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. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 21 december 2018

Inhoudsopgave

I ALGEMEEN

1. Inleiding

De leden van de VVD-fractie, de CDA-fractie, de D66-fractie en de DENK-fractie hebben met belangstelling kennisgenomen van het Wetsvoorstel digitale overheid. Zij hebben hierover diverse 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.
Waarschijnlijk is er geen ander beleidsdomein dat zo sterk wordt beïnvloed door de snel voortschrijdende technologische ontwikkeling als de digitale overheid. Met dit voorstel wordt de richting bepaald waarin de digitale overheid zich in de komende jaren ontwikkelt. In de voorliggende

kst-34972-6
ISSN 0921 - 7371
's-Gravenhage 2018

eerste tranche worden de zaken geregeld die nu nodig zijn. Ondertussen staat het denken niet stil en oriënteren we ons op nieuwe ontwikkelingen en de noodzaak die hieruit volgt om zaken te regelen via wetgeving. In dat licht bezien heeft dit wetsvoorstel een bijzonder karakter; het heeft een zekere toekomstbestendigheid, waardoor kan worden ingespeeld op nieuwe (technische) ontwikkelingen en gewijzigde inzichten en innovatie kan worden gefaciliteerd. Daarbij moet, in lijn met de advisering door de Raad van State, steeds bezien worden op welke wijze een werkbaar evenwicht kan worden gevonden tussen de benodigde wendbaarheid enerzijds en rechtszekerheid voor burgers en bedrijven anderzijds. In volgende tranches zullen verdere stappen worden gezet in de ontwikkeling van de digitale overheid. Dat geschiedt vanuit bepaalde waarden en waarborgen. Vanuit NL DIGIbeter zijn dat gebruiksvriendelijkheid, privacy, veiligheid en betrouwbaarheid. Deze stapsgewijze benadering sluit aan bij de aanbevelingen van de Commissie Elias.

De VVD-fractie constateert dat er een wetsvoorstel voorligt dat de digitale dienstverlening van de overheid uniformeert. De leden vragen zich af waar de focus van het wetsvoorstel ligt. Ook vragen zij zich af in hoeverre het wetsvoorstel gericht is op de gebruikers van de digitale overheid, wat het wetsvoorstel betekent voor burgers en bedrijven.
Het wetsvoorstel heeft een tweeledige focus. In de eerste plaats wordt de toegang tot digitale dienstverlening van de overheid gereguleerd. Het wetsvoorstel reguleert hetgeen nodig is om burgers en bedrijven veilig en betrouwbaar bij de overheid te kunnen laten inloggen: publieke voorzieningen als onderdeel van de GDI, veilige dienstverlening door overheidsorganen, eisen aan publieke en private identificatiemiddelen, informatieveiligheid, privacybescherming, voorkoming van misbruik en toezicht. Dit wordt aangeduid als het eID-stelsel. In de tweede plaats biedt het wetsvoorstel de grondslag voor de aanwijzing van (technische en interoperabiliteits-) standaarden, die door overheidsinstanties verplicht moeten worden toegepast teneinde het elektronische verkeer met burgers en bedrijven beter te laten verlopen. Terecht constateert de VVD dat het wetsvoorstel zich vooral richt tot de overheid zelf; het brengt mee dat overheidsinstanties (degenen tot wie de wet zich richt) hun bedrijfsvoering en werkprocessen moeten aanpassen. Dit zal er toe leiden dat burgers en bedrijven – de gebruikers van digitale overheidsdiensten – veilig, betrouwbaar en gebruiksvriendelijk bij de overheid kunnen inloggen.
De leden van de VVD-fractie krijgen voorts graag een reactie op de vragen, of er ook gekeken is naar de invloed van het wetsvoorstel op de digitale economie en de cyberveiligheid, hoe het bijdraagt aan de economische ontwikkeling in Nederland en aan een gecoördineerde aanpak van de overheid om Nederland online veiliger te maken.
Het wetsvoorstel voorziet in regels over cyberveiligheid. De focus ligt hierbij op de veiligheid van de toegang tot de digitale overheid en op de toepassing van de standaarden HTTPS en TLS, technische voorschriften die zorgen voor veilige verbindingen tussen (overheids)websites. Hiermee wordt, naast bestaande kaders zoals de EU Algemene verordening gegevensbescherming (AVG) en de Voorschriften informatiebeveiliging Rijksdienst (VIR), een basis gelegd voor het door overheidsorganisaties voldoen aan informatiebeveiligingsnormen, in het bijzonder bij de toegang tot hun elektronische dienstverlening. Cyberveiligheid begint bij het goed regelen en invullen van verantwoordelijkheden voor informatiebeveiliging die overheidsorganisaties zelf hebben. Het wetsvoorstel voorziet in verplichtingen voor organisaties die aansluiten op de digitale overheid en de wijze waarop de controle daarop plaatsvindt. Tevens is het voor cyberveiligheid van belang dat organisaties er rekening mee houden dat, ondanks dat informatiesystemen beveiligd zijn, er altijd inbreuken op systemen kunnen plaatsvinden. Het wetsvoorstel regelt ook dat er

herstelvermogen is. Dat betekent dat als er onverhoopt inbreuken op informatiesystemen of processen plaatsvinden, organisaties moeten zorgen dat zij die snel in het vizier krijgen en moeten samenwerken om deze op te lossen. Daarbij kent het wetsvoorstel aan de Minister van BZK ten aanzien van de aanpak van misbruik en fraude binnen het eID-stelsel bevoegdheden toe om coördinerend op te treden, om geconstateerde inbreuken op veiligheid of misbruik snel te kunnen herkennen en zo nodig te herstellen.
Over maatregelen ter bevordering van de cyberveiligheid bij de overheid in het algemeen is uw Kamer afzonderlijk geïnformeerd bij brief van 16 oktober jl. (TK 2018–2019, 26 643 nr. 574). In het algemeen geldt dat de digitale economie gebaat is bij een betrouwbare digitale infrastructuur. In die zin dragen de zaken die het wetsvoorstel regelt om cyberveiligheid te verbeteren inherent bij aan de versterking van de digitale economie.
De leden van de VVD-fractie constateren dat er geen publiek inlogmiddel voor bedrijven komt en vragen zich af wat de reden daarvoor is. Voorts missen de leden van de VVD-fractie in het geheel van voorzieningen, die voorzieningen die juist voor het bedrijfsleven van belang zijn; zij vragen zich af of het mogelijk is de digitale basisvoorzieningen die voor burgers worden geregeld, zoals inloggen, in deze wet ook voor de digitale economie te regelen. Voorts vragen zij zich af, of er andere manieren zijn om behulpzaam te zijn bij het beslechten van de grens tussen digitale overheid en digitale economie. Ook de leden van de D66-fractie vragen zich af in hoeverre het de bedoeling is om publieke middelen buiten het publieke domein te gebruiken en of dat breed inzetbaar wordt. De leden van de CDA-fractie vragen in dit verband of het wetsvoorstel voldoet aan de uitgangspunten in de strategische verkenning eID-stelsel Nederland (2012), waarin werd gepleit voor een nationaal stelsel waarin overheid en bedrijfsleven samenwerken om burgers, consumenten en bedrijven goed, snel en veilig elektronisch te kunnen bedienen.
Voor bedrijven zal geen publiek middel worden uitgegeven. Reden hiervoor is dat het huidige stelsel van private middelen voor bedrijven naar tevredenheid functioneert. Nut en noodzaak van een publiek middel voor bedrijven ontbreken. Wel wordt met het wetsvoorstel het stelsel van private middelen voor bedrijven 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 toezicht ingericht en gelden er bepalingen met betrekking tot privacybescherming en misbruik. Het in het wetsvoorstel bepaalde inzake private middelen voor bedrijven heeft een brede reikwijdte en geldt ook voor andere organisaties. Het wetsvoorstel spreekt om die reden ook over «bedrijfs- en organisatiemiddel», daarmee doelend op het inloggen bij de overheid door een onderneming of rechtspersoon als bedoeld in de Handelsregisterwet 2007.
Het verhogen van het betrouwbaarheidsniveau van de inlogmiddelen die worden gebruikt bij dienstverlening van de (semi)overheid heeft prioriteit. Het wetsvoorstel regelt geen basisvoorzieningen voor digitale transacties in de private (commerciële) sector, met uitzondering van de wijze van inloggen bij zorgverleners en pensioenuitvoerders. Dit houdt verband met het feit dat DigiD is ontwikkeld voor het inloggen bij dienstverleners die burgers in hun administratie herkennen aan de hand van het burgerservicenummer (bsn). Om die reden wordt via het inloggen met DigiD het bsn van de inloggende persoon geleverd aan de dienstverlener. Dit vergt dat dienstverleners gerechtigd zijn om bij de uitoefening van hun taak het bsn te verwerken, waardoor breed gebruik in het private domein niet mogelijk is. Voor zover mogelijk en noodzakelijk worden de grenzen tussen de digitale overheid en de digitale economie geslecht doordat het mogelijk wordt publieke middelen te gebruiken om in te loggen bij pensioenuitvoerders en zorgverleners. Het wetsvoorstel biedt voorts de

mogelijkheid om de grens te slechten door toelating van een privaat inlogmiddel voor natuurlijke personen en door de erkenning van private inlogmiddelen voor bedrijven, waarna deze middelen zowel in het private domein als publieke domein gebruikt kunnen worden. Indien in de toekomst blijkt dat bij consumenten de behoefte ontstaat om publieke middelen of andere basisvoorzieningen van de overheid te gebruiken bij economische transacties, zal worden bezien op welke wijze dit mogelijk is met inachtneming van de regels over verwerking van het bsn en de Wet markt en overheid. Om de e basisvoorzieningen voor de digitale economie te kunnen regelen, moeten de voordelen opwegen tegen de kosten, informatieveiligheidsrisico's voor de overheid en regeldruk voor private dienstverleners. Dit kan in een volgende tranche van het wetsvoorstel geregeld worden. Uitgangspunt van het kabinet is dat het inloggen bij commerciële dienstverleners (dus: buiten het publieke domein) zoveel mogelijk aan de markt moet worden overgelaten en de overheid hier geen rol heeft; het is van belang deze markt niet te verstoren en het groeipotentieel van marktpartijen niet te belemmeren.
De VVD-fractie vraagt voorts naar eventuele volgende tranches van de Wet digitale overheid, hoeveel tranches er zullen volgen, wat die zullen regelen en wat de bijbehorende tijdlijn is.
Met dit wetsvoorstel wordt de digitale overheid verankerd en wordt richting gegeven aan wat daarvoor 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 onvoorziene ontwikkelingen, ook buiten het kader van eID-voorzieningen en -functionaliteiten. Voor zover dit niet het geval is, bijvoorbeeld omdat deze ontwikkelingen de reikwijdte van het huidige wetsvoorstel te buiten gaan of omdat herijking van gemaakte keuzes nodig is, liggen vervolgtranches in de rede. Het is op dit moment niet exact te zeggen hoeveel tranches van de wet nog zullen volgen, wat deze regelen en wat de planning hiervan is. Dit hangt af van de aard van de ontwikkelingen, alsmede van nut en noodzaak van verankering in formele wetgeving. Zaken waaraan voor een volgende tranche wordt gedacht zijn de verbetering van de persoonlijke informatiepositie van burgers, bredere toepassing van standaarden voor digitale dienstverlening, het digitaal machtigen van derden, meer functionaliteiten van MijnOverheid en informatieveiligheid. Over deze onderwerpen vindt de gedachtenvorming momenteel volop plaats; in feite is daarmee de voorbereiding van een volgende tranche reeds gestart.
De VVD-fractie vraagt zich voorts af waarom er voor de titel «wet digitale overheid» is gekozen, in hoeverre de inhoud van de wet, na wijziging naar aanleiding van de consultatie, in overeenstemming is met de titel, alsmede waarom de titel is gewijzigd ten opzichte van de consultatieversie van het wetsvoorstel.
De oorspronkelijke titel van het wetsvoorstel, de «Wet generieke digitale infrastructuur (GDI)», was ingegeven door de wens bestaande en toekomstige publieke voorzieningen van de GDI van een wettelijke basis te voorzien. Gaandeweg de voorbereiding van het wetsvoorstel groeide het besef dat deze titel niet helemaal recht doet aan de aard en inhoud van de voorgenomen bepalingen. De huidige titel brengt beter tot uitdrukking waar het om gaat: regulering van het digitaal werkende openbaar bestuur, met inbegrip van de voorzieningen die daarvoor beschikbaar zijn, vanuit de gedachte dat dienstverlening in het publieke domein aan burgers en bedrijven veilig en betrouwbaar moet zijn.
De VVD-fractie vraagt aandacht voor de initiatiefnota van de leden Middendorp en Verhoeven over online identiteit en regie op persoonsgegevens (TK 34 993). Daarin wordt een online identiteit bij de digitale overheid voorgesteld door het combineren van: 1) een veilig inlogsysteem, 2) het plaatsen van geselecteerde persoonsgegevens in een digitale kluis, 3) een digitaal contactadres voor iedere Nederlander. Met

die drie componenten kan een online identiteit voor natuurlijke personen bij de digitale overheid worden gecreëerd. De leden van de VVD-fractie vragen in hoeverre het mogelijk is om met het onderhavige wetsvoorstel de in de initiatiefnota voorgestelde digitale kluis te introduceren, inclusief de verplichting van bestuursorganen en andere organen om deze kluis ook daadwerkelijk te gebruiken.
Over de wenselijkheid en haalbaarheid van de ideeën zoals voorgesteld in de initiatiefnota wordt momenteel van gedachten gewisseld met uw Kamer. Op een aantal punten is meer duidelijkheid gewenst over de precieze intenties en over de mogelijke realisatiewijze om te kunnen inschatten welke gevolgen de initiatiefnota heeft, bijvoorbeeld voor voorzieningen, systemen, capaciteit en kosten, alsmede om te kunnen bepalen welke wet- en regelgeving nodig is en in hoeverre het onderhavige wetsvoorstel daarvoor een basis zou kunnen bieden.
De leden van de CDA-fractie onderschrijven het uitgangspunt dat digitalisering mogelijkheden biedt voor betere overheidsdienstverlening. De CDA-fractie is met de Afdeling advisering van de Raad van State van mening dat toegang van burgers (en bedrijven) tot, en communicatie met de overheid, een basisrecht en een publieke verantwoordelijkheid is, die niet afhankelijk mogen worden van private partijen. De regering wordt verzocht nader in te gaan op dit uitgangspunt. Ook vraagt de CDA-fractie aandacht voor de positie van organisaties die niet vallen in de categorie burger of bedrijf.
De overheid zal voor burgers zelf identificatiemiddelen op meerdere betrouwbaarheidsniveaus uitgeven. Hiertoe is een zorgplicht voor de Minister van BZK in het wetsvoorstel opgenomen. Naast de invoering van deze publieke middelen, biedt het wetsvoorstel voor de Minister van BZK de mogelijkheid om een of enkele private middelen toe te laten, waarvan burgers gebruik kunnen maken bij het afnemen van overheidsdiensten. Er is dus geen sprake van afhankelijkheid van private partijen. Voor bedrijven zal geen publiek middel worden uitgegeven. Reden hiervoor is dat het huidige stelsel van private middelen voor bedrijven naar tevredenheid functioneert. Nut en noodzaak van een publiek middel ontbreken hier. Wel wordt met het wetsvoorstel het stelsel van private middelen voor bedrijven 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 toezicht ingericht en gelden er bepalingen inzake privacybescherming en misbruik. Het in het wetsvoorstel bepaalde inzake private middelen voor bedrijven heeft een brede reikwijdte en geldt ook voor andere organisaties. Het wetsvoorstel spreekt om die reden ook over «bedrijfs- en organisatiemiddel», daarmee doelend op het inloggen bij de overheid door een onderneming of rechtspersoon als bedoeld in de Handelsregisterwet 2007.
Voor wat betreft een recht op toegang tot en communicatie met de overheid kan ik u mededelen, dat ik voornemens ben in de Algemene wet bestuursrecht (Awb), naast de papieren weg, een aanspraak op digitaal zaken doen met de overheid op te nemen. Ook ben ik voornemens in meer algemene zin, dus los van digitale overheidsdienstverlening, een zorgplicht voor bestuursorganen op te nemen, welke strekt tot ondersteuning bij communicatie met de overheid, opdat toegang tot de overheid verder wordt vergemakkelijkt.
De CDA-fractie constateert dat in het wetsvoorstel het onderscheid tussen burger- en bedrijfs- en organisatiemiddelen qua online identiteit en universele oplossingen niet is opgeheven. Voor bedrijven en organisaties is er bijvoorbeeld nog steeds maar één privaat middel en publieke middelen kunnen niet privaat gebruikt worden en daarmee bijdragen aan

