



AUTOMATISCHE PASPOORTCONTROLE NIET WATERDICHT

Dubieuze douanepoortjes

LUCHTHAVEN SCHIPHOL BESCHIKT SINDS EIND MEI OVER TWEE POORTJES DIE PASPOORTEN ELEKTRONISCH CONTROLEREN. VANWEGE DE INGEWIKKELDE INTERNATIONALE CONTEXT, ZOWEL DIPLOMATIEK ALS TECHNISCH, ZIJN ER TWIJFELS OF HET SYSTEEM WEL WATERDICHT IS TE KRIJGEN. DE STANDAARD VOOR DE ELEKTRONISCHE PAS SCHRIJFT NAMELIJK GEEN EENDUIDIG NIVEAU VAN BEVEILIGING VOOR.

HET GEMAK DIENT DE REIZIGER. Met dat idee zette luchthaven Schiphol eind mei bij de douanepassage twee consoles neer die paspoorten elektronisch controleren. Bovendien doet elektronica die controle beter dan de mens, zo verwacht het ministerie van Justitie. Vervalsers van fysieke paspoorten zijn daarin namelijk zo bedreven dat douaniers meestal niet voldoende tijd hebben om de valse exemplaren eruit te vissen. Die elektronica heeft echter ook een keerzijde: als de vervalsers eenmaal de digitale codes kent die het paspoort verifiëren, dan ligt, anders dan bij het vervalsen van elk fysieke exemplaar afzonderlijk, de hele paspoortwereld open. Die wereld zit ingewikkeld in elkaar, want ook voor geheime diensten en andere stiekeme staatsorganen is het paspoort een geliefd doelwit. Zo werd Israël er eerder dit jaar van beschuldigd Britse

paspoorten te hebben misbruikt om een geheim moordcommando naar Dubai te sturen. Naast vervalste paspoorten leveren ook sommige bonafide exemplaren een probleem op in het internationale personenverkeer. Neem bijvoorbeeld de passen die worden uitgegeven door de regering van Noord-Cyprus: die geven toegang tot slechts zes landen.

Wie de ambitie heeft om de papieren documenten met een chip uit te rusten en vervolgens poortjes te laten beslissen over de echtheid, stuit dus op twee vragen: hoe vast te stellen of het paspoort echt is en bij de huidige drager hoort, en hoe om te gaan met de talloze diplomatieke gevoeligheden. Beide vragen blijken ook nog eens innig met elkaar te zijn verstrengeld.

Het elektronische paspoort bevat een RFID-chip met een geheugen van 32 of 72 kB, die

met de buitenwereld communiceert volgens de standaard ISO-14443, waarvan bijvoorbeeld ook de OV-chipkaart gebruikmaakt. Het is dus mogelijk middels standaardapparatuur contact te leggen met de chip. Cryptografische beveiliging is daarbij een optie, maar niet verplicht. In het geval van de OV-chipkaart kun je je afvragen of encryptie, die er na alle commotie om de veiligheid van de kaart aan is toegevoegd, de moeite waard is. Maar de persoonsgegevens op de paspoortchip, onder meer naam, pasfoto en vingerafdrukken, mogen niet zomaar worden uitgelezen, laat staan gewijzigd.

VINGERAFDRUK

En daar begint de schoen te wringen. De standaard voor het elektronische paspoort, oorspronkelijk ontwikkeld door de internationale luchtvaartorganisatie ICAO, schrijft namelijk geen eenduidig niveau van beveiliging voor. Zo is encryptie van de communicatie tussen pas en uitleesapparatuur optioneel, waardoor paspoorten van sommige landen met gemak zijn af te luisteren. De encryptie zelf gebruikt een sleutel op basis van geboortedatum, vervaldatum en documentnummer. Dat leidt tot een vrij klein aantal mogelijke combinaties, waar de juiste snel uit te plukken valt – een kwestie van proberen. In Europees verband is daarom afgesproken een andere, sterkere vorm van encryptie in te voeren.

