticatiemiddel technisch mogelijk maken om in te loggen bij overheidsvoorzieningen in andere EU-lidstaten. Door Nederland genotificeerde authenticatiemiddelen mogen door buitenlandse overheidsdienstverleners niet geweigerd worden.

Het Ministerie van Economische Zaken (hierna: “EZ”) is niet alleen de dossierhouder van de verordening elektronische identiteiten, maar ook beleidsverantwoordelijk. In juli 2015 heeft Privacy Management Partners voor EZ een PIA uitgevoerd voor het eIDAS-knooppunt.

EZ heeft vervolgens Logius gevraagd om een architectuur op te stellen voor de zaken die Nederland moet regelen om te kunnen voldoen aan de eIDAS-verordening. Momenteel bevindt het project zich nog in de ontwerpfase, waarbij de doelarchitectuur en de overkoepelende (project)startarchitectuur van eIDAS reeds gereed zijn. In de startarchitectuur worden de beleidskeuzes en architectuurprincipes beschreven, maar ook de technische specificaties van de koppelvlakken tussen de componenten die nodig zijn om het hele stelsel te laten werken.

Logius heeft Privacy Management Partners gevraagd een PIA uit te voeren op de overkoepelende startarchitectuur voor eIDAS, versie 1.0. Over deze overkoepelende startarchitectuur heeft Logius een tussenrapport ontvangen. De daaruit voortvloeiende aanbevelingen zijn door de opdrachtgever, voor zover hij dat mogelijk en wenselijk heeft geacht, verwerkt in de startarchitectuur, leidend tot versie 1.1. Daarna is de beoordeling geactualiseerd en vastgelegd in dit eindrapport.

[4] Wij geven de voorkeur aan de ingeburgerde term PIA boven de AVG-term DPIA (“data protection impact assessment”) of de Nederlandse vertaling daarvan, “gegevensbeschermingseffectbeoordeling”.

2 Reikwijdte

Deze PIA is beperkt tot datgene wat specifiek ingericht wordt om in Nederland te kunnen voldoen aan de eIDAS-verplichtingen op het gebied van identificatie en authenticatie, onder de aanname dat Nederland het eTD-stelsel gaat aanmelden bij de Europese Commissie. Dit is in eerste instantie uitgewerkt in de startarchitectuur van mei 2016.[5] Vervolgens is een versie 1.1 van de startarchitectuur opgesteld. Deze is beoordeeld aan de hand van het daarin opgenomen overzicht van wijzigingen.

Concreet gaat het om de eIDAS-berichtenservice en het BRP-koppelpunt. Daarnaast wordt ten behoeve van eIDAS de functionaliteit uitgebreid van het BSNk en van het eTD-stelsel.

Op deze vier componenten zullen nog specifieke PIA's worden uitgevoerd. In die PIA's zal onder meer gekeken worden naar de wijze waarop technisch invulling wordt gegeven aan de gewenste functionaliteit. Dat geldt in het bijzonder voor alle secundaire gegevensverwerking, zoals technisch noodzakelijke tijdelijke opslag en met name ook logging.

Deze PIA op de startarchitectuur eIDAS beoordeelt daarom uitsluitend voor elke component:
- het doel en de functionaliteit;
- de (persoons)gegevensverwerkende processen ten behoeve van die functionaliteit, waaronder de opslag van data binnen de component;
- alle inkomende en uitgaande stromen van persoonsgegevens.[6]

Out of scope

Het eTD-stelsel beschouwen we als gegeven. Dat geldt in het bijzonder dus ook voor:
- polymorfe pseudonimisering (binnen het eTD-stelsel overigens nog te implementeren), zowel de techniek zelf, de wijze waarop die wordt toegepast als de rol daarbij van het BSNk;
- de eisen aan het eIDAS-koppelpunt (of andere eIDAS-specifieke onderdelen) die rechtstreeks voortvloeien uit het uitgangspunt dat het eIDAS-koppelpunt zich richting het eTD-stelsel voordoet als een authenticatiedienstverlener.
  N.B. Deze eisen zijn out of scope, maar de wijze waarop daaraan invulling is gegeven is in scope. Dat het eIDAS-koppelpunt zich in technische zin *richting het eTD-stelsel moet kunnen voordoen als authenticatiedienst betekent verder niet dat het koppelpunt daarmee zonder meer ook aan alle overige eisen van het eTD-stelsel hoeft te voldoen.*

Al hetgeen er in andere lidstaten gebeurt voor wat betreft het voldoen aan eIDAS, tot aan de koppelvlakken met het Nederlandse eIDAS-knooppunt, beschouwen we als gegeven. Het is de verantwoordelijkheid van de lidstaten zelf om aan de eIDAS-verordening te voldoen.

De programmatuur van de Nederlandse eIDAS-proxy en eIDAS-connector beschouwen we als gegeven, aangezien DG DIGIT elk van de lidstaten een referentie-implementatie van de nationale eIDAS software (eIDAS-connector en eIDAS-proxy service) levert. DG DIGIT voert hierover immers ook het changemanagement en ontwikkelt de releases.

Gebruik van de eIDAS-infrastructuur voor gegevensuitwisseling met niet-EER-landen, zoals Turkije en Zwitserland, is op verzoek van opdrachtgever out of scope.

Andere eIDAS-onderdelen dan identificatie en authenticatie zijn out of scope. Het gaat hier om elektronische vertrouwensdiensten zoals elektronische handtekeningen en zegels.

[5] Inclusief een daarin later doorgevoerde wijziging.
[6] Dus zowel tussen de componenten onderling als van en naar eTD-stelsel, buitenland enz.

Tot slot bevat de PIA geen beoordeling over hetgeen door de EU dwingend is voorgeschreven. Zo is niet getoetst hoe de eIDAS-verordening en de uitvoeringsverordeningen zich verhouden tot de AVG.

In scope

Het Nederlandse eIDAS-koppelpunt, specifiek de eIDAS-berichtenservice, is volledig in scope. Dat geldt zowel voor de 'interne' gegevensopslag en -verwerking als voor alle inkomende en uitgaande gegevensstromen.

Het BRP-koppelpunt is volledig in scope . Het gaat dan om het (indien mogelijk) matchen van eIDAS minimale datasets met in de BRP[7] ingeschreven personen, en, indien dat lukt, het koppelen van het BSN van de persoon aan het UID waarmee deze is 'binnengekomen'. Eventuele aanvullende activiteiten van RvIG gericht op het (kunnen) inschrijven van een persoon in de BRP en het toekennen van een BSN vallen buiten het BRP-koppelpunt en daarmee buiten de reikwijdte van de PIA.

Zoals hierboven aangegeven beschouwen we de functionaliteit van het BSNk als gegeven. Dat geldt ook voor de interactie van het BSNk met de eIDAS-berichtenservice conform eTD-afspraken. Wel in scope is de functionaliteit van eIDAS-specifieke aanvullingen op het BSNk, maar weer niet de implementatie daarvan.

Relevante onderdelen startarchitectuur

Het bovenstaande betekent dat met name de hierna opgesomde onderdelen van de startarchitectuur versie 1.1 van belang zijn.

- Hst. 4 Use Cases
- Par. 3.1 Nederlands eIDAS-koppelpunt
- Par. 3.2 Het BRP-koppelpunt
- Par. 5.1 Gedrag eIDAS-Koppelpunten
- Par. 5.2 Gedrag BRP-Koppelpunt
- Par. 5.3 Gedrag eTD-stelsel (alleen de aanpassingen t.b.v. eIDAS)
- Par. 5.4 Gedrag BSNk (alleen de aanpassingen t.b.v. eIDAS)
- Bijlage 3 Interactie Flow bij Use Cases[8]

[7] Inclusief de RNI.
[8] Inclusief de uitwerking daarvan in de ons toegezonden Powerpoint-bestanden.

3 Verantwoording

Ter voorbereiding op dit onderzoek hebben de onderzoekers zich verdiept in de beschikbare documentatie, waaronder:

- de 'Startarchitectuur, Nationale implementatie van eIDAS met het stelsel Elektronische Toegangsdiensten', versie 1.0 (mei 2016);
- de eIDAS-verordening met de bijbehorende uitvoeringsverordeningen;
- de reactie op het verslag van de kwaliteitstoets van de startarchitectuur (24 mei 2016);
- de beschrijving van het afsprakenstelsel eTD[9];
- een beschrijving van de eIDAS use cases door de Werkgroep ontwerp en bouw eIDAS (25 augustus 2016) en het bijbehorende bestand eIDAS-RFC IVE.pptx;
- de notitie 'Wijzigingsvoorstel startarchitectuur' (30 juni 2016);
- de Privacy Impact Assessment eIDAS-knooppunt, versie 1.0 (31 juli 2015).

Vervolgens zijn er gesprekken gevoerd en workshops gehouden met de vertegenwoordigers van Logius, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), het Ministerie van Economische Zaken (EZ) en RvIG. Op basis van de aldus verkregen informatie en inzichten is een tussenrapport opgesteld en met de opdrachtgever besproken. Vervolgens zijn er conclusies en aanbevelingen geformuleerd en eveneens met de opdrachtgever besproken. Op basis daarvan is een concept eindrapport opgesteld. Mede naar aanleiding daarvan is de startarchitectuur geactualiseerd (versie 1.1). Het eindrapport is vervolgens nog aangepast op basis van een beoordeling van de startarchitectuur versie 1.1 aan de hand van het daarin opgenomen overzicht van wijzigingen.

Bij de PIA waren met name de volgende personen betrokken:

Vanuit Logius/BZK:

- dr.ir. M. Gerritsen (projectleider eIDAS)
- M.C. Menzo MA (secretaris eIDAS)
- M.R. Dollenkamp MSc (architect startarchitectuur)
- mr. E. van Geest (juriste)

Vanuit EZ:

- drs. I. Vennekens (architect startarchitectuur)

Vanuit RvIG:

- ir. E. Verweij (architect startarchitectuur)

Onderhavige PIA is uitgevoerd aan de hand van het Toetsmodel PIA Rijksdienst, een verplicht instrument voor de Rijksoverheid. Dit toetsmodel bestaat uit een verklarend deel (deel A) en een vragenlijst (deel B). De antwoorden op de vragen van deel B zijn te vinden in hoofdstuk 5.

Op 28 mei 2018 wordt de Algemene Verordening Gegevensbescherming van kracht. Vanaf dan vervangt deze Richtlijn 95/46/EG en de Wet bescherming persoonsgegevens. Aangezien de eIDAS-verordening in september 2018 van kracht wordt, is in deze PIA de AVG gehanteerd als privacyjuridisch kader voor de beoordeling.[10]

[9] Zie https://afsprakenstelsel.etoegang.nl, geraadpleegd in de periode juli t/m september 2016.
[10] Ook voor het van kracht worden van de AVG zullen sommige onderdelen van de eIDAS-infrastructuur al gaan draaien, bijv. om deze te kunnen testen. Hierop is in de huidige overgangstermijn met name nog de Wbp van toepassing. Aangezien de AVG echter op vrijwel alle onderdelen strenger of uitgebreider is dan de Wbp, levert dit geen aanvullende aandachtspunten op.

4 Kaders

De beoordeling in deze PIA geschiedt primair aan de hand van de AVG.[11] In aanvulling daarop is uiteraard ook specifieke regelgeving m.b.t. de eIDAS-infrastructuur en haar componenten van belang. Deels bestaat die al, deels is zij nog in wording. Zie paragraaf 4.1. Verder hebben er in het verleden ook al privacybeoordelingen plaatsgevonden van eIDAS. Die bespreken we in paragraaf 4.2.

4.1 Wet- en regelgeving

In paragraaf zetten we de specifieke regelgeving m.b.t. (privacyaspecten van) de eIDAS-infrastructuur en haar componenten op een rijtje. Deels bestaat die al, deels is zij nog in wording. De privacyeisen die de eIDAS-regelgeving zelf stelt, lichten we vervolgens nog uit.

4.1.1 Bestaande regelgeving

- eIDAS-verordening en Uitvoeringsverordeningen 2015/1501 en 2015/1502. Deze bevatten een aantal bepalingen die relevant zijn vanuit het oogpunt van privacy. Zie bijlage D.
- Wet elektronisch berichtenverkeer belastingdienst, Besluit verwerking persoonsgegevens generieke digitale infrastructuur, Regeling voorzieningen GDI. Deze bevatten een grondslag voor en stellen regels aan (de verwerking van persoonsgegevens door) het BSNk. De toelichting bij het Besluit gaat ook in op de verwerkersrol die authenticatiediensten hebben ten aanzien van het BSN.

4.1.2 Regelgeving in wording

- Wet generieke digitale infrastructuur (WGDI). De WGDI maakt onderdeel uit van het project Digitaal 2017. Dit project moet ervoor zorgen dat zowel burgers als ondernemers hun overheidszaken uiterlijk in 2017 digitaal kunnen regelen. De WGDI zal een aantal zaken regelen ten aanzien van onder meer eIDAS en het eTD-stelsel, maar zal geen bepalingen bevatten ten aanzien van het onderdeel “elektronische identificatie” van de eIDAS-verordening.

4.2 Eerdere privacybeoordelingen

In juli 2015 hebben wij in opdracht van het Ministerie van EZ een PIA uitgevoerd op het eIDAS-knooppunt.[12] In december 2015 heeft de Autoriteit Persoonsgegevens (AP) advies uitgebracht aan de Minister van EZ over de eIDAS-uitvoeringswet. In dat advies werd nadrukkelijk teruggegrepen op de PIA voor het eIDAS-knooppunt. Hieronder vatten we beide adviezen samen. Met het oog op de leesbaarheid hebben wij ervoor gekozen de eerdere PIA zoveel mogelijk in het huidige document te verwerken in plaats van er voortdurend naar te verwijzen. De aanbevelingen uit die PIA hebben geleid tot diverse risicomitigerende maatregelen, maar zijn daarmee niet allemaal komen te vervallen: zie bijlage C voor details.

4.2.1 PIA eIDAS-knooppunt

In juli 2015 hebben wij in opdracht van het Ministerie van EZ een PIA uitgevoerd op het eIDAS-knooppunt.[13] De belangrijkste aanbevelingen van deze PIA waren de onderstaande.

- Wet- en regelgeving
  - Schep duidelijkheid over de verantwoordelijkheid voor het eIDAS-knooppunt.
  - Creëer een expliciete wettelijke basis voor het omzetten van het BSN tot een ander persoonsnummer.
  - Leg op Europees niveau vast welke informatie betrokkenen moeten krijgen over de privacyaspecten van de eIDAS-knooppunten.

[11] Niet de Wbp, omdat die op het moment dat de eIDAS-verordening in werking treedt opgevolgd zal zijn door de AVG.
[12] Dat destijds nog abusievelijk als “eIDAS-koppelpunt” door het leven ging. Dit is in de onderhavige tekst gecorrigeerd.
[13] Zie de Memorie van Toelichting bij de Uitvoeringswet eIDAS (KS II 34413 nr. 3).

- Uniformeer de beveiligingseisen voor de eIDAS-knooppunten op EU-niveau en leg die bindend op.
- Indien het eIDAS-knooppunt wordt ondergebracht bij een of meer eID-makelaars, stel dan specifieke minimumeisen op ten aanzien van informatiebeveiliging.
- Maak eisen op het gebied van privacy en informatiebeveiliging onderdeel van de voorwaarden waaronder private dienstverleners op eIDAS mogen aansluiten.

– Inrichting van het eIDAS-knooppunt
  - Voer, voordat het eIDAS-knooppunt intern of extern wordt ondergebracht, een risico-evaluatie uit op de door de betreffende partij geboden technische en bestuurlijke omgeving.
  - Tref passende informatiebeveiligingsmaatregelen, zeker in geval er wordt gekozen voor encryptie per schakel in plaats van end-to-end encryptie.
– Verdere verloop van het ontwikkeltraject
  - Voer op Europees niveau een PIA uit op de referentie-implementaties voor de eIDAS proxy en de eIDAS-connector.
  - Voer telkens wanneer er een mogelijkheid wordt gecreëerd om via eIDAS bepaalde attributen te verwerken die buiten de verplichte en aanvullende attributen vallen zoals gedefinieerd in Europese uitvoeringshandeling 2015/1501, de zogenoemde “andersoortige attributen”, een aanvullende PIA uit.

4.2.2 Advies AP

In december 2015 heeft de Autoriteit Persoonsgegevens (AP) advies uitgebracht aan de Minister van EZ over de eIDAS-uitvoeringswet.[14] In dat advies werd nadrukkelijk teruggegrepen op de PIA voor het eIDAS-knooppunt. De hoofdpunten van het advies van de AP waren de onderstaande:

– De Memorie van Toelichting stelt dat het eIDAS-knooppunt geen andere gegevens op zal slaan dan loggegevens. Het kortstondig opslaan van gerouteerde gegevens is technisch gezien echter onvermijdelijk.
– De Memorie van Toelichting maakt duidelijk dat de Minister van EZ de verwerkingsverantwoordelijke is voor het eIDAS-koppelpunt, en bovendien wat zijn grondslag is voor de daarvoor benodigde gegevensverwerking.
– Het werken met verwerkersovereenkomsten is bedenkelijk vanwege de complexiteit en de omvang van eIDAS en het eTD-stelsel, alsook de onderlinge samenhang tussen beide.
– Het is zeer wenselijk dat er vanuit de Europese Unie bindende beveiligingseisen gesteld worden. Hoe dan ook zal de Minister van EZ primair moeten toezien op de naleving van beveiligingseisen, ook door eventuele verwerkers.
– Voor het omzetten van het BSN in een pseudoniem is een wettelijke basis vereist.
– De AP heeft bij brief van d.d. 7 mei 2015[15] haar zorgen geuit m.b.t. het eID-stelsel. Uit een globale analyse van de AP is onder meer naar voren gekomen dat de verdeling van de verantwoordelijkheden, alsmede de beveiliging van de verwerking(en) en het gebruik van het BSN onvoldoende in beschouwing zijn genomen.
– Geef in de Memorie van Toelichting aan waarom wel of geen gebruik wordt gemaakt van beleidsruimte die de eIDAS-verordening laat.

[14] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/z2015-00746_brief.pdf
[15] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_introductieplateau_eid.pdf.

5 Beoordeling

In dit hoofdstuk geven wij een beoordeling van de privacyrisico's van de startarchitectuur aan de hand van de vragenlijst van het Toetsmodel PIA Rijksdienst. De beschrijving van de in te richten eIDAS-infrastructuur beperkt zich daarbij tot de hoofdlijnen. Details zijn te vinden in de bijlagen en in de startarchitectuur zelf.

Omwille van de duidelijkheid en overzichtelijkheid hebben wij ervoor gekozen om de beantwoording van de vragen van het Toetsmodel te beperken tot die situaties die op basis van de eIDAS-verordening[16] verplicht geregeld moeten worden. Dat wil zeggen: authenticatie ten behoeve van overheidsdienstverleners waarbij slechts de minimale dataset wordt uitgewisseld. In het volgende hoofdstuk gaan we in op de andere situaties, waarbij er dus sprake is van gebruik van de eIDAS-infrastructuur door private dienstverleners en/of het uitwisselen van andersoortige attributen die buiten de verplichte en aanvullende attributen zoals gedefinieerd in Europese uitvoeringshandeling 2015/1501 vallen.

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. Wilt u als verwerkingsverantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?
Zoals in hoofdstuk 2 nader wordt toegelicht, richt deze PIA zich met name op de eIDAS-berichtenservice, het BRP-koppelpunt en (de functionaliteit die wordt toegevoegd aan) het BSNk.

Verantwoordelijkheid
De hierboven beschreven componenten zorgen er in samenhang voor dat enerzijds Nederland kan voldoen aan de uit de eIDAS-regelgeving voortvloeiende verplichting om het voor houders van EU-authenticatiemiddelen mogelijk te maken om in te loggen bij Nederlandse dienstverleners, en anderzijds dat het voor Nederlanders mogelijk wordt om met hun nationale identificatiemiddelen in te loggen bij dienstverleners in andere lidstaten. Het gaat immers om één specifiek geheel van componenten dat specifiek en uitsluitend met het oog op eIDAS wordt ingericht door EZ en BZK gezamenlijk. Doel en middelen van deze verwerking worden door beide ministers gezamenlijk vastgesteld. Er is daarmee ook sprake van gezamenlijke verantwoordelijkheid in de zin van artikel 26 AVG.

Verwerkte gegevens
Hieronder beschrijven we op hoofdlijnen welke persoonsgegevens er in het kader van eIDAS verwerkt worden. Details zijn te vinden in de startarchitectuur, alsook in de bijlagen bij dit rapport, met name bijlage A: Data flows en bijlage D: Persoonsnummers. We beperken ons hier tot de Use Cases II-A en III-A (natuurlijke personen). De Use Cases II-B en III-B komen verderop aan de orde onder het kopje "Rechtspersonen".

eIDAS is gericht op (grensoverschrijdende) online authenticatie. De startarchitectuur beschrijft de functionaliteit die noodzakelijk is om het Nederlandse eIDAS-koppelpunt in te richten, en om dat te koppelen aan enerzijds de eIDAS-knooppunten van de andere lidstaten en anderzijds het Nederlandse eTD-stelsel. De daarbij behorende gegevensverwerking bestaat primair uit het routeren van authenticatieverzoeken voor personen die gebruik willen maken van een grensoverschrijdende online dienst, en van de authenticatieberichten die daarop het antwoord vormen. Belangrijke onderdelen van de authenticatieberichten zijn identiteitsattributen en persoonsnummers.

