HOOGHIEMSTRA & PARTNERS

strategisch en juridisch advies

Definitief rapport

HOOGHIEMSTRA & PARTNERS

Strategische visie Plan van Aanpak geïntegreerd eID-stelsel

Versie 20 april 2020

Inhoudsopgave

1. Managementsamenvatting

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft mr. dr. Theo Hooghiemstra van Hooghiemstra & Partners, een onafhankelijk strategisch-juridisch adviesbureau op het raakvlak van technologie en recht, benaderd om een strategische visie te geven in de vorm van een integraal Plan van Aanpak om te komen tot een geïntegreerd stelsel van elektronische identificatie en authenticatie voor burgers en bedrijven (eID-stelsel). Met andere woorden is gevraagd om een strategische visie voor een geïntegreerd eID-stelsel. Onder een geïntegreerd stelsel in de context van deze strategische visie wordt verstaan een stelsel waarin burgers, bedrijven en overheden met de door hen gekozen elektronische authenticatiemiddelen gebruik kunnen maken van digitale diensten van publieke en private dienstverleners.

De keuze voor een geïntegreerd stelsel doet recht aan het doel van de Europese verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS-verordening) om een interne markt voor middelen te creëren en het vertrouwen in elektronische transacties in de interne markt te vergroten. Deze verordening maakt geen onderscheid tussen middelen voor burgers en bedrijven. Beleidsmatig uitgangspunt is een open stelsel waaraan na toelating ook private leveranciers van eID-diensten kunnen deelnemen.

Gelet op de opdracht – en mede gelet op de tijd die voor deze opdracht beschikbaar was – is de strategische visie beperkt tot hoofdlijnen, met name vanuit strategisch-juridisch perspectief. In een geïntegreerd eID-stelsel zullen ook vertrouwensdiensten worden geleverd waaruit wilsuitingen blijken (denk hierbij bijvoorbeeld aan een elektronische handtekening). Deze diensten zijn, evenals de online identiteit, buiten scope gelaten.

Na een beschrijving van het bestaande landschap, inclusief de stand van zaken rondom het wetgevingsproces van de Wet digitale overheid (Wdo) en de Algemene Maatregelen van Bestuur die in procedure zijn, is geschetst wat de kenmerken van het gewenste eID-stelsel zijn.

Het gewenste stelsel valt samen te vatten als een geïntegreerd stelsel met oplossingen voor actoren gerelateerd aan de rol die zij spelen bij het afnemen van een dienst. Tot dit stelsel kunnen alleen partijen toetreden die aan de gestelde eisen voldoen. Bovendien biedt het stelsel burgers en bedrijven waarborgen op het gebied van gegevensbescherming, keuzevrijheid, veiligheid en continuïteit. In het eID-stelsel is een juiste balans gevonden tussen de belangen en rechten van alle stelselpartijen. Deze strategische visie leidt tot de volgende zeven adviezen.

Ten eerste is het advies de huidige governance-structuur van het eTD-stelsel aan te passen, zodra het eTD-stelsel opgaat in een geïntegreerd eID-stelsel. Om te komen tot een geïntegreerd eID-stelsel zal een programma moeten worden opgezet waarin dit stelsel wordt ontworpen en ontwikkeld. De nieuwe governance-structuur zal tevens binnen dit programma moeten worden meegenomen. Daarbij dient ook rekening te worden gehouden met de huidige governance in het publieke domein, zoals bij DigiD. Onafhankelijkheid en representativiteit van stelselpartijen dienen gewaarborgd te zijn. Geadviseerd wordt alle stelselpartijen die een rol (gaan) spelen in het geïntegreerde eID-stelsel op korte termijn te laten beginnen met het opstellen van een gemeenschappelijke agenda voor de wensen van gebruikers ten behoeve van de ontwikkeling van het eID-stelsel. Daarbij wordt aanbevolen de wensen van burgers continu te monitoren en de wensen van andere gebruikers in een gestructureerd overleg te bespreken. Bij de opzet van het programma zal de positie van het gestructureerde overleg worden bepaald. Geadviseerd wordt dat de minister van Binnenlandse Zaken en Koninkrijksrelaties een voorzitter aanwijst die het gestructureerde overleg voorzit. Hiermee wordt hij daadwerkelijk als stelselverantwoordelijke in positie gebracht. Aanbevolen wordt gelijk te beginnen met de voorbereidingen. Hiertoe dient het ministerie van Binnenlandse Zaken

en Koninkrijksrelaties menskracht en (financiële) middelen te reserveren om dit praktisch mogelijk te maken. Dit geldt zowel voor het inrichten van het gestructureerde overleg als het opzetten en inrichten van een programma.

Een tweede belangrijk resultaat van dit programma is een duurzaam financieringsmodel. Geadviseerd wordt om de komende maanden binnen het gestructureerde overleg de opties voor een duurzaam financieringsmodel inhoud te geven, bijgestaan door (financiële en procesmatige) experts. Daarnaast wordt geadviseerd om in de ministeriële regeling behorende bij de Wdo, aandacht te besteden aan het bekostigingsmodel in relatie tot de bijbehorende governance.

Ten derde wordt geadviseerd – vooruitlopend op het tot stand komen van een geïntegreerd eID-stelsel – dat het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een snelle groei van de eID-markt bevordert. Bij het bevorderen van deze snelle groei is cruciaal dat dit de ontwikkeling van een geïntegreerd eID-stelsel niet belemmert. Binnen een jaar kan het volgende worden gerealiseerd:

- Programmatische ontwikkeling van een eTD-stelsel voor het burgerdomein, inclusief andere toegelaten (binnenlandse en buitenlandse) partijen die aan de gestelde eisen voldoen, naast het huidige eTD-stelsel voor het bedrijvendomein. Dit wordt door experts als kansrijk gezien. Er dient nog wel een impactanalyse plaats te vinden;
- Beproef, met de intentie om daarna daadwerkelijk tot implementatie over te gaan, toepassingen op de betrouwbaarheidsniveaus substantieel en hoog. Buiten de zorgsector kan dit meestal niveau substantieel zijn. Binnen de zorgsector is in veel gevallen eIDAS betrouwbaarheidsniveau hoog noodzakelijk vanwege het medisch beroepsgeheim, de AVG en eIDAS. Daarbij kan bijvoorbeeld worden gedacht aan bestaande toepassingen met PKI. Gelet op de Corona-crisis is versnelling binnen het zorgdomein noodzakelijk;
- Inzichtelijk maken van de kosten van middelen en eID-diensten;
- Versneld bepalen van het betrouwbaarheidsniveau waarop digitale overheidsdiensten worden geleverd;
- Burgers helpen bij het maken van een keuze tussen middelen.

Bovendien wordt geadviseerd om bij het bevorderen van een snelle groei van de eID-markt rekening te houden met een toekomstbestendige oplossing door het hergebruik van middelen in andere domeinen (B2C, B2B, G2G) als mogelijkheid open te houden zodat dit kan worden meegenomen in het ontwerp van het geïntegreerd eID stelsel. Maatschappelijk gezien betreft dit een enorme kansrijke en relevante markt.

Ten vierde wordt wat betreft gegevensbescherming geadviseerd om rekening te houden met de verbodsbepaling in de AVG voor het verwerken van bijzondere categorieën van persoonsgegevens, tenzij daarvoor een in de wet genoemde grondslag voor bestaat. Dit kan bijvoorbeeld van belang zijn voor de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon. Bovendien dienen de rechten van betrokkenen, de transparantie en de verwerkingsverantwoordelijkheden van de deelnemers duidelijk te worden uitgewerkt en belegd om te voorkomen dat de gebruiker van het kastje naar de muur wordt gestuurd als er iets fout gaat in de lange authenticatieketen.

Regel in de tweede tranche van de Wdo de voorwaarden voor het gebruik van bijzondere categorieën van persoonsgegevens, mits goed doordacht en noodzakelijk om te komen tot een hoog betrouwbaarheidsniveau en bijbehorende gegevensbescherming, dan wel ten behoeve van de gebruiksvriendelijkheid van de betreffende middelen.

Ten vijfde wordt geadviseerd om in het geïntegreerde eID stelsel authenticatie en machtigen te ontkoppelen. Zo komt uiteindelijk een echt geïntegreerd eID-stelsel tot stand. Ontkoppeling van authenticatie en machtigen is van belang omdat daarmee de huidige lock-ins in het eTD-stelsel worden voorkomen. Tevens wordt de huidige situatie

doorbroken dat machtigingsdiensten in het burgerdomein slechts zijn voorbehouden aan overheidspartijen. In een volledig geïntegreerd stelsel dient deze machtigingsdienst ook door een private partij geleverd te kunnen worden. In de huidige eerste tranche van de Wdo is de ontkoppeling van authenticatie en machtigen nog niet geregeld. De ontkoppeling dient daarom in de tweede tranche van de Wdo geregeld te worden. Zorg daarbij voor voldoende functionaliteit om te kunnen machtigen.

Ten zesde wordt geadviseerd om het Agentschap Telecom, de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt een samenwerkingsprotocol te laten opstellen. Dit is van belang omdat het Agentschap Telecom AT weliswaar is aangewezen als onafhankelijk toezichthouder om toezicht te houden op de Wdo en zo nodig handhavend op te treden, maar daarnaast ook de Autoriteit Persoonsgegevens als toezichthouder op de AVG en andere dataprotectie-wetten en de Autoriteit Consument en Markt als markttoezichthouder taken hebben met betrekking tot toezichts- en handhavingstaken aangaande het eID-stelsel. Noodzakelijk is dat deze toezichthouders samen afspraken maken over de wijze van behandeling van aangelegenheden waarbij de aan hen opgedragen taken of de uitoefening van de aan hen toegekende bevoegdheden elkaar raken of overlappen.

