Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

34 972 Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)

Nr. 10

NOTA NAAR AANLEIDING VAN HET NADER VERSLAG

Ontvangen 13 juni 2019

Inhoudsopgave

I ALGEMEEN

1. Inleiding

De leden van de VVD-fractie, de CDA-fractie, de D66-fractie en de GroenLinks-fractie hebben kennisgenomen van de nota naar aanleiding van het verslag bij het Wetsvoorstel digitale overheid. Zij hebben hierover diverse nadere vragen en opmerkingen. Ik bedank de fracties voor hun bijdrage en ga in deze nota graag in op de gestelde vragen. Bij de beantwoording is zoveel mogelijk de indeling en volgorde van het verslag aangehouden, met dien verstande dat vergelijkbare vragen zijn samengenomen.

De leden van de VVD-fractie vragen de regering in te gaan op de vraag hoe dit wetsvoorstel, los van de cyberveiligheid, bij kan dragen aan de economische ontwikkeling in Nederland, daarbij ook betrekkende hoe in

kst-34972-10
ISSN 0921 - 7371
's-Gravenhage 2019

de multi-middelenstrategie de overheid als grote klant innovatie bij niet-publieke middelen kan stimuleren.
Er zijn verschillende manieren waarop dit wetsvoorstel bijdraagt aan economische ontwikkeling. In de eerste plaats doordat met digitalisering administratieve lasten voor burgers en bedrijven worden verminderd. In de tweede plaats doordat het nationale eID-beleid onderdeel uitmaakt van de Europese ontwikkelingen om het concurrentievermogen van Europa te versterken door een beter werkende interne digitale markt te realiseren (o.a. EU-verordeningen eIDAS en Single Digital Gateway). In de derde plaats zal naar verwachting de komst en ontwikkeling van bedrijven op de eID markt, anders gezegd: aanbieders van private middelen, worden gestimuleerd en daarmee ook innovaties.
De VVD-fractie vraagt of nader beargumenteerd kan worden waarom er geen publiek inlogmiddel voor bedrijven komt en of dit op termijn uitgesloten wordt.
In het verleden is een publiek middel voor bedrijven ontwikkeld (DigiD bedrijven). Dit werd weinig gebruikt en is uitgefaseerd. Er is toen voor gekozen om gebruik te maken van kennis en voorzieningen die in het bedrijfsleven al aanwezig waren en – middels publiek-private samenwerking (pps) – aan te sluiten bij het sinds 2008 functionerende eHerkenning. Dit stelsel van private inlogmiddelen voor bedrijven heeft zich sinds die tijd bewezen. Momenteel zijn er ruim 400 dienstverleners aangesloten met 1300 diensten en zijn er bijna 300.000 inlogmiddelen verstrekt aan bedrijven. Hoewel ik voor de toekomst niets uitsluit, is er op dit moment geen reden om hiervan af te wijken en een publiek middel voor bedrijven in te voeren. Wel wordt dit stelsel met het wetsvoorstel publiekrechtelijk ingekaderd; deze middelen behoeven erkenning door de Minister van BZK op basis van vooraf gestelde veiligheids- en betrouwbaarheidseisen, alvorens ze door bedrijven kunnen worden gebruikt om overheidsdiensten af te nemen. Ook wordt terzake toezicht ingericht en gelden er bepalingen met betrekking tot privacybescherming en misbruikbestrijding. Het voorgaande laat onverlet dat de erkende middelen ook buiten het overheidsdomein (dus: bij de toegang tot commerciële dienstverlening) kunnen worden gebruikt.
De leden van de VVD-fractie en de CDA-fractie vragen om een nadere onderbouwing van het gestelde, dat publieke middelen niet gebruikt mogen worden in het private/commerciële domein, maar dat dit op termijn, op basis van bij consumenten gebleken behoeften, niet uitgesloten wordt. Op basis van welke criteria zou een publiek middel in de private sector met private aanbieders kunnen concurreren? Hoe wordt geborgd dat de multi-middelenstrategie niet verstoord wordt door oneerlijke concurrentie door het publieke middel? Op welke wijze wordt de behoefte van consumenten gemeten? En waarom kunnen private middelen niet universeel worden gebruikt bij de overheid?
Het meerjarige beleidsdoel, zoals eerder verwoord in brieven aan uw Kamer, is dat burgers in de toekomst voor één of meerdere elektronische identificatiemiddelen kunnen kiezen en daarmee overal (dus: zowel bij de overheid als bij bedrijven) veilig en betrouwbaar zaken kunnen doen. Primaire doel is dat burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de overheid; de beschikbaarheid van meerdere inlogmiddelen is een middel om dat doel te bereiken. Naar genoemd doel wordt beheerst en stapsgewijs toe gewerkt, met in achtneming van bestaande structuren, (ICT-)voorzieningen en dienstverlening (dus geen *big bang*). Voor nu betekent dit, dat het gebruik van publieke middelen wordt beperkt tot het publieke domein. Reden hiervoor is in de eerste plaats dat het huidige publieke middel DigiD, dat de basis vormt voor doorontwikkeling naar hogere betrouwbaarheidsniveaus, functioneert op basis van het BSN (een gevoelig persoonsgegeven) en, daaruit voortvloeiend, vanwege de aard van de betrokken dienstverlening, is bedoeld voor gebruik door de overheid.

Er zijn op dit moment veiligheids,- technische, juridische en organisatorische belemmeringen om dit anders in te richten. In de tweede plaats mag ingevolge de Wet markt en overheid geen sprake zijn van oneerlijk concurrentievoordeel. Een publiek middel, dat in feite wordt betaald door de belastingbetaler, mag niet gratis worden «hergebruikt» in het commerciële domein, d.w.z. concurreren met private middelen. Uitgangspunt van het kabinet is vooralsnog, dat het inloggen buiten het publieke domein zoveel mogelijk aan de markt moet worden overgelaten en de overheid hier momenteel geen rol heeft; het is van belang deze markt niet te verstoren en het groeipotentieel van marktpartijen niet te belemmeren. Dat dit nu niet aan de orde is, wil niet zeggen dat het gebruik van publieke middelen in het commerciële domein op voorhand wordt uitgesloten. Het op een hoger betrouwbaarheidsniveau brengen van het publieke middel heeft echter de komende jaren prioriteit. Bovendien biedt het wetsvoorstel de ruimte om private middelen, die worden gebruikt bij toegang tot de overheid, ook in te zetten in het commerciële domein. Op die manier wordt de digitale sleutelbos voor burgers verkleind en werkt door de overheid geborgde zekerheid door ten nutte van het commerciële domein. Daarnaast wordt gekeken naar de mogelijkheid van het gebruik van afgeleide middelen. In plaats van het ter beschikking stellen van een publiek middel neemt de overheid in dat geval een stap in het uitgifteproces van (private) middelen voor haar rekening door zekerheid over de identiteit van de gebruiker te bieden. De inlogmethode wordt dan technisch en organisatorisch van overheidswege gefaciliteerd, hetgeen mogelijk ook voordelen biedt op het punt van bekostiging. Voorts kan hierop in de toekomst worden voortgebouwd door private middelenaanbieders, zodat de overheid stimuleert dat generieke inlogmiddelen in het commerciële domein worden gerealiseerd. Op deze manier krijgt de burger de beschikking over meerdere methoden om in te loggen in beide domeinen, waarbij wetsaanpassing mogelijk niet nodig is. Ik onderzoek deze mogelijkheden thans in samenwerking met gemeenten, zoals ik u heb bericht bij brief van 14 mei jl. op het IRMA-manifest.

In hoeverre het bedrijfsleven en de burger – naast eventuele private middelen – behoefte heeft aan een breed inzetbaar publiek middel en bereid is hiervoor te betalen, is op dit moment onzeker en zal de komende jaren moeten blijken. Voor een beschouwing over de vraag naar het (universele) gebruik van private burgermiddelen bij de overheid verwijs ik naar paragraaf 3.
De leden van de VVD-fractie vragen aandacht voor de initiatiefnota over online identiteit en regie op persoonsgegevens van de leden Middendorp en Verhoeven, waarin een digitale kluis wordt voorgesteld (TK 34 993). De leden vragen zich af in hoeverre de regering mogelijkheden ziet om dat idee in het onderhavige wetsvoorstel te verankeren. De leden vragen hoe de regering aan kijkt tegen het gebruik van één bron voor (bepaalde) persoonsgegevens. Refererend aan de nota naar aanleiding van het verslag, waarin wordt verwezen naar extra benodigde informatie over de precieze intenties en de mogelijke realisatiewijze van de ideeën in de initiatiefnota, vragen de leden van wie die informatie moet komen en of het zoeken naar deze informatie onderdeel is van de uitvoering van de motie van de leden Koerhuis en Den Boer.
Conform de motie van de leden Koerhuis en Den Boer heeft het kabinet onderzoek gedaan naar online identiteit en regie op gegevens; uw Kamer zal hierover naar verwachting binnen enkele weken worden geïnformeerd. Ik acht het onwenselijk om op de uitkomsten vooruit te lopen door het idee van een digitale kluis in het onderhavige wetsvoorstel te verankeren. In algemene zin zij echter opgemerkt, zoals ook aangegeven in het nota-overleg van 26 november 2018, dat de basisregistraties reeds als zodanig fungeren en verplicht gebruik hiervan door de overheid reeds wettelijk verankerd is. Voorts is de bedoelde informatieverschaffing