Wel verplicht is het beveiligen van de gegevens op de chip, om tegen te gaan dat die onbevoegd worden gewijzigd. Van de gegevens wordt een digitale 'vingerafdruk' gemaakt volgens een wiskundig onomkeerbaar proces. Het is niet mogelijk de gegevens zo te veranderen dat de vingerafdruk hetzelfde blijft. Omdat ook een ingebakken, unieke sleutel van de chip wordt meegenomen, is het niet mogelijk een kaart met vingerafdruk en al te klonen. Een nieuwe vingerafdruk maken bij nieuwe gegevens kan alleen als de sleutel be-



De elektronische paspoortlezer op Schiphol.

poort van een verzonnen land op naam van Elvis Presley goedgekeurde. Binnen de door ICAO opgestelde standaard heeft Nederland inmiddels de touwtjes strak getrokken. Van Beek weet echter nog een waslijst van potentiële lekken. Hij voorziet bijvoorbeeld dat criminelen een keer een uitleesapparaat gaan stelen om het uit elkaar te halen op zoek naar zwaktes, al dan niet in de software. 'Daarom is het belangrijk dat de software een openbronkarakter krijgt', stelt hij. 'Dan kan iedereen de kracht van de beveiliging verifiëren. Ik zou twee jaar de tijd nemen om te testen voor ik poortjes invoerde.'

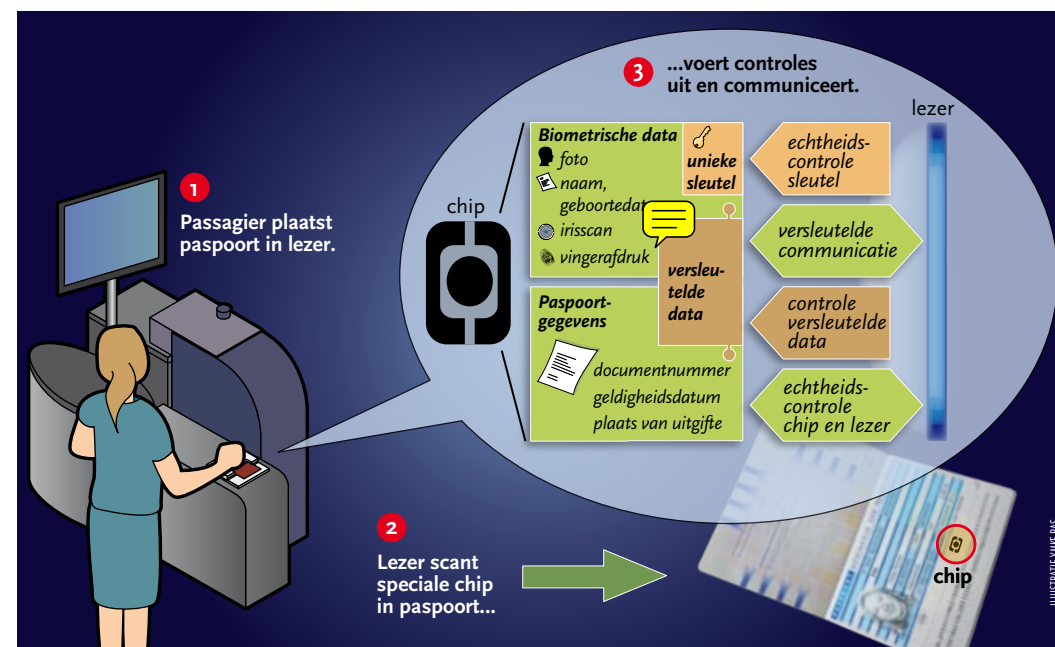
Maar dat gebeurt dus niet. Van Beek vermoedt dat nationale belangen en politieke druk een internationaal veilig systeem in de weg staan. De jongste versie van de Europese uitleesapparatuur is bijvoorbeeld gemaakt door het Duitse

'De software moet een openbronkarakter krijgen'

Bundesamt für Sicherheit in der Informationstechnik. Het is niet vanzelfsprekend dat Groot-Brittannië dat helemaal vertrouwt, laat staan de Verenigde Staten of China. Sowieso willen landen graag eigen keuzes maken, voor het paspoort, de uitleesapparatuur en het uitwisselsysteem voor publieke sleutels.