Ten zevende wordt geadviseerd om de bestuurlijke continuïteit te verhogen door als ministerie van Binnenlandse Zaken en Koninkrijksrelaties de regie te nemen om te komen tot een stabiel en geïntegreerd eID-stelsel. De bestuurlijke continuïteit kan enerzijds worden verhoogd door bij de start van het programma de strategische uitgangspunten vast te stellen en anderzijds door dit juridisch te borgen. De Wdo en de bijbehorende uitvoeringsregelingen bieden hiervoor het anker. Borg juridisch de bestuurlijke continuïteit door:

A. Randvoorwaarden en aanvullende eisen aan erkende stelselpartijen te stellen in de ministeriële regeling, en
B. Onderwerpen die in de eerste tranche van de Wdo nog niet zijn geregeld, te regelen in de tweede en volgende tranches van deze wet of andere relevante wet- en regelgeving.

2. Inleiding

2.1 Aanleiding

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft mr. dr. Theo Hooghiemstra van Hooghiemstra & Partners, een onafhankelijk strategisch-juridisch adviesbureau op het raakvlak van technologie en recht, benaderd om een integraal Plan van Aanpak (PvA) op te stellen voor een te combineren stelsel van elektronische identificatie en authenticatie voor burgers en bedrijven. Theo Hooghiemstra is gevraagd om als conceptueel denker en netwerker bij het op te stellen PvA vanuit zijn bureau een pragmatische coördinator te betrekken in de persoon van senior adviseur mr. ir. Mark de Hek.

2.2 Opdrachtformulering

De opdracht is als volgt geformuleerd:

"Stel Theo Hooghiemstra als conceptueel denker en netwerker en een kundige, pragmatische coördinator voor de organisatorische planning & uitwerking – en eventuele extra benodigde ondersteuning – van Hooghiemstra & Partners ter beschikking voor het opstellen van een integraal PvA voor een nieuw gecombineerd stelsel van elektronische identificatie en authenticatie van burgers en bedrijven.

Maak bij de totstandkoming van het PvA gebruik van de specifieke kennis, ervaring en netwerken van Theo Hooghiemstra en zijn collega's.
De opdrachtgever voor deze opdracht - namens BZK - is Marc de Jong, programma-directeur bij het ministerie van BZK."

2.3 Scope

Gelet op de opdracht – en mede gelet op de tijd die voor deze opdracht beschikbaar was – is de strategische visie beperkt tot hoofdlijnen, met name vanuit strategisch-juridisch perspectief. In een geïntegreerd eID-stelsel zullen vertrouwensdiensten worden geleverd waaruit wilsuitingen blijken (denk hierbij bijvoorbeeld aan een elektronische handtekening). Deze diensten zijn, evenals de online identiteit, buiten scope gelaten.

2.4 Werkwijze

Bij dit advies is gebruik gemaakt van de specifieke expertise en ervaring van Theo Hooghiemstra en van de experts binnen zijn netwerk. Tevens is gebruik gemaakt van informatie die ter beschikking is gesteld door de opdrachtgever en relevante openbare documentatie. De experts zijn geraadpleegd in interviews en in expert-sessies. Hun expert-opinions en relevante documentatie zijn gebruikt voor het opstellen van deze strategische visie.

2.5 Voorgeschiedenis

Na een lang (wetgevings-)proces heeft de Tweede Kamer de Wdo aangenomen. Daarmee is een keuze gemaakt voor een wettelijke basis voor een eID-stelsel waaraan alle partijen kunnen deelnemen, mits zij voldoen aan de gestelde eisen (systeem van open toelating). Voorafgaand aan het systeem van open toelating was beoogd een aanbestedingsprocedure te volgen om partijen aan te wijzen die middelen zouden leveren voor authenticatie op met name het betrouwbaarheidsniveau substantieel en hoog in het publieke domein.
Al meer dan 20 jaar hebben de nodige ontwikkelingen plaatsgevonden om betrouwbaar digitaal inloggen bij

publieke dienstverleners mogelijk te maken. In 1999 was er al de ambitie om te komen tot een elektronische nationale identiteitskaart (eNIK) op betrouwbaarheidsniveau hoog. Op dit moment maken burgers gebruik van DigiD waarmee kan worden ingelogd bij de overheid en organisaties met een publieke taak (hoofdzakelijk op betrouwbaarheidsniveau laag). Tevens heeft de overheid geïnvesteerd in het uitgeven van paspoorten, identiteitskaarten en rijbewijzen waarop een elektronisch authenticatiemiddel is geplaatst. Daarnaast is het afsprakenstelsel Elektronische Toegangsdiensten met de merken eHerkenning en Idensys[1] (eTD-stelsel) tot stand gekomen waarmee kan worden ingelogd bij dienstverleners op de betrouwbaarheidsniveaus laag, substantieel en hoog. Bovendien hebben pilots plaatsgevonden waarbij burgers niet alleen met DigiD, maar ook met andere online authenticatiemiddelen konden inloggen: iDIN voor inloggen bij de Belastingdienst en Idensys voor inloggen bij diverse zorgpartijen, gemeenten en de Belastingdienst. In de loop der tijd hebben diverse dienstverleners hun eigen ontsluitende diensten ontwikkeld (bijvoorbeeld UWV, DUO, Belastingdienst) of zijn hiermee bezig (toegangsverleningsservice (TVS) van VWS). Alle bovenstaande ontwikkelingen bij elkaar hebben geleid tot een vergaande versnippering van het stelsellandschap.

2.6 Waarom een geïntegreerd stelsel?

Onder een geïntegreerd stelsel in de context van deze strategische visie wordt verstaan een stelsel waarin burgers, bedrijven en overheden met de door hen gekozen elektronische authenticatiemiddelen gebruik kunnen maken van digitale diensten van publieke en private dienstverleners.

De keuze voor een geïntegreerd stelsel doet recht aan het doel van de Europese verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS-verordening) om een interne markt voor middelen te creëren en het vertrouwen in elektronische transacties in de interne markt te vergroten door te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden, en bijgevolg ook de doeltreffendheid van publieke en private onlinediensten, e-business en elektronische handel in de Unie te verhogen.[2] Deze verordening maakt geen onderscheid tussen middelen voor burgers en bedrijven.
Bovendien heeft het eID-stelsel op grond van de Wdo als doel om op betrouwbare wijze de identiteit vast te stellen van degene die een dienst wil afnemen bij een dienstverlener. Een natuurlijke of rechtspersoon kan hiertoe gemachtigd zijn door een rechtspersoon of andere natuurlijke persoon. Ook vanuit deze gedachte wordt gestreefd naar een geïntegreerd stelsel waarin het burger- en bedrijvendomein samenvloeien. Beleidsmatig uitgangspunt is een open stelsel waaraan na toelating ook private leveranciers van eID-diensten kunnen deelnemen.[3]
Tot slot is er een steeds luider wordende roep om authenticatiemiddelen die in zowel het publieke als private domein kunnen worden gebruikt.

2.7 Indeling strategische visie

Deze strategische visie is als volgt opgebouwd. Na de voorafgaande managementsamenvatting en inleiding staat in het volgende hoofdstuk 3 beschreven hoe het bestaande landschap eruit ziet, inclusief de stand van zaken rondom het wetgevingsproces van de Wdo en de Algemene Maatregelen van Bestuur (AMvB's) die in procedure zijn. In hoofdstuk 4 zijn de kenmerken van het gewenste eID-stelsel geschetst. Het gewenste stelsel valt samen te vatten als een geïntegreerd stelsel met oplossingen voor actoren, gerelateerd aan de rol die zij spelen bij het afnemen van een dienst. Tot dit stelsel kunnen alleen partijen toetreden die aan de gestelde eisen voldoen. Bovendien biedt het stelsel burgers en bedrijven waarborgen op het gebied van

[1] Idensys heeft slechts als pilot bestaan.
[2] eIDAS-Verordening , overweging 2.
[3] Tweede nota van wijziging van 21 oktober 2019 (Tweede Kamer, vergaderjaar 2019–2020, 34 972, nr. 14).

gegevensbescherming, keuzevrijheid, veiligheid en continuïteit. In hoofdstuk 5 wordt de voorgestelde strategische visie gepresenteerd voor een PvA om te komen tot het gewenste geïntegreerde eID-stelsel. Hoofdstuk 6 bevat tot besluit enkele aanbevelingen.
De bevindingen van de strategische visie zijn gevisualiseerd in twee figuren, die als bijlage zijn toegevoegd:

1) Figuur 1: Het gewenste eID-stelsel;
2) Figuur 2: Eisen aan potentiële leveranciers van eID-diensten.

3. Het bestaande landschap

3.1 Veel ervaring maar ook versnippering en verkokering

In het huidige stelsellandschap is het nodige bereikt en is al veel ervaring opgedaan met het afsprakenstelsel eTD en met DigiD. Hetgeen wat er nu al is, vormt een goed fundament voor doorontwikkeling naar een geïntegreerd eID-stelsel. Het huidige stelsellandschap wordt echter ook gekenmerkt door versnippering en verkokering, terwijl er een toenemende behoefte aan middelen is die in zowel het publieke als het private domein kunnen worden gebruikt. Voor het burgerdomein is DigiD ontwikkeld dat alleen kan worden gebruikt voor het afnemen van digitale diensten van dienstverleners in het BSN-domein. Voor het bedrijvendomein bestaat het eerder genoemde afsprakenstelsel eTD waarmee bedrijven kunnen inloggen bij publieke dienstverleners. Het eTD-stelsel kan ook worden gebruikt in het business-to-businessdomein (B2B) en het government-to-governementdomein (G2G). Dit stelsel is eIDAS-genotificeerd en maakt inloggen op betrouwbaarheidsniveau substantieel en hoog mogelijk.
Tevens hebben diverse publieke dienstverleners hun eigen ontsluitende dienst ontwikkeld of zijn hiermee bezig. Veel publieke dienstverleners hebben het betrouwbaarheidsniveau van hun digitale dienstverlening nog niet bepaald. Wel is bepaald dat in de zorgsector op grond van het medisch beroepsgeheim, AVG en eIDAS eigenlijk in de meeste situaties in kunnen loggen op betrouwbaarheidsniveau hoog noodzakelijk is.[4]
DigiD kent een groot aantal gebruikers, maar veel gebruikers kunnen vooralsnog alleen inloggen op betrouwbaarheidsniveau laag. In de zorgsector is, zeker gelet op de huidige Corona-crisis, op zo kort mogelijke termijn de behoefte aan minimaal brede beschikbaarheid van authenticatie op niveau substantieel en liefst op niveau hoog.
Tot slot is de ontwikkeling van het eID-stelsel momenteel sterk gericht op het inloggen van burgers en bedrijven in het publieke domein, en nog niet op het inloggen in het private domein.

