Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 788

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 oktober 2021

Met mijn brief van 19 maart 2021 (Kamerstuk 26 643, nr. 750) informeerde ik Uw Kamer over de voortgang van de aanpak in het domein Toegang. In deze brief informeer ik Uw Kamer over de voortgang die de afgelopen maanden binnen dit domein geboekt is en geef ik een vooruitblik op de (nabije) toekomst. Daarnaast maak ik van deze gelegenheid gebruik om Uw Kamer te informeren over de invoering van de Wet elektronische publicaties (Kamerstuk 35 218). Gelet op de complexiteit van dit domein en de oproep van de stakeholders (gedaan in het bijgaande assurance rapport van PWC)[1] ga ik in deze voortgangsrapportage uitvoerig in op de samenhangende delen van het domein en de actuele stand van zaken. Om ervoor te zorgen dat Uw Kamer gemakkelijk kan zien wat de voortgang is ten aanzien van vorige voortgangsrapportages, die nog een andere opbouw hadden, heb ik een bijlage toegevoegd[2]. Deze bijlage laat zien hoe de beleidsinzet van de vorige voortgangsrapportages aansluit op de huidige rapportage.

1. Inleiding en context

In essentie kan de digitale overheid gezien worden als een huis met verschillende kamers. In iedere kamer bevindt zich een dienstverlener van de overheid, zoals de Belastingdienst of de RDW. Het domein Toegang waarborgt een veilige, betrouwbare en toegankelijke toegang tot de digitale dienstverlening voor burgers en bedrijven.

Met DigiD (publiek inlogmiddel voor burgers) en eHerkenning (privaat inlogmiddel voor bedrijven) wordt betrouwbare toegang verleend tot de digitale dienstverlening van de overheid. Het is belangrijk dat deze middelen zo inclusief mogelijk zijn, zodat iedereen die daar recht op heeft toegang kan krijgen tot de digitale dienstverlening.

[1] Raadpleegbaar via www.tweedekamer.nl
[2] Raadpleegbaar via www.tweedekamer.nl

kst-26643-788
ISSN 0921 - 7371
's-Gravenhage 2021

Het domein Toegang heeft in de kern twee doelen. Domein toegang staat voor:

1. (Persoonlijke) toegang verlenen tot een goede, efficiënte digitale dienstverlening voor burgers en bedrijven. Zij kunnen via een inclusieve verlening van toegang op een toegankelijke, begrijpelijke en gebruiksvriendelijke wijze gebruik maken van de digitale dienstverlening.
2. De betrouwbaarheid van de private en publieke inlogmiddelen, zodat persoonsgegevens zo goed mogelijk beschermd zijn.

Leeswijzer:

In deze voortgangsrapportage wordt in paragraaf 2 ingegaan op het juridisch kader voor het domein toegang, zoals opgenomen in het wetsvoorstel Digitale Overheid (Wdo). Het wetsvoorstel voorziet voor burgers in de mogelijkheid om naast het publieke middel voor burgers (DigiD) ook gebruik te maken van inlogmiddelen van private partijen (binnen de publieke dienstverlening). De inrichting van het Stelsel Toegang (hierna: stelsel) waarbinnen de toelating van en het toezicht op deze private inlogmiddelen vorm moet krijgen is reeds gestart. In paragraaf 3 licht ik mijn beleid toe gericht op het borgen van een gebruiksvriendelijke en inclusieve toegankelijkheid van de digitale overheidsdienstverlening. Bijzondere speerpunten daarbinnen zijn het vrijwillig machtigen van derden voor de burger die moeite heeft met de digitale overheidsdienstverlening en de wettelijke vertegenwoordiging in die gevallen waarin een burger niet zelf kan of mag handelen. In paragraaf 4 staat mijn beleid gericht op realiseren van het gebruik van inlogmiddelen op een hoger betrouwbaarheidsniveau centraal. In paragraaf 5 ga ik in op de initiatieven van de Europese Commissie waarin in lijn met mijn voorgenomen beleid, de verbreding van een veilige, betrouwbare en toegankelijke dienstverlening naar het private domein centraal staat. Tot slot ga ik kort in op de invoering van de Wet elektronische publicaties.

