Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 590

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 januari 2019

Met mijn brief d.d. 16 juli 2018 berichtte ik u over de voortgang van het programma eID over de periode januari tot en met juni 2018 (Kamerstuk 26 643, nr. 550). Het programma eID heeft tot doel om gebruiksvriendelijke, veilige en betrouwbare digitale interactie van burgers en bedrijven met de overheid mogelijk te maken. In deze brief informeer ik u over de aanpak van de implementatie eID.

Terugblik

In bijlage twee geef ik een overzicht van de voortgang van het programma eID in de tweede helft van 2018. Ik ga daarbij onder meer in op de behandeling van de ingediende wetsvoorstellen, de stand van zaken met betrekking tot de ontwikkeling van voorzieningen en de aanbesteding van één of meerdere private authenticatiediensten.

Wendbaar en flexibel

De digitale overheid wordt sterk beïnvloed door snel voortschrijdende technologische ontwikkelingen. Om die ontwikkelingen in goede banen te kunnen leiden moeten we wendbaar en flexibel zijn. Dat betekent dat wij in kleinere stappen gaan werken, zodat we vooruitgang boeken en waar nodig bij kunnen sturen. Mijn wetsvoorstel Digitale overheid biedt daarvoor de ruimte (Kamerstuk 34 972).

Implementatie

De fase van implementatie start; niet overheidsbreed, maar – gezien eerdere adviezen en lessons learned – stap voor stap. Ik kan en wil niet wachten op volledig voltooide oplossingen voor alle sectoren en gebruikers. IJkpunten voor de implementatie zijn de waarden gebruiksvriendelijkheid, veiligheid en betrouwbaarheid uit de agenda NL DIGIbeter, alsmede digitale inclusie. Over digitale inclusie informeerde ik

kst-26643-590
ISSN 0921 - 7371
's-Gravenhage 2019

u op 12 december 2018 met mijn brief «Digitale inclusie – iedereen moet kunnen meedoen» (Kamerstuk 26 643, nr. 583). De groep mensen die digitaal zaken doet met de overheid wil ik vergroten. Dat vergt een aanpak die de gebruiker centraal stelt en die oog heeft voor het oplossen van belemmeringen. Deze ijkpunten vormen het kompas voor de komende jaren. Het eindplaatje staat niet vast, maar wordt bepaald door hoe wij met dit kompas inspelen op de voortschrijdende technologische ontwikkelingen. Voor de volledigheid merk ik op dat voor burgers die dat wensen, fysieke interactie met de overheid mogelijk blijft.

Ik licht in deze brief het belang van de implementatie toe aan de hand van een casus in het burger- en een casus in het bedrijvendomein. Vervolgens ga ik in op de implementatie problematiek en licht ik de vier actielijnen voor 2019 en verder toe. Dan ga ik in op de startsituatie voor de actielijn Substantieel. Ik besluit met een aantal conclusies.

Belang van implementatie: casussen in burger- (zorg) en bedrijvendomein (UWV)

In de zorg is het verkrijgen van de juiste informatie op het juiste moment, op de juiste plek en bij de juiste persoon cruciaal. Goede en tijdige informatie-uitwisseling tussen zorgaanbieders en met patiënten draagt bij aan goede kwaliteit van zorg. Het kabinet heeft daarom meer dan € 400 miljoen beschikbaar gesteld voor versnellingsprogramma's voor informatie-uitwisseling in diverse (zorg)sectoren, gericht op uitwisseling met burgers en tussen zorgprofessionals onderling.

Het UWV wisselt bij ziekte, arbeidsongeschiktheid, zwangerschap, indiensttreding of ontslag, gegevens uit met werkgevers en werknemers. Dit zijn veelal intensieve en ingewikkelde administratieve processen, die veel tijd en geld kosten. Als er misverstanden ontstaan door onjuiste gegevens, kan dit de werkgever of de werknemer schade opleveren. De potentiële maatschappelijke baten van het digitaliseren van deze uitwisselingsprocessen zijn fors.

Voor de digitalisering in deze sectoren is het noodzakelijk dat de waarborgen dat de juiste persoon de gegevens inziet, aanlevert of ontvangt worden verhoogd. Omdat in beide domeinen zeer gevoelige persoonlijke informatie wordt uitgewisseld, heeft de Autoriteit Persoonsgegevens (AP) zowel het UWV als het Ministerie van VWS bericht dat digitale dienstverlening pas aan de Algemene verordening gegevensbescherming (AVG) kan voldoen, als deze op een hoger betrouwbaarheidsniveau plaatsvindt. De Minister van VWS wil dit de komende twee jaar realiseren, maar is daarvoor afhankelijk van de ontwikkelingen in het programma eID. Voor de uitwisseling met het UWV verlangt de AP vanaf november 2019 in ieder geval 2-factor inloggen[1]. Ik hanteer deze aanwijzingen van de AP als richtinggevend voor de overige sectoren.

