No.W04.17.0400/I

**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**

Bij Kabinetsmissive van 21 december 2017, no.2017002224, heeft Uwe Majesteit, op voordracht van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet houdende regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), met memorie van toelichting.

Samenleving en overheid digitaliseren. Dit vereist regels over wat wordt genoemd de (generieke) digitale infrastructuur.[[1]](#footnote-1) Dit wetsvoorstel geeft regels voor de meest urgente onderdelen daarvan: elektronisch verkeer van en met de overheid (inbegrepen elektronische identificatiemiddelen), informatieveiligheid, toegang tot publieke dienstverlening voor burgers, en verantwoordelijkheidsverdeling voor infrastructuur en voorzieningen.

De Afdeling advisering van de Raad van State onderschrijft ten volle de noodzaak om op de kortst mogelijke termijn burgers, bedrijven en overheidsorganisaties elektronische identificatiemiddelen op een hoog beveiligd niveau te verschaffen. Betrouwbare toegang van burgers tot de overheid (“inloggen”) en tot publieke voorzieningen (zorg, onderwijs, werk en inkomen, persoonsregistraties, enzovoorts) en het veilig en ongestoord functioneren van overheidsorganisaties zijn hiervan afhankelijk. Daartoe is standaardisatie in de generieke digitale infrastructuur die overheidsorganisaties gebruiken een noodzakelijke voorwaarde. Om deze voorwaarde te realiseren moet één verantwoordelijk bewindspersoon deze technische standaarden vaststellen en aan overheidsorganen (centraal en decentraal) dwingend kunnen voorschrijven, met bevoegdheden van toezicht en ingrijpen. Het wetsvoorstel regelt zulks op zijn best halfslachtig. Dat is onwerkbaar[[2]](#footnote-2) en gegeven het cruciale belang van standaardisatie niet verantwoord.

Met het oog op toegang van de burger tot de overheid, stelt het wetsvoorstel niet alleen regels voor publieke identificatiemiddelen maar ook voor private. De Afdeling onderschrijft dat een stelsel van private naast publieke middelen nuttig is. Toegang van burgers tot de overheid is een basisrecht dat evenwel niet afhankelijk mag worden van private partijen. Dit uitgangspunt is niet onomwonden en consequent in het wetsvoorstel neergelegd; daarnaast is de precieze verhouding tussen publieke en private middelen onvoldoende inzichtelijk vormgegeven en toegelicht.

De Afdeling advisering van de Raad van State adviseert dit wetsvoorstel pas naar de Tweede Kamer te sturen nadat het op genoemde punten wezenlijk is aangepast.

1. Verantwoordelijkheid voor het stelsel als geheel

Het wetsvoorstel definieert en reguleert een deel van de generieke digitale infrastructuur: een stelsel dat burgers en bedrijven in staat stelt zich te identificeren[[3]](#footnote-3) om toegang te krijgen tot elektronische diensten van de overheid of van “aangewezen organisaties” van buiten de overheid (zoals pensioenfondsen, zorgverleners, zorgverzekeraars en instellingen voor hoger onderwijs). Het stelsel wordt bij en krachtens[[4]](#footnote-4) de wet ingesteld en vormgegeven; de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) krijgt een zorgplicht voor het inrichten en in stand houden van het stelsel.[[5]](#footnote-5)

Het wetsvoorstel vormt de eerste tranche van de Wet digitale overheid. Het regelt de meest urgente onderwerpen en biedt de basis voor verdere uitbreiding en modernisering, maar gaat daar overigens in de toelichting niet nader op in.

Deze generieke digitale infrastructuur is organisatorisch complex: het stelsel wordt gebruikt door honderden bestuursorganen (zoals provincies, gemeenten en zelfstandige bestuursorganen), rechterlijke organen en door organisaties buiten de overheid. Aan al deze bestuursorganen en organisaties worden in het wetsvoorstel eisen gesteld.

* Zij worden verplicht om alle inlogmiddelen die door de minister van BZK zijn toegelaten (naast het bekende DigiD en varianten daarvan ook een of meer private inlogmiddelen) te accepteren.[[6]](#footnote-6)
* Zij moeten ervoor zorgen dat de toegang tot hun elektronische diensten goed werkt en betrouwbaar en veilig is; zij rapporteren daarover aan de Minister.[[7]](#footnote-7) Zij moeten tevens bepalen voor welke diensten zij authenticatie op een bepaald betrouwbaarheidsniveau gaan voorschrijven.[[8]](#footnote-8)
* Zodra Nederland zijn eigen stelsel voor identificatiemiddelen heeft aangemeld bij de Europese Commissie moeten bestuursorganen ook alle buitenlandse identificatiemiddelen die bij de Commissie zijn aangemeld accepteren.

De generieke digitale infrastructuur beoogt burgers en bedrijven in staat te stellen op een veilige en gebruikersvriendelijke manier elektronisch contact te onderhouden met de overheid. Burgers hebben zelden goed zicht op het grote aantal organisaties waarover de overheidstaak is verdeeld en op die taakverdeling. Het is voor hen moeilijk te begrijpen en te hanteren wanneer elke organisatie, belast met een deel van de overheidstaak, de digitale communicatie met burgers in een ander tempo en op een andere manier aanpakt.