2. Juridisch kader

Het wetsvoorstel Digitale Overheid (Wdo) (Kamerstuk 35 868) legt het juridisch fundament onder de ontwikkeling van een veilig toegankelijke digitale overheid. Uit de Wdo vloeit de stelselverantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties voort.

Stelselinrichting

Eén van de doelstellingen van de Wet Digitale Overheid (Wdo) is om burgers, naast het publieke inlogmiddel voor burgers (DigiD), ook private inlogmiddelen te kunnen laten gebruiken op de hogere betrouwbaarheidsniveaus. Daartoe moet het stelsel Toegang ingericht worden.

Binnen dit stelsel wordt gezorgd dat het publieke inlogmiddel voor burgers beschikbaar is, dat een systeem voor open toelating van private inlogmiddelen wordt ingericht, en dat de benodigde voorzieningen beschikbaar zijn om deze inlogmiddelen in een stelsel te laten samenwerken.

Onder deze stelselinrichting, valt ook de inrichting van het zogeheten herstelvermogen. Het stelsel wordt zodanig ingericht dat mogelijk misbruik herkend kan worden, zodat actie kan worden ondernomen. Zo kan ervoor worden gezorgd dat burgers en bedrijven die daar problemen van ondervinden snel geholpen worden.

In voorbereiding op het in werking treden van de Wdo ben ik gestart met de inrichting van dit stelsel. Hiermee beoog ik zo snel mogelijk na het in werking treden van de wet ook het stelsel operationeel te hebben om de bovengenoemde doelen te realiseren.

Toezicht op het stelsel

De Wdo voorziet in toezicht op de inlogmiddelen en op overheden om te zorgen dat inlogmiddelen veilig en betrouwbaar zijn en dat overheidsdienstverleners het juiste betrouwbaarheidsniveau inzetten. Ik richt daarom toezicht en handhaving op het stelsel in. Het Agentschap Telecom zal toezicht houden op de aanbieders van inlogmiddelen. Voor toezicht op verplichtingen uit de Wdo die zich richten tot overheden wordt aangehaakt bij bestaand interbestuurlijk toezicht.

Veiliger inloggen met publieke en private inlogmiddelen

Met de Wdo wordt afgedwongen dat inlogmiddelen op hogere betrouwbaarheidsniveaus door dienstverleners worden ingezet. Deze ontwikkeling is reeds in volle gang. Dit is nodig om veilige digitale overheidsdienstverlening in de toekomst te kunnen blijven aanbieden. Het wetsvoorstel voorziet erin dat burgers de mogelijkheid krijgen om, naast publiek inlogmiddel DigiD, ook gebruik te maken van private inlogmiddelen binnen de digitale dienstverlening. Op deze manier verdwijnt de afhankelijkheid van één inlogmiddel en kunnen burgers over meerdere (terug)valopties beschikken.

Voor bedrijven zullen de huidige inlogmiddelen van eHerkenning als toegelaten bedrijfs- en organisatiemiddel beschikbaar blijven en samen met andere toe te laten private en publieke inlogmiddelen onder de publiekrechtelijke structuur van de Wdo worden gebracht. Zoals ik uw Kamer voor de zomer heb bericht, onderzoek ik op dit moment samen met de Staatssecretaris van Financiën Fiscaliteit en Belastingen of en hoe voor bedrijven een publiek inlogmiddel kan worden aangeboden.[3]

Om te zorgen dat burgers en bedrijven met een (door hen aangeschaft) toegelaten inlogmiddel overal binnen de overheid terecht kunnen, regelt de Wdo dat (semi)overheden deze inlogmiddelen moeten accepteren. De burger komt zo nooit voor een dichte digitale deur te staan.

Het wetsvoorstel Wdo zorgt er kortom voor dat de toegankelijkheid, maar tegelijkertijd ook de veiligheid en betrouwbaarheid, zo goed mogelijk worden geborgd.

Stand van zaken parlementaire behandeling Wdo

Het wetsvoorstel voor de Wdo ligt nu ter behandeling in de Eerste Kamer. In de schriftelijke behandeling zijn vragen gesteld en zorgen geuit over onder meer de borging van privacybescherming bij inzet van (private) inlogmiddelen. Om tegemoet te komen aan die zorgen is daarom door mij een novelle ingediend bij de Tweede Kamer waarin eisen met betrekking tot privacy by design, een verhandelverbod van gegevens en open source op wetsniveau worden verankerd.