3.2 Huidige knelpunten

In de huidige situatie is een aantal belangrijke knelpunten te benoemen die de verdere ontwikkeling naar een geïntegreerd eID-stelsel belemmeren. In de eerste plaats is dit het *ontbreken van een governance-model* voor het geïntegreerde eID-stelsel waarin onafhankelijkheid en representativiteit van stelselpartijen zijn gewaarborgd. De minister van BZK dient zijn rol als stelselverantwoordelijke waar te kunnen maken. Hij is daarvoor nog niet in positie gebracht. De governancestructuur van het bestaande eTD-stelsel functioneert goed voor het eTD-stelsel voor bedrijven maar nog niet voor het publieke domein. Het speelveld van het geïntegreerde eID-stelsel is te groot voor de governancestructuur van het bestaande eTD-stelsel. Ook zal rekening dienen te worden gehouden met de huidige governance van DigiD. Het geïntegreerde eID-stelsel vergt een bijbehorende governance.

Een ander belangrijk knelpunt is de *bekostiging* van het stelsel. De volgende aspecten zijn hierbij met name van belang:

- De markt voor identificatie op betrouwbaarheidsniveau substantieel is vooralsnog aanzienlijk groter dan die voor authenticatie op betrouwbaarheidsniveau hoog;
- Veel publieke dienstverleners hebben nog niet de gewenste betrouwbaarheid bepaald voor hun digitale dienstverlening waardoor nog geen goed beeld bestaat van de publieke kant van de eID-markt;
- De grote diversiteit in gebruikers. Aan de ene kant van het spectrum staan de gebruikers die een zeer beperkt aantal authenticatietransacties uitvoeren en als gevolg hiervan niet bereid zijn om te betalen voor een privaat middel. Aan de andere kant van het spectrum staan de ‘grootverbruikers’ met een groot aantal

[4] Zie PBLQ/PrivacyCare, “Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg”, mei 2016.

transacties die een veel grotere betalingsbereidheid lijken te hebben;
- Het ontbreekt nog aan duidelijkheid over de kosten van de generieke voorzieningen en hoe deze worden omgeslagen.

Gelet hierop en in aanmerking nemende de vele koerswijzigingen die de afgelopen jaren hebben plaatsgevonden, hebben private partijen een afwachtende houding ingenomen.

Tevens is een knelpunt dat het huidige stelsel nog niet voorziet in een *machtigingsvoorziening* met voldoende functionaliteit. Er is een urgente maatschappelijke behoefte aan een goedwerkende machtigingsoplossing. Zonder een dergelijke voorziening worden burgers buitengesloten die digitale diensten willen afnemen bij dienstverleners, en de hulp van anderen nodig hebben. In het burgerdomein is een machtigingsvoorziening nog in ontwikkeling. Deze zal een goed doordachte machtigingsoplossing moeten bieden voor wettelijke vertegenwoordiging (onvrijwillig machtigen) en vrijwillig machtigen. Daarnaast zijn in het huidige eTD-stelsel authenticatie en machtigen nog aan elkaar gekoppeld en is de functionaliteit van de machtigingsvoorziening nog beperkt. Bovendien gaat het huidige eTD-stelsel uit van verticale machtiging terwijl het in het burgerdomein veelal gaat om horizontale machtiging. Het is van belang om machtigen en authenticatie van elkaar los te koppelen. Immers, het moet mogelijk zijn dat een machtigingsregister wordt bevraagd, zonder dat authenticatie plaatsvindt. Bijvoorbeeld om te controleren of iemand die zegt namens een ander op te treden (anders dan op een digitale wijze, bijvoorbeeld op papier, per telefoon of aan een balie), ook daadwerkelijk is gemachtigd. Tevens leidt de koppeling tot afhankelijkheden en lock-in situaties die in een open stelsel niet thuishoren.

3.3 Wetgevingsproces

Inmiddels is de eerste tranche van de Wdo door de Tweede Kamer aangenomen. Daarnaast zijn twee AMvB's in procedure. Dit betreft in de eerste plaats het Besluit digitale overheid dat regels stelt inzake informatieveiligheid en de verwerking van persoonsgegevens die gebruikt worden in het kader van de toegang tot elektronische overheidsdienstverlening. In het bijzonder dient de AMvB ter uitvoering van de artikelen 4 en 16 van de Wdo.

Daarnaast is het Besluit bedrijfs- en organisatiemiddel in procedure. Dit besluit stelt regels inzake de erkenning van private partijen die elektronische identificatiemiddelen leveren en de daarbij betrokken diensten aanbieden. Dit besluit dient meer in het bijzonder tot uitvoering van de artikelen 11, eerste, tweede, derde en vijfde lid, en 13, eerste, vierde en vijfde lid, van de Wdo.

Met de tweede tranche van de Wdo zal het onderscheid tussen het publieke en private domein geheel moeten verdwijnen. Een eerste aanknopingspunt voor het bijeenbrengen van deze domeinen is de nog op te stellen ministeriële regeling waarin voor beide domeinen één pakket van aanvullende eisen zal worden opgenomen. De ministeriële regeling heeft onder meer betrekking op technische standaarden, algemene eisen met betrekking tot erkende diensten, regels voor authenticatie-, ontsluitings- en machtigingsdiensten, interoperabiliteit, niveau van dienstverlening en (het indienen van) een aanvraag. Met het oog op het te realiseren geïntegreerde stelsel is deze ministeriële regeling van groot belang.

3.4 Rollen binnen het stelsel

Op grond van de Wdo is de minister van BZK stelselverantwoordelijke en is regisseur voor de inrichting en verdere ontwikkeling van het stelsel. Binnen het eID-stelsel kunnen verschillende rollen worden onderscheiden:

middeluitgevers, authenticatiediensten, machtigingsdiensten en ontsluitende diensten[5, 6]. Deze rollen kunnen door private en publieke partijen worden vervuld. Publieke en private identificatiemiddelen worden door de minister toegelaten voordat ze mogen worden gebruikt (artikel 9 Wdo). Voordat middeluitgevers, authenticatiediensten, machtigingsdiensten en ontsluitende diensten mogen deelnemen aan het stelsel, worden ze erkend (artikel 11 Wdo). Daarnaast moet het mogelijk zijn voor andere burgers en bedrijven uit de EU om digitale diensten af te nemen; hiertoe bestaat het eIDAS-knooppunt (zie figuur 1).

Opgemerkt wordt dat met betrekking tot elektronische dienstverlening aan burgers in het publieke domein private identificatiemiddelen kunnen worden toegelaten door verlening van een erkenning door de minister. Echter, de bijbehorende diensten worden niet erkend.[7] Dit in tegenstelling tot de bij bedrijfs- en organisatiemiddelen behorende diensten die wel door de minister worden erkend.

Natuurlijke personen kunnen binnen het stelsel verschillende rollen vervullen: zij kunnen namens zichzelf optreden of gemachtigd zijn om dat namens een andere natuurlijke persoon of rechtspersoon te doen. Om deze diverse vormen van machtigen binnen het stelsel mogelijk te maken, is een machtigingsvoorziening met voldoende functionaliteit nodig.

[5] Tezamen leveranciers van eID-diensten genoemd. Zie artikel 1 Wdo voor definities.
[6] In het eTD-stelsel herkenningsmakelaar genoemd.
[7] Dit houdt in dat aan een private middelenuitgever of private authenticatiedienst een erkenning ter zake van een door hem aangeboden respectievelijk gefaciliteerd privaat identificatiemiddel verleend kan worden, indien aan de bij of krachtens algemene maatregel van bestuur gestelde eisen met betrekking tot de werking, beveiliging en betrouwbaarheid van de partij en het middel wordt voldaan. Overigens biedt artikel 9, derde lid, van de Wdo wel de mogelijkheid om private ontsluitende diensten toe te laten voor verlening van een erkenning.

4. Het gewenste eID-stelsel

4.1 Kenmerken

Gelet op de urgentie om tot een geïntegreerd eID-stelsel te komen, moet het mogelijk zijn om binnen vier jaar een dergelijk stelsel toekomstbestendig te ontwikkelen. In hoofdstuk 5 wordt bij de strategische visie voor een integraal PvA eID-stelsel aangegeven hoe het gewenste eID-stelsel gefaseerd te bereiken is. In dit hoofdstuk komen de kenmerken van het gewenste eID-stelsel aan bod en de eisen die aan stelselpartijen en middelen gesteld dienen te worden.

In het gewenste geïntegreerde eID-stelsel staan de *actoren centraal*. Onder actoren worden verstaan natuurlijke en rechtspersonen. Binnen vier jaar zullen ook machines (opkomst van machine-to-machine koppelingen) steeds belangrijkere actoren worden. Actoren kunnen met hun middelen bij zowel publieke als private dienstverleners op een gebruiksvriendelijke manier inloggen op het gewenste betrouwbaarheidsniveau. De kern van een geïntegreerd eID-stelsel is vrij verkeer van publieke middelen in het private domein en private middelen in het publieke domein. Middelen worden gekenmerkt door een unieke identifier. Deze identifier kan vele vormen aannemen. Dit kan het BSN zijn; ook kan worden gedacht aan andere identifiers zoals andere unieke nummers of uniek identificerende fysieke, fysiologische of gedrag gerelateerde kenmerken van een persoon. Iedere gebruiker is in staat gebruik te maken van het stelsel. Dit betekent dat gebruik van het stelsel eenvoudig is en er geen drempels zijn om van het stelsel gebruik te maken (inclusie). Tevens hebben de gebruikers keuzevrijheid met betrekking tot de middelen. Naast private middelen kunnen gebruikers gebruik maken van een basaal middel waarmee bij eventueel falen van het stelsel gebruik kan worden gemaakt van vitale overheidsdiensten. De overheid communiceert op begrijpelijke wijze met de gebruikers over het eID-stelsel, waardoor zij onder meer een goed geïnformeerde keuze kunnen maken tussen middelen. Burgers en bedrijven hebben vertrouwen in de authenticatiemiddelen en de middelen zijn goed herkenbaar.

