



Aan de Voorzitter van de Tweede Kamer der Staten-
Generaal
Postbus 20018
2500 EA Den Haag

**Ministerie van
Binnenlandse Zaken en
Koninkrijksrelaties
DGOO**

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag

Kenmerk
2019-0000480955

Uw kenmerk

Datum 23 september 2019
Betreft Voortgangsrapportage Digitale toegang

Met mijn brief d.d. 29 januari 2019 (TK 26 643, nr. 590) berichtte ik u over de aanpak van de implementatie van eID. In deze brief rapporteer ik over de tussentijdse resultaten daarvan. Ik heb ervoor gekozen om deze voortgangsrapportage niet te beperken tot alleen eID, maar te rapporteren over alle voorzieningen waarmee burgers of bedrijven toegang krijgen tot digitale interactie met de overheid en organisaties met een publieke taak. Door deze voorzieningen op het domein Toegang in samenhang te bezien, kan ik beter sturen op de toegankelijkheid van de overheidsdienstverlening voor alle burgers en bedrijven en uw Kamer integraal informeren.

Achtereenvolgens behandel ik in deze brief:

- de stand van zaken met betrekking tot relevante wet- en regelgeving;
- de huidige stand van zaken van de implementatiestrategie van eID.

In de bijlagen komen aan bod:

- bijlage 1: dekkingsgraad DigiD en de voortgang van de lopende actielijnen;
- bijlage 2: de implementatie-ervaringen van verschillende dienstverleners;
- bijlage 3: de beantwoording van vragen van uw Kamer, zoals gesteld tijdens het AO Paspoorten en eID van 21 februari 2019.

De hoofddoelen die ik wil bereiken zijn:

- Iedereen kan op een veilige, betrouwbare, toegankelijke, begrijpelijke, gebruiksvriendelijke, en persoonlijke wijze met de overheid interacteren¹.
- Steeds meer mensen kunnen in de almaar digitaler wordende maatschappij participeren doordat de overheid intelligent en in samenwerking met burgers/bedrijven/belanghebbenden, voortdurend optimaal gebruik maakt van de ontwikkelingen in het digitale domein.
- Wij beschermen hierbij de grondrechten en de publieke waarden.

Een groot aantal partijen werkt aan het bereiken van deze maatschappelijke doelen. BZK beschouwt de implementatie als een gezamenlijke verantwoordelijkheid.

¹ N.B. Wet en regelgeving als AVG en eIDAS beperkt zich niet tot het verkeer met de overheid.

De stand van zaken met betrekking tot relevante wet- en regelgeving

Om de beoogde doelen te bereiken heb ik het wetsvoorstel digitale overheid ingediend bij uw Kamer. Op 11 juni 2019 zond ik de Nota naar aanleiding van het verslag bij de wijziging van de Paspoortwet aan uw Kamer (TK 35 047, nr. 8). Op 12 juni 2019 zond ik de Nota naar aanleiding van het nader verslag Wet digitale overheid aan uw Kamer (TK 34 972, nr. 10). Op 5 juli 2019 informeerde ik u over mijn voornemen een andere toelatingssystematiek voor inlogmiddelen voor burgers te kiezen, namelijk open toelating in plaats van een Europese aanbesteding (TK 34 972 nr. 11). Op de Nota van wijziging die hiertoe is opgesteld brengt de Raad van State op korte termijn advies uit. Ik zal daarom de Nota van wijziging binnen enkele weken aan uw Kamer sturen. Ondertussen wordt gewerkt aan de voorbereiding van de uitvoeringsregelgeving bij beide wetsvoorstellen.

De huidige stand van zaken van de implementatiestrategie van eID

In de vorige voortgangsrapportage (TK 26 643, nr. 590) beschreef ik een wendbare implementatieaanpak die in kleine stappen voortgang boekt en de *lessons learned* optimaal benut. Deze aanpak is geoperationaliseerd in vier parallelle actielijnen, te weten:

- Actielijn 1: Brede beweging naar 2 factor-inloggen (met sms-code of app);
- Actielijn 2: Lerende uitrol 'Substantieel';
- Actielijn 3: Lerende inzet niveau 'Hoog' bij noodzaak of maatschappelijke baten;
- Actielijn 4: Het vergroten van de mogelijkheden van burgers voor toegang tot het niveau 'Substantieel'.

