Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 550

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 juli 2018

Op 31 januari 2018 zond ik u de voortgangsrapportage van het programma eID over de periode juni tot en met december 2017 (Kamerstuk 26 643, nr. 514). In onderhavige brief meld ik u de voortgang van de wetgeving en het programma over de maanden januari tot en met juni 2018 en geef ik een korte vooruitblik. In deze brief beantwoord ik tevens, conform mijn toezegging in het Algemeen Overleg (AO) Digitale Overheid van 14 maart 2018 (Kamerstuk 26 643, nr. 533), enkele specifieke vragen die door de verschillende leden in dat AO werden gesteld.

Algemeen

Nagenoeg alle dienstverleners in het zogenoemde BSN-domein verlenen digitaal toegang tot hun dienstverlening door middel van DigiD. Veelal is alleen een gebruikersnaam en een wachtwoord vereist. Een aantal dienstverleners vereist twee-factorauthenticatie (door middel van SMS of de DigiD App). Voor veel elektronische dienstverlening zijn echter inlogmethoden met een hoger niveau van betrouwbaarheid gewenst. Het programma eID heeft daarvoor «DigiD Substantieel» en «DigiD Hoog» ontwikkeld. Kernwaarden hierbij zijn veiligheid van inloggen, voldoende waarborgen voor de privacy en het borgen van gebruiksgemak. Inlogmethoden met hogere betrouwbaarheidsniveaus maken tegelijkertijd nieuwe vormen van elektronische dienstverlening mogelijk (innovatie), zoals bijvoorbeeld de ontwikkeling van persoonlijke gezondheidsomgevingen en patiëntportalen.

Ik sluit hiermee aan bij de Nederlandse Digitaliseringsstrategie, die de strategische doorvertaling van de ambities uit het Regeerakkoord bevat (Kamerstuk 26 643, nr. 541) en bij de agenda digitale overheid NLDIGIbeter, die ik op 13 juli 2018 aan uw Kamer zal aanbieden (Kamerstuk 26 643, nr. 549).
Uitgangpunt voor mij is dat overheidsdienstverlening in beginsel digitaal toegankelijk moet zijn. Aandachtpunt daarbij is inclusie: het gebruik van

kst-26643-550
ISSN 0921 - 7371
's-Gravenhage 2018

(digitale) dienstverlening door personen die minder digitaal vaardig zijn. Ik zal een separate brief over inclusie voor het einde van 2018 naar uw Kamer sturen.

Bij de verhoging van betrouwbaarheid zal de overheid zowel inlogmethoden op niveau «Substantieel» als niveau «Hoog» mogelijk maken. Beide inlogmethoden zijn noodzakelijk. We zullen allereerst zorgen voor brede beschikbaarheid van inlogmethoden op het niveau «Substantieel». Daarmee wordt een betekenisvolle stap gezet in verhoging van de betrouwbaarheid. Dit is ook nodig omdat de middelen op niveau «Hoog» in de komende jaren pas geleidelijk worden ingevoerd, via het natuurlijke vervangingspatroon van de rijbewijzen en identiteitskaarten.
Het betrouwbaarheidsniveau «Substantieel», in combinatie van publieke en één of meerdere (nog te verwerven) private authenticatiediensten, is gereed voor bredere implementatie. In de tweede helft van dit jaar zal ik een implementatieplan voor het betrouwbaarheidsniveau «Substantieel» opstellen.

Nieuwe rijbewijzen zijn gereed voor «DigiD Hoog». De gebruiksvriendelijkheid wordt op dit moment in een pilot beproefd. De urgentie om te starten met het mogelijk maken van inlogmethoden op niveau «Hoog» is bijvoorbeeld groot voor dienstverlening die medische gegevens betreft. Daarom is het rijbewijs al gereed gemaakt voor «DigiD Hoog» en zal dat met de NIK in 2019 het geval kunnen zijn. In de tussentijd zullen we blijven beproeven op welke wijze inloggen op het hoogste betrouwbaarheidsniveau zo gebruiksvriendelijk mogelijk kan worden.