[16] Onder de aanname dat Nederland het eTD-stelsel gaat aanmelden bij de Europese Commissie.

Terminologie
In de context van eIDAS worden diverse persoonsgegevens (attributen) verwerkt teneinde individuen te kunnen identificeren en authenticeren. Om welke attributen het concreet gaat, staat verderop onder het kopje "Attributen" beschreven. Het is van belang de terminologie duidelijk voor ogen te hebben, aangezien deze anders verwarrend kan werken. Uitvoeringsverordening 2015/1501 spreekt van een "minimaal gegevenspakket". De startarchitectuur gebruikt hiervoor de term "minimale dataset". Deze minimale dataset bestaat uit "verplichte en aanvullende attributen". Daarnaast kunnen er naast de minimale dataset nog allerlei andersoortige attributen verwerkt worden. Met andere woorden: er is sprake van een minimale dataset, en een andersoortig attribuut maakt geen onderdeel hiervan uit.

De eIDAS-verordening regelt alleen het aanleveren van attributen aan publieke dienstverleners. Wel bevat de verordening een overweging die lidstaten oproept om de eIDAS-infrastructuur ook beschikbaar te stellen aan private dienstverleners[17]. De startarchitectuur is zo ingericht dat deze ook andersoortige attributen kan verwerken.

Attributen
De eIDAS-regelgeving definieert een zogeheten *minimale dataset*. Deze minimale dataset bestaat uit twee soorten attributen. *Verplichte attributen* moeten altijd worden meegezonden als er via eIDAS een authenticatiebericht van de ene naar de andere lidstaat gaat. *Aanvullende attributen* worden meegezonden als de online dienstverlener daarom verzoekt.

De verplichte attributen voor natuurlijke personen zijn:
- de achternaam;
- de voornaam of -namen;
- de geboortedatum;
- een unieke identificatiecode (UID).

De aanvullende attributen voor natuurlijke personen zijn:
- de voor- en achternamen bij geboorte;
- de geboorteplaats;
- het huidige (woon)adres;
- het geslacht.

De lidstaten zijn zoals gezegd verplicht om bij grensoverschrijdend authenticatieverkeer in eIDAS-verband de minimale dataset te verwerken: de verplichte attributen standaard, de aanvullende attributen desgevraagd. Dat houdt echter geen verplichting in om deze attributen na ontvangst ook verder te verwerken. In het bijzonder hoeft de eIDAS-berichtenservice deze niet standaard door te sturen aan de publieke dienstverlener die het authenticatieverzoek heeft gedaan. In plaats daarvan zoekt de berichtenservice uit het oogpunt van dataminimalisatie in de dienstencatalogus van het eTD-stelsel op welke attributen de publieke dienstverlener nodig heeft voor het kunnen verlenen van de gevraagde dienst.

Lidstaten kunnen met elkaar afspraken maken over het via de eIDAS-infrastructuur uitwisselen van andere attributen dan die uit de minimale dataset. De privacyaspecten van deze *andersoortige attributen (buiten de minimale dataset)* komen in het volgende hoofdstuk aan bod.

[17] Zie overweging (17): "De lidstaten dienen de private sector aan te moedigen vrijwillig gebruik te maken van elektronische identificatiemiddelen die onder een aangemeld stelsel vallen, indien identificatie bij onlinediensten of elektronische transacties nodig is".

Persoonsnummers
Voor betrouwbare identificatie zijn *persoonsnummers* onontbeerlijk. Met een 'persoonsnummer' bedoelen we hier iedere identificatiecode die bedoeld is om een natuurlijke persoon uniek te vertegenwoordigen. In de Nederlandse eIDAS-implementatie figureren in de eerste plaats twee 'basispersoonsnummers': het burgerservicenummer (BSN) en de hierboven geïntroduceerde unieke identificatiecode (UID). Het UID is door eIDAS voorgeschreven; de bedoeling is dat authenticatieberichten vanuit een lidstaat aan overheidsdiensten in een andere lidstaat die betrekking hebben op dezelfde persoon altijd hetzelfde UID bevatten. Naast deze basispersoonsnummers maken eIDAS-berichtenservice, BRP-koppelpunt en BSNk gebruik van polymorfe pseudonimisering, een functionaliteit van het eTD-stelsel. Zie verder het antwoord op vraag 2, subvraag e en bijlage B.

Rechtspersonen
Vanuit privacyoogpunt zijn de gegevens die verwerkt worden in de Use Cases II-A en III-A, zoals hierboven, het belangrijkst. Deze gaan immers over authenticatie van natuurlijke personen. De Use Cases II-B en III-B, die gaan over rechtspersonen, mogen echter niet zonder meer veronachtzaamd worden.

Voor rechtspersonen bestaat de minimale dataset uit de onderstaande verplichte en aanvullende attributen.[18]

De verplichte attributen voor rechtspersonen zijn:
- de huidige wettelijke naam;
- de unieke identificatiecode.

De aanvullende attributen voor rechtspersonen zijn:
- het huidig adres;
- het btw-nummer;
- het fiscaal referentienummer;
- het vennootschapsnummer;
- het identificatienummer voor juridische entiteiten;
- het EORI-nummer;
- het accijnsnummer;
- de bedrijfsindelingscode.

Gegevens over bedrijven kunnen onder omstandigheden ook persoonsgegevens zijn. De Artikel 29-Werkgroep[19] citeert in dit verband de e-privacyrichtlijn:

> *[I]nformatie over rechtspersonen [kan] ook op eigen merites worden beschouwd als informatie "betreffende" natuurlijke personen. Dat kan het geval zijn als de naam van de rechtspersoon is afgeleid van de naam van een natuurlijke persoon. Een andere geval kan zich voordoen bij bedrijfs-e-mail, die normaliter wordt gebruikt door een specifieke werknemer, of bij informatie over een klein bedrijf (rechtens eerder een voorwerp dan een rechtspersoon) die ook iets zegt over het gedrag van de eigenaar. Wanneer informatie over een rechtspersoon of een bedrijf op grond van de criteria "inhoud", "doel" of "resultaat" kan worden beschouwd als informatie "betreffende" een natuurlijke persoon, geldt in al deze*

[18] Zie voor een toelichting op de verschillende onder 'aanvullende attributen' genoemde nummers de verwijzingen in Uitvoeringsverordening 2015/1501 naar andere EU-regelgeving.
[19] De Artikel 29-Werkgroep is het officiële, onafhankelijke advies- en overlegorgaan van de Europese privacytoezichthouders. Zij speelt een belangrijke rol in de totstandkoming van Europees beleid voor de bescherming van persoonsgegevens.

gevallen dat deze informatie als persoonsgegeven moet worden beschouwd en dat de regels voor gegevensbescherming van toepassing moeten zijn.

Het hier genoemde voorbeeld van de naam van de rechtspersoon die afgeleid is van de naam van een natuurlijke persoon, is relevant in de context van eIDAS. Immers, de huidige naam van de rechtspersoon is naast het UID nu juist het enige verplichte attribuut, dat dus in alle eIDAS-authenticatieberichten per definitie vermeld wordt. Het is bijgevolg heel goed mogelijk dat hier sprake is van een persoonsgegeven. Vaak zal dat ook niet zo zijn, maar binnen de eIDAS-infrastructuur is er geen mogelijkheid om na te gaan wat nu het geval is. Het is daardoor onvermijdelijk om de verplichte attributen over rechtspersonen te behandelen als persoonsgegevens. Ook sommige aanvullende attributen kunnen persoonsgegevens zijn, in het bijzonder het huidige adres (zal bijvoorbeeld bij eenmanszaken vaak het woonadres van de eigenaar zijn) en het btw-nummer (bevat voor Nederlandse eenmanszaken het BSN van de eigenaar). Ook deze zullen dus als persoonsgegevens behandeld moeten worden. Dat gezegd hebbend, zien wij geen aanvullende aandachtspunten in verband met deze attributen. Er zijn dus uiteindelijk geen gevolgen voor de beoordeling van de privacyrisico's.[20]

Voor de goede orde plaatsen wij bij deze laatste conclusie twee kanttekeningen.
Het kan op het eerste gezicht verwondering wekken dat het niet als een privacyrisico wordt aangemerkt dat voor eenmanszaken het BSN in de vorm van het btw-nummer over de lijn gaat, terwijl datzelfde BSN in de eIDAS-infrastructuur zo zorgvuldig afgeschermd wordt waar mogelijk. Dit is echter een onvermijdelijk gevolg van de Nederlandse keuze om het btw-nummer te baseren op het BSN, aangezien op basis van de eIDAS-regelgeving het btw-nummer als optioneel attribuut desgevraagd verplicht meegezonden moet worden.
Daarnaast kan het gebruik van andersoortige attributen buiten de minimale dataset ook hier extra privacyrisico's met zich meebrengen. Zie daarvoor het volgende hoofdstuk.

2. Andere specifieke persoonsgegevens?
Let op: zoals in de inleiding van dit hoofdstuk is aangegeven, zijn de antwoorden op de deelvragen hieronder van toepassing op de minimale dataset, *niet* op eventuele andersoortige attributen buiten die minimale dataset.[21]

a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?
Nee. De verplichte en aanvullende attributen uit de minimale dataset bevatten niet van zulke gegevens.

b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?
Nee. Het gericht verwerken van gegevens over kwetsbare groepen of personen is geen doelstelling van eIDAS. Maar aangezien eIDAS een generieke voorziening is, zullen er onvermijdelijk ook gegevens van kwetsbare personen of personen uit kwetsbare groepen bij het eIDAS-koppelpunt passeren. Deze zijn echter niet direct als zodanig herkenbaar. Wel kan de eIDAS-berichtenservice in de Use Cases II-A en II-B zien welke dienst iemand van welke overheidsinstantie wil afnemen. Dat kan een indicatie zijn dat iemand mogelijk tot een bepaalde kwetsbare groep behoort. De berichtenservice slaat echter geen historie op van authenticatieverzoeken. Zij heeft dus geen zicht op de frequentie van dit soort verzoeken, en is evenmin in staat om verzoeken aan verschillende overheidsinstanties aan elkaar te relateren.

[20] Met dien verstande, dat de privacyrisico's voor individuele personen ook deels voor rechtspersonen gelden.
[21] Zie daarvoor het volgende hoofdstuk.

c. Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?
Nee.[22] Burgers kunnen immers niet inloggen op componenten van de eIDAS-infrastructuur. Gebruikersnamen, wachtwoorden en andere inloggegevens kunnen uiteraard wel een rol spelen bij de authenticaties waarvan de resultaten door de eIDAS-infrastructuur gerouteerd worden. De authenticatieberichten bevatten echter niet zelf deze gegevens, alleen informatie over het resultaat van een poging tot authenticatie.

d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?
Nee. Hiervoor gelden dezelfde kanttekeningen als bij de vorige deelvraag.

e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?
Ja. Bijlage B "Persoonsnummers" gaat uitvoerig in op de verschillende persoonsnummers binnen de eIDAS-infrastructuur en hun rol en functie. Welke persoonsnummers er waar worden opgeslagen en uitgewisseld staat beschreven in hoofdstuk 3 t/m 5 van de startarchitectuur. In het kort komt dit neer op het onderstaande.

De startarchitectuur kent een tweetal 'basispersoonsnummers', te weten het BSN en de UID's. Daarnaast wordt er gewerkt met polymorfe pseudonimisering. Het BSN wordt gebruikt wanneer een overheidsdienstverlener aangeeft dat voor een bepaalde dienst een BSN vereist is.[23] UID's moeten uit hoofde van de eIDAS-regelgeving verplicht gebruikt worden bij het grensoverschrijdend uitwisselen van authenticatiegegevens, en dienen zo persistent mogelijk te zijn. Om te kunnen aansluiten op het eTD-stelsel, en met het oog op privacybescherming en de verplichting om privacy-by-design toe te passen, werkt de eIDAS-infrastructuur in plaats van met deze basispersoonsnummers zelf, zo veel mogelijk met daarvan afgeleide zogeheten polymorfe pseudoniemen (PP's). Deze worden aangemaakt door het BSNk en opgeslagen bij de berichtenservice, die ze aan het bijbehorende UID koppelt. Het polymorfe pseudoniem kan gebaseerd zijn op het BSN (PP-BSN) of op het UID (PP-EU). Voor een specifiek buitenlands authenticatieverzoek (Use Case II) wordt het polymorfe pseudoniem door het BSNk omgezet in een dienstverlenerspecifiek pseudoniem. Bij BSN-diensten kan de dienstverlener uit het pseudoniem het BSN afleiden. Voor niet BSN-diensten wordt het pseudoniem gebaseerd op het UID, dat er echter niet uit afgeleid kan worden door de dienstverlener. Die ontvangt voor hetzelfde buitenlandse UID echter wel telkens hetzelfde pseudoniem. De eerste keer worden voor een gebruiker van een BSN-dienst een PP-EU, PP-PS en een PP-BSN aangemaakt. Voor een niet BSN-dienst wordt alleen een PP-EU aangemaakt.

Voor personen die zich op basis van het eTD-stelsel bij buitenlandse dienstverleners willen authenticeren maakt de eIDAS-berichtenservice (met behulp van het BSNk, en voor zover nodig) per lidstaat verschillende, onderling niet te relateren UID's aan. Uit deze UID's is het BSN niet af te leiden. Er wordt dus op geen enkele manier ooit een BSN verstrekt aan een andere lidstaat.

Een en ander houdt ook in dat de eIDAS-berichtenservice nooit een onversleuteld BSN krijgt aangeleverd of kan achterhalen.

Juridische aspecten verwerking BSN
Uitvoeringsverordening 2015/1501 bij de eIDAS-verordening bepaalt in art. 11 lid 1:

[22] Zoals vrijwel alle informatiesystemen waarin persoonsgegevens worden verwerkt, zullen ook de eIDAS-componenten inloggegevens verwerken over de gebruikers van het systeem. Deze secundaire gegevensverwerking valt echter buiten de reikwijdte van deze PIA.
[23] Dit speelt alleen in Use Case II-A, bij authenticatie met een middel uit een andere lidstaat.

Het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of een rechtspersoon op unieke wijze vertegenwoordigt, voldoet bij gebruik in een grensoverschrijdende context aan de vereisten die in de bijlage zijn opgenomen.

En in de bijlage:

Vereisten betreffende het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of rechtspersoon op unieke wijze vertegenwoordigt, als bedoeld in artikel 11

Minimaal gegevenspakket voor een natuurlijke persoon

Het minimale gegevenspakket voor een natuurlijke persoon bevat al de volgende verplichte attributen: ...
d) unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft.

De vraag is wat dit in de huidige juridische context (dat wil zeggen: uitgaande van de AVG en ongewijzigde regels over het BSN) betekent voor het mogen of moeten gebruiken van het BSN in de Nederlandse eIDAS-implementatie.[24]

Relevant in dat verband zijn met name de artikelen 10 en 11 van de Wet algemene bepalingen gebruik burgerservicenummer (Wabb):

Artikel 10

Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik maken van het burgerservicenummer, met inachtneming van hetgeen bij of krachtens dit hoofdstuk is bepaald.

Artikel 11

(1) Bij het uitwisselen van persoonsgegevens tussen gebruikers onderling, waarbij een persoonsnummer wordt gebruikt als middel om persoonsgegevens in verband te brengen met een persoon aan wie een burgerservicenummer is toegekend, wordt het burgerservicenummer van die persoon vermeld.

(2) Het eerste lid is niet van toepassing voor zover:

(a). ten behoeve van de desbetreffende gegevensverwerking bij of krachtens wet het gebruik van een ander persoonsnummer dan het burgerservicenummer is voorgeschreven;

Art. 11 lid 1 bepaalt, kort gezegd, dat als een overheidsinstantie een persoonsnummer gebruikt voor het koppelen van de gegevens van iemand die een BSN heeft, zij dat BSN bij die gegevens moet vermelden.

Art. 11 lid 2 onder a bepaalt, kort gezegd, dat die verplichting uit het eerste lid niet geldt als de wet voorschrijft dat de overheidsinstantie een ander nummer gebruikt.

[24] N.B. We beperken ons ook hier tot het gebruik van de eIDAS-infrastructuur door Nederlandse overheidsdienstverleners.

Dat andere nummer is in de eIDAS-context het UID (unieke identificatiecode).

Allereerst concluderen wij op basis van art. 10 Wabb dat er in beginsel geen bezwaar is dat overheidsdienstverleners, die eIDAS implementeren, het BSN gebruiken. Merk op dat dit in het bijzonder betekent dat er een onjuistheid zat in onze PIA op het eIDAS-knooppunt van vorig jaar: daarin gaven we immers aan dat er nog een wettelijke basis gecreëerd moest worden voor het pseudonimiseren van het BSN, maar dat lijkt dus niet nodig te zijn. Ook dat valt te scharen onder art. 10 Wabb.[25]

De volgende vraag is in hoeverre gebruik van het UID is voorgeschreven in de zin van art. 11 lid 2 onder a Wabb. De eIDAS-verordening schrijft gebruik van het UID voor met het oog op de interoperabiliteit tussen lidstaten, maar zegt niets over gebruik van het UID in de nationale eIDAS-implementaties. Onzes inziens is er dus, als het gaat om de Nederlandse eIDAS-implementatie, geen sprake van dat het gebruik van een ander nummer dan het BSN is voorgeschreven (althans niet het UID).

Als dat zo is, dan is de uitzondering van art. 11 lid 2 onder a niet van toepassing, en is derhalve art. 11 lid 1 van toepassing. De vervolgvraag is dan in hoeverre er in de eIDAS-implementatie sprake is van het gebruik van persoonsnummers anders dan het BSN. Het lijkt ons evident dat dit het geval is. Al het gegevensverkeer van eIDAS gaat vergezeld van persoonsnummers, te weten het UID en pseudoniemen (gebaseerd op het UID of het BSN), en de bedoeling van die persoonsnummers is om de betreffende persoon op unieke wijze te vertegenwoordigen. Wellicht worden de persoonsnummers niet in de hele implementatie zo gebruikt (technisch kun je berichten ook anders aan elkaar koppelen, en het lijkt ons zelfs waarschijnlijk dat daar de persoonsnummers niet voor gebruikt worden), maar uiteindelijk zijn ze daar wel voor bedoeld.

Dit alles leidt ons tot de onderstaande conclusies.

Voor personen die een BSN hebben, en voor zover het gaat om het gebruik van de eIDAS-infrastructuur door overheidsdienstverleners:

- *mag* een overheidsinstantie het BSN verwerken, mits dit toegestaan wordt door de privacywetgeving;[26]

- *moet* de eIDAS-infrastructuur bij berichten die het UID of eTD-persoonsnummers bevatten altijd ook het BSN meesturen,

- *tenzij* het gebruik van het UID of de eTD-persoonsnummers bij of krachtens wet wordt voorgeschreven.

Uiteraard is het niet de bedoeling om bij al het eIDAS-berichtenverkeer het BSN mee te sturen. In aansluiting op het eTD-stelsel wordt er immers nu juist gebruik gemaakt van polymorfe pseudonimisering om te voorkomen dat het BSN door het hele stelsel verspreid raakt en gebruikt wordt voor diensten waarvoor het niet vereist is. Om dit beoogde gebruik van UID's en polymorfe pseudoniemen zonder begeleidend BSN mogelijk te maken, zal het blijkens het bovenstaande wettelijk verplicht moeten worden gesteld. Het ligt voor de hand om dat te doen in de Wet GDI. Het zou wellicht mogelijk zijn om met de geest van de wet in het achterhoofd hierboven naar een andere uitkomst te redeneren. Dat laat echter onverlet dat dit punt tot veel discussie kan leiden als het niet helder geregeld wordt.

[25] Zie ook artikel X, lid 3 Wet EBV.
[26] In het bijzonder is hiermee voorzien in de wettelijke grondslag die art. 24 Wbp vereist.

Het BRP-koppelpunt houdt bij welke UID's gekoppeld zijn aan welke versleutelde BSN's. De noodzaak hiertoe is voldoende onderbouwd. Zie de paragraaf getiteld "Opslaan UID bij BRP-koppelpunt" achteraan bijlage B.

3. Kan van elk van de onder vraag 1 en vraag 2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.
Bij de vragen 1 en 2 zijn twee soorten persoonsgegevens besproken: (identiteits)attributen en persoonsnummers.

Waar het gaat om gegevensuitwisseling met de eIDAS-knooppunten uit andere lidstaten ontvangt en verstrekt het Nederlandse eIDAS-koppelpunt alleen die gegevens waartoe de eIDAS-regelgeving ook verplicht[27], te weten het UID en de minimale dataset. Voor beide Use Cases geldt dat de aanvullende attributen uit de minimale dataset alleen worden doorgegeven als daarom wordt gevraagd.[28]

Voor de gegevensopslag en gegevensstromen in de startarchitectuur geldt, met inachtneming van onderstaande kanttekeningen, dat deze noodzakelijk zijn om de verplichte eIDAS-gegevensuitwisselingen te faciliteren, waaronder het verzorgen van de aansluiting op het eTD-stelsel.

- Het verwerken van het BSN in de Nederlandse eIDAS-implementatie, waaronder het omzetten ervan in pseudoniemen, heeft een wettelijke basis in het hierboven geciteerde art. 10 Wabb.

- Het verwerken van polymorfe pseudoniemen is een vorm van privacy-by-design[29] die bedoeld is om zoveel mogelijk de mogelijkheden te beperken om gegevens te koppelen waar dat niet noodzakelijk is.

