Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan	Staatssecretaris van BZK
Van	CZW

Binnenlandse Zaken en Koninkrijksrelaties
Const tut onele Zaken en Wetgeving

Contactpersoon

T

Datum
2 oktober 2019

Kenmerk
2019-0000521643

nota

Juridische knelpunten KTDI

Aanleiding

Op 1 juli heeft dhr. Middendorp (VVD) Kamervragen aan u gesteld over twee artikelen in het Financieel Dagblad van 1 juli: 'Overheid lanceert digitaal paspoort' en "We maken het paspoort Trump- en Poetin-proof'. Deze zijn dd 25 sept. door u beantwoord.

Voorts hebben op 10 juli de leden Den Boer en Verhoeven (D66) vragen gesteld aan de staatssecretaris van J&V over het bericht 'Canada en Nederland testen trans-Atlantische vluchten zonder paspoort'. Deze vragen gaan over het "Known Traveller Digital Identity (KTDI)" concept en raken aan andere pilots met verschillende vormen van virtuele of digitale identiteiten.
De concept-beantwoording is door J&V ambtelijk aan BZK voorgelegd.

In deze nota wordt u geïnformeerd over de politieke en juridische risico's die de beoogde KTDI-pilot met rechtsgevolgen met zich zou brengen.

- Een pilot waarbij sprake is van uitgifte van een digitale identiteit is niet rechtmatig. Daarvoor is randvoorwaardelijk - indien noodzaak en wenselijkheid komen vast te staan - dat de Paspoortwet wordt aangepast. RvIG is het niet met deze zienswijze eens.

- De CIO adviseert om de innovatieve en complexe KTDI-pilot te beperken tot een technische pilot, die enerzijds alle onrechtmatigheidsrisico's en privacyrisico's afdoende mitigeert en anderzijds antwoorden op vragen rondom datagebruik, privacy en impact op bestaande systemen in kaart brengt.

Advies

- Kennisnemen van deze nota, waarin de KTDI-pilots worden beoordeeld vanuit juridisch perspectief;
- Kennisnemen van het CIO-voorstel om de KTDI-pilot te beperken tot een technische pilot in een labomgeving. Het is aan DIO en RVIg om u te adviseren over de vraag, hoe met het CIO-advies om te gaan;
- Opvolging van het CIO-advies zou betekenen dat de beantwoording van J&V-vragen op onderdelen aanpassing behoeft. Dit brengt opnieuw afstemming met J&V met zich.

- Indien wordt overwogen over te gaan tot uitgifte van een digitaal paspoort/digitale identiteit moeten de nut en noodzaak, gevolgen en de wenselijkheid in kaart zijn gebracht, en in samenhang met andere (BZK) trajecten op het gebied van digitale identiteitsontwikkeling worden bezien. Dit is een meerjarig traject, waarbij stapsgewijs wordt gehandeld.
- Deelname aan pilots op uw beleidsterrein zouden aan u moeten worden voorgelegd, waarbij alle relevante aspecten en wegingsfactoren in kaart zijn gebracht. Onomkeerbare beslissingen moeten worden voorkomen.

Betrokken BZK onderdelen
CZW, DIO, RvIG, CIO

Toel chting
In het kader van innovatie werkt BZK aan een aantal verkennende trajecten in het identiteitsdomein. Hiertoe worden de maatschappelijke behoefte en de beleidsmatige, technische, organisatorische, juridische en financiële gevolgen in kaart gebracht, zodat kan worden besloten of voortgang van het traject wenselijk en haalbaar is. Een ervan heeft betrekking op KTDI.

Bij het KTDI- project zijn door Nederland en Canada voornemens tot deelname uitgesproken waarbij de KTDI-app gedurende zes maanden zal worden toegepast. Dit stuit echter op juridische en andere knelpunten. J&V is vanuit Nederland - om redenen van verantwoordelijkheid voor grenspassage/personenverkeer - de trekker van het project, maar het onderwerp ligt ook op uw terrein, omdat voor oa grenspassage een door de overheid uitgegeven en gevalideerd reisdocument wordt overwogen.

