

Vergaderjaar 2023–2024

25 764

Reisdocumenten

Nr. 149

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 1 juli 2024

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de staatssecretarissen van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties over de brief van 10 januari 2024 over Start uitvoering Digital Travel Credential (DTC) pilot (Kamerstuk 25 764, nr. 145).

De vragen en opmerkingen zijn op 18 april 2024 aan de staatssecretarissen van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties voorgelegd. Bij brief van 1 juli 2024 zijn de vragen beantwoord.

De fungerend voorzitter van de commissie,
Kathmann

De adjunct-griffier van de commissie,
Boeve

Inhoudsopgave

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersonen	2
Vragen en opmerkingen van de leden van de PVV-fractie	2
Vragen en opmerkingen van de leden van de PvdA-GroenLinks-fractie	6
Vragen en opmerkingen van de leden van de VVD-fractie	8
Vragen en opmerkingen van het lid van de NSC-fractie	8
Vragen en opmerkingen van het lid van de BBB-fractie	10

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersonen

Allereerst wil ik de leden hartelijk danken voor hun inbreng. Op verzoek van de Europese Commissie heeft Nederland een pilot uitgevoerd met als doel de Digital Travel Credential (DTC) te testen, waarmee processen op en rond de grens effectiever en efficiënter uitgevoerd kunnen worden. Nederland heeft hiermee als eerste land ter wereld een DTC-pilot uitgevoerd waarbij reizigers thuis een DTC konden aanmaken en gebruiken voor het boarding- en grensproces op een intercontinentale route (tussen Canada en Nederland). Er is dan ook veel internationale aandacht geweest voor de pilot. De Europese Commissie zal later dit jaar een voorstel doen inzake een DTC-verordening. Met het uitvoeren van de pilot heeft Nederland veel kennis en ervaring opgedaan die van waarde zijn voor deze aanstaande verordening. De vragen die de Commissie Digitale Zaken heeft gesteld dragen hier verder aan bij. De evaluatie van de resultaten en inzichten was tevens onderdeel van de pilot en is gedeeld met de Europese Commissie. Het evaluatie-rapport is ook voor u bijgesloten bij de beantwoording van de vragen.

Vragen en opmerkingen van de leden van de PVV-fractie

De leden van de PVV-fractie bedanken de Staatssecretaris voor de brief van 10 januari 2024 inzake de Nederlandse deelname aan een Europese pilot met een digitaal reisdocument. Naar aanleiding hiervan hebben deze leden nog enkele vragen.

De leden van de PVV-fractie lezen in de brief dat pilotdeelnemers zelf een Digital Travel Credential (DTC) creëren door de chip van het paspoort via een speciaal ontwikkelde applicatie op de smartphone uit te lezen. Tevens worden pilotdeelnemers gevraagd een gezichtsportret (selfie) te maken. Deze leden zouden graag vernemen in hoeverre geborgd kan worden dat het gebruik van een foto niet kan leiden tot een vals-positieve uitslag.

De leden van de PvdA-GroenLinks-fractie of er tijdens de pilot ook rekening wordt gehouden met het risico op false positives en negatives. Kan de bewindspersoon aangeven of hier reeds ervaringen mee zijn die gedeeld kunnen worden? Of anders betrokken kunnen worden in de evaluatie?

De leden van de NSC-fractie vragen welke methoden er worden gebruikt om de gezichten van DTC-houders (via selfies) te vergelijken met die in het paspoort. Wordt het AI-model bijvoorbeeld achter het DTC nog actief getraind op foto's van reizigers? Wordt ook rekening gehouden met mogelijke bias van dergelijke fotoverificatie? Is deze fotoverificatie tevens robuust bestendig tegen identiteitsfraude, zoals foto's van foto's of deepfakes? Tot slot vragen deze leden waar reizigers terecht kunnen als de

applicatie hen onterecht niet kan identificeren of hen onterecht verkeerd identificeert.

Ten derde zijn de leden van de PvdA-GroenLinks-fractie benieuwd naar de momenten waarop het nieuwe DTC niet goed werkt. Zo zijn er meerdere voorbeelden uit het recente verleden waarbij gezichtsherkenningstechnologie aantoonbaar slechter werkt bij mensen met een donkere huidskleur (ook wel «dark-skin-bias» genoemd). Kan de bewindspersoon aangeven of er bij deze pilot rekening wordt gehouden met dit probleem en vergelijkbare problemen waarbij gezichtsherkenningstechnologie een onbewuste bias heeft ten aanzien van specifieke groepen personen?