een «digital single market», die juist beoogd wordt met de eIDAS-verordening. De leden van de CDA-fractie vragen om hierop nader in te gaan.
Door in te loggen met het burgermiddel krijgen de dienstverleners de beschikking over het bsn van de inloggende persoon. Dienstverleners gebruiken echter het KvK- of RSIN-nummer om bedrijven te identificeren. Voor identificatie van rechtspersonen is daarom eHerkenning ontwikkeld. Voor zzp-ers is het bij sommige dienstverleners mogelijk om zowel in te loggen met publieke middelen als met eHerkenning. Het wetsvoorstel laat deze keuze ongemoeid. Het wetsvoorstel sluit aan bij de huidige praktijk. Afhankelijk van de ervaringen die worden opgedaan in het burger- en bedrijvendomein kan worden overwogen om deze domeinen verder te harmoniseren. Dit leidt dan mogelijk tot een aanvulling in een volgende tranche.
De leden van de CDA-fractie vragen voorts of de voorgestelde digitale infrastructuur aansluit bij de behoeften van de digitale samenleving, waarin de behoefte van de burger daadwerkelijk centraal wordt gesteld, waarbij de burger de generieke voorzieningen die hij al kent en gebruikt ook universeel kan gebruiken bij de overheid.
Het wetsvoorstel zorgt dat burgers en bedrijven overheidsbreed terecht kunnen met de door de Minister van BZK aangewezen middelen. Zij kunnen als gevolg van het wetsvoorstel met reeds bekende middelen, zoals DigiD en eHerkenning, digitaal zaken regelen bij overheidsorganisaties. Het gebruik van organisatiespecifieke inlogmethoden is niet langer toegestaan in het (semi)publieke domein behoudens uitzonderingsgevallen. Tot het gebruik van andere generieke voorzieningen door overheidsinstanties kan bij algemene maatregel van bestuur op basis van het wetsvoorstel worden verplicht.
Voorts constateert de CDA-fractie dat de Europese eIDAS-verordening bepaalt dat het vanaf september 2018 voor burgers en bedrijven mogelijk moet zijn om met de nationale, genotificeerde middelen in te loggen bij alle overheidsorganisaties binnen de EU. De leden van de fractie vragen zich af wat de stand van zaken is in de andere lidstaten, alsmede wat de stand van zaken is met betrekking tot het grensoverschrijdend gebruik van eID-middelen.
Sinds het van kracht worden van de eIDAS-verordening op 29 september 2018 is het voor Duitsers mogelijk om met hun eID-middel bij Nederlandse dienstverleners in te loggen. Dienstverleners werken hard aan het gereed maken van hun eigen dienstverlening hiervoor en een gestage groei in het aantal inlogpogingen geeft daar blijk van. In totaal zijn er nu zes EU-landen met een genotificeerd middel, te weten Duitsland, Kroatië, Estland, Luxemburg, Italië en Spanje. Naast Duitsland worden ook de verbindingen met deze landen gelegd. In Nederland wordt notificatie van inlogmiddelen voor bedrijven voorbereid (eHerkenning). Deze notificatie is volgens plan in 2019 afgerond. Aan de notificatie van publieke middelen voor burgers wordt eveneens gewerkt en deze zal naar verwachting in 2020 afgerond zijn.
De leden van de CDA-fractie constateren, dat er op het gebied van ICT en informatiebeveiliging reeds tal van audits bestaan. Deze leden vragen met welke externe audits op dit gebied medeoverheden op dit moment te maken hebben. De leden vragen zich af hoe zich hiertoe de aankondiging verhoudt dat de stand van zaken met betrekking tot de informatiebeveiliging controleerbaar of auditbaar moet zijn.
Vanaf 2018 leggen medeoverheden verantwoording af via de Eenduidige Normatiek Single Information Audit (ENSIA) methodiek. Doel hiervan is het verantwoordingsproces over informatieveiligheid van medeoverheden verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke planning & control-cyclus. Zo moeten medeoverheden over de Basisregistratie Personen (BRP), de elektronische infrastructuur gebruikt bij uitvoering van de taken op het gebied van werk

en inkomen (Suwinet), de Basisregistratie adressen en gebouwen (BAG), Basisregistratie grootschalige topografie (BGT), de Basisregistratie ondergrond (BRO) en DigiD verticaal verantwoording afleggen. De horizontale verantwoording aan de gemeenteraad vormt hiervoor de basis. Voor specifieke normen van die registraties vullen de medeoverheden een vragenlijst in (zelfevaluatie). Daarnaast dient er voor Suwinet en DigiD een audit plaats te vinden door een onafhankelijke auditor. Aldus is informatiebeveiliging controleerbaar. Met het onderhavige wetsvoorstel zal de DigiD-audit worden omgevormd tot een «toegang tot de digitale overheid audit». Deze sluit nauw aan bij de bestaande systematiek; de auditlast neemt niet toe. De genoemde zelfevaluaties en de Suwinet audit blijven daarnaast van toepassing. Hierdoor is informatiebeveiliging, en specifiek de beveiliging van de toegang tot elektronische diensten, controleerbaar. Zoals ik onlangs heb aangekondigd, wordt de systematiek van de zelfevaluaties geëvalueerd om tot een verbetering van de verantwoording te komen.

De leden van de CDA-fractie refereren aan het feit, dat informatieveiligheid bij het ontwerp van de toegang tot elektronische dienstverlening centraal staat (MvT blz. 2), alsmede «privacy by design» (MvT blz. 23). Zij vragen in dit verband waar het gebruikersgemak is gebleven en of de ontsluiting ook vormgegeven wordt met het oog op de gebruiker.
Privacy, beveiliging en gebruiksvriendelijkheid zijn communicerende vaten en aspecten die onderling gewogen moeten worden. Bij een middel dat veilig is, maar op een zodanige manier is vormgegeven dat het moeilijk te gebruiken is, zal het gebruik ervan achterblijven. Om als privacy maatregel effect te kunnen hebben en uiteindelijk snel een belangrijke bijdrage te kunnen leveren in breder verband (privacybescherming bij dienstaanbieders) is het belangrijk dat het eID stelsel werkbaar is in termen van gebruikersgemak. Dat heeft een positief effect op het gebruik en adoptiesnelheid. Gebruiksvriendelijkheid en laagdrempelige toepasbaarheid is voor zowel burgers als overheden een belangrijk uitgangpunt. Dat geldt zowel voor het gebruik door burgers als de wijze waarop aansluiting door overheidsorganisaties kan worden gerealiseerd. Het past ook in het beleidskader NL DIGIbeter, waarin inclusie, zorgen dat iedereen kan meedoen, een speerpunt is.

De leden van de CDA-fractie vragen welke stappen worden gezet om de ambitie te verwezenlijken, dat in 2020 in beginsel alle actieve DigiD-gebruikers kunnen beschikken over een elektronisch identificatiemiddel op het betrouwbaarheidsniveau substantieel of hoog. De CDA-fractie vraagt zich voorts af welke lasten het wetsvoorstel voor de actieve DigiD-gebruikers meebrengt.

De regering heeft de ambitie om te bevorderen dat in 2020 in beginsel alle actieve DigiD-gebruikers – thans ruim 13,5 miljoen burgers – kunnen beschikken over een elektronisch identificatiemiddel op het betrouwbaarheidsniveau substantieel of hoog. De huidige oplossingen voor DigiD substantieel bereiken thans niet de totale gewenste doelgroep. 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. Ik zoek doorlopend naar mogelijkheden en alternatieven voor deze doelgroep, alsmede welke bruikbare alternatieven er zijn voor het aanschaffen van een kaartlezer. Zowel het onderzoek naar de mogelijkheden voor het tijdelijk opwaarderen van de DigiD-app naar het niveau substantieel op niet-Android smartphones als het verkennen van andere mogelijkheden vallen daaronder. De verwachting is desondanks dat niet op de hele korte termijn de beoogde doelgroep bereikt zal kunnen worden. Om een groot deel van de doelgroep snel een alternatief identificatiemiddel op niveau substantieel te kunnen bieden start ik daarom op korte termijn een aanbesteding voor een privaat middel op niveau substantieel.

De geleidelijke introductie van DigiD op betrouwbaarheidsniveau hoog is reeds gestart met de uitgifte van daarvoor geschikte rijbewijzen. Samen met sectoren waarin vraag is naar het hoogste betrouwbaarheidsniveau, zoals die sectoren waarin medische persoonsgegevens worden verwerkt, werk ik aan de verdere invoering. Op dit moment wordt tevens gewerkt aan de beschikbaarheid van DigiD hoog op de Nederlandse identiteitskaart. Daarnaast wordt tevens bezien of private alternatieven op niveau hoog kunnen worden ingezet. Wat de kosten (leges) voor burgers concreet zullen zijn zal in grote mate afhangen van gekozen oplossingen. Het streven is daarbij uiteraard deze kosten zo beperkt mogelijk te houden. In de loop van 2019 is hierover naar verwachting meer bekend.
De CDA-fractie constateert terecht dat het wetsvoorstel op verschillende punten de grondslag biedt voor nadere uitwerking in een algemene maatregel van bestuur. Gevraagd wordt of hierop een voorhangprocedure van toepassing is, en zo nee, waarom niet.
Een voorhangprocedure bij deze amvb's was aanvankelijk niet voorzien. Reden hiervan is dat de kaders ter zake in het wetsvoorstel zijn opgenomen en worden toegelicht in de memorie van toelichting. Door deze wijze van delegatie, die in lijn is met het uitgangspunt van het primaat van de wetgever, kan vroegtijdig(e) inzicht en betrokkenheid door uw Kamer gerealiseerd worden. Voor de verplichte amvb's, te weten die inzake informatieveiligheid en persoonsgegevens (uitwerking van de voorgestelde artikelen 4 en 16) en inzake bedrijfs- en organisatiemiddelen en bijbehorende diensten (uitwerking van de voorgestelde artikelen 11–13 en 22) zal ik echter toch een voorhangprocedure hanteren, omdat deze een zwaartepunt in de uitvoering vormen. Ik zal hiertoe bij nota van wijziging een voorhangprocedure in het wetsvoorstel opnemen.

De leden van de DENK-fractie leden vragen zich af, of Nederland goed genoeg ontwikkeld is om over te gaan op digitaal stemmen.
De Minister van BZK heeft in haar brief van 15 juni jl. (TK 2017–2018, 33 829 nr 83) aangegeven dat ons stemproces nu niet kwetsbaar is voor digitale dreigingen. Het kabinet wil, gelet op de dreigingen die thans worden onderkend, dergelijke kwetsbaarheden ook niet in het stemproces introduceren. Wel wil het kabinet stappen zetten naar het elektronisch tellen van de stembiljetten. Om elektronisch te kunnen tellen is een ander stembiljet nodig. De Minister van BZK heeft uw Kamer toegezegd begin 2019 concrete voorstellen te zullen doen voor een nieuw stembiljet zodat uw Kamer zich daarover kan uitspreken.

2. Standaarden

De leden van de VVD-fractie stellen terecht vast, dat het wetsvoorstel een grondslag bevat om bij algemene maatregel van bestuur open standaarden aan te wijzen die overheden dienen te hanteren in het elektronisch verkeer met andere overheden, met burgers en met bedrijven. Ingevolge artikel 3, tweede lid, kan een standaard bij algemene maatregel van bestuur worden aangewezen. Dit is een niet-imperatieve bepaling. De VVD-fractie vraagt zich af, waarom is gekozen voor een niet-imperatieve bepaling als een generieke digitale infrastructuur wenselijk is. De CDA-fractie constateert in aansluiting hierop dat het «pas toe of leg uit»-principe voor bepaalde open standaarden het meest proportionele instrument blijft. Echter, voor sommige standaarden is het bevorderen van het gebruik onvoldoende en moeten overheidsorganisaties de standaard eenvoudigweg toepassen. De leden van de CDA-fractie vragen of de regering dit onderscheid nader kan toelichten en welke afweging bij het besluit om open standaarden op te leggen wordt gemaakt. Voorts vragen de leden van de CDA-fractie op welke termijn de regering van plan is gebruik te maken van deze mogelijkheid.

Het open karakter van standaarden betekent dat deze algemeen kenbaar en beschikbaar zijn. De term «open» staat los van toepassing. Kabinetsbeleid is dat open standaarden worden toegepast, tenzij een overheidsorganisatie goede reden heeft om dat niet te doen (zogeheten «pas toe of leg uit»). Met dit wetsvoorstel (artikel 3) wordt er in voorzien dat in bepaalde gevallen de toepassing van open standaarden wordt verplicht. Bij algemene maatregel van bestuur wordt dan toepassing voorgeschreven wanneer dat noodzakelijk en proportioneel is gelet op de goede werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid of de doelmatigheid van het elektronische verkeer, dan wel noodzakelijk is ter uitvoering van internationaal of Europees recht. Of hiervan sprake is zal door mij per geval worden bezien in nauwe samenwerking met de andere departementen, wiens organen (zoals uitvoeringsorganisaties) betrokken zijn. Alleen indien de noodzaak tot aanwijzing vaststaat en de standaard in een amvb wordt opgenomen, is deze voor de organen waarvoor deze geldt (generiek) van toepassing en mogen zij hiervan niet (langer) afwijken. De regering heeft het voornemen om als eerste de open standaard HTTPS te verplichten. De amvb die daarin voorziet wordt momenteel voorbereid en zal naar verwachting worden vastgesteld (kort) nadat de wet in werking is getreden.
De VVD-fractie vraagt zich in dit verband af, of een bij amvb aangewezen standaard voor alle organen, zoals genoemd in artikel 2 van de wet, geldt, of dat de standaard per orgaan kan verschillen. De leden vragen in hoeverre dat laatste voor de hand ligt vanuit het oogpunt van eenduidigheid en duidelijkheid van de generieke digitale infrastructuur.
Het kabinet zal per geval bezien wat het benodigde functionele toepassingsbereik van de aan te wijzen standaard is, alsmede voor welke organen de verplichting tot toepassing noodzakelijk is. Het voorgestelde artikel 3, derde lid, maakt in dit verband differentiatie mogelijk. Wanneer eenduidigheid en generieke toepassing dit vereisen, zal evenwel een ruime (functionele en/of personele) werkingssfeer in de desbetreffende amvb worden verankerd. Niet altijd is een standaard voor ieder orgaan relevant.
De VVD-fractie vraagt zich voorts af, of de Kamer wordt geïnformeerd als wordt overgegaan tot het vaststellen van een algemene maatregel van bestuur.
Het voornemen tot aanwijzing van een standaard zal worden gepubliceerd in het kader van (internet)consultatie. Een ieder kan van het voornemen kennis nemen en hierop reageren. De verkregen input wordt in het verdere voorbereidingsproces van de amvb meegenomen. Vanzelfsprekend ben ik te allen tijde bereid middels een technische briefing inzicht te geven in de (technische) uitvoeringsdetails.
De VVD-fractie heeft een aantal vragen over hetgeen het wetsvoorstel regelt met betrekking tot de overheidshuishouding als het gaat om persoonsgegevens. Zij vragen zich af wat de rijksoverheid met deze wet kan opleggen als het gaat om bronnen waar gegevens opgeslagen worden, bijvoorbeeld het gebruik van één bron voor (bepaalde) persoonsgegevens.
Het wetsvoorstel laat onverlet dat de vigerende regels ten aanzien van de verwerking van persoonsgegevens door overheidsorganisaties van toepassing zijn. Voor de omgang met persoonsgegevens geldt voor overheidsorganisaties het kader van de AVG, de Uitvoeringswet AVG en domeinspecifieke (privacy)wetgeving. Dit geldt ook voor de eenmalige uitvraag van gegevens. Dit wetsvoorstel raakt de overheidshuishouding in zoverre, dat het voorstel eisen stelt aan identificatie van burgers als zij zaken doen met de overheid of als door de overheid inzage wordt gegeven in hun informatie, waaronder hun persoonsgegevens. Hierdoor wordt bijgedragen aan de bescherming van persoonsgegevens bij deze organisaties.