Om gebruikers in deze positie te brengen, dient een aantal essentiële *functionele keuzes* met betrekking tot de architectuur van het stelsel te worden gemaakt. De belangrijkste zijn de ontkoppeling van identiteit en attributen[8] en de ontkoppeling van authenticatie en machtigen. Dit is met name van belang om de vele lock-ins in het bestaande stelsel weg te nemen.

Op grond van de geraadpleegde experts en documentatie, zijn belangrijke kenmerken van het gewenste eID-stelsel (zie ook figuur 1):

Governance

- Heldere beschrijving, verdeling en vastlegging van taken, bevoegdheden en verantwoordelijkheden en voldoende checks & balances;
- In de governance zijn gebruikers, dienstverleners en leveranciers van eID-diensten representatief vertegenwoordigd;
- De minister van BZK is als stelselverantwoordelijke regisseur van het stelsel;
- De eisen aan het stelsel zijn technologieneutraal;
- Het geïntegreerde eID-stelsel is “open”: alle toegelaten middelen en erkende leveranciers van eID-diensten zijn deel van het stelsel.

[8] Een attribuut is een uniek kenmerk of gegeven van een natuurlijke of rechtspersoon.

Bekostiging

- Financiering van het stelsel is duidelijk;
- Middelen zijn ‘gratis’ voor burgers (via leges voor hun ID); bedrijven dragen zelf de kosten van hun middelen;
- Leveranciers van eID-diensten hebben een goede business case;
- Alle stelselpartijen kunnen (voor zover nodig) gebruik maken van centrale voorzieningen.

Veiligheid

- Gegevensbescherming burgers is gewaarborgd (AVG): ‘AVG-by-design’, dataminimalisatie, herstel van identiteitsfraude, uitoefening rechten betrokkenen;
- Middelen hebben een zeker vervangingsritme (weerstand tegen nieuwe vormen van cybercriminaliteit);
- Fraude- en misbruikdetectie, -bestrijding en herstel zijn adequaat en eenvoudig ingericht.

Dienstverleners

- Dienstverleners hebben het betrouwbaarheidsniveau van hun digitale dienstverlening bepaald;
- Dienstverleners accepteren elk (toegelaten) authenticatiemiddel op het juiste niveau of hoger;
- Dienstverleners worden ontzorgd.

Stelsel

- Eén onafhankelijke toezichthouder voor het geïntegreerde eID-stelsel;
- Toezicht & handhaving zijn onafhankelijk, uitvoerbaar en effectief;
- Beheer, incident- en calamiteitenafhandeling en support zijn adequaat en eenvoudig ingericht;
- Functionaliteit machtigingsvoorziening is voldoende.

Systeem & techniek

- Stelsel waarborgt continuïteit (geen ‘single points of failure’);
- Leveranciers van eID-diensten innoveren en werken steeds efficiënter;
- Gebruikte technieken binnen het stelsel zijn schaalbaar en voorkomen ‘lock in’ situaties.
- Het stelsel is gestandaardiseerd ten behoeve van veiligheid en interoperabiliteit.[9]

4.2 Eisen aan stelselpartijen en middelen

Om erkend te worden, dienen publieke én private leveranciers van eID-diensten en middelen aan diverse eisen te voldoen (zie figuur 2: Eisen aan potentiële marktpartijen + overheidsdiensten).

1. *Wettelijke* eisen:
   - Eisen uit de eIDAS- en uitvoeringsverordeningen;
   - Eisen uit de AVG;
   - Eisen uit de Wdo en onderliggende algemene maatregelen van bestuur en ministeriële regeling;
   - Eisen uit de Wet markt en overheid (deze hebben uitsluitend betrekking op publieke stelselpartijen).
2. Eisen met betrekking tot *keuzevrijheid*

[9] Dankzij (marktconforme, (inter-)nationale) standaarden weten stelseldeelnemers aan welke eisen zij bij en na erkenning dienen te voldoen (transparantie). Door het gebruik van standaarden wordt bijvoorbeeld de interoperabiliteit van het stelsel gewaarborgd. Bijkomend voordeel is dat (onafhankelijke) conformiteitsbeoordelende instanties aan de hand van schema’s kunnen controleren of de standaarden op een juiste wijze worden toegepast.

- Alle burgers en bedrijven hebben keuzevrijheid bij het kiezen van hun middelen en waar zij hun machtigingen vastleggen.

3. Eisen met betrekking tot *beschikbaarheid*
   - Alle burgers en bedrijven moeten gebruik kunnen maken van het stelsel.[10]
4. Eisen met betrekking tot *preventie*
   - Misbruik wordt zoveel mogelijk voorkomen.
5. Eisen met betrekking tot *herstelvermogen*
   - Ongewenste gevolgen van fouten in, fraude met en/of misbruik van persoonsgegevens kunnen ongedaan worden gemaakt;
6. Eisen met betrekking tot *het gebruik van standaarden*
   - Stelselpartijen werken conform (onderling afgesproken) standaarden.
7. Eisen met betrekking tot *financiële gezondheid*
   - De financiële gezondheid van leveranciers van eID-diensten is van belang voor de continuïteit van de dienstverlening.
8. Eisen met betrekking tot de *integriteit* van leveranciers van eID-diensten
   - Aangezien persoonsgegevens worden verwerkt is het van belang dat leveranciers van eID-diensten integer handelen.
9. Eisen met betrekking tot *gebruiksvriendelijkheid*
   - Gebruiksvriendelijkheid is een belangrijke factor voor succes. Keuze en aanschaf van middel en inloggen bij dienstverleners moet voor iedereen (inclusiviteit) begrijpelijk en eenvoudig zijn.[11] Daarnaast kunnen gebruikers onderscheid maken in bona- en malafide aanbieders van middelen.

[10] Hiermee wordt operationele beschikbaarheid bedoeld (het stelsel is altijd toegankelijk voor de gebruiker (burger/bedrijf). Het gaat hierbij nadrukkelijk niet om dekkingsgraad. Verwacht wordt dat de (private) deelnemers aan het stelsel gezamenlijk zorgen voor voldoende dekkingsgraad.
[11] Zie in dit verband bijvoorbeeld het Verdrag inzake de rechten van personen met een handicap.

5. Strategische visie voor een integraal PvA eID-stelsel

5.1 Inleiding

Gelet op de gevoelde urgentie om snel tot een geïntegreerd eID-stelsel te komen, moet het mogelijk zijn om binnen vier jaar een dergelijk stelsel te ontwikkelen. Om te komen tot een geïntegreerd eID-stelsel zal een programma moeten worden opgezet waarin dit stelsel wordt ontworpen en ontwikkeld. Binnen dit programma dient bijvoorbeeld de nieuwe governance-structuur te worden meegenomen, evenals het inrichten van een duurzaam financieringsmodel. Parallel kan dan binnen dit duurzame programma een traject worden ingericht met ‘quick wins’ die een snelle groei van de eID Markt mogelijk maken. De uitdaging is om deze groeifase zo kort mogelijk te houden en al op gang te brengen, terwijl het geïntegreerde stelsel parallel programmatisch wordt ontwikkeld. Daarnaast dient, zodra dat feitelijk kan, het hergebruik van middelen in andere domeinen (B2C, B2B, G2G) te worden geregeld. Tot die tijd dient dit te worden voorbereid om te komen tot gunstige businessmodellen voor een duurzaam financieringsmodel.

Om te komen tot een geïntegreerd eID-stelsel zullen in het op te zetten programma in ieder geval de volgende aspecten moeten worden opgepakt:

1. Governance;
2. Financierings- en bekostigingsmodel;
3. Bevorderen snelle groei eID-markt;
4. Ontkoppelen authenticatie en machtigen;
5. Gegevensbescherming;
6. Toezicht en handhaving;
7. Bestuurlijke continuïteit.

Per aspect wordt op hoofdlijnen aangegeven wat het te volgen groeipad is en de termijn waarbinnen dit pad kan worden gevolgd.

5.2 Governance

Voor succes en draagvlak is het noodzakelijk dat alle deelnemers, dat wil zeggen gebruikers, dienstverleners, leveranciers van eID-diensten, medewerking verlenen aan de ontwikkeling van het eID-stelsel. Hiervoor is essentieel dat vertrouwen wordt georganiseerd. Daarnaast zal de minister als stelselverantwoordelijke en regisseur bij de (door-)ontwikkeling van het stelsel zijn taak moeten kunnen vervullen. De minister is nog niet in positie gebracht om de rol van stelselverantwoordelijke waar te maken.

De binnen het programma te ontwerpen en te ontwikkelen nieuwe governance-structuur vergt dat de governance-structuur van het eTD-stelsel wordt aangepast zodra het eTD-stelsel opgaat in een geïntegreerd eID-stelsel. Tevens dient rekening te worden gehouden met de huidige governance in het publieke domein, zoals bij DigiD.