Dit burgerperspectief betekent dat de organisaties die worden aangesloten op de generieke digitale infrastructuur hun communicatie op een gestandaardiseerde en voorspelbare manier dienen aan te bieden; en dat de invoering en modernisering van de elektronische communicatie niet teveel in de tijd moet uiteenlopen. Het belang van standaardisatie en synchronisatie speelt niet alleen bij deze eerste tranche, maar is ook van belang bij volgende tranches van de Wet digitale overheid.

De Afdeling acht het dan ook van belang dat de minister van BZK over voldoende bevoegdheden beschikt om de standaardisatie in technisch opzicht en de synchronisatie van dit proces daadwerkelijk te kunnen realiseren – niet alleen op basis van dit voorstel, maar ook voor de verdere uitbouw van de digitale overheidscommunicatie. Standaardisatie gaat immers niet vanzelf.

Vanuit dit belang en perspectief acht de Afdeling het wetsvoorstel op de navolgende onderdelen onvoldoende.[[9]](#footnote-9)

* Bevoegdheden. De verhouding tussen de minister die verantwoordelijk is voor het beheer van de generieke digitale infrastructuur en andere ministers, bestuursorganen en andere overheden is op het punt van de technische standaardisatie onduidelijk. De minister “bevordert” de interoperabiliteit tussen infrastructuren, diensten en organisaties,[[10]](#footnote-10) maar kan deze niet dwingend voorschrijven. Zo ontbreekt in het voorstel een bevoegdheid om besluiten van overheidsorganisaties over standaarden en andere technische specificaties die een snelle en betrouwbare aansluiting op de generieke digitale infrastructuur in de weg staan te schorsen of te vernietigen, alsmede een bevoegdheid om op deze punten bindende aanwijzingen te geven en zo nodig in laatste instantie werkzaamheden zelf te doen uitvoeren, op kosten van de betreffende organisatie.
* Bestuurlijk toezicht.[[11]](#footnote-11) De minister van BZK krijgt geen bijzondere toezichtsbevoegdheden. Volgens de toelichting geldt het reguliere toezicht (aangevuld met een jaarlijkse audit, uit te brengen aan de minister). Meer concreet: elke vakminister oefent toezicht uit op de eigen uitvoeringsorganisaties, en op de zelfstandige bestuursorganen en de aangewezen organisaties die op zijn beleidsterrein liggen. En: decentrale overheden zijn zelf verantwoordelijk voor de naleving van de wet. De minister heeft alleen de bevoegdheden van het zogenoemde generiek interbestuurlijk toezicht: van rijk op provincies, van provincies op gemeenten. Dat toezicht is bedoeld als sober en terughoudend en in hoofdzaak gericht op bestuurlijke en financiële verhoudingen. Het is bedoeld noch ingericht voor technische, organisatorische en uitvoerende kwesties, zoals die zich voordoen in de digitale (overheids-)infrastructuur. De vormgeving van het bestuurlijk toezicht moet om die reden opnieuw worden doordacht en het voorstel moet vervolgens worden aangepast.
* Toezicht op naleving van voorschriften. Het voorstel maakt het mogelijk om toezichthouders aan te wijzen, die de beschikking krijgen over de klassieke toezichtsbevoegdheden. Zo kunnen zij plaatsen betreden, inzage vorderen van zakelijke gegevens en bescheiden, zaken onderzoeken en daarvan monsters nemen. Zij kunnen toezicht houden op organisaties die zijn aangesloten op de generieke digitale infrastructuur, op bedrijven die private identificatiemiddelen verschaffen en op bedrijven die worden ingeschakeld bij de identificatie.[[12]](#footnote-12) Deze fysieke vorm van toezicht past niet goed in de verhouding met bestuursorganen. Waar het gaat om toezicht op genoemde bedrijven is dat wel voorstelbaar. Het valt echter op dat geen bevoegdheden worden toegekend die toegesneden zijn op een digitaal stelsel, zoals toegang tot geautomatiseerde programma’s en gegevens. Het voorstel verdient nadere uitwerking en toelichting, met daarbij jegens bedrijven als uitgangspunt dat er een passend instrumentarium moet zijn om te kunnen ingrijpen, vergezeld van passende waarborgen.