De leden van de BBB-fractie lezen dat met een DTC verschillende gegevens uit de paspoortchip worden gedeeld. Kan nader worden toegelicht om welke gegevens het hier gaat? Om het risico op look-a-like te voorkomen is een controle van het bijbehorende geldige, fysieke, paspoort vereist.

Ten tweede zijn de leden van de PvdA-GroenLinks-fractie verrast om te lezen dat voor reizigers met een Nederlands paspoort dat is uitgegeven na 30 augustus 2021 het BSN niet wordt gedeeld in een DTC, waarbij voor reizigers met een Nederlands paspoort dat is uitgegeven voor 30 augustus 2021 dat wel het geval is. De leden concluderen hieruit dat het delen van een BSN niet noodzakelijk is voor een DTC. Kan de Staatssecretaris hierop reflecteren? Kan de Staatssecretaris aangeven of het technisch mogelijk is om voor reizigers van wie het paspoort voor 30 augustus 2021 is uitgegeven het BSN niet te delen in een DTC? Indien dat mogelijk is, kan de Staatssecretaris aangeven waarom daar niet voor gekozen is? Indien dat niet mogelijk is, kan de Staatssecretaris aangeven waar de moeilijkheden precies in zitten?

Antwoord:

In de pilot is bij het aanmaken van de DTC gezichtsvergelijking gebruikt om te voorkomen dat een DTC wordt aangemaakt en verstuurd met het reisdocument van een ander persoon. Zulke systemen zijn nooit perfect, evenals overigens manuele controles dat niet zijn. Het gebruik van zulke systemen brengt niet per se meer of minder risico's met zich mee dan manuele controles.

Beide methoden hebben hun beperkingen en kunnen leiden tot fouten in de vorm van vals positieven (foutieve goedkeuringen) en vals negatieven (foutieve afwijzingen). Een vals positief houdt in dat een persoon ten onrechte wordt goedgekeurd als de rechtmatige houder van een document, terwijl een vals negatief betekent dat een rechtmatige houder ten onrechte wordt afgewezen. Welke het meest nadelig is, hangt af van de toepassing en context van gezichtsvergelijking.

Gezichtsvergelijking gebeurt met vergelijkingssoftware. Deze maakt gebruik van drempelwaarden waarbij een systeem strenger of minder streng kan worden ingesteld. Hoe strenger een systeem, hoe minder vals positieven en hoe meer vals negatieven. De mate waarin een systeem foutgevoelig is, neemt met doorontwikkelingen verder af. Binnen de pilot is gebruik gemaakt van een modern, hoogwaardig algoritme. Daarbij zijn anti-fraude technologieën zoals *liveness detection*, toegepast om te voorkomen dat vervalsingen of manipulaties van foto's worden geaccepteerd, zoals deepfakes.

Look-a-like fraude is een voorbeeld van een vals positief. Het maakt daarbij niet uit op basis van welk type document dit oordeel gebaseerd is en of het een digitaal of fysiek document betreft. Het gaat immers om de vergelijking tussen een persoon en een gezichtsopname. Geautomati-

seerde gezichtsvergelijking heeft met de juiste drempelwaarde een zeer grote nauwkeurigheid bij het detecteren van fouten, waaronder vals positieven resultaten. In het geval van een vals positief is er toezicht bij de DTC-gate door een grenswachter. Een vals positief zal er toe leiden dat iemand meedoet aan de pilot met een document waarvan deze niet de houder is. Binnen de pilot leidde een vals negatief ertoe dat iemand geen DTC kan aanmaken en niet mee kon doen met de pilot en via het reguliere grensproces moest reizen.

In het geval van non-matches is belangrijk om aan te geven dat, deze in de meeste gevallen terecht waren. Een non-match houdt in dat een persoon probeert namens een andere persoon te handelen en een DTC probeert aan te maken met een document waarvan hij geen documenthouder is.

Als een systeem een bias kent, is de balans tussen vals positieve en negatieve matches anders voor mensen met specifieke eigenschappen. Ook hier geldt dat het afhankelijk is van de toepassing en context of dit voordelig of nadelig is voor de persoon die het betreft. Het spreekt voor zich dat een bias in alle gevallen onwenselijk is. Systemen en algoritmen worden daarop actief ontwikkeld en getest. In onafhankelijk NIST-onderzoek¹, gebaseerd op wetenschappelijke principes, is aangetoond dat de software gebruikt in de pilot hoog scoort in zowel de afwezigheid van een bias, als de performance over het geheel. Verder ben ik in antwoorden op eerdere vragen van de Commissie voor Digitale Zaken specifiek ingegaan op vragen over bias in de pilot².