Deze casuïstiek laat de maatschappelijke urgentie zien van een hoger betrouwbaarheidsniveau van toegang tot digitale dienstverlening en de implementatie en het gebruik daarvan. Ik verbind mij dan ook aan de realisatie van de plannen van de ministeries van VWS en SZW, maar zie deze uitdrukkelijk als voorlopers op de overige dienstverleners en overheden.

[1] Met 2-factor inloggen wordt bedoeld voor het burgerdomein: inloggen met ofwel DigiD-gebruikersnaam, wachtwoord en sms, ofwel DigiD-gebruikersnaam, wachtwoord en app. Voor het bedrijvendomein wordt bedoeld: eHerkenning 2 gebruikersnaam + wachtwoord + sms of tokencode

Implementatieproblematiek

Het programma eID heeft als opdracht het opleveren van authenticatiediensten op betrouwbaarheidsniveau Substantieel en Hoog[2]. Het programma ontzorgt (overheids-)dienstverleners door aansluiting op deze authenticatiediensten te vergemakkelijken.

Op het *burgerdomein* zijn er toegankelijkheidsproblemen waarover ik u in mijn vorige rapportage in juli 2018 informeerde (Kamerstuk 26 643, nr. 550). Dit komt voort uit het feit dat de inlogmiddelen DigiD Substantieel en Hoog voor een brede groep burgers nog niet toegankelijk zijn, onder andere omdat Apple-producten de chips op de identiteitsdocumenten niet kunnen lezen, omdat nog niet iedereen beschikt over een identiteitsbewijs met uitleesbare chip en omdat er nog een oplossing moet worden gevonden voor anders dan mobiele toegang (pc's en laptops).

De belemmeringen in het *bedrijvendomein* hebben een ander karakter. Deze zijn veelal op korte termijn oplosbaar, maar omdat het er relatief veel zijn, moet de aanpak voortvarend worden opgepakt om de invoering van hogere betrouwbaarheidsniveaus niet onnodig te belemmeren. Dit betreft problemen op het gebied van interoperabiliteit, aansluiten en techniek. Daarnaast is er ook sprake van een groot aantal partijen die mogelijk uitgesloten worden omdat een inschrijving bij de Kamer van Koophandel (KvK) wordt vereist voor en door eHerkenning op de niveaus Substantieel en Hoog[3]. Dit probleem treft instanties die niet bij de KvK zijn ingeschreven zoals de Hoge Colleges van Staat, organisaties zonder rechtspersoon en kerken.

Actielijnen voor implementatie

Het is noodzakelijk om zo snel mogelijk hogere niveaus van betrouwbaarheid te introduceren. Door stapsgewijs te implementeren en rekening te houden met wat er nu mogelijk is, bieden we ruimte voor voortdurende innovatie, terwijl er tegelijkertijd wordt gewerkt aan oplossingen die veilig, betrouwbaar en gebruiksvriendelijk zijn.

In samenwerking met de dienstverleners is besproken dat de stapsgewijze implementatie wordt ingezet langs de volgende parallelle actielijnen:
1. Een brede beweging naar 2-factor inloggen (met DigiD app of sms-code)
2. Een lerende uitrol van «Substantieel», te beginnen in de zorgsector in het burgerdomein en bij het UWV in het bedrijvendomein.
3. Een lerende uitrol van «Hoog» bij noodzaak of maatschappelijke baten.
4. Het vergroten van de mogelijkheden van burgers voor toegang tot het niveau Substantieel.

De actielijnen 1, 2 en 3 zijn van toepassing op zowel het burger- als het bedrijvendomein. Actielijn 4 betreft alleen het burgerdomein.

---

[2] In bijlage 1 is een tabel opgenomen met daarin een uitleg van de terminologie van de verschillende authenticatieniveaus.

[3] Voor eHerkenning op het niveau Substantieel en Hoog is het nodig dat de bevoegdheid van de persoon in relatie tot de rechtspersoon kan worden geverifieerd. Dit gebeurt via het Handelsregister.

Actielijn 1: Brede beweging naar 2-factor inloggen

Doordat inlogmiddelen op niveau Substantieel nog niet op een voldoende gebruiksvriendelijke manier toegankelijk zijn, hebben te weinig burgers gemakkelijk toegang tot een hoger betrouwbaarheidsniveau.