* Calamiteiten. Bij een ernstige storing of ernstige aantasting van de werking, beveiliging of betrouwbaarheid van de elektronische dienstverlening, of bij misbruik of oneigenlijk gebruikt van de toegang tot elektronische dienstverlening, kan de Minister de toegang tot elektronische dienstverlening van een bestuursorgaan of aangewezen organisatie onderbreken.[[13]](#footnote-13) Het valt op dat de minister pas kan ingrijpen wanneer een storing of aantasting zich al voordoet, en niet al bij een ernstige dreiging daarvan. Verder is de samenhang met andere wetgeving van belang. In het voorstel van een Cybersecuritywet, waarin de EU-richtlijn over beveiliging van netwerk- en informatiesystemen wordt geïmplementeerd, worden instanties aangewezen met een coördinerende taak bij het beveiligen van vitale infrastructuren (“bevoegde autoriteiten”). De minister van Economische Zaken en Klimaat wordt aangewezen als bevoegde autoriteit voor de digitale infrastructuur.[[14]](#footnote-14) Ook in het stelsel van de Telecommunicatiewet komen noodbevoegdheden (bevoegdheden die alleen toegepast mogen worden onder buitengewone omstandigheden) toe aan de minister van Economische Zaken en Klimaat.[[15]](#footnote-15) Dit roept de vraag op waarom de Minister van BZK geen bijzondere bevoegdheden heeft voor het overheidsgedeelte van de digitale infrastructuur, dat onderwerp is van het voorliggende wetsvoorstel.
* Identiteitsfraude. In de toelichting wordt terecht ingegaan op de groei van het probleem van identiteitsfraude.[[16]](#footnote-16) Dit probleem hangt nauw samen met de uitgifte van identificatiemiddelen, maar ook met het inloggen met zulke middelen bij de overheid. De minister krijgt de plicht om maatregelen te treffen bij een vermoeden van misbruik van een identificatiemiddel.[[17]](#footnote-17) Wat in het voorstel ontbreekt is een duidelijk belegde verantwoordelijkheid voor het oplossen van de problemen waar slachtoffers van identiteitsfraude mee te maken krijgen. Zo is niet geregeld welk orgaan daarvoor verantwoordelijk is, waar het slachtoffer zich kan melden en hoe hij op een eenvoudige manier een identificatiemiddel tijdelijk kan onderbreken, bijvoorbeeld bij zoekgeraakte of gestolen documenten.[[18]](#footnote-18)

De Afdeling adviseert het voorstel aan te passen aan de hand van de hiervoor genoemde punten.

2. Publieke en private identificatiemiddelen

Het voorstel beoogt te regelen dat burgers, bedrijven en organisaties op een betrouwbare manier kunnen inloggen bij bestuursorganen en aangewezen organisaties (met name zorginstellingen, zorgverleners, instellingen voor hoger onderwijs en pensioenfondsen).

Voor burgers komen er door de overheid gecreëerde identificatiemiddelen op drie “betrouwbaarheidsniveaus” (deze betrouwbaarheidsniveaus – laag, substantieel en hoog – zijn gedefinieerd in de “eIDAS-verordening” van de Europese Unie).[[19]](#footnote-19) Het huidige DigiD, dat al sinds 2005 in gebruik is, heeft betrouwbaarheidsniveau “laag”. Het zal worden aangevuld met “Versterkt DigiD” op niveau “substantieel”.[[20]](#footnote-20) Verder komt er een identificatiemiddel via een chip op de identiteitskaart en het rijbewijs, op betrouwbaarheidsniveau “hoog”. De burger betaalt voor de verstrekking van deze middelen leges.[[21]](#footnote-21) Daarnaast komen er voor burgers private identificatiemiddelen, die door de minister van BZK worden toegelaten. De eIDAS-verordening biedt de mogelijkheid om zulke private middelen toe te laten (die dan moeten voldoen aan de betrouwbaarheidseisen van de verordening), maar verplicht daar niet toe.

Bedrijven en organisaties kunnen uitsluitend inloggen met een zogeheten bedrijfs- en organisatiemiddel, dat via publiek-private samenwerking is ontwikkeld en door de Minister van BZK wordt erkend.[[22]](#footnote-22) De inlogmethode voor bedrijven en organisaties zal ook gelden voor overheidsorganisaties.

Een burger die, om toegang tot de overheid krijgen, een privaat identificatiemiddel gebruikt, bijvoorbeeld door het hanteren van een bankpas voorzien van een elektronische identificatie, moet zich realiseren dat hij daarmee juridisch gezien een overeenkomst afsluit met de onderneming die dat middel verschaft (in dit voorbeeld, zijn bank), de voorwaarden die die onderneming hanteert accepteert en voor deze dienstverlening betaalt.

Het voorstel kiest aldus voor een gemengd publiek en privaat stelsel. De Afdeling begrijpt de keuze om naast publieke, ook private identificatiemiddelen toe te staan. Economische ontwikkeling, innovatie en keuzevrijheid van burgers en bedrijven worden immers bevorderd indien het stelsel meerdere identificatiemiddelen toelaat. Het is bovendien van wezenlijk belang dat de eenzijdige afhankelijkheid van één middel in de digitale infrastructuur (‘single points of failure’) wordt verkleind door voor eenzelfde doel, in dit geval identificatie en inloggen, meer middelen (instrumenten) beschikbaar te doen zijn. De Afdeling merkt evenwel op dat de vormgeving van een stelsel van private naast publieke middelen ook de navolgende vragen oproept die in het wetsvoorstel nadere toelichting of aanpassing behoeven.

