

Vergaderjaar 2015–2016

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 419

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 25 augustus 2016

Hierbij informeer ik u over de voortgang van het kabinetsbeleid over de verdere ontwikkeling van de infrastructuur voor (digitaal) inloggen en identificeren. Over dit zogeheten eID beleid heb ik u, mede naar aanleiding van enkele door uw Kamer aanvaarde moties van het lid De Caluwé¹, eerder onder meer geïnformeerd met mijn brief van 14 december 2015². Ook is, mede op uw verzoek, een BIT-toets uitgevoerd, waarvan ik u de resultaten en mijn reactie daarop recent afzonderlijk heb gestuurd³.

Doelstelling van het eID beleid is modernisering van inloggen en overgaan op een hogere beveiliging voor officiële online identificatie. Nederlanders kunnen in de toekomst kiezen uit meerdere manieren om in te loggen en zich te identificeren in het BSN-domein⁴. Zo'n multimiddelenaanpak maakt de publieke dienstverlening in ons land veiliger in geval van een nooit uit te sluiten storing of hack. Deze inlogmiddelen worden enerzijds door de overheid zelf aangeboden in diverse publieke varianten (zwaarder beveiligde versies van DigiD, waaronder een nieuw eRijbewijs en nieuwe identiteitskaart (eNIK)), anderzijds door private partijen. Zo is het een mogelijkheid dat de nieuwste technologie op bankpassen hiervoor geschikt wordt gemaakt en zijn er ook andere private partijen die solide inlogmiddelen aanbieden. Het is, zoals eerder met u besproken, echter niet zo dat ieder inlogmiddel wordt toegestaan. Er is een nadrukkelijk onderscheid met bijvoorbeeld inlogmethoden zoals bekend van sociale media toepassingen. Er gelden strenge eisen voor geautoriseerde digitale toegang tot de dienstverlening in het BSN-domein en het kunnen vaststellen van de identiteit of andere kenmerken zoals leeftijd. Het stellen

¹ Kamerstuk 26 643, nrs. 374 – 376.

² Kamerstuk 26 643, nr. 379

³ Kamerstuk 26 643, nr. 414

⁴ BSN-domein of publiek domein: dienstverlening door overheden en andere instanties die gerechtigd zijn het Burgerservicenummer (BSN) te gebruiken.

van deze (wettelijke) eisen en het toezicht op naleving daarvan is een overheidstaak onder politieke verantwoordelijkheid van de Minister van BZK.

Binnen het programma eID zijn in de afgelopen periode pilots gehouden met een aantal nieuwe manieren om in te loggen in het BSN-domein. De commissie Evaluatie pilots publieke en private authenticatiemiddelen (commissie Kuipers) heeft deze pilots geëvalueerd en is kort geleden met haar bevindingen gekomen⁵. De commissie concludeert dat «alles overziende ... er voldoende aanleiding is om te komen tot zo concreet mogelijke vervolgstappen in de multimiddelenaanpak».

Ook heeft er in de afgelopen periode intensief interdepartementaal en interbestuurlijk overleg plaatsgevonden en overleg met andere (private) partijen om te komen tot gezamenlijke uitgangspunten. Er zijn nu adequate uitgangspunten voor nadere (wettelijke) normering van toegang tot het BSN-domein opgeleverd, waarover ik u eveneens informeer middels deze brief.

Het oordeel van de commissie Kuipers, de adviezen van het BIT en de uitkomsten van genoemd overleg, bieden de grondslag voor een verantwoord besluit om door te zetten naar een volgende fase binnen het programma. Deze stap van de *verkenningsfase* naar de *uitrolfase* is beoogd te starten per 1 oktober 2016. Graag ga ik hierover voor die tijd met uw Kamer in gesprek; tot dan zullen geen onomkeerbare stappen worden gezet. Vanuit aandacht voor minder digivaardigen blijft ook off line dienstverlening vooralsnog mogelijk.