De voortgang op deze actielijnen wordt in bijlage 1 toegelicht. De gehanteerde aanpak is noodzakelijk gezien de implementatieproblematiek rondom DigiD. Ik beschreef in de vorige voortgangsrapportage dat die problematiek het gevolg is van onvoldoende mogelijkheden voor grootschaliger gebruik van het authenticatiemiddel DigiD op de betrouwbaarheidsniveaus Substantieel en Hoog. Deze problematiek m.b.t. de zgn. 'dekkingsgraad' bestaat nog steeds, maar er is ook een doorbraak te melden. In de afgelopen periode heeft Nederland samen met andere landen bij Apple gepleit voor openstelling van de NFC. Apple heeft onlangs aangekondigd eind dit jaar de NFC reader (waarmee een smartphone een identiteitsbewijs kan uitlezen) open te stellen vanaf softwareversie iOS 13 voor de modernste typen Apple smartphones. Dit betekent dat de theoretische² dekkingsgraad van DigiD Substantieel toeneemt van circa <50% naar 65%.³ Het toekomstige bereik van DigiD is en blijft afhankelijk van het beleid van de producenten van smartphones met betrekking tot de functionaliteiten die zij aanbieden en ondersteunen. Mede daarom investeer ik in een aantal tijdelijke overbruggingsmaatregelen (actielijn 4), waardoor de huidige dekkingsgraad van DigiD Substantieel verder kan worden vergroot.

² Theoretisch, want de potentiële dekkingsgraad van het middel betekent nog niet dat dit percentage van de bevolking het middel ook gebruikt. Bijvoorbeeld omdat een burger liever een PC gebruikt of iemand anders wil machtigen

³ Dit is het percentage burgers dat, na de openstelling van Apple, een telefoon met geschikte NFC reader heeft.

Op dit moment kunnen nog niet alle burgers op alle niveaus inloggen. Zo is DigiD Substantieel alleen met mobiele telefoons te gebruiken. Voor DigiD Hoog is een nieuw type identiteitsbewijs nodig en moet er nog een NFC- of kaartlezer gebruikt worden. Het duurt nog een aantal jaren (natuurlijke vervangingscyclus van documenten) voordat iedereen dat nieuwe type identiteitsbewijs heeft. Ook is machtigen nog niet voldoende gebruiksvriendelijk. In bijlage 1 ga ik uitgebreider in op de aandachtspunten m.b.t. de dekkingsgraad.

Zoals ik in mijn vorige voortgangsrapportage meldde, kan de overheid de benodigde beweging naar betrouwbaarder inloggen niet alleen maken. Wij hebben hierbij de kennis en kunde nodig die beschikbaar is in de markt. Het is mijn overtuiging dat een combinatie van DigiD met het toelaten van marktpartijen noodzakelijk is.

Daartoe neem ik de volgende aanvullende acties:

1. Ik laat onderzoeken hoe ik de kracht van het "merk" DigiD kan blijven benutten. Het "merk" DigiD wordt immers door vrijwel alle burgers van de doelgroep een of meerdere malen per jaar gebruikt en wordt door hen ervaren als herkenbaar en vertrouwd. Zo wil ik bezien hoe gewerkt kan worden met private inlogmethoden binnen een omgeving met DigiD.
2. Aan private authenticatiemiddelen en diensten zullen eisen worden gesteld met betrekking tot onder andere veiligheid, betrouwbaarheid, gebruiksvriendelijkheid en interoperabiliteit. Partijen die aan deze eisen voldoen, moeten vervolgens snel en probleemloos kunnen aansluiten op de digitale overheid. Ik wil onderzoeken of er in het huidige DigiD stelsel belemmeringen bestaan voor de toetreding van private authenticatiediensten en deze wegnemen, zonder concessies te doen aan de genoemde eisen.

Voor de tweede actie wil ik dus extra prioriteit geven aan de toelating van private authenticatiediensten. Daarom start ik een nieuwe actielijn 5, gericht op een beheerste en voorspoedige toelating van oplossingen van marktpartijen. Onnodige belemmeringen voor toelating neem ik weg.

Daarnaast wil ik het programma Machtigen nadrukkelijker in verbinding brengen met eID. Immers, wanneer dienstverleners overgaan naar hogere betrouwbaarheidsniveaus, heeft dit ook consequenties voor de burgers voor wie interactie met de overheid lastig is en die daarvoor hulp van anderen nodig hebben. Zoals ik u vorig jaar berichtte (bijlage bij brief TK 26 643 nr. 552) komen de voorzieningen van het programma Machtigen de komende jaren stapsgewijs beschikbaar.

Op dit moment zijn slechts vier overheidsdienstverleners aangesloten op Machtigen en betreft dit een aparte aansluiting. Op termijn is het de bedoeling dat *alle* organisaties waarbij met DigiD kan worden ingelogd, ook een mogelijkheid bieden om digitaal zaken voor anderen te regelen. Daarnaast vergt het huidige Machtigen een verbetering in de gebruiksvriendelijkheid, zodat ook burgers die wel digitaal willen interacteren met de overheid, maar de hulp van anderen nodig hebben, er gebruik van kunnen maken.