Onafhankelijkheid en representativiteit van stelselpartijen dienen gewaarborgd te zijn in de nieuwe governance. Voor een geïntegreerd eID-stelsel is een governance-model vereist waarin deelnemende partijen representatief zijn vertegenwoordigd, onafhankelijk van elkaar zijn en elkaar vertrouwen. Het model dient tevens te voorzien in checks & balances die voorkomen dat een deelnemende partij teveel zeggenschap heeft binnen het stelsel. Dit geldt ook voor de ontwikkelingsfase van het geïntegreerde stelsel waarin binnen een programma tot het ontwerp en de

inrichting van het stelsel moet worden gekomen. Geadviseerd wordt alle stelselpartijen die een rol (gaan) spelen in het geïntegreerde eID-stelsel op korte termijn te laten beginnen met het opstellen van een gemeenschappelijke agenda voor de wensen van gebruikers ten behoeve van de ontwikkeling van het eID-stelsel. Daarbij wordt aanbevolen de wensen van burgers continu te monitoren en de wensen van andere gebruikers in een gestructureerd overleg te bespreken. Bij de opzet van het programma zal de positie van het gestructureerde overleg moeten worden bepaald. Geadviseerd wordt dat de minister van BZK een voorzitter aanwijst die het gestructureerde overleg voorzit. Hiermee wordt hij daadwerkelijk als stelselverantwoordelijke in positie gebracht. Als stelselverantwoordelijke dient de minister de kaders te geven waarbinnen de standaarden worden ontwikkeld en dient hij aan te geven wat er binnen het stelsel noodzakelijkerwijs ontwikkeld dient te worden. Bovendien dient hij te gaan beschikken over de mogelijkheid om alvorens in te stemmen met een voorstel, hierover onafhankelijk advies te vragen. Zo nodig dient de minister als stelselverantwoordelijke een knoop door te kunnen hakken en doorzettingsmacht te krijgen als de deelnemende partijen er onderling niet uit komen. Geadviseerd wordt dat de door de minister benoemde voorzitter van het georganiseerd overleg een doorslaggevende stem heeft bij het staken der stemmen. Het voorgaande dient in een uitvoeringsregeling te worden uitgewerkt.

Aanbevolen wordt gelijk te beginnen met de voorbereidingen. Hiertoe dient het ministerie van BZK menskracht en (financiële) middelen te reserveren om dit zowel juridisch als praktisch mogelijk te maken. Dit geldt zowel voor het inrichten van het gestructureerde overleg als het opzetten en inrichten van een programma.

5.3 Financieringsmodel

Een tweede belangrijk resultaat van het te ontwerpen en in te richten programma is een duurzaam financieringsmodel. Geadviseerd wordt om de komende maanden binnen het gestructureerde overleg de opties voor een duurzaam financieringsmodel inhoud te geven, bijgestaan door (financiële en procesmatige) experts. Daarnaast wordt geadviseerd om in de ministeriële regeling behorende bij de Wdo, aandacht te besteden aan het bekostigingsmodel in relatie tot de bijbehorende governance.

Op dit moment is nog een relatief beperkt aantal leveranciers van eID-diensten actief binnen het eTD-stelsel. Dit zal veranderen door het systeem van open toelating van de Wdo als gevolg waarvan ook middelen en voorzieningen uit het publieke domein worden toegelaten (voor zover de Wet markt en overheid en de AVG dit toelaten). Voor het business model van de bestaande leveranciers biedt dit enerzijds een risico gelet op de gedane investeringen. Immers, meer stelselpartijen gaan deelnemen aan het speelveld. Anderzijds biedt het een kans dat het speelveld veel groter wordt door toevoeging van het burgerdomein. De uitdaging is om in dit complexe speelveld de juiste balans te vinden. Het bestaande eTD-stelsel biedt voor deze ontwikkeling een goede basis omdat dit stelsel al een mooi mechanisme biedt om vraag en aanbod bij elkaar te brengen en doorontwikkeling te kanaliseren, namelijk een gedetailleerde systematiek van releases voor standaarden.

Bij het ontwikkelen van een financieringsmodel is het voor de business case van belang om de eID-markt als geheel te benaderen en geen onderscheid te maken tussen het publieke en private domein. Voor het draagvlak is van belang dat het financieringsmodel door de stelselpartijen zelf binnen de governancestructuur en onder voorzitterschap van een door de minister benoemde voorzitter wordt vormgegeven. Zij worden bijgestaan door (financiële en procesmatige) experts. Aandachtpunten hierbij zijn in ieder geval het vervangingsritme van middelen en de beheersbaarheid van de stelselkosten. Gelet op de soms tegengestelde belangen van partijen zal het model nooit een ultieme oplossing bieden waarbij de belangen van alle stelseldeelnemers in gelijke mate gediend zijn. Dit betekent dat keuzes gemaakt moeten worden; in het uiterste geval door de stelselverantwoordelijke minister. De Wdo, AMvB's en in het bijzonder de ministeriële regeling spelen een belangrijke rol bij het creëren van een passend financieringsmodel.

Voor zover publieke middelen tot het geïntegreerde eID-stelsel worden toegelaten, dient rekening te worden gehouden met de Wet markt en overheid. Marktpartijen die zelf een privaat middel op de markt willen brengen mogen hierbij geen oneerlijke concurrentie ondervinden van de overheid.[12] De overheid kan private partijen bijvoorbeeld tegemoetkomen door een (kostbare) stap in het uitgifteproces van private middelen voor haar rekening te nemen door zekerheid te bieden over de identiteit van de gebruiker. In dit scenario komen de open-stelsel-gedachte en het idee dat identificatie een publieke taak is, bijeen.

De op te stellen ministeriele regeling behorende bij de Wdo is van cruciaal belang voor het bekostigingsmodel. Daarbij dient zoveel mogelijk helderheid te bestaan over de bekostiging van bij wie de kosten (investeringen en operationele kosten) neerslaan en bij wie de baten.

5.4 Bevorderen snelle groei eID-markt

Geadviseerd wordt om parallel aan het programma dat het eID stelsel ontwerpt en ontwikkelt een traject in te richten met ‘quick wins’ die een snelle groei van de eID Markt mogelijk maakt. De eID-markt zit weliswaar in een groeifase, maar is nog niet volwassen. De uitdaging is om deze groeifase zo kort mogelijk te houden en al op gang te brengen, terwijl het geïntegreerde stelsel parallel wordt ontwikkeld. De eID-markt is een tweezijdige markt, in die zin dat partijen aan beide zijden van de markt, dus bedrijven/burgers én (overheids-)dienstverleners, beiden in voldoende mate gebruik moeten maken van het stelsel om de markt volwassen te maken. Er zijn diverse mogelijkheden om een snelle groei te bevorderen. Voor een versnelling is het belangrijk om (programmatisch) toe te werken naar een eTD-stelsel voor het burgerdomein dat een brede toepassing kent voor identificatie op betrouwbaarheidsniveau substantieel. Met dit stelsel kunnen tegelijkertijd toepassingen op betrouwbaarheidsniveau hoog worden beproefd voor bepaalde doelgroepen en uitgerold. Voor de het eerstkomende jaar betekent dit onder meer:

- Ontwikkelen van een eTD-stelsel voor het burgerdomein, inclusief het systeem van open toelating, naast het huidige eTD-stelsel voor het bedrijvendomein. Daarbij dient ook de positie van DigiD te worden betrokken omdat dit door heel veel burgers wordt gebruikt. Mede door de huidige Corona-crisis is in het burgerdomein een versnelling noodzakelijk van de uitrol van de middelen substantieel, en specifiek voor de zorgsector (met name bij communicatie door zorgaanbieders met hun medisch beroepsgeheim) ook juist middelen op het niveau hoog.[13] Uiteindelijk worden alle burgers ooit eens patiënt en kan niveau hoog zich breed gaan verspreiden. Een impactanalyse moet worden uitgevoerd.
- Beproef, met de intentie om daarna daadwerkelijk tot implementatie over te gaan, toepassingen op de betrouwbaarheidsniveaus substantieel en hoog. Buiten de zorgsector kan dit in de meeste gevallen betrouwbaarheidsniveau substantieel zijn. Op korte termijn valt daar de snelste groei te verwachten. Binnen de zorgsector is in veel gevallen betrouwbaarheidsniveau hoog noodzakelijk vanwege het medisch beroepsgeheim, de AVG en eIDAS. Daarbij kan worden gedacht aan bestaande toepassingen met PKI;
- Versneld bepalen betrouwbaarheidsniveaus waarop digitale overheidsdiensten worden geleverd;
- Inzichtelijk maken van de kosten van middelen en eID-diensten;
- Burgers helpen bij het maken van een keuze tussen middelen.

[12] In dit verband wordt verwezen naar een aanbeveling van de commissie-Kuipers: “Voor het daadwerkelijk tot stand komen van private authenticatiemiddelen is het essentieel dat duidelijkheid gaat ontstaan rond de businessmodellen voor die middelen, en in het bijzonder welke doorbelasting naar de overheid zal gaan plaatsvinden. Die duidelijkheid is ook snel vereist, omdat de private partijen pas gaan investeren in de beschikbaarheid van hun middelen voor het BSN-domein nadat die duidelijkheid is ontstaan. De overheid moet snel bepalen langs welke lijnen zij die gewenste duidelijkheid kan gaan geven en in hoeverre daarbij sprake kan zijn van een onderlinge afstemming van partijen binnen het BSN-domein.”
[13] PBLQ/PrivacyCare, “Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg”, mei 2016.

Daarnaast dient zodra dat feitelijk kan het hergebruik van middelen in andere domeinen (B2C, B2B, G2G) te worden geregeld. Tot die tijd kan dit alvast worden voorbereid. Maatschappelijk gezien betreft dit een enorme kansrijke en relevante markt, die bij zal dragen aan gunstige businessmodellen om te komen tot een duurzaam financieringsmodel.

5.5 Gegevensbescherming

De AVG en het Besluit digitale overheid stellen kaders voor het verwerken van persoonsgegevens, waaronder het BSN. Hiervoor bestaat een wettelijke grondslag in artikel 16 Wdo. Daarnaast dienen er duidelijke, specifieke afspraken te worden gemaakt en maatregelen te worden getroffen om te voorkomen dat leveranciers van eID-diensten op grond van het feit dat een BSN wordt gebruikt, kunnen herleiden bij welke dienstverlener een burger heeft ingelogd. Uitgangspunt is ‘AVG-by-design’: een afweging tussen dataminimalisatie en herstelvermogen.