Om te controleren in hoeverre Nederland zijn zaakjes op orde heeft, deed Van Beek een beroep op de Wet openbaarheid van bestuur. Veel van waar hij om vroeg, bleek niet openbaar. Een van de opmerkelijkste feiten die hij achterhaalde was dat het ministerie van Justitie, belast met de opsporing van valse paspoorten, vorig jaar nog niet bleek te beschikken over uitleesapparatuur. Nederland heeft dus nooit de mogelijkheid gehad om te testen of er pogingen gedaan zijn de eerste generatie e-paspoorten te vervalsen.

Het ministerie zag af van de mogelijkheid mee te werken aan dit verhaal, maar aangenomen mag worden dat van eerdere fouten is geleerd. Het is niet waarschijnlijk dat Elvis Presley uit Graceland er bij de nieuwe proef op Schiphol door komt. Toch lijkt het raadzaam bij daadwerkelijke invoering van automatische poortjes bescheiden te beginnen. 'Het zou een goed idee zijn om de buitengrenzen van de Schengenlanden te nemen', zegt Van Beek. Die landen hebben immers al verregaande samenwerking op het gebied van personenverkeer. Niettemin is het wachten op de eerste hacker die erdoorheen breekt. ●



Schematische weergave van de versleutelde communicatie tussen paspoortchip en lezer. De lezer creëert die sleutel op basis van geboortedatum, documentnummer en geldigheidsdatum. Alle paspoortgegevens liggen eenmalig versleuteld vast op de chip. Ook bevat de chip een unieke sleutel.

kend is. Die sleutel moet dus een goed bewaard geheim zijn van het ministerie in het land van uitgifte. Als hij uitlekt, ligt de weg naar grootschalige uitgifte van valse paspoorten open.

Om te controleren of het paspoort echt is, is een andere, publieke sleutel nodig. Die moet over de hele wereld worden gedistribueerd, wil het systeem goed werken. Dat levert meteen diplomatieke problemen op. Mensen van veel nationaliteiten zijn welkom op Noord-Cyprus, maar slechts weinig landen zullen bereid zijn de lokale autoriteiten daar hun publieke sleutel toe te vertrouwen. Rijkstaties zullen zich allicht afvragen in hoeverre arme landen hun geheime sleutel geheim kunnen houden, dus of gebruik van hun publieke sleutel enige waarde heeft. Tot de beveiliging hoort ook dat het paspoort zich niet door elk apparaat laat uitlezen. Dat vergt certificering van de uitleesapparaten, waarvoor

ook weer een internationale waarborg moet bestaan. Bovendien moet het paspoort detecteren of het certificaat van het apparaat up-to-date is.

De ingewikkelde internationale context, zowel diplomatiek als technisch, staat in contrast met de inspanningen die onverlaten zullen willen plegen om door de beveiliging heen te breken. Bij de OV-chipkaart staat niet zoveel op het spel en is het de vraag of criminelen het de moeite waard vinden een technisch mogelijke, maar ingewikkelde kraak te zetten. Bij het paspoort ligt dat anders. Daarom zijn er mensen die twijfelen of het systeem wel waterdicht is te krijgen.

Een van de bekendste critici van het elektronische paspoort is freelance consultant Jeroen van Beek, die zich eerder bij TNO en KPMG met digitale veiligheid bezighield. Hij verwierf bekendheid toen hij liet zien dat een eerdere profopstelling op Schiphol een pas-