Ik zal daarom in actielijn 1 toevoegen dat dienstverleners gaan aansluiten op Machtigen. Machtigen wordt in deze actielijn tevens gebruiksvriendelijker

gemaakt. Daarnaast zal ik onderzoeken of het wenselijk en mogelijk is om in het burgerdomein gebruik te maken van private machtigingsoplossingen. Ik zal u daarover in mijn hierboven aangekondigde brief bij de Nota van wijziging op de wet Digitale Overheid informeren. De reden is ook hier het vergroten van de mogelijkheden om zo spoedig mogelijk zoveel mogelijk burgers met alle overheidsdienstverleners te kunnen laten interacteren.

Financiën

Nu de implementatiefase gestart is, is het urgent om de financiële afspraken rondom Toegang waar nodig aan te scherpen en uit te voeren.

In de vorige voortgangsrapportage heb ik aangegeven dat met de huidige systematiek van doorbelasting een toename van digitale interactie leidt tot een toename van kosten voor de dienstverleners. Dit zou belemmerend kunnen werken op de wens om zoveel mogelijk mensen digitaal zaken te laten doen met de overheid. Ik onderzoek daarom of het mogelijk en wenselijk is om de bekostigingssystematiek zodanig in te richten dat deze negatieve prikkel wordt afgezwakt dan wel vervangen door een positieve. De bekostigingssystematiek raakt bijna alle departementen en is in het verleden door het kabinet vastgesteld.

De wet Digitale Overheid biedt de mogelijkheid om wendbaar en flexibel in te kunnen spelen op de snel voortschrijdende technologische ontwikkelingen, zonder afbreuk te doen aan de rechtszekerheid en waarborgen voor burgers en bedrijven. De komende maanden wordt extra aandacht geschonken aan het ontwikkelen van de uitvoeringsregelgeving, om deze wet goed te kunnen gebruiken. Gelijktijdig met het voorbereiden van de onderliggende regelgeving, vindt een brede uitvoeringstoets plaats. Op dat moment ontstaat er ook een beter zicht op de kosten die met de implementatie zijn gemoeid. Ik verwacht u hierover nader te kunnen informeren in de volgende voortgangsrapportage, die ik u begin 2020 zal aanbieden.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops

Bijlage 1: Dekkingsgraad van DigiD en de voortgang van de lopende actielijnen.

Aandachtspunten m.b.t. de dekkingsgraad van DigiD

DigiD Substantieel, DigiD Hoog en Machtigen kennen qua dekkingsgraad de volgende aandachtspunten:

- Ondanks de verwachte doorbraak bij Apple en de inzet op tijdelijke overbruggingsmaatregelen is de dekkingsgraad van DigiD Substantieel nog te laag om als enige inlogoplossing te kunnen fungeren voor interactie met de digitale overheid. Mijn doel is dat alle burgers toegang moeten kunnen hebben tot alle digitale diensten met de meest gangbare huidige middelen. DigiD Substantieel is een 'mobile only' oplossing. Inloggen met DigiD Substantieel op een PC zonder daarbij gebruik te moeten maken van een smartphone is nog niet in beeld;
- Voor DigiD Hoog is de huidige dekkingsgraad lager dan die voor DigiD Substantieel. Mogelijke overbruggingsmaatregelen, zoals zuilen, zijn praktisch niet geschikt om te kunnen inloggen op het eIDAS-betrouwbaarheidsniveau Hoog. Daarnaast dient de gebruiker voor gebruik van DigiD Hoog te beschikken over een nieuw identiteitsbewijs met daarvoor benodigde technologie op de chip. Deze worden uitgegeven via het bestaande uitgifteproces van identiteitsdocumenten. Dit proces kent een vervangingstermijn van tien jaar waardoor de komende jaren niet alle burgers beschikken over een identiteitsbewijs waarmee zij op Hoog kunnen inloggen. Net als bij Substantieel is de dekkingsgraad van de mobiele oplossing voor DigiD Hoog te laag om als enige oplossing te kunnen fungeren voor het inloggen op de digitale overheid;
- In tegenstelling tot DigiD Substantieel is er wel een technisch werkende oplossing om te kunnen inloggen op een PC met DigiD Hoog zonder gebruik te moeten maken van een smartphone. In dat geval dient de gebruiker te beschikken over een kaartlezer. Over het algemeen hebben burgers die echter niet in hun bezit. Bovendien geldt ook hier dat de gebruiker dient te beschikken over een nieuw identiteitsbewijs, waarbij de hierboven genoemde vervangingstermijn aan de orde is.
- De voorziening om vrijwillig te machtigen is beschikbaar, maar kent knelpunten in de gebruiksvriendelijkheid en in het aanbieden van vrijwillig machtigen door dienstverleners.