- Het PP-PS wordt in deze architectuurfase al wel aangemaakt en opgeslagen, maar nog niet aan een directe, concrete doelstelling voor gebruik gekoppeld. De reden hiervoor is dat in de volgende architectuurfase aanvullende functionaliteit wordt voorzien ten aanzien van het bestrijden van fraude en misbruik. Het PP-PS is juist bedoeld om daarbij een privacy-by-design aanpak te ondersteunen. In die zin worden door middel van de hier op voorhand beschreven verwerking van het PP-PS privacyrisico's gemitigeerd, aangezien het hier uitsluitend voor wordt aangemaakt en op één plek aan een UID wordt gekoppeld. De reden waarom er nu al in deze architectuurfase voorzieningen voor het verwerken van het PP-PS worden getroffen, is dat als wanneer dit pas in een latere fase zou moeten gaan gebeuren, dit onnodig veel wijzigingen en kosten met zich mee zou brengen. Om deze redenen beoordelen wij het aanmaken en opslaan van het PP-PS binnen de context van deze PIA als niet problematisch.

- Of een dienstverlener de attributen of het BSN waar hij om vraagt ook daadwerkelijk vereist, is primair aan de dienstverlener zelf ter beoordeling. Dit is niet de verantwoordelijkheid van de

[27] Waar het Use Case III betreft: aangenomen dat het noodzakelijk wordt geacht om als Nederland een stelsel van elektronische identificatie, concreet: het eTD-stelsel, aan te melden bij de EU, opdat het mogelijk wordt om met eTD-authenticatiemiddelen in te loggen bij overheidsdienstverleners in andere lidstaten.
[28] In Use Case II staat dat gespecificeerd in het authenticatieverzoek dat vanuit het buitenland binnenkomt. In Use Case III haalt de eIDAS-berichtenservice deze informatie uit de dienstencatalogus van het eTD-stelsel.
[29] Zoals bedoeld in artikel 25 AVG.

eIDAS-infrastructuur. Wel sluit de infrastructuur hiervoor aan op het eTD-stelsel door in Use Case II deze informatie op te halen uit de dienstencatalogus die aldaar wordt bijgehouden.[30]

4. Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?
Niet van toepassing.

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?
De eIDAS-infrastructuur wordt ontwikkeld om enerzijds te voldoen aan de verplichting die voor Nederland voortvloeit uit de eIDAS-regelgeving om het voor houders van EU-authenticatiemiddelen mogelijk te maken om in te loggen bij Nederlandse dienstverleners, en om het anderzijds voor Nederlanders mogelijk te maken om met hun nationale identificatiemiddelen in te loggen bij dienstverleners in andere lidstaten. Het eTD-stelsel speelt een belangrijke rol, omdat het in beide Use Cases noodzakelijk is om de koppeling met andere lidstaten te effectueren.
Er komt in Nederland geen aanvullende wet- en regelgeving voor dit onderdeel van eIDAS.[31] Indirect van belang voor eIDAS is de Uniforme Set van Eisen die door BZK wordt ontwikkeld voor het verlenen van authenticatiediensten ten behoeve van het publieke domein. Deze zal een plaats krijgen in de Wet op de generieke digitale infrastructuur (Wet GDI).[32] In deze wet zou onder meer ook het eIDAS-koppelpunt een duidelijke plek moeten krijgen, nu is gebleken dat dat meer omvat dan het eIDAS-knooppunt waarover de eIDAS-regelgeving spreekt.[33]

II. Doelbinding, koppeling, kwaliteit en profilering

Doeleinden/doelbinding en koppeling

6. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?
De doelstellingen voor het verwerken van persoonsgegevens door het eIDAS-systeem zijn vastgelegd in de eIDAS-verordening. In de startarchitectuur worden die doelstellingen vertaald naar de architectuur die daarin beschreven wordt. Het doel van de verwerking van persoonsgegevens in de startarchitectuur is het faciliteren van grensoverschrijdende dienstverlening binnen de EU/EER door het routeren van het daarvoor benodigde gegevensverkeer over authenticatie (authenticatiedienst) van burgers en bedrijven naar publieke en private dienstverleners, opdat burgers en bedrijven zich ook in andere lidstaten kunnen authenticeren met hun nationale identificatiemiddel.

Het inrichten van een eIDAS-knooppunt en het daarop aansluiten van genotificeerde stelsels voor elektronische identificatie van andere lidstaten zijn expliciete verplichtingen uit de eIDAS-verordening

[30] Dit is voor wat betreft de diensten catalogus tegelijkertijd een vorm van privacy by design (dataminimalisatie) als bedoeld in artikel 25 AVG.
[31] Zie de Memorie van Toelichting bij de Uitvoeringswet eIDAS (KS II 34413 nr. 3), blz. 10: “De eidas-verordening maakt zowel feitelijke uitvoeringswerkzaamheden als aanpassing van regelgeving noodzakelijk. Het deel van de eidas-verordening over elektronische identificatie vereist enkel feitelijke uitvoering.”
[32] Deze bepalingen in de Wet GDI zullen dan uiteraard wel zo geformuleerd dienen te worden dat deze het dataverkeer met de eIDAS-componenten toelaten.
[33] Zie hoofdstuk 7 direct onder “Bron PIA”.

en de daarmee samenhangende uitvoeringsverordeningen. Het aan de eIDAS-infrastructuur koppelen van het eTD-stelsel is zeer bevorderlijk voor de mogelijkheden voor Nederlandse burgers om zich online te identificeren bij dienstverleners in andere lidstaten. Daarmee is het doel van de eIDAS-infrastructuur legitiem en welbepaald (art. 5 lid 1 onder b AVG).

Het doel van de verwerking van persoonsgegevens in de eIDAS-infrastructuur kan als volgt worden omschreven: "Het faciliteren van grensoverschrijdende dienstverlening binnen de EU/EER door het van en naar Nederland routeren van het daarvoor benodigde gegevensverkeer over authenticatie (authenticatiedienst) van burgers en bedrijven richting online dienstverleners, opdat deze burgers en bedrijven zich kunnen authenticeren met hun nationale identificatiemiddel."

Bovenstaande hoofddoelstelling van de eIDAS-infrastructuur vertaalt zich op onderstaande wijze tot doeleinden van de verwerking door de vier hoofdcomponenten.

eIDAS-berichtenservice
Het voornaamste doel van de verwerking van persoonsgegevens door de eIDAS-berichtenservice is het routeren van authenticatieverzoeken en authenticatieberichten tussen enerzijds het eTD-stelsel en anderzijds (via de eIDAS-connector en proxy service) de eIDAS-knooppunten in andere lidstaten anderzijds. Om dat te kunnen doen transformeert de berichtenservice eIDAS-berichten naar eTD-berichten en andersom. Ook zorgt de berichtenservice voor het benodigde gegevensverkeer met het BRP-koppelpunt en het BSNk.

BRP-koppelpunt
Het doel van de verwerking van persoonsgegevens bij het BRP-koppelpunt is het ontsluiten van persoonskenmerken van Nederlandse natuurlijke personen en niet-ingezetenen. Daartoe gaat het BRP-koppelpunt na of een natuurlijk persoon die gebruik maakt van een buitenlands authenticatiemiddel, en die verzoekt om een BSN-dienst, staat opgenomen in de Basisregistratie personen (BRP). Is dat niet het geval, dan kan het proces pas verder gaan nadat (buiten eIDAS om) een BSN is verkregen.[34]

BSNk
Het BSNk is een bouwblok van de GDI. Voor wat eIDAS betreft, gaat het BSNk zorg dragen voor het omzetten van het BSN en het UID in polymorfe pseudoniemen. Daarnaast zet het BSNk deze polymorfe pseudoniemen in concrete gevallen om tot dienstverlenerspecifieke pseudoniemen.

Voor al deze componenten wordt in de startarchitectuur op basis van de taak zoals hierboven beschreven aangegeven welke eisen worden gesteld om die taak te kunnen uitvoeren, en welke persoonsgegevens vervolgens voor die taken via interfaces onderling worden uitgewisseld (zowel input als output). In tabellen (hoofdstuk 4) is inzichtelijk gemaakt welke service, door welke actor/consumer welke input/output data voor welk doel verwerkt. Hiermee is feitelijk de verwerking van specifieke persoonsgegevens voor specifieke doelen tot op detailniveau vastgesteld.

Tijdens het uitvoeren van de PIA is, anders dan in dit rapport expliciet wordt vermeld, op dit detailniveau niet kunnen blijken van persoonsgegevens die niet voor een specifiek doel worden verwerkt.

[34] In een enkel geval kan de overheidsdienstverlener ook besluiten om (een variant van) de dienst te verlenen zonder dat de aanvrager beschikt over een BSN.

7. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).

8. Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

De vragen 7 en 8 lenen zich voor een integrale beantwoording en beoordeling. Vraag 7 richt zich ten aanzien van het eIDAS-koppelpunt met name op het principe van dataminimalisatie. Vraag 8 richt zich op het principe van verenigbaarheid. Feitelijk komt het bij het eIDAS-koppelpunt neer op een vervlechting van beide onderwerpen.

Het Nederlandse eIDAS-koppelpunt is een aan het eTD-stelsel gekoppelde nieuwe voorziening voor grensoverschrijdende authenticatie. Burgers en bedrijven in Nederland kunnen met hun nationale toegangsmiddelen in de EU/EER-lidstaten inloggen bij overheids- en private dienstverleners. Omgekeerd kunnen burgers en bedrijven uit de EU/EER in Nederland inloggen. Het eIDAS-koppelpunt wordt, zoals eerder vermeld, ontworpen om aan de eIDAS-verordening te kunnen voldoen.

Het eIDAS-koppelpunt haakt hiermee ook aan bij het eTD-stelsel. Het koppelpunt voegt als het ware “functionaliteit” toe aan het eTD-stelsel. Het eIDAS-koppelpunt faciliteert de interoperabiliteit tussen het Nederlandse eTD-stelsel en buitenlandse eIDAS-koppelpunten. Richting de buitenlandse eIDAS knooppunten voldoet het Nederlandse koppelpunt aan de eIDAS-standaard, en richting het eTD-stelsel aan de daar geldende standaarden.

Dit impliceert, dat het eIDAS-koppelpunt voor zijn dienstverlening maximaal gebruik maakt van bestaande componenten van het eTD-stelsel, zoals authenticatiediensten en herkenningsmakelaars, en van het BSNk. Feitelijk is het dus een uitbreiding op onderdelen van reeds in het eTD-stelsel aanwezige functionaliteiten, specifiek gericht op het via het eTD-stelsel grensoverschrijdend inloggen vanuit Nederland en omgekeerd vanuit de EU/EER-lidstaten. Die functionaliteit biedt het eIDAS-koppelpunt immers. Daarbij worden door het eIDAS-koppelpunt en het BRP-koppelpunt dus nieuwe gegevens gebruikt voor een nieuw doel, te weten het voldoen aan de doelstellingen van de eIDAS-verordening.

In Use Case II-A bijvoorbeeld (vanuit het buitenland inloggen op een BSN-dienst in Nederland) betreft het hier deels nieuwe gegevens, namelijk de gegevens die hiervoor in de verordening zijn gedefinieerd (in ieder geval het UID, en tot op zekere hoogte mogelijk ook attributen uit de minimale dataset), en het genereren van het PP-EU, het PP-PS, het PP-BSN en de dienstverlenerspecifieke versleutelde pseudoniemen (EP’s). In dit proces wordt ook gebruik gemaakt van al bestaande gegevens, namelijk het door het BRP-koppelpunt gebruiken van persoonsgegevens uit de BRP om na te gaan of een persoon een BSN heeft. De verplichte attributen en de aanvullende attributen zijn persoonsgegevens die voor het grootste deel in het eTD-stelsel ook al worden gehanteerd. De vertaling door de eIDAS-berichtenservice van eIDAS-attributen naar eTD-attributen en omgekeerd duidt hier ook op.

In de startarchitectuur is tot in detail beschreven welke persoonsgegevens voor welke doeleinden door welke componenten van het eIDAS-koppelpunt worden verwerkt. In de antwoorden hierboven op de vragen 1 tot en met 6 wordt dit eveneens uitgewerkt. In de Use Cases is inzichtelijk gemaakt hoe de

afhandeling van grensoverschrijdende authenticatieverzoeken verloopt, zowel vanuit Nederland als vanuit de EU/EER-lidstaten, alsook de interactie met het eTD-stelsel.

Tegen de hierboven beschreven achtergrond kan voor wat betreft het eIDAS-koppelpunt het onderstaande gesteld worden.

1. Het gaat bij het eIDAS-koppelpunt voor een deel om het gebruik van nieuwe persoonsgegevens voor bestaande doelen binnen een al bestaand systeem (het eTD-stelsel).
2. Het gaat het bij het eIDAS-koppelpunt deels ook om het nastreven van nieuwe c.q. aanvullende doeleinden door nieuwe en bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, te vergelijken, te delen, te koppelen of anderszins verder te verwerken (eIDAS-verordening als 'nieuwe' aanvulling op het eTD-stelsel).

Na een beoordeling van het geheel komen wij tot de conclusie, dat de principes dataminimalisatie[35] en verenigbaarheid bij het verwerken van persoonsgegevens door het eIDAS-koppelpunt (inclusief de interactie met het eID-stelsel) worden gerespecteerd. Binnen de scope van deze PIA signaleren wij hier geen andere privacyrisico's dan reeds besproken in de antwoorden op de eerdere vragen en in het volgende hoofdstuk.

9. Indien u positief hebt geantwoord op vragen 7 of 8, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) de Autoriteit Persoonsgegevens (AP) indien er geen FG is?
Zie ook het antwoord op vraag 1. De verwerkingen van het eIDAS-koppelpunt zullen worden gemeld bij de FG van het Ministerie van EZ. De verwerkingen van het BRP-koppelpunt worden gemeld bij de FG van het Ministerie van BZK.

10. Indien u positief geantwoord hebt op vragen 7 of 8, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?
Gelet op de verwijzing naar de vragen 7 en 8 richt deze vraag zich met name op de controles die nodig zijn aan om te waarborgen dat voldaan wordt aan de principes dataminimalisatie en verenigbaarheid.

Ook deze vraag leent zich voor een integrale beantwoording. Voor deze beantwoording hebben wij voor wat betreft controles in het kader van dataminimalisatie en verenigbaar gebruik van data in de authenticatieprocessen geput uit de Use Cases (zie hoofdstuk 4 van de startarchitectuur), waarin deze controles zijn verweven in de daarin beschreven stappen.

Het gaat onder meer om de volgende controles:

Use Case II-A (inloggen in Nederland bij niet BSN-dienst)

- De eIDAS-berichtenservice bevraagt na ontvangst van een autheticatieverzoek van de eTD-makelaar de eTD-stelselcatalogus voor het vereiste betrouwbaarheidsniveau, benodigde attributen en de indicatie BSN-dienst. Hiermee controleert de eIDAS berichtenservice of er niet te veel attributen of onnodig het BSN worden gevraagd.
- De eIDAS-berichtenservice vormt het eTD-bericht om tot het eIDAS bericht, ondertekent het en stuurt het bericht door naar de NL eIDAS-connector.
- De eIDAS-berichtenservice controleert een bericht op integriteit en veiligheid.

[35] Behoudens de opmerkingen aan het eind van het antwoord op vraag 3, waarnaar kortheidshalve wordt verwezen.

– De eIDAS-berichtenservice controleert of het pseudoniem (PP-EU) behorende tot deUID al in de eIDAS-koppeltabel voorkomt. Als dit zo is, wordt rechtstreeks de BSNk aangeroepen voor het aanmaken van een DV PP-EU.
– De eTD-makelaar verifieert het bericht en toetst of de authenticatie voldoende betrouwbaar was (LOA).

Use Case II-A (inloggen in Nederland bij een BSN-dienst)
– De eIDAS-berichtenservice bevraagt na ontvangst van een authenticatieverzoek van de eTD-makelaar de eTD-stelselcatalogus voor het vereiste betrouwbaarheidsniveau, benodigde attributen en de indicatie BSN-dienst. Hiermee controleert de eIDAS-berichtenservice of er niet te veel attributen of onnodig het BSN worden gevraagd.
– De eIDAS-berichtenservice vormt het eTD bericht om tot het eIDAS bericht, ondertekent het en stuurt het bericht door naar de NL eIDAS-connector.
– De eIDAS-berichtenservice controleert een bericht op integriteit en veiligheid.
– De eIDAS-berichtenservice controleert of het pseudoniem (PP-BSN) behorende tot deUID al in de eIDAS koppeltabel voorkomt. Als dit zo is, wordt rechtstreeks de BSNk aangeroepen voor het aanmaken van een DV PP-BSN.
– De eTD-makelaar verifieert het authenticatie bericht van de eIDAS berichtenservice en toetst of de authenticatie voldoende betrouwbaar is voordat het naar de dienstverlener gaat (LOA).
– Als bij controle stap 10 geen UID wordt gevonden, dat volgt eerst een valideer proces. De eIDAS-berichtenservice stuurt de attributen van de persoon naar het BRP koppelpunt.
Het BRP koppelpunt probeert een match met een bekende identiteit tot stand te brengen. Als de matching niet lukt, worden aanvullende authenticatieprocessen uitgevoerd.

Use Case III-A (vanuit Nederland inloggen bij dienstverlener in andere lidstaat)
– De eIDAS-berichtenservice bepaalt aan de hand van de attributen die de buitenlandse eIDAS-connector vraagt of het een authenticatieverzoek voor een natuurlijke persoon (III-A) of een niet-natuurlijk persoon (III-B) is.
– De eIDAS-berichtenservice achterhaalt de corresponderende dienst uit het eTD dienstenregister. De te kiezen dienst is afhankelijk van het vereiste betrouwbaarheidsniveau en of het een natuurlijk of rechtspersoon betreft.
– De eTD-Authenticatiedienst (hierna: AD) toetst of de authenticatie voldoende betrouwbaar was.
– De eIDAS-berichtenservice verifieert de integriteit en veiligheid van het eTD bericht.
– De eIDAS-berichtenservice ondertekent de eIDAS berichten.

Use Case III-B (vanuit Nederland inloggen bij een dienstverlener in een andere lidstaat; de dienstafnemer is een niet-natuurlijke persoon)
– De eIDAS-berichtenservice achterhaalt de corresponderende dienst uit het eTD dienstenregister. De te kiezen dienst is afhankelijk van het vereiste betrouwbaarheidsniveau en of het een natuurlijk of rechtspersoon betreft.
– De AD toetst of de authenticatie voldoende betrouwbaar was.
– Het machtigingsregister toetst of de natuurlijke persoon bevoegd is om de dienst namens de niet-natuurlijke persoon af te nemen.
– De eIDAS-berichtenservice verifieert de integriteit en veiligheid van het eTD berichten.
– De eIDAS-berichtenservice ondertekent de eIDAS berichten.

Kwaliteit

11. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel of overheidsICT-systeem verwerkte persoonsgegevens na te gaan?
In de beantwoording van vraag 10 zijn controlestappen verwerkt die tegelijkertijd de juistheid, nauwkeurigheid en actualiteit van berichten en data controleren.
Een aandachtspunt zijn nog wel de kwaliteitsissues die het gevolg kunnen zijn van een gebrek aan eenduidigheid in de verondersteld unieke koppeling tussen individuen enerzijds en persoonsnummers als het BSN en de UID anderzijds. Zo'n gebrek aan eenduidigheid kan verschillende oorzaken hebben: een nummer wordt dubbel uitgegeven, er worden meer nummers uitgegeven aan dezelfde persoon, het aan een persoon gekoppelde nummer verandert in de tijd (is niet persistent). De verantwoordelijkheid voor deze kwaliteitsissues ligt in beginsel weliswaar buiten de eIDAS-infrastructuur, maar het is wel zinvol om na te gaan of eIDAS niet een rol kan spelen bij het mitigeren ervan.[36]

Profilering

12. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?
Nee, in de startarchitectuur is niet voorzien en wordt niet beoogd om de verzamelde/verwerkte persoonsgegevens te gebruiken om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen.[37]

13. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?
Niet van toepassing (zie het antwoord op vraag 12).

III. Betrokken instanties/systemen en verantwoordelijkheid

14. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder 5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?
In de Use Cases in hoofdstuk 4 van de startarchitectuur is dit in stappen in het authenticatieproces beschreven. In de tekeningen in bijlage A zijn de dataflows tussen de componenten aangegeven en is tevens inzichtelijk gemaakt welke data bij welke component wordt opgeslagen.

15. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid

[36] In versie 1.1 van de startarchitectuur is hierin deels voorzien door het toevoegen van de service "Verwijder koppeling".
[37] Een dergelijke gegevensverwerking kan aan de orde zijn als het gaat om het bestrijden van misbruik en fraude waarbij gebruik wordt gemaakt van eIDAS. Hieraan is aandacht besteed in het antwoord op vraag 3. Dat valt echter buiten de reikwijdte van de onderhavige PIA. Het is wel een vraag die telkenmale in de volgende architectuurfasen aan de orde dient te komen.

en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?
De verantwoordelijkheden voor de verwerkingen van persoonsgegevens door het Nederlandse eIDAS-koppelpunt zijn als volgt:

- De Minister van Economische Zaken is de verwerkingsverantwoordelijke voor de verwerkingen van persoonsgegevens door het eIDAS-koppelpunt (connector, proxy en berichtenservice) (bron: startarchitectuur eIDAS versie 1.1, par. 3.1).
- De Minister van Binnenlandse Zaken en Koninkrijksrelaties is de verwerkingsverantwoordelijke voor de verwerkingen door het BRP-koppelpunt en voor het BSNk (bron: startarchitectuur eIDAS versie 1.1, par. 3.2).