inderdaad onderdeel van de uitvoering van de motie van de leden Koerhuis en Den Boer.
De leden van de VVD-fractie zien dat de regering verschillende middelen voor verschillende rollen dan wel doelgroepen wil houden. Is de regering het met de leden van de VVD-fractie eens dat dit onderscheid ertoe leidt dat (persoons)gegevens exclusief worden gekoppeld aan een elektronisch identificatiemiddel? Zo ja, wat voor invloed heeft die binding van (persoons)gegevens aan een middel op initiatieven die persoonsgegevens juist aan burgers willen koppelen, zoals digitale datakluizen, en elektronische identificatiemiddelen? Wat is de invloed van het erkennen van aparte middelen voor burgers, bedrijven en/of sectoren op het initiatief van de digitale datakluis?
Zoals hiervoor aangegeven, heeft het kabinet onderzoek gedaan naar online identiteit en regie op gegevens, op welke uitkomsten ik niet vooruit wil lopen. Ik kan dus nog niet concreet ingaan op de vraag. Op deze plaats volsta ik met erop te wijzen, dat de koppeling van (persoons)gegevens aan een elektronisch identificatiemiddel los staat van c.q. niet in de weg staat aan eventuele initiatieven op het punt van online identiteit in breder verband.
De leden van de CDA-fractie vragen om een nadere onderbouwing van het in de nota naar aanleiding van het verslag gestelde, dat het huidige stelsel van private middelen voor bedrijven naar tevredenheid functioneert. Wanneer is dit geëvalueerd en wie heeft de classificatie daarvan als goed vastgesteld; waren dat de bedrijven of de leveranciers van de middelen? De CDA-fractie vraagt in dit verband of een overzicht kan worden gegeven van de actuele stand van zaken van de bedrijfsmiddelen per authenticatieniveau en het gebruik.
De kwalificatie baseer ik op de manier waarop eHerkenning is ingericht en op de monitoring daarvan door beheerorganisatie Logius. eHerkenning is onderdeel van het ETD-stelsel, waarbinnen meerdere marktaanbieders met elkaar concurreren. De aanbieders staan onder toezicht van Agentschap Telecom, dat toetst of partijen aan de gestelde eisen per betrouwbaarheidsniveau voldoen, zoals op het gebied van beveiliging en privacybescherming. Ook is een Taskforce eHerkenning in het leven geroepen om verbeterpunten bij de implementatie van eHerkenning op te pakken. eHerkenning is aangemeld bij de Europese Commissie (notificatie). eHerkenning is bewust als netwerk ontworpen om zo de kans op verstoringen te minimaliseren. Op deze manier is er geen «single point of failure». Het feit dat private partijen de middelen uitgeven en met elkaar concurreren drukt de prijs per middel en is daarmee in het voordeel van de gebruiker. Voor twee van de leveranciers worden klantenervaringen verzameld door een extern bureau. De meeste aspecten scoren vier van de vijf sterren. Ik heb afspraken met de overige vier marktpartijen gemaakt om dit op korte termijn ook voor hen in beeld te brengen. Zie ook: https://www.eherkenning.nl/inloggen-met-eherkenning/leveranciers/leveranciersoverzicht/
De stand per eind 2018 is dat er 403 overheidsdienstverleners zijn aangesloten op eHerkenning. Er zijn 286.000 middelen uitgegeven en afgelopen jaar 5,5 miljoen logins gefaciliteerd. Op dit moment is ongeveer 90% van de middelen aan te merken als niveau laag (waarvan de helft met twee-factor authenticatie) en 10% als niveau substantieel. Het aandeel op niveau hoog bedraagt nog slechts 0,1%.
De leden van de CDA-fractie vragen of in de afweging, om een apart stelsel voor bedrijven in stand te houden, ook de toekomstige wijzigingen zijn meegewogen die het voorliggende wetsvoorstel met zich meebrengt voor bedrijven en organisaties, zoals bijvoorbeeld dat een groot aantal bedrijven meer middelen zal moeten aanvragen en dat een groot aantal bedrijven hoger gekwalificeerde middelen zal moeten aanvragen wanneer de acceptatieplicht wordt ingevoerd en huidige alternatieve voorzieningen worden beëindigd. Het CDA vraagt wat de te verwachten wijzigingen voor

bedrijven en organisaties zijn als gevolg van het wetsvoorstel en of de effecten en kosten daarvan juist en volledig zijn doorgerekend in de lastenparagraaf in de memorie van toelichting.
De kosten en effecten zoals opgenomen in de lastenparagraaf van de memorie van toelichting zijn juist. Er is gerekend met (gemiddeld) één aan te schaffen middel per bedrijf. Dit is gedaan omdat het in principe niet nodig is om meerdere middelen per bedrijf te kopen en 96% van het bedrijfsleven bestaat uit kleine bedrijven, waaronder ZZP'ers. Daarbij verwacht ik wel dat bepaalde grotere bedrijven meerdere middelen zullen willen aanschaffen om zaken met de overheid te kunnen doen omdat binnen deze bedrijven taken en bevoegdheden over meer mensen zijn verdeeld. Daartegenover staat echter weer een aanzienlijke groep bedrijven (groot en klein) die een intermediair heeft, waardoor het bedrijf zelf geen middel hoeft aan te schaffen. Een machtiging is dan voldoende. Er is verder uitgegaan van de prijs voor een middel op niveau substantieel. Zo is ook rekening gehouden met de bedrijven die een upgrade moeten kopen naar het niveau dat ingevolge deze wet is vereist.
De leden van de CDA-fractie hebben een aantal vragen over samenloop van elektronische identificatiemiddelen. Zij vragen zich in de eerste plaats af, of het creëren van de mogelijkheid van samenloop niet in strijd is met de uitgangspunten van de eIDAS-verordening, die juist aanstuurt op meer universeel gebruik van vertrouwde elektronische identificatiemiddelen, zowel binnen als tussen lidstaten.
De eIDAS-verordening maakt veilig en betrouwbaar inloggen bij de overheid door burgers en bedrijven mogelijk en voorziet hiertoe in beperkte harmonisatie. Lidstaten zijn ingevolge de verordening niet verplicht om een eigen stelsel van eID-middelen in te voeren, noch zijn ze verplicht dit te notificeren. Kern van de verordening is artikel 6, dat verplicht tot erkenning van genotificeerde middelen op de betrouwbaarheidsniveaus substantieel en hoog in het geval sprake is van grensoverschrijdende identificatie om toegang te krijgen tot een elektronische overheidsdienst, en de dienstverlener in kwestie het betrouwbaarheidsniveau substantieel of hoog voor de toegang tot die dienst gebruikt. Dit beginsel van wederzijdse erkenning, te hanteren bij grensoverschrijdende overheidsdienstverlening, is ook opgenomen in het wetsvoorstel. De eIDAS-verordening maakt geen onderscheid tussen een burger- en bedrijvendomein, maar staat hieraan ook niet in de weg; het binnen een lidstaat beperken van de gebruiksmogelijkheid, zoals voorshands in Nederland – en bijvoorbeeld ook in Duitsland en Italië – gebeurt, is toegestaan. Niettemin heb ik het voornemen beheerst en stapsgewijs toe te werken naar een meer geïntegreerd gebruik. Dit wetsvoorstel biedt hiertoe ruimte.
De leden van de CDA-fractie vragen zich voorts af, hoe willekeur voorkomen zal worden, bijvoorbeeld dat de Advocatenpas niet gebruikt mag worden om in te loggen bij de Belastingdienst en de UZI-pas wel.
In het door de CDA-fractie genoemde voorbeeld wordt gesproken van het gebruik van identificatiemiddelen voor professionals bij publieke dienstverlening. Het gaat hierbij om identificatiemiddelen die thans in min of meer gesloten (interne) systemen functioneren, zoals de Unieke Zorgverlener Identificatie (UZI) pas in het zorgdomein of de Advocatenpas binnen de rechtspleging. Dit betreft niet het inloggen voor (semi)publieke dienstverlening en valt in beginsel buiten de werkingssfeer van het wetsvoorstel. Echter, bij wijze van uitzondering kan, in samenspraak met de Minister die het mede aangaat, ingevolge artikel 8, derde lid, worden bepaald dat een door BZK toegelaten publiek identificatiemiddel kan worden gebruikt voor het verlenen van toegang tot gesloten/interne systemen. Een dergelijke regeling zou het gebruik van DigiD ter vervanging van de UZI-pas mogelijk kunnen maken, maar niet het gebruik van de UZI-pas of de Advocatenpas bij publieke dienstverlening van bijvoorbeeld de Belastingdienst. De toepassing van artikel 8, derde lid,