Het is de leden van de VVD-fractie opgevallen dat veel zaken bij algemene maatregel van bestuur worden bepaald en dat ook sprake is van ministeriële regelingen en beleidsregels. De VVD-fractie vraagt zich af of er een overzicht kan worden gegeven van de onderwerpen die bij algemene maatregel van bestuur, ministeriële regeling dan wel beleidsregels nader worden uitgewerkt.
Het wetsvoorstel behoeft op onderdelen nadere uitwerking. Het wetsvoorstel bevat hiertoe een aantal delegatiebepalingen. Het gaat daarbij om de volgende uitvoeringsregelgeving:

- Amvb informatieveiligheid en persoonsgegevens, uitwerking van artt. 4 en 16 WDO;
- Regeling classificering betrouwbaarheidsniveaus, uitwerking van art. 6 WDO;
- Regeling gebruik(svoorschriften), uitwerking van art. 10 WDO;
- Amvb bedrijfs- en organisatiemiddelen en bijbehorende diensten, uitwerking van artt. 11- 13 en 22 WDO;
- Regeling bekostiging, uitwerking van artt. 20–21 WDO;
- Regeling aansluiting, uitwerking van art. 29 WDO.
- Beleidsregels toelating, uitwerking van art. 9 WDO.

Daarnaast zijn op enkele onderdelen nadere regels mogelijk; hiertoe zijn «kan» bepalingen opgenomen. Deze zijn in het bovenstaande overzicht niet meegenomen, omdat nog niet duidelijk is in hoeverre, op welke wijze en op welke termijn hiervan gebruik gaat worden gemaakt.

De leden van de CDA-fractie constateren dat overheidsorganisaties binnen het Rijk bij aanschaf of (ver)bouw van ICT-systemen de open standaarden hanteren, die op de zogeheten «pas toe of leg uit»-lijst staan. Afwijken van deze verplichting mag alleen in geval van zwaarwegende redenen; verantwoording hierover moet worden afgelegd in het jaarverslag. De leden van de CDA-fractie vragen hoe deze verantwoording achteraf zich verhoudt tot de zorgplicht van de Minister. De leden vragen of de bedoelde afweging niet gemaakt zou moeten worden in goed overleg, mede in verband met de constatering dat rond de adoptie van open standaarden er in jaarverslagen onvoldoende verantwoord wordt waarom het tempo op dat vlak laag ligt.

Het open standaardenbeleid geeft overheidsorganisaties de vrijheid 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. Dat is bewust, omdat organisaties doorgaans zelf het beste in staat zijn een afweging te maken inzake het al dan niet toepassen van standaarden. Zij kunnen daardoor bijvoorbeeld hun eigen investeringsmoment bepalen. Het zou te ver voeren om overheidsorganisaties te vragen om bij afwijking vooraf de Minister te consulteren. Daarmee zou een complex en uitgebreid systeem in het leven worden geroepen en worden onnodige interbestuurlijke lasten veroorzaakt die niet opwegen tegen de maatschappelijke baten. Wanneer de adoptie achterblijft, wordt op mijn verzoek door het Forum Standaardisatie ingezet op het voeren van gesprekken, het geven van voorlichting en waar nodig het interveniëren op hoogbestuurlijk niveau, zoals via het Overheidsbreed Beleidsoverleg Digitale Overheid. Met dit wetsvoorstel kan indien nodig gebruik worden gemaakt van de mogelijkheid die artikel 3 biedt en kunnen overheidsorganisaties tot toepassing worden verplicht.

De leden van de CDA-fractie vragen wat de stand van zaken is met betrekking tot de afspraken tussen overheden. Deze leden constateren dat de afspraken in het kader van het Nationaal Beraad Digitale Overheid een geldigheid hadden tot eind december 2017.

De afspraak zoals gemaakt door het Nationaal Beraad Digitale Overheid was erop gericht beter te voldoen aan een aantal standaarden. In 2,5 jaar tijd is hierdoor voor deze standaarden de gemiddelde adoptiegraad onder overheden toegenomen van 35% naar meer dan 80%. De opvolger van het Nationaal Beraad, het Overheidsbreed Beleidsoverleg Digitale Overheid, heeft begin 2018 de ambitie uitgesproken om de achterblijvers alsnog over de streep te trekken. In de meest recente meting van eind september 2018 is de gemiddelde adoptie verder gestegen naar 87%. Via de koepels zullen de achterblijvers worden aangesproken en zo nodig geholpen worden om alsnog te voldoen aan de streefbeeldafspraak. Aanvullend op de streefbeeldafspraak uit 2017 zijn er begin 2018 twee nieuwe streefbeeldafspraken gemaakt: naast het over de streep halen van de restgroep van de afspraak uit 2017, is er een afspraak gemaakt om de standaard HTTPS uiterlijk eind 2018 op alle overheidssites te hebben toegepast en conform NCSC advies te hebben geconfigureerd. Uiterlijk eind 2019 moeten overheidsorganisaties de anti-phishing e-mail standaarden (DKIM/SPF/DMARC) en de standaarden tegen meeluisteren van e-mail (STARTTLS en DANE) hebben toegepast. Verder wordt de adoptie van de informatieveiligheidstandaarden halfjaarlijks gemonitord. De laatste meting dateert van september. Onlangs heb ik in een brief aan uw kamer aangekondigd dat begin volgend jaar wordt bezien in hoeverre de implementatieafspraken zijn behaald en of meer harde verplichtingen opportuun zijn om de veiligheid van digitale communicatie met de overheid via web en e-mail te bevorderen.

De leden van de CDA-fractie vragen hoe het gebruik van de verplichte standaarden jaarlijks zal worden gemonitord.

De adoptie van de «pas toe of leg uit»-lijst wordt jaarlijks gemeten door het Bureau Forum Standaardisatie. Wanneer bij amvb open standaarden verplicht worden gesteld, zal het gebruik daarvan eveneens in de monitoring door het Bureau Forum Standaardisatie meelopen.

De leden van de D66-fractie vragen welke overheidsinformatie op dit moment vastgelegd is middels software die gebruik maakt van gesloten standaarden. De D66-fractie vraagt of snel zal worden toegewerkt naar volledige open standaarden middels de te introduceren wettelijke basis. Voorts vraagt de D66-fractie voor welke standaarden in welke domeinen dit onmogelijk wordt geacht en of het kan voorkomen dat indien bepaalde open standaarden verplicht worden, contracten met particuliere softwareverleners opgezegd moeten worden en welke kosten dit met zich mee brengt. Dit zou met name een probleem kunnen zijn bij overheidsinstanties die nog een slag te maken hebben wat open standaarden betreft, zoals waterschappen.

Momenteel wordt niet gemeten welke overheidsinformatie is vastgelegd met open standaarden. Wel wordt gemeten in hoeverre overheden voldoen aan standaarden van de «pas toe of leg uit»-lijst bij aanbestedingen en wordt in de toekomst de naleving gemonitord van de standaarden die verplicht zijn bij amvb. Kabinetsbeleid is het toepassen van open standaarden om te voorkomen dat de rechtszekerheid wordt bedreigd, de informatieveiligheid wordt ondermijnd, de kosten te hoog zijn, de leveranciersafhankelijkheid te groot is of de archivering van documenten en gegevens gevaar loopt. Op voorhand zie ik geen sector waar het principieel onmogelijk zou zijn om open standaarden toe te passen. Of er wrijving optreedt, en hoe groot deze is, is evenwel afhankelijk van het soort standaard. De impact van het verplicht stellen van een standaard zal per geval in kaart worden gebracht. Onder andere worden dan de kosten van het verplicht stellen en eventuele aanpassingen van software onderzocht. Het is denkbaar dat contractvoorwaarden aangepast

moeten worden. Per voorgenomen amvb wordt bekeken of een overgangsperiode in de rede ligt om de overstap naar het werken met een verplichte standaard mogelijk te maken. Bovendien zal de voorgenomen amvb breed ter consultatie worden voorgelegd, opdat op uitvoerbaarheid kan worden getoetst.

De leden van de CDA-fractie vragen zich voorts af op welke wijze besloten wordt om een open standaard verplicht te stellen en aan welke voorwaarden moet worden voldaan. Ook vraagt de CDA-fractie zich af, hoe vervolgens wordt gecontroleerd of dit daadwerkelijk opgevolgd wordt door de overheidsinstanties.

Verplichte toepassing door overheidsinstanties, oftewel het niet langer mogelijk maken van de «leg uit-optie», is het «ultimum remedium» van het openstandaardenbeleid. Verplichtstelling wordt door mij, in samenspraak met de andere betrokken departementen, overwogen wanneer de goede werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid of de doelmatigheid van het elektronisch verkeer in gevaar komen. Artikel 3 van het wetsvoorstel bevat de voorwaarden waaraan moet worden voldaan, wil een open standaard verplicht kunnen worden gesteld. Het voornemen tot aanwijzing van een standaard zal worden gepubliceerd in het kader van (internet)consultatie. Een ieder kan hiervan kennis nemen en reageren. De verkregen input wordt in het verdere voorbereidingsproces van de amvb meegenomen. Het (interbestuurlijke) toezicht op de naleving vindt plaats binnen de eigen beleidskolom. Hiertoe wijst de Minister die het aangaat toezichthoudende ambtenaren aan.

De leden van de D66-fractie lezen dat de regering van plan is bij amvb de Europese toegankelijkheidsnorm EN 201 549 toe te passen als standaard en vragen of de regering kan toelichten op welke wijze dit websites in de publieke sector toegankelijker maakt.

De Europese toegankelijkheidsnorm EN 301549 is verankerd in de Webtoegankelijkheidsrichtlijn (EU-richtlijn nr 2016/2102). Deze richtlijn is omgezet in het (Tijdelijk) Besluit digitale toegankelijkheid overheid. Omdat de omzetting in nationale regelgeving voor 23 september 2018 diende plaats te vinden, is deze amvb vooruitlopend op inwerkingtreding van de onderhavige wet op 1 juli 2018 van kracht geworden. Na inwerkingtreding zal de wet de grondslag gaan vormen voor het Besluit digitale toegankelijkheid overheid. Verplichte toepassing van norm EN 301549 – die gebaseerd is op de wereldwijd geaccepteerde toegankelijkheidsstandaard WCAG 2.0/2.1 – houdt in dat overheidsinstanties de noodzakelijke maatregelen moeten treffen om hun websites en mobiele applicaties toegankelijker te maken. Ze zijn verplicht hierover onderbouwd verantwoording af te leggen in een openbare toegankelijkheidsverklaring. In gevallen waarbij (nog) niet kan worden aangetoond dat aan alle eisen uit EN 301549 wordt voldaan moet in de toegankelijkheidsverklaring voor elke niet nageleefde eis worden aangegeven wat daarvan de oorzaak is, wat het gevolg is voor mensen met een functiebeperking, of een alternatief beschikbaar is, welke maatregelen de overheidsinstantie neemt om in de toekomst wel te gaan voldoen en een planning wanneer de maatregelen zullen zijn uitgevoerd. Dit wordt door mij gemonitord.

Voorts zijn de leden van de D66-fractie zeer positief over het verplichten van de HTTPS en TLS standaard op basis van dit wetsvoorstel en vragen wanneer aan dit voornemen gevolg zal worden gegeven.

Het verheugt mij dat de fractie D66-steun uitspreekt voor het verplicht stellen van de HTTPS en TLS standaard. Het voornemen is om een amvb die tot toepassing van deze open standaarden verplicht, vast te stellen (kort) nadat de onderhavige wet in werking is getreden.

De leden van de DENK-fractie lezen in par. 2.6. MvT maatregelen om fraude te voorkomen. Zij constateren dat uit nieuwsberichten blijkt dat elektronisch stemmen niet perfect te beveiligen is en dat de genoemde maatregelen ook niet waterdicht zijn. De DENK-fractie vraagt zich af, of dit systeem niet te onveilig is om gebruikt te worden. De leden vragen zich af, hoe actueel en veilig de software is die gebruikt wordt in geval van elektronische verkiezingen. De leden van de DENK-fractie vragen zich voorts af, hoe bestendig de software is tegen mogelijke cyberaanvallen. De DENK-fractie vraagt zich ten slotte af, of het niet verstandiger is om op block-chain technologie te wachten alvorens over te gaan op digitaal stemmen.

In Nederland wordt niet elektronisch gestemd. De Ondersteunende Software Verkiezingen (OSV) wordt niet gebruikt bij het stemmen en ook niet bij het tellen van de stembiljetten. Dat gebeurt handmatig. OSV wordt gebruikt bij het aggregeren van de tellingen met als doel de totaaluitslag en de zetelverdeling uit te rekenen. De Minister van BZK heeft in haar brief van 15 oktober jl. uw Kamer gemeld dat de Kiesraad, in wiens opdracht de OSV is ontwikkeld, blijft investeren in verdere verbeteringen. Het Ministerie van BZK biedt de Kiesraad alle mogelijke ondersteuning die de Raad daarbij wenst. Dat geldt zowel voor het verbeteren van programmatuur voor de komende verkiezingen als, zou de Kiesraad daartoe besluiten, voor de vernieuwing ervan voor de langere termijn. De Kiesraad werkt nu concreet aan een aantal verbeteringen in OSV ten behoeve van de verkiezingen van 2019. De Kiesraad betrekt externe beveiligingsdeskundigen daarbij om mogelijke (nieuwe) kwetsbaarheden in kaart te brengen en om te kunnen beoordelen welke maatregelen daar effectief tegen getroffen kunnen worden. De Kiesraad neemt daarin uiteraard de kwetsbaarheden mee die eerder door een aantal instanties/personen zijn gesignaleerd. Daarbij moet gedacht worden aan bijvoorbeeld de encryptie, de data-integriteit en beveiligingsupdates. De Kiesraad en het Ministerie van BZK zullen in de komende weken met de externe beveiligingsdeskundigen ook bepalen of het nodig is aanpassingen door te voeren in de instructies die de gemeenten krijgen voor het gebruik van OSV bij de verkiezingen. Ik memoreer tevens dat recent een wetsvoorstel is ingediend bij uw Kamer om het mogelijk te maken dat de processenverbaal en de opgave van de burgemeesters op het internet openbaar gemaakt worden. Dat is een belangrijke stap om de controleerbaarheid en transparantie van het berekenen van de uitslag te vergroten.