Wat is Known Traveller Digital Identity?
Het doel van KTDI is het vergemakkelijken van het hele vliegreisproces voor ‘bekende’ passagiers. Enerzijds zou KTDI de doorstroom op vliegvelden versoepelen, anderzijds ervaart de reiziger meer gemak, omdat hij zijn data in een keer ter beschikking stelt ten behoeve van verschillende stappen in zijn reis. Grenspassage is daar een van. Beoogd wordt KTDI vorm te geven in de zin, dat nadat de reiziger deelname aan KTDI heeft bevestigd, zijn paspoortgegevens worden omgezet in een digitale identiteit die wordt afgegeven en gecertificeerd door een overheidsinstantie (gedacht wordt aan de gemeente Haarlemmermeer/ Schipholbalie). Deze digitale identiteit komt op de mobiele telefoon van de reiziger en in de blockchain van de KTDI-software te staan. Vervolgens worden de noodzakelijke gegevens gedeeld met bijvoorbeeld de KMar (grenspassage) en vliegtuigmaatschappijen (boarding). In de toekomst zouden gegevens ook aan andere private partijen in de reisketen (oa hotels, autoverhuurbedrijven) doorgegeven kunnen worden. Bij de grenspassage wordt de deelnemer gecheckt d.m.v. gezichtsherkenning. Alle processtappen van de reiziger worden in de KTDI-blockchain vastgelegd, zodat de deelnemende partijen weten waar de reiziger zich in het proces bevindt.

Betrokken partijen en stand van zaken
Het concept komt uit de gezamenlijke koker van de ICAO (Internationale burgerluchtvaartorganisatie) en het World Economic Forum (WEF) en is gelanceerd op de jaarlijkse bijeenkomst van het WEF in Davos in 2018. Er is een publiek-privaat consortium ingericht, bestaande uit het WEF, Accenture (zakelijke dienstverlening m.b.t. ICT en technologie), Canadese autoriteiten, Air Canada, Toronto Pearson International Airport, Aéroports de Montréal, KLM Royal Dutch

Airlines en Schiphol Nederland B.V en het ministerie van J&V. Bij J&V is directie Migratiebeleid de trekker. Daarnaast zijn RvIG en de KMar nauw betrokken. De ontwikkeling van de benodigde software is gerealiseerd door Idemia, de producent van Nederlandse reisdocumenten. De app wordt ontwikkeld door Accenture.

Het project is ingericht met de intentie van deelname van alle partijen in pilots met KTDI in 2020. Deze intentie wilde men medio 2019 vastleggen in een Memorandum of Understanding (MoU). Ondertekening van het MoU is uitgesteld naar uiterlijk 30 november van dit jaar. Wel is op 26 juni een Letter of Intent (LoI) ondertekend (bijgevoegd). Deze is juridisch niet bindend. Voor NL heeft de Nederlandse ambassadeur in Canada getekend met mandaat van de Staatssecretaris van J&V.

Vormgeving pilot
Men wil, na een korte technische en operationele test, door een besloten doelgroep bestaande uit medewerkers van de betrokken partijen, medio 2020 gedurende een periode van 6 maanden een pilot uitvoeren met echte grenspassage. Ingezet wordt op een vorm, waarin 10.000 passagiers (waarvan 5.000 Nederlanders) door Air Canada en KLM uitgenodigd worden om deel te nemen aan de pilot tussen Schiphol en Montréal en Toronto, wiens paspoortgegevens na instemming en via afgifte van een digitale identiteit worden verstrekt aan de KTDI-blockchain. Dit zou opslag van deze gegevens (inclusief gezichtsopname) in verschillende (publieke en private) centrale systemen/databases betekenen. De geselecteerde reizigers passeren de grens zonder het tonen en uitlezen van hun paspoort.

Knelpunten
Geen juridische grondslag voor virtuele identiteit/reisdocument
De beoogde KTDI- pilot heeft, na de technische/operationele test, rechtsgevolgen; in de tweede fase gaat het om het bij wijze van experiment uitvoeren van rechtshandelingen. De beoogde vorm, dus middels de uitgifte/validatie van een digitale identiteit, stuit echter op bezwaren. De Paspoortwetgeving geeft namelijk geen ruimte voor (experimenten met) andere verschijningsvormen van reisdocumenten.