De technische DTC-standaard is vastgesteld door ICAO (de internationale burgerluchtvaartorganisatie). Deze is gebaseerd op de data van de chip van het paspoort. Voor alle landen die een paspoort uitgeven met een chip is het verplicht om de Machine Readable Zone (MRZ), foto en een *secure object* (beveiligd object) te personaliseren op de chip. Voor de pilot werd de informatie in de MRZ en het secure object verzonden. Het secure object betreft de digitale echtheidskenmerken waarmee de integriteit en authenticiteit van de gegevens gecontroleerd kunnen worden. De MRZ betreft de gegevens die onderaan het paspoort staan. Deze is gebaseerd op een internationale standaard die het mogelijk maakt overal ter wereld paspoortgegevens op een gelijkvormige wijze uit te lezen.

De MRZ bevat achternaam, voornaam, geboortedatum, nationaliteit, geslacht, documentnummer, land van uitgifte en geldigheidsdatum document. In het Nederlandse paspoort uitgegeven voor 30 augustus 2021 staat ook het Burgerservicenummer (BSN) in de MRZ. Nederland heeft ooit de keuze gemaakt het BSN te verwerken in de MRZ, om geautomatiseerd uitlezen door Nederlandse organisaties mogelijk te maken. Sinds 30 augustus 2021 staat het BSN alleen nog op de achterkant van de houderpagina in het document. Hoewel het BSN in de pilot geen functie heeft, is het niet mogelijk om het BSN na het uitlezen van de MRZ te verwijderen uit de DTC. Er is namelijk een digitale handtekening geplaatst over de MRZ welke een onderdeel is van de digitale echtheidskenmerken. Indien het BSN uit de DTC wordt verwijderd, verbreekt men dit echtheidskenmerk en kan niet langer worden gevalideerd of het een integer en authentiek document betreft. Het is dus technisch niet mogelijk voor reizigers van wie het paspoort voor 30 augustus 2021 is uitgegeven het BSN niet te delen in een DTC.

¹ De onafhankelijke National Institute of Standards and Technology (NIST) toetst gezichtsherkenningsoftware op nauwkeurigheid en rechtvaardigheid.

² VSO inzake de brief deelname Nederland aan een Europese pilot met een digitaal reisdocument, 13 juli 2023 (Kamerstuk 25 764, nr. 143).

De leden van de PVV-fractie lezen dat met een DTC-controle voorafgaande de grenspassage kan worden uitgevoerd. Pilotdeelnemers kunnen bij aankomst naar een «tap & go» poortje, waar een foto van de reiziger gemaakt wordt die vergeleken wordt met de foto uit de paspoortchip. Deze leden willen graag weten of dit de standaardroutine wordt, of dat «kunnen» inhoudt dat de tap & go steekproefsgewijs wordt ingezet.

Antwoord:

Tijdens de DTC-pilot konden deelnemers bij aankomst op Schiphol de grens middels een tap & go-poort passeren in plaats van via de manuele balie of de e-gates. Het tap & go-proces werd niet steekproefsgewijs ingezet, maar vormde het alternatieve grensproces specifiek voor DTC-pilotdeelnemers. Het woord «kunnen» moet dan ook gelezen worden als vrijwillige keuze tussen manuele en geautomatiseerde controle. Voor alle reizigers van buiten Schengen, inclusief DTC-deelnemers, worden bij het passeren van de grens controles uitgevoerd. Bij DTC-pilotdeelnemers waren de grenscontroles grotendeels al uitgevoerd voordat zij bij de grens arriveerden, waardoor zij de grens konden passeren via de tap & go-poort in plaats van de manuele balie.

Tot slot willen de leden van de PVV-fractie graag van de Staatssecretaris vernemen in hoeverre paspoortchips veilig zijn wanneer fysieke controles gereduceerd worden of zelfs verdwijnen en deze aan het systeem worden overgelaten. Op welke wijze kan de Staatssecretaris garanderen dat voorkomen wordt dat een potentieel kwaadwillend persoon die, door het ontbreken van een fysieke controle, door kan lopen op basis van een vals-positieve DTC en een gekraakte paspoortchip?

Antwoord:

De Schengengrenscodes dient als kader voor het uitvoeren van de paspoortcontroles en de toegang tot het Schengengebied. Het verifiëren van de identiteit is hierbij een belangrijk onderdeel. Aan de manuele balie wordt dit visueel gedaan door de grenswachter. Net zoals aan de geautomatiseerde grenscontrolepoortjes (e-gates) is bij de DTC-pilot geautomatiseerd vastgesteld of de documenthouder en de persoon die het aanbiedt overeenstemmen.