* Basisrecht. Toegang van burgers (en bedrijven) tot en communicatie met de overheid is een basisrecht, een publieke verantwoordelijkheid en mag niet afhankelijk worden van private partijen. Daarom moet de overheid zelf, met eigen middelen, waarborgen – niet alleen juridisch, maar ook feitelijk – dat burgers elektronische toegang tot de overheid hebben op een voldoende hoog betrouwbaarheidsniveau. Dit principiële uitgangspunt is in de toelichting bij het wetsvoorstel niet onomwonden verwoord en in het voorstel en de toelichting evenmin consequent doorgevoerd. Er is bijvoorbeeld een risico dat het toelaten van private middelen de invoering van publieke middelen op verschillende betrouwbaarheidsniveaus vertraagt of hindert; het Bureau ICT-toetsing heeft op dit risico gewezen.[[23]](#footnote-23)
* Inloggen door de overheid bij de overheid. Het voorstel bepaalt dat overheidsorganisaties alleen met (private) bedrijfs- en organisatiemiddelen kunnen inloggen bij bestuursorganen als zij elkaar beveiligde gegevens willen toesturen (dat wil zeggen: als de gegevensuitwisseling plaatsvindt op betrouwbaarheidsniveau substantieel of hoog).[[24]](#footnote-24) Het is de Afdeling niet duidelijk waarom vertrouwelijk gegevensverkeer tussen overheden onderling alleen mogelijk zou moeten zijn via private middelen. Het ligt juist meer in de rede dat de overheid door middel van door de overheid gecreëerde identificatiemiddelen zoveel mogelijk controle heeft over zulke gegevensuitwisseling om haar verantwoordelijkheid voor een veilig verloop te kunnen waarmaken.
* Marktordening en gelijk speelveld. De minister kan ingevolge dit wetsvoorstel[[25]](#footnote-25) het gebruik van private identificatiemiddelen voor toegang tot de overheid toelaten. Hij bepaalt op dat moment hoeveel private middelen hij toelaat en de duur van de toelating.[[26]](#footnote-26) Het wetsvoorstel gaat uit van een situatie van schaarste en kiest voor een stelsel met een vergelijkende toets op basis van vooraf bekendgemaakte criteria.[[27]](#footnote-27) De veronderstelde schaarste en de keuze voor dit stelsel wordt slechts summier toegelicht. Er is met andere woorden niet gekozen voor een open stelsel, waarbij iedere aanbieder van een identificatiemiddel die aan bepaalde eisen voldoet tot de markt wordt toegelaten.[[28]](#footnote-28) Bij de verdeling van schaarse rechten, het in het wetsvoorstel gekozen stelsel, dient evenwel een gelijk speelveld te bestaan. Dat houdt in dat een passende mate van openbaarheid moet zijn verzekerd over het aantal toelatingen en de duur daarvan, de selectieprocedure, het aanvraagtijdvak en de toe te passen criteria. De minister moet hierover tijdig voorafgaand aan de start van de procedure duidelijkheid scheppen. Die duidelijkheid bevatten het wetsvoorstel en de toelichting nog niet. Er wordt in het wetsvoorstel evenmin bijzondere aandacht besteed aan (bestaande) private authenticatiediensten die ook gebruikt (kunnen) worden door burgers om zich te identificeren bij overheidsdiensten, en aan de vraag welke regels daarvoor (gaan) gelden dan wel hoe deze bestaande private authenticatiemiddelen zich (gaan) verhouden tot het in het wetsvoorstel beoogde stelsel van toelating van private middelen.

De Afdeling adviseert de hiervoor genoemde punten nader te bezien en waar nodig het voorstel aan te passen.

3. Gebruik Burgerservicenummer buiten de overheid

Het wetsvoorstel stelt regels voor elektronische dienstverlening door de overheid, maar is mede van toepassing op organisaties buiten de overheid die nu al gebruik maken van het Burgerservicenummer (BSN) en DigiD: instellingen voor hoger onderwijs, pensioenfondsen, zorgaanbieders en zorgverzekeraars. Ook andere organisaties die het BSN mogen gebruiken kunnen – bij algemene maatregel van bestuur of bij ministerieel besluit – onder het stelsel worden gebracht.[[29]](#footnote-29) Zulke organisaties kunnen dan gebruik maken van het stelsel van publieke en private identificatiemiddelen, dat in het voorstel wordt neergezet. Zij worden dan aangesloten op de generieke digitale infrastructuur en komen onder het toezicht te staan van de minister van BZK.[[30]](#footnote-30)

De Wet algemene bepalingen burgerservicenummer bepaalt weliswaar dat organisaties buiten de overheid het BSN alleen mogen gebruiken als zij daar bij of krachtens de wet toestemming voor hebben gekregen, maar bevat zelf geen criteria. Het voorliggende wetsvoorstel bevat die criteria evenmin. Dat betekent dat de reikwijdte van het wetsvoorstel bij bijzondere wet kan worden uitgebreid en dat er geen algemene criteria zijn om te bepalen welke organisaties daarvoor in aanmerking komen.[[31]](#footnote-31) De Afdeling acht het van belang dat het gebruik van publieke identificatiemiddelen en het BSN alleen wordt uitgebreid tot organisaties buiten de overheid op basis van duidelijke, wettelijke criteria. Zij adviseert dergelijke criteria op te nemen in dit wetsvoorstel of in de Wet algemene bepalingen burgerservicenummer.