De wetsbepalingen over het document en over de uitgifte ervan gaan – mede op basis van internationale en Europese voorschriften - uit van fysieke documenten. Deze zijn drager van een uitleesbare chip. Om (tijdelijk) afwijken hiervan mogelijk te maken, is noodzakelijk dat in een wet in formele zin wordt bepaald van welke bepalingen in de Paspoortwet mag worden afgeweken en onder welke voorwaarden. Daarnaast is aanvullende regelgeving noodzakelijk om de op dit nieuwe proces van uitgifte van een virtueel document toegesneden procedures vast te leggen. Dit is belangrijk, omdat de Paspoortwet de rechtszekerheid en rechtsgelijkheid van aanvragers van reisdocumenten en een veilig en betrouwbaar reisdocumentenproces moet borgen.

Problemen ontstaan bij:

1. De bepalingen die zien op het van rechtswege vervallen, wijzigen, weigeren, vervallen verklaren en inhouden van een document: deze bepalingen zien op het fysieke document waar een digitale identiteit van is afgeleid. Een experiment kan alleen gehouden worden als er een koppeling is tussen de status van het fysieke document en de digitale

identiteit op de smartphone van de aanvrager. Als die koppeling niet kan worden gemaakt, kan niet worden gegarandeerd dat de houder mag reizen. Het is een groot risico als iemand zonder geldig fysiek paspoort toch een daarvan afgeleid digitaal reisdocument heeft. De bepalingen in de Paspoortwet zouden dus moeten worden aangepast op deze situaties om risico's te vermijden.

2. De bepalingen over de verwerking van persoonsgegevens: dit is limitatief geregeld in de Paspoortwet. Een pilot die uitgifte van een digitale identiteit behelst, wijkt hiervan af.

Technische randvoorwaarden nog niet vervuld
In het verlengde hiervan is - wanneer een pilot in de vorm van een digitale identiteit zou worden overwogen - het cruciaal dat de benodigde technische systemen aanwezig zijn om de *real-time* koppeling te leggen tussen de status van het fysieke document en het virtuele document. Idemia gaat uit van een centraal aanvraag- en uitgifte system voor reisdocumenten, waarin ook de foto wordt opgeslagen. Een dergelijk centraal systeem bestaat (nog) niet**.** Bovendien ligt de opslag van biometrie politiek uiterst gevoelig (in de aanloop naar het AO Vernieuwing reisdocumentenstelsel (VRS) op 7 november, hebt u over opslag van biometrische gegeven, kritische vragen ontvangen). Het centrale aanvraag- en uitgifte systeem moet communiceren met een centraal identificatie-systeem. Ook dit systeem moet nog worden gebouwd. Bij de bouw van deze technische systemen moet worden gegarandeerd dat er niet gefraudeerd of 'geshopt' kan worden met de aanvraag en het gebruik van verschillende documenten.

Impact op lopende trajecten
In het KTDI-project is het gebruik van digitale identificatie verkend. Naast de toepassing ervan in het – publieke en private - reisdomein, wordt ook gedacht aan digitale identificatie als betrouwbare methode waarmee de houder elektronisch zaken kan doen met instellingen binnen en buiten de overheid. Dit betekent dat dit een vorm van een publiek identificatiemiddel zou kunnen worden, waarbij de vraag rijst, hoe het zich verhoudt tot DigiD hoog/eNIK. Laatstgenoemde is onderwerp van de WDO en wijziging Paspoortwet (eID-programma), welke wetsvoorstellen momenteel in de TK aanhangig zijn.
Deze wetsvoorstellen regelen, in samenhang, digitale identificatie op de hogere betrouwbaarheidsniveaus. Zoals bekend zullen in dit traject stapsgewijs, en voorshands alleen t.b.v. het verkrijgen van elektronische diensten in het publieke domein, zonder inbegrip van grenspassage, publieke en private middelen worden toegelaten die aan strenge eisen voldoen.