N.B. De Minister van EZ is behalve verwerkingsverantwoordelijke voor het eIDAS-koppelpunt ook politiek verantwoordelijk voor, en toezichthouder op, het eTD-stelsel.

In de startarchitectuur eIDAS wordt in feite voor iedere component in het Nederlandse eIDAS-koppelpunt de richting voor hun verantwoordelijkheden aangegeven door de beschrijving van hun doelstellingen, taken c.q. services, en de daarmee gepaard gaande gegevensverwerkingen. In die zin zou het duidelijk moeten zijn waar deelverantwoordelijkheden aangaande gegevensverwerkende services op operationeel niveau liggen. Uit de workshops blijkt, dat het verder inrichten van de algehele governance voor wat betreft het eIDAS-koppelpunt in de navolgende ontwerpfasen nog gestalte moet krijgen.

In de antwoorden op de vragen 7 en 8 hebben wij de relatie van het eIDAS-koppelpunt met het eTD-stelsel uiteengezet. Kortweg: het eIDAS koppelpunt faciliteert de interoperabiliteit tussen het Nederlandse eTD-stelsel en buitenlandse eIDAS-koppelpunten. Het eIDAS-koppelpunt maakt voor zijn dienstverlening maximaal gebruik van bestaande componenten van het eTD-stelsel, zoals authenticatiediensten en herkenningsmakelaars, en van het BSNk.

Vanwege deze vervlechting met het eTD-stelsel is het opportuun om als eIDAS-koppelpunt zo veel mogelijk aan te haken bij de ontwikkelingen rondom de inrichting van de governance en het toezicht in het eTD-stelsel. Van belang is om daarbij rekening te houden met de uitkomsten van het Rapport “Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel)” van de Algemene Rekenkamer dat op 8 september 2016 is aangeboden aan de Tweede kamer. Het eTD-stelsel is namelijk een onderdeel van het eID-stelsel.

De uitkomsten zijn kortweg onder meer:

- De verantwoordelijkheden voor het eID-stelsel zijn niet eenduidig belegd en de governancestructuur is ingewikkeld.
- Op wezenlijke onderdelen van het eID-stelsel moeten nog besluiten worden genomen of uitgewerkt.
- Een integrale visie op de inrichting van het toezicht voor het eID-stelsel ontbreekt.

De Minister van BZK onderschrijft in zijn reactie op deze uitkomsten, dat de verantwoordelijkheden voor het eID-stelsel niet eenduidig zijn belegd en dat de governancestructuur ingewikkeld is. De minister heeft toegelicht, dat het kabinet om deze reden in 2015 de verantwoordelijkheidsverdeling ten aanzien van dit onderwerp duidelijker heeft belegd bij de minister van BZK en de minister van EZ. Om de complexiteit verder te reduceren zijn in de afgelopen maanden de verantwoordelijkheden in de aansturing van het programma verduidelijkt, bijvoorbeeld door de instelling van een hoogambtelijke stuurgroep onder leiding van de directeur-generaal Overheidsorganisatie, die tevens de opdrachtgever is van het programma Impuls eID. Verder merkte de minister op dat de Digicommissaris wordt geconsulteerd over de besluitvorming, evenals de Regieraad Identificatie en Authenticatie (I&A). De

minister heeft toegezegd om zich in de toekomst, daar waar mogelijk, te blijven inzetten om de complexiteit van het programma verder te reduceren. Dit neemt volgens hem overigens niet weg dat het volledig uitbannen van risico's bij innovaties als deze per definitie niet kan.

Wij bevelen aan om, uit het oogpunt van convergentie, met het eIDAS-koppelpunt zo veel mogelijk aan te haken bij c.q. af te stemmen op het verbeterproces van de governance en het toezicht in het eID-stelsel (voor zover dit het eTD-stelsel raakt).

16. **Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?**
De beantwoording van deze vraag valt buiten de scope van deze PIA. De beantwoording zal worden meegenomen in de PIA's die nog gaan worden uitgevoerd op de verschillende eIDAS-componenten.

17. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?
Zie het antwoord op de vorige vraag.

18. **Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?**
Ja. In de startarchitectuur zijn alle stappen van de verwerking, in de zin van soorten gegevens, opslag en uitwisselingen, in kaart gebracht.[38] [39]

Hoofdstuk 3 bevat een beschrijving van het eIDAS-koppelpunt, de eisen die daaraan gesteld worden en de architectuurbeslissingen die erover genomen zijn. Hetzelfde hoofdstuk bevat ook een beschrijving van het eTD-stelsel, met de architectuurbeslissingen en de eisen in relatie tot het eIDAS-koppelpunt.

Hoofdstuk 4 maakt de relaties inzichtelijk tussen de verschillende componenten van de Nederlandse eIDAS-infrastructuur, zowel onderling als met het eTD-stelsel en met de eIDAS-koppelpunten van de andere EU/EER-lidstaten.

Verder komen in hoofdstuk 4 de gedragingen van de berichtenservice, het BRP-koppelpunt en het eTD-stelsel aan de orde, de wijze waarop zij zijn gestructureerd, hun koppelvlakken, en welke soort berichten (objecten) voor welke services aan welke actor c.q. afnemer over deze interfaces worden verzonden. Bij de objecten kan het onder meer gaan om attributen, polymorfe pseudoniemen en encryptiesleutels.

Bijlage 3 van de startarchitectuur bevat de processtappen en de visualisering daarvan middels dataflows die het authenticatieverkeer in de Use Cases II-A, II-B, III-A en III-B beschrijven.

Tenslotte zijn er nog de uitgebreide stapsgewijze beschrijvingen van de Use Cases die ook weer van tekeningen zijn voorzien.

In deze fase van ontwikkeling van de Nederlandse eIDAS-infrastructuur gaat het nog om architectuurbeschrijvingen, die (op onderdelen) voor de doorsnee burger niet (geheel) begrijpelijk zijn. Deze beschrijvingen vormen de input voor nog in de volgende ontwerpfasen voor betrokkenen te

[38] Met uitzondering van de gegevens in mogelijke de logfiles. Dit wordt in de volgende ontwerpfasen meegenomen.
[39] De nummering hieronder verwijst naar versie 1.0 van de startarchitectuur. Bijlage III is met versie 1.1 (om redenen van onderhoudbaarheid) komen te vervallen als expliciet onderdeel van de startarchitectuur.

generen informatie, waarin op zo laagdrempelig mogelijke wijze inzichtelijk kan worden gemaakt bij wie, waarom en hoe er persoonsgegevens worden verwerkt.

19. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

20. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?
Nee, de rol van het eIDAS-koppelpunt is beperkt tot uitwisseling van authenticatiegegevens tussen partijen in lidstaten van de EU/EER.[40]

IV. Betrokken instanties/systemen en verantwoordelijkheid

Beveiliging

21. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan?
Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?
Hoofdstuk 6 van de startarchitectuur eIDAS besteedt aandacht aan informatiebeveiliging.

Aan de onderstaande wetgeving en voorschriften wordt gerefereerd.
- Voorschrift Informatiebeveiliging Rijksdienst (VIR).
- Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2013 (VIR-BI 2013). Het VIR-BI 2013 geeft aan dat maatregelen proportioneel, efficiënt en effectief dienen te zijn in relatie tot de belangen. In de praktijk betekent dit doorgaans dat een risicoanalyse aan de basis van keuzes ligt.
- Wet Bescherming Persoonsgegevens (WBP). Hoe om te gaan met WBP is verder toegelicht in CBP Richtsnoeren Beveiliging van Persoonsgegevens.[41]

Vervolgens worden de volgende relevante richtlijnen en normenkaders genoemd:
- Baseline Informatiebeveiliging Rijksdienst (BIR);
- NCSC ICT-Beveiligingsrichtlijnen voor webapplicaties;
- ISO 27001 / 27002.

Op de startarchitectuur is een aparte risico-analyse uitgevoerd, waarin onder meer naar informatiebeveiliging is gekeken.

Verder wordt in het kader van de informatiebeveiliging aandacht besteed aan de in de startarchitectuur beschreven wijzigingen van het afsprakenstelsel eTD, in het bijzonder de overgang

[40] Voor zover het gaat om het uitvoeren van de eIDAS -verordening. Er is sprake van het gebruik van de eIDAS-infrastructuur voor authenticatieverkeer met derde landen, met name Turkije en Zwitserland. Zulk gebruik valt echter buiten de reikwijdte van de onderhavige PIA.
[41] Zie CBP Richtsnoeren Beveiliging van Persoonsgegevens op https://autoriteitpersoonsgegevens.nl.

naar het werken met polymorfe pseudoniemen als pseudonimiseringsvorm. Polymorfe pseudonimisering zorgt ervoor dat partijen met elkaar kunnen communiceren over personen op een betrouwbare, veilige en vertrouwelijke manier. Polymorfe pseudonimisering is gebaseerd op een beproefde versleutelingstechnologie.[42] Ook wordt inzicht verschaft in de gebruikte communicatievorm en integriteit/endpoints over de componenten heen bij grensoverschrijdende authenticatie.

In bovengenoemde zin wordt er in de startarchitectuur uitgebreid aandacht besteed aan informatiebeveiliging. Dat is in deze projectfase prijzenswaardig. Het betekent ook, dat er in de volgende ontwerpfasen van de eIDAS-infrastructuur aandacht zal moeten worden besteed aan de beleidsmatige aspecten van informatiebeveiliging waar in de vraagstelling op wordt gedoeld.

Door opdrachtgever is opgemerkt, dat er door een externe partij nog een verdergaande informatiebeveiligingsrisicoanalyse op het eIDAS-koppelpunt is uitgevoerd. Dat is een logische stap in vervolg op het voorgaande. Op basis hiervan zal aan het informatiebeveiligingsbeleid met de hieruit voortvloeiende beveiligingsmaatregelen vorm en inhoud kunnen worden gegeven.

22. Indien (een deel van) de verwerking bij een verwerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die verwerker?
In de startarchitectuur wordt geen aandacht besteed aan eventuele verwerkers. Daar leent zich dit document ook nog niet voor; dit onderwerp zal in de volgende ontwerpfasen aan de orde moeten komen. Uit de met opdrachtgever gehouden workshops is al wel naar voren gekomen, dat het Ministerie van EZ vanaf 2018 gaat overwegen om de berichtenservice door private partijen te laten hosten.

Hoewel de beantwoording van deze vraag hiermee formeel buiten de reikwijdte van de onderhavige PIA valt, menen wij er goed aan te doen op dit vlak de volgende kanttekeningen te plaatsen.

Bij het inschakelen van verwerkers wijzen wij op soortgelijke risico's die zijn gesignaleerd in de PIA betreffende het Introductieplateau eID-Stelsel, versie 1.0, van 31 juli 2015, als gevolg van ongewenste samenloop van rollen en het doorbreken van functiescheidingen. Dergelijke risico's kunnen zich ook voordoen ingeval van verwerkers voor het eIDAS-koppelpunt, die bijvoorbeeld ook rollen in het eTD-stelsel vervullen. Privacyrisico's kunnen ook ontstaan indien meerdere deelnemers aan het eTD-stelsel gebruik maken van dezelfde verwerker.

Dergelijke omstandigheden vereisen volgens de PIA op het eID-stelsel nadere regulering en toetsing van de scheiding (Chinese muren) van meerdere vormen van dienstverlening binnen één organisatie en systeem. Deze risicosignalering met het voorstel voor mitigerende maatregelen is inmiddels opgepakt en wordt verder uitgewerkt. De voorstellen worden in de ontwikkeling van het Introductieplateau eID meegenomen. Gezien de relatie van het eIDAS-koppelpunt met het eTD-stelsel kunnen wij ons voorstellen, dat dergelijke risicomitigerende maatregelen ook ten aanzien van mogelijke verwerkers van het eIDAS-koppelpunt worden meegenomen. Mogelijk zijn in aanvulling daarop nog verwerkersovereenkomsten nodig met de in te schakelen partijen.

23. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op

[42] Polymorfe pseudonimisering als zodanig valt buiten de reikwijdte van de onderhavige PIA. Een goed begrip ervan is echter wel noodzakelijk om een goed beeld te hebben van (de noodzaak van) de wijze waarop er binnen de eIDAS-infrastructuur met deze pseudoniemen wordt omgegaan. Zie bijlage B voor een beschrijving van polymorfe pseudonimisering.

kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?
Voor de beantwoording van deze vraag verwijzen wij naar ons antwoord bij vraag 21. De beantwoording op het detailniveau die deze vraag beoogt, zal in de volgende ontwerpfasen aan de orde moeten komen.

24. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

Bewaring/vernietiging

25. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.[43]

26. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

27. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief loggegevens, vernietigd? Is er controle op de vernietiging, en door wie?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

V. Transparantie en rechten van betrokkenen

Transparantie

28. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

29.Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

[43] Het ligt voor de hand om hiervoor aan te haken bij de Regeling EBV en de Wet GDI.

30. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

Rechten van betrokkenen

31. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt. Wij merken hier alvast op dat eventuele toestemming in het algemeen niet de grondslag voor de verwerking zal vormen: die is te vinden in de noodzaak van het gebruik van eIDAS om online toegang tot de gevraagde dienst te kunnen bieden.[44]

32.Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verwerkingsverantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

33. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?
De beantwoording van deze vraag valt, gezien de fase van ontwerp van eIDAS, buiten de reikwijdte van de onderhavige PIA en zal daarom in de vervolgfasen moeten worden opgepakt.

[44] In de context van overheidsdienstverleners gaat het dan over de grondslag in artikel 6 lid 1 onder e AVG (vervulling van een publieke taak). Voor private dienstverleners zal het doorgaans gaan om de grondslag in artikel 6 lid 1 onder b AVG (voorbereiding van een overeenkomst).

6 Private dienstverleners, andersoortige attributen

In het vorige hoofdstuk hebben wij de vragen van het Toetsmodel PIA Rijksdienst beantwoord voor die situaties die op basis van de eIDAS-verordening[45] verplicht geregeld moeten worden. Dat wil zeggen: authenticatie ten behoeve van overheidsdienstverleners waarbij slechts de minimale dataset wordt uitgewisseld. In dit hoofdstuk gaan we in op de andere situaties, waarbij er dus sprake is van gebruik van de eIDAS-infrastructuur door private dienstverleners en/of het uitwisselen van andersoortige attributen buiten de minimale dataset.

6.1 Private dienstverleners

De eIDAS-verordening regelt het gebruik van de eIDAS-infrastructuur door publieke dienstverleners. Uit overweging (17) bij de verordening blijkt echter dat het nadrukkelijk de bedoeling is dat ook private dienstverleners van de infrastructuur gebruik gaan maken. Ten tijde van de PIA eIDAS-knooppunt was de lijn nog dat Nederland in eerste instantie alleen gebruik door publieke Nederlandse dienstverleners zou toestaan. Die lijn is inmiddels losgelaten: ook private dienstverleners kunnen in Nederland vanaf het begin gebruik gaan maken van eIDAS. En uiteraard valt omgekeerd te verwachten dat private dienstverleners uit andere lidstaten zich via eIDAS met authenticatieverzoeken zullen wenden tot Nederlandse identiteitsdienstverleners.

De eIDAS-verordening bepaalt dat een aanmeldende lidstaat aan vertrouwende partijen die geen openbare instanties zijn voorwaarden mag stellen voor toegang via eIDAS tot het genotificeerde stelsel voor elektronische identificatie.

Bij het gebruik van de eIDAS-infrastructuur door private dienstverleners is er sprake van een stapeling van factoren die mogelijk privacyrisico's met zich meebrengen. In de eerste plaats zijn de bepalingen, en daarmee ook de waarborgen, van de eIDAS-verordening niet op private dienstverleners van toepassing. In de tweede plaats zijn private dienstverleners niet gebonden aan specifieke eisen van zorgvuldigheid en behoorlijk bestuur die gelden voor publieke instanties. Tot slot is bij het ontwerpen van de eIDAS-infrastructuur slechts beperkt rekening gehouden met de specifieke privacyaspecten van het gebruik ervan door private dienstverleners.

Om deze redenen dient het gebruik van de eIDAS-infrastructuur met nadere waarborgen omkleed te worden. De startarchitectuur geeft hieraan al op twee manieren invulling. In de eerste plaats krijgen Nederlandse private dienstverleners niet het buitenlandse UID verstrekt, maar een daarvan afgeleid polymorf pseudoniem dat voor elke dienstverlener verschillend is. Dat maakt het voor deze partijen moeilijker om onderling gegevens te koppelen op basis van een unieke identificatiecode. In de tweede plaats worden buitenlandse identiteiten niet vastgelegd bij het BRP-koppelpunt als er niet om een BSN-dienst gevraagd wordt.

In aanvulling op deze maatregelen ligt het voor de hand om bij het stellen van eisen aan het gebruik van eIDAS door private dienstverleners de volgende twee uitgangspunten te hanteren:[46]

– Aan het gebruik van buitenlandse authenticatie-informatie door Nederlandse private dienstverleners worden ten minste dezelfde eisen gesteld als het eTD-stelsel aan hen stelt m.b.t. het gebruik van Nederlandse authenticatie-informatie.[47]

[45] Onder de aanname dat Nederland het eTD-stelsel gaat aanmelden bij de Europese Commissie.
[46] Als vertrekpunt, niet als harde voorwaarde. In de uitwerking kan blijken dat het uitgangspunt niet volledig vol te houden is.
[47] Dit uitgangspunt is waarschijnlijk al grotendeels geborgd in de aansluiteisen van het eTD-stelsel.

– Aan buitenlandse private dienstverleners en het gebruik dat zij maken van Nederlandse authenticatie-informatie worden ten minste dezelfde eisen gesteld als het Nederlandse eTD-stelsel stelt aan (Nederlandse) private dienstverleners.[48]

Een belangrijk uitvloeisel van het tweede uitgangspunt is dat voor een Nederlandse burger, met behulp van polymorfe pseudonimisering, voor elke buitenlandse private dienstverlener waar hij zich wil authenticeren met een middel uit het Nederlandse eTD-stelsel een aparte unieke identificatiecode wordt geconstrueerd.[49]

Tot slot merken wij op dat het goed denkbaar is dat de combinatie van private dienstverleners met het gebruik van andersoortige attributen (zie de volgende paragraaf) tot extra privacyrisico's leidt.

6.2 Andersoortige attributen

De hierboven beschreven minimale dataset kan in de toekomst worden uitgebreid met andersoortige attributen. De eIDAS-verordening zegt daar zelf overigens niets over. Wel bepaalt art. 8 onder d van Uitvoeringsverordening 2015/1501 dat het door de eIDAS-knooppunten gebruikte berichtformaat de nodige flexibiliteit moet bieden om te kunnen voldoen aan de behoefte aan andersoortige attributen met betrekking tot identificatie.

Welke andersoortige attributen buiten de minimale dataset er via de eIDAS-infrastructuur uitgewisseld gaan worden is sectorspecifiek. In het onderwijs kan bijvoorbeeld gedacht worden aan eerder behaalde diploma's en certificeringen. Welke gegevens deze andersoortige attributen zullen gaan bevatten hangt dus geheel af van het soort dienstverlening waarvoor ze gebruikt gaan worden. Dat betekent dat het daarbij in sommige gevallen heel goed om gevoelige of zelfs bijzondere persoonsgegevens kan gaan, al is dat wel afhankelijk van hoe strikt of ruim de term "met betrekking tot identificatie" hierboven moet worden opgevat.

Het idee is dat er over het gebruik van andersoortige attributen per sector op Europees niveau afspraken gemaakt worden. Inmiddels loopt er al een pilot, genaamd TAXUD, op het gebied van belastingheffing.

Het is niet duidelijk hoe andersoortige attributen buiten de minimale dataset precies aan de eIDAS-infrastructuur toegevoegd worden. Dient dit bijvoorbeeld altijd door alle lidstaten gezamenlijk te worden besloten, of kan een groep lidstaten hierover ook onderling afspraken maken? En aan welke voorwaarden moet er dan voldaan worden? Door de opdrachtgever is aangegeven[50] dat er voor de uitwisseling van andersoortige attributen altijd toestemming van de burger zal worden gevraagd, maar dit uitgangspunt lijkt nationaal noch op EU-niveau te zijn verankerd.

De inhoud van andersoortige attributen kan op belangrijke punten verschillen van de minimale dataset van eIDAS. De eIDAS-infrastructuur kent geen gerichte maatregelen voor het mitigeren van specifieke risico's die het mogelijke toekomstige gebruik van bepaalde (combinaties van) andersoortige attributen met zich mee kan brengen. Het is daarom bepaald niet ondenkbaar dat het toelaten van andersoortige attributen buiten de minimale dataset belangrijke privacyrisico's met zich meebrengt. Te denken valt aan onvoldoende beveiliging van gevoelige gegevens of stapeling van gegevens bij hot

[48] In de EU-context zal dit uitgangspunt, zeker op korte termijn, slechts ten dele te realiseren zijn. Dat neemt echter niet weg dat het wel als leidraad gehanteerd kan worden bij de *peer review* in het kader van de notificatie van eID-stelsels van andere lidstaten. In het uiterste geval kan Nederland besluiten om buitenlandse private dienstverleners of andersoortige attributen buiten de minimale dataset te weigeren.
[49] De tegenhanger van het UID dat voor publieke instanties wordt geleverd, en dat vanwege de bepalingen van de eIDAS-verordening niet per instantie verschillend kan zijn.
[50] In de PIA workshop van 26 juli 2016.

spots zoals de eIDAS-berichtenservice. Waarborgen voor dat proces, zoals de verplichting om de privacyrisico's te beoordelen, zijn derhalve noodzakelijk.