Voortgang van de actielijnen

Per actielijn wordt hieronder de voortgang gerapporteerd. In bijlage 2 heeft een aantal grote dienstverleners daarnaast hun eigen implementatie-ervaring opgetekend.

Actielijn 1: Brede beweging naar 2 factor-inloggen (met sms-code of DigiD App)

Als no regret-actie, die later de brede uitrol naar het niveau 'Substantieel' en 'Hoog' kan vergemakkelijken en versnellen, ben ik gestart met het stimuleren van het gebruik van de DigiD App. Een grote impuls werd gegeven doordat het UWV, per 15 mei 2019 haar klanten verplicht laat inloggen met de DigiD App of sms-

controle. Inloggen bij DUO was al eerder verplicht via de DigiD App of sms-controle.

Voor klanten van het UWV betekende de verplichting om met 2 factor-authenticatie in te loggen dat, zoals reeds voorzien, bewindvoerders en een deel van de Nederlanders in het buitenland geen toegang meer hebben tot de digitale dienstverlening van het UWV. Ik werk samen met de Raad voor de Rechtspraak aan een oplossing dat bewindvoerders gemakkelijk hun klanten kunnen vertegenwoordigen. Begin 2020 zal een pilot worden gedaan met bewindvoerders. Daarna kunnen bewindvoerders bij alle dienstverleners die zijn aangesloten op het machtigingskoppelvlak ook namens hun cliënten inloggen.

Mede dankzij de overstap van het UWV is een behoorlijke groei te zien in het aantal 2 factor-authenticaties dat met behulp van de DigiD App of met sms-controle is uitgevoerd. In januari 2019 betrof dit 18% van de gelukke authenticaties, in juni 2019 was dit ruim 40%. Het gebruik van de DigiD App binnen de groep van 2 factor-authenticaties (die bestaat uit zowel verificatie met de DigiD App als per sms) was in januari 2019 29% en is in juni 2019 gegroeid naar 44%.

Om het gebruik van de DigiD App breed te stimuleren is een online campagne voorbereid, die vanaf eind september 2019 van start gaat. Deze campagne richt zich in eerste instantie op studenten, maar wordt later, eventueel aangepast, uitgebreid naar andere doelgroepen.

In actielijn 1 wordt ook gewerkt aan een aansluitplan voor dienstverleners die zijn aangewezen door de wet Digitale Overheid. Het gaat om duizenden organisaties in de zorg en enkele honderden organisaties in andere domeinen, die nog niet zijn aangesloten op DigiD. Op dit moment zijn ruim 600 organisaties op DigiD aangesloten. In de zorg wordt onder meer gewerkt aan een oplossing met clusteraansluitingen. Naast het vergroten van het aantal aansluitingen ligt er ook een opgave op het tempo van aansluiten. Tot slot is het van belang dat voldoende transacties mogelijk zijn per aansluiting.

Actielijn 2: Lerende uitrol niveau 'Substantieel'

DigiD Substantieel

In deze actielijn heb ik gekozen voor een lerende uitrol van het authenticatieniveau 'Substantieel'. Hierbij wordt een strategie gehanteerd waarbij wij ons richten op twee specifieke sectoren: de zorg (burgerdomein) en het UWV (bedrijvendomein), waar de noodzaak en de bereidheid om tempo te maken het grootst zijn. Daarnaast wordt gewerkt aan het wegnemen van belemmeringen voor de implementatie.

In het zorgdomein is het streven dat burgers vanaf 1 januari 2021 op niveau Substantieel inloggen bij hun zorgverleners. In de taskforce Zorg wordt gericht gewerkt aan het ontzorgen van de zorgverleners, door het aansluitingsproces verder te optimaliseren en te verkorten. Zo wordt onder meer onderzocht hoe de auditlast verder kan worden beperkt.

Het programma machtigen start in Q4 met een pilot in de zorg. Moeders kunnen dan het medisch dossier van hun minderjarige kind inzien bij een ziekenhuis. Machtigen levert hierbij de informatie aan het ziekenhuis zodat zij het dossier kunnen tonen aan een moeder met ouderlijk gezag.

eHerkenning

Ondernemers kunnen bij de digitale overheid inloggen dankzij het publiek-private afsprakenstelsel eHerkenning, waarbinnen private authenticatiediensten en ontsluitende diensten participeren. De taskforce die ik in december 2018 voor het bedrijvendomein heb opgericht om resterende belemmeringen weg te nemen, boekt goede vooruitgang. Zo is in juni een versie van eHerkenning opgeleverd waarmee het mogelijk wordt dat ook eenmanszaken bij het UWV en de Belastingdienst kunnen inloggen zodra die organisaties deze nieuwe versie geïmplementeerd hebben. Daarnaast is met de eHerkenning-leveranciers afgesproken dat de Ketenmachtigingsfunctionaliteit vóór 1 oktober 2019 breed beschikbaar wordt gesteld. Dit is van direct belang voor het UWV, omdat veel bedrijven en organisaties hun zaken uitbesteden aan een intermediair, bijvoorbeeld voor de ziekmeldingen.