[3] Kamerstuk 34 972, nr. 53

3. De gebruiksvriendelijke en inclusieve toegang tot de digitale overheid.

In mijn beleid draag ik zorg voor een toegankelijke digitale overheid, voor burgers en bedrijven in Nederland en binnen de Europese Unie. Mijn beleid behelst de praktische toegang tot de digitale dienstverlening, maar ook de inclusieve toegankelijkheid van inlogmiddelen.

Toegankelijkheid

Dienstverlening vanuit de overheid vindt steeds vaker digitaal plaats. Niet iedereen is even digitaal vaardig en een grote groep burgers heeft behoefte aan ondersteuning. Voor burgers die niet digitaal zaken kunnen of willen doen, blijft een analoge dienstverlening openstaan (via een balie of telefonisch).

Ook onderzoek ik nu hoe burgers zonder smartphone meegenomen kunnen worden in de ontwikkeling naar hogere betrouwbaarheidsniveaus. Hetzelfde geldt voor burgers die niet beschikken over Nederlandse identiteitsdocumenten die nodig zijn om betrouwbaarheidsniveaus te verhogen naar substantieel of hoog. Ik onderzoek maatregelen om hiervoor (technische) oplossingen te bedenken zodat geen enkele burger wordt uitgesloten en de overheid voor iedereen veilig en digitaal toegankelijk blijft.

Bij de uitgifte van een DigiD aan Nederlanders en Europese burgers in het buitenland is de procedure dat mensen de activeringscode dienen op te halen bij daarvoor aangewezen DigiD-balies in Nederland of in het buitenland. In de praktijk betekent dit soms dat mensen hiervoor ver moeten reizen. In deze Corona-periode bleek dit vaak niet mogelijk te zijn en ben ik samen met de Minister van Buitenlandse Zaken een proef gestart om DigiD volledig digitaal uit te geven.

Afgelopen mei is een eerste korte proef uitgevoerd met uitgifte van de DigiD activeringscode via een video belafspraak met het 24/7 contact center van het Ministerie van Buitenlandse Zaken. Deze proef is succesvol verlopen en is in verband met de Coronamaatregelen verlengd. De komende maanden onderzoekt de Minister van Buitenlandse Zaken op welke wijze een structurele oplossing voor de activering kan aanbieden, waarbij ik ook kijk naar in hoeverre deze werkwijze kan worden toegepast in andere situaties.

Toegankelijkheid via machtiging

Voor de groep burgers die niet kan meekomen is een goed werkende machtigingsfunctie een uitkomst. Met deze functie kan men iemand machtigen om zijn digitale dienstverlening voor of met hem/haar te regelen.

Aansluiting op vrijwillig machtigen

Sinds april 2021 sluit de zorgsector gefaseerd aan op de publieke machtigingsvoorziening. Inmiddels is het eerste ziekenhuis aangesloten, waarmee het gehele aansluitproces voor deze voorziening is beproefd. Andere zorgaanbieders kunnen hier nu ook op aansluiten. De snelheid waarmee de zorgaanbieders aansluiten wordt bepaald door de zorgaanbieders en hun ICT-leveranciers zelf.

Daarnaast bereid ik op dit moment de grootschalige aansluiting van andere sectoren op vrijwillig machtigen voor. Naar verwachting sluit de gemeente Den Haag in oktober 2021 aan en wordt met de VNG bekeken hoe andere gemeenten aangesloten kunnen worden. Dit betreft een proefaansluiting op basis waarvan wordt gekeken naar wat nodig is voor het aansluiten van gemeenten.

Baliemachtigen

Met baliemachtigen wordt het mogelijk gemaakt om een machtiging te registreren bij een balie. Dit biedt een uitkomst voor minder digitaal vaardige mensen. Samen met de Belastingdienst wordt een onderzoek gedaan naar de mogelijkheden hiertoe. Ik verwacht dat dit in het tweede kwartaal van 2022 kan worden beproefd.