3. Elektronische identificatie (eID)

De leden van de VVD-fractie constateren dat met het wetsvoorstel de mogelijkheid wordt gecreëerd om één of meerdere door private partijen uitgegeven identificatiemiddelen te laten fungeren als een gelijkwaardige elektronische toegangsvoorziening bij dienstverlening van de overheid. Zij vragen zich af, in hoeverre er sprake is van een multimiddelenstrategie en in hoeverre het beleid er op gericht is om privaat uitgegeven inlogmiddelen daadwerkelijk toe te laten. Het komt de leden van de VVD-fractie voor dat er nu sprake is van een «overheidsmiddel plus terugvaloptie»-strategie. De VVD-fractie meent dat er veel meer zekerheid zou moeten worden gegeven aan de private aanbieders en vragen zich af, in hoeverre dat in het wetsvoorstel verankerd is. Zij vragen zich voorts af, wat in het wetsvoorstel moet worden opgenomen om dat voor elkaar te krijgen.

De centrale doelstelling in het wetsvoorstel is om ervoor te zorgen dat er identificatiemiddelen op hogere betrouwbaarheidsniveaus continu beschikbaar zijn. Burgers moeten veilig en ongestoord zaken kunnen doen met de overheid. Om dat snel voor elkaar te krijgen is het noodzakelijk dat een of meerdere alternatieven voor het huidige middel met een hoge dekkingsgraad beschikbaar komen. Burgers kunnen dan ook een privaat middel als hun primaire inlogmiddel gebruiken; dat zal dus niet slechts een terugvaloptie voor het publieke middel zijn. Om dat te realiseren maakt het wetsvoorstel het mogelijk om een of meerdere private identificatiemiddelen toe te laten. Op dit moment wordt een aanbesteding voorbereid om in dit kader één of meerdere private authenticatiemiddelen te verwerven, waarbij de markt vooraf duidelijkheid wordt geboden over de opdracht. In lijn met de doelen in NL DIGIbeter wil ik daarbij oog hebben voor innovatieve dienstverlening. Het kan dus zijn dat er in de toekomst meerdere (dus: publieke en private) middelen te gebruiken zijn door burgers, maar een multimiddelenstrategie of het creëren van een markt daarvoor is geen doel in zichzelf.
Voorts vragen de leden van de VVD-fractie hoe het aanwijzen van een privaat identificatiemiddel als toegelaten identificatiemiddel gaat. Zij vragen zich af waarom is gekozen voor aanbesteden via de Aanbestedingswet en niet voor accreditatie.
De aanwijzing van een privaat middel als toegelaten identificatiemiddel komt tot stand via een openbare aanbesteding. Op basis van de mate waarin voldaan wordt aan de aanbestedingscriteria kan een middel worden aangewezen. Van een besluit tot toelating van een middel wordt mededeling gedaan door plaatsing in de Staatscourant waarbij het betrouwbaarheidsniveau van het betreffende middel wordt vermeld. Door middel van de procedure conform de Aanbestedingswet 2012 kan het Ministerie van BZK verplichte levering afdwingen, alsmede de private partij op aspecten zoals betaalbaarheid en dekkingsgraad selecteren. De keuze voor accreditatie zou meebrengen dat de private leverancier wel gerechtigd maar niet verplicht is om te leveren. Deze onzekerheid is voor de gebruiker van de middelen en voor de publieke dienstverleners ongewenst, alsmede conflicterend met het belang van het realiseren van een betrouwbaar alternatief voor DigiD om de continuïteit van dienstverlening te waarborgen. Tevens zou de keuze voor accreditatie kunnen leiden tot de toelating van een onbeperkt aantal private authenticatiemiddelen, wat de ontzorging van dienstverleners, en daarmee de uitvoerbaarheid, niet ten goede komt.
Voorts vraagt de VVD-fractie zich af in hoeverre de onafhankelijke toezichthouder een certificerende instelling wordt die een level playing field organiseert voor private en publieke middelen of dat het meer een voorportaal voor een aanbestedingsprocedure is. De VVD-fractie vraagt of het de bedoeling is dat mensen in de toekomst met een «dropdown-menu» uit private en publieke aanbieders kunnen kiezen om in te loggen bij de overheid. Ook vragen de leden van de VVD-fractie zich af, hoe ver private partijen zijn in het ontwikkelen van dergelijke middelen.
De Minister van BZK zal toezichthoudende ambtenaren aanwijzen om te controleren of leveranciers van erkende middelen en diensten aan de eisen voldoen, zowel op het moment van de aanbesteding als in een later stadium. Certificeren of het organiseren van een «level playing field» is geen taak van de toezichthoudende ambtenaren. Zij faciliteren de Minister van BZK bij het toelaten van burgermiddelen en het erkennen van bedrijfs-en organisatiemiddelen, alsmede de eventuele intrekking daarvan. Private partijen ontwikkelen middelen die mogelijk aan de betrouwbaarheidseisen voldoen. De marktconsultatie heeft dit bevestigd. Indien private middelen worden toegelaten door BZK naast het publieke middel, is een «dropdown-menu» een voor de hand liggende technische wijze om de opties aan gebruikers te presenteren. Het hangt dan van de voorkeur van de burger af in welke mate het middel gebruikt wordt.

Met betrekking tot de reikwijdte van de bestuursorganen waar het wetsvoorstel betrekking op heeft, zo lezen de leden van de VVD-fractie, geldt de wet in de eerste plaats voor zgn. «a-bestuursorganen», voor zover zij elektronische diensten ter uitvoering van een publieke taak, in het algemeen belang of anderszins, waarbij het bsn wordt verwerkt, verlenen. Daarnaast geldt de wet ook nog voor andere organen en bepaalde aangewezen organisaties. De VVD-fractie vraagt zich af, of gesteld kan worden dat het in alle gevallen gaat om organen en organisaties die een taak uitoefenen in het kader van het domein van het bsn.
Het gestelde is juist. Het wetsvoorstel richt zich tot organen en organisaties die elektronische diensten verlenen aan natuurlijke personen, ondernemingen of rechtspersonen ter uitoefening van een publieke taak, in het algemeen belang of anderszins waarbij het bsn wordt verwerkt.
De leden van de VVD-fractie constateren dat in de bijlage bij het wetsvoorstel categorieën van instanties worden aangewezen waarvoor de wet straks geldt. Zij vragen zich af in hoeverre wordt overwogen om daar categorieën aan toe te voegen. Voorts vragen zij zich af of de wet moet worden gewijzigd als er daadwerkelijk categorieën worden toegevoegd.
Op dit moment wordt niet overwogen nieuwe categorieën organisaties aan te wijzen. Als het in de toekomst in de rede zou liggen categorieën toe te voegen, behoeft de wet niet te worden gewijzigd. Ingevolge artikel 2, vierde lid, van het wetsvoorstel kan de bijlage bij de wet bij algemene maatregel van bestuur worden gewijzigd en kunnen categorieën van organisaties aan de bijlage worden toegevoegd.
De VVD-fractie vraagt zich af wat de betekenis is van het in de memorie van toelichting gestelde dat toegelaten publieke middelen «in beginsel» uitsluitend worden gebruikt voor de toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties.
Publieke middelen zijn bedoeld voor gebruik in het publieke domein, dat wil zeggen voor het afnemen van elektronische diensten van bestuursorganen en aangewezen organisaties, zijnde instanties die ter uitoefening van een publieke taak, in het algemeen belang of anderszins het bsn verwerken. Op deze hoofdregel bestaat, onder strikte voorwaarden, een tweetal uitzonderingen. Ingevolge artikel 8, tweede lid, van het wetsvoorstel kan bij ministeriële regeling worden bepaald dat een publiek middel tevens kan worden gebruikt voor de toegang tot daarbij bepaalde private of commerciële diensten van aangewezen organisaties (gecombineerde elektronische dienstverlening). Het betreft specifiek omschreven aangewezen organisaties, bijvoorbeeld zorgverzekeraars en zorgverleners, voor specifiek omschreven diensten anders dan diensten ter uitoefening van een publieke taak, in het algemeen belang of waarbij het bsn wordt verwerkt. Voorts is het, ingevolge het voorgestelde artikel 8, derde lid, mogelijk bij ministeriële regeling te bepalen dat een publiek middel tevens kan worden gebruikt ten behoeve van aangewezen organisaties voor het verlenen van toegang tot een intern (gesloten) systeem voor de elektronische uitwisseling van gegevens waarbij het bsn wordt verwerkt, zoals dat bijvoorbeeld binnen en tussen zorginstellingen bestaat voor het onderling uitwisselen van medische gegevens. In de bovenstaande gevallen gelden vanzelfsprekend alle regels van het wetsvoorstel, waaronder die met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot de desbetreffende diensten en met betrekking tot toezicht.
De leden van de VVD-fractie vragen om een nadere verduidelijking van de functie van de routeringsvoorziening, inzicht in de kosten en de planning daarvan, alsmede een uitleg van het begrip «koppelvlak».
Tijdens de consultatie van het wetsvoorstel hebben dienstverleners aangegeven ontzorgd te willen worden ter zake van de verplichting tot acceptatie van c.q. aansluiting op publieke en private middelen. Daarom is besloten tot realisering van een zogeheten routeringsvoorziening, die als doel heeft het ontzorgen van dienstverleners door het leveren van één

aanspreekpunt, één contract, één factuur en één (technisch) koppelvlak. In de loop van 2019 zullen dienstverleners op deze voorziening worden aangesloten. De verwachte kosten zijn opgenomen in de business case en bedragen naar verwachting enkele miljoenen, door te rekenen aan de ervan gebruikmakende dienstverleners. De verwachte opslag op een authenticatietransactie is in de orde van enkele eurocenten. Een koppelvlak, ook wel interface (schakel) genoemd, verzorgt volgens bepaalde standaarden de uitwisseling van gegevens tussen informatiesystemen, waardoor deze systemen met elkaar kunnen communiceren. Een koppelvlak zet dus informatie van het ene systeem om in begrijpelijke en herkenbare informatie van een ander systeem.
De CDA-fractie vraagt naar voorbeelden om inzichtelijk te maken hoe bestuursorganen en aangewezen organisaties hun elektronische diensten classificeren op onderscheidenlijk het betrouwbaarheidsniveau substantieel of hoog.

De diensten die door overheidsorganisaties worden geleverd zijn divers. Dat geldt ook voor de behoefte aan digitale identiteitsvaststelling daarvoor en de mate van zekerheid die nodig is gelet op het te beschermen belang. Over het algemeen geldt dat hoe hoger het betrouwbaarheidsniveau van een identificatiemiddel is, hoe meer controles en stappen moeten worden doorlopen. Deze controles volgen uit de eIDAS-verordening, die daaraan op Europees niveau regels stelt. Dat betekent over het algemeen: hoe hoger het betrouwbaarheidsniveau, hoe kostbaarder en wat minder eenvoudig in het gebruik. De systematiek van de regels die worden gesteld aan de inzet van betrouwbaarheidsniveaus, en de kaders die daaromtrent in de uitvoeringsregelgeving zullen worden uitgewerkt, is vergelijkbaar met de afwegingen die in informatiebeveiliging in het algemeen gangbaar zijn en die ook in de AVG worden gehanteerd. Wat redelijk is om in te zetten als betrouwbaarheidsniveau hangt dan af van het soort dienstverlening, de gegevens die worden ontsloten en de overige controlestappen die door de overheidsdienstverlener worden ingebouwd. Voorbeeld van een proces dat op niveau substantieel kan plaatsvinden is bijvoorbeeld een vergunningaanvraag bij een gemeente, waar bij de aanvraag geen gegevens worden verstrekt en voor de verlening nog tal van controlestappen zullen volgen. Anders is dat voor de toegang tot gezondheidsgegevens waarop een medisch beroepsgeheim rust. Als deze informatie na inloggen digitaal wordt ontsloten is de mate van zekerheid die nodig is over de identiteit van de patiënt van zeer groot belang, en zal betrouwbaarheidsniveau hoog noodzakelijk zijn. Overigens zal ik bij het opstellen van de uitvoeringsregelgeving rekening houden met de thans veelgebruikte «handreiking betrouwbaarheidsniveaus» van het Forum Standaardisatie. Door daarop aan te sluiten beoog ik zoveel mogelijk aan te sluiten bij de (nu nog vrijblijvende) huidige praktijk en de overgang naar de nieuwe situatie zo eenvoudig mogelijk te maken.

De leden van de CDA-fractie constateren dat in het wetsvoorstel het uitgangspunt is opgenomen, dat publieke middelen niet buiten het (semi)publieke domein worden gebruikt. De CDA-fractie vraagt naar onderbouwing van deze principiële keuze en of de keuze van de consument in deze niet voorop zou moeten staan.

Het publieke middel is ontwikkeld ten behoeve van overheidsdienstverleners die burgers herkennen aan de hand van hun bsn. Het gebruik van het publieke middel is daarmee beperkt tot digitale dienstverlening van organisaties die gerechtigd zijn het bsn te gebruiken. Mocht in de toekomst blijken dat de consument met een publiek middel ook zou willen inloggen in het private domein, dan zal het belang van de consument moeten worden afgewogen tegen aspecten zoals het gebruik van het bsn

door private partijen, regeldruk voor het bedrijfsleven, naleving van de Wet markt en overheid – ter voorkoming van marktverstoring –, eventuele informatieveiligheidsrisico's en kosten voor de overheid.
De leden van de CDA-fractie vragen waarom er geen publiek middel kan worden gebruikt voor het bedrijfsmatig in contact komen met de overheid. De leden van de CDA-fractie vragen ook in te gaan op de opmerkingen die het Adviescollege Toetsing Regeldruk maakt over de eHerkenningsmiddelen. Voorts vraagt de CDA-fractie zich af, waarom de regering in de keuze van de ondernemer treedt in het geval dat ondernemingen die op naam van een natuurlijk persoon staan, gebruik kunnen maken van dienstverlening waarbij het mogelijk is om te identificeren met DigiD en met eHerkenning. De leden van de CDA-fractie vragen of de conclusie gerechtvaardigd is, dat regulering van de huidige situatie geschiedt met het oog op het verbieden van digitale dienstverlening voor bedrijven waarbij de toegang op basis van identificatie met een publiek middel wordt verleend.

DigiD is niet toegerust om bij de authenticatie andere nummers dan het bsn te leveren aan de dienstverlener. Het private bedrijfsmiddel eHerkenning is ontwikkeld voor de gevallen waarin het KvK- of RSIN-nummer is vereist. Alhoewel niet van overheidswege uitgegeven, moet dit bedrijfsmiddel aan strenge eisen voldoen en zal het aan toezicht van de door de Minister van BZK aangewezen ambtenaren worden onderworpen. Het bedrijfsmiddel blijkt in de praktijk toereikend voor het inloggen bij dienstverlening aan bedrijven in het publieke domein, waardoor de nut en noodzaak voor het introduceren van een publiek middel ontbreekt. Aan de aanbeveling van het Adviescollege Toetsing Regeldruk (ATR) om de betrouwbaarheidsniveaus van eHerkenning te uniformeren en terug te brengen tot de drie niveaus wordt uitvoering gegeven. Voorts wordt bij de uitwerking van de lagere regelgeving rekening gehouden met de behoefte aan gebruiksvriendelijke machtigingssystemen. Door de ATR is tevens aanbevolen om in overleg met aanbieders van eHerkenningsmiddelen te komen tot een standaardisering van abonnementen en aanvullende diensten. Het is mogelijk dat een standaardisering tot minder kosten zal leiden, maar eHerkenning is een stelsel met concurrerende aanbieders van inlogmiddelen die zich juist moeten onderscheiden om keuzemogelijkheden voor klanten te bieden, zodat klanten optimaal bediend kunnen worden. In lijn met het ATR-advies om het gebruik van machtigingsvoorzieningen bij eHerkenning te vereenvoudigen, wordt bij de uitwerking van de lagere regelgeving rekening gehouden met de behoefte aan gebruiksvriendelijke machtigingssystemen.