4. Bescherming van persoonsgegevens

Het wetsvoorstel brengt met zich mee dat een groot aantal persoonsgegevens op diverse plaatsen zal worden verwerkt. De bevoegdheid om persoonsgegevens, waaronder het BSN, te verwerken wordt toegekend aan de minister van BZK, bestuursorganen, aangewezen organisaties, uitgevers van private identificatiemiddelen en erkende diensten die betrokken zijn bij authenticatie. De enige beperking aan deze verwerkingsbevoegdheid is dat verwerking noodzakelijk moet zijn voor de uitvoering van de wet of voor de werking van het identificatiemiddel. Bij algemene maatregel van bestuur worden nadere regels gesteld.[[32]](#footnote-32) De Afdeling heeft twee aandachtspunten.

a. *Daadwerkelijke bescherming*

De Afdeling constateert dat de toelichting op het wetsvoorstel terecht uitgebreid en adequaat ingaat op de verhouding met de Algemene Verordening Gegevensbescherming (AVG).[[33]](#footnote-33) Daarbij is van belang dat de AVG, anders dan de privacyrichtlijn[[34]](#footnote-34), een verordening is die rechtstreekse werking in de Nederlandse rechtsorde heeft. Dit brengt met zich dat de wetgever slechts ruimte heeft om nadere regels te stellen voor zover de AVG dat uitdrukkelijk toelaat. De vraag is daarom in hoeverre er onder het regime van de AVG nog bevoegdheid is om bij algemene maatregel van bestuur nadere regels te stellen voor de afzonderlijke in de toelichting aangesneden onderwerpen.[[35]](#footnote-35) Daarop gaat de toelichting niet in. Voor zover de AVG wel ruimte biedt voor dergelijke regels gaat de Afdeling er van uit dat in dat kader passende aandacht zal worden geschonken aan de vraag hoe burgers begrijpelijk en nauwkeurig worden geïnformeerd over keuzes, toestemmingen en machtigingen die zij worden geacht te maken en te geven.

De Afdeling adviseert in de toelichting op het bovenstaande in te gaan en het wetsvoorstel zo nodig aan te passen.

b. *Inloggen door een ander dan de burger*

De Afdeling vraagt voorts aandacht voor het fenomeen van inloggen door een ander dan de burger zelf. Bij ministeriële regeling kan worden bepaald dat een publiek inlogmiddel kan worden gebruikt om aangewezen organisaties toegang te geven tot een systeem voor de elektronische uitwisseling van gegevens. Volgens de toelichting kan het gaan om de uitwisseling van patiëntgegevens binnen en tussen zorginstellingen. Gebruik van een publiek identificatiemiddel is van belang om zeker te weten dat het om de juiste persoon gaat, aldus de toelichting.[[36]](#footnote-36)

Het artikel en de toelichting zijn niet duidelijk waar het gaat om de rol van de burger. Indien de bepaling inhoudt dat het identificatiemiddel (en de gegevens die met een identificatiemiddel kunnen worden gegenereerd) niet wordt gebruikt door de burger zelf maar door een zorginstelling, zonder dat de burger daarvan op de hoogte is, dan staat dat haaks op het stelsel. Een identificatiemiddel is immers een middel in handen van de burger, die met dat middel toegang krijgt tot een elektronische systeem van een bestuursorgaan of bijvoorbeeld een zorginstelling. Hij is de unieke gebruiker van dat middel. Om diezelfde reden mogen burgers ook niet toestaan dat een ander een fotokopie maakt van hun paspoort of identiteitskaart. De Afdeling adviseert de bepaling te heroverwegen of nauwkeuriger te formuleren.

5. Machtiging en elektronische handtekening

a. *Betrouwbaarheidsniveaus bij machtiging*

Natuurlijke personen, bedrijven en organisaties kunnen elektronisch gemachtigd worden om in te loggen namens een natuurlijk persoon, bedrijf of organisatie.[[37]](#footnote-37) Het voorstel stelt geen eisen aan de betrouwbaarheid van zulke machtigingen. Dit contrasteert sterk met de regels voor inloggen zelf, die gebaseerd zijn op een uitgewerkt stelsel van betrouwbaarheidsniveaus.