Wet- en regelgeving

Het voorstel voor de Wet digitale overheid is op 19 juni 2018 ingediend bij uw Kamer (Kamerstuk 34 972). Afhankelijk van de voortgang van de behandeling door de beide Kamers, zal inwerkingtreding naar verwachting in 2019 kunnen plaatsvinden. Gelet op het randvoorwaardelijke karakter van het wetsvoorstel, zet ik mij graag met uw Kamer in voor een snelle behandeling.
De wet zal gefaseerd worden ingevoerd, afhankelijk van de mate waarin de uitvoerende organisaties in staat zijn te voldoen aan de gestelde eisen. Bij de verdere voorbereiding van de uitvoeringsregelgeving zal de uitvoeringstoetsing een prominente plaats innemen met het oog op een gecontroleerde invoering van de wet.

In het kielzog van de Wet digitale overheid is een separate wijziging van de Paspoortwet voorbereid om inloggen met een Nederlandse Identiteitskaart (NIK) via DigiD op het betrouwbaarheidsniveau «Hoog» mogelijk te maken. Ik verwacht dat het wetsvoorstel na het zomerreces aan de Kamer kan worden aangeboden.

NFC (Near Field Communication)

NFC is contactloze communicatie tussen twee apparaten op korte afstand van elkaar. NFC is een tweeweg-communicatie (dus verzenden en ontvangen) tussen bijvoorbeeld een mobiele telefoon en een wettelijk identificatiedocument of voor contactloos betalen met een betaalpas bij een pinapparaat.
De publieke inlogmiddelen «DigiD Substantieel» en «DigiD Hoog» vereisen het eenmalig respectievelijk telkens uitlezen van de chip van een identiteitsdocument (de toepassing van NFC per niveau wordt in het vervolg van deze brief toegelicht). Dit kan met de NFC-functie in mobiele apparaten (tablets en smartphones) of NFC-lezers verbonden aan computers.

Het uitlezen van identiteitsdocumenten is nu al mogelijk met een aan een computer verbonden kaartlezer en met mobiele apparaten met een Android besturingssysteem voorzien van een NFC-functie. Bij apparatuur voorzien van het iOS besturingssysteem (Apple) kan dit vooralsnog niet. Apple heeft de benodigde functionaliteit binnen de NFC voor deze toepassing niet toereikend opengezet. Ik acht het van wezenlijk belang dat alle gebruikers van gangbare mobiele apparaten de mogelijkheid tot het gebruik van de meer betrouwbare inlogmiddelen krijgen. Daarom is het zeer wenselijk dat Apple afdoende toegang verleent tot de NFC-functie op zijn toestellen.
Dit probleem speelt ook internationaal en in andere Europese landen; de in Nederland gezochte oplossingen voor hoogwaardige authenticatie worden immers ook in andere landen gebruikt. In de Europese afstemmingsgroep waarin de voortgang van eIDAS wordt besproken is deze problematiek geagendeerd.

«DigiD substantieel»

Sinds november 2017 is «DigiD Substantieel» te installeren door de bestaande chips op Nederlandse identiteitsdocumenten *eenmalig* uit te lezen met een NFC-lezer op mobiele apparaten met het Android besturingssysteem. Beoogd wordt daarmee te voldoen aan het Europese betrouwbaarheidsniveau «Substantieel». Dit niveau zal voor de meeste digitale dienstverlening, op termijn, de norm worden.

Op dit moment worden oplossingen onderzocht en getest voor de niet-Android toestellen. Omdat bij «DigiD Substantieel« de chip slechts *eenmalig* moet worden uitgelezen, wordt gedacht aan oplossingen zoals een selfservice kiosk op nader te bepalen punten in steden en dorpen, waarna de burger voortaan met zijn niet-Android toestel «DigiD Substantieel» kan gebruiken. Voorts is het toelaten van één of meerdere private authenticatiediensten één van de mogelijkheden om de dekkingsgraad van het betrouwbaarheidsniveau «Substantieel» te verhogen. In het implementatieplan voor «Substantieel» zal ik ook aandacht besteden aan inclusie (door middel van bijvoorbeeld machtigen), het handhaven van fysieke mogelijkheden van dienstverlening (post, telefoon) en het op termijn uitfaseren van het laagste niveau van DigiD. Ook het voorlopig handhaven van DigiD twee-factorauthenticatie vormt onderdeel van dit plan.