Ik zal u eens per half jaar informeren over de voortgang van de Impuls eID, te beginnen via het dashboard ICT (bij de Jaarrapportage Bedrijfsvoering Rijk) op de derde woensdag in mei 2017 (stand 31 december 2016) en één keer in september/oktober 2017 (stand 30 juni 2017).

Context

De daadwerkelijke start van de uitrol van meerdere manieren van inloggen en officiële online identificatie is een cruciaal onderdeel van de doelstelling uit het Regeerakkoord⁶ dat Nederlanders per eind 2017 hun zaken met de overheid en private organisaties in het BSN-domein digitaal kunnen doen. Diverse beleidsvoornemens op andere terreinen zoals de zorg (eHealth) en de modernisering van de interactie bij belasting- en toeslagzaken zijn hiervan afhankelijk.

Het onophoudelijk en met voorrang verder investeren in de infrastructuur voor digitaal inloggen is noodzakelijk vanwege (i) kwaliteitsverbetering van de publieke dienstverlening, (ii) het steeds grimmiger dreigingsbeeld, bijvoorbeeld ten aanzien van mogelijkheden voor identiteitsfraude en (iii) het binnen de financiële kaders blijven bij de uitvoering van deze dienstverlening.

Tien jaar geleden werd DigiD ingevoerd. Het is hoog tijd voor een impuls om inloggen en identificeren te beveiligen naar de standaarden van vandaag, waarbij burgers tevens meer ruimte krijgen om een inlogmiddel te kiezen wat bij hem of haar past. Niets doen is in deze technologisch snel veranderende wereld geen optie.

⁵ De rapportage en het advies van de voor de evaluatie ingerichte Commissie Kuipers is als bijlage bij deze brief gevoegd, raadpleegbaar via www.tweedekamer.nl

⁶ Bruggen slaan, 29 oktober 2012, p. 11

Nederland neemt een koppositie in op het gebied van digitale dienstverlening. Digitale dienstverlening groeit explosief: in 2013 waren er 100 mln. transacties met het huidige DigiD, in 2015 waren dat er al 200 mln., met enkele honderden dienstverlenende organisaties. De Impuls eID geeft binnen deze context verder invulling aan de wettelijke zorgplicht van de Minister van BZK voor elektronische identificatie (artikel X wet EBV). De impuls is bovenal een noodzakelijke en urgente investering in de veerkracht van onze informatiesamenleving. Juist waar het de meest gevoelige informatie betreft, waaronder gezondheidsgegevens en tal van transacties tussen burgers, professionals en publieke dienstverleners, is een nieuwe vorm van bescherming nodig. Meerdere inlogmanieren zijn essentieel om disruptie tegen te gaan.

Kern van de multimiddelenaanpak onder publiek toezicht

Zoals eerder met u gedeeld, heeft het kabinet besloten dat met name voor inloggen en identificeren door burgers, beroepsbeoefenaren en zzp-ers op de digitale dienstverlening van overheidsorganisaties en private rechtspersonen die gerechtigd zijn het burgerservicenummer te gebruiken, met spoed een kwaliteitssprong nodig is. Samengevat richt het beleid zich op iedereen die vandaag gebruik maakt van DigiD. Tot vandaag kan deze doelgroep slechts op één manier en met slechts één middel (DigiD) inloggen en zich identificeren. Die afhankelijkheid is – te – kwetsbaar. Het kabinet gaat daarom mensen (i) de vrijheid geven om zelf uit meerdere door de overheid erkende inlogmiddelen te kiezen en (ii) daarbij de beschikking geven over ook hoger beveiligde middelen dan tot nu toe, voor toekomstige informatie-uitwisselingen waarvoor dat is vereist. Voor authenticatie van niet-natuurlijke personen zijn en blijven er daarnaast de ook thans al beschikbare eHerkenning inlogmiddelen⁷.