van het wetsvoorstel is, om redenen van zijn algemene verantwoordelijkheid voor de generieke digitale infrastructuur, waaronder voorzieningen voor elektronische identificatie door burgers en bedrijven, voorbehouden aan de Minister van BZK. De voorbereiding van afgewogen en samenhangende regels terzake zal geschieden in samenspraak met de Minister die het mede aangaat. Op deze wijze wordt willekeur voorkomen.
De CDA-fractie vraagt zich af welke samenlopen nu al zijn onderkend, naast de zzp'er en of daar reeds overleg over is gevoerd met de desbetreffende vakministers. De leden van de CDA-fractie denken aan het volgende voorbeeld: over hoeveel gereguleerde elektronische identificatiemiddelen moet een arts beschikken in het onlineverkeer met de publieke sector, als die arts bestuurder is van een praktijkmaatschap, tevens bestuurder is van het stichtingsbestuur van de beroepsgroep en ook patiënt is in dat ziekenhuis?
Met name met de zorgsector en het Ministerie van VWS wordt intensief overlegd over de reikwijdte en de gebruiksmogelijkheden van het eID-stelsel. Dit heeft erin geresulteerd, dat het wetsvoorstel – dat de toegang tot elektronische dienstverlening in het publieke domein betreft – zich mede richt tot zorgaanbieders, zorgverzekeraars en indicatieorganen. In beginsel kan het nodig zijn dat een arts over meerdere middelen beschikt: vooralsnog is de UZI-pas nodig om in te loggen binnen het gesloten (interne) zorgsysteem, een bedrijfs-en organisatiemiddel ten behoeve van beroepsmatig (extern) verkeer met de overheid en een publiek middel (DigiD op een hoger betrouwbaarheidsniveau) om als patiënt in te loggen. Ook hier geldt echter, dat wordt toegewerkt naar een meer geïntegreerd en universeel gebruik. Voorbeeld in dit verband is dat het wetsvoorstel de ruimte biedt om bij ministeriële regeling te bepalen dat een publiek identificatiemiddel tevens kan worden gebruikt in gesloten systemen zoals dat binnen en tussen zorginstellingen bestaat voor het onderling digitaal uitwisselen van patiëntgegevens (artikel 8, derde lid). De zorgmedewerker gebruikt in dat geval zijn publieke middel (niet dat van de patiënt) om in te loggen in het gesloten systeem. Wat betreft de interne bedrijfsvoering en uitwisseling van medische gegevens binnen het zorgdomein is het van belang dat gegevens aan de juiste persoon gekoppeld worden en dat alleen bevoegd zorgpersoneel de individuele medische gegevens kan verwerken. Zekerheid omtrent de identiteit van degenen die met die privacygevoelige gegevens omgaan is daarbij van groot belang. Het wetsvoorstel biedt voorts ruimte om natuurlijke personen in de uitoefening van hun beroep op bedrijf (zzp'ers) te faciliteren. Zie hetgeen hierover bij de volgende vraag wordt opgemerkt.
De leden van de CDA-fractie vragen in paragraaf 3 van dit verslag naar de samenloop van een burgermiddel om in te loggen bij de overheid en een bedrijfsmiddel om in te loggen bij de overheid en de betekenis daarvan voor zzp'ers. De leden van de CDA-fractie begrijpen dat het hanteren van beide middelen geen recht is, maar afhankelijk van de optie die de dienstverlener aanbiedt en vraagt terzake naar nadere onderbouwing. Het is dienstverleners toegestaan beide inlogmethoden door zzp'ers te laten gebruiken. Of dienstverleners dit daadwerkelijk doen is afhankelijk van de inrichting van hun interne systeem. Als zij bedrijven alleen herkennen aan de hand van het KvK- of RSIN-nummer, kan een publiek middel (op basis van het BSN) geweigerd worden. Indien blijkt dat in de praktijk bij zzp'ers behoefte bestaat aan keuzevrijheid en dit voor overheden technisch en financieel uitvoerbaar is, dan is het mogelijk gebruik te maken van de bevoegdheid in artikel 7, vijfde lid, van het wetsvoorstel om bij ministeriële regeling dienstverleners tot het aanbieden van beide inlogmethoden te verplichten. Voor de zzp'er bestaat dan ook de mogelijkheid met zijn publieke middel in te loggen.
De leden van de CDA-fractie lezen in de nota naar aanleiding van het verslag, dat het sinds het van kracht worden van de eIDAS-verordening voor Duitsers mogelijk is om met hun eID-middel bij Nederlandse

dienstverleners in te loggen, dienstverleners hard werken aan het gereed maken van hun eigen dienstverlening hiervoor en dat een gestage groei in het aantal inlogpogingen daar blijk van geeft. De leden vragen in dat verband of ze het goed begrijpen, dat Duitsers in de praktijk niet met hun eID-middel kunnen inloggen bij Nederlandse dienstverleners, omdat er tot nu toe alleen sprake is van «inlogpogingen».
Burgers uit andere EU-lidstaten kunnen met genotificeerde middelen wel degelijk inloggen en diensten afnemen bij steeds meer Nederlandse dienstverleners. Het Duitse (burger)middel is genotificeerd en bruikbaar in Nederland bij onder meer de SVB, het Omgevingsloket en het digitaal loket van de Afdeling bestuursrechtspraak van de Raad van State.
De leden van de CDA-fractie constateren, dat de huidige oplossingen voor DigiD substantieel thans niet de totale gewenste doelgroep bereiken. Dit hangt samen met het feit dat een aanzienlijk deel van de doelgroep niet beschikt over een smartphone met een Android besturingssysteem met NFC-lezer. De leden vragen of kan worden aangeven hoeveel van de ruim 13,5 miljoen actieve DigiD-gebruikers beschikken over een smartphone met een Android besturingssysteem met NFC-lezer.
Uit onderzoek is gebleken dat ongeveer de helft van het aantal DigiD-gebruikers beschikt over een smartphone met een geschikt Android besturingssysteem met NFC-lezer.
De regering stelt, dat zij op korte termijn een aanbesteding start voor een privaat middel op niveau substantieel, om een groot deel van de doelgroep snel een alternatief identificatiemiddel op niveau substantieel te kunnen bieden. De leden van de CDA-fractie vragen, waarom de regering niet heeft gekozen voor een systeem van accreditatie, juist met het oog op bereik en snelheid.
Bij de beantwoording van de vragen in paragraaf 3 zal ik ingaan op de verwerving van een alternatief privaat middel. Op deze plek volsta ik met een algemene toelichting op het instrument accreditatie. Hierbij gaat het om conformiteitsbeoordeling: het proces waarin wordt aangetoond of voldaan is aan de vooraf vastgestelde eisen voor een product of dienst, uitmondend in een certificaat van conformiteit. Het betreft een privaat (zelfregulerings)instrument, dat wil zeggen ontwikkeld buiten de overheid. Niettemin wordt het in bepaalde gevallen ook ingezet door de overheid, te weten bij wijze van hulpmiddel bij vergunningverlening, toelating of erkenning. Conformiteitsvermoeden en vergunningverlening zijn dus verschillende zaken. Gelet op de betrokken publieke belangen en verantwoordelijkheden is besluitvorming (eindoordeel) voorbehouden aan het bevoegd gezag; ook kan conformiteitsbeoordeling overheidstoezicht niet vervangen. Het kabinetsstandpunt inzake accreditatie en het gebruik ervan in het overheidsbeleid bevat de geldende kaders (Kamerstukken 2015–2016, 29 304, nr 6). Van belang is te benadrukken, dat het toepassen van accreditatie op zichzelf niets zegt over het bereik van middelen en snelle beschikbaarheid ervan. Zowel in een aanbestedingsprocedure als bij andere manieren van verwerving gelden de eIDAS-eisen en kan er voor gekozen worden om conformiteit met die eisen te laten aantonen via accreditatie (zie voorts paragraaf 3.2).
De leden van de D66-fractie lezen in de nota naar aanleiding van het verslag dat dit wetsvoorstel een eerste tranche is van meerdere voorstellen rondom de digitale overheid en vragen toe te lichten welke tranches nog volgen en wat de inhoud van deze wetsvoorstellen zal zijn. Dit wetsvoorstel geeft richting aan wat voor realisering van de digitale overheid op dit moment het meest nodig is: voorzieningen en eisen voor veilige en betrouwbare overheidsdienstverlening. De wet biedt een zekere mate van toekomstbestendigheid, maakt innovatie mogelijk en kan inspelen op ontwikkelingen, in het bijzonder binnen het kader van eID. Voor zover ontwikkelingen de reikwijdte van het huidige wetsvoorstel te buiten gaan of omdat herijking van gemaakte keuzes nodig is, liggen vervolgtranches in de rede. Er kan nog niet goed worden aangegeven

hoeveel tranches van de wet zullen volgen en wat deze precies zullen regelen. Dit hangt af van de aard van de ontwikkelingen, alsmede van nut en noodzaak van verankering in formele wetgeving. Wel is duidelijk dat voor de tweede tranche primair wordt gedacht aan functionaliteiten rondom de verbetering van de persoonlijke informatiepositie van burgers, zoals ook aangegeven in NL Digibeter: persoonlijk datamanagement, waaronder inzage in eigen gegevens in overheidsregistraties en verstrekkingen, correctie, bepalen aan wie gegevens worden verstrekt, voorkomen van onnodig uitvragen in ketens van dienstverlening (*once only*). Ook tweezijdigheid van de berichtenbox, integratie van MijnOverheid voor burgers & voor bedrijven en realisering van een berichtenoverzicht zullen naar verwachting een plek krijgen in en op basis van de tweede tranche. Over deze onderwerpen vindt de gedachtenvorming momenteel plaats, op basis van nadere analyses, gesprekken met medeoverheden en uitvoeringsorganisaties en overleg over de samenhang met andere, bestaande regelgeving.

2. Standaarden

De leden van de D66-fractie lezen in de nota naar aanleiding van het verslag dat het open standaardenbeleid overheidsorganisaties de vrijheid geeft om hun eigen afweging te maken over het al dan niet gebruiken van een standaard die is opgenomen op de «pas toe of leg uit» lijst. Zij vragen op welke wijze artikel 3 deze vrijblijvendheid verandert en of de regering de intentie heeft deze vrijblijvendheid te veranderen. De leden vragen ook of er snel zal worden toegewerkt naar volledige open standaarden middels te de introduceren wettelijke basis.

Het beleid inzake open standaarden biedt overheidsorganisaties de mogelijkheid zelf het investeringsmoment te bepalen waarbij zij de open standaarden van de «pas toe of leg uit lijst» toepassen. Helemaal niet toepassen kan, bij investeringen van meer dan € 50.000, slechts in geval van zwaarwegende redenen. Die redenen moeten bovendien worden opgenomen in het jaarverslag van de organisatie. In de praktijk is gebleken dat in sommige gevallen die vrijheid en het drempelbedrag niet aansluiten bij de urgentie om bepaalde standaarden toe te passen of bij de noodzaak om als gehele overheid dezelfde standaarden toe te passen op hetzelfde moment. Informatieveiligheidstandaarden zijn hiervan een goed voorbeeld. Artikel 3 van het wetsvoorstel biedt de grondslag om bij algemene maatregel van bestuur een verplicht toe te passen open standaard aan te wijzen. In dat geval kunnen organisaties niet meer van toepassing afwijken en vervalt de ruimte om zelf een moment te kiezen om als organisatie te standaard te gaan gebruiken. Het «pas toe of leg uit»-principe blijft echter voor bepaalde open standaarden het meest proportionele instrument, omdat dit dienstverleners de gelegenheid geeft om zelf het investeringsmoment te bepalen waarbij zij de standaarden toepassen; dit helpt om desinvesteringen bij de verschillende organisaties te voorkomen. De intentie is open standaarden niet per definitie verplicht te stellen, maar alleen wanneer dat noodzakelijk en proportioneel is voor de werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid of de doelmatigheid van het elektronische verkeer met of tussen bestuursorganen of indien dit voortvloeit uit internationale verplichtingen. Dit wordt per geval bezien.