«DigiD Hoog»

Zoals hiervoor al geduid moet bij DigiD op betrouwbaarheidsniveau «Hoog» niet *éénmalig*, maar *bij elke inlog* een wettelijk identiteitsdocument worden uitgelezen. Sinds 4 juni 2018 worden rijbewijzen uitgegeven met een nieuwe chip die geschikt is om via de DigiD-app en via NFC-lezers aan computers in te loggen op websites van overheidsdienstverleners op het hoogste Europese betrouwbaarheidsniveau («Hoog»). Op dit moment vindt een pilot plaats (met ca. 200 deelnemers). Bij een succesvolle uitkomst van de pilot kunnen burgers vanaf een nog te bepalen tijdstip inloggen met gebruikmaking van de nieuwe chip op het rijbewijs.
De Nederlandse Identiteitskaart (NIK) kan pas geschikt gemaakt worden voor inloggen op het hoogste betrouwbaarheidsniveau als de gewijzigde Paspoortwet in werking is getreden. Zoals gemeld, verwacht ik dat dit wetsvoorstel na het zomerreces naar de Kamer kan worden gezonden.

Vanwege het feit dat voor «DigiD Hoog» bij elke inlog het identificatiedocument uitgelezen moet worden, speelt de problematiek van de niet beschikbare NFC-lezer op mobiele apparaten zonder Android besturings-

systeem sterker. Bij «DigiD Hoog» zijn aparte NFC-lezers voor niet-Android bezitters op dit moment het enige alternatief om de chip op de identiteitsdocumenten bij elke inlog uit te lezen.

De geleidelijke introductie van «DigiD Hoog» is dus al gestart met de uitgifte van daarvoor geschikte rijbewijzen. Samen met sectoren waarin vraag is naar het hoogste betrouwbaarheidsniveau, zoals die sectoren waarin medische persoonsgegevens worden verwerkt, werk ik aan de verdere invoering van «DigiD Hoog». Ik zal hierbij ook de uitkomsten van de huidige pilot meenemen en u hierover in de volgende voortgangsrapportage informeren.

In het AO van 14 maart 2018 (Kamerstuk 26 643, nr. 533) is door het lid Van der Molen gevraagd naar de levensduur van de chip. De technische levensduur van de chip is gelijk aan de geldigheid van deze identiteitsdocumenten, namelijk tien jaar. De gebruiker kan zijn identiteitsdocument dus gedurende de gehele geldigheidsduur van het document gebruiken. Uiteraard gaat daarnaast de ontwikkeling van de chip (voor nieuw uit te reiken kaarten) en voor de centrale software door. Nieuw uit te geven identiteitsdocumenten zullen telkens met de meest actuele chips worden uitgerust.

Toelatingsprocedure voor één of meerdere private authenticatiediensten

De resultaten van de marktconsultatie naar één of meerdere private authenticatiediensten waren veelbelovend, zoals ik uw Kamer in mijn brief van 31 januari 2018 (Kamerstuk 26 643, nr. 514) heb gemeld. Ik heb daarom begin dit jaar besloten over te gaan tot de voorbereiding van een procedure tot verwerving van de inzet van één of meerdere private authenticatiediensten. Het streven is deze in de loop van 2019 gereed te hebben voor gebruik voor het inloggen bij een aantal dienstverleners. Naar verwachting wordt deze overheidsopdracht in het najaar van 2018 gepubliceerd op TenderNed, het digitaal aanbestedingssysteem voor overheidsopdrachten. Vanaf dan kunnen potentiële aanbieders intekenen op deze opdracht.