Toegankelijkheid via wettelijke vertegenwoordiging

Voor burgers die wettelijk gezien geen zaken met de overheid *mogen* doen is wettelijke vertegenwoordiging op basis van de wet van toepassing. Denk hierbij aan mensen die onder curatele of bewind staan, maar ook aan minderjarige kinderen. Om hun vertegenwoordigers hun recht op vertegenwoordiging digitaal te kunnen laten uitoefenen werk ik aan de volgende diensten:

Bewindvoering

De bevoegdheidsverklaringsdienst wordt een dienst die dienstverleners, burgers en bedrijven helpt om de bevoegdheid te bepalen van de persoon die een dienst (namens een ander) afneemt. Deze dienst helpt om gegevens in de verschillende registers te ontsluiten en verstrekt hierover een verklaring van vertegenwoordiging aan een dienstverlener. Denk hierbij aan het centraal curatele- en bewindregister (CCBR) en aan het ouderlijk gezagregister, maar ook aan het machtigingsregister in de publieke machtigingsvoorziening (DigiD Machtigen). In de praktijk betekent dit dat mensen die onder bewind staan hierdoor ook digitaal vertegenwoordigd kunnen worden. Bewindvoerders kunnen hun taak dus digitaal uitvoeren. Ik werk momenteel aan deze dienst en verwacht dat deze eind 2022 gefaseerd in gebruik genomen kan worden. Dit is nuttig, omdat de keten (raad voor de rechtspraak, CJIB) dan getest kan worden.

Met een blik op de toekomst is de verwachting dat het bewindvoeringsregister eind van dit jaar kan worden ontsloten voor gebruik door het CJIB. Dit gebeurt in eerste instantie in de vorm van een pilot. Eenzelfde traject loopt tussen de VNG en IVO Rechtspraak, met het doel om begin 2022 rond bewindvoering pilots te starten met een aantal gemeenten.

Pilot ouderlijk gezag in de zorg

Zoals ik Uw Kamer informeerde in de vorige voortgangsrapportage van 19 maart 2021, werk ik momenteel samen met het Ministerie van Volksgezondheid, Welzijn en Sport aan de voorbereidingen van een pilot ouderlijk gezag in de zorg. Gezien de verschillende soorten ouderlijk gezag en de complexiteit van het vaststellen hiervan, start ik met ouderlijk gezag dat is af te leiden uit de BRP. Ter afleiding van de gezagsrelatie uit de Basisregistratie personen (BRP) zijn in samenwerking met het Ministerie van Justitie en Veiligheid afleidingsregels ouderlijk gezag opgesteld. In de praktijk zou dit betekenen dat een persoon met ouderlijk gezag ook langs de digitale weg het medische dossier van het kind bijvoorbeeld kan inzien.

De verwachting is dat in het eerste kwartaal van 2022 gestart kan worden met de pilot ouderlijk gezag in de zorg met een aantal zorgverleners (ziekenhuizen). In een later stadium probeer ik ook andere vormen van ouderlijk gezag (voogdij) uit andere registers (Centraal Gezagsregister) te ontsluiten. Beoogd wordt om met Jeugdzorg, de Nationale Politie en de Koninklijke Marechaussee (KMar) een proef te doen.

Nabestaandenmachtiging

Een andere groep waarvoor het belangrijk is om digitaal zaken af te kunnen handelen met de overheid, zijn nabestaanden. Hiervoor werk ik gefaseerd aan een zogenoemde nabestaandenmachtiging. De eerste stap hier naartoe is een digitale oplossing voor nabestaanden om een vertegenwoordiger zaken digitaal te laten regelen met de Belastingdienst. Deze oplossing is op 28 september jl. in gebruik genomen.
Deze dienstverlening is een van de acties die ik, mede naar aanleiding van het onderzoek van de Ombudsman uit 2018 over digitale post aan overledenen, neem om het contact langs digitale weg tussen nabestaanden en de overheid te verbeteren.

Internationaal en Europees inloggen: toegankelijkere interne markt onder eIDAS

De eIDAS-verordening draagt bij aan een goede werking van de digitale interne Europese markt.[4] De verordening stelt de voorwaarden vast waaronder lidstaten elkaars inlogmiddelen (eID's) wederzijds moeten erkennen. De eIDAS-verordening definieert deze wederzijds erkende inlogmiddelen als eID's. Daarmee regelt de verordening dat «openbare instanties» (overheden en organisaties met publiekrechtelijke taken) erkende eID's op de betrouwbaarheidsniveaus «substantieel» en «hoog» kosteloos dienen toe te laten bij grensoverschrijdende transacties in het publieke domein. Sinds 2019 kunnen Europese burgers en bedrijven met alle inlogmiddelen die Europees erkend zijn, inloggen bij digitale diensten van overheden en organisaties met een publiekrechtelijke taak die aangesloten zijn op het Nederlandse eIDAS-koppelpunt (eIDAS-in).