7 Wijzigingen in de startarchitectuur

Naar aanleiding van (onder meer) bevindingen gedurende het PIA-proces is de hier beoordeelde versie 1.0 van de startarchitectuur bijgesteld. De nieuwe versie 1.1 kwam kort voor het afronden van dit PIA-rapport beschikbaar. Het was daardoor niet mogelijk om het hele PIA-rapport aan de nieuwe situatie aan te passen. Waar dat redelijkerwijs nog mogelijk was, is de hoofdtekst wel met versie 1.1 in lijn gebracht.

Evenmin was het mogelijk om versie 1.1 van de startarchitectuur volledig tegen het licht te houden om de verschillen met versie 1.0 scherp te krijgen. Wij hebben ons bij het beoordelen van versie 1.1 gebaseerd op bijlage 4 van dat document, die de wijzigingen ten opzichte van versie 1.0 opsomt.

De algehele indruk is dat er met versie 1.1 een aantal verbeteringen op privacyvlak zijn doorgevoerd. Hieronder geven wij per onderdeel van die opsomming dat relevant is voor deze PIA (blauwe tekst) aan hoe het in het onderhavige rapport is verwerkt.

Beleidsbeslissing:
- De mogelijkheid tot toevoegen van persoonsgegevens aan de BRP verwijderd (inclusief de registratie van een nog onbekend persoon en uitgifte van een nieuw BSN), met uitzondering van bijlage 2.

Het al dan niet toevoegen van persoonsgegevens aan de BRP valt buiten de reikwijdte van deze PIA.

Bron werkgroep ontwerp & bouw:
- RfC van ICTU op opvragen polymorfe pseudoniemen bij BSNk doorgevoerd: de eIDAS berichtenservice ontvangt versleuteld BSN en levert die aan BSNk voor opvragen van PP- BSN en PP-PS. Het BSNk bevraagt niet langer zelf het BRP-koppelpunt voor het BSN.

Deze wijziging is relevant voor deze PIA, maar was daar al in verwerkt.

- eIDAS identiteitmanager & verificatiedienst zijn in elkaar geschoven. De resulterende component heet nu “BRP koppelpunt”.

De termen “(eIDAS) identiteitmanager” en “(BRP) verificatiedienst” zijn geschrapt en vervangen door “BRP-koppelpunt”.

- De eIDAS berichtenservice levert aan de eTD makelaar bij attributen in de bronvermelding ook het land: “eIDAS:BE”, “eIDAS: DE”, etc.

Dit is een logische wijziging, die de gegevenskwaliteit bevordert.

- Functionaliteit toegevoegd voor het vanuit het BRP koppelpunt uit de koppeltabel van de eIDAS berichtenservice kunnen verwijderen van entries indien de koppeling aan het BSN onjuist bleek of het BSN is gewijzigd.

Dit is een positieve wijziging, aangezien die de gegevenskwaliteit bevordert.

Bron PIA (onder voorbehoud van definitieve rapport en de bespreking daarvan):
- Toegevoegd dat de eIDAS connector en de eIDAS proxy service samen het eIDAS knooppunt vormen. Het eIDAS koppelpunt is het eIDAS knooppunt plus de eIDAS berichtenservice.

Deze wijziging is zoveel mogelijk verwerkt in de PIA. Het betreft een aanscherping naar aanleiding van een discussie over de reikwijdte van de bepalingen in de uitvoeringsverordeningen over het knooppunt. Door deze aanscherping is nu duidelijk dat deze bepalingen slechts betrekking hebben op de eIDAS-conncetor en eIDAS-proxy service, en niet op de eIDAS-berichtenservice.

- Het BRP koppelpunt ontvangt niet bij iedere inlog op een BSN dienst de persoonsattributen. De functie “ontvangActueleAttributen” vervalt daarom.

Dit is een positieve wijziging. De tekst van de PIA is hier zoveel mogelijk op aangepast.

- Argumentatie voor het opslaan van PP-PS in de koppeltabel van de eIDAS berichtenservice toegevoegd.

Deze wijziging is verwerkt in de PIA.

- Vanuit eIDAS Berichtenservice indien mogelijk naam meegeven. Eis aan eTD toegevoegd om deze te tonen.

Deze wijziging betreft de naam van de dienstverlener (§ 5.3.4.1 van versie 1.1). Dit is relevant vanuit privacyoogpunt, aangezien de herkenningsmakelaar en authenticatiedienst hiermee informatie krijgen over de dienst waarop iemand wil inloggen. De wijziging valt echter buiten de reikwijdte van deze PIA.

- Wijzigingsprocedure toegevoegd voor koppelingen UID aan BSN.

Dit betreft de service “Verwijder koppeling” (§ 5.1.4.2). Dit is een positieve wijziging, aangezien die de gegevenskwaliteit bevordert.

- IB Hoofdstuk: Gegevens in de eIDAS koppeltabel versleuteld/hashed opslaan.

Dit is een positieve wijziging, aangezien die de informatiebeveiliging bevordert.

- Misbruik eisen vanuit USvE IB Hoofdstuk (PP-PS) (voetnoot bij uitwerking in 5)

Dit is een onderdeel van de onderbouwing van de noodzaak van het vanaf het begin verwerken van het PP-PS, zie hierboven.

- Toetsing op gevraagde attributen vooraf door Autoriteit Persoonsgegevens. Advies toegevoegd om hier actief op te toetsen

Op zich valt toetsing vooraf door de Autoriteit Persoonsgegevens vanuit privacyoogpunt toe te juichen. Daarbij dient wel de kanttekening geplaatst te worden dat in de praktijk de kans klein is dat de Autoriteit zo’n voorafgaande toets ook daadwerkelijk gaat uitvoeren, tenzij deze zou vallen onder art. 36 lid 1 AVG.

- Beschikbaarheid: Inzetten 2de makelaar op de eIDAS berichtenservice in IB hoofdstuk toegevoegd

Dit is een positieve wijziging, aangezien die de informatiebeveiliging bevordert.

- Consent per lidstaat: aandachtspunt eTD hoofdstuk 5 toegevoegd.

Het gaat hier om de tekst bij de derde bullet in de tabel in paragraaf 5.3.4.1 van de startarchitectuur. De problematiek waar deze tekst naar verwijst is de volgende. Binnen het eTD-stelsel kunnen authenticatiediensten en machtigingsregisters bijhouden welke toestemming gebruikers aan dienstverleners hebben gegeven voor het gebruik van hun gegevens door dienstverleners. De gebruiker hoeft dan niet bij ieder contact met de betreffende dienstverlener opnieuw zijn toestemming te geven. Deze werkwijze kan niet zonder meer ook worden toegepast in de context van eIDAS. In beginsel ‘ziet’ de authenticatiedienst of het machtigingsregister alleen het buitenlandse eIDAS-knooppunt, en niet de dienstverlener zelf. Het onthouden van toestemming voor zo’n buitenlands eIDAS-knooppunt zou ertoe leiden dat ten onrechte toestemming voor een dienstverlener in de betreffende lidstaat ook toegepast zou worden voor de overige dienstverleners in die lidstaat. In EU-verband is echter afgesproken dat de eIDAS-knooppunten de naam van de dienstverlener aan elkaar zouden behoren door te geven. In Nederland is besloten om deze naam binnen het eTD-stelsel ook door te geven aan de authenticatiedienst c.q. het machtigingsregister. Dit is primair een beveiligingsmaatregel, die het mogelijk maakt om de gebruiker een overzicht te geven op welke plekken er met zijn

authenticatiemiddel is ingelogd. De hier beschreven maatregel komt erop neer dat toestemming alleen ‘hergebruikt’ mag worden als de specifieke dienstverlener bekend is. Dit is een positieve wijziging, aangezien die het juist hanteren van toestemming bevordert. Overigens heeft Nederland er inmiddels voor gekozen om voorlopig in eIDAS-verband vooralsnog niet met toestemming te gaan werken.

- Inzet HSM voor eIDAS berichtenservice in 2018 in IB hoofdstuk toegevoegd.
Dit is een positieve wijziging, aangezien die de informatiebeveiliging bevordert.

8 Conclusies

In dit hoofdstuk presenteren wij, kort samengevat en thematisch gerangschikt, de belangrijkste privacyrisico's waarvan in de vorige drie hoofdstukken is gebleken. Het volgende hoofdstuk doet aanbevelingen voor het mitigeren van deze risico's.

Alvorens we ingaan op de gebleken privacyrisico's, hechten we er belang aan om erop te wijzen dat belangrijke (mogelijke) privacyrisico's in deze PIA niet beoordeeld zijn. In de eerste plaats is dat omdat een aantal zaken in hoofdstuk 2 explicite buiten scope zijn geplaatst. Privacyrisico's zien wij zeker gelet op het feit dat inherent is aan architecturen als eIDAS en eTD dat er "onder water" bij componenten en interfaces logging van (meta)data plaatsvindt, uit het oogpunt van onder meer beheer, beveiliging, incidentmanagement, fraudebestrijding en om te kunnen voldoen aan verzoeken betreffende de rechten van betrokkenen. Gezien het feit dat het daarbij om grote databases kan gaan, zijn hier onlosmakelijk privacyrisico's aan verbonden. Denk hierbij aan aspecten als dataminimalisatie, doelbinding en profiling. Aan deze aspecten zal in de PIA's op de componenten nadrukkelijk aandacht moeten worden besteed. Naast de in hoofdstuk 2 expliciet uitgesloten zaken gaat het ook om andere in de startarchitectuur niet uitgewerkte zaken, zoals governance. Ook de risico's van het gebruik van eIDAS door private dienstverleners en het gebruik van andersoortige attributen buiten de minimale dataset hebben wij hier slechts kunnen aanstippen, omdat die in concrete gevallen nader moeten worden beoordeeld.

Algemeen

Bij het opstellen van de startarchitectuur is invulling gegeven aan het uitgangspunt van privacy-by-design. Hoofdstuk 6 van de startarchitectuur beschrijft een aantal maatregelen op dat gebied, waaronder pseudonimisering en andere vormen van dataminimalisatie. Deze leiden er onder meer toe dat op geen enkele manier ooit een BSN wordt verstrekt aan een andere lidstaat.

Verantwoordelijkheden en governance

- De verdeling van verantwoordelijkheden binnen eIDAS is van groot belang (en een verplichting uit hoofde van de AVG). Onduidelijkheden met betrekking tot deze verantwoordelijkheidsverdeling brengen privacyrisico's met zich mee. Gezien de relatie van het eIDAS-koppelpunt met het eTD-stelsel kunnen ook op dit vlak ten aanzien van het eTD-stelsel door eerdere PIA's en de Autoriteit Persoonsgegevens gesignaleerde privacyrisico's spelen. Deze risico's kunnen zich voordoen ten aanzien van privacyprincipes zoals doelbinding (het gebruik van persoonsgegevens voor doeleinden waarvoor ze niet verzameld zijn), transparantie ("de burger raakt het spoor bijster" over welke van zijn gegevens waar worden opgeslagen en verder verwerkt, en wie daarvoor verantwoordelijk is), rechten van betrokkenen (de burger weet niet waar en hoe hij zijn rechten kan effectueren) en beveiliging (het gemeld worden van datalekken is bijv. onvoldoende gewaarborgd).
- De ministers van EZ en BZK zijn gezamenlijk verwerkingsverantwoordelijke voor de Nederlandse eIDAS-implementatie.
- Met een duidelijke verdeling van verantwoordelijkheden, zoals beschreven in het antwoord op vraag 1 in hoofdstuk 5, tussen met name de Ministers van EZ en BZK, zijn deze privacyrisico's niet zonder meer in voldoende mate gemitigeerd.[51] Ook een goede en effectieve governance binnen de organisaties van de verantwoordelijken en tussen eIDAS en het eTD-stelsel is noodzakelijk.

[51] Wij verwijzen hiervoor naar de samenhang tussen dit onderwerp en de bevindingen in par. 4.2 van deze PIA en de beantwoording van vraag 15

Bewerkers

– Bij het inschakelen van (private of publieke) bewerkers gelden er soortgelijke risico's als zijn gesignaleerd in de PIA's op het eID-stelsel. Deze hangen met name samen met ongewenste samenloop van rollen en het doorbreken van functiescheidingen. Dergelijke risico's zullen zich met name voordoen wanneer door eIDAS ingeschakelde bewerkers ook rollen vervullen binnen het eTD-stelsel.

Wettelijk kader

– Naast de eIDAS-verordening en de uitvoeringsverordeningen 1501 en 1502 is er vanuit Europa geen aanvullende wetgeving gemaakt. Deze zijn vrijwel uitsluitend gericht op de interactie tussen lidstaten, en zeggen nauwelijks iets over de nationale eIDAS-implementaties. Mede gelet op de opmerkingen hierboven, over het belang van goede governance en een duidelijke verdeling van verantwoordelijkheden, treden er risico's op als deze zaken niet goed worden uitgewerkt in Nederlandse wet- en regelgeving.
– Het gebruik van het BSN binnen het eIDAS berichtenverkeer leidt gemakkelijk tot juridische discussies. Een concreet risico is dat een situatie ontstaat waarin, althans volgens de letter van de wet, het BSN 'onnodig' verplicht moet worden meegezonden bij veel eIDAS-berichtenverkeer.

Kwaliteit

– De veronderstelde unieke koppeling tussen individuen enerzijds en persoonsnummers als het BSN en de UID anderzijds kan in de praktijk minder eenduidig zijn.

Private dienstverleners

– Het gebruik van de eIDAS-infrastructuur door private dienstverleners brengt mogelijk privacyrisico's met zich mee, doordat met (de privacyaspecten van) dit gebruik in de EU-regelgeving en in de Nederlandse eIDAS-implementatie nog slechts beperkt rekening is gehouden.

Andersoortige attributen

– Het is niet duidelijk hoe andersoortige attributen buiten de minimale dataset precies aan de eIDAS-infrastructuur toegevoegd worden, en aan welke voorwaarden dan moet worden voldaan. De inhoud van deze andersoortige attributen kan veel privacygevoeliger zijn dan de minimale dataset van eIDAS. De bestaande maatregelen mitigeren slechts beperkt de specifieke risico's die gebruik van bepaalde (combinaties van) andersoortige attributen met zich mee kan brengen.

9 Aanbevelingen

In het vorige hoofdstuk zijn de door ons waargenomen risico's aan de orde gesteld. In dit hoofdstuk zullen onze aanbevelingen volgen.

Verantwoordelijkheden en governance

- Regel de gezamenlijk verantwoordelijkheid van de beide ministers ten aanzien van eIDAS en het eTD-stelsel, zoals bedoeld in artikel 26 AVG.
- Ga als Ministerie van EZ en Ministerie van BZK door met het gezamenlijk en integraal uitwerken van verantwoordelijkheidsvraagstukken.
  - Maak duidelijke afspraken over wie waarvoor verantwoordelijk is. Regel de verantwoordelijkheden en voeg deze zoveel mogelijk toe aan bestaande afsprakenstelsels, wetten en ministeriële besluiten. Doe dit zo integraal en consistent mogelijk.
  - Beleg verantwoordelijkheden bij concreet benoemde onderdelen van de ministeries. Benoem wie binnen welk ministerie de ambtelijke verantwoordelijkheid draagt.
  - Aandachtspunten hierbij zijn onder meer:
    - Wie is binnen het Ministerie van BZK verantwoordelijk voor het BSNk en respectievelijk het BRP-koppelpunt?
    - Wie neemt de uiteindelijke beslissing als men het oneens is met elkaar?
    - Hoe scheidt het Ministerie van EZ zijn rol en verantwoordelijkheden ten aanzien van eIDAS enerzijds en het eTD-stelsel anderzijds?
- Haak, uit het oogpunt van convergentie, met het eIDAS-koppelpunt zo veel mogelijk aan bij c.q. stem af op het verbeterproces van de governance en het toezicht in het eID-stelsel (voor zover dit het eTD-stelsel raakt).

Bewerkers

- Regel de rol van bewerkers, inclusief eisen op het gebied van privacy en informatiebeveiliging in de Regeling EBV, de Wet GDI en het afsprakenstelsel.
- Draag daarbij zorg voor nadere regulering en toetsing van de scheiding van meerdere vormen van dienstverlening binnen één organisatie en systeem (ook wel 'Chinese muren' genaamd).

Wettelijk kader

- Leg in aanvulling op de eIDAS-verordening en de uitvoeringswet eIDAS de contouren van de Nederlandse eIDAS-implementatie, zoals de componenten, rollen, taken, bevoegdheden en verantwoordelijkheden, vast in de Wet GDI.
- Tref een zeer duidelijke regeling voor het gebruik van het BSN, het UID en de polymorfe pseudoniemen in de Wet GDI en de Ministeriële regeling inzake elektronisch berichtenverkeer (Regeling EBV).

Kwaliteit

- Ga na of er nog extra maatregelen nodig zijn voor het mitigeren van risico's die kunnen optreden wanneer persoonsnummers niet uniek aan individuen gekoppeld blijken te zijn.

Private dienstverleners

- Voer een aanvullende PIA uit bij gebruik van eIDAS door private dienstverleners.

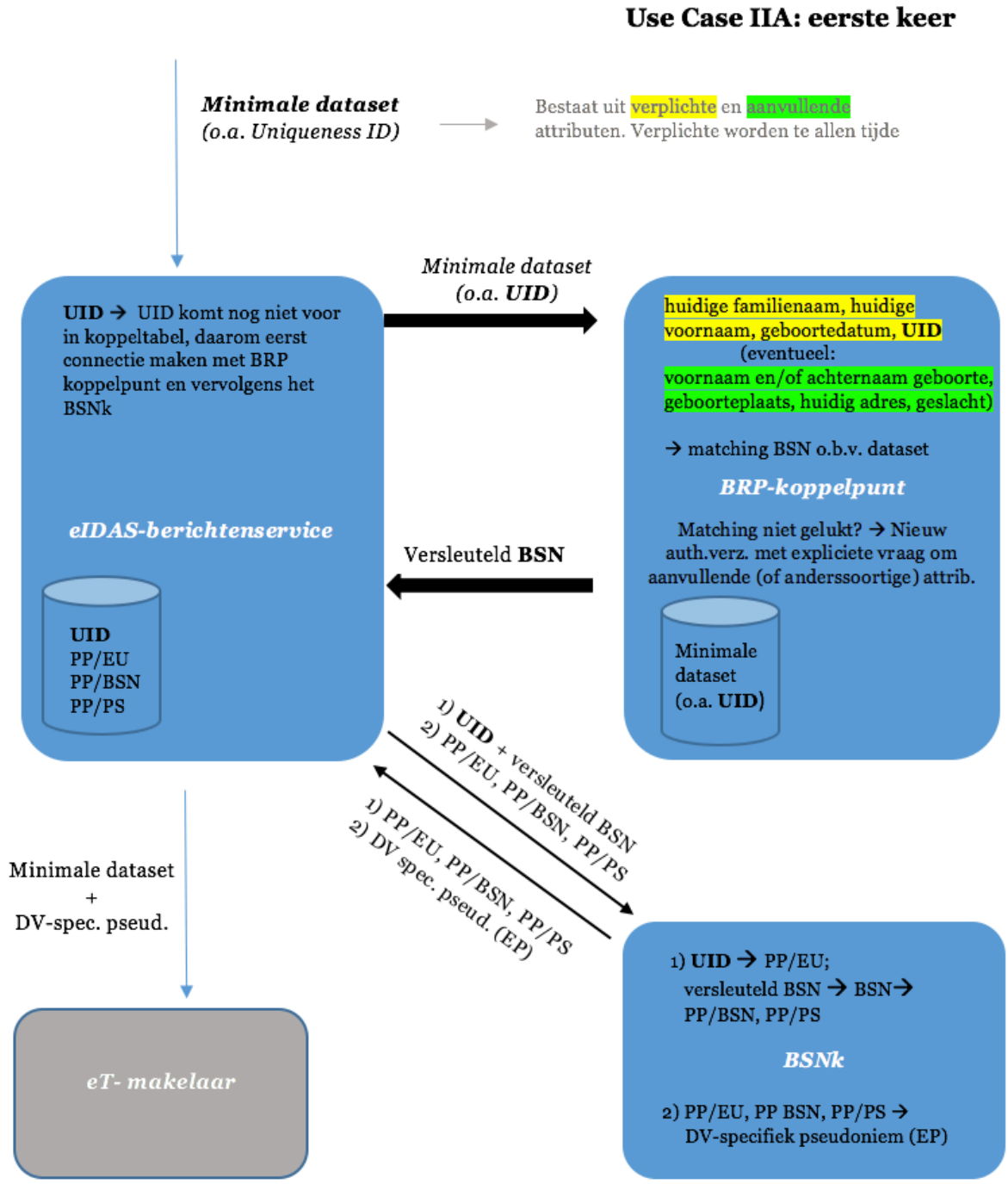
– Hanteer ten aanzien van het gebruik van eIDAS door private dienstverleners de volgende uitgangspunten:
  - Aan het gebruik van buitenlandse authenticatie-informatie door Nederlandse private dienstverleners worden ten minste dezelfde eisen gesteld als het eTD-stelsel aan hen stelt m.b.t. het gebruik van Nederlandse authenticatie-informatie.[52]
  - Aan buitenlandse private dienstverleners en het gebruik dat zij maken van Nederlandse authenticatie-informatie worden ten minste dezelfde eisen gesteld als het Nederlandse eTD-stelsel stelt aan (Nederlandse) private dienstverleners.[53]