Een no regret actie, die later de brede uitrol naar het niveau «Substantieel» en «Hoog» kan vergemakkelijken en versnellen, is het nu al beginnen met het stimuleren van het gebruik van de DigiD App. Deze 2-factor oplossing is een goede stap in het verhogen van het betrouwbaarheidsniveau en laat de gebruikers wennen aan het gebruik van een App als methode om in te loggen. Ik wil derhalve het gebruik van de App stimuleren en ik overweeg daarom een landelijke voorlichtingscampagne en wil afspraken maken met de dienstverleners om ditzelfde te doen.

Als overbrugging kan er voorlopig gebruik gemaakt worden van identificatie met DigiD en wachtwoord waarbij wordt bevestigd met een sms bericht. Deze voorziening is toegankelijk voor alle huidige DigiD-gebruikers.

Een vergelijkbare situatie en aanpak zijn aan de orde op het bedrijvendomein.

Actielijn 2: Lerende uitrol «Substantieel»

Omdat de randvoorwaarden voor een brede uitrol van het authenticatieniveau «Substantieel» nog niet zijn vervuld kies ik voor een lerende uitrol voor dit authenticatieniveau. Voor deze lerende uitrol hanteer ik de volgende strategie:

A. Richten op specifieke sectoren: de zorg en het UWV

Op basis van de eerder genoemde aanwijzing van de AP voor wat betreft het verwerken van gevoelige persoonlijke gegevens, is in die domeinen de noodzaak en bereidheid om tempo te maken het hoogst. Daarom ligt het in de rede om bij de genoemde lerende aanpak te kiezen voor het zorgdomein en de uitwisselingsprocessen van bedrijven met UWV, om in die domeinen zo snel mogelijk tot een hoger betrouwbaarheidsniveau te komen.

B. Wegnemen van belemmeringen

De strategie is erop gericht dat alle betrokken partijen zich tijdens de implementatie kunnen focussen op het signaleren en wegnemen van belemmeringen.

In het *burgerdomein* zijn onder andere de volgende belemmeringen geconstateerd:

- Er zijn circa 2,5 miljoen mensen die hulp nodig hebben bij de (digitale) interactie met de overheid. Hierover informeerde ik u op 12 december 2018 in de brief over digitale inclusie (Kamerstuk 26 643, nr. 583). Met de ingebruikname van een hoger betrouwbaarheidsniveau, voorzie ik dat de behoefte aan een goede machtigingsvoorziening sterk toeneemt.
- Het veilig en betrouwbaar aansluiten op verschillende mogelijkheden (DigiD, privaat middel, machtigen, etc) vergt voor kleine dienstverleners, zoals huisartsen en kleine gemeenten, een verhoudingsgewijs (te) grote inspanning. Deze dienstverleners beschikken over relatief beperkte mogelijkheden om hun klanten toegang te bieden tot hun digitale dienstverlening. Ondersteuning van deze groep om deze zo

efficiënt mogelijk aan te laten sluiten bij toename van het betrouwbaarheidsniveau en bij gebruik van bijvoorbeeld machtigen wordt steeds belangrijker.
- In de huidige systematiek van doorbelasting leidt een toename van digitale interactie tot toename van de kosten voor dienstverleners. Dat verhoudt zich niet met de wens om de groep mensen die digitaal zakendoet met de overheid te vergroten.

Voor het *bedrijvendomein* heb ik in december een taskforce opgericht, die als taak heeft oplossingen te ontwikkelen die de belemmeringen die ik onder «Implementatieproblematiek» beschreef weg te nemen.

C. Starten is belangrijk

Er zullen voortdurend nieuwe innovaties komen die een bijdrage kunnen leveren aan een betrouwbare, veilige, digitale interactie. Wachten is echter geen optie. Bij aanvang zijn onvermijdelijk overbruggingsmaatregelen, zoals zuilen, balies en kaartlezers noodzakelijk. De voortgang van deze maatregelen licht ik verderop toe.

Actielijn 3: Lerende inzet Hoog bij noodzaak of maatschappelijke baten.

De pilot DigiD Hoog in het burgerdomein om met een rijbewijs met uitleesbare chip en een smartphone met NFC-reader (Near Field Communication) in te loggen is succesvol verlopen. Na de inwerkingtreding van de gewijzigde paspoortwet, mogelijk in 2019, komt deze voorziening ook beschikbaar op de nieuw uitgegeven Nederlandse identiteitskaart (NIK). Op dit betrouwbaarheidsniveau is het bij elke inlog noodzakelijk om een daarvoor geschikt identiteitsbewijs uit te kunnen lezen.