De conclusie dat regulering van de huidige situatie geschiedt met het oog op het verbieden van digitale dienstverlening voor bedrijven waarbij de toegang op basis van identificatie met een publiek middel wordt verleend, is niet gerechtvaardigd; de regering voert geen bepaling in die dienstverleners verbiedt beide inlogmethoden aan te bieden aan ondernemers. Het gebruik van een publiek middel kan wel ondoelmatig zijn omdat dienstverleners bedrijven in hun administratie herkennen aan de hand van het KvK- of RSIN-nummer in plaats van het bsn. Alleen in het geval ondernemingen op naam staan van een natuurlijke persoon, bestaat bij sommige dienstverleners de mogelijkheid om zowel in te loggen met eHerkenning als met een publieke middel. Het wetsvoorstel treedt niet in de vrijheid van ondernemers om tussen deze opties te kiezen.

De D66-fractie is van mening dat toegang tot elektronische diensten van de overheid betrouwbaar en veilig moet zijn en dat het goed is dat deze wet dit vastlegt. De leden van de D66-fractie verbazen zich over het feit dat de kosten die het Rijk maakt samenhangend met de verstrekking van een

publiek identificatiemiddel met een hoger betrouwbaarheidsniveau, ten laste worden gebracht van de burger en vragen hoe dit samenhangt met het basisrecht van burgers tot communicatie met de overheid. De leden vragen zich af, of de overheid zelf, met eigen middelen, niet zorg voor deze overheidscommunicatie dient te dragen en of er een mogelijkheid is andere modellen voor het bekostigen te onderzoeken.

Het feit dat er een, in dit wetsvoorstel verankerde, publieke verantwoordelijkheid is voor het ontwikkelen en uitgeven van publieke identificatiemiddelen op een voldoende hoog betrouwbaarheidsniveau, brengt niet zonder meer met zich, dat (volledige) bekostiging ter zake ook door de (Rijks)overheid dient te geschieden. In dit verband zijn meerdere bekostigingsmodellen onderzocht en is door het kabinet besloten tot de bekostiging zoals opgenomen in de artikelen 20 – 22 van het wetsvoorstel. Bij de publieke identificatiemiddelen zal een gedeelte van de kosten die het Rijk maakt worden doorbelast aan burgers. Dit is in lijn met hetgeen gebruikelijk is bij leges (retributies): het betreft een betaling aan de overheid waar een individueel aanwijsbare tegenprestatie van de overheid tegenover staat. Anders dan de kosten van aanschaf van het publieke identificatiemiddel, zijn de kosten van het gebruik ervan niet voor rekening van de gebruiker. Deze worden doorbelast aan de publieke dienstverlener; de kosten die het Rijk maakt, samenhangend met het realiseren van publieke middelen en voorzieningen, worden ten laste gebracht van de bestuursorganen en aangewezen organisaties.
De leden van de D66-fractie zouden graag, net als de Raad van State, het basisrecht voor burgers tot communicatie met de overheid in het wetsvoorstel doorgevoerd zien en vragen zich af waarom dit niet is opgenomen. Zij stellen dat het feit, dat dit recht een bredere werkingssfeer heeft dan onderhavig voorstel, de verwerking in dit wetvoorstel niet hoeft te belemmeren.
Met de D66-fractie ben ik van mening dat er een recht op communicatie met de overheid bestaat. Dit gaat echter de werkingssfeer van het wetsvoorstel digitale overheid te buiten. Algemene regels over bestuurlijk verkeer (communicatie) met de overheid zijn neergelegd in de Awb. Momenteel bereid ik samen met mijn ambtgenoot van Justitie en Veiligheid een wijziging van de Awb voor, waardoor burgers naast de papieren weg een aanspraak krijgen op digitaal zaken doen met de overheid. Tevens zijn wij voornemens – los van digitalisering – bestuursorganen te verplichten ondersteuning te bieden bij communicatie met de overheid. Naar verwachting zal dit wetsvoorstel in 2019 bij uw kamer worden ingediend.

De D66-fractie vraagt voorts hoe uitvoeringsorganisaties en dienstverleners kunnen bepalen wat het vereiste betrouwbaarheidsniveau is bij elektronische identificatie, welke regels hierbij gelden en of hier toezicht op is. Ook vragen zij, gelet op artikel 6 lid 4 van het wetsvoorstel, dat ruimte biedt om tijdelijk een inlogmiddel met een lager betrouwbaarheidsniveau toe te staan, hoe lang een dergelijke afwijking van het hogere betrouwbaarheidsniveau toegestaan is en of het verstandig zou zijn hieraan een deadline te koppelen.

Mijn doelstelling is om overheidsdienstverlening zo snel als mogelijk naar een hoger betrouwbaarheidsniveau te brengen. Daar zijn de inspanningen op gericht. Om verplichtingen op te kunnen leggen is het echter van belang dat deze redelijkerwijs kunnen worden ingevuld. Of dat kan hangt van een aantal factoren af. Zo moeten middelen op de voorgeschreven betrouwbaarheidsniveaus breed beschikbaar zijn. Voor overheidsorganisaties geldt daarbij dat zij vaak te maken hebben met bestaande processen en informatiesystemen («legacy») en dat

aanpassing de nodige tijd kost. Het is belangrijk om daar realistisch in te zijn en te zorgen dat overheidsorganisaties dat op een ordentelijke manier kunnen doen. De tijd die nodig is of gegund wordt hangt in belangrijke mate af van het belang en complexiteit van de dienstverlening. Dit betekent niet dat er geen einddatum op zit. Organisaties zullen de snelheid moeten betrachten die zij redelijkerwijs aan kunnen. Maar ik wil er wel voor wil waken dat organisaties overhaast gaan implementeren; dit kan namelijk andere implementatie – en veiligheidsrisico's met zich brengen, hetgeen uiteindelijk per saldo weinig winst oplevert. Het wetsvoorstel voorziet in toezicht op de naleving van de juiste inzet van betrouwbaarheidsniveaus. Het toezicht op de naleving van classificering door dienstverleners loopt via de reguliere (interbestuurlijke) lijnen. Voor het toezicht op naleving van de verplichting door ministeries en zelfstandige bestuursorganen geldt dat de Minister, op wiens beleidsterrein het betreffende bestuursorgaan of het desbetreffende zelfstandige bestuursorgaan of aangewezen organisatie werkzaam is, een toezichthouder aanwijst.

De leden van de D66-fractie vragen welke technische voorschriften zijn verbonden aan het toelatingsbesluit inzake een privaat middel en of deze uit eIDAS volgen. Zij vragen tevens of deze eisen voldoende zijn en of de regering voornemens is aanvullende eisen te stellen.

De voorschriften die aan private identificatiemiddelen gesteld worden om te worden toegelaten volgen allereerst uit de eIDAS verordening 2015/1502 van de Europese Commissie. Deze uitvoeringsverordening beschrijft de technische en procedurele stappen (controles) die moeten plaatsvinden om te zorgen dat aan middelen een betrouwbaarheidsniveau «substantieel» of «hoog» kan worden toegeschreven. Daarnaast worden voor de toelating voorschriften gesteld die niet direct voortvloeien uit eIDAS-normen, maar die voor Nederland aanvullend zijn en voortkomen uit nationale beleids- en inrichtingskeuzes, zoals het gebruik van pseudonimisering voor privacybescherming en het gebruik van het zogeheten BSN-koppelregister (een publieke voorziening die mogelijk maakt dat gebruikers centraal inzage kunnen krijgen in hun middelen). De eIDAS-verordening laat de ruimte om nationaal deze aanvullende eisen te stellen.

De leden van de D66-fractie vragen of het klopt dat niet elk privaat middel dat aan de voorwaarden voldoet wordt toegelaten. Zij vragen zich af, op welke wijze dan een keuze wordt gemaakt tussen aanbieders die aan de voorwaarden voldoen. Voorts vragen zij zich af, wanneer sprake is van noodzaak van een privaat middel voor de beschikbaarheid en toegankelijkheid van elektronische dienstverlening aan natuurlijke personen.

Zoals hiervoor ook is aangegeven, is de doelstelling van het wetsvoorstel ervoor te zorgen dat er identificatiemiddelen op hogere betrouwbaarheidsniveaus continu beschikbaar zijn. Burgers moeten veilig en ongestoord zaken kunnen doen met de overheid. Om dat snel voor elkaar te krijgen is het noodzakelijk dat een alternatief met een hoge dekkingsgraad beschikbaar komt. Om dat te realiseren maakt het wetsvoorstel het mogelijk om een of meerdere private identificatiemiddelen toe te laten. Op dit moment wordt een aanbesteding voorbereid om in dit kader één of meerdere private authenticatiemiddelen te verwerven, waarbij de markt vooraf duidelijkheid wordt geboden over de opdracht.
De D66-fractie constateert dat de reikwijdte van organisaties die de plicht hebben om bij elektronische dienstverlening de toegelaten identificatiemiddelen te accepteren vrij breed is. Hier vallen ook pensioenuitvoerders, zorgaanbieders, ziektekostenverzekeraars, indicatieorganen en de

universiteiten en hogescholen onder. De leden van de D66-fractie vragen zich af welke kosten deze plicht met zich mee brengt voor deze organisaties.

Bij elektronische overheidsdienstverlening staat de burger centraal. Het is belangrijk dat burgers bij alle overheidsdienstverleners in kunnen loggen met dezelfde betrouwbare (publieke of private) middelen. Zowel voor burgers als voor de dienstverleners is het efficiënt en gebruiksvriendelijk overal met dezelfde betrouwbare middelen te kunnen werken. Daarom voorziet het wetsvoorstel in een acceptatieplicht voor dienstverleners. Om overheidsdienstverlening digitaal beschikbaar te maken, zal de dienstverlener een aansluiting moeten hebben op een authenticatiedienst. Dit kost geld; voor DigiD betaalt een dienstverlener op dit moment ca. 12 eurocent per inlog. Een groot aantal van de genoemde organisaties maakt nu al gebruik van DigiD, zoals pensioenuitvoerders en ziektekostenverzekeraars. Ook veel zorgaanbieders maken reeds gebruik van DigiD. De organisaties moeten zelf de kosten dragen voor het ontwikkelen van hun eigen elektronische diensten. De kosten voor beheer en exploitatie van de toegelaten en erkende middelen en de kosten voor de ontwikkeling van de publieke voorzieningen zullen ook worden doorbelast, hetgeen voor hen betekent dat die kosten zullen stijgen. Daar staat tegenover dat deze wijze van communiceren op andere vlakken juist naar verwachting kostenvoordelen zal opleveren (bijvoorbeeld in de zorg).
De leden van de D66-fractie lezen dat het streven is dat in de toekomst voor alle personen met een bsn een elektronisch identificatiemiddel op de betrouwbaarheidsniveaus substantieel en hoog beschikbaar komt, en dat voor een bepaalde periode ongelijkheid kan ontstaan tussen burgers die wel of niet een rijbewijs of identiteitskaart hebben. De D66-fractie constateert dat zij die dit niet hebben, niet kunnen inloggen op betrouwbaarheidsniveau substantieel/hoog en derhalve geen toegang krijgen tot de elektronische dienst die de overheid aanbiedt. De fractie vraagt op welke wijze er zorg voor zal worden gedragen dat elk persoon met een bsn die dat wenst toegang kan krijgen tot een elektronische overheidsdienst waarbij het betrouwbaarheidsniveau substantieel of hoog is.

Aan het beschikbaar komen van publieke middelen op betrouwbaarheidsniveau substantieel en hoog wordt hard gewerkt. De daadwerkelijke uitgifte zal stapsgewijs geschieden. Niet alle burgers met een bsn zullen op hetzelfde moment gaan beschikken over een publiek middel op een hoger betrouwbaarheidsniveau, bijvoorbeeld omdat voor rijbewijzen en identiteitskaarten een geldigheidsduur geldt. Om die reden voorziet het wetsvoorstel in de mogelijkheid tot gefaseerde inwerkingtreding en overgangsrecht. Onder meer kan gedurende een bepaalde periode worden toegestaan dat de toegang tot diensten, waarvoor eigenlijk authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, kan geschieden met gebruikmaking van identificatiemiddelen met betrouwbaarheidsniveau laag respectievelijk substantieel.

4. Privacy

De leden van de D66-fractie vragen of de uitgevoerde privacy impact assessments (PIA's) aan de kamer kunnen worden toegezonden.

Ook ik hecht groot belang aan de waarborging van de privacy. Voor het vertrouwen in de digitale overheid is een zorgvuldige omgang met persoonsgegevens essentieel. Ik geef graag gehoor aan het verzoek om de uitgevoerde PIA's aan uw kamer toe te zenden bij gelegenheid van de komende eID-voortgangsrapportage. Een aantal van deze PIA's is reeds aan uw Kamer toegezonden.

De D66-fractieleden vragen zich af waar in de wet is terug te vinden dat de gegevensverwerking zodanig wordt ingericht, dat geen van de bij authenticatie betrokken partijen (inclusief dienstverleners) kan zien welke andere websites door de houder van het middel worden bezocht. Daarnaast vragen deze leden waarom er voor gekozen is om de uitwerking van artikel 15 tot en met 18 AVG (recht van inzage en rectificatie) niet in de wet op te nemen, maar dit in uitvoeringsregelgeving vast te leggen. De D66-fractie vraagt of dit recht niet van fundamentelere betekenis zou zijn als het ook in de wet wordt vastgelegd en uitgewerkt. De D66-fractieleden hebben inzake dataminimalisatie eveneens de vraag hoe dit bewerkstelligd zal worden en waarom dit principe geen plaats heeft in de wet.

Voor het eID stelsel is het van belang dat de bescherming van persoonsgegevens op een adequate wijze, conform de AVG, wordt ingericht. Het inrichten van maatregelen om te voorkomen dat partijen ongeoorloofd gebruik maken van persoonsgegevens maakt daarvan onderdeel uit. De wijze waarop dat gebeurt moet in de inrichting van het stelsel vorm krijgen, waarbij ruimte moet zijn risico's te ondervangen. Dit betekent onder meer dat op het niveau van de wet niet te veel gestuurd wordt om deze inrichtingskeuzes niet onbedoeld rigide te maken.