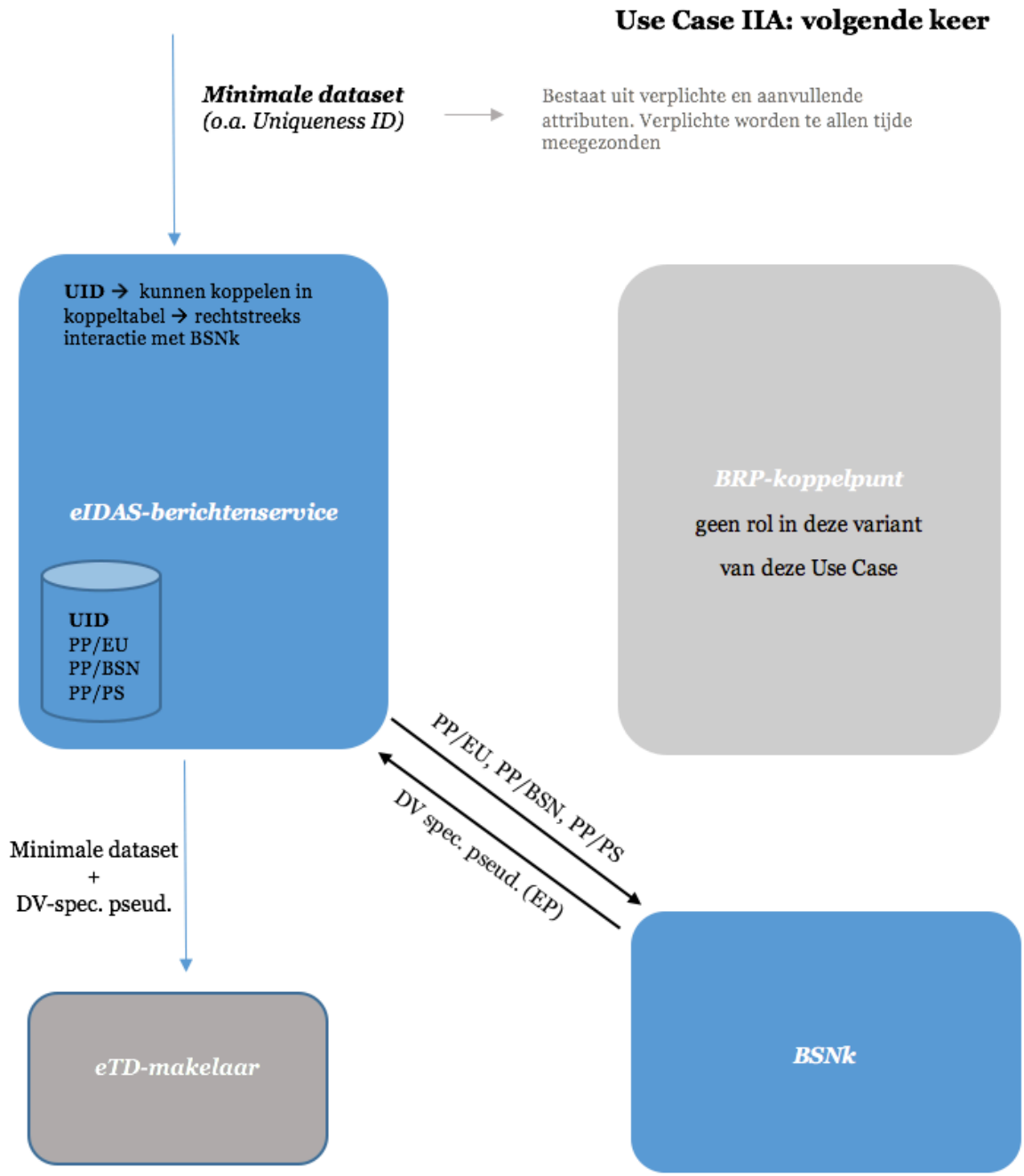
Andersoortige attributen

– Tref waarborgen, bijvoorbeeld op sector- of domeinniveau, rondom het proces van het toelaten van een uitwisseling van andersoortige stelselattributen buiten de minimale dataset via eIDAS, waaronder de verplichting om de privacyrisico's te beoordelen.

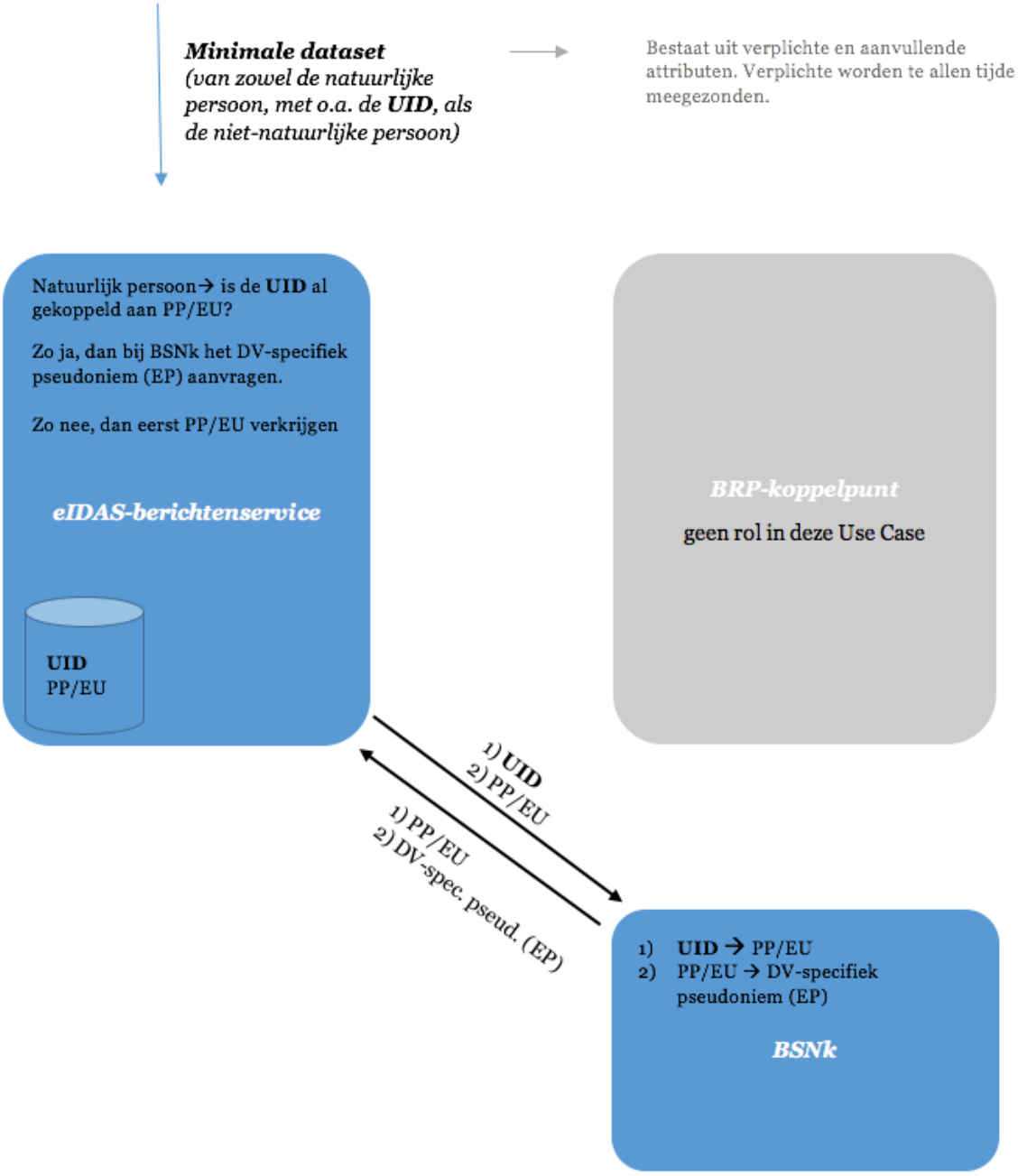
[52] Dit uitgangspunt is waarschijnlijk al grotendeels geborgd in de aansluiteisen van het eTD-stelsel.
[53] In de EU-context zal dit uitgangspunt, zeker op korte termijn, slechts ten dele te realiseren zijn. Dat neemt echter niet weg dat het wel als leidraad gehanteerd kan worden bij de *peer review* in het kader van de notificatie van eID-stelsels van andere lidstaten. In het uiterste geval kan Nederland besluiten om buitenlandse private dienstverleners of andersoortige attributen buiten de minimale dataset te weigeren.

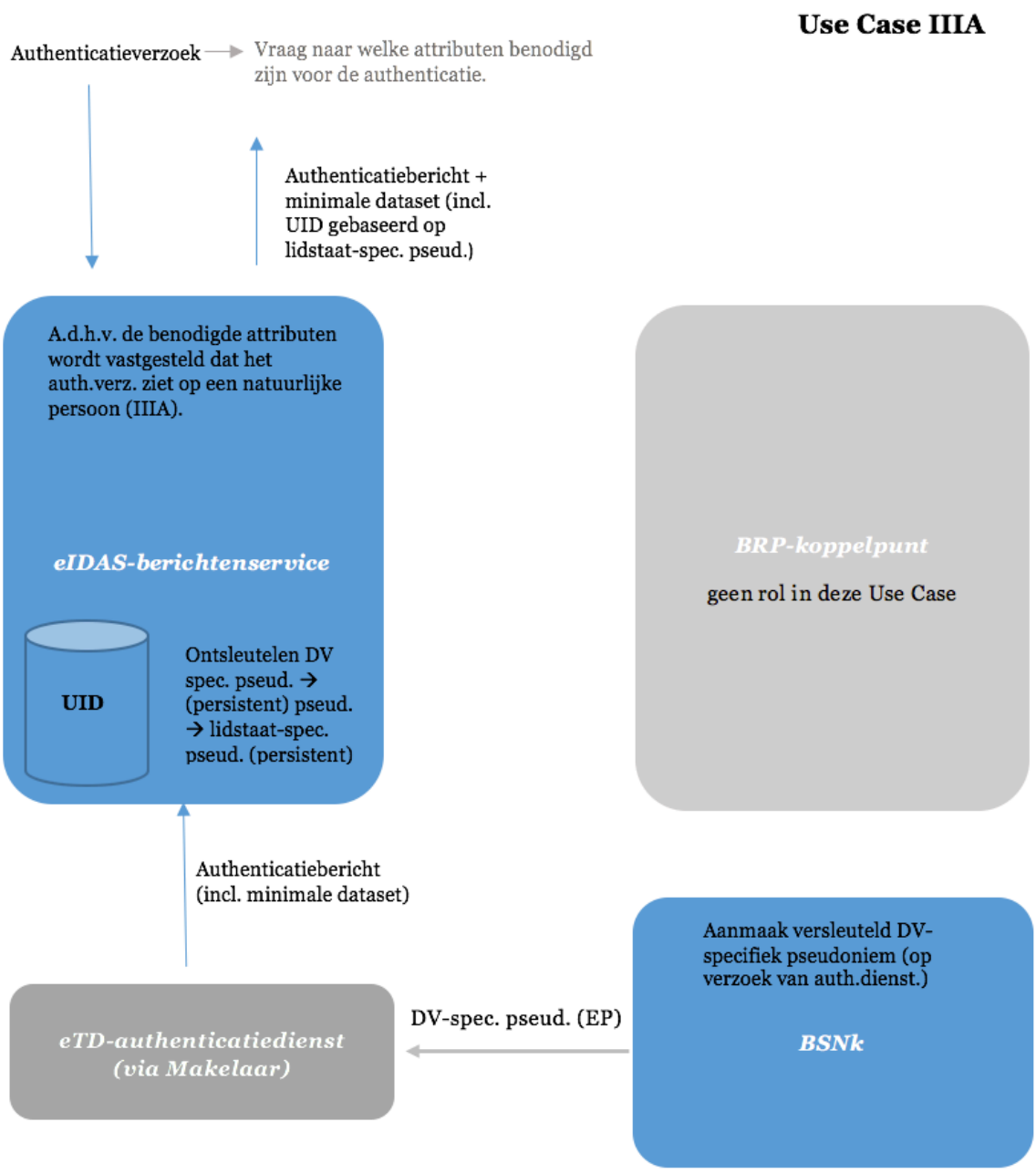
Bijlage A Data flows

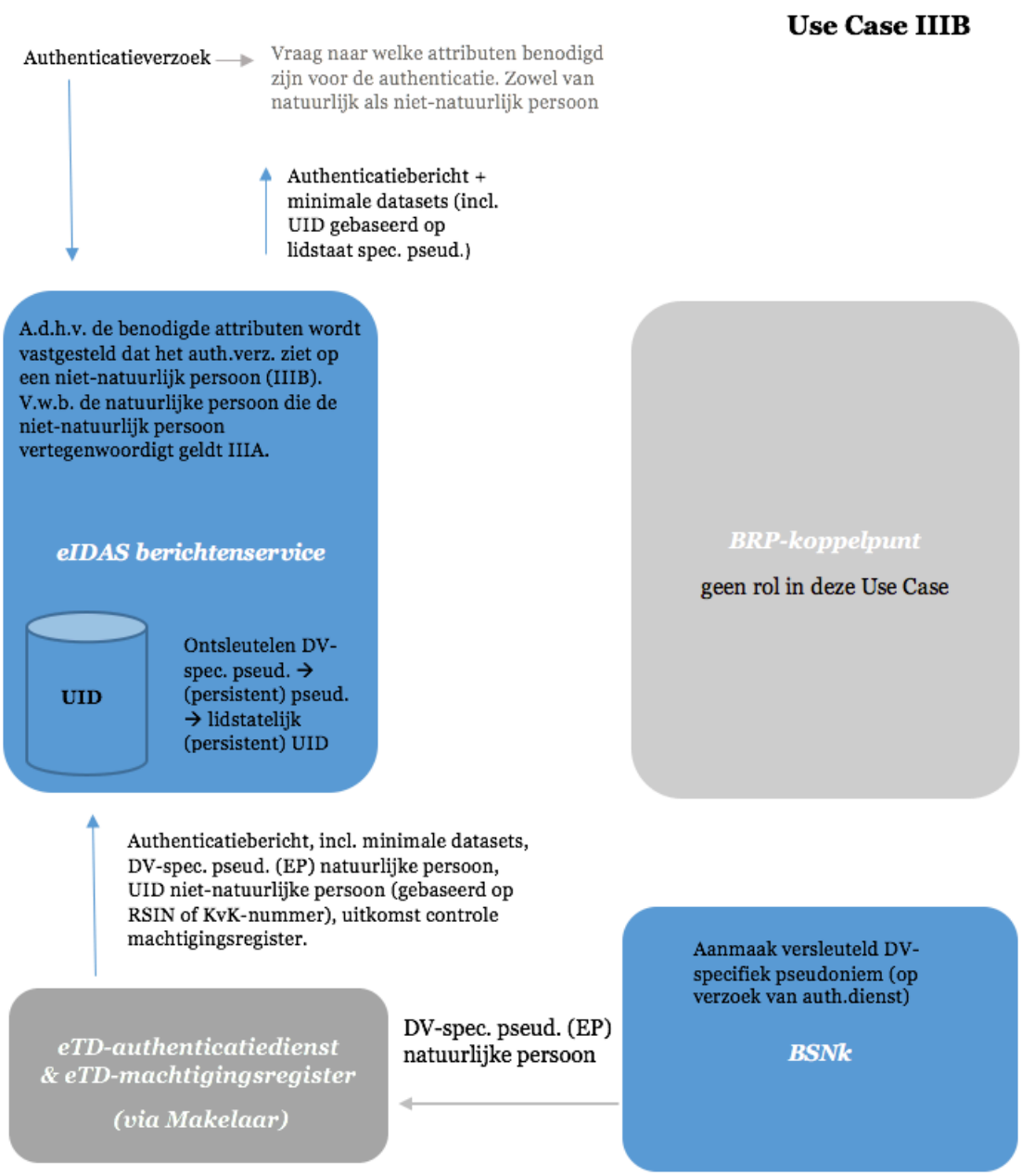



Use Case IIA: volgende keer
Minimale dataset
(o.a. Uniqueness ID)
Bestaat uit verplichte en aanvullende attributen. Verplichte worden te allen tijde meegezonden
UID → kunnen koppelen in koppeltabel → rechtstreeks interactie met BSNk
eIDAS-berichtenservice
UID
PP/EU
PP/BSN
PP/PS
BRP-koppelpunt
geen rol in deze variant
van deze Use Case
PP/EU, PP/BSN, PP/PS
DV spec. pseud. (EP)
Minimale dataset
+
DV-spec. pseud.
eTD-makelaar
BSNk
* Hier wordt ook wel gesproken over de actuele attributen

Use Case II-B


Minimale dataset
(van zowel de natuurlijke persoon, met o.a. de UID, als de niet-natuurlijke persoon)
Bestaat uit verplichte en aanvullende attributen. Verplichte worden te allen tijde meegezonden.
Natuurlijk persoon→ is de UID al gekoppeld aan PP/EU?
Zo ja, dan bij BSNk het DV-specifiek pseudoniem (EP) aanvragen.
Zo nee, dan eerst PP/EU verkrijgen
eIDAS-berichtenservice
UID
PP/EU
BRP-koppelpunt
geen rol in deze Use Case
1) UID
2) PP/EU
1) PP/EU
2) DV-spec. pseud. (EP)
1) UID → PP/EU
2) PP/EU → DV-specifiek pseudoniem (EP)
BSNk


Use Case IIIA
Authenticatieverzoek
Vraag naar welke attributen benodigd zijn voor de authenticatie.
Authenticatiebericht + minimale dataset (incl. UID gebaseerd op lidstaat-spec. pseud.)
A.d.h.v. de benodigde attributen wordt vastgesteld dat het auth.verz. ziet op een natuurlijke persoon (IIIA).
eIDAS-berichtenservice
UID
Ontsleutelen DV spec. pseud. → (persistent) pseud. → lidstaat-spec. pseud. (persistent)
BRP-koppelpunt
geen rol in deze Use Case
Authenticatiebericht (incl. minimale dataset)
Aanmaak versleuteld DV-specifiek pseudoniem (op verzoek van auth.dienst.)
BSNk
DV-spec. pseud. (EP)
eTD-authenticatiedienst (via Makelaar)


Use Case IIIB
Authenticatieverzoek
Vraag naar welke attributen benodigd zijn voor de authenticatie. Zowel van natuurlijk als niet-natuurlijk persoon
Authenticatiebericht + minimale datasets (incl. UID gebaseerd op lidstaat spec. pseud.)
A.d.h.v. de benodigde attributen wordt vastgesteld dat het auth.verz. ziet op een niet-natuurlijk persoon (IIIB). V.w.b. de natuurlijke persoon die de niet-natuurlijk persoon vertegenwoordigt geldt IIIA.
eIDAS berichtenservice
UID
Ontsleutelen DV-spec. pseud. → (persistent) pseud. → lidstatelijk (persistent) UID
BRP-koppelpunt
geen rol in deze Use Case
Authenticatiebericht, incl. minimale datasets, DV-spec. pseud. (EP) natuurlijke persoon, UID niet-natuurlijke persoon (gebaseerd op RSIN of KvK-nummer), uitkomst controle machtigingsregister.
eTD-authenticatiedienst & eTD-machtigingsregister
(via Makelaar)
DV-spec. pseud. (EP) natuurlijke persoon
Aanmaak versleuteld DV-specifiek pseudoniem (op verzoek van auth.dienst)
BSNk

Bijlage B Persoonsnummers

In de startarchitectuur figureren diverse typen persoonsnummers.
Enerzijds zijn dit de 'basispersoonsnummers': de UID's van eIDAS, en het BSN van het eTD-stelsel.
Anderzijds zijn dit pseudoniemen die ontstaan bij het werken met polymorfe pseudonimisering. Deze kunnen worden onderscheiden in polymorfe pseudoniemen, specifieke pseudoniemen en versleutelde pseudoniemen.

Basispersoonsnummers

Het eIDAS-koppelpunt verknoopt het Nederlandse eTD-stelsel met zijn tegenhangers in andere lidstaten.

BSN

Om een goede verbinding met het eTD-stelsel te kunnen leggen, moet het koppelpunt kunnen werken met de daar gehanteerde persoonsnummers. Dat is in de eerste plaats het BSN. Het BSN kan en mag echter alleen gebruikt worden voor BSN-diensten. Voor niet-BSN-diensten werkt het eTD-stelsel met een van het BSN afgeleid persoonsnummer, dat niet tot het BSN valt terug te herleiden.

UID's

Uitvoeringsverordening 2015/1501 schrijft voor dat lidstaten bij eIDAS-verkeer met andere lidstaten gebruik maken van unieke identificatiecodes (UID's) voor burgers en bedrijven. De lidstaten dienen de UID's zo vorm te geven dat deze "zo lang mogelijk stabiel blijven".