Het kabinet heeft met genoeg kennis genomen van de conclusie uit de recente evaluatie van de pilots, dat deze zogeheten multimiddelenaanpak van meerdere inlogmiddelen naast elkaar – mits zorgvuldig stap voor stap doorgevoerd – in de praktijk goed blijkt te kunnen werken voor de doelgroep waarvoor hij is bedoeld. In de pilots is met een steekproef van deelnemers geëxperimenteerd met diverse zowel publieke als private middelen, waarmee zij konden inloggen op websites van dienstverleners in het zogeheten BSN-domein⁸. Bij private inlogmiddelen moet worden gedacht aan middelen die mensen eventueel ook (kunnen gaan) gebruiken voor bijvoorbeeld kopen bij webwinkels of internet bankieren. Bij publieke middelen komen er, conform de motie De Caluwé⁹, naast de huidige varianten van DigiD ook op niveau substantieel en hoog beveiligde varianten van DigiD. Mensen kiezen aldus in de toekomst zelf hun inlogmiddel dat voor hen vertrouwd is en past bij de eigen gebruiksvoorkeur¹⁰.

Als gezegd, betekent het voorgaande uitdrukkelijk niet dat in de toekomst ieder inlogmiddel in de publieke dienstverlening wordt toegestaan. Zoals in mijn al genoemde brief van 14 december 2015 aangekondigd, komt de toelating van alle publieke en private inlogmiddelen voor het BSN-domein

⁷ In bijlage I worden uitgebreider ingegaan op een en ander, raadpleegbaar via www.tweedekamer.nl

⁸ BSN-domein of publiek domein: dienstverlening door overheden en andere instanties die gerechtigd zijn het BSN te gebruiken.

⁹ Kamerstuk 26 643, nr. 376.

¹⁰ In bijlage II wordt de feitelijke gang van zaken in de beoogde eindsituatie uitgebreider geschetst.

onder één publiekrechtelijk regime en worden bij wet¹¹ eisen gesteld waaraan inlogmiddelen voor gebruik in het publieke domein moeten voldoen, alsook waaraan hierbij betrokken partijen moeten voldoen. Gedurende de pilots de afgelopen maanden en mede op basis van de daarbij verder opgedane kennis en ervaring, is een voorstel voor de inrichting van dit regime – conform ook uw verzoek¹² – op hoofdlijnen inmiddels gereed gemaakt. Bij de voorbereiding van het wettelijke regime zijn relevante stakeholders, waaronder private aanbieders van authenticatiemiddelen, onder meer banken en beoogd toezichthouders betrokken. De nieuwe Europese eIDAS verordening is daarbij leidend geweest¹³.

De Impuls eID

Centraal uitgangspunt bij de Impuls eID is, in lijn met de genoemde aanbevelingen van het BIT, de commissie Kuipers en de bevindingen van uw commissie Elias, het toepassen van een stapsgewijze aanpak. Een gecontroleerde uitrol met een groei via meerdere «stappen», waar nodig ondersteund door nieuwe pilots, biedt heldere momenten van overgang naar de volgende fase en zodoende structuur in het overleg over de voortgang met uw Kamer.

Het kabinet heeft er voor gekozen om de stapsgewijze uitrol vorm te geven als een per 1 oktober a.s. te starten, centraal gestuurde programmatische operatie gedurende twee jaar. Deze Impuls eID dient er in te resulteren dat per uiterlijk oktober 2018 in beginsel alle dienstverleners in het BSN-domein in staat zijn om grootschalig alle door de Minister van BZK toegelaten inlogmiddelen in hun digitale dienstverlening te accepteren. Het kabinet kiest bij het uitwerken van de planning voor het gaandeweg realiseren van dit resultaat in de diverse geledingen van de publieke dienstverlening, met de Zorg en de Belastingdienst als eerste prioriteiten («de voorlopers»).

Ter illustratie een duiding van de voorloper «zorg».