De verdere uitrol van eHerkenning in het bedrijvendomein verloopt voorspoedig. De Belastingdienst en de Douane zijn daarmee in mei 2019 live gegaan op hun zakelijke portalen. Dit geeft naar verwachting een flinke impuls aan het gebruik van eHerkenning. Stapsgewijs zullen zij steeds meer digitale diensten, waarvoor met eHerkenning moet worden ingelogd, hierop aanbieden.

Voor veel van de (rest)groepen die niet in het Handelsregister staan ingeschreven is samen met de KvK en de Belastingdienst een oplossing gevonden door inschrijving toch mogelijk te maken of op andere wijze een eHerkenningsmiddel te kunnen verkrijgen. Hierdoor is deze restgroep de afgelopen maanden van naar schatting 60.000 organisaties teruggebracht naar 9.500 organisaties. Voor de laatste groepen wordt ook aan een zo generiek mogelijke oplossing gewerkt in samenwerking met het UWV, de Belastingdienst, de RvO en de KvK.

Op 4 juni jl. is de landelijke mediacampagne eHerkenning gestart. Met de slogan 'eHerkenning straks onmisbaar, nu verkrijgbaar' wordt erop ingezet om meer bekendheid te generen en het gebruik daarmee verder te stimuleren. Op 6 juni jl. heeft het Europese eIDAS-coöperatienetwerk ingestemd met de notificatie aan de Europese Commissie van eHerkenning. Hiermee kan eHerkenning binnen afzienbare tijd door alle Nederlandse ondernemers en organisaties gebruikt worden om in te loggen bij overheidsdienstverleners in andere EU lidstaten, zoals aan uw Kamer is toegezegd⁴.

Actielijn 3: Lerende inzet niveau 'Hoog' bij noodzaak of maatschappelijke baten

Zoals eerder aangegeven kent gebruik van DigiD Hoog door een eindgebruiker een aantal randvoorwaarden. Net als bij DigiD Substantieel is een geschikte telefoon nodig (of een NFC-kaartlezer bij een PC), en daarnaast zijn relatief nieuwe identiteitsbewijzen nodig, die een natuurlijk vervangingsritme kennen van 10 jaar. De uitrol van deze kaarten neemt dus nog flink wat tijd in beslag; de ontwikkeling verloopt voorspoedig.

De elektronische Nederlandse identiteitskaart (eNIK) is technisch gereed. Om daadwerkelijk de eNIK uit te kunnen geven heeft de Rijksdienst voor Identiteitsgegevens (RvIG) nog minimaal vier maanden voorbereidingstijd nodig. Deze tijd is nodig om de eNIK in productie te nemen en alle betrokken partners te informeren. Na uitgifte kan de kaart geactiveerd en gebruikt worden met DigiD. Als de burger niet meer over de pincode beschikt, is echter een pin-reset-functie vereist, waarmee burgers een nieuwe pincode kunnen aanvragen. Die functionaliteit is naar verwachting gereed in de tweede helft van 2020. Daarom zal activatie en gebruik van de eFunctionality dan pas beschikbaar worden gesteld. De datum voor uitgifte en gebruikersnaam van de eNIK is voorts afhankelijk van de goedkeuring op de wetgeving (Paspoortwet voor uitgifte en Wet digitale overheid voor gebruikersnaam).

Sinds juni vorig jaar uitgegeven rijbewijzen kunnen straks gebruikt worden om via DigiD Hoog in te loggen. De RDW stuurt een burger een code per brief toe waarmee hij een zelfgekozen pincode kan instellen. De functionaliteit en apparatuur voor deze brief staan klaar in afwachting van inwerkingtreding van de Wet digitale overheid. Voor het daadwerkelijk kunnen gebruiken van DigiD Hoog moeten DigiD-componenten nog worden aangepast. De inbouw van de functionaliteit in de DigiD-smartphone-app en desktop-app (voor gebruik van een losse NFC-cardreader aan PC) is wel al succesvol beproefd, maar moet nog in de productie-releases worden ingepland.

⁴ De wet Digitale Overheid maakt het mogelijk dat eHerkenningssystemen, in afwachting van erkenning, voor een afgebakende periode van 18 maanden kunnen participeren in het eHerkenningstelsel.