Voorzien wordt dat bij de ontwikkeling en uitgifte van middelen bijzondere categorieën van persoonsgegevens een toenemende rol zullen spelen. Biometrische gegevens met het oog op de unieke identificatie van een persoon kwalificeren zich als een bijzondere categorie van persoonsgegevens in de zin van artikel 9 van de AVG. Verwerking van deze gegevens is in beginsel verboden (artikel 9, eerste lid, AVG). De Nederlandse wetgever heeft met betrekking tot het verbod om deze bijzondere persoonsgegevens te verwerken een uitzondering gemaakt in artikel 29 van de UAVG. In dit artikel is bepaald dat het verbod om deze gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing is, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Deze noodzakelijkheid dient nog te worden aangetoond.

Bovendien dienen de rechten van betrokkenen, de transparantie en de verwerkingsverantwoordelijkheden van de deelnemers duidelijk te worden uitgewerkt en belegd om te voorkomen dat de gebruiker van het kastje naar de muur wordt gestuurd als er iets fout gaat in de lange authenticatieketen.

5.6 Ontkoppel authenticatie en machtigen

Gezien de grote diversiteit aan situaties waarin burgers en bedrijven zich willen of moeten laten vertegenwoordigen in de digitale interactie met dienstverleners, is een goed doordacht geïntegreerd stelsel van machtigen van groot belang. Deze moet een betrouwbaarheidsniveau bieden dat overeenkomt met het niveau dat vereist is bij zelf inloggen. De huidige machtigingsvoorziening beschikt hiervoor echter nog niet over de vereiste functionaliteit; die zal moeten worden ontwikkeld. Daarnaast zou machtigen losgekoppeld moeten worden van authenticatie. In het huidige eTD-stelsel zijn machtigingenregister en middel aan elkaar gekoppeld met een lock-in tot gevolg. Bovendien is het leveren van machtigingsdiensten in het burgerdomein nu voorbehouden aan de overheid. In een volledig geïntegreerd stelsel zou deze dienst ook door een private partij geleverd moeten kunnen worden. Geadviseerd wordt om authenticatie en machtigen in de tweede tranche van de Wdo te ontkoppelen. Dan kunnen machtigingsdiensten in het burgerdomein ook door een private partij geleverd worden. In de voorbereiding is vooral het onderzoeken en goed doordenken van een veilige, betrouwbare en interoperabele wijze van machtigen van belang. Daarnaast dient te worden gezorgd voor voldoende functionaliteit om te kunnen machtigen.

5.7 Toezicht en handhaving

Het Agentschap Telecom (AT) is als onafhankelijk toezichthouder aangewezen om toezicht te houden op de Wdo en zo nodig handhavend op te treden. Daarnaast hebben ook de Autoriteit Persoonsgegevens (AP) als toezichthouder op de AVG en de Autoriteit Consument en Markt (ACM) als markttoezichthouder toezichts- en handhavingstaken met betrekking tot het eID-stelsel. Het is van belang dat deze toezichthouders afspraken maken

over de wijze van behandeling van aangelegenheden waarbij de aan hen opgedragen taken of de uitoefening van de aan hen toegekende bevoegdheden elkaar raken of overlappen. Geadviseerd wordt om deze afspraken vast te leggen in een samenwerkingsprotocol.

5.8 Bestuurlijke continuïteit

Om de bestuurlijke continuïteit te verhogen dient het ministerie van BZK de regie te nemen om te komen tot een stabiel en geïntegreerd eID-stelsel. De bestuurlijke continuïteit kan juridisch beter worden geborgd door:

A. Randvoorden en aanvullende eisen aan erkende stelselpartijen te stellen in de ministeriële regeling, en
B. Onderwerpen die in de eerste tranche van de Wdo nog niet zijn geregeld, te regelen in de tweede en volgende tranches van deze wet of andere relevante wet- en regelgeving.

Bestuurlijke continuïteit is voor alle stelselpartijen van belang die toekomstbestendig voldoende zekerheid moeten hebben. Zoals aangegeven in paragraaf 2.5 over de voorgeschiedenis was in de afgelopen 20 jaar in het geheel geen sprake van bestuurlijke continuïteit. Als gevolg van eIDAS en de AVG als rechtstreeks bindende Europese Verordeningen en de uitwerking daarvan in de Wdo en nadere regelgeving is het noodzakelijk de bestuurlijke continuïteit ten aanzien van een geïntegreerd eID-stelsel te verhogen. De bestuurlijke continuïteit kan enerzijds worden verhoogd door bij de start van het programma de strategische uitgangspunten vast te stellen en anderzijds door dit juridisch te borgen. De Wdo en de bijbehorende uitvoeringsregelingen bieden hiervoor het anker.

De in procedure zijnde AMvB's bij de Wdo maken nog een onderscheid tussen het burger- en bedrijvendomein. In de nog dit jaar op te stellen ministeriële regeling zal één pakket van aanvullende maatregelen moeten worden geformuleerd voor het burger- en bedrijvendomein. Hierna volgen randvoorwaarden en eisen die aan erkende stelselpartijen gesteld zouden kunnen worden. Daarna volgen de onderwerpen die in de eerste tranche van de Wdo nog niet zijn geregeld en in de tweede tranche geregeld zullen moeten worden in het kader van bestuurlijke continuïteit en een heldere verdelen van taken en verantwoordelijkheden met in achtneming van gegevensbescherming, toezicht, handhaving en inrichting. De aanvullende regelingen kunnen worden ingevuld aan de hand van het op te zetten programma waarin dit stelsel wordt ontworpen en ontwikkeld aan de hand van onderhavig strategisch advies voor een geïntegreerd eID-stelsel.

Ad A) Randvoorwaarden in de ministeriële regeling

1) Governance-structuur aanpassen op een integraal eID-stelsel. Dat betekent een heldere beschrijving van taken, bevoegdheden en verantwoordelijkheden en voldoende checks & balances;
2) Waarborgen ten aanzien van onafhankelijkheid en representativiteit van gebruikers, dienstverleners en stelselpartijen in de governance;
3) Het financierings- en bekostigingsmodel. Daarbij dient helderheid te bestaan over de bekostiging van bij wie de kosten (investeringen en operationele kosten) neerslaan en bij wie de baten;
4) Nadere eisen ten aanzien van toezicht en handhaving.

Eisen in de ministeriële regeling

5) Eisen aan stelselpartijen op het gebied van financiële gezondheid en integriteit om continuïteit van dienstverlening en gegevensbescherming te waarborgen;
6) Eisen ten aanzien van gegevensbescherming, voor zover de AMvB's hierin nog niet voorzien. Zoals de eis dat middelen een zeker vervangingsritme hebben (weerstand tegen nieuwe vormen van cybercriminaliteit).

Ad B) Tweede tranche Wdo

De eerste tranche van de Wdo voorziet nog niet in het ontkoppelen van authenticatie en machtigen. Dat kan in de tweede tranche geregeld en nu voorbereid worden. Dan kunnen machtigingsdiensten in het burgerdomein ook door een private partij geleverd worden. Voordat dit op een veilige, betrouwbare en interoperabele wijze kan, dient dit verder goed doordacht te worden.

6. Aanbevelingen

6.1 Governance

Pas de huidige governance-structuur van het eTD-stelsel aan, zodra het eTD-stelsel opgaat in een geïntegreerd eID-stelsel. Hou daarbij ook rekening met de huidige governance in het publieke domein, zoals bij DigiD, Zet om te komen tot een geïntegreerd eID-stelsel een programma op waarin dit stelsel wordt ontworpen en ontwikkeld. Neem de nieuwe governance-structuur binnen dit programma mee. Waarborg daarbij onafhankelijkheid en representativiteit van stelselpartijen, Stel een gemeenschappelijke agenda op voor de wensen van burgers en bedrijven ten behoeve van de ontwikkeling van het eID-stelsel. Monitor continu de wensen van burgers en bespreek de wensen van bedrijven in een gestructureerd overleg, waarin ook nadrukkelijk aandacht wordt gevraagd voor de belangen van deze partijen in het private domein, te meer deze van groot belang zijn voor het financierings- en businessmodel van het eID-stelsel; Breng de minister in de positie om de rol van stelselverantwoordelijke van het te creëren geïntegreerde eID-stelsel echt waar te kunnen maken. Maak het mogelijk door hiervoor menskracht en (financiële) middelen te reserveren. Dit geldt zowel voor het inrichten van het gestructureerde overleg als het opzetten en inrichten van een programma.

6.2 Financieringsmodel

Zorg dat een duurzaam financieringsmodel deel uit maakt van het op te zetten programma waarin een geïntegreerd eID-stelsel wordt ontworpen en ontwikkeld. Laat binnen de nieuwe governance-structuur van dit programma de stelselpartijen een financieringsmodel inhoud geven onder voorzitterschap van een door de stelselverantwoordelijke aangestelde voorzitter, bijgestaan door (financiële en procesmatige) experts. Besteed in de ministeriële regeling behorende bij de Wdo, aandacht aan het bekostigingsmodel in relatie tot de bijbehorende governance.

6.3 Bevorderen snelle groei eID-markt

Richt als ministerie van BZK parallel aan het programma dat het eID stelsel ontwerpt en ontwikkelt een traject in met ‘quick wins’ dat een snelle groei van de eID Markt als volgt mogelijk maakt:

- Ontwikkel op programmatische wijze een eTD-stelsel voor het burgerdomein, inclusief andere toegelaten (binnenlandse en buitenlandse) partijen die aan de gestelde eisen voldoen, naast het huidige eTD-stelsel voor het bedrijvendomein;
- Beproef, met de intentie om daarna daadwerkelijk tot implementatie over te gaan, toepassingen op de betrouwbaarheidsniveaus substantieel en hoog. Buiten de zorgsector kan dit meestal niveau substantieel zijn. Binnen de zorgsector is in veel gevallen eIDAS betrouwbaarheidsniveau hoog noodzakelijk vanwege het medisch beroepsgeheim, de AVG en eIDAS. Daarbij kan bijvoorbeeld worden gedacht aan bestaande toepassingen met PKI. Gelet op de Corona-crisis is versnelling binnen met name het zorgdomein noodzakelijk;
- Bepaal versneld de betrouwbaarheidsniveaus waarop digitale overheidsdiensten worden geleverd;
- Maak de kosten van middelen en eID-diensten inzichtelijk;
- Help burgers bij het maken van een keuze tussen middelen.