De leden van de D66-fractie lezen dat na verplichtstelling van een open standaard door middel van een amvb, toezicht op de naleving plaatsvindt binnen de eigen beleidskolom door toezichthoudende ambtenaren. De leden vragen of toegelicht kan worden of hier sprake is van een slager die eigen vlees keurt en op welke wijze de Minister van Binnenlandse Zaken

het overzicht houdt op naleving van de open standaard die middels amvb verplicht is gesteld.

Het toezicht op de naleving vindt plaats binnen de eigen beleidskolom. Dit is niet problematisch, mede gelet op het feit dat in aanvulling daarop monitoring van de naleving plaatsvindt door het Forum Standaardisatie. Het Forum adviseert aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Ministers van Economische Zaken en Klimaat en Justitie en Veiligheid, al dan niet via het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). Deze monitor wordt jaarlijks behandeld in het OBDO en toegezonden aan uw Kamer. Door de adoptie van ook wettelijk verplichte standaarden te laten meelopen in een jaarlijkse monitor wordt transparant welke specifieke organisaties niet voldoen. Daarnaast zal ik per verplichtstelling op grond van artikel 3, van een standaard of groep van standaarden, in de nota van toelichting bij de betreffende AmvB aandacht besteden aan de vraag of aanvullende monitoring en/of toezichtsmaatregelen noodzakelijk zijn. Voorshands zie ik geen meerwaarde in het organiseren van een overkoepelend separaat toezicht op de naleving van wettelijk verplichte standaarden, omdat het bereik van elke algemene maatregel van bestuur waarmee standaarden verplicht worden gesteld anders kan zijn. Een standaard verplichten is immers pas aan de orde als dit noodzakelijk en proportioneel is voor de werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid of de doelmatigheid van het elektronische verkeer met of tussen bestuursorganen of indien dit voortvloeit uit internationale verplichtingen.

De leden van de D66-fractie lezen dat op 1 juli 2018 de Europese toegankelijkheidsnorm EN301549 verplicht is geworden. Op deze manier moeten overheidsinstanties de noodzakelijke maatregelen treffen om hun websites en mobiele applicaties toegankelijker te maken. Dit wordt door de Minister van Binnenlandse Zaken gemonitord. De leden vragen of toegelicht kan worden wat de uitkomst is van deze monitor is en of alle websites en mobiele applicaties van de overheid aan deze standaard voldoen.

Het Tijdelijk besluit digitale toegankelijkheid, waarin wordt gerefereerd aan EN 301 549, is op 1 juli 2018 in werking getreden. Het besluit wordt gefaseerd van toepassing: op 23 september 2019 voor websites die vanaf 23 september 2018 zijn gepubliceerd, op 23 september 2020 voor websites die vóór 23 september 2018 zijn gepubliceerd en op 23 juni 2021 voor mobiele applicaties. Over de naleving van het besluit en de mate waarin websites en mobiele applicaties van overheidsinstanties voldoen aan de standaard dient uiterlijk op 23 december 2021 voor de eerste keer te worden gerapporteerd aan de Europese Commissie en daarna elke drie jaar, zo is bepaald in de Europese webtoegankelijkheidsrichtlijn 2016/2102. Vooruitlopend daarop wordt een nulmeting uitgevoerd naar de toegankelijkheid van websites van overheidsinstanties, op basis van de in oktober 2018 door de Europese Commissie vastgestelde toezichtsmethodiek. De resultaten van deze nulmeting zullen in de tweede helft van 2019 worden gedeeld met uw Kamer.

De leden van de GroenLinks-fractie ontvangen graag een nadere toelichting op het voornemen om de open standaard HTTPS te verplichten. Ook vragen ze wanneer de verplichting van open documentstandaarden wordt ingesteld, waar één van de grootste afhankelijkheden van leveranciers bestaat, met alle door meerdere instanties en onderzoek en genoemde nadelen en risico's op gebied van kosten, informatieveiligheid, archivering, rechtszekerheid, leveranciersafhankelijkheid.

De verplichting HTTPS toe te passen – deze zal in een amvb op basis van het wetsvoorstel worden opgenomen – is het sluitstuk van gevoerd beleid. Voor HTTPS geldt sinds 2017 de zogenaamde «pas toe of leg uit»-regel. Aanvullend is bestuurlijk een streefbeeldafspraak gemaakt om de standaard voor het einde van 2018 bij alle overheidswebsites toegepast te hebben. Hoewel het gebruik de afgelopen jaren fors is toegenomen, is het streven van 100% toepassing niet gehaald. De voorgenomen wettelijke verplichting dwingt partijen, die de standaard nog niet toepassen, dit alsnog te doen. Voor documentstandaarden geldt al dat overheidsorganisaties de open standaard kunnen toepassen naast de gesloten variant, maar dit gebeurt momenteel onvoldoende. Daarom zet ik in op een vergelijkbare aanpak, met verplichting als sluitstuk. Het Forum Standaardisatie zal dit jaar een streefbeeldafspraak voorbereiden over open documentstandaarden waarvoor momenteel het «pas toe of leg uit» regime geldt. Als blijkt dat dit onvoldoende effect heeft, wordt verplichte toepassing overwogen.

3. Elektronische identificatie (eID)

De leden van de VVD-fractie en de CDA-fractie hebben vragen gesteld die zich concentreren rond de thema's accreditatie en verwerving van een privaat burgermiddel. De vragen, die mede lijken ingegeven door de wens tot zoveel mogelijk universeel gebruik bij de overheid, zoveel mogelijk (en gelijke) kansen voor aanbieders van private middelen en gelijkwaardigheid van publieke en private (burger)middelen, worden hieronder themagewijs behandeld. Voorafgaand daaraan ga ik, bij wijze van inleiding, kort in op de beleidsmatige uitgangspunten.

1. Inloggen bij de overheid

Dit wetsvoorstel regelt hetgeen nodig is om burgers en bedrijven veilig en betrouwbaar bij de (semi) overheid te kunnen laten inloggen. Om dit doel te bereiken is het wenselijk dat voor burgers, naast de beschikbaarheid van publieke middelen op verschillende betrouwbaarheidsniveaus, één of meerdere private alternatieven met een hoge dekkingsgraad beschikbaar komen. Het beschikbaar komen van meerdere middelen noch het creëren van een markt zijn doelen op zich, maar zijn ondersteunend aan het primaire beleidsdoel: veilig en betrouwbaar inloggen. Belangrijk daarbij is dat de burger gebruiksvriendelijk kan beschikken over meerdere inlogmethoden. In dit verband wordt voor bedrijven volstaan met private middelen; in de praktijk bestaat een over het algemeen naar tevredenheid werkend en dekkend stelsel, dat gecontinueerd wordt. Digitale transacties in de commerciële sector vallen buiten de werkingssfeer van dit wetvoorstel.
Het wetsvoorstel sluit aan bij de feitelijke situatie en bestaande digitale voorzieningen, waarbij ruimte wordt gelaten voor doorontwikkeling, innovatie en harmonisatie. Ik ga hierbij beheerst en stapsgewijs te werk, met oog voor risico's, gebleken behoeften en marktwerking. Uiteindelijke doel is dat burgers en bedrijven veilig, betrouwbaar en eenvoudig transacties kunnen verrichten in de hele digitale wereld. De route daarnaartoe is een meerjarig traject, dat blijvend zal moeten anticiperen op (innovatieve) ontwikkelingen. Zo bestaat de mogelijkheid dat in de toekomst inloggen mogelijk zal zijn zonder gebruikmaking van fysieke kaarten. Belangrijk is dat de te nemen stappen moeten passen binnen het langere termijnbeeld, zoals verwoord in de beleidsvisie over overheidsdienstverlening NL DIGIbeter en de recente eID voortgangsrapportage, die aan uw Kamer zijn gezonden.
Dit wetsvoorstel vormt de eerste stap en heeft het veilig, betrouwbaar en gebruiksvriendelijk inloggen bij de overheid tot doel. Hierbij heeft het voor burgers breed beschikbaar komen van – publieke en private – inlogmid-

delen op hogere betrouwbaarheidsniveaus de hoogste prioriteit. In dit verband wordt sinds mei 2018 geleidelijk een publiek middel op betrouwbaarheidsniveau hoog geïntroduceerd via de uitgifte van rijbewijzen met een (na vaststelling van dit wetsvoorstel te activeren) e-functionaliteit. In reactie op de vragen van de CDA-fractie naar het tijdstip van geschiktheid van alle rijbewijzen voor DigiD hoog, alsmede naar welk deel van de totale gewenste doelgroep daarmee wordt bereikt merk ik op, dat rijbewijzen worden uitgegeven via de natuurlijke cyclus van 10 jaar, waardoor invoering van voor eID geschikte rijbewijzen naar verwachting een aantal jaren in beslag zal nemen. Hiermee kan uiteindelijk een groot deel van de Nederlandse bevolking worden bereikt, maar voor volledige dekking zal inzet van meerdere methoden nodig zijn. Tevens worden voorbereidingen getroffen voor het beschikbaar komen van DigiD hoog op de Nederlandse identiteitskaart. Hiertoe is bij uw Kamer het voorstel tot wijziging van de Paspoortwet (Kamerstukken 2018/2019, 35 047 (R2108) ingediend.

