

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3480

Vragen van het lid **Leijten** (SP) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het nieuws dat de SMS-controle van DigiD wordt uitgefaseerd* (ingezonden 17 mei 2022).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 8 juli 2022).

Vraag 1

Klopt het dat na de uitfasering van de SMS-controle van DigiD er alleen nog authenticatie via de app kan worden gedaan? En zo ja, is het dan juist dat deze app alleen verkrijgbaar is voor Apple en Google telefoons?¹

Antwoord 1

Voorop staat dat SMS-authenticatie, zoals gesteld in het commissiedebat van 22 maart jl., voorlopig behouden blijft. Belangrijk is echter wel dat er oog blijft voor een continue verbetering van de beveiliging en de veiligheidseisen. Hierbij moet onder andere voldaan worden aan de veiligheidseisen die gesteld zijn binnen Europa. Binnen de eIDAS regelgeving wordt er onderscheid gemaakt tussen de niveaus laag, substantieel en hoog. Hierbij is het met name van belang dat er een nauwkeurige en betrouwbare identiteitsvaststelling plaats kan vinden. Tweefactor-authenticatie, zoals SMS-authenticatie, behoort tot het laagste niveau. De DigiD app is alleen verkrijgbaar voor Android en iOS telefoons.

Vraag 2

Kunt u aangeven waarom gekozen wordt inwoners te dwingen gebruik te maken van Amerikaanse techbedrijven en daarmee hun marktmacht te versterken? Kunt u uw antwoord toelichten?

Antwoord 2

De redenen hiervoor zijn praktisch en niet principieel van aard. De voornaamste redenen om de DigiD-app in beginsel alleen voor de besturingssystemen iOS en Android aan te bieden zijn:

Bereik; meer dan 99% van de smartphones gebruikt iOS of Android als besturingssysteem.

¹ <https://www.security.nl/posting/695698/Overheid+gaat+inloggen+via+DigiD+met+sms-controle+op+termijn+uitfaseren>.

Betrouwbaarheid van de app store; er moet voldoende vertrouwen zijn in de app store; zo moet de software bijvoorbeeld deugdelijk zijn en voldoen aan de standaarden van de store. Ondeugdelijke apps in de stores van iOS en Android worden verwijderd.

Bezitsfactor; bij een digitale authenticatie moet er zekerheid bestaan over de identiteit van de gebruiker, dit vraagt bepaalde technologie die op dit moment alleen door Apple in iOS en door Google in Android wordt aangeboden.

Vraag 3

Klopt het dat er geen alternatief wordt geboden voor partijen die geen gebruik maken van de diensten van Google of Apple en daardoor ook geen toegang meer hebben tot de overheidsdiensten? Wat gaat u ondernemen om te regelen dat er wel alternatieven worden geboden?

Antwoord 3

Naast het gebruik van de DigiD-app op de besturingssystemen iOS of Android is SMS het huidige alternatief. In de verdere ontwikkeling van DigiD speelt naast veiligheid ook inclusiviteit een belangrijke rol.

Vraag 4

Kunt u toelichten hoe het besluit om geen andere mogelijkheden naast de apps van Google en Apple strookt met het «comply or explain»-principe van de overheid ten aanzien van open source?

Vraag Antwoord 4

Er is geen expliciet besluit, zoals toegelicht in de beantwoording van vraag 2. Het «Pas toe of leg uit»-principe is van toepassing op het openstandaardenbeleid van de overheid. In het geval van het ontwikkelen van software gaat het om het «Open Tenzij»-principe zoals gesteld in de Kamerbrief verstuurd op 17 april 2020 met als onderwerp «Beleidsbrief vrijgeven van de broncode van overheidssoftware» (Kamerstuk 26 643, nr. 676). Voor het vrijgeven van bestaande software moet er een afweging worden gemaakt ten aanzien van de veiligheid van de software en de informatie die met de applicatie verwerkt wordt. Zoals gesteld in de Kamerbrief kost het vrijgeven van broncode bij bestaande software de nodige investeringen.