Iedere lidstaat maakt zijn eigen UID's aan, bedoeld voor authenticatie via de door die lidstaat genotificeerde stelsels van elektronische identificatie. Het UID bevat codes voor zowel het land van authenticatie als het land van dienstverlening.[54]

Burgers kunnen beschikken over authenticatiemiddelen uit verschillende lidstaten. Wanneer zij die in een eIDAS-context gebruiken, krijgen zij dus ook UID's van verschillende lidstaten toegekend. De eIDAS-verordening voorziet niet in het koppelen van deze verschillende UID's. De Nederlandse eIDAS-implementatie in het geval een persoon BSN-diensten wil afnemen. De koppeling loopt dan via het BSN.

De eIDAS-berichtenservice maakt (met behulp van het BSNk, en voor zover nodig) voor personen die zich op basis van het eTD-stelsel bij buitenlandse dienstverleners willen authenticeren per lidstaat verschillende, onderling niet te relateren UID's aan. Uit deze UID's is het BSN niet af te leiden. Er wordt dus op geen enkele manier ooit een BSN verstrekt aan een andere lidstaat.

Polymorfe pseudonimisering

Hieronder beschrijven we hoe eIDAS gebruik maakt van polymorfe pseudonimisering. Om dat goed te kunnen doen, leggen we eerst uit van hoe die techniek toegepast wordt in het eTD-stelsel.

eTD-stelsel

Binnen het eTD-stelsel is het BSN het unieke persoonsnummer die gebruikt wordt om verschillende personen uit elkaar te houden. Niet alle op het eTD-stelsel aangesloten partijen mogen echter met het BSN werken, en waar zij dat (als verwerkers) wel mogen is het niet altijd wenselijk. Naast het BSN kent het eTD-stelsel daarom een van het BSN afgeleid persoonsnummer, dat wel uniek verbonden is met een bepaald BSN, maar niet (op cryptografische wijze) tot dat BSN valt terug te herleiden. Dit persoonsnummer zullen we aanduiden met de afkorting "PS". Voor BSN-diensten maken dienstverleners gebruik van het BSN, voor niet-BSN-diensten van het PS.

[54] Denk aan een UID in de vorm NL/BE/234234234.

Wanneer het bij het bovenstaande zou blijven, dan zouden er op veel plaatsen in het eTD-stelsel gegevens beschikbaar zijn gekoppeld aan BSN's of PS'en, en daarmee ook eenvoudig onderling te koppelen. Om dat te vermijden, wordt polymorfe pseudonimisering ingezet.

Het proces van polymorfe pseudonimisering is voor een willekeurig persoonsnummer toe te passen, en bestaat conceptueel gezien uit een drietal stappen.

> *N.B. Stap 2 staat niet beschreven in de startarchitectuur. Deze is toegevoegd om duidelijk te maken dat het dienstverlenerspecifieke pseudoniem door het BSNk 'verstopt' wordt in het versleutelde pseudoniem.*

Stap 1: Persoonsnummer X wordt door de sleutelbeheerautoriteit[55] omgezet in een polymorf pseudoniem PP-X.
Polymorfe pseudoniemen hebben twee onderscheidende kenmerken:
- A Persoonsnummer X zit erin 'verstopt'. Dat wil zeggen dat dit persoonsnummer uit het polymorfe pseudoniem terug te herleiden is, maar uitsluitend voor een partij die de beschikking heeft (gekregen) over het daarvoor benodigde cryptografische sleutelmateriaal.
- B Voor iedere authenticatiedienst wordt een eigen polymorf pseudoniem aangemaakt, en deze zijn onderling niet (op cryptografische wijze) aan elkaar te relateren.

In feite horen er bij persoonsnummer X dus verschillende PP-X'en, te weten één voor elke authenticatiedienst.

Stap 2: Het polymorf pseudoniem wordt door het BSNk omgezet in een dienstverlenerspecifiek pseudoniem.
Dienstverlenerspecifieke pseudoniemen hebben drie onderscheidende kenmerken:
(1) Het oorspronkelijke persoonsnummer X zit er nog steeds in 'verstopt' (zie Stap 1).
(2) Bij één persoonsnummer X hoort één dienstverlenerspecifiek pseudoniem. Verschillende PP-X'en leiden dus tot hetzelfde dienstverlenerspecifieke pseudoniem.[56]
(3) De dienstverlenerspecifieke pseudoniemen voor verschillende dienstverleners zijn niet (op cryptografische wijze) aan elkaar te relateren.

Stap 3: Het dienstverlenerspecifieke pseudoniem wordt door het BSNk omgezet in een versleuteld pseudoniem. De dienstverlener ontvangt het versleutelde pseudoniem via de authenticatiedienst. Bij toetreding tot het stelsel heeft de dienstverlener al de beschikking gekregen over cryptografisch sleutelmateriaal waarmee hij het versleutelde pseudoniem terug kan herleiden tot het dienstverlenerspecifieke pseudoniem. In aanvulling daarop kan de dienstverlener in sommige gevallen de beschikking krijgen over cryptografisch sleutelmateriaal waarmee hij uit het versleutelde pseudoniem het persoonsnummer X kan afleiden.[57] Voor alle versleutelde pseudoniemen afgeleid van persoonsnummer X (dus voor elke combinatie van authenticatiedienst en dienstverlener) geldt dat deze onderling niet (op cryptografische wijze) aan elkaar te relateren zijn.

De wijze van toepassing van polymorfe pseudonimisering binnen het eTD-stelsel hangt ervan af of er sprake is van een BSN-dienst of van een niet-BSN-dienst.

---

[55] Voor het eTD-stelsel is dat het BSNk.
[56] Iedere dienstverlener heeft een eigen dienstverlenerspecifiek pseudoniem, maar hij krijgt wel van verschillende authenticatiediensten hetzelfde dienstverlenerspecifieke pseudoniem (ook al hebben die authenticatiediensten verschillende polymorfe pseudoniemen ontvangen).
[57] Deze mogelijkheid wordt in het eTD-stelsel gebruikt voor BSN-diensten.

BSN-dienst: De polymorfe pseudonimisering door het BSNk gaat uit van het BSN en levert het polymorfe pseudoniem PP-BSN op. Dat wordt, zoals hierboven beschreven, stapsgewijs omgezet in een versleuteld pseudoniem dat specifiek bedoeld is voor een bepaalde dienstverlener. De dienstverlener krijgt (ook) de beschikking over sleutelmateriaal dat hem in staat stelt om uit het versleutelde pseudoniem het daarin 'verstopte' BSN te herleiden.

Niet-BSN-dienst: De polymorfe pseudonimisering door het BSNk gaat uit van het PS en levert het polymorfe pseudoniem PP-PS op. Dat wordt, zoals hierboven beschreven, stapsgewijs omgezet in een versleuteld pseudoniem dat specifiek bedoeld is voor een bepaalde dienstverlener. De dienstverlener krijgt (alleen) de beschikking over sleutelmateriaal dat hem in staat stelt om uit het versleutelde pseudoniem het daarin 'verstopte' dienstverlenerspecifieke pseudoniem te herleiden.

Nederlandse eIDAS-implementatie

De Nederlandse eIDAS-implementatie heeft alleen te maken met polymorfe pseudonimisering in Use Case II.[58] We beschrijven deze op hoog niveau, de details zijn te vinden in de beschrijving van de verschillende componenten en de gegevensstromen.

In Use Case II-A wil een persoon met een buitenlands identificatiemiddel inloggen bij een Nederlandse dienstverlener. Het authenticatiebericht bevat een door de betreffende lidstaat gefourneerd UID. Het eIDAS-koppelpunt gedraagt zich in deze Use Case richting het eTD-stelsel als een authenticatiedienst. De gang van zaken hangt ervan af of er al dan niet sprake is van een BSN-dienst.

Voor een BSN-dienst wordt het bij het UID behorende PP-BSN opgezocht. Het BSN wordt door het BSNk omgezet in een polymorf pseudoniem specifiek voor het eIDAS-koppelpunt. Deze maakt, precies zoals een authenticatiedienst dat in het eTD-stelsel zou doen, een op het BSN gebaseerd versleuteld pseudoniem aan en stuurt dat door naar de dienstverlener. Die kan er het BSN uit terug herleiden.

Voor een niet-BSN-dienst wordt het UID door het BSNk omgezet in een polymorf pseudoniem specifiek voor het eIDAS-koppelpunt. Als de persoon in kwestie een BSN heeft (of kan krijgen) dan wordt dit pseudoniem gebaseerd op de van het BSN afgeleid persoonsnummer PS. Heeft de persoon in kwestie geen BSN, en kan hij dit ook niet krijgen, dan wordt het pseudoniem gebaseerd op het UID. Het eIDAS-koppelpunt maakt vervolgens een versleuteld pseudoniem aan en stuurt dat door naar de dienstverlener. Die kan er het dienstverlenerspecifieke pseudoniem uit terug herleiden. Als het polymorfe pseudoniem gebaseerd was op de PS, dan is dit dienstverlenerspecifieke pseudoniem gelijk aan de het dienstverlenerspecifieke pseudoniem dat voor deze combinatie van burger en dienstverlener elders in het eTD-stelsel gebruikt wordt.

Opslaan UID bij BRP-koppelpunt

In de oorspronkelijke startarchitectuur was er een duidelijke reden om het UID op te slaan bij het BRP-koppelpunt, aangezien het BSNk daarmee het BRP-koppelpunt bevroeg. Hoewel die bevraging met de RFC komt te vervallen, blijken er ook in de nieuwe situatie goede gronden te zijn om het UID op te slaan in het BRP-koppelpunt.

Vastleggen voor welk UID een matching-verzoek is gedaan dat niet geautomatiseerd kan worden afgehandeld, maakt de handmatige afhandeling eenvoudiger omdat het daarbij dan direct duidelijk is wanneer eenzelfde gebruiker meerdere inlogpogingen heeft gedaan.

[58] Voor de overzichtelijkheid beperken we ons hier tot Use Case IIA.

Wanneer de handmatige beoordeling wel een koppeling oplevert, dan is de sessie met de gebruiker al (lang) beëindigd. Het heeft dan dus geen zin om het UID en het versleutelde BSN aan de eIDAS-berichtenservice te sturen. Door deze op te slaan totdat de gebruiker een nieuwe poging onderneemt, kan het proces geautomatiseerd worden afgehandeld. Er staat dan immers nog geen PP-BSN geregistreerd bij de eIDAS-berichtendienst, dus het BRP-koppelpunt wordt opnieuw bevraagd en kan op basis van het UID direct het versleutelde BSN terugsturen.

Verkeerde koppelingen door het BRP-koppelpunt zijn niet geheel te voorkomen. Zo'n verkeerde koppeling kan voor beide betrokkenen (de aanvrager en de persoon aan wie hij ten onrechte is gekoppeld) vervelende gevolgen hebben. Als blijkt dat een verkeerde koppeling is gelegd, kan het BRP-koppelpunt een verzoek doen aan de eIDAS-berichtendienst om een UID te verwijderen[59], zodat een nieuw verzoek met dat UID weer als een eerste aanvraag wordt behandeld.

Tot slot komt het ook voor dat een persoon een ander BSN krijgt, bijvoorbeeld omdat hij twee BSN's heeft gekregen (dan vervalt de oude) of omdat er twee personen hetzelfde BSN hebben gekregen (verkeerde koppeling in het interne BRP-proces). Door een vervallen BSN te versleutelen met de BSNk-sleutel kan worden vastgesteld of deze voorkomt in de tabel met opgeslagen UID's en versleutelde BSN's. Blijkt dat zo te zijn, dan kan ook in dit geval aan de eIDAS-berichtenservice worden verzocht om dit UID te verwijderen, zodat bij het eerstvolgende verzoek een goede koppeling kan worden gelegd.

[59] Of historisch te maken voor tracingdoeleinden.

Bijlage C Aanbevelingen uit PIA eIDAS-koppelpunt

De PIA op het eIDAS-koppelpunt die wij in 2015 hebben uitgevoerd, bevatte een aantal aanbevelingen. Er is voor gekozen om die niet integraal te verwerken in dit rapport. Dat betekent dat ze in principe nog overeind staan. Hieronder herhalen we deze aanbevelingen, met daaraan toegevoegd telkens een weergave door opdrachtgever van de huidige stand van zaken en onze reactie daarop.

Aanbeveling 1

Artikel 1 sub d Wbp schrijft voor dat er minimaal één verantwoordelijke is voor het eIDAS-koppelpunt.[60] De analyse van de Artikel 29 Werkgroep op het STORK-project laat zien dat er iets voor te zeggen valt dat de exploitant van een eIDAS-node een verantwoordelijke is vanwege zijn taken ('feitelijke verantwoordelijkheid'), maar ook dat deze een bewerker kan zijn voor de overheidsdienstverleners. Om aan deze discussie een eind te maken en helderheid te scheppen in wie nu eigenlijk de verantwoordelijke is en dus wie verantwoordelijk is voor de naleving van de verplichtingen van de Wbp, de rechten van de betrokkene moet waarborgen en aansprakelijk is als het mis gaat, adviseren wij om bij wet een verantwoordelijke voor het koppelpunt aan te wijzen. Dit is in lijn met het uitgangspunt dat verantwoordelijkheden daar moeten worden belegd waar dat de naleving van de regelgeving met betrekking tot gegevensbescherming in de praktijk voldoende is gewaarborgd.[61] Daarmee wordt deze partij een 'formele verantwoordelijke'.[62]
Er zijn dan drie basisvarianten mogelijk:

1) <u>De Minister van EZ is de verantwoordelijke</u>
   De wet wijst in dit geval de Minister van EZ aan als verantwoordelijke in de zin van de Wbp. Er zijn dan een aantal subvarianten denkbaar:

   a) *In-house oplossing:* De Minister van EZ is verantwoordelijke en de oplossing wordt binnen EZ gehost.
   b) *Semi-inhouse oplossing:* De Minister van EZ is verantwoordelijke, maar de oplossing wordt elders binnen het Rijk gehost. Die overheidsinstantie wordt dan bewerker voor EZ.
   c) *Externe oplossing:* De Minister van EZ is verantwoordelijke, maar de oplossing wordt bij een private partij gehost (bijv. een eID-makelaar). Die partij wordt dan bewerker voor EZ.

2) <u>De eID-makelaar (of een andere private partij) is verantwoordelijke</u>
   De wet wijst in dit geval de private partij die voldoet aan specifieke criteria aan als verantwoordelijke in de zin van de Wbp. De Minister van EZ is alleen nog beleidsverantwoordelijk, maar geen 'verantwoordelijke' in de zin van de Wbp.

3) <u>De overheidsdienstverleners die gebruik maken van eID zijn de verantwoordelijke</u>
   In deze variant is de exploitant van het eIDAS-koppelpunt slechts een bewerker voor de aangesloten partijen. Deze variant werd door de Artikel 29 Werkgroep als mogelijkheid

[60] Artikel 2.5e van het wetsvoorstel bepaalt weliswaar dat de Minister van Economische Zaken verantwoordelijke is voor enkele verwerkingen die samenhangen met vertrouwensdiensten, maar dat is een ander onderwerp in de verordening, dat geen direct verband houdt met elektronische identificatie.

[61] Zie ook het Advies van de Artikel 29 Werkgroep inzake de begrippen 'verantwoordelijke' en 'bewerker' van 16 februari 2010 (WP 169).

[62] De artikel 29 Werkgroep spreekt in dat geval over een verantwoordelijke "op grond van een uitdrukkelijke juridische bevoegdheid", dat wil zeggen dat de voor de verwerking verantwoordelijke of de specifieke criteria voor zijn aanstelling zijn vastgelegd in nationale of communautaire wetgeving (Opinie van 16 februari 2010, WP169, pagina 12).

geopperd.[63] Een bewerkersrol voor het koppelpunt past ons insziens echter niet vanwege het feit dat de Wbp voorschrijft dat de verantwoordelijke toezicht moet houden op de bewerker (art. 14 lid 1) en dat de verantwoordelijke instructies mag/moet geven aan de bewerker (art. 14 lid 3 juncto artikel 12 lid 1). Dat impliceert dat er een relatie is tussen de verantwoordelijke en de bewerker waarin deze rechten van de verantwoordelijke ook geoperationaliseerd kunnen worden. Van dat laatste zal geen sprake zijn als het koppelpunt bewerker is voor de partijen die daarop zijn aangesloten. Daarnaast brengt deze variant aanzienlijke administratieve lasten met zich mee, omdat er met heel veel partijen afspraken moeten worden gemaakt. Bovendien is het waarschijnlijk niet goed mogelijk om bij Nederlandse wet een buitenlandse overheidsdienstverlener te benoemen tot verantwoordelijke. Daarom raden wij deze variant af.

Welke variant gekozen wordt, is vooral afhankelijk van de vraag wie (in juridische zin) de regie over het koppelpunt zal moeten gaan voeren en dus de kaders mag stellen (anders dan bij wet- en regelgeving) waarbinnen de gegevens worden verwerkt. Deze partij is dan verantwoordelijk voor de nakoming van de verplichtingen van de Wbp en het waarborgen van de rechten van de betrokkenen. Daarnaast is hij aansprakelijk voor de schade of het nadeel dat voortvloeit uit het niet-naleven van die verplichtingen, zelfs als die schade of dat nadeel is veroorzaakt door de bewerker.

Reactie opdrachtgever

De Autoriteit Persoonsgegevens heeft in zijn advies over de uitvoeringswet onder meer aangegeven dat de verantwoordelijkheid voor het knooppunt goed moet zijn belegd. Dit advies is ter harte genomen. De Minister van Economische Zaken is voorlopig zowel verantwoordelijke voor het eIDAS-koppelpunt in de zin van de Wet Bescherming Persoonsgegevens (artikel 1d) als beheerder van het koppelpunt. Op deze manier wordt de complexiteit verminderd en is de verantwoordelijkheid eenduidig belegd. In de Memorie van Toelichting is geëxpliciteerd dat de Minister van EZ de verantwoordelijke is, en in ieder geval tot september 2018 ook de beheerder. Na die datum kan EZ eventueel een private partij inschakelen als beheerder van het knooppunt. Deze partij wordt dan bewerker voor de Minister van EZ als verantwoordelijke.

Onze reactie

Hiermee is de verantwoordelijkheid voor het eIDAS-koppelpunt voldoende geregeld. Dit is ook zo in het onderhavige rapport verwoord.

Aanbeveling 2

Het omzetten van het BSN in een andere unieke identifier is een verwerking die een grondslag moet hebben in de wet (art. 24 Wbp). Derhalve bevelen wij aan om de omzetting van het BSN ten behoeve van de verwerking via het eIDAS-koppelpunt een expliciete wettelijke basis te geven.

Onze reactie

Deze aanbeveling blijkt bij nader inzien waarschijnlijk onjuist. Zie onder het kopje “Juridische aspecten verwerking BSN” bij het antwoord op vraag 2 onder e in hoofdstuk 5.

Aanbeveling 3

De informatie aan de betrokkene over de privacyaspecten van de eIDAS-koppelpunten zou in Europa in principe overal hetzelfde moeten zijn. Daarnaast zou – gelet op het grensoverschrijdende karakter

[63] Dit was ook de variant die wordt gebruikt door SWIFT dat het berichtenverkeer in het internationale bankwezen afhandelt. In dat geval hebben we echter gezien dat die rol al snel kan omslaan tot verantwoordelijke. Zie Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128.

van de verwerking – de informatie in alle officiële talen van de Unie beschikbaar moeten zijn. Ook zal de informatie via de aangesloten overheidsdienstverleners moeten worden verstrekt omdat het koppelpunt geen interface heeft om met de betrokkene te communiceren. Wij bevelen daarom aan om de te verstrekken informatie over de privacyaspecten van het koppelpunt op Europees niveau in regelgeving vast te leggen.

Reactie opdrachtgever

De privacy-aspecten zijn grotendeels hetzelfde, aangezien de verordening en de uitvoeringshandelingen bepalingen bevatten ten aanzien van de verwerking van persoonsgegevens bij het grensoverschrijdend gebruik van elektronische identificatiemiddelen. Bovendien geldt de AVG, die zekerheid biedt op gebied van gegevensbescherming. Zo zijn overheden verplicht aan gebruikers te melden welke gegevens zij bewerken en voor welk doel hun gegevens gebruikt worden. Op dit moment staat bovendien dit harmonisatie van toegang tot diensten op de Europese agenda. Deze discussie is lopend. Informatie over privacy-aspecten heeft Nederland in deze bijeenkomsten aangekaart.

Onze reactie

Het is verheugend te constateren dat dit punt is aangekaart en aandacht krijgt. Wij zien daarin echter geen reden om deze aanbeveling in te trekken.

Aanbeveling 4

Momenteel stellen de Lidstaten zeer uiteenlopende eisen aan de beveiliging van verwerkingen van persoonsgegevens. Daardoor dreigt een lappendeken te ontstaan van beveiligingsmaatregelen, waardoor de identiteitsgegevens in de ene Lidstaat anders worden beveiligd dan in de andere Lidstaat. Dat is gelet op het Europese karakter van het netwerk niet logisch. Wij bevelen daarom aan om de beveiligingseisen voor de koppelpunten gedetailleerd uit te werken op Europees niveau en deze bindend op te leggen aan de Lidstaten.

Reactie opdrachtgever

Aanbevolen wordt om de eisen op het gebied van informatiebeveiliging Europees bindend op te leggen. Probleem is dat dit pas over minimaal vijf jaar kan, als eIDAS weer heronderhandeld wordt. Dus dit is een onrealistische wens. Wel heeft EZ in het *cooperation network* aangegeven dat hiervoor aandacht moet zijn.