* Een stelsel van machtigingen zal tenminste aan dezelfde betrouwbaarheidseisen moeten voldoen als het stelsel van identificatiemiddelen: als een bestuursorgaan alleen elektronische identificatie op betrouwbaarheidsniveau substantieel of hoog accepteert, zal ook identificatie via machtiging op dat niveau moeten plaatsvinden.
* Daarnaast zal onderzocht moeten worden welke aanvullende eisen zullen moeten gelden ter bescherming van de persoon die de machtiging verleent. Zo kan worden bepaald dat een machtiging alleen betrekking heeft op nauwkeurig omschreven handelingen en dat de machtiging voor een beperkte periode geldt.[[38]](#footnote-38)

De Afdeling adviseert het voorstel op deze punten aan te passen.

b. *Gebruik van DigiD als elektronische handtekening*

DigiD wordt in sommige gevallen gebruikt als elektronische handtekening, bij voorbeeld om de elektronische aangifte inkomstenbelasting te ondertekenen. Bovendien wordt DigiD Machtigen in sommige gevallen gebruikt om namens de gemachtigde een elektronische handtekening te zetten. Voor deze toepassingen lijkt onvoldoende wettelijke grondslag te bestaan.[[39]](#footnote-39) Indien het de bedoeling is dat DigiD en andere identificatiemiddelen en middelen voor elektronische machtiging, ook in de toekomst, zullen worden gebruikt als elektronische handtekening, acht de Afdeling het van belang dit wettelijk te regelen.

De Afdeling adviseert het voorstel met dit punt aan te vullen.

6. Verhouding tussen wet en uitvoeringsregelingen

a. *Algemeen*

In haar advies over het voorstel van Wet modernisering elektronisch bestuurlijk verkeer heeft de Afdeling opgemerkt dat is beoogd het voorstel techniekonafhankelijk vorm te geven, maar dat in dat wetsvoorstel onder de abstracte, moeilijk te begrijpen formuleringen in feite concrete begrippen worden aangeduid. Het gaat dan om begrippen als MijnOverheid, berichtenbox en contact- of webformulieren. De Afdeling adviseerde die begrippen in het voorstel zelf uitdrukkelijk te noemen en de abstracte termen achterwege te laten.[[40]](#footnote-40)

Het nu voorliggende voorstel is eveneens abstract en techniekonafhankelijk geformuleerd. De uitwerking van de abstracte begrippen wordt gedelegeerd aan lagere regelgeving. Zo zijn begrippen als DigiD, MijnOverheid, DigiD Machtigen en het BSN-Koppelregister geregeld in de (ministeriële) Regeling voorzieningen GDI, die – met aanpassingen – onder het wetsvoorstel zal komen te hangen. Het is aannemelijk dat MijnOverheid en het BSN-Koppelregister, die een centrale plaats innemen in de communicatie tussen overheid en burger, de komende jaren zullen blijven bestaan. Het is meer passend om deze centrale onderdelen van de generieke digitale infrastructuur in de wet zelf te regelen.

De Afdeling adviseert de hoofdzaken van de Regeling voorzieningen GDI in de wet zelf op te nemen.

b. *Uitgifte van identificatiemiddelen*

De minister van BZK is verantwoordelijk voor de uitgifte van DigiD op niveau laag, en op termijn voor de uitgifte van DigiD op hogere niveaus. Het voorstel geeft hem wel de verantwoordelijkheid voor de generieke digitale infrastructuur, maar niet voor de uitgifte van deze publieke identificatiemiddelen. In lijn met punt 1 van dit advies, waarin wordt benadrukt dat de minister voldoende bevoegdheden moet hebben om zijn verantwoordelijkheid voor het stelsel waar te maken, adviseert de Afdeling de verantwoordelijkheid voor dit centrale onderdeel van het stelsel wettelijk te regelen.

7. De Afdeling verwijst naar de bij dit advies behorende redactionele bijlage.

De Afdeling advisering van de Raad van State geeft U in overweging het voorstel van wet niet te zenden aan de Tweede Kamer der Staten-Generaal dan nadat met het vorenstaande rekening zal zijn gehouden.

De vice-president van de Raad van State,

Redactionele bijlage bij het advies van de Afdeling advisering van de Raad van State betreffende no.W04.17.0400/I