Omdat bij elke inlog het gebruik van de identiteitskaart noodzakelijk is, is voor de implementatie van Hoog, zowel de Apple problematiek, als de beperkte beschikbaarheid van identiteitsbewijzen met uitleesbare chip een belemmerende factor. Wel is bij DigiD Hoog naast een mobiele oplossing, ook een PC-oplossing gecombineerd met een kaartlezer nagenoeg gereed. Vooralsnog is deze oplossing voor het niveau Substantieel niet gerealiseerd. Vanwege het beperkte bereik kan slechts op kleinere schaal gestart worden met een lerende uitrol van middelen op niveau Hoog. Ik kies dan ook voor die gebieden waar het noodzakelijk geacht is niveau Hoog in te zetten en de gebieden waar de maatschappelijke en financiële baten het mogelijk maken de aanloopproblemen op acceptabele wijze te compenseren.

In het bedrijvendomein is eHerkenning niveau 4 beschikbaar. Eventuele aanloopproblemen bij het gebruik worden opgepakt door de eerder toegelichte taskforce.

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

Omdat het verhogen van de betrouwbaarheidsniveaus op korte termijn veel belemmeringen kent, is dit een risico voor het vergroten van digitale inclusie. Omdat ik uitsluiting wil voorkomen en zoveel mogelijk burgers op een zo eenvoudig mogelijke wijze toegang wil bieden tot een authenticatiemiddel op niveau Substantieel, loopt er een aantal parallelle sporen om een oplossing te bieden voor de toegankelijkheidsproblemen. Deze sporen zijn:
- het verkrijgen van alternatieve authenticatiediensten (naast DigiD) via een Europese aanbesteding;

- het verbeteren van de mogelijkheden dat burgers en bedrijven iemand kunnen machtigen om de digitale diensten af te nemen. Hiervoor wordt het programma Machtigen uitgevoerd;
- het faciliteren van burgers om op een alternatieve wijze het niveau Substantieel te verkrijgen.

Deze verschillende sporen vergen tijd. Ik blijf parallel werken aan het beproeven van alternatieve oplossingen voor de Apple-problematiek, waarbij het uitgangspunt is dat deze net zo eenvoudig, gebruiksvriendelijk en goedkoop zijn als de Android werkwijze. Dit is onderdeel van permanente ontwikkeling en innovatie.

Startpositie en nadere maatregelen t.a.v. actielijn 2 voor burgers

In deze brief heb ik u meegenomen in de implementatiestrategie. Zoals ik al eerder in de brief opmerkte zijn op dit moment de randvoorwaarden voor een brede uitrol van het authenticatieniveau «Substantieel» nog niet vervuld. Om de doelen van actielijn 2 in het burgerdomein te behalen zijn overbruggingsmaatregelen nodig. In bijlage 2 worden deze opgesomd. De maatregelen worden al enige tijd voorbereid. Het betreft een fors aantal, die technisch meer complex zijn en daardoor meer tijd blijken te kosten om deze te realiseren. Vanwege het belang van de beschikbaarheid van Substantieel zal ik daarom op korte termijn laten inventariseren of versnellingen mogelijk zijn. Ik zal u hierover in de volgende voortgangsrapportage in juli 2019 informeren.

Conclusies

Ik heb in deze brief mijn strategie toegelicht voor de digitale toegang tot interactie met de overheid. Ik kies voor een stimulerende brede aanpak door voor alle sectoren op de kortst mogelijke termijn naar 2-factor inloggen te gaan.
Daarnaast kies ik voor een lerende maar – gelet op de urgentie – niet vrijblijvende aanpak voor de uitrol van het betrouwbaarheidsniveau Substantieel door in eerste instantie te focussen op het zorgdomein en UWV. Ik verbind mij daarmee aan de doelen die mijn collega's van VWS en SZW hebben gesteld. Aanvullend zal ik mij inzetten om de randvoorwaarden te scheppen zodat de digitale toegang tot interactie met de gehele overheid op een hoger betrouwbaarheidsniveau in de komende jaren wordt gerealiseerd. Door in de komende periode te focussen op twee sectoren verwacht ik meer snelheid en rendement te bereiken en tevens te kunnen ontdekken wat wel en wat niet werkt. Ook andere sectoren zullen van deze leerervaringen profiteren. Het blijft vanzelfsprekend de bedoeling dat het betrouwbaarheidsniveau van de digitale diensten van alle andere sectoren en alle andere dienstverleners wordt verhoogd.