Geautomatiseerde grenscontroles zijn bijzonder effectief in het nauwkeurig vaststellen van biometrische overeenkomsten en daarmee het detecteren van frauduleuze documenten en identiteitsvervalsing. De aanpak met minder visuele controles door grenswachten en meer geautomatiseerde controles is hiermee niet onveilig. Door de combinatie van geautomatiseerde vergelijkingen, chipcontroles, fysieke documentcontroles en menselijk toezicht worden risico's door kwaadwillende personen geminimaliseerd.

In de DTC-pilot was het fysieke document nog altijd nodig voor de grenscontrole. Hiermee wordt gecontroleerd of de chip in het paspoort gekopieerd is en of deze integer en authentiek is. Deze validatie vindt ook plaats bij de e-gates. Alleen bij een juiste combinatie van reiziger, paspoort en DTC kon de grens gepasseerd worden.

Voor wat betreft de casus met betrekking tot ontbrekende fysieke controle wijs ik erop dat Nederland hoge eisen stelt aan de beveiliging van documenten die worden toegestaan voor het gebruik van de e-gates en geautomatiseerde controles.

De veiligheid van paspoortchips is een topprioriteit. Deze paspoortchips worden ontwikkeld en geproduceerd volgens strenge internationale en nationale normen, waardoor ze bestand zijn tegen diverse bedreigingen op het gebied van cyberveiligheid. Bovendien worden geavanceerde

technologieën ingezet voor het detecteren van vervalsingen en manipulaties van paspoortchips, waardoor de integriteit van het systeem wordt gehandhaafd. De DTC-pilot was mogelijk dankzij deze veiligheidsnormen.

Vragen en opmerkingen van de leden van de PvdA-GroenLinks-fractie

De leden van de PvdA-GroenLinks-fractie hebben met veel interesse kennisgenomen van de plannen rondom het Digital Travel Credential (DTC) pilot. Wel hebben deze leden nog enkele vragen en opmerkingen.

Nederlandse DTC pilot

Ten eerste vragen de leden van de PvdA-GroenLinks-fractie welke besturingssystemen geschikt zijn voor de DTC-pilot. Kan de Staatssecretaris aangeven of dit de gangbare iOS en Android systemen betreft? Is er een keuze gemaakt om tijdens de pilot de DTC ook op andere besturingssystemen, zoals Sailfish OS, te testen?

En in het kader van digitale ongelijkheid; kan de Staatssecretaris aangeven welke garanties er zijn op de beschikbaarheid van de DTC voor verouderde apparaten? Welke minimumvereisten zijn er? Kan hierbij rekening worden gehouden met een zo breed mogelijke beschikbaarheid, zodat het hebben van een nieuw apparaat geen rol speelt in het wel of niet kunnen gebruiken «

Antwoord:

Het doel van de pilot was om het concept van de DTC in het grensproces te beproeven. Zodoende was de pilot toegankelijk voor een selecte doelgroep: houders van een Nederlands, Belgisch of Canadees paspoort van 18 jaar en ouder met een rechtstreekse KLM-vlucht van Canada naar Nederland. Gezien deze beperkte scope en doelgroep, en beperkte financiële middelen, is besloten om de applicatie enkel beschikbaar te stellen voor de meest gangbare besturingssystemen, namelijk iOS en Android.

Ten tweede zijn de leden van de PvdA-GroenLinks-fractie benieuwd wat de gevolgen zijn voor reizigers die geen gebruik kunnen of willen maken van DTC. Kan de Staatssecretaris hierop reflecteren? Hoeveel meer tijd gaat het reizigers kosten die geen gebruik maken van DTC en hoe apprecieert de bewindspersoon dit verschil in reisgemak? En hierop aansluitend: is het risico op «function creep» voldoende afgebakend? Hoe wordt voorkomen dat bij verdere inzet van de DTC de reikwijdte van het gebruik niet te veel uitbreidt of mensen indirect druk ervaren om van het systeem gebruik te maken?

De leden van de BBB vragen of de controle bij de grens of bij het inchecken echt veel sneller dan wel veiliger wordt. Is er vanuit de pilot reeds bekend wat de tijdswinst en de winst qua efficiëntie is?

Antwoord:

Reizigers die geen gebruik wensten te maken van DTC konden de grens passeren middels het reguliere proces en gebruik maken van de geautomatiseerde grenspassage of de manuele balie. Dit proces werd niet anders of langduriger door de pilot.