Rol private partijen bij o.a. verwerking gegevens van paspoorthouder
In de J&V-Kamervragen wordt gevraagd naar de privacyaspecten van de beoogde pilot en naar de rol van het bedrijfsleven hierin: Wat gebeurt er met de persoonsgegevens en biometrie van 5.000 Nederlanders die in de blockchain van KTDI terecht komen, ook na afloop van de pilot? Hoe en waar worden de data opgeslagen? Wie is de eigenaar van die data, en welke rechten hebben de deelnemende partijen en met name bedrijven als WEF, Accenture en Idemia? Hadden er geen aanbestedingsprocedures moeten worden doorlopen?

Verschil van mening juridische grondslag; advies CIO
De afgelopen weken is, mede naar aanleiding van de beide sets Kamervragen, binnen BZK overlegd over de beleidsmatige, technische en juridische aspecten van de voorgenomen KTDI-pilots. CZW concludeert dat, voorzover al sprake zou

zijn van beleidsmatig en technisch vervulde randvoorwaarden, er juridische haken en ogen kleven aan een pilot waarbij sprake is van het uitgeven van een digitale identiteit voor grenspassage. Hiervoor bestaat namelijk thans geen wettelijke grondslag.

Zienswijze RvIG
RvIG is het niet eens met de lezing van CZW dat de Paspoortwet zich verzet tegen het gebruik van de gegevens in het paspoort: 'Identiteit', 'digitale identiteit' en 'digitale documenten' zijn juridisch niet gedefinieerd, dus kan niet geconcludeerd worden dat er binnen KTDI sprake is van de uitgifte daarvan. Het bestaande paspoort bevat een chip die uitleesbaar is volgens open standaarden. Het is in de praktijk heel gebruikelijk dat de chip wordt uitgelezen. De Paspoortwet bepaalt niet in welke situaties het document gebruikt mag worden en of de gegevens in de chip uitgelezen mogen worden. Dat is bepaald in bijzondere wetten en regelingen. Zo bepaalt de Wet op identificatieplicht dat het paspoort gebruikt kan worden om te voldoen aan de algemene identificatieplicht. De Schengengrenscode bepaalt dat het paspoort overlegd dient te worden voor de grenscontrole. De Regeling voorzieningen GDI bepaalt dat paspoorten met een chip gebruikt (en uitgelezen) mogen worden voor DigiD Substantieel. Het gaat hier niet om digitale identiteiten of digitale documenten, maar om de vraag of het huidige paspoort gebruikt mag worden zoals dat beoogd is in de KTDI-opzet. Die vraag moet primair beantwoord worden in het licht van de AVG.

Daarnaast houdt het bezwaar van CZW 'dat niet gegarandeerd kan worden dat de houder mag reizen' volgens RvIG geen stand: Het paspoort is in een eerder stadium gecontroleerd en uitgelezen. De Kmar leest het paspoort niet opnieuw uit aan de grens, maar vertrouwt op de juistheid van de eerdere controle. Bij de grenspassage wordt de deelnemer biometrisch herkend en worden de op grond van de Schengengrenscode verplichte controles uitgevoerd, zoals het controleren van het Schengeninformatiesysteem (SIS). Geautomatiseerde grenscontrole is geregeld in de Schengengrenscode (Verordening (EU) 2016/399, geamendeerd door Verordening (EU) 2017/2225). Tevens wordt de SLTD (stolen and lost travel documents database) en RPS gecheckt.

RvIG adviseert dan ook om een derde partij (de landsadvocaat) de juridische grondslag te laten beoordelen.

Zienswijze CZW
De bezwaren van CZW zien niet op het gebruik van gegevens uit de chip in het document. Het feit dat een paspoort een chip bevat is een technische eis en onderdeel van de definitie van wat een voor grenspassage benodigd reisdocument is. Deze definitie is vastgelegd in de paspoortwetgeving. Het uitlezen van de chip ten behoeve van o.a. grenscontrole maakt onderdeel uit van het eveneens wettelijk geregelde *gebruik* van het paspoort. Indien gewenst, zou ook het uitlezen van de chip ten behoeve van het creëren van een breed bruikbare digitale identiteit wettelijk kunnen worden vastgelegd. Het gaat in de pilot *juist* om digitale identiteit. Voor de KTDI-pilot is de afgifte van een virtuele identiteit met tussenkomst en gevalideerd door de overheid een randvoorwaarde. Vanuit de KTDI-app zal namelijk het signaal aan bijvoorbeeld de Kmar worden gestuurd dat betrokkene rechtmatig de grens mag passeren. Zonder de verificatie/ validatie van de gegevens van betrokkene door de overheid (*de facto* dus afgifte van een geldig virtueel reisdocument) is garantie van rechtmatige grenspassage niet mogelijk.