2. Accreditatie; betekenis en functie

Door beide fracties worden vragen gesteld over de aard en functie van accreditatie, in het bijzonder waarom het wetsvoorstel hierin alleen bij het bedrijfs- en organisatiemiddel voorziet en nut en noodzaak om accreditatie ook bij het burgermiddel te gaan hanteren. Ter verduidelijking ga ik in op het instrument accreditatie en de rol die dit bij overheidsbeleid kan spelen.

Accreditatie is het door een onafhankelijke, deskundige (geaccrediteerde private) instantie uitgevoerde, proces waarin wordt aangetoond of voldaan is aan vooraf vastgestelde (kwaliteits)eisen voor een product of dienst. Het wordt ook wel aangeduid als conformiteitsbeoordeling. Accreditatie kan door de overheid bijvoorbeeld worden ingezet in het kader van aanbesteding, inkoop, beoordeling van een aanvraag voor het nemen van een besluit of bij wijze van toezichtsondersteuning. Accreditatie en aanbesteding sluiten elkaar dus niet uit. Wanneer publieke belangen in het geding zijn en sprake is van regelgeving en wettelijke eisen waaraan moet worden voldaan, fungeert (verplicht voorgeschreven) conformiteitsbeoordeling als hulpmiddel voor het bevoegde gezag bij het verlenen of weigeren van een vergunning/toelating/erkenning. De eisen waarop wordt getoetst, zijn dan voordien door de overheid gesteld in wet- of regelgeving. De overlegging van een certificaat van conformiteit levert een vermoeden op dat de betrokken partij voldoet aan de gestelde eisen.

Deze systematiek is in het wetsvoorstel opgenomen terzake van het bedrijfs- en organisatiemiddel (artikel 11). Hierbij is sprake van een «open» stelsel, dat wil zeggen voor alle partijen toegankelijk; als een private aanbieder van een bedrijfs- en organisatiemiddel kan aantonen dat hij aan de (op de Europese eIDAS-verordening gebaseerde) veiligheids- en betrouwbaarheidseisen voldoet, wordt hij in beginsel door de Minister van BZK erkend. Erkenning van het bedrijvenmiddel komt dus niet alleen door accreditatie tot stand, oftewel een certificaat *sec* creëert geen recht en is geen synoniem voor toelating. Voor de verkrijging van een erkenning is een besluit van het bevoegd gezag nodig, te weten een beschikking waarbij wordt vastgesteld dat aan bepaalde eisen wordt voldaan.

Door een «open stelsel» wordt ruimte aan de markt gelaten, is er sprake van concurrentie en is er ruimte innovatieve middelen toe te laten, vooral indien de eisen doelgericht geformuleerd zijn. Nadeel is dat er bij een erkenning geen leveringsverplichting is – duidelijk is slechts *dat* aan de eisen wordt voldaan –, waardoor in theorie de kans bestaat dat er geen middelen beschikbaar zijn. In reactie op het door de leden van de

CDA-fractie gestelde is het, mede gezien de ervaringen op dit terrein (zie ook paragraaf 1), niet de verwachting dat private leveranciers van bedrijfsmiddelen investeren in accreditatie en het doorlopen van een erkenningsprocedure om vervolgens niet te leveren. Bij private burgermiddelen is dit nog onzeker, reden waarom in het wetsvoorstel gekozen is voor een verwervingsstrategie waarbij sprake is van leveringszekerheid. In antwoord op de VVD-fractie merk ik op, dat in dat verband is overwogen om bij de voorbereiding van de aanbesteding accreditatie/certificering een rol te laten spelen; om reden van efficiëncy is er echter voor gekozen de te kwaliteits- en veiligheidseisen deel te laten uitmaken van het bestek, waarbij de aanbestedende instantie (de Minister van BZK) de conformiteit integraal beoordeelt. Overigens is het zo, dat de kwaliteits- en veiligheidscriteria voor publieke en private burgermiddelen gelijk zijn; bij beide wordt uitgegaan van de eIDAS-eisen. Er is sprake van gelijkwaardige middelen, waarmee een gebruiker in de richting van de overheid hetzelfde kan. Een privaat middel kan daarnaast ook in het commerciële domein worden gebruikt. Nogmaals: het voorgaande staat los van een eventuele rol die accreditatie/certificeren kan vervullen.

Uit de vragen van de VVD-fractie en de CDA-fractie maak ik op, dat de beschikbaarheid van meerdere middelen en een *level playing field* voor hen belangrijk zijn. Zij vragen naar de mogelijkheden van zoveel mogelijk (en gelijke) kansen voor aanbieders van private middelen en daarmee van toelating van private burgermiddelen indien deze aan de eisen voldoen. De keuze voor dergelijk «open» stelsel kan leiden tot de toelating van een veelvoud aan private middelen, hetgeen gevolgen heeft voor de benodigde ontzorging van dienstverleners en daarmee de uitvoerbaarheid. Dit klemt in het burgerdomein omdat het burgermiddel functioneert op basis van het bsn. Dit stelt systeemtechnisch en organisatorisch zware eisen aan de beveiliging. Anderzijds zou door een meer «open» stelsel, met name indien de betrokken eisen techniekonafhankelijk worden geformuleerd, ruimte worden gelaten aan de markt en aan innovatie. Zoals gezegd kan er daarbij voor gekozen worden om conformiteit met die eisen te laten aantonen via accreditatie/certificering, dat hoeft echter niet.

3. Verwervingsstrategie privaat burgermiddel

Het is wenselijk dat, naast de beschikbaarheid van publieke middelen op verschillende betrouwbaarheidsniveaus, private alternatieven met een hoge dekkingsgraad op deze niveaus beschikbaar komen. Burgers kunnen dan ook een privaat middel als hun primaire inlogmiddel gebruiken. Om dat te realiseren maakt het wetsvoorstel het op dit moment mogelijk om een of meerdere private identificatiemiddelen toe te laten. Beoogd was dit via een aanbestedingsprocedure te realiseren. Hiervoor is gekozen om redenen van beheersbaarheid; bij een of enkele private partijen kan de overheid direct sturen op zaken als veiligheid, betrouwbaarheid, privacybescherming en communicatie. Bovendien is sprake van – voor een hoge dekkingsgraad relevante – leveringszekerheid; de gegunde partijen zijn verplicht een middel te leveren tegen een vooraf bepaalde prijs. Burgers weten dan waar zij aan toe zijn. Onderkend werd, dat de overheid zich bij een aanbesteding voor een langere periode vastlegt op een beperkt aantal oplossingen; er is na gunning gedurende een aantal jaren minder ruimte voor innovatie en concurrentie door de markt.
Dit was ten tijde van de indiening van dit wetsvoorstel geen doorslaggevend argument, omdat toen sprake was van een beperkt aantal gegadigden en weinig ontwikkeling op de markt. De voorbereidingen voor een aanbesteding zijn gestart; publicatie kan nog in 2019 plaatsvinden. Daarna duurt het nog enkele maanden totdat een voorlopige gunning is afgerond. Hierbij is niet de verwachting dat de aanbesteding geen enkel

identificatiemiddel zal opleveren. Het aanbestedingstraject kan parallel aan het wetstraject plaatsvinden.
Inmiddels zijn echter de feiten en omstandigheden significant gewijzigd; het tempo waarmee innovatie zich voltrekt is het afgelopen jaar sterk toegenomen, de ontwikkeling van inlogmiddelen versnelt en het aantal gegadigden in de markt groeit. Hierbij past een meer wendbare en daarmee toekomstvaste toelatingssystematiek; aanbesteden ligt dan minder voor de hand. Dit vormt voor mij de aanleiding om een andere verwervingsstrategie te overwegen, onverminderd het doel om zo snel mogelijk private alternatieven en een hoge dekkingsgraad te realiseren. Mogelijk kan dat tevens, en beter, via een meer open toelatingssysteem (erkenning).
Vanuit de wens te kunnen inspelen op nieuwe ontwikkelingen ben ik voornemens innovatie te bevorderen en meer gebruik te maken van wat de markt te bieden heeft. Vanzelfsprekend zonder daarbij concessies te doen aan de kernwaarden toegankelijkheid, veiligheid, betrouwbaarheid en gebruiksvriendelijkheid, zoals verankerd in de agenda NLDIGIbeter. Momenteel oriënteer ik mij daarom op de haalbaarheid en vormgeving van een open toelatingssysteem. Ik ben tevens in gesprek met de markt om alle consequenties van een andere toelatingssystematiek in beeld te brengen alvorens definitief te beslissen over het toelatingssysteem. Hierbij wordt gekeken naar financiële- en beheersaspecten (mede in relatie tot de bekostiging van het publieke middel en publieke voorzieningen), continuïteit, uitvoerbaarheid, snelheid/doorlooptijd, toekomstbestendigheid en coherentie met het bedrijvendomein. Met deze heroverweging wordt tevens tegemoetgekomen aan de vragen en opmerkingen van de leden van de VVD-fractie en de CDA-fractie, waarin de wens doorklinkt tot zoveel mogelijk gelijke kansen voor private partijen, ruimte voor private burgermiddelen en het toestaan van middelen indien aan de (op eIDAS gebaseerde) eisen wordt voldaan. Ik ben voornemens Uw Kamer binnen enkele weken nader te informeren over deze heroverweging. Indien een ander stelsel van toelating opportuun blijkt, zal ik een nota van wijziging indienen.
Met het bovenstaande zijn de door de VVD-fractie en de CDA-fractie gestelde vragen naar de door mij voorgestane koers en het al dan niet maximeren van het aantal private partijen beantwoord.