* In het wetsvoorstel zelf tot uitdrukking brengen dat het voorstel een eerste tranche van regelgeving voor digitalisering van de overheid bevat (de citeertitel wekt een verwachting die nu nog niet wordt waargemaakt). In de toelichting uitvoeriger ingaan op de volgende tranches dan nu gebeurt (paragraaf I.1 (Aanleiding)).
* In artikel 1 het begrip “elektronische dienstverlening” vervangen door een neutralere term (bijvoorbeeld elektronische communicatie of elektronisch berichtenverkeer), om te voorkomen dat handelingen zoals het intrekken van een vergunning, het opleggen van een last onder bestuursdwang en het opleggen van een bestuurlijke boete worden gekwalificeerd als dienstverlening.
* In artikel 1 een definitie opnemen van “de voorziening, bedoeld in artikel 5, eerste lid, onderdeel b,”, bijvoorbeeld: elektronische machtiging. Die term kan dan gebruikt worden in de artikelen 8, eerste, tweede en derde lid, en 10, tweede lid.
* Eén begrip introduceren en definiëren dat zowel bestuursorganen als aangewezen organisaties omvat; de term “bestuursorgaan” niet gebruiken in een betekenis die afwijkt van die in de Algemene wet bestuursrecht (artikel 2, eerste lid).
* Punt 3 van het advies van de Afdeling advisering van 12 februari 2018 over het Tijdelijk besluit digitale toegankelijkheid overheid, zaak W04.18.0021, in acht nemen bij het aanwijzen van standaarden op basis van artikel 3. Voorts de afbakening van organisaties in artikel 3 afstemmen op artikel 1 van dat Tijdelijk besluit.
* Artikel 3 onderbrengen in een afzonderlijk hoofdstuk: het artikel regelt een apart onderwerp en betreft een grotere groep organisaties dan de rest van het voorstel.
* Artikel 4 overbrengen naar en combineren met artikel 6. In het tweede lid regelen aan welke eisen een auditor moet voldoen (de in de wetgeving meeste gebruikelijke betekenis – controleur van jaarrekeningen – zal hier niet zijn bedoeld).
* De regels voor authenticatiediensten, attributendiensten, machtigingsdiensten en ontsluitende diensten niet opnemen in § 4.3 (Elektronische dienstverlening aan bedrijven), nu die diensten (blijkens de definities in artikel 1) ook gaan over identificatie van of namens natuurlijke personen.
* Artikel 11, negende lid, uitbreiden tot registers waarin natuurlijke personen zijn opgenomen, nu het blijkens de toelichting op het artikel mede gaat om het BIG-register.
* In artikel 25 verduidelijken dat bij een experiment alleen kan worden afgeweken van het verbod om andere dan toegelaten middelen te accepteren, nu dat blijkens de toelichting de bedoeling is. Voorts aanwijzing 2.42, tweede lid, met toelichting, van de Aanwijzingen voor de regelgeving (Ar) in acht nemen.
* Artikel 26 achterwege laten, nu dit al is geregeld (artikel XI, derde lid, van de Wet elektronisch berichtenverkeer belastingdienst).
* Te zijner tijd de verwijzing naar artikel X van de Wet elektronisch berichtenverkeer belastingdienst in artikel 2:17, tweede lid, van het voorstel van Wet modernisering elektronisch bestuurlijk verkeer vervangen door een verwijzing naar artikel 5 van de Wet digitale overheid.
* De Regeling voorzieningen GDI omhangen. Voorts een bepaling opnemen waarin de zelfstandige algemene maatregel van bestuur ter implementatie van EU-richtlijn 2016/2102 wordt omgehangen naar artikel 3, tweede en derde lid.
* Artikel 29, derde lid, zo aanpassen dat het tijdstip waarop de acceptatieplicht (artikelen 7 en 13) ingaat voor de verschillende bestuursorganen en aangewezen organisaties blijkt uit een Staatsblad of de Staatscourant (kenbaarheidsvereiste, vergelijk aanwijzing 4.15 Ar), bijvoorbeeld door te bepalen dat het aansluitschema wordt gepubliceerd in de Staatscourant.
1. De generieke digitale infrastructuur bestaat uit standaarden, producten en digitale basisvoorzieningen die gezamenlijk gebruikt worden door overheden, publieke organisaties en in een aantal gevallen ook private partijen. Hierdoor is het mogelijk om primaire processen doelmatig in te richten en te blijven ontwikkelen. [↑](#footnote-ref-1)
2. Belangrijke redenen dat grote ICT projecten in de overheid vastlopen, zoals recent de Basisregistratie personen en het KEI-project voor de rechtspraak, zijn het gebrek aan daadwerkelijke standaardisatie en aan éénduidige sturing. Rapport van de commissie Parlementair onderzoek naar ICT-projecten bij de overheid (commissie-Elias), Kamerstukken II 2014/15, 33 326, nr. 5, blz. 72-73. [↑](#footnote-ref-2)
3. Het voorstel maakt onderscheid tussen identificatie (opgeven van de identiteit) en authenticatie (controleren van de juistheid van de opgegeven identiteit). De vragen in dit advies gaan over identificatie, huiselijk verwoord als “inloggen”. [↑](#footnote-ref-3)