Vraag 5

Kunt u aangeven waarom de overheid de DigiD-app niet open source heeft laten ontwikkelen? Is zij als nog van plan dit te gaan doen zodat de app ook in de F-droidstore aangeboden kan worden?

Antwoord 5

DigiD gebruikt open source componenten, maar publiceert de broncode van de app (nog) niet. Een verkenning of het mogelijk is om de broncode van DigiD open source te publiceren is gaande, maar het publiceren van de broncode moet wel op een verantwoordelijke en veilige manier mogelijk zijn. Veiligheid en bescherming van gegevens van gebruikers blijven in de doorontwikkeling altijd een factor. Het risico bestaat dat de broncode gebruikt wordt om de app te klonen om via die weg gegevens afhandig te maken van de gebruiker.

Vraag 6

Is het juist dat in de huidige app trackers zijn aangetroffen? Wat zijn de gevolgen van deze trackers in de app?²

Antwoord 6

Het is juist dat de app trackers van respectievelijk Microsoft en Google bevat. Dit is noodzakelijk voor de (technische) ondersteunings- en beheerfunctionaliteit van de applicatie. De twee Microsoft trackers zorgen ervoor dat informatie bij het ontwikkelteam van DigiD terecht komt als de applicatie niet stabiel werkt of crasht. Deze gegevens worden niet naar Microsoft gezonden, maar alleen naar het ontwikkelplatform van DigiD. Het betreft geen persoonlijke

² exodus (exodus-privacy.eu.org).

gegevens en de trackers hebben ook niet als doel om het gedrag van de gebruiker te volgen.

De tracker van Google is nodig voor technische ondersteuning van de push-notificatiefunctie in Android. Een push-notificatie kan vanuit een applicatie een bericht sturen naar de gebruiker dat er een bericht klaar staat in de applicatie. Bij DigiD gebeurt dit alleen in uitzonderlijke gevallen en nooit met persoonsgegevens. Voor het versturen van een push-notificatie wordt expliciet toestemming gevraagd aan de gebruiker om deze functionaliteit al dan niet toe te staan.

Vraag 7

Hoe gaat u voorkomen dat door het gebruik van deze apps data van Nederlandse burgers worden doorgegeven aan de Amerikaanse overheid, omdat beide bedrijven onder de zogenaamde Patriot Act vallen?

Antwoord 7

Beide bedrijven hebben geen inzicht in de gegevens van de gebruikers van de applicatie. Zij hebben geen toegang tot de inloggegevens, noch tot de informatie die de burger via het inloggen wil inzien. De DigiD-app stuurt geen gegevens door naar Apple of Google.

Notificatiedata lopen wel via een centrale poort in het besturingssysteem. Om die reden wordt er zo min mogelijk gebruik gemaakt van notificaties en wordt hier nooit gevoelige of persoonlijke informatie gedeeld. Als gebruiker is het mogelijk om notificaties uit te schakelen.

Vraag 8

Kunt u aangeven hoe het uitfaseren van SMS bij DigiD samenhangt met uw garantie dat de toegang tot en het gebruik van DigiD niet verslechterd zullen worden, in het commissiedebat inzake digitale overheid op 22 maart 2022?³

Antwoord 8

Zoals verder toegelicht in de beantwoording op vraag 1 staat voorop dat SMS-authenticatie voorlopig behouden blijft, maar is het belangrijk dat er oog blijft voor continue verbetering van de beveiliging en de veiligheidseisen. Bij de verdere ontwikkeling van de app is voortdurend aandacht voor inclusiviteit, toegankelijkheid en het gebruikersgemak. Mensen kunnen ondersteuning vragen via de Helpdesk van DigiD en via Informatiepunten Digitale Overheid, bijvoorbeeld in bibliotheken. In de voortgangsrapportage van het domein Toegang zal ik dit najaar verder ingaan op de veiligheidsniveaus en inclusie.

³ <https://www.tweedekamer.nl/kamerstukken/detail?id=2021Z02985&did=2022D11752>.