

Vergaderjaar 2019–2020

34 972

Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)

Nr. 26

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 januari 2020

Tijdens de behandeling van het wetsvoorstel tot wijziging van de Paspoortwet (Kamerstuk 35 047 (R2108)), op 23 januari jl. (Handelingen II 2019/20, nr. 45, debat over het wetsvoorstel wijziging van de paspoort wet in verband met de invoering van elektronische identificatie met een publiek identificatiemiddel en het uitbreiden van het basisregister reisdocumenten), heeft uw Kamer een aantal vragen gesteld die primair betrekking hebben op het wetsvoorstel digitale overheid. Ik hecht eraan deze vragen te beantwoorden voorafgaand aan de behandeling van het wetsvoorstel digitale overheid (Kamerstuk 34 972), welke is voorzien op 30 januari a.s. (Handelingen II 2019/20, nr. 48, debat over de wet digitale overheid).

Ik beantwoord en cluster deze vragen naar onderwerp.

Uitrol en beschikbaarheid publieke inlogmiddel

Het lid Verhoeven (D66) heeft mij gevraagd waarom 35% van de mensen geen gebruik kan maken van DigiD op betrouwbaarheidsniveau substantieel, gezien de theoretische dekkinggraad van 65%. Tevens is gevraagd of mensen die geen smartphone hebben, er een moeten aanschaffen, of een kaartlezer nodig is, en of inloggen zonder smartphone mogelijk blijft. De heer Verhoeven vraagt verder in hoeverre het toekomstig gebruik van DigiD afhankelijk is van de producenten van smartphones. Ten slotte heeft hij gevraagd of ik probeer om de dekkinggraad nog te verhogen, en naar welk percentage ik streef met behulp van private inlogmiddelen.

De vragen die de heer Verhoeven stelt, hebben betrekking op de implementatie van inlogmiddelen. Voor een meer gedetailleerde toelichting verwijs ik naar de Voortgangsrapportage Toegang, waarin ik u meer in de breedte informeer over de voortgang van de implementatie van de

inlogmiddelen. Deze Voortgangsrapportage ontvangt u eveneens voorafgaand aan de plenaire behandeling van de Wet digitale overheid.

De oplossing waarmee 65% van de huidige DigiD-gebruikers op het niveau substantieel wordt bediend, maakt gebruik van de zogeheten NFC-chip in smartphones. Het bereik zegt wat over de hoeveelheid mensen die geen smartphone bezit én over iedereen die wel over een smartphone beschikt, maar deze functionaliteit niet op zijn telefoon heeft. Mijn uitgangspunt is dat iedereen moet kunnen meedoen. Wij mogen en willen niemand uitsluiten. Ik zoek daarom doorlopend naar mogelijkheden om deze groep te faciliteren. Dat doe ik enerzijds door het bereik van de huidige oplossing te vergroten, maar ook door te zoeken naar alternatieven om inloggen op betrouwbaarheidsniveau substantieel mogelijk te maken. Ik doe dat ook om niet afhankelijk te zijn van een enkele oplossing of leverancier. Die alternatieven kunnen daarom ook private inlogmiddelen zijn. En voor iedereen waarvoor de digitale weg echt niet mogelijk is, zal volgens de Algemene wet bestuursrecht de papieren weg mogelijk blijven, tenzij dit bij andere wet uitdrukkelijk wordt uitgesloten. Het wetsvoorstel digitale overheid beoogt niet om digitaal verkeer te verplichten, wel om de voorzieningen daarvoor te reguleren.

Verplichting om op hogere betrouwbaarheidsniveaus in te loggen

De heer Verhoeven heeft gevraagd of het inloggen met een ID-kaart of rijbewijs met chip bij sommige overheden verplicht wordt.