Hierbij doe ik recht aan de implementatiestrategie van «je doel bereiken in kleine stappen». Door naast veiligheid en betrouwbaarheid ook te streven naar gebruiksvriendelijkheid, beoog ik de groep mensen en bedrijven die digitaal zaken doen met de overheid te vergroten. De voortgang van de implementatie hangt af van onder meer technische voortgang, marktraadpleging en acceptatie door gebruikers. Dit heeft invloed op de kosten die met de totale implementatie, waaronder overbruggingsmaatregelen, gemoeid zijn. Ik zal dit volgen en indien nodig bijsturen. In de eerstvolgende voortgangsrapportage ga ik daar nader op in. De halfjaarlijkse voortgangsrapportage zal ik in het vervolg opbouwen langs de vier genoemde actielijnen.

Tot slot wil ik benadrukken dat een spoedige behandeling van de Wet digitale overheid en van de wijziging van de Paspoortwet rand voorwaardelijk is om deze aanpak te kunnen uitvoeren.

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

Bij deze brief zijn de volgende bijlagen gevoegd:
1. Tabel Indicatie betrouwbaarheidsniveaus
2. Voortgangsrapportage programma eID
3. Privacyvisie[4]
4. Privacy Impact Assessments (PIA) voor DigiD Hoog[5]
5. Maatschappelijke kosten-batenanalyse (MKBA Machtigingsstelsel)[6]

[4] Raadpleegbaar via www.tweedekamer.nl
[5] Raadpleegbaar via www.tweedekamer.nl
[6] Raadpleegbaar via www.tweedekamer.nl

Bijlage 1

Indicatie betrouwbaarheidsniveau's

Onderstaande tabel geeft een indicatie van de wijze waarop de dienstverlening van overheidsaanbieders kan worden ingeschaald. De criteria uit de tabel komen uit de Handreiking betrouwbaarheidsniveaus van het Forum Standaardisatie. Daarbij geldt dat voor de inschaling van de betrouwbaarheidsniveaus momenteel wordt gewerkt aan criteria, die worden opgenomen in uitvoeringsregelgeving onder de Wet digitale overheid (WDO). De criteria uit de Handreiking betrouwbaarheidsniveaus zullen daarbij als vertrekpunt dienen.

Daarnaast geeft de tabel aan welke middelen (voor burger- en bedrijvendomein) beogen te corresponderen op de eIDAS betrouwbaarheidsniveaus (electronic IDentification Authentication and trust Services). In het kader van de uitvoeringsregelgeving onder de WDO, wordt voor beide domeinen gewerkt aan de invulling van de vereisten op basis van de eIDAS verordening. Daarna kan definitieve toetsing van de middelen plaatsvinden.

eIDAS	**Criteria**	**Burgerdomein**	**Bedrijvendomein**
Geen eisen aan authenticatie	Geen verwerking persoonsgegevens (klasse 0) Geen BSN Geen rechtsgevolg Geen wijzigingen in basisregistratie Economisch belang nihil Publiek belang niet van toepassing		
Laag	Persoonsgegevens max. klasse 1 BSN zelf verstrekt of impliciet in authenticatie Mogelijk indirect rechtsgevolg Alleen wijziging van niet risicovolle basisregistratiegegevens Gering economisch belang Publiek belang laag	(DigiD gebruikersnaam + wachtwoord) of DigiD-gebruikersnaam + wachtwoord + sms-code of DigiD-app + pincode	eHerkenning 1 gebruikersnaam +wachtwoord of eHerkenning 2 gebruikersnaam + sterk wachtwoord of eHerkenning 2 gebruikersnaam + wachtwoord + sms of tokencode
Substantieel	Persoonsgegevens max. klasse 2 Verzwarende factor voor persoonsgegevens bovenop klasse 1 (aard verwerking) BSN verwerkt in combinatie met aanvullende persoonsgegevens Direct rechtsgevolg Opgeven of wijzigen van basisregistratiegegevens die niet onder Hoog vallen Gemiddeld economisch belang Gemiddeld publiek belang	DigiD-app + eenmalig extra ID-check of Privaat Middel verkregen door Europese aanbesteding	eHerkenning 3 gebruikersnaam + wachtwoord + sms of tokencode + verificatie KvK

eIDAS	Criteria	Burgerdomein	Bedrijvendomein
Hoog	Persoonsgegevens klasse 3 Verzwarende factor voor persoonsgegevens bovenop klasse 2 (aard verwerking) BSN verwerkt in combinatie met aanvullende persoonsgegevens Direct creëren, muteren of effectief beëindigen van (authentieke) basisregistratiegegevens Groot economisch belang Groot publiek belang	Inloggen met identiteitsbewijs en DigiD-app (altijd uitlezen id-bewijs via smartphone of kaartlezer)	eHerkenning 4 gebruikersnaam + wachtwoord + sms of tokencode + verificatie KvK + uitlezen identiteitsbewijs

Bijlage 2: **Voortgangsrapportage programma eID**

Deze bijlage is onderdeel van de brief over de implementatie eID en bevat de rapportage over de voortgang van het programma eID in de tweede helft van 2018.