eIDAS

De Europese eIDAS-verordening regelt dat burgers en bedrijven uit EU-landen digitaal zaken moeten kunnen doen met de overheden van de andere EU-landen. De verplichting om buitenlandse inlogmiddelen te accepteren gaat op 29 september 2018 in.
De implementatie van de eIDAS-verordening voor inkomend digitaal verkeer is momenteel in volle gang. Overheidsdienstverleners zijn via diverse kanalen geïnformeerd over de eIDAS-verordening en werken aan hun aansluiting. De centrale voorziening voor de doorgeleiding van de buitenlandse authenticaties naar de Nederlandse overheidsdienstverleners is gereed. Daarmee voldoet Nederland aan de vereisten van de verordening. Er wordt bovendien voor dienstverlening waarbij, in aanvulling op de minimale eIDAS-dataset, een burgerservicenummer is vereist, een speciale voorziening ontwikkeld. Deze voorziening vergelijkt en koppelt de gegevens van elektronische inlogmiddelen van andere Lidstaten met de gegevens in de Basisregistratie Personen.
In het AO werd door het lid Den Boer gevraagd naar de implementatiekosten van de eIDAS-voorzieningen. De beheer- en exploitatiekosten voor inkomend eIDAS-verkeer worden geraamd op € 4,5 miljoen op jaarbasis. Deze kosten zullen worden doorbelast aan de overheidsdienstverleners. Volgens plan zal het in 2019 mogelijk zijn voor burgers en bedrijven om met Nederlandse eID-middelen in te loggen bij overheden van andere EU-lidstaten.

Overig

De businesscase

In het AO van 14 maart 2018 2018 (Kamerstuk 26 643, nr. 533) merkte het lid Van der Molen op dat, omdat er meer digitale dienstverlening is, de digitale fraude toeneemt, of je de dienstverlening nu verder beveiligt of niet. Mijn doel is het tegengaan van identiteitsfraude en ongeautoriseerde toegang. Om die reden is de ontwikkeling gestart om te komen tot eID-middelen op een hoger betrouwbaarheidsniveau. In de businesscase is een inschatting gemaakt van de aan maatschappelijke fraude gerelateerde kosten die door het gebruik van betrouwbaardere inlogmiddelen kunnen worden vermeden (Kamerstuk 29 643, nr. 528).

In het AO werd door het lid Van der Molen ook gevraagd naar de kosten van het aansluiten van één of meerdere private authenticatiediensten. De hoogte van de aansluitkosten zal duidelijk worden wanneer deze opdracht is gegund. De kosten van het daadwerkelijk gebruik hiervan worden doorbelast aan de overheidsdienstverleners.

Voor het financieel overzicht en het overzicht van de documentatie verwijs ik naar het Rijks ICT-Dashboard: https://www.rijksictdashboard.nl/projecten/261022
In de volgende rapportage zal ik nader ingaan op de kosten en baten van het programma eID, de financiering daarvan, alsmede de te verwachten meerjarige kosten en baten. Ook besteed ik daarin aandacht aan de aanbevelingen die Ecorys deed in de businesscase.

Attributendiensten

Een attribuut is een eigenschap van een persoon, bijvoorbeeld zijn voornamen, zijn leeftijd, het feit dat de persoon ouder is dan 18 jaar, zijn geslacht, beroep e.d. Het lid Van der Molen vroeg in hetzelfde AO hoe het zit met de attributendienst.
Bij authenticatie in het BSN-domein wordt nu via DigiD geen attribuut geleverd, maar enkel het BSN (al dan niet in een versleutelde vorm). Door de (automatische) koppeling met de BRP halen de dienstverleners de persoonsgegevens op die vereist zijn voor de afhandeling van het verzoek, zoals geboortedatum en adres. In de ontwikkelde eID-infrastructuur is rekening houden met een verdere doorontwikkeling, waarbij andere attributenregisters dan de BRP kunnen worden geraadpleegd.