In casu zou dit geschieden door afgifte van een virtuele identiteit (vID) die is afgeleid van het fysieke en wettelijk verankerde reis- en identificatiedocument. Identificatie (digitaal en fysiek) is of wordt wettelijk geregeld: zowel internationaal (eIDAS-verordening), als nationaal, nl via inregelen van het eID-stelsel en de introductie van de eNIK; beide in wetsvoorstellen nu aanhangig in de Tweede Kamer.

- Aangezien de door de overheid gevalideerde gegevens de basis vormen voor rechtmatige grenspassage, is het essentieel dat die gevalideerde set gegevens 24/7 corresponderen met de status van het bovenliggende document. Deze status blijkt uit de registraties en technische systemen in het reisdocumentenstelsel. Er zal dus een betrouwbare en waterdichte koppeling tussen beide documenten moeten zijn om frauduleus gebruik van de gegevens volledig te kunnen uitsluiten.
- Cruciaal is dat gegevens worden gevalideerd; dat gaat verder dan gebruik ervan. Dat is ook waarom de Nederlandse *overheid* door private partijen is benaderd voor deelname aan de pilot.
- De toegang tot en opslag van persoonsgegevens, inclusief biometrie, behoeft altijd wettelijke verankering, ook t.b.v. een pilot.

Inschakeling van de Landsadvocaat door BZK behoeft instemming van de Juridisch Adviseur. Hij stemt hiermee niet in; het opschalen en afhandelen van een verschil van juridisch inzicht behoort binnen het departement te geschieden. U bent verantwoordelijk voor het waarborgen van een veilige en betrouwbare identificatie in het publieke domein, ook bij grenspassage. Om de risico's van innovatie bij een dergelijke cruciale overheidstaak te kunnen beheersen, is zorgvuldige inkadering vereist. Dat is de reden waarom er thans 2 wetsvoorstellen in de TK aanhangig zijn die dit verankeren.

Advies CIO (bijgevoegd)
De CIO komt op basis van input van DIO, CZW en RvIG tot de conclusie dat KTDI, een interessant innovatief initiatief is, waarvan de technische invulling nog niet stabiel en de door RvIG beoogde uitwerking bij de CIO nog niet voldoende bekend is. Om die reden en met het oog op het bevorderen van innovatie adviseert de CIO om de pilot in eerste instantie in een labomgeving technisch door te lichten, zodat de huidige onduidelijkheden concreet kunnen worden. Parallel kan dan worden gewerkt aan voorbereiding de beoogde pilot met rechtsgevolgen, onder meer met het oog op rechtmatigheid (uitwerking AVG en bezien van nut en noodzaak wetswijziging). Dat is een meerjarig traject, dat in meer samenhang tussen betrokken partijen moeten gebeuren dan tot op heden het geval was.

Pol tieke context
Het onderwerp kan op aandacht en kritiek rekenen in de media en het Parlement. De Kamerleden die de vragen hebben gesteld zijn goed op de hoogte van de ontwikkelingen rond eID en volgen het onderwerp nauwlettend. Daarnaast zijn deze leden kritisch op mogelijke privacy-schendingen. Op 5 september verscheen het artikel 'Wildgroei van gezichtsherkenning regelt zich niet vanzelf' in het FD over gezichtsherkenningssoftware en de rol van de overheid daarin. Daarin wordt ook gerefereerd aan deze pilot en het met behulp van een digtiale identiteit afgeven van biometrische data van Nederlanders aan Schiphol, KLM en Air Canada.

Communicatie

N.v.t.