Wet- en regelgeving

In de op 21 december 2018 door uw Kamer ontvangen Nota naar aanleiding van het verslag heb ik uw Kamer geïnformeerd over het voorstel voor de Wet digitale overheid (Kamerstuk 34 972, nr. 6), die rand voorwaardelijk is om burgers en bedrijven een veiligere wijze van inloggen te bieden.
Op 1 oktober werd de wijziging van de Paspoortwet bij de Tweede Kamer aangeboden. Deze wetswijziging is vereist in verband met de invoering van elektronische identificatie op het hoogste betrouwbaarheidsniveau (DigiD Hoog) met de Nederlandse Identiteitskaart (NIK) (Kamerstuk 35 047 (R2108)).

Implementatieplan

In de Voortgangsrapportage eID van 16 juli 2018 (Kamerstuk 26 643, nr. 550) kondigde ik het Implementatieplan voor het betrouwbaarheidsniveau «Substantieel» aan. In de onderhavige brief heb ik de vier parallelle actielijnen van het implementatieplan geschetst.

DigiD app

De DigiD App kwam in november 2017 gereed voor gebruik. In 2018 zijn diverse verbeteringen van de gebruikersvriendelijkheid gerealiseerd. Aan de gebruiksvriendelijkheid wordt doorgewerkt in 2019. Een belangrijke verbetering is het activeren van de DigiD app vanaf één device (telefoon of tablet) waarop de app is geïnstalleerd. Het is niet langer nodig om naar mijn.digid.nl te gaan en er zijn geen twee apparaten meer nodig.
Veel overheidsdienstverleners willen hun dienstverlening ontsluiten met een app. Om het inloggen bij dergelijke apps net zo veilig te laten verlopen als via een vaste computer, is de mogelijkheid gebouwd om met de DigiD-app bij andere apps in te loggen (app2app). In december is de technische ontwikkeling aan de DigiD-app opgeleverd. Voor de Berichtenbox-app van MijnOverheid wordt het als eerste mogelijk om op deze manier in te loggen.

Startpositie en nadere maatregelen t.a.v. actielijn 2 voor burgers

DigiD «Substantieel» (alternatieven voor Apple gebruikers)

In de brief heb ik aangegeven dat ik de startpositie en nadere maatregelen ten aanzien van actielijn 2 voor burgers heb laten inventariseren. In deze paragraaf zet ik deze maatregelen en de status ervan uiteen.
DigiD Substantieel vergt een koppeling tussen een identiteitsdocument en het inloggen. Wij hebben een oplossing nodig voor die groep burgers, die niet beschikken over een smartphone met een geschikte NFC-lezer (Near Field Communication). Apple heeft de NFC-lezer in zijn toestellen niet voldoende open gesteld voor dit doel[7]. Het gevolg hiervan is dat een gebruikersvriendelijke toegang tot dit authenticatieniveau voor meer dan 60% van de burgers nog niet is geregeld. Er is een aantal – elkaar aanvullende – overbruggingsmaatregelen nodig om alle burgers toegang

[7] Voor een nadere toelichting en uitleg van NFC verwijs ik naar mijn brief van 16 juli 2018 (Kamerstuk 26 643, nr. 550, p. 2).

tot dit niveau te geven. Ik geef u hier een inventarisatie van de overbruggingsmaatregelen en de status daarvan:

• Servicezuilen

Logius heeft een eerste oplossingsrichting uitgewerkt, als overbruggingsmaatregel voor Apple-gebruikers. Door middel van een servicezuil met NFC-lezer kan iemand de controle van zijn of haar identiteitsbewijs uitvoeren. Hiermee wordt hun DigiD-app (die kan wel geïnstalleerd worden op een Apple-toestel) versterkt naar het betrouwbaarheidsniveau «Substantieel».
De servicezuiloplossing voor DigiD «Substantieel» is technisch gereed. In het voorjaar van 2019 start een pilot met bibliotheken, gemeentes en zorgverleners. Na evaluatie van de pilot vindt besluitvorming plaats over de eventuele bredere uitrol. Voor deze brede uitrol is een aanbesteding en een implementatieplan nodig.