Het DTC-concept, waarbij een reiziger voorafgaand aan diens reis gegevens stuurt, is er op gericht grensprozessen doelgerichter en efficiënter te laten verlopen. Dit is mogelijk door een verdere doorontwikkeling van het reisdocument. De eerdere stappen waren het internationaal

standaardiseren van de verschijningsvorm, het toevoegen van de MRZ en het toevoegen van een chip.

Al deze stappen hebben het eenvoudiger gemaakt om documenten te controleren op echtheid en te koppelen aan de rechtmatig houder. De DTC kan als vervolgstap gezien worden. Een stap die, gezien het mondiaal toenemen van reizigersaantallen, druk op de arbeidsmarkt en verwachtingen van reizigers ook nodig is. In Nederland, maar ook daarbuiten. De DTC kan de verwerkingstijd per reiziger aan de grens doen afnemen. De druk op personeel neemt daardoor af en dat zal in rijvorming te merken zijn. Echter, hoe zich dit uit in reizigersgemak is nu moeilijk te bepalen, omdat dit mede afhangt van de verordening en de wijze van implementatie aan grenzen.

Uit de resultaten van de pilot blijkt dat er bij grenspassage een tijdswinst is bij het gebruik van DTC ten opzichte van het reguliere uitlezen van de paspoortchip en het bevragen van de registers aan de grens. Hierbij moet wel opgemerkt worden dat pilot-deelnemers voorafgaand aan hun reis enige tijd hebben moeten besteden aan het aanmaken en delen van DTC.

Function-creep is een punt van aandacht bij het scheppen van het juridisch kader. Het functioneren van het paspoort is duidelijk juridisch ingebed. Daar geldt dat een houder zelf verantwoordelijk is voor het al dan niet delen van diens document. Op dit punt zullen we afwachten hoe de conceptverordening de DTC juridisch zal duiden.

Privacy en wetgeving

De leden van de PvdA-GroenLinks-fractie willen /allereerst de bewindspersoon bedanken voor de uitgebreide focus op privacy en wetgeving. De leden hebben hier een aantal aanvullende vragen over.

Ten eerste zijn de leden benieuwd naar de manier waarop reizigers ondubbelzinnig en specifiek geïnformeerd worden over de inhoud en de aspecten van de pilot. Kan de bewindspersoon deze tekst delen? Kan de Staatssecretaris hierbij ook aangeven waarom bepaalde keuzes wel of niet gemaakt zijn bij het opstellen van deze informatietekst?

Vragen van de BBB. Gebruikmakers kunnen hun DTC delen met de overheid en de luchtvaartmaatschappij. Hoe wordt het aan gebruikers kenbaar gemaakt dat de Algemene Verordening Gegevensbescherming (AVG) van toepassing is en hoe worden zij geïnformeerd over hun rechten met betrekking tot de verwerking van hun persoonsgegevens?

Antwoord:

In de uitnodigingsmail zijn potentiële pilotdeelnemers verwezen naar de online informatievoorziening waar het privacy statement is opgenomen³. In de applicatie zijn de belangrijkste privacy gerelateerde zaken weergegeven zoals de betrokken partijen, de te verwerken persoonsgegevens en bewaartermijn, en is nogmaals een link naar het online privacy statement opgenomen. Na het zien van deze informatie is aan deelnemers gevraagd om expliciete toestemming voor deelname en de verwerking van hun persoonsgegevens door middel van een door hen aan te vinken toestemmingsverklaring.

In zowel de applicatie als in het statement is vermeld dat de AVG op de gegevensverwerkingen binnen de pilot van toepassing was. In het statement is ook uitgelegd hoe deelnemers gebruik konden maken van

³ <https://www.rijksoverheid.nl/documenten/publicaties/2023/02/23/nederlandse-deelname-aan-europese-dtc-pilot>

rechten als inzage, correctie, verwijdering en het intrekken van hun toestemming. Daarbij is ook uitgelegd dat deelnemers op elk moment zonder negatief gevolg hun deelname konden beëindigen en op reguliere wijze konden boarden en/of de grenscontrole ondergaan. Door de bij de pilot betrokken partijen is een centraal contactpunt gecreëerd waar betrokkenen terecht konden met hun beroepen op hun rechten en overige vragen. In het privacy statement zijn ten slotte ook de contactgegevens van de Autoriteit Persoonsgegevens (AP) opgenomen met vermelding dat men daar terecht kan voor de uitoefening van hun rechten en overige vragen.