Daarnaast heeft Nederland op basis van de verordening zowel het publieke inlogmiddel DigiD voor burgers als de private inlogmiddelen van eHerkenning voor bedrijven, succesvol Europees doen erkennen voor gebruik over de grens.[5] Bovendien zijn de technische voorzieningen gerealiseerd die nodig zijn voor het gebruik van deze inlogmiddelen in andere lidstaten (eIDAS-uit). De inlogmiddelen voor bedrijven binnen het stelsel voor eHerkenning zijn aangesloten op deze voorzieningen. Voor het publieke inlogmiddel voor burgers (DigiD) vindt deze aansluiting naar verwachting begin 2022 plaats.

4. Veilige en betrouwbare toegang tot de digitale overheid.

In mijn beleid draag ik op verschillende manieren zorg voor een veilige en betrouwbare toegang tot de digitale dienstverlening van de overheid.

---

[4] COM (2012) 0238, COD (2012)0146 (Verordening (EU) Nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

[5] Kamerstukken 32 851 en 26 643, nr. 68.

eID en een hogere mate van betrouwbaarheid

De eIDAS-verordening erkent drie betrouwbaarheidsniveaus voor elektronische identificatie. Deze betrouwbaarheidsniveaus; laag, substantieel en hoog, betreffen digitale inlogmiddelen die respectievelijk een beperkte, een substantiële en een hoge mate van veiligheid en vertrouwen bieden in iemands opgegeven of beweerde identiteit. Zowel het stelsel van eHerkenning als DigiD zijn Europees erkend en kennen de drie betrouwbaarheidsniveaus.

Ik zet in op het verder uitfaseren van het gebruik van inlogmiddelen op betrouwbaarheidsniveau laag door burgers en bedrijven om in te loggen bij overheden en organisaties met een publiekrechtelijke taak bij hun digitale dienstverlening. Bij privacygevoelige (gegevens)transacties, stimuleer ik dat in het publieke domein sterker ingezet wordt op een substantieel of hoog betrouwbaarheidsniveau. Dit is in lijn met de Handreiking Betrouwbaarheidsniveaus van het Forum Standaardisatie.[6] Het blijft echter wel van groot belang dat diensten beschikbaar blijven en gebruikers zo weinig mogelijk hinder ondervinden. Daarom wordt bij ingang van de Wdo tijdelijk het gebruik van een lager betrouwbaarheidsniveaus toegestaan in de aanloopperiode naar een hoger betrouwbaarheidsniveau. Onder de Wdo zullen de hogere betrouwbaarheidsniveaus wettelijk worden geregeld. Ook dan zal worden voorzien in een overgangstermijn.

Meer (overheids)dienstverleners gebruiken betrouwbare inlogmiddelen

Aantal aansluitingen eHerkenning

Een belangrijke manier om fraude te voorkomen en zo gegevens te beschermen is door het verhogen van betrouwbaarheidsniveaus van inlogmiddelen. In de voorgaande rapportage gaf ik al aan dat steeds meer bedrijven en overheidsdienstverleners zich aansluiten bij veilige digitale inlogmogelijkheden.

De afgelopen maanden is in het bedrijvendomein het aantal uitgegeven inlogmiddelen en aangesloten overheidsdienstverleners opnieuw flink gegroeid. In totaal zijn nu ruim 670.000 eHerkenning inlogmiddelen voor bedrijven uitgegeven, waarvan 400.000 van het eIDAS-betrouwbaarheidsniveau substantieel (eH3). Het aantal overheidsorganisaties dat inmiddels het inlogmiddel eHerkenning gebruikt is gestegen naar 534.