Uitkomsten Gateway Review en CIO-oordeel

In het tweede kwartaal van 2018 zijn twee reviews afgerond over het programma eID, namelijk een Gateway Review (mei) en, recent, een CIO-oordeel. De aanbevelingen uit de Gateway Review treft u in de bijlage aan. Het CIO-oordeel is in lijn met deze aanbevelingen.
Met de instelling van de programmadirectie I is één van de aanbevelingen uit de Gateway Review inmiddels gerealiseerd. Bij deze directie wordt binnen het Ministerie van BZK de regie op de samenhang tussen de diverse ICT-programma's belegd. Deze nieuwe directie zal fungeren als opdrachtgever van de diverse programma's binnen het I- domein, zoals de programma's eID, Machtigen en vervolg BRP.
De Gateway-review geeft zinvolle aanbevelingen voor de uitvoering van het programma eID. De programmadirectie zal gevolg geven aan deze aanbevelingen, aan het CIO-oordeel en aan aanbevelingen zoals die van

de Commissie BRP. In de volgende voortgangsrapportage eID zal ik nader ingaan op de voortgang van deze aanbevelingen. Die voortgangsrapportage ontvangt u in januari 2019.

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

BIJLAGE:

AANBEVELINGEN GATEWAY REVIEW

De aanbevelingen van de Gateway Review luiden als volgt.

1. Realiseer vanuit de stelselverantwoordelijkheid voor de digitale overheid, in co-creatie met alle spelers (publiek, semipubliek) en stakeholders een meerjarige roadmap van de digitale overheid. Zodat alle partijen helderheid hebben wat zij hiervan mogen verwachten, wat zij daarin zelf voor een rol hebben en zij hierop ook hun eigen acties kunnen richten.
2. Start per direct met voortdurende communicatie waarin helder is: wat de hoofdboodschap is (waarom, wat, wanneer), welke rollen en rolverdeling wordt afgesproken(wie, wat, wanneer). Maak vooral gebruik van de uitvoeringsorganisaties en gemeenten, provincies als communicatie kanaal/organisatie. Richt vanuit het besef dat burgers een bepaalde verwachting hebben over de veiligheid van inlogmiddelen en privacy, een feedback loop in voor interactie en bijsturing op zowel boodschap als middelen.
3. Versterk de governance op de realisatie door:
   a. Prioriteit te geven aan de bundeling onder één programmamanager van projectactiviteiten die nu in de realisatiefase zijn beland.
   b. De bestaande programboard onder de stuurgroep om te vormen tot een gemandateerd besluitvormend orgaan op directeuren niveau. Beleg daar ook de budgetsturing en volg daarbij de normale prince2 uitgangspunten voor de samenstelling van senior-users en -suppliers. Leg daar de verantwoordelijkheid voor de realisatie van de producten en diensten in hun samenhang en planning. Op termijn moet deze rol worden overgenomen door de nieuw gevormde programmaraad Logius.
   c. Versterk/richt de quality assurance binnen het programma in waarin naast budgetbeheer,kwaliteitsbewaking ook effecten op investeringen en exploitatie-effecten van de opgeleverde producten en hun beheer en dienstverleningsafspraken.
   d. Ga door met de aanstelling/werving van de Programmadirecteur I en beleg bij deze functionaris de volgende taken:
      i. «schakel/buffer» tussen strategie en stelsel enerzijds en realisatie anderzijds vanwege het verschil in tempo (kaasstolp-management).
      ii. toezichthouder op de productrealisatie (integrale planning en voortgangsbewaking) en
      iii. sturing op de samenhang van eID met andere ontwikkelingen van het stelsel en de producten in de keten en de aansturing van de programmamanager.
4. Versterk de control functie vanuit de CIO/BZK op de gekozen technische oplossingen bij de verschillende partijen. Vraag de Rijks CIO een uitspraak te doen over de samenhang van de gekozen onderliggende architectuur producten.
5. Herbevestig en expliciteer de in gang gezette werving/aanbesteding voor het private middel substantieel met doorontwikkeling naar hoog en de daarbij gehanteerde criteria.