4. Vervolgstappen verwervingsstrategie privaat burgermiddel en samenvoeging domeinen

De verwervingsstrategie ten aanzien van private inlogmiddelen voor burgers wordt heroverwogen met als doel om de uitkomst van deze oriëntatie nog in de eerste tranche mee te nemen. In dit verband worden momenteel aspecten als beheersbaarheid, financiering en doorlooptijd bij zowel beperkte als open toelating bezien. Wanneer deze oriëntatie is afgerond en ik op basis daarvan een afweging heb gemaakt, zal ik uw Kamer berichten.
Daarnaast is het van belang dat het burger- en bedrijvendomein op termijn naar elkaar kunnen toegroeien. Op dit punt maak ik daarmee een start door de mogelijkheden te benutten die de eerste tranche biedt om deze domeinen in uitvoeringsregelgeving inhoudelijk naar elkaar te laten toegroeien. Het doel op de lange termijn is om de domeinen naar elkaar toe te laten groeien, maar dat niet overhaast te doen. De prioriteit – en daarmee de eerste stap – is dat overheidsdienstverleners spoedig en beheerst veiligere inlogmiddelen implementeren. Het tegelijkertijd opheffen van de scheiding tussen het burger- en bedrijvendomein verhoogt de complexiteit aanzienlijk. Zo zullen de materiële eisen aan de leveranciers van private middelen moeten worden geüniformeerd. De samenvoeging voor beide domeinen zal, zowel voor overheidsorganisaties, als voor de middelenleveranciers, consequenties hebben en op

uitvoerbaarheid moeten worden bezien. Ik zal met de overheid en markt in gesprek gaan om het draagvlak voor een volledige opheffing van deze scheiding te onderzoeken. Desgewenst kan de WDO in een volgende tranche worden aangepast.
Tevens is van belang dat in de toekomst de rol van de overheid in het commerciële/private domein wordt gedefinieerd. Ik acht het van belang om als overheid ook daar een rol te gaan spelen, en de vraag is hoe zo'n rol het best wordt ingevuld. Daartoe wordt naast het inzetten van het publieke middel teneinde een faciliterende rol te vervullen in het commerciële domein ook gekeken naar andere inlogmethoden die binnen de huidige tranche van dit wetsvoorstel passen. Zo wordt, zoals ik al op 14 mei vermelde in mijn reactie (TK 26 643–609) op het IRMA-manifest, onderzoek gedaan naar de methodiek en bruikbaarheid van afgeleide middelen waarbij de overheid bij de uitgifte van (private) middelen een rol neemt door digitale zekerheid over identiteitsvaststelling te bieden waarop wordt voortgebouwd.

5. Overige vragen

De leden van de VVD-fractie vragen of de multi-middelenstrategie gericht is op één markt met meerdere private middelen en één publiek middel, die alle vanuit concurrentieperspectief gelijk zijn, of dat de multi-middelenstrategie gericht is op enerzijds één markt waar afnemers, niet zijnde de overheid, private middelen gebruiken en anderzijds één andere markt waar één afnemer, zijnde de overheid, gebruik maakt van het publieke middel en één privaat middel.

Beoogd wordt – ongeacht de uiteindelijke verwervingsstrategie – overheidsdienstverlening voor burgers op verschillende betrouwbaarheidsniveaus mogelijk te maken via publieke en private middelen. Digitale transacties buiten de overheid vallen buiten de werkingssfeer van dit wetvoorstel.
Met het publieke middel kan een burger alleen bij de (semi)overheid terecht; overheidsdienstverleners herkennen burgers aan de hand van hun bsn.

De leden van de VVD-fractie vragen in hoeverre er bij de huidige multi-middelenstrategie sprake is van gelijke kansen voor alle middelen en of de behandeling van de publieke middelen anders zal zijn. Ook vragen zij zich af in hoeverre is gekeken naar de staatssteunaspecten bij de totstandkoming van publieke middelen. Ook vraagt de VVD-fractie of een aanbesteding gescheiden wordt van de DigiD-operatie en of de overheid haar middelen in één keer voor alle diensten aanbesteedt.

De aan de toelating van publieke en private middelen ten grondslag liggende eisen zijn dezelfde, te weten in ieder geval de aan de eIDAS-verordening ontleende eisen. Bij een openbare aanbesteding kunnen alle private partijen meedingen, in die zin is sprake van gelijke kansen. Op basis van de mate waarin voldaan wordt aan de aanbestedingscriteria kan een middel uiteindelijk worden aangewezen. Bij een open stelsel (erkenning systematiek) kunnen alle private partijen die aan de eisen voldoen worden toegelaten. Dan is er, nog meer dan bij aanbesteding, sprake van gelijke kansen. Toepasselijkheid van de staatssteunregels en de aanbestedingsregels is niet aan de orde bij publieke middelen; deze worden – onder de verantwoordelijkheid van de Minister van BZK – door de overheid zelf ontwikkeld.
De (door)ontwikkeling van publieke middelen (DigiD) hangt inhoudelijk samen met de verwervingsstrategie terzake van private middelen; ze moeten immers aan dezelfde eisen voldoen. Procesmatig staan beide echter los van elkaar. Bij een aanbesteding wordt in één keer aanbesteed.

Bij een open stelsel is dit naar zijn aard anders. Aanvragen voor een toelating (erkenning) kunnen vanaf inwerkingtreding van de WDO en bijbehorende uitvoeringsregelgeving ingediend worden; private partijen kunnen daarna op ieder moment instappen.

De leden van de VVD-fractie vragen naar de werkwijze bij de overige geaccrediteerde eIDAS-vertrouwensdiensten op de TSL-lijst (Trusted Services List) van Nederland, bijvoorbeeld de diensten rond het gebruik van een elektronische handtekening. Voorts vragen zij op welke wijze de overige eIDAS-vertrouwensdiensten samenhangen met de erkenning van private elektronische identificatiemiddelen voor burgers door een aanbesteding en hoe die koppeling is geborgd. Ook vragen de leden van de VVD-fractie of erkenning van het burgermiddel door middel van een aanbesteding te combineren is met een stelsel waarin alle overige vertrouwensdiensten, inclusief het bedrijvenmiddel, door accreditatie tot stand komen.
Voor de eIDAS-vertrouwensdiensten geldt een systeem van open toelating: de Minister van EZK kan ze – na accreditatie – de status «gekwalificeerd» toekennen. Dit wordt niet door het onderhavige wetsvoorstel geregeld, maar is sinds 2016 separaat geregeld door de Telecommunicatiewet juncto de eIDAS-verordening. Marktpartijen en ook overheidsinstanties kunnen gekwalificeerde vertrouwensdiensten inkopen. Overheidsinstanties zijn daarbij aanbesteding plichtig. De toelating van overige eIDAS-vertrouwensdiensten hangt niet samen met de toelating van private identificatiemiddelen; koppeling is dus niet nodig. De eIDAS-verordening kent namelijk een verschillend regime voor (toelating van) vertrouwensdiensten en diensten/middelen voor identificatie, en staat niet in de weg aan de combinatie van aanbesteding van een privaat burgermiddel en open toelating van overige vertrouwensdiensten (incl. bedrijvenmiddel). Voor de duidelijkheid zij benadrukt, dat het bedrijvenmiddel ook niet door accreditatie *sec* tot stand komt (zie hierboven paragraaf 3.2).
Met betrekking tot private inlogmiddelen vragen de leden van de VVD-fractie of gekeken is hoe in andere landen de prijsvorming voor private en publieke middelen gaat. Hetzelfde geldt voor de financiering van en investeringen in private en publieke middelen. Is er sprake van accreditatie of aanbesteding? Zijn er in het buitenland voorbeelden die kunnen helpen bij een echte multi-middelenstrategie? In hoeverre is er gekeken naar alternatieven in België?
De ontwikkelingen en bekostigingssystematiek in andere Europese landen zijn onderling verschillend. Zo is in het Verenigd Koninkrijk sprake van open toelating van private middelen; het stelsel wordt gefinancierd door de overheid. Vanwege de onbeheersbaarheid van de kosten wordt nu aanbesteding overwogen. In België is sprake van enkele *preferred suppliers*, die een vergoeding van de overheid ontvangen. Voorts zal ik, in het licht van mijn voornemen een andere verwervingsstrategie voor private burgermiddelen te gaan hanteren, de situatie in Denemarken en Duitsland nog nader bezien. Hoewel het nuttig is van ervaringen van andere lidstaten te leren, geldt de kanttekening dat elders sprake is van een andere context, waardoor het lastig is zaken 1 op 1 over te nemen. Zo kennen veel lidstaten, anders dan Nederland, geen van overheidswege uitgegeven (dus: publieke) middelen, waardoor men meer afhankelijk is van de markt.
Voorts vragen de leden van de VVD-fractie of de financiering van DigiD marktconform zal geschieden, alsmede in hoeverre is of wordt overwogen in plaats van een eigen publiek middel te ontwikkelen een middel in het buitenland te kopen.
Momenteel werk ik aan de bekostiging van het stelsel. De kosten van DigiD worden thans integraal doorbelast aan de overheidsdienstverleners op basis van een prijs per inlog. De financiering van DigiD zal in de