De leden van PvdA-GroenLinks zijn voorts blij om te lezen dat de DTC versleuteld wordt opgeslagen op het eigen apparaat. Tegelijk lezen deze leden ook dat de DTC aan een specifiek voor de pilot ontwikkeld opslagsysteem wordt verstuurd. Kan de Staatssecretaris aangeven of de DTC op dit opslagsysteem eveneens versleuteld wordt opgeslagen? Bevindt dit systeem zich in de EU en is de leverancier van het systeem een Europese organisatie? Kan de Staatssecretaris aangeven welke maatregelen er zijn genomen om te voorkomen dat onbevoegde actoren mogelijk toegang kunnen krijgen tot dit systeem?

Kan de Staatssecretaris aangeven of de gegevens die op dit opslagsysteem staan na gebruik niet alleen gewist, maar ook overschreven worden met andere data zodat het niet mogelijk is om deze gegevens terug te halen?

Antwoord:

De gebruikte software en hardware is binnen Europa ontwikkeld door een Europese organisatie. Daarbij geldt «privacy en security by design» als ontwerpprincipe. De DTC-gegevens worden zowel op het apparaat van de reiziger als op het voor de pilot ontwikkelde opslagsysteem versleuteld opgeslagen.

Het in de pilot gebruikte systeem en de leverancier zijn getoetst volgens het Defensie Beveiligings Beleid (DBB) waarbij voldaan moet worden aan strenge eisen inzake cybersecurity.

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben kennisgenomen van de brief Start uitvoering Digital Travel Credential. Zij hebben daarover geen verdere vragen of opmerkingen.

Vragen en opmerkingen van de leden van de NSC-fractie

De leden van de NSC-fractie hebben kennisgenomen van de pilot. Daarbij hebben zij nog enkele vragen aan de Minister.

Nederlandse DTC-pilot

De leden van de NSC-fractie constateren dat de opzet van de DTC zeer vergelijkbaar is met de Europese digitale identiteit. Deze leden vragen daarom of het DTC een volledig separaat traject is ten opzichte van de Europese identiteitswallets en of er ambities zijn om op termijn deze initiatieven samen te voegen.

Antwoord:

DTC en het Europese Raamwerk voor Digitale Identiteit (EDI) zijn separate trajecten die elkaar kunnen aanvullen. De samenhang tussen deze trajecten wordt daarom zowel op Europees als nationaal niveau in de gaten gehouden. Onder het Europese Raamwerk voor Digitale Identiteit

krijgen burgers en bedrijven die dat willen beschikking over een nationaal uitgegeven of erkende EDI-wallet. Zij kunnen daarmee onder andere inloggen, persoonlijke gegevens delen en elektronisch ondertekenen. Het Europese raamwerk vereist dat EDI-wallets in de hele Europese Unie gebruikt kunnen worden. Zo wordt onder meer gewerkt aan het kunnen openen van een bankrekening en het tonen van een digitaal rijbewijs, diploma's en andere persoonlijke of professionele kwalificaties. DTC is ontwikkeld in de context van de burgerluchtvaart en uitsluitend bedoeld om reizen en reisprocessen te ondersteunen, bijvoorbeeld om efficiënter en gemakkelijker grenzen over te kunnen steken. De DTC is een mondiale ontwikkeling, die ook moet kunnen werken buiten Europa. Bovendien moet DTC rekening houden met de standaarden en systemen van bestaande grensovergangen. Het is niet ondenkbaar dat in een later stadium de DTC ook opgeslagen wordt in een EDI-wallet.

De leden van de NSC-fractie lezen dat de Autoriteit Persoonsgegevens betrokken is bij de pilot DTC. Deze leden vragen of de Autoriteit Persoonsgegevens op voorhand al aandachtspunten heeft aangegeven bij de uitrol van het DTC.

Antwoord:

De AP heeft op voorhand aandachtspunten meegegeven voor de DTC-pilot, die volgens de AP door de partijen konden worden opgevat als preventieve guidance. Voorafgaand daaraan was reeds een Data Protection Impact Assessment (DPIA) uitgevoerd. Met de specifieke aandachtspunten van de AP is deze DPIA nog eens bijgewerkt en zijn waar nodig mitigerende acties getroffen. Op basis daarvan hebben de verwerkingsverantwoordelijke partijen geconcludeerd dat geen sprake was van gemiddelde of hoge restrisico's die doorgang van de pilot in de weg zouden staan. Het evaluatierapport van de pilot is tevens met de AP gedeeld. Zij is voornemens een *sideletter* te publiceren inzake de bescherming van persoonsgegevens en privacyrechten bij het gebruik van DTC in het reisproces en vastlegging daarvan in aanstaande wetgeving.

De leden van de NSC-fractie lezen dat een DTC niet langer wordt bewaard dan noodzakelijk, maar deze leden vragen of de gedeelde biometrische gegevens nog via een ander kanaal elders opgeslagen kunnen worden, bijvoorbeeld voor opsporings- of inlichtingendoeleinden.