De wet digitale overheid en uitvoeringsregelgeving regelen de kaders die gelden voor verwerkingen van persoonsgegevens die plaatsvinden in het kader van het eID stelsel. Zo dienen de verwerkingen over een wettelijke grondslag te beschikken onder meer ten aanzien van de verwerking van het bsn. Ook worden de gegevens die mogen worden verwerkt vastgesteld, alsmede aan wie deze mogen worden verstrekt en hoe lang de gegevens mogen worden bewaard. De AVG verlangt dat deze aspecten bij wet worden geregeld.
De belangrijke rechten van inzage en rectificatie uit de AVG, een rechtstreeks werkende EU-verordening, gelden voor gebruikers direct. Opname van deze rechten in het onderhavige wetsvoorstel is niet nodig en – vanwege de rechtstreekse toepasselijkheid van de AVG – niet toegestaan. Datzelfde geldt voor de privacybeginselen uit de AVG, waaronder dataminimalisatie, proportionaliteit en subsidiariteit. Deze rechten voor gebruikers en privacybeginselen vormen het kader dat de verantwoordelijke bij de inrichting van de verwerkingen van persoonsgegevens moet hanteren. Dit gebeurt ook bij de inrichting van het eID-stelsel. Om deze inrichting te sturen is een privacyvisie opgesteld, waarin de toepasselijke privacyregels zijn geïnventariseerd, en waarin stapsgewijs wordt aangegeven hoe deze doorwerken bij de inrichting van het eID-stelsel. Ik zal deze privacyvisie aan de Kamer zenden bij gelegenheid van de volgende eID-voortgangsrapportage zodat inzicht wordt geboden in de wijze waarop ik als verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens binnen het eID stelsel de naleving van privacywetgeving ter hand neem. Daarbij merk ik op dat naleving van privacywetgeving een doorlopende activiteit is, en dat adequate naleving niet statisch is. Dat betekent dat door de tijd maatregelen die getroffen worden om een adequate bescherming van persoonsgegevens te realiseren kunnen wijzigen, bijvoorbeeld door voortschrijdende beschermingstechnieken, maar ook door veranderende dreigingen. Overigens draag ik zorg voor een voorziening die gebruikers, die immers meerdere middelen kunnen hebben, in staat stelt op een centraal punt in te zien welke middelen zij hebben aangevraagd. Dit is geregeld omdat de inrichting van zo'n voorziening niet logischerwijs uit de uitwerking van de AVG zou voortvloeien. Dat rechtvaardigt ook de regeling ervan in het wetsvoorstel.

5. Misbruik van de GDI

De leden van de VVD-fractie vragen zich af hoe, ingeval een identificatiemiddel wordt ingetrokken, de aansprakelijkheid is geregeld en voor wie de kosten zijn.

Alle actoren in het eID stelsel, zowel middelenuitgevers als de Minister van BZK, moeten de mogelijkheid hebben om, indien zij signaleren dat er (mogelijk) misbruik plaatsvindt met identificatiemiddelen, deze te blokkeren of in te trekken. Daarmee kan immers (verdere) schade of nadeel voor zowel burgers en overheden worden voorkomen. Daarbij geldt dat iedereen binnen het eID stelsel zorgvuldig dient te handelen. BZK en middelenuitgevers zullen niet lichtvaardig mogen overgaan tot het intrekken van een identificatiemiddel. Daartoe dienen zij zorgvuldig te werk te gaan en gegronde redenen moeten hebben. Aan de andere kant dienen burgers – net als met fysieke identiteitsdocumenten – zorgvuldig met hun identificatiemiddelen om te gaan, omdat onzorgvuldig gebruik misbruik in de hand kan werken. Deze verantwoordelijkheden maken dat niet een eenduidig antwoord mogelijk is op de vraag wie in een concreet geval aansprakelijk is voor de gevolgen van een intrekking en de gevolgen ervan moet dragen. Dat zal – aan de hand van de reguliere aansprakelijkheidsregels moeten worden bepaald. Daarbij zal het gaan om vragen als zorgvuldigheid van handelen en verwijtbaarheid in concrete situaties.

6. Toezicht en handhaving

Ook al is een overheidstaak op afstand gezet, vanuit zijn verantwoordelijkheid dient de Minister de betrokken zelfstandige bestuursorganen zo nodig tot naleving van de wet te bewegen, zo lezen de leden van de CDA-fractie. De CDA-fractie vraagt zich af welke middelen de Minister(s) hierbij ter beschikking staan.

Waar het wetsvoorstel spreekt over de Minister die het aangaat, is deze bevoegd toezichthoudende ambtenaren aan te wijzen. Er is voor gekozen aan te sluiten bij bestaande toezichtstructuren in het desbetreffende beleidsdomein, zoals uitgeoefend door bijvoorbeeld de ILT, de IGJ en de Arbeidsinspectie. Voor wat betreft zelfstandige bestuursorganen zijn de beschikbare instrumenten opgenomen in de Kaderwet Zbo's; in het uiterste geval kan de desbetreffende Minister een vernietigingsbesluit nemen of een taakverwaarlozingsvoorziening treffen. Daarnaast beschikt de Minister van BZK ingevolge dit wetsvoorstel over bijzondere bevoegdheden indien bijvoorbeeld sprake is van een ernstige aantasting van de veiligheid of van (dreigend) misbruik.

Voorts constateert de CDA-fractie dat ter zake van medeoverheden het primaat voor de controle op de naleving bij horizontale verantwoording binnen een bestuurslaag ligt. De leden van de CDA-fractie constateren, dat de praktijk uitwijst dat gemeenteraden, provinciale staten en algemene besturen vaak de nodige informatie ontberen om als toezichthouder op te treden. Zij vragen zich af welke stappen hierop zijn ondernomen of de regering overweegt te ondernemen.

Evenals ten aanzien van Zbo's is er bij decentrale overheden voor gekozen aan te sluiten bij bestaande toezichtstructuren. Dat betekent dat in lijn met de reguliere verantwoordingssystematiek en informatiebevoegdheden moet worden gehandeld. Daarnaast is echter, conform de Gemeentewet en Provinciewet, interbestuurlijk toezicht en het in dat verband beschikbare instrumentarium aan de orde. Dit toezicht is gebaseerd op vertrouwen. Wel is het zo, dat de Minister van BZK ingevolge dit wetsvoorstel over bijzondere bevoegdheden beschikt indien bijvoorbeeld

sprake is van een ernstige aantasting van de veiligheid of van (dreigend) misbruik. Medeoverheden wordt de gelegenheid gegeven in de praktijk met het wetsvoorstel te gaan werken. Vanuit mijn ministerie is hiervoor desgewenst voorlichting en ondersteuning beschikbaar. Mocht blijken dat aanvullend instrumentarium noodzakelijk is, dan zullen nadere maatregelen worden overwogen.

De CDA-fractie vraagt zich af wat de positie van de burgemeester is op het vlak van informatieveiligheid als verantwoordelijke voor openbare orde en veiligheid.

Inzake informatieveiligheid bij de toegang tot elektronische dienstverlening voorziet het wetsvoorstel in specifieke regels en verantwoordelijkheden. De Minister van BZK stelt informatieveiligheidsregels aan bestuursorganen en aangewezen organisaties, waaronder een auditplicht. De publieke dienstverleners, waaronder gemeenten, moeten deze regels naleven. De in dit verband voorgenomen algemene maatregel van bestuur zal, zoals bij punt 1 van deze nota is aangegeven, aan uw kamer worden toegezonden. De Minister van BZK houdt voorts toezicht op de naleving van de gestelde regels; hij beziet de te overleggen auditverklaringen, gaat indien nodig – en in overleg met de domeinspecifieke toezichthouder – in gesprek over verbetering en kan in het uiterste geval noodmaatregelen nemen. Het is de Minister van BZK die in casu doorzettingsmacht heeft en over bijzondere bevoegdheden beschikt indien bijvoorbeeld sprake is van een ernstige aantasting van de veiligheid of van (dreigend) misbruik. De bevoegdheden van de Minister richten zich op de borging of het herstel van de betrouwbare toegang tot elektronische dienstverlening. In het geval van (diensten van) een gemeente heeft de burgemeester geen specifieke taak vanwege zijn verantwoordelijkheid voor openbare orde en veiligheid; wel dient hij als bestuursorgaan zorg te dragen voor de naleving van het wetsvoorstel.

De leden van de CDA-fractie vragen, of het de bedoeling is dat het Agentschap Telecom de volledige taak van toezichthouder op erkende diensten overneemt.
Ingevolge het wetsvoorstel zullen ambtenaren worden aangewezen die toezien op de naleving van de bepalingen van het wetsvoorstel. Voor wat betreft de bepalingen inzake erkende diensten (dit zijn private partijen) in het bedrijvendomein, heb ik het voornemen ambtenaren van het Agentschap Telecom, onderdeel van het Ministerie van Economische Zaken en Klimaat, aan te wijzen.
De leden van de CDA-fractie vragen voorts of aan de hand van voorbeelden kan worden geschetst wanneer de meldplicht bij veiligheidsinbreuken met beperkte impact achterwege kan blijven.
Het wetsvoorstel kent een plicht om veiligheidsinbreuken te melden. In de memorie van toelichting is opgenomen dat bij veiligheidsinbreuken met een «beperkte impact» deze plicht minder voor de hand ligt. Eerst merk ik op dat op grond van het wetsvoorstel niet te snel mag worden aangenomen dat een melding achterwege mag blijven. Waar het om gaat is dat veiligheidsinbreuken met relevantie en grote gevolgen voor veel personen, over organisaties heen, gesignaleerd worden. Dat is niet alleen van belang voor transparantie, maar ook om de gevolgen snel en effectief te kunnen herstellen. Door de veiligheidsinbreuken met beperkte impact niet te melden, bijvoorbeeld een of enkele geblokkeerde DigiD's, wordt ervoor gezorgd de veiligheidsinbreuken die wel gemeld worden de aandacht kunnen krijgen en niet vertroebeld raken in een groter aantal meldingen. Ik hecht eraan op te merken dat dit geenszins betekent dat op inbreuken met beperkte impact geen actie moet worden ondernomen. Het niet melden ervan bij een toezichthouder doet daar op geen enkele wijze afbreuk aan. Immers, ook veiligheidsinbreuken met beperkte impact

kunnen vervelende gevolgen hebben voor personen die het betreft. De gehanteerde systematiek is vergelijkbaar met de wijze die de meldplicht datalekken uit de AVG hanteert. De gevolgen voor betrokkenen, en de mate waarin deze reeds zijn hersteld kunnen meewegen bij de vraag of inbreuken moeten worden gemeld.
De leden van de D66-fractie lezen in de toelichting dat in 2015 alleen al 15 000 DigiD's zijn geblokkeerd vanwege (een vermoeden van) fraude. De D66-fractie constateert, in aansluiting op het advies van de Raad van State, dat niet is geregeld welk orgaan verantwoordelijk is voor het oplossen van de problemen waar slachtoffers van identiteitsfraude mee te maken krijgen, en waar het slachtoffer zich kan melden, of hoe hij op een eenvoudige manier een identificatiemiddel tijdelijk kan onderbreken. De D66 fractie vraagt zich af waarom de verankering van deze taken in deze wet niet opportuun is.
De problemen waar slachtoffers van identiteitsfraude mee te maken krijgen, zijn serieus en hebben mijn aandacht. In 2010 is door BZK het Centraal Meldpunt Identiteitsfraude- en fouten (CMI) ingericht. Het CMI, onderdeel van mijn ministerie, biedt advies en hulp aan slachtoffers van identiteitsfraude. Via www.Rijksoverheid.nl, www.rvig.nl en www.slachtofferwijzer.nl wordt informatie verschaft over taken en werkwijze van het CMI, samenwerking met de ketenpartners (o.a. de RDW, KMAR, politie en OM), preventie, het herkennen en melden van identiteitsfraude en te nemen maatregelen. Ook kunnen er meldformulieren worden gedownload. Het door slachtoffers/gebruikers tijdelijk laten onderbreken (blokkeren) van DigiD is geregeld in de Regeling voorzieningen GDI. Het onderhavige wetsvoorstel bevat voorts bevoegdheden van de Minister van BZK in het geval van (vermoed) misbruik van een elektronisch identificatiemiddel. In aanvulling daarop zal ik de opportuniteit bezien van een meer algemene wettelijke verankering van de verantwoordelijkheid van de Minister van BZK bij de aanpak van identiteitsfraude. Gelet op de reikwijdte van het onderhavige wetsvoorstel (elektronische identificatie bij de toegang tot overheidsdienstverlening) en het feit dat identiteitsfraude een complex geheel is en een bredere portee heeft dan digitale identificatie (zo zijn er meerdere identiteitsdocumenten en is er samenhang met bijvoorbeeld de BRP) ligt regulering in de Wet digitale overheid niet in de rede.
De leden van de D66-fractie lezen dat dienstverleners geacht worden jaarlijks een audit te laten uitvoeren om te toetsen op de naleving aan de eisen aan de werking, betrouwbaarheid en beveiliging van de toegang van de elektronische dienstverlening. Dit wordt door de leden ondersteund. De leden vragen of deze auditverklaring openbaar wordt gemaakt en zo nee, wat de onderbouwing hiervan is.
Het verheugt mij dat de auditplicht met betrekking tot de toegang tot elektronische diensten door de D66-fractie wordt ondersteund. De auditverklaring wordt niet openbaar gemaakt, aangezien deze inzicht geeft in eventuele non-conformiteit met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang van de elektronische dienstverlening. Bij openbaarmaking zouden kwaadwillende derden hier misbruik van kunnen maken. Het is ingevolge het wetsvoorstel mijn verantwoordelijkheid om een risicogebaseerde afweging te maken met betrekking tot de vraag, of de non-conformiteit een acute bedreiging vormt. Als dit het geval is dan kan de toegang van de betreffende dienstverlener tot de elektronische dienstverlening (tijdelijk) worden opgeschort (afgesloten) tot dat de non-conformiteit is opgelost. Als er geen sprake is van een acute bedreiging dan zal aan de dienstverlener, op basis van een risicoafweging, een vooraf vastgestelde periode worden gegund om de non-conformiteit op te lossen. Mocht dit binnen die periode niet zijn opgelost, dan kan alsnog (tijdelijke) opschorting van de toegang tot de elektronische dienstverlening volgen. Overigens laat het feit, dat een auditverklaring niet openbaar wordt gemaakt, informatieverschaffing aan vertegenwoor-

digende organen (zoals de gemeenteraad) in het kader van de algemene verantwoordingsplicht jegens deze organen onverlet.
De leden van de D66-fractie merken op dat het wetsvoorstel ook afgeleide identificatie mogelijk maakt. Dit zou betekenen dat bij de aanvraag voor eHerkenning kan worden gesteund op de identificatie van bijvoorbeeld DigiD. De leden van de D66-fractie vragen zich af, of hieruit volgt dat het van belang is dat de veiligheidseisen voor het bedrijvenmiddel vergelijkbaar zijn met de veiligheidseisen van het burgermiddel en andersom.
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. De veiligheidseisen voor zowel het bedrijvenmiddel als het burgermiddel volgen uit de eIDAS-verordening en bieden een vergelijkbaar beschermingsniveau.
Voorts vragen de leden wie of welke instantie er toezicht op houdt dat de eisen die gesteld worden aan de inlogmiddelen vergelijkbaar zijn, en of het klopt dat op het bedrijvenmiddel het Agentschap Telecom toezicht houdt, en op het burgermiddel aangewezen ambtenaren (artikel 17 wetsvoorstel). De D66-fractie vraagt naar de wenselijkheid van twee verschillende toezichthouders, gelet op de mogelijkheden tot afgeleide identificatie.
Het is mijn verantwoordelijkheid ervoor zorg te dragen dat de eisen aan de inlogmiddelen – in aansluiting op de eIDAS verordening – een gelijkwaardig beschermingsniveau bieden. Er zullen toezichthoudende ambtenaren worden aangewezen voor het bedrijfs- en organisatiemiddel en voor het burgermiddel. Naar verwachting zullen ambtenaren van het Agentschap Telecom door mij worden aangewezen om toezicht te houden op het bedrijfs- en organisatiemiddel; voor het burgermiddel beraad ik mij nog op de precieze vormgeving. Vanzelfsprekend zal ik er voor zorgdragen dat de toezichtsregimes adequaat zijn ingericht en onderling zijn afgestemd.