Uitfasering eHerkenning niveau 1(eH1)

Per 1 juli 2021 is eHerkenning niveau 1 uitgefaseerd. Het wordt niet meer verkocht en er kan niet meer mee worden ingelogd. Dit niveau stamt nog uit de begintijd van de digitale overheid en voldeed niet meer aan de huidige eisen voor betrouwbaarheid. Om dit te realiseren werkte Logius samen met leveranciers en de belangrijkste gebruikers namelijk van Justis, RVO en VNG. Door goede samenwerking met deze belangrijke partners is de overgang naar hogere betrouwbaarheidsniveaus soepel verlopen. Een deel van de klanten heeft naar aanleiding van de campagne hun eH1 al voor 1 juli 2021 laten omzetten. Het belangrijkste deel wacht hier echter mee tot het echt noodzakelijk is. Op deze manier worden circa

[6] https://www.forumstandaardisatie.nl/sites/default/files/BFS/4-basisinformatie/publicaties/fs-handreiking-betrouwbaarheidsniveus-v4_0.pdf

78.000 inlogmiddelen met eH1 niveau omgezet naar een hoger betrouwbaarheidsniveau.

Compensatie kosten voor het gebruik eH3 bij aangifte Belastingdienst

In 2020 is een specifiek eH3 Belastingdienst inlogmiddel voor bedrijven en organisaties gerealiseerd. Bij de Rijksdienst voor Ondernemend Nederland (RVO) kunnen bedrijven en organisaties compensatie van de aanschafkosten krijgen voor dit inlogmiddel. Hiermee wordt tegemoetgekomen aan de wens van Uw Kamer dat het inlogmiddel waarmee bedrijven belastingaangifte doen weer kosteloos moet worden. Inmiddels zijn bijna 15.000 van deze speciale eH3 Belastingdienst inlogmiddelen voor bedrijven in gebruik. In totaal zijn daarvoor nu 2232 compensaties aangevraagd en uitgekeerd.

Door de toenemende dreiging van cybercriminaliteit, is het belangrijk dat inlogmiddelen een zo hoog mogelijk betrouwbaarheidsniveau hebben. Overgang naar een hoger betrouwbaarheidsniveau brengt kosten met zich mee voor bedrijven. Zoals uiteengezet in mijn brief van 14 juli 2021, in reactie op motie van de leden Middendorp en Van der Molen (Kamerstuk 34 972, nr. 28), onderzoeken de Staatssecretaris van Financiën – Fiscaliteit en Belastingen en ik of deze compensatieregeling voor het eH3 Belastingdienst inlogmiddel voor bedrijven in de tweede helft van 2022 kan worden vervangen door een kosteloos publiek inlogmiddel voor het doen van de belastingaangifte door bedrijven.[7]

Een betrouwbaar DigiD

Er wordt continu gewerkt aan de veiligheid en beschikbaarheid van digitale inlogmiddelen. Dat is ook nodig, want het aantal cyberaanvallen blijft toenemen. Zo zijn er in 2021 tot nu toe ruim 3600 verzoeken ingediend om sites te laten verwijderen die zich voordeden als DigiD. En in de eerste maanden van 2021 werden meer dan 13.000 DigiD-accounts verwijderd zodat er geen misbruik van gemaakt kon worden.

Tot eind augustus is er 388 miljoen keer ingelogd met DigiD. Hiervan werd er 193 miljoen keer ingelogd met de DigiD app. Er zijn inmiddels 11 miljoen gebruikers van de DigiD app. 5 miljoen daarvan hebben de ID-check toegevoegd aan de app en kunnen daarmee inloggen op eIDAS niveau substantieel. 95% van de DigiD-gebruikers heeft een telefoonnummer toegevoegd en/of de DigiD app geactiveerd en kunnen daarmee 2-factor inloggen met sms-controle of de DigiD app.

Betrouwbare toegang voor alle organisaties

Conform de motie van het lid Van der Molen[8] zullen organisaties zonder registratie in het Handelsregister niet worden verplicht om met eHerkenning zaken te doen met de overheid. De reden hiervoor is dat voor deze organisaties een gezaghebbende bron ontbreekt op basis waarvan de identiteit en de bevoegdheid van de vertegenwoordigers van de organisatie kunnen worden geverifieerd.

Afgelopen twee jaar is het aantal organisaties waaraan geen voldoende betrouwbaar inlogmiddel voor bedrijven kan worden verstrekt flink teruggebracht. Het gaat dan bijvoorbeeld om de Hoge Colleges van Staat, kerkgenootschappen en ambassades. Hiervoor zijn oplossingen gereali-

[7] Kamerstuk 34 972, nr. 53
[8] Motie van het lid Van der Molen, Kamerstuk 35 570 VII, nr. 16

seerd, bestaande uit een registratie in een gezaghebbende bron, zoals het Handelsregister en de protocollaire basisadministratie vanuit ambassades.