Antwoord:

De DTC en de biometrische gegevens worden niet langer dan noodzakelijk bewaard en ook niet elders opgeslagen voor andere doeleinden. De DTC die een reiziger deelt met de Koninklijke Marechaussee wordt alleen gebruikt voor het uitvoeren van de grenscontroles en het passeren van de grens.

De leden van de NSC-fractie vragen hoe eenvoudig een DTC is te hacken of te «spoofen». Heeft de Staatssecretaris daarnaast een «red team» het DTC al eens laten aanvallen?

De leden van de NSC-fractie vragen in welke mate de «travel credential wallets», welke zeer gevoelige persoonsgegevens bevatten, vatbaar zijn voor «store now, decrypt later»-aanvallen middels een kwantumcomputer. Zo ja, dan vragen deze leden welke voorbereidingen de staatsecretaris heeft getroffen om de wallets op termijn quantumveilig te maken.

Antwoord:

Wat betreft het hacken of «spoofen» van een DTC is het belangrijk op te merken dat een DTC een extractie is van de data van de chip van het paspoort. De digitale echtheidskenmerken die de integriteit van de data en

de authenticiteit waarborgen blijven intact bij een DTC. Hierdoor zijn de beveiligingsmaatregelen die van toepassing zijn op de informatie in de chip van het paspoort ook van toepassing op de DTC. Bovendien wordt wereldwijd samengewerkt door verschillende organisaties om eventuele inbreuken op de integriteit van paspoorten te signaleren en hierop adequaat te reageren.

Het risico van quantumcomputing bestaat voor de DTC evenzogoed als voor paspoorten en identiteitsdocumenten die een chip bevatten. De kerngedachte is dat quantumcomputers een gevaar vormen voor cryptografie, omdat zij deze in korte tijd kunnen kraken. De chips van paspoorten ontlenen hun betrouwbaarheid aan cryptografie. Mede om die reden is het van groot belang dat paspoorten en andere identiteitsdocumenten een beperkte geldigheid kennen. Daarmee kan voorkomen worden dat op een later moment, op grote schaal, misbruik gemaakt wordt van eerder verkregen gegevens. Hoe korter de geldigheid van het document, hoe beter het beschermd is tegen dit risico. De geldigheid van de DTC is nooit langer dan de geldigheid van het document, waarop het gebaseerd is. Het risico van quantumcomputing voor paspoortchips is bekend. In ICAO-verband wordt samengewerkt met de International Organization for Standardization om afspraken te maken over de gebruikte cryptografie in de paspoorten. Door het wereldwijde gebruik van het paspoort is het noodzakelijk dat dit internationaal wordt opgepakt.

Vragen en opmerkingen van de leden van de BBB-fractie

De leden van de BBB-fractie hebben kennisgenomen van de nota Start uitvoering Digital Travel Credential (DTC). De leden hebben vragen en opmerkingen over de nota.

De eerste vraag die de leden van de BBB-fractie hebben is in hoeverre het DTC-concept afwijkt van (bijvoorbeeld) de reeds in gebruik zijnde eGates-systematiek op Schiphol. Graag ontvangen deze leden een korte uiteenzetting over de verschillen tussen de systemen.

Antwoord:

Deze twee processen zijn grotendeels gelijk. Zowel bij de geautomatiseerde grenscontrole (e-gates) als de tap & go DTC poort wordt gebruik gemaakt van geautomatiseerde gezichtsvergelijking, voor de reiziger de grens mag passeren. Echter, het moment *waarop* de inreiscontroles in de e-gates en tap & go worden uitgevoerd verschilt. Bij de e-gates worden bepaalde reguliere grensprocessen pas op de grens zelf uitgevoerd. Het gaat hierbij om het uitlezen van het paspoort, waaronder de chip en het bevragen van de registers⁴. Ook wordt pas in de e-gate de documenthouder vergeleken met de foto in de paspoortchip.

Met een DTC kunnen de controles behorend bij het grensproces, al grotendeels uitgevoerd worden voordat de reiziger aan de grens verschijnt. Aanvullend hoeft op de grens de paspoortchip niet volledig uitgelezen te worden, aangezien dit reeds gedaan is bij het aanmaken en ontvangen van de DTC. In de DTC zit ook het gezichtsportret dat op de chip van het paspoort staat. Op de grens wordt de reiziger gematcht met de foto die met de DTC klaar staat in de gallery op de tap & go-poort. Het paspoort hoeft daardoor niet meer geopend te worden en kan gesloten tegen de grenspoort getapt worden, zodat wordt gecontroleerd dat de DTC toebehoort aan de houder van het reisdocument. Op basis van de

⁴ Conform de Schengengrenscore worden relevante registers gecontroleerd of de persoon gezocht wordt, en of de persoon voldoet aan de vereisten voor toegang tot het Schengen-gebied.

uitkomsten van de DTC-pilot is gebleken dat het DTC proces op de grens sneller is dan het proces in de e-gates.