Actielijn 4: Het vergroten van de mogelijkheden van burgers voor toegang tot het niveau 'Substantieel'

Om zoveel mogelijk burgers op een zo eenvoudig mogelijke wijze toegang te bieden tot een authenticatiemiddel op niveau Substantieel, loopt een aantal parallelle sporen om een oplossing te bieden voor de eerder beschreven ontoereikende dekkinggraad.

Daarnaast is op het innovatiespoor een projectteam ingericht, voor het opleveren van een alternatieve methode om op een smartphone, zonder gebruik te maken van een NFC-reader, toch op niveau Substantieel te komen. Immers, ook nadat Apple de NFC-reader heeft opengesteld, zijn nog niet alle smartphones in staat om een identiteitsbewijs uit te lezen. Een prototype wordt nu ontwikkeld en zal vervolgens in een pilot getest worden.

Als laatste worden in deze actielijn tijdelijke overbruggingsmaatregelen ontwikkeld die burgers kunnen gebruiken om het authenticatieniveau van hun DigiD App te verhogen naar Substantieel, wanneer dit op hun huidige smartphone niet mogelijk is. De overbruggingsmaatregelen zijn tijdelijk, omdat ik immers beoog de huidige beperkingen te kunnen opheffen.

In mijn vorige voortgangsrapportage over eID heb ik een aantal alternatieven voor tijdelijke overbrugging genoemd, waarvan ik er drie het meest kansrijk acht, te weten: servicezuilen, gastgebruik en een balieproces:

- Er zijn inmiddels servicezuilen ontwikkeld met een NFC-lezer, waarmee op dit moment op tien plaatsen (ziekenhuizen, gemeentehuizen, bibliotheken) in het land een pilot wordt uitgevoerd. Burgers kunnen bij een zuil, met hun smartphone met DigiD App en het juiste rijbewijs, paspoort of identiteitskaart, hun DigiD App op niveau Substantieel brengen. Uit de beproeving blijkt dat de zuilen technisch werken. Wat nader onderzocht zal moeten worden, is wat de gebruikersbeleving is.
- Daarnaast heeft Logius een app voor gastgebruik ontwikkeld. Dankzij deze app voor gastgebruik kunnen burgers, bijvoorbeeld bij hun zorgverlener, maar ook bij een bekende, via een andere telefoon of tablet hun eigen DigiD App op niveau Substantieel brengen. Dit is vergelijkbaar met het gebruik van een servicezuil. De volgende stap is deze app te beproeven in een pilot.
- Ik ben bezig uit te werken hoe burgers via een balie kunnen worden geholpen met het verhogen van het betrouwbaarheidsniveau van hun DigiD.

Bijlage 2: Ervaringen bij implementatie-inspanningen door dienstverleners

UWV over de implementatie van 2 factor-inloggen:

"UWV stelt vanaf 15 mei 2019 het 2 factor inloggen verplicht voor burgers voor toegang tot de digitale dienstverlening van UWV. 2 factor-authenticatie vereist een extra code naast gebruikersnaam/wachtwoord via een sms-functie (mobiel én vaste telefoon) of het gebruik van de DigiD-app (mobiel). UWV vindt het belangrijk dat de persoonsgegevens van burgers goed beveiligd zijn en loopt hiermee vooruit op de wettelijke verplichtingen Wet digitale overheid. 2 factor-authenticatie is zeker nog niet het structureel beoogde niveau, maar voldoet conform het voorgestelde overgangsrecht Wet digitale overheid.

De overgang naar 2-factor authenticatie heeft effect op burgers die voor 15 mei wel digitaal dienstverlening van UWV gebruikten, maar niet de overstap naar sms-functie of DigiD-app kunnen maken. Voor deze burgers biedt UWV de mogelijkheid om over te stappen naar dienstverlening op papier. UWV constateert vanaf 15 mei een significante toename van aanmeldingen voor papieren dienstverlening.

De belangrijkste reden hiervoor is dat het DigiD-account door burgers gedeeld werd met anderen. Vanwege de strikt persoonlijke aard van DigiD niet wenselijk. DigiD met de twee-factorauthenticatie is lastiger uit te lenen dan DigiD met naam/wachtwoord.

Het uitlenen van het DigiD-account gebeurde bij:

- 1. Burgers/belangenbehartigers die ter ondersteuning van een andere burger de digitale dienstverlening van UWV gebruiken via het DigiD-account van de betreffende burger.*
- 2. Professionele bewindvoerders die met behulp van het DigiD-account van cliënten de zaken van deze cliënten behartigen en digitaal inloggen met dit account.*

Voor de eerste groep sluit UWV eind 2019 aan op Machtigen. Machtigen biedt een veilige manier van machtigen en is geschikt voor burger-burgermachtigen, waardoor het 'uitlenen' van het DigiD account niet meer nodig is.