De grootste resterende groep is die van de buitenlandse ondernemingen zonder vestiging in Nederland. Deze kunnen niet worden ingeschreven in het Handelsregister. Voor deze categorie organisaties wordt een nieuw register ontwikkeld. In eerste instantie is dit register alleen bedoeld voor die organisaties die een relatie hebben met de Belastingdienst, bijvoorbeeld voor aangifte omzetbelasting. De Belastingdienst zal, in overleg met de Kamer van Koophandel, dit register ontwikkelen. In de volgende voortgangsrapportage zal ik Uw Kamer verder informeren over de voortgang van dit initiatief.

5. Toekomst onder Europese vlag

De Europese Commissie heeft op 3 juni 2021 een wetsvoorstel ingediend voor een «raamwerk voor een Europese Digitale Identiteit», dat de huidige eIDAS-verordening herziet. De Commissie deed ook een aanbeveling voor een met de lidstaten te ontwikkelen «*Toolbox*».[9] De Minister van Buitenlandse Zaken informeerde Uw Kamer op 9 juli 2021 over de positie van het Kabinet in het BNC-fiche[10].

Het voorstel van de Commissie sluit aan op het Nederlandse beleid voor elektronische identificatie en uitwisseling van gegevens. Het Nederlandse beleid heeft tot doel dat alle ingezetenen en bedrijven in Nederland en in andere Europese landen op een veilige, betrouwbare, toegankelijke en gebruiksvriendelijke manier zoveel mogelijk digitaal transacties kunnen verrichten in het publieke en in het private domein. Het kabinet wil in de tweede tranche van de Wdo de grondslag verankeren voor het delen van gegevens in combinatie met een digitale bronidentiteit. Die kan dan op termijn gebruikt worden in oplossingen zoals een «*e-wallet»* waaraan allerlei attributen gekoppeld zouden kunnen worden. Het is de overheid die zulke oplossingen toelaat en er toezicht op houdt binnen het nationale eID-stelsel.[11] Daarbinnen zullen burgers en bedrijven zoveel mogelijk zelf de regie hebben over hun gegevens op hogere betrouwbaarheidsniveaus.[12]

In het kader hiervan onderneem ik verschillende acties. Op het terrein van 1) regie op digitale identiteit, 2) digitale bronidentiteit en 3) grensoverschrijdende elektronische identificatie zet ik de nodige initiatieven in om te komen tot nadere beleidsvorming en uitvoering. Dit draagt bij aan de doorontwikkeling en regulering van het eID-stelsel met het oog op technische oplossingen zoals *wallets*. Hieronder licht ik deze acties toe.

Regie op je digitale identiteit («Self Sovereign Identity»)

Een manier om gegevensbescherming beter te waarborgen is het inzetten van Self Sovereign Identity. Self-sovereign Identity (SSI) is een nieuwe manier van denken over digitale identiteit, gestoeld op het principe dat individuen controle zouden moeten hebben over hun digitale identiteit en de gerelateerde gegevens. De burger krijgt als het ware zelfbeschikking over de gegevens.

---

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&qid=1625048320890&from=NL

[10] Kamerstuk 22 112, nr. 3161

[11] Kamerstukken 26 643 en 32 761, nr. 743

[12] Kamerstuk 32 761, nr. 147.

Door deze belofte is SSI bij de Nederlandse overheid niet onopgemerkt gebleven. Inmiddels is SSI een relevant onderwerp geworden bij diverse partijen, zoals overheden, bedrijven en kennisinstellingen, en vinden er veel projecten plaats. Ik zal deze ontwikkeling kritisch onderzoeken en blijven experimenteren.

Om dit te bewerkstelligen ben ik een analyse van het SSI-ecosysteem gestart. Dit zorgt ervoor dat ik in de toekomst een duidelijke positie kan innemen en richting kan geven aan toekomstige beleidskeuzes. Op dit moment wordt deze analyse uitgevoerd door Innopay en TNO. Dit onderzoek zal ik in 2021 nog delen met uw Kamer.