• Koppelen van een Iphone aan een externe reader

Er wordt gewerkt aan een oplossing waarin door het koppelen van een Iphone aan een externe reader het voor burgers mogelijk moet worden om met deze methode een identiteitsbewijs uit te kunnen lezen. Na het beproeven van deze oplossing moet de bijdrage van deze oplossing aan de implementatieproblematiek worden vastgesteld.

• Koppelen van een Iphone + externe reader voor een PC

Een andere mogelijkheid is om een kaartlezer via de USB-lezer aan een PC te koppelen. Dit kan zowel een eigen PC zijn als een PC van een ander (huisarts of bibliotheek). Door deze oplossing te verbinden met de telefoon van de gebruiker kan ook het betrouwbaarheidsniveau tot het niveau Substantieel worden verhoogd. Het onderzoek hiernaar moet nog worden gestart.

• Het opwaarderen van het niveau bij een balie.

Het onderzoek naar het realiseren van een technische oplossing is gestart.

• Het realiseren van een oplossing op de PC van de gebruiker

Het realiseren van een oplossing op een PC vergt ook een andere technische oplossing omdat in tegenstelling tot een smartphone er geen eenduidige relatie is tussen de gebruiker en het apparaat. De technische realisatie en beproeving van deze oplossing moet nog worden gestart.

• Gastgebruik

Een beproeving wordt voorbereid om een burger zonder geschikt apparaat zijn DigiD te laten versterken naar niveau DigiD Substantieel. De gebruiker maakt daarbij éénmalig (voor het activeren) gebruik van het apparaat van een vertrouwd persoon. Dit wordt gastgebruik genoemd. Na het beproeven van deze oplossing moet de bijdrage van deze oplossing aan de implementatieproblematiek worden vastgesteld.

Het tijdig realiseren van deze overbruggingsmaatregelen is cruciaal voor de in de brief uiteengezette implementatiestrategie en de digitale inclusie. Zoals toegezegd informeer ik u in de volgende voortgangsrapportage over deze maatregelen.

DigiD Hoog (mobiele app en desktop app)

De pilot om in te loggen met DigiD met eRijbewijs op het betrouwbaarheidsniveau «Hoog» is succesvol verlopen. Na inwerkingtreding van de Wet digitale overheid kan gestart worden met het beschikbaar stellen van deze oplossing aan burgers. De rijbewijzen die sinds juni 2018 worden uitgeleverd zijn geschikt voor inloggen met DigiD «Hoog». Tot 1 januari 2019 zijn er circa één miljoen rijbewijzen uitgegeven met een eID-functionaliteit.
In 2019 vindt verdere (door)ontwikkeling plaats om inloggen met DigiD «Hoog» met eNIK (Nederlandse Identiteitskaart) mogelijk te maken. Het moment waarop deze mogelijkheid voor burgers beschikbaar komt hangt mede af van inwerkingtreding van de Wet digitale overheid en van de gewijzigde Paspoortwet.

BSNk polymorfe pseudoniemen

Via BSNk PP (BSN-koppelregister polymorfe pseudoniemen (PP)) wordt een authenticatiemiddel, respectievelijk inlogmiddel, gekoppeld aan het BSN van de gebruiker. In voorbereiding op de Wet digitale overheid is er in 2018 een koppeling gemaakt tussen het rijbewijs en het BSNk PP ten behoeve van DigiD «Hoog». Elk nieuw uitgegeven rijbewijs wordt via deze infrastructuur geactiveerd.

Het BSNk PP is in 2018 geschikt gemaakt voor het inloggen van de eerste Europese burgers volgens de eIDAS-verordening. Er is een koppeling gelegd met het Nederlandse eIDAS-koppelpunt. Dit koppelpunt zorgt voor connectie naar elk van de aangesloten lidstaten en het stelsel Elektronische Toegangsdiensten (ETD). Ook is het BSNk PP aangesloten op de MachtigingenRegister van het ETD-stelsel ten behoeve van eenmanszaken.
In 2019 wordt BSNk PP verder doorontwikkeld ten behoeve van o.a.:
- De realisatie van het Misbruikbestrijdingsregister ten behoeve van detectie van fraude met een authenticatiemiddel respectievelijk inlogmiddel;
- De realisatie van een koppeling tussen de Nederlandse Identiteitskaart en het BSNk PP ten behoeve van DigiD «Hoog», in voorbereiding op de Wet digitale overheid en de gewijzigde Paspoortwet;
- Voorbereiding op de aansluiting van inlogmiddelen van een private authenticatiedienst(en).