toekomst dusdanig zijn, dat toegelaten private middelen ook financieel een reëel alternatief vormen voor het publieke middel. Vanzelfsprekend zullen de uitgangspunten van de Wet markt en overheid in acht worden genomen. Het van overheidswege ontwikkelen van een middel voor burgers is, gelet op de betrokken publieke belangen, staand kabinetsbeleid. DigiD wordt sinds jaar en dag en op grote schaal door burgers gehanteerd bij hun toegang tot overheidsdienstverlening; het publieke middel wordt momenteel doorontwikkeld tot een nog veiliger en betrouwbaarder middel. Uw Kamer verzocht in 2016, bij motie van het lid de Caluwé, om de ontwikkeling van in ieder geval een publiek middel. Mijn verantwoordelijkheid terzake is daarom verankerd in het wetsvoorstel.
De leden van de CDA-fractie constateren, naar aanleiding van de aanbeveling van het Adviescollege Toetsing Regeldruk (ATR) over standaardisering bij eHerkenning, dat de keuzemogelijkheden voor klanten niet bepaald worden door de markt, maar door de overheid. De leden vragen de regering hierop nader in te gaan.
Het klopt dat de overheid eisen stelt aan toe te laten bedrijfs- en organisatiemiddelen en aan het betrouwbaarheidsniveau van dienstverlening. Bij en krachtens het onderhavige wetsvoorstel worden immers kaders gesteld, bijvoorbeeld over de classificering van de betrouwbaarheidsniveaus. Echter: binnen deze wettelijke kaders zijn nog wel degelijk keuzes door de markt mogelijk. Zo stel ik geen eisen aan de prijs; de private aanbieders van de middelen concurreren met elkaar op prijs en gebruiksvriendelijkheid, hetgeen in het voordeel uitpakt van de gebruiker die het middel aanschaft.
De CDA-fractie constateert dat voor de toelating van private identificatiemiddelen voorschriften worden gesteld, en heeft diverse vragen gesteld over de specifieke invulling daarvan dan wel de verplichting van functionaliteiten (BSNk) of specifieke (pseudonimiserings)technieken door het wetsvoorstel en hoe invulling is gegeven aan gesignaleerde risico's (zoals het voorkomen van hotspots) in de eerder uitgevoerde gegevensbeschermingseffectbeoordeling op het stelsel.
Gezien het onderlinge verband pak ik deze vragen samen tot de kern, namelijk de vraag of en in hoeverre concrete (technische) maatregelen door het wetsvoorstel worden verlangd.
Het is onwenselijk en ongebruikelijk om op wetsniveau concrete (technische) maatregelen voor te schrijven. Het wetsvoorstel beoogt techniek-onafhankelijke inrichting van privacybeschermende maatregelen mogelijk te maken en te houden. Welke specifieke privacybeschermende technieken worden gebruikt, in samenhang met organisatorische en operationele maatregelen, wordt bepaald door de wijze waarop invulling wordt gegeven aan privacybescherming door de verwerkingsverantwoordelijke. Deze dient een adequaat beschermingsniveau te realiseren. Dat kan op verschillende manieren en zal bovendien, door voortschrijding van technische ontwikkelingen, door de tijd kunnen veranderen. Het wetsvoorstel staat er overigens ook niet aan in de weg dat specifieke technieken worden ingezet, als resultaat van onderbouwde keuzes bij de implementatie.
Ik merk in algemene zin ten aanzien van privacybescherming nog op dat een (te) sterke, vaak technische focus, zoals op het voorkomen van verzamelingen van persoonsgegevens (ook wel hotspots genoemd) en daaraan gerelateerde risico's, in zichzelf het gevaar draagt dat risico's in het stelsel verschuiven, bijvoorbeeld een gebrek aan herstelvermogen als er binnen het stelsel onverhoopt iets misgaat. Privacywetgeving biedt een kader om verwerkingen van persoonsgegevens veilig en verantwoord te realiseren. Dat is ook het doel van het eID stelsel. Ik benader daarom de inrichting van privacybescherming voor het stelsel integraal, als een samenstel van samenhangende en elkaar aanvullende maatregelen. Voorkomen moet worden dat we ons blindstaren op een aantal technische

maatregelen. Daarbij is privacybescherming geen eenmalige activiteit. Het blijft een continu proces waarbij door de tijd risico's en maatregelen herijkt moeten worden en maatregelen zo nodig moeten worden bijgesteld.
De leden van de CDA-fractie vragen welke gevolgen de aanvullende eisen mogelijk zullen hebben voor het resultaat van de aanbesteding en of de regering het mogelijk acht, dat aanbesteding geen enkel privaat identificatiemiddel zal opleveren.

De eisen die worden gesteld aan inlogmiddelen dienen te voldoen aan de vereisten die gelden op basis van de eIDAS-verordening en terzake geldende privacywetgeving, en dienen ertoe burgers adequaat te beschermen. Dat vormt de basis voor het stellen van eisen, niet de inschatting van de resultaten van een verwerving.

De leden van de CDA-fractie vragen, welke randvoorwaarden in het kader van de aanbesteding (of accreditatie) kunnen worden gesteld aan buitenlandse partijen, voor zover mogelijk op basis van Europese wetgeving, om aanbieder te kunnen worden van een identificatiemiddel in Nederland.

Het uitgangspunt is dat partijen die aanbieden aantoonbaar aan de eisen die worden gesteld moeten kunnen voldoen. Deze eisen zijn niet anders dan voor binnen de EU gevestigde partijen. Voor buiten de EU gevestigde partijen geldt reeds – op grond van de AVG – dat zij moeten kunnen aantonen dat een sprake is van gelijkwaardig beschermingsniveau voor persoonsgegevens.

De leden van de CDA-fractie vragen, welke randvoorwaarden in het kader van de aanbesteding (of toelating) kunnen worden gesteld aan buitenlandse partijen, voor zover mogelijk op basis van Europese wetgeving, om aanbieder te kunnen worden van een identificatiemiddel in Nederland. De leden van de CDA-fractie vragen voorts of elektronische toegang tot overheidsdienstverlening naar de opvatting van de regering tot de vitale infrastructuur behoort en zo ja, welke eisen op grond daarvan aan aanbieders kunnen worden gesteld.
De wettelijke eisen aan nationale en buitenlandse aanbieders zijn hetzelfde; de eisen worden in beginsel non discriminatoir toegepast. Het door mij nemen of opleggen van maatregelen om acute veiligheidsproblemen aan te pakken, is ingevolge het wetsvoorstel mogelijk. Vanzelfsprekend dient dit op basis van een zorgvuldige weging, inschatting van de dreiging en een risicoanalyse te geschieden. Ook is in 2017 de vitaliteit van DigiD vastgesteld. Dit betekent dat een meldplicht bij het Nationaal Cyber Security Centrum (NCSC) geldt ingeval van ernstige digitale veiligheidsincidenten. De aanwijzing als «vitaal» heeft geen gevolgen voor de eisen die in het kader van dit wetsvoorstel worden gesteld.

De leden van de CDA-fractie vragen of zij goed hebben begrepen dat de betrouwbaarheidsniveaus substantieel en hoog moeten bereikt worden met het huidige DigiD als fundament en of dat fundament technisch toereikend is om op voort te bouwen. De leden vragen voorts of het wetsvoorstel ook vormen van afgeleide identificatie mogelijk maakt.
De betrouwbaarheidsniveaus substantieel en hoog kunnen bereikt worden met het huidige DigiD als fundament; dat is hiervoor geschikt en bedoeld. Afgeleide identificatie, waaronder de situatie dat een privaat middel de aanvraag baseert op DigiD, is mogelijk en toegestaan. Het wetsvoorstel laat, in aansluiting op de eIDAS uitvoeringsverordening 1502, ruimte om bij het proces van uitgifte van middelen te steunen op een eerder uitgevoerde controle, vaak de verificatiestap van identiteit, die doorgaans verhoudingsgewijs veel inspanning van de gebruiker vraagt en voor de

middelenuitgever een relatief groot deel van de kosten bepaalt. Onder een afgeleid identificatiemiddel wordt verstaan een identificatiemiddel dat voor een controlestap steunt op een eerder uitgevoerde controle. Overigens zullen, om afleiding van middelen op een veilige en betrouwbare manier mogelijk te maken, daaraan voorwaarden worden verbonden.

4. Privacy

De D66-fractieleden vragen toe te lichten op welke wijze de regering uitvoering geeft aan artikel 15 tot en met 18 AVG aangaande het recht van inzage en rectificatie.

Het wetsvoorstel en voorgenomen uitvoeringsregelgeving zullen de juridische kaders bevatten die gelden voor verwerkingen van persoonsgegevens die plaatsvinden in het kader van het eID stelsel. Dit geldt niet voor de artikelen 15 tot en met 18 AVG (rechten van inzage en rectificatie voor gebruikers). Opname van deze rechten in het wetsvoorstel is niet nodig en, vanwege de rechtstreekse toepasselijkheid van de AVG, zelfs niet toegestaan. Wel werken deze rechten door in de technische en organisatorische inrichting en vormgeving van de voorzieningen in het stelsel. De wijze waarop dit wordt gerealiseerd staat beschreven in de Privacyvisie eID, zoals u die bij gelegenheid van de Voortgangsrapportage eID eind januari jl. is toegestuurd.

5. Misbruik van de GDI

Over dit onderdeel zijn geen vragen gesteld of opmerkingen gemaakt.

6. Toezicht en handhaving

De leden van de VVD-fractie vragen of het toezicht op de private middelen, die straks in het publieke domein worden gebruikt, wordt belegd bij de door de Minister aan te wijzen ambtenaren. Voorts vragen de leden welke rol Logius en de Rijksdienst voor identiteitsgegevens in dezen hebben. De leden van de CDA-fractie constateren dat het Ministerie van BZK een breed pakket van taken en verantwoordelijkheden krijgt, en vragen te onderbouwen waarom het Ministerie van BZK niet alleen de aanbesteding uitvoert, maar ook toezicht houdt, audits verricht en zelf als leverancier van DigiD optreedt.

Het private alternatief voor het publieke middel en het publieke middel zelf, zijn gelijkwaardig en uitwisselbaar waar het overheidsdienstverlening betreft. Vanwege die sterke publieke component is er in het wetsvoorstel voor gekozen het toezicht op de private burgermiddelen tot mijn verantwoordelijkheid te rekenen. Ik constateer met u dat het eID-stelsel een groot aantal taken met zich brengt. Dat is op zichzelf geen probleem, het past in mijn stelselverantwoordelijkheid voor de digitale overheid, maar een vervolgvraag is dan hoe ongewenste samenval van taken wordt voorkomen en toezicht adequaat en onafhankelijk wordt ingericht.

Vooropgesteld moet daarbij worden, dat een toezichtsrol voor Logius als beheerorganisatie en RVIG als nauw betrokkene bij de ontwikkeling van DigiD hoog (eNIK) niet is voorzien (*Chinese walls*). Gelet op de opgedane kennis en ervaring met het toezicht op DigiD en het feit, dat een aanbesteding hooguit slechts tot een of enkele extra middelen leidt, was het opportuun het toezicht – in dat geval in feite contractbeheer – te beleggen bij door mij aan te wijzen ambtenaren, met gebruik van interne controlemechanismen, mogelijk ondersteund door ambtenaren van het Agentschap Telecom en (externe) auditdiensten.