Voor de tweede groep wacht UWV op de overheidsbrede ontwikkelingen op het gebied van uitbreiding van machtigen voor bewindvoerders/inkomensbeheerders en andere wettelijke vertegenwoordigers. Tot die tijd zal deze groep aangewezen zijn op communicatie via het papieren kanaal.

Een andere doelgroep waarvoor de overgang naar 2-factor authenticatie lastig is, zijn Nederlanders in het buitenland. Zij krijgen de brief met activeringscode, conform kaders en processen van het ministerie van BZK, alleen op adressen in Nederland, bij grensgemeentes of op enkele ambassades. Dat kan ver reizen met zich meebrengen, waardoor ook deze klanten terugvallen op papier."

VWS over de implementatie van niveau 'Substantieel':

"In het kader van de wet digitale overheid zullen de komende jaren alle zorgaanbieders (circa 12.000) moeten worden aangesloten op DigiD (en de overige middelen uit de Wet digitale overheid). Om hen hierbij te ondersteunen wordt door VWS gewerkt aan het beschikbaar komen van de routeringsdienst TVS

(toegangsverleningsservice) voor de zorg. Het streven is om deze vanaf 1 januari 2020 beschikbaar te hebben voor het zorgdomein. Zo kunnen eind 2020 (in ieder geval) zorgaanbieders die afhankelijk zijn van digitale toegang voor het leveren van zorg zijn aangesloten op DigiD Substantieel.

Daarnaast werkt de zorg ook mee aan pilots met oplossingen om het betrouwbaarheidsniveau van DigiD op te hogen naar Substantieel. In een aantal ziekenhuizen is bijvoorbeeld de DigiD-servicezuil geplaatst. De ervaring hiermee is tot op heden positief. Meerdere zorginstellingen, voornamelijk ziekenhuizen, hebben dan ook hun interesse aangegeven voor het installeren van een servicezuil binnen hun organisatie."

De Belastingdienst over de implementatie van eHerkenning 3:

"Op het nieuwe zakelijke portaal loggen steeds meer ondernemers in met eHerkenning niveau 3 voor de digitale diensten Omzetbelasting en Loonheffingen. Later dit jaar kunnen ondernemers ook in Mijn Belastingdienst Zakelijk terecht voor de Vennootschapsbelasting. Om ondernemers te motiveren om tijdig over te stappen naar eHerkenning (ruim voor de einddatum van het oude portaal) wordt een communicatie-campagne gestart en ondersteuning geboden. De Belastingdienst sluit hierbij aan op de overheidsbrede initiatieven rondom eHerkenning. Over de communicatie en de knelpunten bij de implementatie (restgroepen, onbekendheid en kosten eHerkenning) wordt afgestemd met Logius, UWV, EZK, KVK en de eHerkenningsleveranciers."

UWV over de implementatie van eHerkenning 3:

"UWV wil de toegang tot digitale dienstverlening voor werkgevers (bedrijven) beter beveiligen en is vanaf november 2018 aangesloten op eHerkenning. Werkgevers/bedrijven hebben de mogelijkheid om vóór 1 november 2019 een eHerkenningsmiddel aan te schaffen om gebruik te blijven maken van de digitale dienstverlening op het UWV-werkgeversportaal. Vanwege de gevoeligheid van de gegevens bij UWV moet dit middel minimaal niveau EH3 zijn. Dit correspondeert met het vereiste niveau substantieel uit de eIDAS-verordening. De Autoriteit Persoonsgegevens heeft eerder richting UWV aangegeven het huidige niveau van toegang tot de gegevens niet voldoende te vinden. UWV moet daarom op 1 november 2019 de toegang verlenen op het juiste niveau EH3. Dat betekent dat UWV zonder EH3- middel geen toegang meer mag geven en werkgevers dan moeten terugvallen op de papieren weg.

De overgangperiode van één jaar is bedoeld om werkgevers de mogelijkheid te geven deze middelen tijdig aan te schaffen en is uitgebreid door UWV gecommuniceerd. Vanaf 1 november 2019 is het niet meer mogelijk digitaal in te loggen bij UWV zonder eHerkenning. UWV constateert echter dat het aantal werkgevers dat de juiste certificaten heeft aangeschaft, nog gering is en verwacht derhalve op 1 november 2019 complicaties voor werkgevers/bedrijven die niet tijdig zijn. Werkgevers hebben dan geen digitale toegang meer tot het werkgeversportaal en kunnen niet tijdig aan verplichtingen voldoen zoals ziek- en herstelmeldingen. UWV blijft actief zoeken en inzetten op manieren om werkgevers te bewegen tijdig eHerkenningsmiddelen aan te schaffen om te voorkomen dat zij niet meer digitaal kunnen inloggen."