Routeringsvoorziening

Ontzorging van kleine overheidsdienstverleners wordt bij toename van het betrouwbaarheidsniveau steeds belangrijker. Kleine partijen beschikken immers over beperkte mogelijkheden. Deze dienstverleners hebben behoefte aan één koppelvlak voor de aansluiting op de toegelaten publieke en private burger-authenticatiemiddelen (inclusief de eIDAS-middelen). Binnen het programma eID wordt daarom gewerkt aan de realisatie van een routeringsvoorziening waarmee mogelijk wordt gemaakt dat dienstverleners maar op één punt behoeven aan te sluiten. Op dit moment worden twee reeds bestaande mogelijkheden verkend, te weten het gebruik van de Identity Bridge bij de Belastingdienst en het gebruik van de Toegangsverleningsservice (TVS), de routeringsvoorziening ontwikkeld door het Ministerie van EZK. Laatstgenoemde verkenning wordt uitgevoerd door het Ministerie van VWS. Daarnaast wordt onderzocht of de huidige makelaars in het bedrijvendomein een rol kunnen spelen in de aansluitingsproblematiek. In 2019 zullen aan de hand van de opgedane ervaringen keuzes worden gemaakt voor de inrichting van de routeringsvoorziening.

Stoppen van pilots met inlogmiddelen van Idensys en iDIN

Over het beëindigen van de pilots met inlogmiddelen van Idensys en iDIN informeer ik uw Kamer door middel van de beantwoording van de schriftelijke vragen gesteld door het lid Middendorp (VVD) over de berichten «Pilots met Idensys stopt per 31 december 2018» en »Einde pilot inloggen met Idensys en iDIN».

Toelatingsprocedure voor één of meerdere private authenticatiediensten

In de vorige kamerbrief (Kamerstuk 26 643, nr. 550) sprak ik de verwachting uit om in 2018 de aanbesteding te kunnen publiceren op TenderNed. Dit bleek niet mogelijk. Het is mijn verwachting de opdracht voor verwerving in de eerste helft van 2019 op TenderNed te publiceren zodat in de tweede helft van 2019 kan worden gestart met de technische implementatie van de private authenticatiediensten.

Machtigen

Het programma machtigen werkt aan de realisatie van de eerder aangegeven gevraagde functionaliteiten en machtigingsoplossing. U bent hierover eerder geïnformeerd (Kamerstuk 26 643, nr. 552). De realisatiefase van het programma loopt stapsgewijs om zo ook in te kunnen spelen op de veranderende wensen en eisen.
Als bijlage 5 bij deze brief is de Maatschappelijke Kosten en Batenanalyse (MKBA) machtigen bijgevoegd[8]. Deze MKBA laat een positieve businesscase zien voor alle betrokkenen. Burgers, bedrijven, professionals en overheidsdienstverleners gaan zowel maatschappelijke baten als ook financiële baten ondervinden van de verbeterde machtigingsfunctionaliteit. De inzichten opgedaan in de MKBA worden eveneens gebruikt voor de toekomstige bekostiging van de machtigingsoplossing.

eIDAS

In 2018 zijn de voorzieningen gereed gekomen waardoor inwoners uit de EU met een genotificeerd inlogmiddel ook bij alle publieke organisaties in Nederland kunnen inloggen. Tevens zijn de voorzieningen gereed om, indien beschikbaar en noodzakelijk, geautomatiseerd een BSN mee te sturen naar de overheidsdienstverleners. Op deze wijze kunnen overheidsdienstverleners voldoen aan de eIDAS Verordening. Een groot aantal overheidsdienstverleners voldoet hier inmiddels aan. Een aantal dienstverleners heeft aangegeven hier iets meer tijd voor nodig te hebben.

Bedrijven

Bedrijven kunnen reeds inloggen bij de overheidsdiensten door gebruik te maken van eHerkenning. Het stelsel van eHerkenning is bij de Europese Commissie aangemeld om genotificeerd te worden. Dit proces zal in de tweede helft van 2019 zijn afgerond. Daarna kunnen Nederlandse bedrijven eHerkenning ook gebruiken bij elektronische dienstverlening van overheden in andere Lidstaten.

Implementatie aanbevelingen CIO oordeel en Gateway-review.

Naar aanleiding van de aanbevelingen uit de Gateway en uit het CIO-oordeel is het afgelopen half jaar een aantal verbetermaatregelen in gang gezet. Ik verwacht deze aanbevelingen voor de komende zomer afdoende te hebben verwerkt.

[8] Raadpleegbaar via www.tweedekamer.nl