7. Financiële bepalingen en gevolgen

De leden van de VVD-fractie vragen wat de kosten voor de overheid zijn als gevolg van het wetsvoorstel. De leden vragen hoe de business case eruit ziet, of het klopt dat de business case voor inloggen bij de overheid met 300 miljoen euro is gestegen en nu uitgaat van een bedrag van één miljard euro, welke kosten voor rekening komen van de bestuursorganen en de aangewezen organisaties die de diensten leveren en hoe de kosten van deze diensten worden bepaald. Ook de leden van de D66-fractie vragen of een beeld kan worden geschetst van de kosten van het uitrollen van een robuuste infrastructuur voor authenticatie en identificatie, inclusief toelating en toezicht.

Op 9 maart 2018 heb ik uw Kamer de geactualiseerde «Business case inloggen in het BSN domein» toegezonden (TK 2017–2018, 26 643, nr. 514). Het is juist dat de door het onafhankelijke bureau geschatte kosten 300 miljoen euro hoger uitvallen en optellen tot een bedrag van bijna één miljard euro voor de komende twaalf jaar. In de aanbiedingsbrief bij het onderzoek heb ik aangegeven wat de oorzaak is van deze kostenstijging. De onderzoekers ondersteunen de opvatting van het kabinet, dat het investeren in het eID-stelsel een essentieel onderdeel is van het meer betrouwbaar maken van de digitale snelweg; aangegeven wordt dat de kosten fors zijn, maar maatschappelijk te verantwoorden vanuit de potentiële baten. De kosten die voor rekening komen van de bestuursor-

ganen en aangewezen organisaties zijn nog niet bepaald. De uitwerking hiervan zal neergelegd worden in nadere regelgeving. Afgesproken is dat deze kosten op dat moment via uitvoeringstoetsen in beeld worden gebracht. Vanzelfsprekend wordt voortdurend bezien of de kosten zo laag mogelijk kunnen worden gehouden.

De leden van de CDA-fractie vragen nader in te gaan op de kritiek, dat betrokken partijen niet consequent betrokken zijn bij de besluiten die worden genomen in het kader van digitale overheid en dat dat de kosten die gepaard zullen gaan met de implementatie en het beheer van de nieuwe generieke digitale infrastructuur en die grotendeels voor rekening zullen komen van de afnemers/dienstverleners volstrekt onduidelijk zijn, waardoor een betrouwbare impactanalyse onmogelijk is.

In de periode van 21 december 2016 tot en met 31 maart 2017 is het voorontwerp van dit wetsvoorstel aan een brede consultatie onderworpen. Hieruit is gebleken dat het nodig is om het stelsel op enkele onderdelen te vereenvoudigen om de uitvoerbaarheid beter te realiseren en kosten te beperken. Dienstverleners wijzen op meerdere koppelvlakken als belangrijke kostendrijver. Naar aanleiding van de consultatiereacties is in het wetsvoorstel opgenomen dat de Minister van BZK verantwoordelijk is voor de inrichting en werking van een routeringsvoorziening, teneinde de toegang tot elektronische dienstverlening te faciliteren. Door middel van één koppelvlak, één contract en één factuur voor dienstverleners wordt de complexiteit verminderd en worden aansluitkosten gedrukt. Aldus worden dienstverleners bij hun elektronische dienstverlening ontzorgd. Kosten van het gebruik van publieke middelen en de in dat verband benodigde infrastructuur hangen grotendeels samen met de mate van gebruik van alle publieke middelen. De kosten voor authenticatie met een bepaald middel zijn sterk gerelateerd aan het totale aantal authenticaties met dat middel. Bij hogere aantallen nemen de kosten significant af. Burgers kunnen kiezen welk toegelaten middel zij gebruiken, waardoor het in de aanvangsfase moeilijk is in te schatten hoe vaak een bepaald middel gebruikt gaat worden en op basis daarvan de kosten van authenticatie in te schatten. De kostencomponenten zijn uiteengezet in de financiële paragraaf in de memorie van toelichting en deze zijn voor zover in deze fase mogelijk gekwantificeerd.

Voorts vraagt de CDA-fractie of een exegese kan worden gegeven van de zinsnede «dat een toekomstbestendige financieringsstrategie moet kunnen mee-ademen met de implicaties van meer gebruik en nieuwe technologische eisen» (MvT blz. 38).

De kosten die het Rijk maakt, samenhangend met het realiseren van publieke identificatiemiddelen en voorzieningen, het eventueel toelaten van private middelen en toezicht op de naleving van toelatingseisen, worden door de Minister van BZK ten laste gebracht van de bestuursorganen en aangewezen organisaties. Door bij ministeriële regeling nadere regels te stellen over deze doorbelasting, kan worden ingespeeld op de ontwikkeling van de kosten van de infrastructuur voor authenticatie. Kosten van publieke middelen en de infrastructuur hangen grotendeels samen met de onvoorspelbare mate van gebruik van alle publieke middelen. Burgers kunnen kiezen welk toegelaten middel zij gebruiken, waardoor het in de aanvangsfase moeilijk is in te schatten hoe vaak een bepaald middel gebruikt gaat worden. De kosten voor authenticatie met een bepaald middel zijn sterk gerelateerd aan het totale aantal authenticaties met dat middel. Bij hogere aantallen nemen de kosten significant af. Het is dus voor een authenticatiedienst in de beginperiode lastig in te schatten tegen welke prijs een middel moet worden aangeboden. De mate van gebruik en exogene technologische ontwikkelingen zullen periodiek

nieuwe en aanvullende eisen stellen aan de infrastructuur. Kosten van beheer, exploitatie en doorontwikkeling zullen daarom pas gedurende de rit volledig duidelijk worden, reden waarom is gekozen voor het stellen van nadere regels bij ministeriële regeling. Hiermee wordt een zekere mate van flexibiliteit gerealiseerd, zonder afbreuk te doen aan duidelijkheid en rechtszekerheid.

De leden van de D66-fractie vragen of de regering kan toelichten op welke wijze een privaat inlogmiddel gefinancierd wordt. De fractie vraagt of de burger dit zelf direct betaalt aan de private partij die het inlogmiddel aanbiedt.

Een privaat inlogmiddel wordt gefinancierd door de private partij die het middel uitgeeft. Indien, nadat een aanbestedingsprocedure is doorlopen – hierin is prijsstelling een wegingsfactor –, één of enkele private identificatiemiddelen worden toegelaten voor gebruik in het publieke domein, krijgen burgers de mogelijkheid over meerdere elektronische middelen te beschikken (keuzevrijheid/terugvaloptie). Zij zullen een privaat middel dan eenmalig moeten aanschaffen bij de desbetreffende private partij. Het staat deze partij in beginsel vrij om burgers hiervoor te laten betalen. Voor het gebruik van het private middel betaalt de burger niet; deze kosten zullen worden doorbelast aan de publieke dienstverlener.

Voorts vragen de leden van de D66-fractie zich af, hoe de regering hier het basisrecht tot communicatie met de overheid beziet en aldus de verantwoordelijkheid om met eigen middelen mogelijk te maken dat ook middels een privaat inlogmiddel ingelogd kan worden.

Met het wetsvoorstel wordt het stelsel van publieke en private identificatiemiddelen publiekrechtelijk gereguleerd teneinde deze middelen te kunnen gebruiken in het publieke domein. Onder meer wordt voorgeschreven dat deze middelen toelating behoeven op basis van vooraf gestelde (op de eIDAS-verordening gebaseerde) eisen en criteria. Met dit wetsvoorstel wordt aldus de aanspraak van burgers op digitaal zaken doen met de overheid, oftewel elektronische communicatie met de overheid, geëffectueerd en gefaciliteerd. Een publiekrechtelijk stelsel brengt echter niet zonder meer met zich, dat (volledige) bekostiging ook door de (Rijks)overheid dient te geschieden. Gelet op het gezamenlijke belang bij generieke infrastructuur, zullen de publieke middelen en voorzieningen deels worden doorbelast aan de (publieke) dienstverleners. Ook het gebruik van toegelaten publieke en private middelen (inloggen) zal door de dienstverlener worden betaald. Om te kunnen inloggen met een privaat middel dient de burger dit eenmalig aan te schaffen. Hiervoor zal hij mogelijk moeten betalen. Omdat het private middel ook door burgers gebruikt kan worden voor inloggen buiten het publieke domein, is het ongewenst als de overheid aanschafkosten voor haar rekening neemt, omdat dit oneerlijke concurrentie stimuleert en marktverstorend kan werken.

De leden van de D66-fractie vragen of een inschatting kan worden gemaakt van de kosten voor gemeenten, nu zij hun digitale infrastructuur moeten aanpassen om het betrouwbaarheidsniveau substantieel of hoog toe te laten.

De kosten, die met de aanpassingen door gemeenten gemoeid zijn, zijn op voorhand lastig te kwantificeren. Bij het opstellen van de uitvoeringsregelgeving inzake de classificering van betrouwbaarheidsniveaus van dienstverlening zal ik rekening houden met de thans veelgebruikte «handreiking betrouwbaarheidsniveaus» van het Forum Standaardisatie. Daardoor wordt aangesloten bij de huidige praktijk en wordt de overgang

naar de nieuwe situatie zo eenvoudig mogelijk gemaakt. Daarnaast is in het wetsvoorstel de keuze gemaakt voor realisering van een routeringsvoorziening. Dit vloeit voort uit de consultatiereacties op het wetsvoorstel. Overheidsorganisaties gaven en geven aan behoefte te hebben aan centrale (publieke) ontzorging in de vorm van 1 contract, 1 factuur, 1 aansluiting. De routeringsvoorziening voorkomt voor een belangrijk deel dat dienstverleners, waaronder gemeenten, aanpassingen moeten doorvoeren als gevolg van (wijziging in) complexiteit; deze zullen centraal worden afgevangen. Overigens betekent het niet dat er in het geheel geen kosten of inspanningen nodig zijn aan de zijde van dienstverleners. Dit is echter in de huidige situatie niet anders.

8. Verhouding tot andere wetgeving

De leden van de VVD-fractie vragen hoe de Wet digitale overheid zich verhoudt tot de momenteel in voorbereiding zijnde Europese richtlijn e-privacy.

De nieuwe voorgenomen EU-regels inzake e-privacy zullen naar verwachting in een verordening worden opgenomen, welke de bestaande richtlijn vervangt. Het toepassingsgebied van de e-privacy regels, destijds geïmplementeerd in de Telecommunicatiewet, is een andere dan die van het onderhavige wetsvoorstel. De e-privacy verordening richt zich tot aanbieders van online communicatiediensten, te weten traditionele telecombedrijven en nieuwe spelers; aanbieders van commerciële elektronische diensten. Voor zover deze bedrijven eveneens private partijen in de zin van het wetsvoorstel digitale overheid zijn, bijvoorbeeld als te erkennen aanbieder van een bedrijfs- en organisatiemiddel dat gebruikt kan worden in het publieke domein, moeten ze tevens aan de eisen van het wetsvoorstel en bijbehorende uitvoeringsregelgeving voldoen, waaronder die op het punt van de bescherming van persoonsgegevens.

De leden van de VVD-fractie constateren voorts dat de regering er niet voor kiest om de Wet op de identificatieplicht aan te passen, maar te zijner tijd de verschillende wetten waarin identificatiemiddelen zijn opgenomen te wijzigen. De VVD-fractie vraagt nader te motiveren waarom de Wet op de identificatieplicht niet wordt aangepast.

In de Wet op de identificatieplicht (WID), een algemene wet, zijn de documenten (o.a. paspoort en rijbewijs) aangewezen waarmee in bij de wet aangewezen gevallen de identiteit van personen kan worden vastgesteld. Daarnaast zijn in een groot aantal (domein)specifieke wetten identificatie- en controleplichten opgenomen waarin verwezen wordt naar een of meer documenten genoemd in de WID. Het gaat daarbij steeds om fysieke controle. In deze systematiek past het niet om in de WID elektronische identificatiemiddelen aan te wijzen voor de gevallen waarin identiteit langs elektronische weg wordt vastgesteld teneinde elektronische overheidsdiensten te kunnen afnemen. Vanwege het verschil in systematiek en toepassingsbereik is er daarom voor gekozen om in voorkomend geval de sectorspecifieke wetgeving te wijzigen indien de overheidsdienstverlening op het desbetreffende terrein wordt gedigitaliseerd. Dit biedt ook de mogelijkheid per dienst te bepalen welk betrouwbaarheidsniveau ten minste is vereist. Bovendien kan dan, indien nodig, bepaald worden dat naast de authenticatie aan de hand van een elektronisch identificatiemiddel ook bepaalde attributen (aanvullende gegevens zoals nationaliteit of leeftijd) aan de betrokken overheidsdienstverlener verstrekt moeten worden.

9. Gevolgen voor burgers en bedrijven

De leden van de CDA-fractie constateren, dat het voorliggende wetsvoorstel voor personen met een (digitale) beperking en voor (internationale) bedrijven buiten het BSN-domein tot lastenverzwaring kan leiden. Zij vragen of de regering deze waarneming deelt, zo nee, waarom niet en zo ja, welke maatregelen de regering neemt om de lastenverzwaring weg te nemen of tenminste te beperken.

Alle overheidsinstanties waarmee burgers en bedrijven elektronisch zaken doen, moeten hun websites en apps op een begrijpelijke en toegankelijke manier inrichten. Hiertoe gelden Europese voorschriften, die in Nederland zijn opgenomen in het (Tijdelijke) Besluit digitale toegankelijkheid overheid (Stb. 2018, nr 141). Inclusie is een speerpunt van dit kabinet; de beleidsagenda NLDigiBeter bevat in dit verband een aantal door mij te nemen maatregelen.
De leden van de CDA-fractie constateren dat in uitvoeringsregelgeving criteria zullen worden opgenomen die relevant zijn voor het door de dienstverlener inschalen van het benodigde betrouwbaarheidsniveau en dat deze criteria in grote mate het kader bepalen waaraan eID-middelen moeten voldoen. De CDA-fractie vraagt of onderkend wordt dat, zolang deze criteria onbekend zijn, burgers en bedrijven in onzekerheid verkeren over welke eID-middelen in de toekomst zullen worden gehanteerd, en ook organisaties in het BSN-domein niet waar zij aan toe zijn. De leden van de CDA-fractie vragen voorts of onderkend wordt dat dit ook leidt tot onzekerheid over investeringen in private eID-middelen, waardoor potentiële aanbieders van private eID-middelen op het betrouwbaarheidsniveau hoog zich niet melden.

Bij het opstellen van de uitvoeringsregelgeving ga ik uit van de thans in de praktijk gehanteerde «handreiking betrouwbaarheidsniveaus» van het Forum Standaardisatie. Grosso modo zullen er geen fundamentele wijzigingen optreden. Ik verwacht het concept hiervoor binnen enkele maanden te kunnen publiceren in het kader van de (internet)consultatie. Hierdoor is de periode waarin over de detailuitwerking onzekerheid voor burgers en bedrijven kan bestaan, beperkt. Daarbij merk ik op dat de consultatie juist ook is bedoeld om deze regels voor overheidsorganisaties werkbaar te maken.