Bijlage 3: Beantwoording van vragen van de Tweede Kamer tijdens het AO
Paspoorten en eID van 21 februari 2019

In het Algemeen Overleg over Paspoorten en eID van 21 februari 2019 heb ik u toegezegd onderstaande vragen te beantwoorden, die door de leden gesteld zijn.

Gebruik DigiD in een private omgeving

De leden Middendorp en Van der Molen stellen vragen over het gebruik van DigiD in het private domein. In de beantwoording van de inbreng van de Kamer bij de wet Digitale Overheid ben ik daarop nader ingegaan (TK 34 972, nr. 10).

Uitgangspunt van het kabinet is vooralsnog, dat het inloggen buiten het publieke domein zoveel mogelijk aan de markt moet worden overgelaten en de overheid hier momenteel geen rol heeft.

De heer Middendorp wijst op de hoge kosten (bijna € 1 miljard over 10 jaar⁵) voor het eID-stelsel. Dat is inderdaad veel geld, maar omvat o.a. de kosten van 10 jaar onderhoud voor het huidige DigiD (ruim € 400 mln.). Dit zijn kosten die in ieder geval gemaakt worden voor DigiD, ook als het programma eID niet gestart zou zijn. Mede op verzoek van de Tweede Kamer is een publiek inlogmiddel op hogere betrouwbaarheidsniveaus (DigiD Substantieel en Hoog) ontwikkeld (motie De Caluwé, TK 26 643, nr. 376).

De leden Middendorp en Van der Molen vragen of DigiD - gelet op de hoge kosten - ook in het private domein gebruikt zou moeten worden. Mijn prioriteit ligt bij het beschikbaar krijgen en stellen van inlogmiddelen (waaronder DigiD en private middelen) op een hogere betrouwbaarheid. Wil DigiD in de private markt gebruikt worden, dan moeten er technische aanpassingen worden gepleegd; immers DigiD stuurt bij elke inlog het BSN mee en dat mag een private marktpartij niet ontvangen.

Bovendien, zoals elders in deze brief wordt toegelicht, ga ik een systeem van open toelating inrichten, waardoor alle private authenticatiediensten die aan de eisen voldoen kunnen worden gebruikt voor het inloggen in het BSN-domein. Ik wil eerst bezien hoe deze markt zich de komende jaren ontwikkelt en dan onderzoeken in hoeverre inloggen met DigiD bij private websites nog nodig, dan wel gewenst is. Daarbij zal ik ook nadrukkelijk toetsen aan de wet Markt en Overheid.

Gebruik van software uit China

De heer Middendorp vraagt of we rekening moeten houden met software uit China. De systemen bij Logius zelf draaien niet op systemen van Chinese merken, maar vandaag de dag is de keten van leveranciers en fabrikanten complex en komen componenten van systemen vaak uit China. Wij zijn ons hiervan bewust en houden hier bij ontwerp van onze systemen rekening mee. In de netwerken die onze systemen met het internet verbinden is enige Chinese netwerkapparatuur in gebruik. De informatie die deze apparatuur passeert is versleuteld. Voor het gebruik van Chinese software, handelt de Rijksoverheid in

⁵ Herijking businesscase inloggen BSN-domein. Aan de Tweede Kamer aangeboden bij Kamerbrief TK 26 643 nr. 528.

lijn met de beleidsnota "Nederland–China een nieuwe balans" en de "China strategie" (brief van de minister van Buitenlandse Zaken van 15 mei 2019; TK 35 207, nr. 1).

Attributendiensten

In mijn brief van 14 mei jl. (TK 26 643 nr. 609) heb ik u toegezegd de Kamer rond de zomer te informeren over de stand van zaken ten aanzien van de pilots met attributendiensten bij gemeenten. Bij gemeenten worden verschillende pilots uitgevoerd met private attributendiensten binnen een breed spectrum aan onderwerpen, variërend van interne processen tot aan pilots in het eID-domein.

De betrokkenheid van BZK is gericht op de pilots met betrekking tot het eID-domein en digitale identiteit. Deze pilots zijn nog in de opstartfase en worden uitgevoerd in het kader van experimenteren en leren. Onderzocht wordt wat de technische, maatschappelijke en juridische aspecten zijn van de toepassing van private attributendiensten. Zodra relevante uitkomsten van de pilots bekend zijn zal ik u daarover informeren. Vanzelfsprekend moeten de pilots voldoen aan de wettelijke kaders die ter zake gelden.