Hou bij het bevorderen van een snelle groei van de eID-markt alvast rekening met een toekomstbestendige oplossing, zoals het in de tweede en derde fase te regelen hergebruik van middelen in andere domeinen (B2C, B2B, G2G). Maatschappelijk gezien betreft dit een enorme kansrijke en relevante markt.

6.4 Gegevensbescherming

Houd rekening met de verbodsbepaling in de AVG voor het verwerken van bijzondere categorieën van persoonsgegevens, tenzij daarvoor een in de wet genoemde grondslag voor bestaat. Dit kan bijvoorbeeld van belang zijn voor de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon. Bovendien dienen de rechten van betrokkenen, de transparantie en de verwerkingsverantwoordelijkheden van de deelnemers duidelijk te worden uitgewerkt en belegd om te voorkomen dat de gebruiker van het kastje naar de muur wordt gestuurd als er iets fout gaat in de lange authenticatieketen.

6.5 Machtigen

Bereid voor en regel dat in de tweede tranche van de Wdo authenticatie en machtigen worden ontkoppeld. Zorg voor voldoende functionaliteit om te kunnen machtigen. Voorkom door ontkoppeling van authenticatie en machtigen de huidige lock-ins. Doorbreek de huidige situatie dat machtigingsdiensten in het burgerdomein slechts zijn voorbehouden aan overheidspartijen. In de huidige eerste tranche van de Wdo is de ontkoppeling van authenticatie en machtigen nog niet geregeld. Regel de ontkoppeling daarom in de tweede tranche van de Wdo.

6.6 Toezicht en handhaving

Leg de afspraken tussen AT, ACM en AP over de wijze van behandeling van kwesties waarbij de aan hen opgedragen taken of de uitoefening van de aan hen toegekende bevoegdheden elkaar raken of overlappen vast in een samenwerkingsprotocol. De AT is als onafhankelijk toezichthouder aangewezen om toezicht te houden op de Wdo en zo nodig handhavend op te treden. Daarnaast hebben ook AP als toezichthouder op de AVG en andere gegevensbeschermingswetten en de ACM als markttoezichthouder toezichts- en handhavingstaken met betrekking tot het eID-stelsel. Het is van belang dat deze toezichthouders afspraken maken over de wijze van behandeling van aangelegenheden waarbij de aan hen opgedragen taken of de uitoefening van de aan hen toegekende bevoegdheden elkaar raken of overlappen

6.7 Bestuurlijke continuïteit

Verhoog de bestuurlijke continuïteit door als ministerie van BZK de regie te nemen om te komen tot een stabiel en geïntegreerd eID-stelsel. De bestuurlijke continuïteit kan enerzijds worden verhoogd door bij de start van het programma de strategische uitgangspunten vast te stellen en anderzijds door dit juridisch te borgen. De Wdo en de bijbehorende uitvoeringsregelingen bieden hiervoor het anker. Borg juridisch de bestuurlijke continuïteit door:

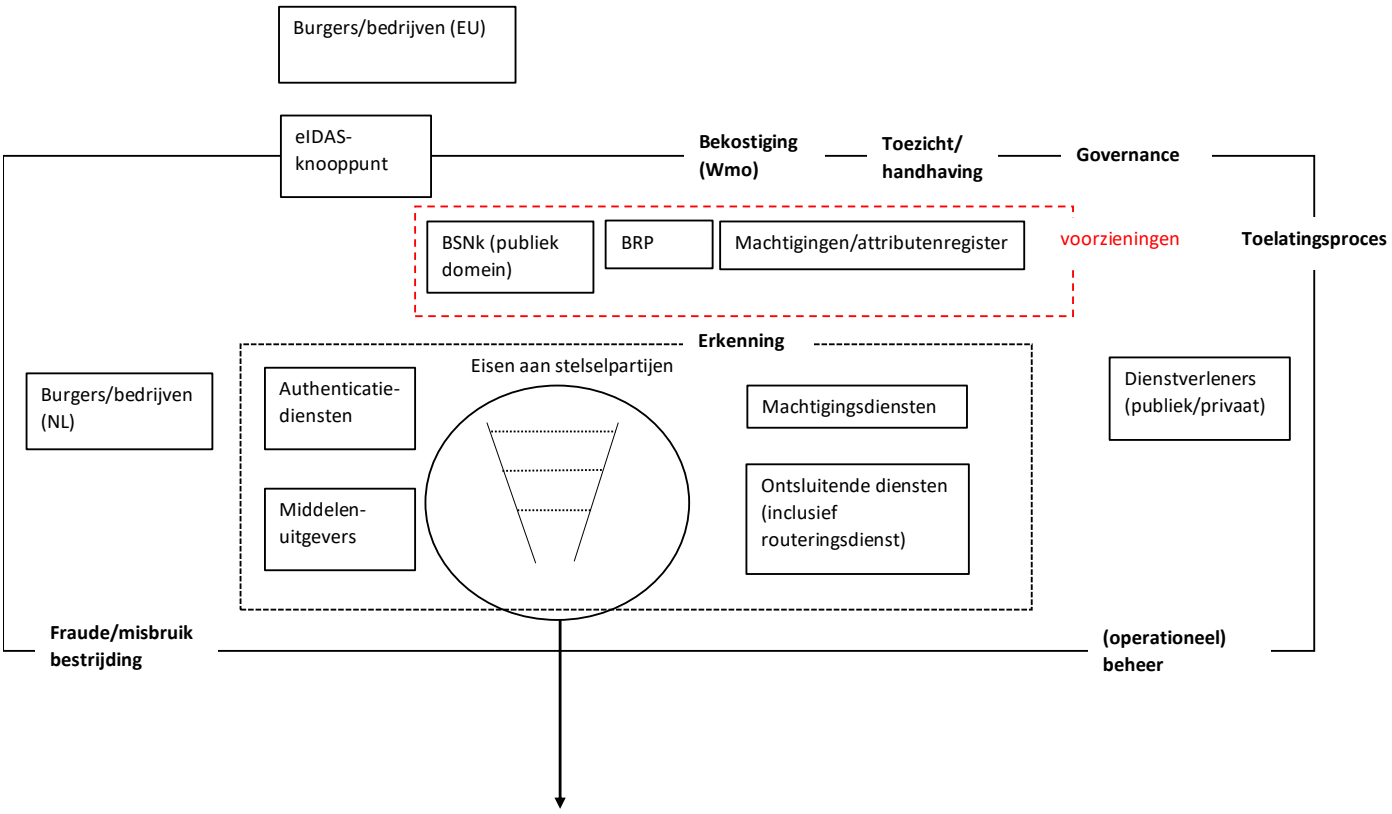
A. Aanvullende randvoorwaarden en eisen aan erkende stelselpartijen te stellen in de ministeriële regeling, en
B. Onderwerpen die in de eerste tranche van de Wdo nog niet zijn geregeld, te regelen in de tweede en volgende tranches van deze wet of andere relevante wet- en regelgeving.