Betrouwbare authenticatiemiddelen zijn een randvoorwaarde voor het realiseren van de eHealthdoelstellingen¹⁴ en het op termijn vervangen van de aparte UZI-pas voor zorgverleners. Het onderzoek naar het betrouwbaarheidsniveau voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg onderschrijft het belang dat er middelen beschikbaar komen op het hoogste betrouwbaarheidsniveau¹⁵. Het onderzoek stelt dat voor inlogmiddelen die gebruikt worden in de zorg minimaal niveau substantieel eIDAS nodig is. Als het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust is het hoogste betrouwbaarheidsniveau (hoog eIDAS) nodig. In overleg met de zorgsector, verenigd in het Informatieberaad, zal een strategie worden ontwikkeld om het gebruik van beschikbare authenticatiemiddelen op het betrouwbaar-

¹¹ De momenteel in voorbereiding zijnde Wet Generieke Digitale Infrastructuur, waarover ik u laatstelijk informeerde in mijn brief Uitgangspunten Wetgeving Generieke Digitale Infrastructuur d.d. 4 december 2015; Kamerstuk 26 643, nr. 373.

¹² Motie De Caluwé, Kamerstuk 26 643, nr. 374.

¹³ Zie bijlage III voor een uitgebreide toelichting, Raadpleegbaar via www.tweedekamer.nl

¹⁴ In 2019: heeft 80% van de chronisch zieken toegang tot bepaalde medische gegevens (van de overige Nederlanders 40%), kan 75% van de chronisch zieken en kwetsbare ouderen die dit wil en er toe in staat is zelfstandig metingen uitvoeren en deze op afstand laten monitoren en heeft iedereen die zorg en ondersteuning thuis ontvangen de mogelijkheid om 24 uur per dag met een zorgverlener te communiceren.

¹⁵ Het «Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg» is namens de Minister van VWS als bijlage bij deze brief gevoegd, Raadpleegbaar via www.tweedekamer.nl

heidsniveau substantieel in de zorg aan te jagen en te faciliteren en op termijn toe te groeien naar patiëntauthenticatie op het hoogste betrouwbaarheidsniveau zodra deze middelen breed beschikbaar komen.

Het kabinet omarmt de positieve energie die de pilots bij de betrokken partijen hebben gegenereerd en wil dit verder uitbouwen. De eerdere opzet van werken met pilots zal ten bate van een goede voorbereiding op de realisatiefase, indachtig de recente adviezen, in de komende maanden worden doorgezet.

Het tijdpad van de uitrol van nieuwe publieke middelen wordt mede beïnvloed door aanbestedingsprocedures. Het kabinet blijft, gezien de bekendheid van en het steeds blijvende vertrouwen in, de merknaam DigiD gebruiken, maar voortaan wel als paraplu van meerdere publieke inlogmanieren. Dit maakt het tevens makkelijker om in de toekomst inlogmanieren op minder ingrijpende wijze blijvend te vernieuwen.