Het feit dat het classificatiemodel nog onbekend is, leidt niet tot onzekerheid over investeringen in private eID-middelen; het classificatiemodel niet ziet op de (vormgeving van de) identificatiemiddelen. Daarvoor gelden de regels uit de eIDAS-verordening. Voor zover terughoudendheid van private aanbieders zou voortkomen uit de onzekerheid of er middelen beschikbaar moeten zijn op de niveaus substantieel en hoog, wijs ik er op dat de classificatieregeling naar verwachting niet ingrijpend zal verschillen met de huidige praktijk, waardoor er op beide betrouwbaarheidsniveaus identificatiemiddelen nodig zijn.
De leden van de D66-fractie vragen naar de lasten die het wetsvoorstel voor burgers meebrengt en hoe hoog de kosten dan zullen zijn per ID-kaart of rijbewijs. Voorts vragen de leden naar het installeren van DigiD hoog en substantieel. De leden vragen hoe niveau substantieel eruit gaat zien, waarom is dit omslachtiger te installeren is dan DigiD hoog, en wat het periodiek heractiveren van DigiD hoog betekent.

Burgers zullen voor de aanschaf van een publiek middel moeten gaan betalen (leges). De precieze meerkosten van de e-NIK en het e-rijbewijs zijn nog niet bekend; ik ga op dit moment uit van enkele euro's. Voor wat betreft DigiD substantieel is een installatieproces nodig. Hiertoe wordt het bestaande elektronische aanvraagproces van DigiD versterkt met een

eenmalige online-controle van een (fysiek) WID-document. De controle geschiedt via een gepersonaliseerde applicatie (gratis app) op een smartphone of tablet die is uitgerust met een NFC-lezer. De beoogde gebruiker dient het document bij het desbetreffende apparaat te houden, waarmee met de microchip wordt gecommuniceerd. Bij een succesvolle controle volgt de melding «controle gelukt». Voor het inloggen bij een dienstverlener is het document daarna niet meer nodig. Voornoemd proces is anders dan bij DigiD-hoog; hierbij is de fysieke drager/kaart zelf – die wel bij elke inlogtransactie gebruikt moet worden – uitgerust met een eID-chip. Periodiek heractiveren van publieke identificatiemiddelen is nodig vanwege het volgende. Bij de aanvraag van een elektronisch identificatiemiddel moet vastgesteld worden dat een burger een geldig, officieel document bezit met identiteitsgegevens die gecontroleerd kunnen worden in de basisregistratie persoonsgegevens. Aangezien identiteitsdocumenten kwijtraken, verlopen, worden ingetrokken of worden gestolen, is het nodig dat burgers met enige regelmaat hun (vernieuwde) document koppelen aan hun elektronische identificatiemiddel.
De leden van de D66-fractie constateren dat mensen die niet over een Android telefoon beschikken een kaartlezer moeten aanschaffen voor DigiD hoog. Zij vragen wat de kosten daarvan zijn en of deze door de overheid worden gedekt. Ook vragen deze leden zich af of er geen mogelijkheid is om DigiD hoog mogelijk te maken voor mensen met een iPhone of zonder fysieke kaart.
Ik acht het van wezenlijk belang dat alle gebruikers van gangbare mobiele apparaten de mogelijkheid krijgen tot het gebruik van de meer betrouwbare inlogmiddelen. Ik heb uw Kamer in de voortgangsrapportage eID van 16 juli 2018 over deze problematiek geïnformeerd. Ook in het AO digitale overheid van 31 oktober 2018 ben ik hierop ingegaan. Ik ben op diverse fronten bezig te onderzoeken of er bruikbare alternatieven zijn voor het aanschaffen van een kaartlezer om DigiD op betrouwbaarheidsniveau substantieel te installeren (DigiD op betrouwbaarheidsniveau hoog werkt zonder installatie). Zowel het geschikt maken van de IPhone als het verkennen van mogelijkheden zonder fysieke kaart vallen daaronder. Tot nu toe hebben deze acties nog geen succes opgeleverd. In de voortgangsrapportage van januari 2019 over eID zal ik uw Kamer hier opnieuw over informeren. De business case beschrijft de situatie als deze alternatieven niet op tijd beschikbaar komen.

10. Overgangsrecht en inwerkingtreding

Over dit onderdeel zijn geen vragen gesteld of opmerkingen gemaakt.

11. Consultatie en advies Autoriteit Persoonsgegevens

De leden van de CDA-fractie constateren dat bijvoorbeeld de Vereniging van Universiteiten en de Vereniging Hogescholen samen met DUO, Studielink en Surf een bijdrage hebben geleverd aan de consultatie, waarbij zij al direct hun zorgen hebben geuit over de technische en financiële gevolgen van het voorliggende wetsvoorstel. Het CDA vraagt of aangegeven kan worden waarom de brede consultatie in twee bladzijden van de memorie van toelichting wordt samengevat en afgedaan. Voorts vraagt de CDA-fractie zich af, welke organisaties een bijdrage hebben geleverd aan de consultatie en op welke wijze hun commentaren zijn verwerkt in het voorliggende wetsvoorstel.

De (openbare) consultatiereacties zijn gepubliceerd en in te zien via www.internetconsultatie.nl/wetgdi. Omwille van de toegankelijkheid en leesbaarheid bevat de memorie van toelichting de hoofdlijnen terzake,

waarbij wordt ingegaan op de belangrijkste commentaren en aanpassingen; deze zijn doorgevoerd omwille van met name de uitvoerbaarheid.

De leden van de CDA-fractie vragen zich af op welke wijze pensioenuitvoerders betrokken zijn geweest bij de vormgeving van het voorliggende wetsvoorstel.

Het Ministerie van SZW was nauw betrokken bij de voorbereiding van het wetsvoorstel. Ook de pensioensector was, in het kader van de (internet-)consultatie, in de gelegenheid om input te leveren op het wetsvoorstel. De Pensioenfederatie heeft van die gelegenheid gebruik gemaakt; de desbetreffende reactie is openbaar en voor een ieder vindbaar op www.internetconsultatie.nl/wetgdi.

De leden van de CDA-fractie vragen voorts of de regering de wens van de Pensioenfederatie deelt om de gegevensuitwisseling tussen overheid en pensioenfondsen integraal te verbeteren om te voorkomen dat pensioendeelnemers pensioenopbouw en pensioenuitkeringen mislopen.

Afgezien van het feit, dat uit de consultatiereactie van de Pensioenfederatie niet afgeleid kan worden dat de wens bestaat om de gegevensuitwisseling tussen overheid en pensioenfondsen integraal te verbeteren, valt het gestelde buiten doel en werkingssfeer van het onderhavige wetsvoorstel.

De leden van de CDA-fractie vragen tenslotte, of de opvatting van de Autoriteit Persoonsgegevens wordt gedeeld, dat wanneer burgers gebruik maken van digitale dienstverlening van de overheid er persoonsgegevens van hen worden verwerkt en dit een inbreuk oplevert op het recht op eerbiediging van de persoonlijke levenssfeer.

In feite maakt iedere verwerking van persoonsgegevens een inbreuk op de persoonlijke levenssfeer. Dit betekent niet dat persoonsgegevens door de overheid niet zouden mogen (of zelfs moeten) worden verwerkt. Het betekent wel dat daarvoor een gerechtvaardigde grondslag moet zijn. Omdat het hier om verwerkingen van persoonsgegevens gaat ter uitvoering van een overheidstaak, voorziet het wetsvoorstel in de grondslag ter zake en wordt de verwerking van persoonsgegevens ingekaderd, zodat deze gelegitimeerd en niet bovenmatig is.

II ARTIKELSGEWIJS

Artikel 8

De leden van de VVD-fractie vragen om een nadere verduidelijking van het voorgestelde artikel 8, leden 2 en 3.
Voor het antwoord verwijs ik kortheidshalve naar hetgeen onder punt 3 uiteen is gezet in reactie op de vraag van de VVD-fractie naar de betekenis van het feit, dat toegelaten publieke middelen in beginsel uitsluitend mogen worden gebruikt in het publieke domein.

Artikel 9, tweede lid

De leden van de CDA-fractie vragen hoe het doorlopen van een selectieprocedure uit de Aanbestedingswet zich verhoudt tot het feit, dat voor private bedrijfs- en organisatiemiddelen erkenning door middel van accreditatie plaatsvindt.

In de huidige praktijk zijn er meerdere private authenticatiediensten actief die naar tevredenheid het bedrijfs- en organisatiemiddel leveren.

Facturering en aansluiting van dienstverlening vindt daarbij decentraal plaats via zogeheten makelaars. Het wetsontwerp dat ter consultatie is gepubliceerd ging uit van hetzelfde model voor de toelating van private middelen voor burgers. In de consultatie is door dienstverleners echter nadrukkelijk verzocht de aansluitcomplexiteit en daarmee samenhangende kosten te reduceren in de vorm van één factuur en aansluiting via één koppelvlak. Dit heeft geresulteerd in de verantwoordelijkheid van de Minister van BZK voor een zogeheten routeringsvoorziening en de noodzaak om meer controle uit te oefenen op het aantal toe te laten private authenticatiediensten/middelen en de kosten. Door het Ministerie van BZK zal centraal worden betaald voor het gebruik van het private burgermiddel; de kosten worden doorbelast aan de dienstverleners. Via de selectieprocedure conform de Aanbestedingswet 2012 kunnen een of enkele private middelen – als alternatief voor een publiek middel – worden geselecteerd op aspecten zoals betrouwbaarheid, betaalbaarheid en dekkingsgraad. Na de selectieprocedure zal blijken of één of meer private authenticatiemiddelen geschikt zijn voor gebruik door burgers in het publieke domein. Indien één privaat middel wordt toegelaten, is het van belang dat de leverancier wordt verplicht tot het leveren ervan om de continuïteit van dienstverlening te waarborgen voor het geval het publieke middel onverhoopt niet beschikbaar is. Met het oog op zowel de gewenste verplichting tot uitvoering als de centrale verrekening is gekozen voor een selectieprocedure conform de Aanbestedingswet 2012 in plaats van accreditatie. Accreditatie ligt wel voor de hand bij private bedrijfs- en organisatiemiddelen. Als deze aan de eisen voldoen, worden ze door mij toegelaten; er is geen beperking voor wat betreft het aantal te erkennen private bedrijfs- en organisatiemiddelen.
Voorts vragen de leden van de CDA-fractie of het juist is, dat het wetsvoorstel de mogelijkheid open laat dat een bedrijfs- en organisatiemiddel gebruikt kan worden als burgermiddel, maar een burgermiddel niet als bedrijfs- en organisatiemiddel.

Deze veronderstelling van de CDA-fractie is onjuist. Natuurlijke personen die handelen in de uitoefening van een beroep of bedrijf kunnen het inlogmiddel voor burgers bij sommige dienstverleners gebruiken naast het bedrijfs- en organisatiemiddel. Het bedrijfs- en organisatiemiddel kan daarentegen niet gebruikt worden om in te loggen bij dienstverlening aan natuurlijke personen, die niet handelen in de uitoefening van beroep of bedrijf.
De leden van de CDA-fractie vragen of het juist is, dat toelating van een privaat middel afhankelijk is van de beoordeling van een ministerie en waarom private middelen niet toegelaten worden, als zij voldoen aan Europese regelgeving (eIDAS).

De constatering dat de toelating van private middelen afhankelijk is van de beoordeling door de Minister van BZK, is juist. Het voldoen aan de betrouwbaarheidseisen, die voortvloeien uit Europese regelgeving, is daarbij één van de criteria. Het komt de beheersbaarheid ten goede om ter zake van het private burgermiddel ook te selecteren op aspecten als betaalbaarheid en dekkingsgraad. Uitsluitend selecteren op het voldoen aan de Europese regelgeving zou kunnen leiden tot een onbeperkt aantal toegelaten middelen, hetgeen de sturing op het stelsel (ontwikkeling, beheer en incidenten), lage aansluitcomplexiteit en lage beheerlasten niet ten goede zou komen.
De leden van de CDA-fractie vragen hoe de voorgestelde selectieprocedure zich verhoudt tot de intentieverklaring van oktober 2015 tussen de Belastingdienst, vijf banken en de Betaalvereniging Nederland, waarin de uitgangspunten voor samenwerking tussen partijen werden vastgelegd in de vorm van een pilot. Zij vragen op welke wijze de succesvolle pilot van

inloggen met iDIN bij de Belastingdienst is verwerkt in het voorliggende wetsvoorstel.

Deze inmiddels beëindigde pilot met iDIN was beperkt tot het gebruik van private inlogmiddelen bij dienstverlening van de Belastingdienst. Pilots zijn qua aard, omvang en tijdsduur beperkt. De in het wetsvoorstel voorziene selectieprocedure beoogt een of enkele private burgermiddelen toe te laten voor overheidsbreed gebruik. De ervaringen met de pilots 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.

Artikel 12

De leden van de VVD-fractie hebben vragen over het voorgestelde artikel 12. Zij vragen zich af waarom is gekozen voor aanwijzing door de Minister van BZK, terwijl eerder is gedacht aan een attributendienst. De leden vragen zich af wat de voor- en nadelen van beide figuren zijn en wat dit voor een orgaan zou zijn geweest.
Aanvankelijk was in het wetsvoorstel voorzien in een attributendienst ten behoeve van het afgeven van elektronische verklaringen over bepaalde kenmerken of gegevens van een natuurlijk persoon of rechtspersoon. Het betrof een publieke voorziening of een door een private partij aan te bieden dienst waarvoor erkenning door de Minister van BZK was vereist. Hiermee werd beoogd ruimte te bieden aan een stelsel van publieke en private diensten die gegevens kunnen verstrekken die niet nodig zijn in het primaire proces van authenticatie, maar wel nodig zijn om overheidsdiensten te kunnen verlenen. Zo zijn sommige diensten gekoppeld aan een leeftijdsgrens of aan het hebben van bepaalde kwalificaties. Op basis van voortschrijdend inzicht is geconstateerd dat eerst bezien moet worden wat de behoefte is aan attributen en wat de (technische) mogelijkheden zijn om attribuutverstrekking te realiseren en integreren in het met het wetsvoorstel voorziene stelsel voor identificatie en authenticatie. Tot op heden functioneert in het publieke domein geen generieke attributenvoorziening. Wel worden op andere manieren attributen betrokken in het authenticatieproces. Zo wordt bij elektronische dienstverlening aan bedrijven het Handelsregister gebruikt als bron om kenmerken over een organisatie of rechtspersoon mee te geven. Met dit wetsvoorstel is aangesloten bij de bestaande praktijk, door gebruik te maken van beschikbare registers die attributen bevatten aan de hand waarvan een onderneming of rechtspersoon kan worden geïdentificeerd; deze attributen kunnen ook van belang zijn voor de toegang tot elektronische dienstverlening. Hiertoe krijgt de Minister van BZK – in voorkomende gevallen in overeenstemming met de Minister die het mede aangaat – de bevoegdheid om attributen aan te wijzen en nadere regels te stellen aan de wijze waarop erkende diensten het betrokken attribuut bij hun activiteiten moeten betrekken. Voordeel hiervan is dat bestaande overheidsdienstverlening ondersteund blijft; nadeel is dat een extra inspanning nodig is om aan gegevens te komen die nodig zijn om de overheidsdienst te verlenen. Het functioneren van een (publieke of private) attributendienst lijkt uit een oogpunt van efficiency meer opportuun. Nut, noodzaak en (technische) modaliteiten hiervan zijn echter nog niet uitgekristalliseerd.

Artikel 29

De leden van de VVD-fractie vragen zich tenslotte af hoe realistisch het is te streven naar gefaseerde inwerkingtreding van de wet met ingang van 1 januari 2019.

Op het moment van schrijven van wetsvoorstel en memorie van toelichting werd gekoerst op inwerkingtreding met ingang van 1 januari 2019. Dit is niet langer realistisch. Het streven is thans de wet medio 2019 in werking te kunnen laten treden.

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