4. Artikel 3; bij algemene maatregel van bestuur worden nadere regels gesteld over standaarden en het functionele toepassingsbereik. [↑](#footnote-ref-4)
5. Artikel 5. [↑](#footnote-ref-5)
6. Artikelen 7, eerste lid, en 13, tweede lid. [↑](#footnote-ref-6)
7. Artikel 4. [↑](#footnote-ref-7)
8. Artikel 6, tweede lid. [↑](#footnote-ref-8)
9. Onverlet artikel 3, tweede en derde lid. De bepaling dat bij algemene maatregel van bestuur standaarden kunnen worden aangewezen en bepaald, neemt de kanttekeningen bij de hierna genoemde onderdelen niet weg. Die bevoegdheid is immers beperkt tot het aanwijzen van open standaarden voor software. [↑](#footnote-ref-9)
10. Artikel 5. [↑](#footnote-ref-10)
11. Artikel 15. [↑](#footnote-ref-11)
12. Artikel 15 in combinatie met titel 5.2 van de Algemene wet bestuursrecht. [↑](#footnote-ref-12)
13. Artikel 16. [↑](#footnote-ref-13)
14. Artikel 4, eerste lid, van het voorstel van een Cybersecuritywet, Kamerstukken II 2017/18, 34 883, nr. 2. [↑](#footnote-ref-14)
15. Hoofdstuk 14 van de Telecommunicatiewet. [↑](#footnote-ref-15)
16. Toelichting, paragraaf 5.2 (Aanpak van misbruik en identiteitsfraude). [↑](#footnote-ref-16)
17. Artikel 16, vierde lid. [↑](#footnote-ref-17)
18. Advies van de commissie evaluatie pilots publieke en private authenticatiemiddelen (commissie-Kuipers), 31 mei 2016, Kamerstukken II 2015/16, 26 643, nr. 419, bijlage, blz. 30. [↑](#footnote-ref-18)
19. Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB 2014, L 257). [↑](#footnote-ref-19)
20. Artikel 3, derde lid, van de Regeling voorzieningen GDI. Bij het inloggen met DigiD wordt een extra controle uitgevoerd aan de hand van een niet-zichtbare chip in een bestaand paspoort, identiteitskaart of rijbewijs. De chip kan worden uitgelezen met een kaartlezer of met een smartphone. Nadere uitleg is te vinden in Stcrt. 2017, Nr. 59901, en in Evaluatierapport pilot DigiD-RDA, DigiD versterkt met controle van het identiteitsbewijs van de RDW, 23 mei 2016, Kamerstukken II 2015/16, 26 643, nr. 419, bijlage. [↑](#footnote-ref-20)
21. Artikel 18. [↑](#footnote-ref-21)
22. Artikel 7, tweede lid, aanhef en onderdeel a, in combinatie met artikel 11, eerste lid. Zie ook de definities van “publiek identificatiemiddel” en “privaat identificatiemiddel” in artikel 1. [↑](#footnote-ref-22)
23. Advies van 13 mei 2016, kenmerk 20 16-0000282302, blz. 6. [↑](#footnote-ref-23)
24. Artikel 13, eerste lid, in combinatie met artikel 6, tweede lid, van de Handelsregisterwet 2007; toelichting op artikel 11. Zie ook de toelichting op artikel 13, waar gesteld wordt: “Bovendien mogen [bestuursorganen en aangewezen organisaties] uitsluitend toegang verlenen tot hun dienstverlening in geval gebruik wordt gemaakt van een erkend bedrijfs- en organisatiemiddel.” [↑](#footnote-ref-24)
25. Artikel 9, tweede lid. [↑](#footnote-ref-25)
26. Artikel 9, tweede en derde lid. [↑](#footnote-ref-26)
27. Artikel 9, tweede lid, aanhef en onderdeel c. [↑](#footnote-ref-27)
28. Toelichting op artikel 9, tweede lid. [↑](#footnote-ref-28)
29. Artikel 2. [↑](#footnote-ref-29)
30. Artikel 15. [↑](#footnote-ref-30)
31. Zie bijvoorbeeld artikel 8, tweede lid, en de toelichting op dit artikellid. Deze bepaling is, ook met de toelichting erbij, niet zonder meer duidelijk. Zorgverzekeraars en zorgverleners hebben immers het recht het BSN te gebruiken. Daar komt bij dat de bepaling zelf een onbepaalde, en daardoor onbeperkte, mogelijkheid biedt om – bij ministeriële regeling – te bepalen dat publieke identificatiemiddelen kunnen worden gebruikt buiten de publieke sector. [↑](#footnote-ref-31)
32. Artikel 14. [↑](#footnote-ref-32)
33. Verordening (EU) 2016/679 van het Europees Parlement en de Raad, 27 april 2016, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, PB 2016, L 119. De verordening treedt in werking op 25 mei 2018. [↑](#footnote-ref-33)
34. Richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Pb 1995, L 281). [↑](#footnote-ref-34)
35. Zie de onderwerpen besproken in paragraaf 4 (Privacy) van de toelichting. [↑](#footnote-ref-35)
36. Artikel 8, derde lid, en de toelichting op dat artikel. [↑](#footnote-ref-36)
37. Artikelen 5, eerste lid, onderdeel b, en 11, tiende lid. [↑](#footnote-ref-37)
38. Vergelijk artikel 5, tweede en zesde lid, van de Regeling voorzieningen GDI. [↑](#footnote-ref-38)
39. DigiD wordt alleen geregeld in de Regeling voorzieningen GDI en daar gedefinieerd als een middel voor de toegang tot elektronische dienstverlening (artikel 1). Daar wordt aan toegevoegd dat DigiD alleen mag worden gebruikt voor het doel waarvoor het is bestemd (artikel 3, zevende lid). [↑](#footnote-ref-39)
40. Advies no. W04.17.0190 van 15 maart 2018, punt 4. [↑](#footnote-ref-40)