Digitale bronidentiteit

In mijn brief van 18 februari 2021 aan Uw Kamer over de visie op het onderwerp digitale identiteit introduceerde ik het concept van de digitale bronidentiteit.[13] De digitale bronidentiteit zal een gezaghebbende bron van identiteitsgegevens zijn waar de burger zelf de regie over kan voeren en die de burger kan gebruiken in de publieke en de private sector. Dit biedt een belangrijk generiek bouwblok voor vertrouwen in de digitale wereld.

Op dit moment wordt gewerkt aan een uitwerking van het concept van de digitale bronidentiteit. Ook wordt gewerkt aan een prototype van hoe dit maatschappelijk goed zou kunnen functioneren. Doorontwikkeling van huidige Europees erkende middelen (eID's) is hierbij een van de opties. Als laatste heb ik een onderzoek uitgezet om vanuit het gebruikersperspectief te onderzoeken hoe we dit concept het beste kunnen ontwerpen. Dit onderzoek wordt in 2021 afgerond en gepubliceerd.

Grensoverschrijdende elektronische identificatie

Met het oog op recente ontwikkelingen op het gebied van digitale identiteit is het voor Nederland opportuun om samen te werken in een internationale context. Deze ontwikkelingen zijn (1) het voorstel vanuit de Europese Commissie voor een Europese digitale identiteit[14] en (2) de naar de Kamer gestuurde Nederlandse visie op digitale identiteit.

Inmiddels zien wij dat het concept van de digitale bronidentiteit in diverse landen ontwikkeld wordt. Het wordt ook wel *foundational identity, source identity* of *motherID* genoemd. Ook sluit dit concept goed aan bij de Europese Commissie voorstellen voor een European Digital Identity Framework.[15]

Grensoverschrijdende samenwerkingen kunnen we gebruiken om waardevolle input te geven op het voorstel van de Europese Commissie voor een Europese digitale identiteit. Ook gebruiken we deze experimenten om de Nederlandse visie te realiseren[16]. Grensoverschrijdende experimenten geven daarnaast invulling aan de ambitie om internationaal samen te werken met andere landen en van elkaar te leren, in lijn met de gedachte achter de door mij opgerichte *Coalition of the Willing:* een

[13] Kamerstukken 26 643 en 32 761, nr. 743
[14] COM (2021) 281, 2021/0136 (COD); C(2021) 3968
[15] COM (2021) 281, 2021/0136 (COD); C(2021) 3968
[16] Kamerstukken 26 643 en 32 761, nr. 743

samenwerkingsverband van acht EU-landen om de digitale transformatie van overheden te versnellen [17].

De komende maanden zal ik naar deze vraagstukken een voorbereidend onderzoek doen, waarin in elk geval het speelveld verkend wordt en in kaart wordt gebracht welke onderdelen deugdelijk onderzocht en/of gereguleerd zijn en welke onderdelen nader onderzoek en beleidsvorming vergen. In de volgende voortgangsrapportage zal ik uw Kamer hierover informeren.

6. Invoering Wet elektronische publicaties (Wep)

Ten slotte maak ik van de gelegenheid gebruik om u te informeren over de invoering van de Wet elektronische publicaties (Wep). De Wep verplicht overheden alle algemene bekendmakingen en kennisgevingen zoals (ontwerp) omgevingsvergunningen te publiceren in een elektronisch publicatieblad dat centraal wordt uitgegeven op officielebekendmakingen.nl. De invoering hiervan heeft op 1 juli jl. succesvol plaatsgevonden. Dit maakt het mogelijk om gebruikers van MijnOverheid per e-mail te attenderen op (voorgenomen) overheidsbesluiten m.b.t. hun directe woonomgeving. De invoering van deze attenderingsservice vergt een half jaar meer dan gepland door vertraging in de opbouw en migratie naar een nieuwe infrastructuur en zal nu medio 2022 worden voltooid. MijnOverheidgebruikers kunnen overigens sinds 15 september op MijnOverheid zien welke publicaties betrekking hebben op hun woonomgeving.

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

[17] Nederland, Belgie, Duitsland, Denemarken, Estland, Finland, Frankrijk en Portugal. Zie: https://www.rijksoverheid.nl/actueel/nieuws/2020/10/05/staatssecretaris-knops-geeft-aftrap-van-%E2%80%9Ccoalition-of-the-willing%E2%80%9D-om-digitale-transformatie-van-overheden-te-versnellen