Het wordt met de wet digitale overheid verplicht om in te loggen op hogere betrouwbaarheidsniveaus dan nu nog het geval is. Inloggen op hogere betrouwbaarheidsniveaus zal straks ook op meerdere wijzen mogelijk zijn, bijvoorbeeld met private middelen. Afhankelijk van de werking van een inlogmiddel kan dit op verschillende manieren. Overheidsorganisaties bepalen zelf welk inlogniveau vereist is. Dat is nodig om de veiligheid van de (persoons)gegevens die bij deze dienstverlening worden verwerkt te waarborgen. De Autoriteit Persoonsgegevens verlangt ook voor bepaalde diensten een hoog inlogniveau, bijvoorbeeld in de zorg.

Kosten van de elektronische identiteitskaart

Het lid Van Raak (SP) heeft gevraagd hoe het zit met de kosten die moeten worden betaald voor een elektronische identiteitskaart (eNIK) en of mensen moeten betalen als zij die niet gebruiken. Tevens vroeg de heer Van Raak wat er gebeurt als mensen net een kaart zonder chip gekocht hebben.

De kosten worden betaald voor het gebruiksklaar maken van de kaart, niet voor het gebruik. Hier geldt de analogie van de reguliere identiteitskaart. De gebruiker betaalt voor de beschikbaarheid, maar het gebruik ervan verschilt per gebruiker. Het gaat erom dat de gebruiker erover kan beschikken en terugvallen als dat nodig is. Bij de aanschaf van middelen zal altijd een risico bestaan dat net voor het verschijnen van een nieuwe functionaliteit een middel wordt gekocht. Dat zal nooit helemaal te voorkomen zijn. Ik zal daar in de communicatie zoveel mogelijk rekening mee houden, om deze situaties tot een minimum te beperken.

Inzet private partijen/banken

De heer Van Raak vraagt zich af waarom het aanbieden van inlogmiddelen wordt overgelaten aan private partijen, waaronder banken.

Zoals ik eerder heb opgemerkt, vind ik het voor de toegankelijkheid van de digitale toegang tot de overheid belangrijk dat er terugvalopties zijn in het geval een middel – dat kan een overheidsmiddel zijn – onverhoopt niet beschikbaar is. Het terugbrengen van de afhankelijkheid van één middel is de essentie. Op de huidige digitale markt ontstaan zeer snel zowel nieuwe dreigingen als innovatieve mogelijkheden om burgers daartegen te beschermen.

Mede daarom is voor mij doorslaggevend om, mede op instigatie van uw Kamer, te kiezen voor een systeem van open toelating, om zo de beschikbaarheid van nieuwe beschermingsmethoden beter te faciliteren en beter mee te kunnen bewegen met de ontwikkelingen en de stand der techniek. Dit zorgt ervoor dat burgers en medeoverheden sneller gebruik kunnen maken van wat de markt hen aan nieuwe (beschermende) mogelijkheden te bieden heeft. Ik heb u daarover in mijn brief van 5 juli 2019 geïnformeerd.¹

Ik ben mij er terdege van bewust dat de inzet van private partijen strenge eisen stelt ten aanzien van privacybescherming. Daar is en wordt terecht veel aandacht voor gevraagd, onder meer door de Cyber Security Raad en het Rathenau Instituut. Op het moment dat private partijen worden ingezet om inloggen bij de (semi-)overheid mogelijk te maken, worden strenge eisen aan inlogmiddelen gesteld. Uitgangspunt daarbij zijn de Europese eIDAS-regels voor inlogmiddelen en de privacy-eisen uit de Algemene Verordening Gegevensbescherming. Daarnaast worden voor de feitelijke inrichting van de middelen regels gesteld aan de wijze waarop gegevens worden opgeslagen, zodat deze niet ongewenst kunnen worden gekoppeld. Ook wordt in de uitvoeringsregelgeving, die ik aan uw Kamer zal voorleggen, bepaald dat gegevens door deze partijen enkel en alleen mogen worden verwerkt voor het bieden van de inlogfunctionaliteit. Ander gebruik wordt expliciet verboden.

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

¹ Kamerstuk 34 972, nr. 11