Financiering

De ontwikkeling van de kosten van de multimiddelenaanpak in de tijd is van vele variabelen afhankelijk. Dat geldt vooral voor de kosten die samenhangen met het gebruik (zie bijlage I) aangezien de mate van gebruik van alle publieke middelen (ook in verhouding tot elkaar) nog onvoorspelbaar is. Het gebruik als zodanig, evenals exogene technologische ontwikkelingen zullen periodiek nieuwe en aanvullende eisen stellen aan het stelsel. Kosten van beheer, exploitatie en doorontwikkeling zullen daarom pas gedurende de rit volledig duidelijk worden. Desalniettemin is er wel een redelijk beeld van de kosten die gepaard gaan met een stapsgewijze uitrol van een robuuste infrastructuur voor authenticatie en identificatie, inclusief toelating en toezicht. Het gaat dan om de kosten van het stelsel in zijn basisinrichting (beleidsarm) en onder bepaalde basisveronderstellingen voor het gebruik. Een eerste grove indicatie van die kosten belooft structureel tenminste € 36 mln. Deze worden via de begroting gedekt, en departementen zullen hieraan naar rato bijdragen. Daarbij is het uitgangspunt uiteraard dat de uitrol zo doelmatig mogelijk wordt uitgevoerd en budgetten disciplinerend werken, zonder daarbij uit het oog te verliezen dat een toekomstbestendige financieringsstrategie moet kunnen mee ademen met de implicaties van meergebruik en nieuwe technologische eisen. Naast bovengenoemde kosten voor het stelsel zal sprake zijn van aanschafkosten voor de burger, beroepsbeoefenaren en zzp-ers voor elk van de middelen. Ook zijn er aansluitkosten voor de dienstaanbieders, evenals structurele kosten voor gebruik voor diezelfde dienstaanbieders. Deze kunnen pas later nader in beeld worden gebracht, nadat ook meer duidelijk is over de beprijzing van de private middelen. Dekking van deze kosten geschiedt door middel van doorbelasten via leges of een concrete prijs voor het product en aan de dienstaanbieders op basis van gebruik. In de huidige aanpak zit besloten dat er niet versneld hoogwaardiger publieke alternatieven worden ingevoerd voor het huidige DigiD, omdat de kosten daarvan naar schatting honderden miljoenen belopen. Dat is nog zonder rekening te houden met de additionele uitvoeringslast bij gemeenten.

Afrondend

In het voorgaande is een aantal ontwikkelingen met elkaar in verband gebracht: (1) de nog altijd explosief groeiende digitalisering en de wens van het kabinet dat deze groei ook in het publieke domein doorzet, (2) het cruciale belang van veiligheid en vertrouwen in digitale identiteitsvaststelling en de kansen tot beter benutten van technische ontwikkelingen hierbij, (3) dit met oog voor betere dienstverlening en kostenbesparing.

Mede gezien de toenemende aantrekkelijkheid voor kwaadwilligen om te sjoemelen met digitale identiteiten en de onmogelijkheid dat volledig uit te bannen, heeft dit alles het kabinet gebracht tot deze Impuls als volgende stap op het terrein van inloggen in het BSN-domein. Naar het verleden kijkend is het gevoerde beleid buitengewoon succesvol geweest. Vanuit alle ontwikkelingen naar de toekomst kijkend kan het beleid nog aan effectiviteit winnen. De pilots afgelopen voorjaar hebben uitgewezen dat de verandering die het kabinet voorstaat in de praktijk, mits met verstand stap voor stap doorgevoerd, goed kan werken.

Wat blijft, is de digitale toegang tot publieke diensten in het BSN-domein zoals burgers deze gewend zijn met het huidige DigiD. Wat verandert, is dat voortaan meerdere inlogmiddelen zullen worden toegestaan. Inmiddels is de situatie in ons land zodanig, dat ook privaat meerdere kwalitatief hoogstaande alternatieve oplossingen beschikbaar zijn, analoog aan bijvoorbeeld het online betalen. Het kabinet kiest ervoor ook die alternatieven onder stringente overheidseisen van continuïteit en veiligheid toe te laten. Met een passend financieringsarrangement ontstaat aldus een onder toezicht van de Minister van BZK opererend «level playing field» voor publieke en private oplossingen. Het kabinet is er van overtuigd, dat de onderlinge concurrentie op prijs en kwaliteit de beste uitgangspositie creëert voor vertrouwde verdere digitalisering in de komende jaren.

Ten aanzien van de wereld van consument en bedrijf heeft het kabinet geconstateerd dat met het door de Minister van EZ gevoerde beleid in de digitale wereld van consument en bedrijf en van bedrijven onderling in feite de voorgestane aanpak al groeit. Met dien verstande, dat daar naast private inlogmiddelen niet tevens publieke inlogmiddelen bestaan. Kopiëren van dat model naar het BSN-domein, is wat het kabinet en de Kamer betreft, zoals inmiddels diverse malen in algemene overleggen besproken, niet aan de orde.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
S.A. Blok