Gebruikmakers van het DTC moeten nog altijd een fysiek paspoort bij zich dragen en voornamelijk is het DTC geen vervanger van het paspoort. Een verplichte digitale identiteit die het bestaande paspoort of identiteitsbewijs vervangt en gekoppeld is aan een vergaande persoonsdigitalisering is voor de leden van de BBB-fractie onwenselijk en gevaarlijk voor de vrijheid van het individu. Is er een scenario waarin het DTC het gebruik van het fysieke paspoort wel volledig vervangt?

Antwoord:

Een DTC en een digitale identiteit zijn niet hetzelfde. Voor een uitgebreide toelichting hierover verwijs ik u naar de vraag van NSC over de verhouding van digitale Europese identiteit en de DTC.

De Europese Commissie komt naar verwachting dit jaar met een verordening inzake een digitaal reisdocument en het faciliteren van reizigers. Het gaat daarbij om het overschrijden van de Europese buitengrenzen. De Commissie heeft aangegeven waarschijnlijk voor te stellen dat gebruik van de DTC ter overschrijding van de Europese buitengrenzen op vrijwillige basis zal zijn. Net zoals het gebruik van geautomatiseerde grenspassage ook op vrijwillige basis is.

Het vervangen van het paspoort met een DTC is momenteel niet aan de orde. Het is denkbaar dat op termijn op specifieke bestemmingen een reis zonder fysiek reisdocument mogelijk wordt, voor reizigers die dit wensen. Dat hangt onder andere af van wetgeving, standaardisering en technische en operationele mogelijkheden van landen. Net zoals nu reeds het geval is. Echter zullen er ook altijd landen zijn die dat niet kunnen faciliteren. Zo zijn er bijvoorbeeld landen die een paspoort zonder chip uitgeven en ook landen die geen gebruik maken van geautomatiseerde grenscontroles.

Een van de krachten van een fysiek paspoort is dat de overheid het uitgifteproces strak onder controle heeft. De leden van de BBB-fractie vragen in hoeverre dit ook geldt voor een digitaal reisdocument dat draait als een app op de smartphone. Kan dit nader worden toegelicht?

Antwoord:

Het is van groot belang dat de overheid garant staat voor de integriteit en authenticiteit van reisdocumenten. De verschijningsvorm staat hier los van. Zodoende moet voor de uitgifte van het reisdocument altijd een fysiek verschijningsmoment blijven, waarbij de overheid garant staat voor de integriteit van de opgenomen gegevens en de koppeling met de afgegeven biometrie. Dit kan ook als het een digitaal middel betreft. Binnen de pilot werd gebruik gemaakt van DTC-type 1 bestaande uit twee componenten: het fysieke document en de virtuele component⁵. Het fysieke document is tot stand gekomen tijdens aanvraagproces zoals beschreven in de Paspoortwet. De virtuele component is op basis van het uitlezen van de paspoortchip, waarbij ook de digitale echtheidskenmerken meegenomen worden. Alle waarborgen rondom de uitgifte van het paspoort zijn hierdoor van toepassing.

⁵ ICAO werkt aan de ontwikkeling van technische DTC-standaarden. DTC-type 1 is de enige versie waarvan de standaardisatie is vastgesteld binnen ICAO. DTC 2 en 3 zijn in ontwikkeling. Dit betreft de verschijningsvorm van een fysiek component. Het uitgangspunt van DTC 2 en DTC 3 is dat de overheid de DTC creëert op de mobiele telefoon. Met een DTC 2 kan zowel het paspoort of de telefoon gebruikt worden. Met een DTC 3 zou het theoretisch mogelijk zijn om het paspoort te vervangen met DTC.

De DTC-pilot geldt als voorbereiding op Europese wetgeving. De leden van deze fractie vragen een nadere toelichting over het traject naar de voorgenomen DTC verordening.

Antwoord:

De Europese Commissie komt naar verwachting dit jaar met een voorstel inzake een digitaal reisdocument en het faciliteren van reizigers. De Kamer wordt geïnformeerd middels een BNC-fiche over het standpunt ten aanzien van deze conceptverordening.