BIJLAGE A: Geraadpleegde documentatie

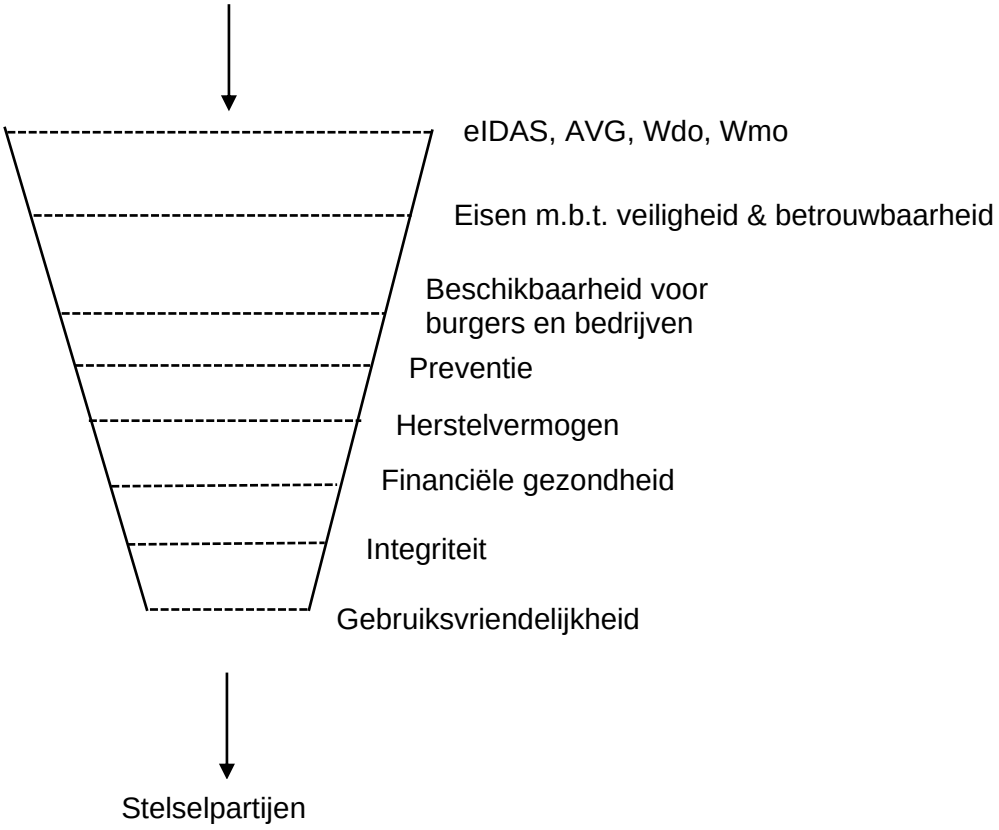
Nr.	
Rapporten	
1	Adviescommissie Authenticatie en Autorisatie Bedrijven (A3 Bedrijven), "*Eindadvies*", 11 november 2011.
2	Algemene Rekenkamer, "*Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel)*", 31 augustus 2016.
3	Bureau ICT-toetsing (BIT), "*Advies op het programma eID*", 12 mei 2016.
4	Commissie Kuipers, "*Advies van de commissie evaluatie pilots publieke en private authenticatiemiddelen*", 31 mei 2016.
5	Cyber Security Raad, "*Naar een veilig eID-stelsel. Advies inzake een veilig, universeel en open digitaal eID-stelsel voor een open, veilige en welvarende samenleving*", 7 november 2019.
6	Danish Agency for Digitisation, "*The future infrastructure for digital identities in Denmark*", september 2015.
7	Ecorys, "*Business Case Inloggen in het BSN-domein; De kosten en baten van het eID-stelsel*", 9 november 2016.
8	Forum Standaardisatie, "*Handreiking voor overheidsorganisaties voor het bepalen van het betrouwbaarheidsniveau voor digitale dienstverlening, versie 4.*", april 2017,
9	Gartner, "*Eindpresentatie benchmark eID*", 31 januari 2020.
10	M.H.A.F. Lokin, "*Wendbaar wetgeven, De wetgever als systeembeheerder*", 2018
11	Mazars, "Privacy Impact Assessment DigiD Substantieel", 6 september 2017
12	Ministerie van BZK, "*eID stelsel Nederland Strategische verkenning en voorstel voor vervolg*", oktober 2012.
13	Ministerie van BZK, "*Reactie naar aanleiding van BIT-advies*" (TK, 2015-2016, 26 643, nr. 414).
14	Ministerie van BZK (?), "*Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel*", 28 juni 2017.
15	Ministerie van BZK, "*Privacyvisie eID*", 10 december 2018.
16	Ministerie van BZK, "*Kamerbrief aanpak implementatie programma eID*", 29 januari 2019.
17	Ministerie van BZK, "*Programmaplan implementatie eID (concept v0.9c)*", 3 juni 2019.
18	Ministerie van BZK, "*Verslag marktconsultatie open toelating authenticatiediensten in burgerdomein*", 20 november 2019.
19	Ministerie van BZK, "*Plan van aanpak Project Open Toelating Authenticatie Diensten in het burgerdomein, versie 1.0*", 27 januari 2020.
20	Panteia, "*Gebruikerservaringen pilots publieke en private eID-middelen*", 27 mei 2016.
21	PBLQ/PrivacyCare, "*Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg*", mei 2016.
22	PBLQ, "*Whitepaper Naar een inlogstelsel voor de informatiesamenleving*", 2018
23	PBLQ, "*Analyse Governance afsprakenstelsels voor Programma Regie op Gegeven Eindrapport*", 3 maart 2019
24	Privacy Management Partners, "*Privacy Impact Assessment Startarchitectuur eIDAS*", 6 december 2016.
25	Programma Regie op Gegevens, "*Afsprakenstelsels in de praktijk, Leerervaringen van afsprakenstelsels om te komen tot een uniforme set van eisen voor persoonlijk datamanagement*", september 2018.
26	F. Roelofs, "*Analysis and comparison of identication and authentication systems under the eIDAS regulation*", 13 oktober 2019.

27	SEO Economisch Onderzoek, "*Rekenmodel eID-stelsel; Berekening van de verrekenprijs*", augustus 2015.
28	Stichting Privacy By Design, "*WDO verbeterpunten voor een goed-ID*", 28 januari 2020
29	Strategisch Beraad eTD-stelsel, "*Strategisch Meerjarenplan elektronische Toegangsdiensten 2019-2020*", 14 februari 2019.
30	Stuurgroep eID, "*MASTERPLAN eID*", 11 september 2014
31	TNO, "*Uitkomsten van een onderzoek naar de betrouwbaarheid en veiligheid van de pilots publieke en private middelen in het BSN domein*", 27 mei 2016
Geraadpleegde verordeningen, wetten en documentatie m.b.t. wetgevingsproces Wdo	
32	Wetsvoorstel Wet digitale overheid (TK, 2017-2018, 34 972, nr. 2).
33	Memorie van Toelichting wetsvoorstel Wet digitale overheid (TK, 2017-2018, 34 972, nr. 3).
34	Eerste nota van wijziging Wdo (TK, 2018–2019, 34 972, nr. 7).
35	Tweede nota van wijziging Wdo (TK, 2019–2020, 34 972, nr. 14).
36	Derde nota van wijziging Wdo (TK, 2019–2020, 34 972, nr. 18).
37	Advies Afdeling Advisering Raad van State en nader rapport (TK, 2017–2018, 34 972, nr. 4).
38	Advies Afdeling Advisering Raad van State en nader rapport (TK, 2017–2018, 34 972, nr. 15).
39	Ontwerpbesluit met Nota van Toelichting digitale overheid (17 maart 2020).
40	Ontwerpbesluit met Nota van Toelichting bedrijfs- en organisatiemiddelen Wdo (17 juni 2019).
41	Autoriteit Persoonsgegevens, "Advies conceptbesluit digitale overheid", 27 maart 2018.
42	VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (eIDAS-verordening).
43	UITVOERINGSVERORDENING (EU) 2015/1501 VAN DE COMMISSIE van 8 september 2015 betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.
44	UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

BIJLAGE B: Figuur 1 – Het gewenste eID stelsel



BIJLAGE C:
Figuur 2 – Eisen aan potentiële leveranciers van eID-diensten



BIJLAGE D: Wettelijk kader

Met de eIDAS-verordening is een Europees wettelijk kader gecreëerd voor veilige elektronische transacties binnen de EU tussen bedrijven, burgers en publieke autoriteiten. De verordening streeft ernaar om het vertrouwen in elektronische transacties in de gehele EU te vergroten en de effectiviteit van publieke en particuliere onlinediensten en elektronische handel te verhogen. De verordening is van toepassing op:

- Stelsels voor elektronische identificatie die door de EU-landen zijn aangemeld bij de Europese Commissie;
- Verleners van vertrouwensdiensten die in de EU zijn gevestigd.

De verordening neemt de bestaande belemmeringen voor het gebruik van elektronische identificatiemiddelen in de EU weg. Een elektronische identificatie die in een EU-land wordt toegekend, moet in alle andere EU-landen worden erkend. Dit is slechts van toepassing wanneer de elektronische identificatie aan de eisen van de verordening voldoet, is aangemeld bij de Commissie en is opgenomen in een lijst. Wederzijdse erkenning van elektronische identificatie is verplicht zijn vanaf het 28 september 2018 en maakt veilige elektronische transacties in de gehele EU makkelijker. Een stelsel voor elektronische identificatie moet één van de drie garantieniveaus vermelden (laag, substantieel en hoog) op grond van dat stelsel uitgegeven vormen van elektronische identificatie. Wederzijdse erkenning is alleen verplicht wanneer de relevante overheidsinstantie de niveaus substantieel of hoog gebruikt om toegang te krijgen tot de online diensten.
In de eIDAS uitvoeringsverordening 2015/1502 (betrouwbaarheidsniveaus) wordt, door het stellen van technische specificaties en procedures, bepaald op welke wijze de vereisten en criteria met betrekking tot betrouwbaarheidsniveaus van stelsels voor elektronische identificatie worden toegepast op elektronische identificatiemiddelen en authenticatiediensten.
De eIDAS uitvoeringsverordening 2015/1501 regelt een aantal aspecten om interoperabiliteit tussen lidstaten mogelijk te maken. Lidstaten worden geacht knooppunten in te richten om een eigen identificatielandschap te ontsluiten voor genotificeerde middelen uit andere lidstaten, en moeten zorgen dat hun eigen middelen in andere lidstaten gebruikt kunnen worden voor diensten waarvoor inloggen op betrouwbaarheidsniveau substantieel of hoog wordt vereist.
Door de AVG worden bestaande rechten van burgers van de Europese Unie (EU) versterkt en nieuwe rechten ingesteld waardoor deze meer controle over hun persoonsgegevens krijgen. Daarnaast schept de AVG diverse verplichtingen voor verwerkingsverantwoordelijkheden.
Met de Uitvoeringswet AVG (UAVG) wordt uitvoering gegeven aan de AVG. In dit verband is vooral van belang dat voor de verwerking van het BSN een wettelijke grondslag nodig is. Voor de verwerking van het BSN door private partijen betekent de regeling dat dient te worden voorzien in een specifieke wettelijke grondslag.
Het voorstel tot de Wet digitale overheid (Wdo) vormt een eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op de verschillende niveaus. Het wetsvoorstel bevat de meest urgente onderwerpen van regelgeving, te weten: de bevoegdheid om bepaalde standaarden te verplichten in het elektronisch verkeer van de overheid; het stellen van regels over informatieveiligheid; de verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI); de digitale toegang tot publieke dienstverlening voor burgers (natuurlijke personen) en bedrijven (rechtspersonen en ondernemingen).
In het ontwerp van het Besluit digitale overheid worden kaders gesteld kaders voor informatieveiligheid en persoonsgegevensverwerking.
Het ontwerp van het Besluit bedrijfs- en organisatiemiddelen Wdo vormt de nadere uitwerking van het stelsel van bedrijfs- en organisatiemiddelen op grond van de voorgenomen wet digitale overheid. Deze middelen worden gebruikt om ondernemingen en rechtspersonen toegang te verlenen tot elektronische overheidsdienstverlening. Het ontwerpbesluit stelt regels over de erkenning van private partijen die deze middelen leveren en daarbij betrokken

diensten aanbieden.
Wet markt en overheid bevat gedragsregels voor overheden die in concurrentie treden met private partijen. Deze gedragsregels (met betrekking tot het doorbereken van kosten, bevoordelingsverbod, gegevensgebruik en functiescheiding) zijn bedoeld om concurrentievervalsing te voorkomen.