Lidstaten moeten zich houden aan de AVG. Deze omvat ook bepalingen voor de verwerking van persoonsidentificatiegegevens van burgers. Het spreekt voor zich dat Nederland de nationale eisen t.a.v. beveiliging van persoonsgegevens niet aan andere lidstaten op kan leggen. Wel kan Nederland in de *peer review* ervoor kiezen om de eID-stelsels van andere landen te evalueren en de beveiligingseisen te toetsen.

Aandachtspunten daarbij zijn de pseudonimisering van identificatiegegevens en encryptie van persoonsgegevens, zodat alleen de dienstverlener ze kan lezen. Tevens is privacy een zeer belangrijk aandachtspunt en moet erop worden toegezien dat alleen die attributen doorgestuurd die voor de dienstverlening van belang zijn (privacy by design).

T.a.v. informatiebeveiliging is het zo dat ISO 27001 geldt, en uitvoeringsverordening 2015/1501 schrijft de vereiste voor om aan de laatste veiligheidseisen te voldoen. Verder zijn er (niet-bindende) richtlijnen opgesteld voor de uitwisseling van persoonsinformatie. Ze gaan primair over de communicatie tussen de lidstaten, maar verder niet over de manier waarop de lidstaten ‘achter de voordeur’ met informatie moeten omgaan.

Onze reactie
Het is verheugend te constateren dat dit punt is aangekaart en aandacht krijgt. Wij zien daarin echter geen reden om deze aanbeveling in te trekken.

Aanbeveling 5 (voor zover Aanbeveling 4 niet wordt gevolgd)
Indien het eIDAS-koppelpunt wordt ondergebracht bij een of meer eID-makelaars, bevelen wij – gelet op het feit dat beveiliging van het gegevensverkeer door het koppelpunt de belangrijkste zorg is als het gaat om de privacyrisico's van de betrokkene – aan om specifieke minimumeisen te stellen op het gebied van informatiebeveiliging die door deze makelaars moeten worden geïmplementeerd. Het kan gaan om technische eisen, maar ook om organisatorische eisen (bijv. periodieke audits).
Als de Minister de verantwoordelijke is en de eID-makelaar de bewerker voor het eIDAS-koppelpunt dan dienen deze eisen in de aanbesteding en de bewerkersovereenkomst worden neergelegd. Bij de aanbesteding dienen de beveiligingseisen een knock-out criterium te zijn.

Reactie opdrachtgever
Zie de reactie op Aanbeveling 1. Voorlopig is er nog geen sprake van het onderbrengen van een koppelpunt bij private partijen via een bewerkersovereenkomst. Dit is ondervangen doordat ervoor gekozen is het knooppunt de komende tijd te beleggen bij de minister van Economische Zaken. De specifieke eisen waaraan EZ voldoet zijn bescheven in de reactie op Aanbeveling 8. Wanneer een makelaar als bewerker een dergelijk knooppunt zelf zou gaan neerzetten, dan zou EZ deze eisen alsnog moeten (laten) opstellen.

Onze reactie
Deze aanbeveling is momenteel dus niet actueel. Dat doet aan de inhoud ervan echter niets af.

Aanbeveling 6
Artikel 7 sub f eIDAS-verordening laat toe dat Lidstaten voorwaarden stellen aan andere vertrouwende partijen dan openbare diensten. Wij adviseren de eisen rondom privacy en security, waaronder het uitvoeren van een privacy impact assessment en/of risicoanalyse op het gebied van informatiebeveiliging, onderdeel uit te laten maken van de aansluitvoorwaarden op het eIDAS-koppelpunt.

Reactie opdrachtgever
Voor nieuwe aansluitingen zal aangesloten worden bij de afspraken en vereisten die een nationaal eID stelsel stelt aan een elke nieuwe aansluiting. Voor aansluitingen op DigiD is er een DigiD-assessment, en voor een aansluiting op eHerkenning wordt dit geregeld met een privaatrechtelijk contract tussen de eHerkenningsmakelaar en de dienstaanbieder. Wel wordt op dit moment gewerkt aan de architectuur van de inbedding van het eIDAS-knooppunt in de nationale stelsels voor elektronische identificatie.

Vooralsnog zijn alleen openbare diensten aangesloten. Wel overwegen enkele private partijen om aan te sluiten op het eIDAS-koppelpunt. Het verplicht uitvoeren van een PIA en/of risico-analyse kan echter een hoge drempel blijken.

Onze reactie
Het is goed mogelijk dat de voorwaarden van DigiD en eHerkenning de noodzaak voor het doen van een PIA geheel of grotendeels wegnemen. Het beoordelen daarvan valt echter buiten de reikwijdte van de onderhavige PIA. Relevant in dit verband is nog art. 35 AVG, dat een PIA verplicht stelt in een aantal gevallen, mede te bepalen door de Autoriteit Persoonsgegevens.

Aanbeveling 7

Alvorens het eIDAS-koppelpunt wordt ondergebracht bij een of meer private partijen, bevelen wij aan om een risico-evaluatie uit te voeren op de door die partijen geboden technische en bestuurlijke omgeving.
Dit geldt ook voor het geval de eIDAS-node bij EZ zelf wordt ondergebracht. In dat laatste geval bevelen wij aan om een Wbp-coördinator van EZ en de Functionaris voor de Gegevensbescherming van EZ betrokken te betrekken bij de implementatie.

Reactie opdrachtgever

De Wbp-coördinator en de privacycoördinator van EZ zijn inmiddels op de hoogte dat het eIDAS knooppunt binnen het ministerie geïmplementeerd wordt. Aan hen zal gerapporteerd worden over de voortgang van de implementatie. De Functionaris voor de Gegevensbescherming zal geïnformeerd worden over de PIA op de startarchitectuur.

Onze reactie

Wij zijn verheugd te constateren dat deze aanbeveling is opgevolgd.

Aanbeveling 8

De keuze tussen end-to-end encryptie en encryptie per schakel in de keten is nog open. End-to-end encryptie heeft het voordeel dat de gegevens niet toegankelijk zijn voor het koppelpunt, waardoor het risico van datadiefstal of misbruik van data de medewerkers vormen wordt verkleind.
In ieder geval, maar zeker als er sprake is van encryptie per schakel, dienen passende maatregelen te worden genomen om deze risico's te verminderen. Deze maatregelen dienen in ieder geval te betreffen:

- Het opleggen van een geheimhoudingsplicht;
- Het vragen van een Verklaring omtrent het gedrag (VOG);
- Het toepassen van functiescheiding en *least privilege*;
- Het loggen van de toegang tot het systeem en de verrichte handelingen; en
- Bewustwording op het gebied van informatiebeveiliging.

Een grondige risicoanalyse op het gebied van informatiebeveiliging alvorens het systeem live gaat zal mogelijk nog tot aanvullende maatregelen op het gebied van *human resource security* leiden.

Reactie opdrachtgever

De eIDAS architectuur[64] staat voor landen die gebruik maken van een proxy service (vrijwel alle EU-lidstaten) geen volledige end-to-end encryptie toe. Immers, dat zou betekenen dat elke Nederlandse dienstverlener alle Europese authenticatiediensten moet kennen en omgekeerd alle Europese authenticatiediensten kennis moeten hebben van elke individuele Nederlandse dienstverlener. Wél vindt er end-to-end encryptie plaats in het Nederlandse gedeelte van de inlogketen en tussen de eIDAS-knooppunten onderling.

Het eIDAS-koppelpunt 'overbrugt' de end-to-end encryptie tussen (1) de eIDAS-knooppunten en (2) de nationale eID-infrastructuur. Voor maximale veiligheid zijn diverse maatregelen al genomen:

- Het eIDAS koppelpunt is in beheer bij DICTU, de Dienst ICT Uitvoering van het Ministerie van EZ. DICTU is ISO 27001 gecertificeerd. Dit betekent dat passende maatregelen voor informatiebeveiliging zijn genomen. DICTU implementeert verder de Baseline Informatiebeveiliging Rijksdienst (BIR). Dit betekent dat algemene maatregelen als antivirus, security updates, personal firewalls etc. etc. binnen de door DICTU geïmplementeerde

[64] https://joinup.ec.europa.eu/sites/default/files/eidas_interoperability_architecture_v1.00.pdf.

infrastructuur van toepassing zijn. Er is bewustwording ten aanzien van (het belang) van informatiebeveiliging.
- Ambtelijke medewerkers leggen de eed af. Inhuur wordt geheimhoudingsplicht opgelegd en leveren verplicht een VOG aan.
- Er vindt logging op het knooppunt plaats, zodat rapportage en audit trail mogelijk zijn. Verder worden aanvullende maatregelen ten behoeve van grootschalig gebruik voorzien, waaronder het dubbel uitvoeren van het koppelpunt en veilig sleutelbeheer met een *hardware security module* (HSM).

Onze reactie
Een gedetailleerde beoordeling van informatiebeveiligingsaspecten valt buiten de reikwijdte van een PIA. Wel zijn we verheugd te constateren dat het eIDAS-koppelpunt (in eerste instantie) wordt ondergebracht bij een onderdeel van EZ dat goed met informatiebeveiliging lijkt om te gaan. Dat doet overigens niet af aan de noodzaak van een risicoanalyse om de specifieke beveiligingsvereisten van de eIDAS-infrastructuur in kaart te brengen.

Aanbeveling 9
Een belangrijk deel van de privacy- en securityaspecten van het eIDAS-koppelpunt wordt ingevuld door de referentie-implementatie en de software die door de Europese Commissie wordt ontwikkeld. Voor zover dit nog niet gedaan is, bevelen wij aan dat op Europees niveau alsnog een PIA, inclusief risico-evaluatie op het gebied van de informatiebeveiliging, op die referentie-implementatie en de software wordt uitgevoerd.

Reactie opdrachtgever
Zodra de referentie-architectuur wordt geïmplementeerd zal er een PIA worden uitgevoerd om de privacy- en securityaspecten van het eIDAS-knooppunt te beoordelen. Gelet op het beginsel van subsidiariteit kan Nederland echter niet afdwingen dat op EU-niveau een PIA wordt uitgevoerd.

Onze reactie
Wij begrijpen dat Nederland de EU niet zonder meer kan dwingen tot het uitvoeren van een PIA. Van het ontbreken daarvan kan echter in EU-verband wel een punt gemaakt worden. Zeker nu de AVG in werking is getreden is het kwestieus om zo'n omvattende infrastructuur als eIDAS in te voeren zonder (kennelijk) daarop een deugdelijke PIA uit te voeren. Nederland zou (zo mogelijk samen met andere lidstaten) zelf een PIA kunnen uitvoeren, en – als daar aanleiding voor is – de uitkomsten daarvan agenderen in Brussel.

Aanbeveling 10
Omdat met het toelaten van andersoortige attributen de privacyrisico's van het eIDAS-koppelpunt mogelijk kunnen wijzigen, met eventuele gevolgen voor de te implementeren maatregelen, adviseren wij om telkens bij de toelating van dergelijke attributen een aanvullende PIA uit te voeren.

Reactie opdrachtgever
De minimale gegevens die worden doorgegeven zijn voor personen de voornaam, achternaam, geboortedatum en een unieke identificatiecode. Bij rechtspersonen gaat het om de wettelijke naam en een unieke identificatiecode. Deze gegevens zijn versleuteld. Dit is een privacybeschermende maatregel waardoor de gegevens onleesbaar zijn ingeval van onderschepping. Ontvangende lidstaten mogen ten behoeve van de identiteitsvaststelling naast de minimale dataset ook een aanvullende dataset opvragen. De aanvullende dataset bestaat uit: voornaam of voornamen en familienaam of

familienamen bij geboorte, geboorteplaats, huidig adres, geslacht. Bij de aanvullende PIA zal hiermee rekening worden gehouden.

Onze reactie

De samenstelling van de minimale dataset is in de eIDAS-regelgeving vastgelegd. De aanbeveling gaat echter juist over het uitwisselen van attributen die buiten deze datasetvallen.[65]

[65] Zie paragraaf 6.2.

Bijlage D Relevante eIDAS-bepalingen

Gegevensverwerking, -bescherming en beveiliging

– eIDAS-verordening
  - (11): “Deze verordening dient te worden toegepast in volledige overeenstemming met de beginselen inzake de bescherming van persoonsgegevens overeenkomstig Richtlijn 95/46/EG[66] van het Europees Parlement en de Raad. In dit verband en met inachtneming van het bij deze verordening vastgestelde beginsel inzake wederzijdse erkenning, mag authenticatie voor een onlinedienst alleen betrekking hebben op de verwerking van die identificatiegegevens die toereikend, ter zake dienend en niet bovenmatig zijn om toegang tot die onlinedienst te verlenen.”
  - art. 5 lid 1: “De verwerking van persoonsgegevens geschiedt in overeenstemming met Richtlijn 95/46/EG.”
    art. 5 lid 2: “Onverminderd het rechtsgevolg dat dat aan het gebruik van pseudoniemen op rond van het nationaal recht wordt toegekend, wordt het gebruik ervan in elektronische transacties niet verboden

– Uitvoeringsverordening (EU) 2015/1501
  - art. 6 lid 1: “De bescherming van privacy en vertrouwelijkheid van de door de knooppunten uitgewisselde gegevens en de handhaving van de integriteit van die gegevens wordt gewaarborgd door middel van de beste beschikbare technische oplossingen en beschermingsmaatregelen.
    art. 6 lid 2: “De knooppunten slaan geen persoonsgegevens op, behalve voor het in artikel 9, lid 3, genoemde doel” (zie hierna)
  - art. 9 lid 3: De exploitant van het knooppunt slaat gegevens op aan de hand waarvan, in geval van een incident, de uitwisseling van berichten in de juiste volgorde kan worden gereconstrueerd teneinde de plaats en de aard van het incident vast te stellen. De gegevens worden zolang bewaard als volgens de nationale voorschriften vereist is en bevatten ten minste de volgende elementen:
    a) de identificatie van het knooppunt;
    b) de identificatie van het bericht;
    c) de datum en de tijd van het bericht

Toepassingsgebied

- eIDAS-verordening
  - art. 2 lid 1: “Deze verordening is van toepassing op stelsels voor elektronische identificatie die zijn aangemeld door een lidstaat […]”

Aanmelding stelsel van elektronische identificatie

- eIDAS-verordening
  - art. 7 onder d t/m f: Een stelsel voor elektronische identificatie komt voor aanmelding in aanmerking indien voldaan wordt aan alle onder a – h benoemde voorwaarwaarden. Voor deze PIA zijn met name sub d – f van belang.

    “d) de aanmeldende lidstaat waarborgt dat de persoonsidentificatiegegevens die de persoon in kwestie op unieke wijze kenmerken op het moment van uitgifte van het elektronische identificatiemiddel op grond van dat stelsel, conform de technische specificaties, normen en procedures voor het respectieve betrouwbaarheidsniveau zoals

[66] De AVG zal de Richtlijn doen vervallen vanaf mei 2018.

neergelegd in de uitvoeringshandeling bedoeld in artikel 8, lid 3, worden gekoppeld aan de natuurlijke persoon of rechtspersoon als bedoeld in artikel 3, punt 1;

e) de partij die het elektronische identificatiemiddel uitgeeft op grond van dat stelsel, zorgt ervoor dat het elektronische identificatiemiddel wordt gekoppeld aan de persoon bedoeld in punt d) van dat artikel, in overeenstemming met de technische specificaties, normen en procedures voor het respectieve betrouwbaarheidsniveau zoals neergelegd in de uitvoeringshandeling bedoeld in artikel 8, lid 3;

f) de aanmeldende lidstaat zorgt voor de beschikbaarheid van onlineauthenticatie, zodat iedere vertrouwende partij die op het grondgebied van een andere lidstaat gevestigd is, de mogelijkheid heeft de ontvangen persoonsidentificatiegegevens in elektronische vorm te bevestigen.

Voor andere vertrouwende partijen dan openbare instanties mag de aanmeldende lidstaat voorwaarden stellen voor toegang tot die authenticatie. Grensoverschrijdende authenticatie is kosteloos wanneer zij wordt uitgevoerd voor een door een openbare instantie verleende onlinedienst.

De lidstaten leggen geen specifieke onevenredige technische eisen op aan vertrouwende partijen die voornemens zijn een dergelijke authenticatie uit te voeren indien dergelijke eisen de interoperabiliteit van de aangemelde stelsels voor elektronische identificatie tegenhouden of in aanzienlijke mate belemmeren;"

Persoonsidentificatiegegevens

- Uitvoeringsverordening (EU) 2015/1501
  - art. 11 lid 1: "Het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of een rechtspersoon op unieke wijze vertegenwoordigt, voldoet bij gebruik in een grensoverschrijdende context aan de vereisten die in de bijlage zijn opgenomen."
    art. 11 lid 2: "Het minimale pakket persoonsidentificatiegegevens voor een natuurlijke persoon die een rechtspersoon vertegenwoordigt, bevat bij gebruik in een grensoverschrijdende context een combinatie van de attributen die in de bijlage voor natuurlijke personen en rechtspersonen zijn vermeld."
    art. 11 lid 3: "De gegevens worden doorgegeven in het oorspronkelijke schrift, voor zover nodig met een transliteratie in Latijns schrift."
  - Bijlage: "Vereisten betreffende het minimale pakket persoonsindentificatiegegevens dat een natuurlijk persoon of rechtspersoon op unieke wijze vertegenwoordigt, als bedoeld in artikel 11."
    1. Minimaal gegevenspakket voor een natuurlijke persoon
    Het minimale gegevenspakket voor een natuurlijke persoon bevat al de volgende verplichte attributen:
    a) huidige familienaam of familienamen;
    b) huidige voornaam of voornamen;
    c) geboortedatum;
    d) unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft.
    Het minimale gegevenspakket voor een natuurlijke persoon kan één of meer van de volgende aanvullende attributen bevatten:
    a) voornaam of voornamen en familienaam of familienamen bij geboorte;
    b) geboorteplaats;
    c) huidig adres;
    d) geslacht.

2. Minimaal gegevenspakket voor een rechtspersoon Het minimale gegevenspakket voor een rechtspersoon bevat al de volgende verplichte attributen:
a) huidige wettelijke naam;
b) unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft.
Het minimale gegevenspakket voor een rechtspersoon kan één of meer van de volgende aanvullende attributen bevatten:
a) huidig adres;
b) btw-nummer;
c) fiscaal referentienummer;
d) de identificatiecode bedoeld in artikel 3, lid 1, van Richtlijn 2009/101/EG van het Europees Parlement en de Raad (1);
e) de identificatiecode voor juridische entiteiten bedoeld in Uitvoeringsverordening (EU) nr. 1247/2012 van de Commissie (2);
f) het registratie- en identificatienummer van marktdeelnemer (EORI-nr.) bedoeld in Uitvoeringsverordening (EU) nr. 1352/2013 van de Commissie (3);
g) het accijnsnummer bedoeld in artikel 2, punt 12, van Verordening (EU) nr. 389/2012 van de Raad (4).

Private dienstverleners

- eIDAS-verordening
  - (17) “De lidstaten dienen de private sector aan te moedigen vrijwillig gebruik te maken van elektronische identificatiemiddelen die onder een genotificeerd stelsel vallen, indien identificatie bij onlinediensten of elektronische transacties nodig is. […] Om het gebruik van dergelijke elektronische identificatiemiddelen door de private sector over de grenzen heen te vergemakkelijken, moet de mogelijkheid tot authenticatie die elke lidstaat biedt, beschikbaar zijn voor buiten het grondgebied van die lidstaat gevestigde vertrouwende partijen uit de private sector, en wel onder dezelfde voorwaarden als in die lidstaat gevestigde vertrouwende partijen. Bijgevolg mag de aanmeldende lidstaat t.a.v. vertrouwende partijen uit de private sector voorwaarden voor toegang tot de authenticatiemiddelen bepalen. Die voorwaarden voor toegang kunnen vermelden of de authenticatiemiddelen voor het genotificeerde stelsel voor elektronische identificatie op dat moment beschikbaar zijn voor vertrouwende partijen uit de private sector.”
  - art. 7 onder f: “de aanmeldende lidstaat zorgt voor de beschikbaarheid van onlineauthenticatie, zodat iedere vertrouwende partij die op het grondgebied van een andere lidstaat gevestigd is, de mogelijkheid heeft de ontvangen persoonsidentificatiegegevens in elektronische vorm te bevestigen.
    “Voor andere vertrouwende partijen dan openbare instanties mag de aanmeldende lidstaat voorwaarden stellen voor toegang tot die authenticatie. Grensoverschrijdende authenticatie is kosteloos wanneer zij wordt uitgevoerd voor een door een openbare instantie verleende onlinedienst.”
- Uitvoeringsverordening (EU) 2015/1501
  - art. 4 lid 2: “De knooppunten zijn in staat om met technische hulpmiddelen onderscheid te maken tussen organen van de publieke sector en andere partijen die van het knooppunt gebruik maken”
  - art. 5 lid 2: “De knooppunten zijn in staat om met technische hulpmiddelen onderscheid te maken tussen organen van de publieke sector en andere partijen die van het knooppunt gebruikmaken.”

- art. 8 onder c: “De knooppunten maken voor de syntaxis van de berichten gebruik van gemeenschappelijk berichtformaten die reeds meermalen zijn toegepast door lidstaten en waarvan de deugdelijkheid in een operationele omgeving is aangetoond.” De syntaxis maakt o.a. mogelijk: “(c) het onderscheid tussen organen van de publieke sector en andere partijen die van het knooppunt gebruik maken”.