Nu ik mij beraad op een andere verwervingsstrategie (zie paragraaf 3.3), die naar verwachting leidt tot een groter aantal middelen, waardoor meer wordt gevergd aan beheersbaarheid, past het om in het verlengde daarvan de inrichting van het toezicht te heroverwegen en dit meer in lijn te brengen met het toezicht op het bedrijvenmiddel (*checks and balances*). Ik bericht u hierover binnen enkele weken, wanneer ik uw Kamer informeer over mijn bevindingen inzake een andere verwervingsstrategie.

7. Financiële bepalingen en gevolgen

De leden van de VVD-fractie vragen waarom de kosten, die voor rekening van de overheidsorganen en aangewezen organisaties komen, nog niet bekend zijn en wanneer die kosten wel bekend zullen zijn. Voorts vragen zij, hoe de kosten van deze organen en aangewezen organisaties worden bepaald en hoe deze organisaties daarover geïnformeerd worden en op welke termijn.

De leden van de D66-fractie verzoeken de regering om een geheel beeld te schetsen van de kosten voor de overheid voor «het inloggen in het BSN-domein». Zij verzoeken dit schematisch weer te geven en hierbij ook een schatting mee te nemen van de kosten die voor rekening komen van de bestuursorganen en aangewezen organisaties.

Zoals in de toelichting bij het wetsvoorstel is vermeld zullen de kosten van exploitatie en doorontwikkeling pas de komende tijd, bij de voorbereiding van de uitvoering van het programma, volledig duidelijk worden. Uitgangspunt is en blijft dat de overheidsdienstverleners de kosten van het inloggen betalen naar rato van gebruik; dit geldt zowel voor het publieke inlogmiddel (DigiD), als voor de (nog te verwerven) private middelen. Daarbij kunnen burgers kiezen van welk middel ze gebruik maken; ze loggen in met DigiD of met een privaat middel. In de toelichting bij het wetsvoorstel (paragraaf 7.3) zijn de financiële gevolgen voor de gebruikers (burgers en bedrijven), de dienstverleners en het Rijk geschetst. Kortheidshalve verwijs ik u hiernaar. Op dit moment is het niet mogelijk de exacte kosten te berekenen van het stelsel. De bekostigingssystematiek, die zal worden neergelegd in een uitvoeringsregeling bij dit wetsvoorstel, zal interdepartementaal worden afgestemd en aan een uitvoeringstoets worden onderworpen.

8. Verhouding tot andere wetgeving

De leden van de GroenLinks-fractie zouden graag een nadere toelichting ontvangen over de verhouding tussen deze wet en de regelgeving op de BES-eilanden. Ook hebben deze leden de vraag hoe de relatie is tussen de voorgestelde wet en de Wet gebruik Friese taal.

Voor de betekenis van deze wet voor het Caribische deel van het Koninkrijk moge ik u verwijzen naar de toelichting bij de voorgestelde wijziging van de Paspoortwet, welk voorstel van Rijkswet bij uw kamer is ingediend (Kamerstukken 2018/2019, 35 047-R2108).

Het onderhavige wetsvoorstel laat de toepasselijkheid van de Wet gebruik Friese taal, die regels bevat met betrekking tot het gebruik van de Friese taal in het bestuurlijk verkeer en in het rechtsverkeer, onverlet.

9. Gevolgen voor burgers en bedrijven

De leden van de D66-fractie vragen of verduidelijkt kan worden wanneer iedereen in Nederland, die nu gebruik maakt van DigiD, op de hogere betrouwbaarheidsniveaus zou moeten kunnen inloggen en wat de

planning is. Voorts vragen zij op welke wijze hier zorg voor wordt gedragen wanneer personen alleen een paspoort hebben en geen ID-kaart of rijbewijs. Ook vragen zij of er al meer bekend is over het totaalplaatje van de kosten die bij de burger komen te liggen voor het realiseren van DigiD niveau hoog en substantieel en of de regering hierbij ook de kosten van bijvoorbeeld de externe kaartlezer meeneemt. Voorts vragen de leden van de D66-fractie of de regering een maximumprijs zal hanteren die burgers moeten betalen aan een private partij voor het aanschaffen van een privaat middel.

Iedereen in Nederland kan inloggen op de hogere betrouwbaarheidsniveaus, als identificatiemiddelen op de niveaus substantieel en hoog breed beschikbaar zijn. DigiD-substantieel is reeds beschikbaar voor gebruikers van smartphones met NFC-lezer. Maatregelen om middelen op betrouwbaarheidsniveau substantieel breder toegankelijk te maken komen naar verwachting in de loop van 2020 beschikbaar. Verschillende maatregelen worden momenteel onderzocht, om te vermijden dat kaartlezers nodig zullen zijn. De kosten van de plaatsing van de chip met de betreffende functionaliteit op het e-rijbewijs en eNIK worden verrekend met de leges. De kosten van het gebruik van het middel worden niet doorberekend aan de burger. Daarnaast wordt gestreefd om een of meer private inlogmiddelen te verwerven die eveneens in de loop van 2020 beschikbaar komen. Bij een aanbod van verschillende inlogmiddelen hebben burgers vrijheid om de kosten van deze middelen mee te laten wegen bij hun keuze. Vooralsnog lijkt het daarom niet noodzakelijk om maximumprijzen te hanteren die burgers moeten betalen aan een private partij.

Het streven is ook om DigiD-hoog in 2020 beschikbaar te hebben op de nieuwe e-NIK. De bij uw kamer ingediende wijziging van de Paspoortwet biedt hiervoor de grondslag. Dit inlogmiddel werkt alleen in combinatie met een NFC-lezer (smartphone en desktop) en een nieuwe eNIK-kaart of nieuw e-rijbewijs en komt daarom vooralsnog niet breed beschikbaar. Vanwege het beperkte bereik kan slechts op kleinere schaal gestart worden met een lerende uitrol van middelen op niveau hoog. Het kabinet kiest er dan ook voor om middelen op niveau hoog in te zetten in de gebieden waar het noodzakelijk wordt geacht en de maatschappelijke en financiële baten daarvan opwegen tegen aanloopproblemen. Daarnaast wordt rekening gehouden met de beperkte beschikbaarheid doordat de diensten in die gebieden, die op de lange termijn nog uitsluitend toegankelijk zullen zijn met een middel op niveau hoog (zoals het zorgdomein), op basis van het wetsvoorstel voorlopig ook toegankelijk zijn met middelen op niveau substantieel, zodat gedurende deze periode maatregelen kunnen worden genomen om de beschikbaarheid uit te breiden.

10. Overgangsrecht en inwerkingtreding

Over dit onderdeel zijn geen vragen gesteld of opmerkingen gemaakt.

11. Consultatie en advies Autoriteit Persoonsgegevens

Over dit onderdeel zijn geen vragen gesteld of opmerkingen gemaakt.

II ARTIKELSGEWIJS

Artikel 9, tweede lid

De leden van de CDA-fractie constateren, naar aanleiding van het aspect betaalbaarheid, dat de burger zowel voor het publieke als het private middel moet betalen. De leden vragen of het juist is, dat die laatste prijsvorming door aanbesteding plaatsvindt en niet door marktwerking.

Zoals in paragraaf 9 is aangegeven, zullen burgers een privaat middel kunnen aanschaffen bij een private partij. Het staat deze partij vrij om burgers hiervoor te laten betalen. Bezien zal worden of het, om redenen van betaalbaarheid en brede beschikbaarheid voor burgers, opportuun is om een maximumprijs te hanteren als voorwaarde voor toelating van een privaat middel. Het is een mogelijkheid dat de overheid deze kosten (deels) voor haar rekening neemt om de aanschafprijs te matigen. Prijsstelling kan zowel in een aanbestedingsprocedure als in een systeem van open toelating (naar welke verwervingsstrategie mijn voorkeur uitgaat, zie paragraaf 3.3) van toepassing zijn; alsdan wordt de prijsvorming van private middelen niet volledig aan de markt overgelaten, maar worden er (maximum) tariefvoorschriften gesteld.
De leden van de CDA-fractie vragen of de ervaringen met de pilots, die hebben bijgedragen aan de keuze om in het wetsvoorstel de mogelijkheid van toelating van private middelen op te nemen en de toegang tot overheidsdienstverlening niet louter door publieke middelen te laten geschieden, betekenen dat de multi-middelenstrategie is losgelaten.

Zoals eerder in deze nota (zie onder meer de paragrafen 3.1 en 3.3) is aangegeven, is het wenselijk dat voor burgers, naast de beschikbaarheid van publieke middelen op verschillende betrouwbaarheidsniveaus, private alternatieven met een hoge dekkingsgraad beschikbaar komen. Dat is het doel, dat als effect zal hebben dat meerdere (multi)middelen beschikbaar zullen zijn.
De leden van de D66-fractie vragen of de noodzaak tot toelating van een privaat middel nu al bestaat vanwege het feit dat er slechts één identificatiemiddel is, en of, indien er één privaat middel is toegelaten, de noodzaak voor nóg een privaat middel dan niet meer aanwezig is.
Ik acht het, om redenen van brede beschikbaarheid, keuzeruimte voor burgers en inspelen op ontwikkelingen in de markt, gewenst dat naast publieke middelen tevens private middelen kunnen worden gebruikt om overheidsdiensten af te nemen. Ik ben daarom voornemens om niet langer een of enkele, maar zoveel mogelijk private middelen toe te laten en mijn verwervingsstrategie terzake aan te passen (zie paragraaf 3.3). Vanzelfsprekend mag en zal dit niet ten koste gaan van de veiligheids- en betrouwbaarheidseisen.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops