W.P. Willems

The Netherlands
Tel:
Mail: *wpwillems @ emgroup.nl*

http://www.emgroup.nl

Aan Het Hof van Justitie van de Europese Unie
en aan de voorzitter van de afdeling
bestuursrechtspraak van de Raad van State

Our ref: NY/NY 2010.0437 D.D. 01.03.2014
Hof ref: Gevoegde prejudiciële zaken C-446/12 – C-449/12 Willems e.a.
RvS ref: 201110934/1/A3 d.d. 11 November 2013
Subject: Remarks prejudicial ruling.

Geachte, heer, mevrouw,

Naar aanleiding van uw bericht d.d. 10.01.2014 m.b.t. de hervatting van de lopende prejudiciële beslissing wil ik graag mijn stelling toelichten dat de verordening nr. 2252/2004 van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en de biometrische gegevens in de door de lidstaten afgegeven paspoorten en reisdocumenten, te weinig waarborgen bieden ter bescherming van zowel de persoon zelf, als van de privacy van de paspoortdrager en daardoor in conflict komt met 8 EVRM.
Ik zal aantonen dat ik mijn verantwoordelijkheid als CEO van de EMGroup niet langer kan waarmaken. Reizen naar derdewereldlanden waar corruptie helaas eerder regel dan uitzondering is, is in verband met mijn persoonlijke veiligheid, niet langer verantwoord. De RFID chip in het paspoort en de methode van verificatie van de gegevens daarop, zijn daarvan de oorzaak.
De volgende punten wil ik graag behandelen, welke aansluiten op zowel het gestelde in vraag 1 alsook op vraag 2 van de Raad van State. In de bijlage vindt u links en bewijsstukken voor de stellingen.

- De techniek van de RFID chip.
  De chip welke als opslagmedium in het paspoort wordt gebruikt is ontoereikend en voldoet zeker niet aan de hoogste veiligheidseisen zoals art. 1 lid 2 voorschrijft. De banken wereld heeft veel betere, intelligentere en veiligere methodes ontwikkeld. Het paspoort is te klonen en te kopiëren. De data zijn niet veilig opgeslagen en kunnen worden gestolen en misbruikt. Met een eenvoudige scanner is de chip uitleesbaar door niet gemachtigde derden. Visa's komen op de chip en zijn door de drager niet te verwijderen. Een personen traceer/volgsysteem wordt mogelijk gemaakt.

- De zekerheid en veiligheid welke door art. 1 lid 2 / (EG) nr. 2252/2004 en art. 1 bis geboden zou moeten worden is ontoereikend.
  Het paspoort is niet het bezit van de drager, het is eigendom van de Staat Der Nederlanden en mag, indien noodzakelijk, niet worden gemodificeerd c.q. beschadigd om de chip buitenwerking te stellen. Aanpassingen zijn strafbaar. De drager heeft geen controle over wie zijn gegevens mag en/of heeft ingezien. Identiteitsdiefstal wordt, ook zonder de moeilijkere maar niet onmogelijk bereikbare biometrische gegevens, veel eenvoudiger gemaakt.

Bij invoering van deze methode van paspoort verstrekking en grenscontrole ontstaat een onoplosbaar conflict waarbij alle voorzorgen van art. 1 lid 2 / (EG) nr. 2252/2004 en art. 1 bis van de verordening te niet gedaan worden. Er ontstaat een inherente schending van de vastgelegde waarborgen in het verdrag tot bescherming van de rechten van de mens 8 EVRM en de fundamentele vrijheden en dat mede door de gebruikte verificatie methode.
De paspoortdrager zal zowel binnen als aan de buitengrenzen van het Schengengebied en later wellicht overal ter wereld, ter verificatie lokaal zijn vingerafdrukken moeten laten scannen om deze te vergelijken met de in de chip opgeslagen scans. Een eerste probleem daarbij is dat hij daarmee zijn onversleutelde gegevens moet afgeven waardoor diefstal van deze gegevens wel heel eenvoudig wordt. Daarnaast vereist een werkbaar systeem dat de landelijke coderingssleutels met "bevriende Staten" (we willen toch niemand uitsluiten ?) worden gedeeld, anders kan er geen vergelijk tussen beide scans gemaakt worden. Externe toegang en uitlezing van de chip, samen met de terplekke afgedwongen vingerafdrukscans, garanderen dat helaas ook onbetrouwbare personen en/of diensten de gegevens kunnen kopiëren en in een data base kunnen opnemen. Dat is in vol conflict met zowel art. 1 lid 2 / (EG) nr. 2252/2004 en art. 1 bis van de verordening, evenals met 8 EVRM.
Het beschermingsniveau dat de verordening zegt te bieden is non existent en ondergeschikt gemaakt aan het gebruiksgemak voor de controlerende instanties, reizigers en overheden.

- De persoonlijke veiligheid van de paspoortdrager.
In de literatuur wordt veelal aangehaald dat aan de uitgezonden code van de chip te herkennen is welk land die chip heeft verstrekt en welke nationaliteit de drager heeft; dat kan dan door terroristen worden gebruikt om doelgericht toe te slaan. Dat is waar; maar er speelt een ander, zeker zo groot gevaar, dat veel waarschijnlijker is. In landen met een hoge graad aan corruptie dreigt met name voor de drager zelf, het reële gevaar om, door middel van zijn ontvreemde vingerafdrukken afgeperst te worden. Zowel in China, Irak, Iran, Indonesië maar bv. ook in Nigeria, viert corruptie hoogtij (zo staat in de Niger delta een installatie van mijn hand bij de Nigerian National Petroleum Corporation op de Warri-Refinery) en daardoor ontstaat een probleem dat tot nu toe door de overheden gemakshalve maar genegeerd wordt; helaas kan ik het niet negeren, omdat het in potentie voor mij levensbedreigend is. Voor het verkrijgen van sommige visa moet het paspoort vaak langere tijd (dagen) worden afgestaan. Het personeel van een bureau of de betreffende ambassade regelt dan het, in dat soort landen bijna altijd noodzakelijke, visum voor je. Aangekomen op de bestemming moet je jouw paspoort weer afgeven aan de douane, allerlei beambten, politie, hotelrecepties, beveiliging, portiers en wie al nog niet meer. Een aantal daarvan kunnen ter controle een scan opeisen. Er hoeft in deze keten maar één corrupte figuur te zitten en er kan een zeer bedreigende situatie ontstaan.
Een situatie die door de makers van de verordening niet goed zijn doordacht en voorzien. In dat soort landen is drugssmokkel vaak een zwaar misdrijf waar lange straffen en zelfs de doodstraf op kan staan. Afgezien van de vraag, of en hoe een potentiële afperser mijn vingerafdrukken van mijn paspoort heeft geplukt en of hij deze vingerafdrukken al dan niet in een belastend dossier of op een drugspakket heeft geplant; http://www.youtube.com/watch?v=MAfAVGES-Yc **ik en hij weten dat het kan** en ik heb door het gebrekkige lokale rechtssysteem geen reëel andere mogelijkheid dan aan de wensen van de afperser tegemoet te komen. Voor mij is dit de reden dat ik onmogelijk aan de vingerafdrukplicht kan voldoen. Natuurlijk kan er ook geprobeerd worden om vingerafdrukken op een andere manier te ontvreemden, maar de drager heeft er zelf invloed op om dat te voorkomen; met de chip worden ze "verplicht" en op een zilverschaaltje aangeboden. A.u.b. repareer deze onnodige fout; door de paspoortdrager de controle over zijn gegevens terug te geven. Met vriendelijke groet,

W. P. Willems

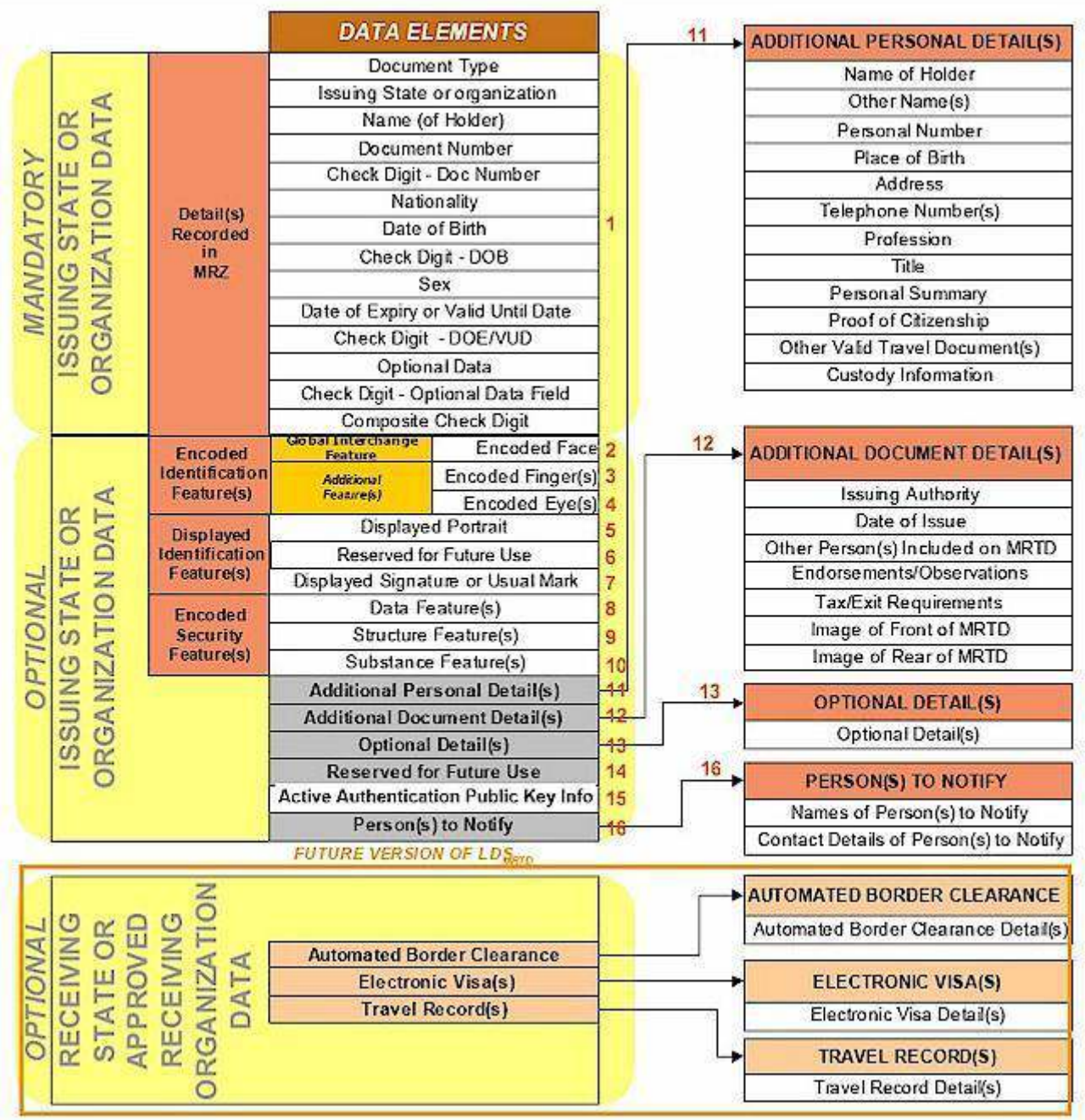
Bijlage Gevoegde prejudiciële zaken C-446/12 – C-449/12 Willems e.a.

1. De techniek van de RFID chip.

https://en.wikipedia.org/wiki/Biometric_passport Goede beschrijving van de techniek en de problemen.

http://biopaspoort.blogspot.nl/ Technische gegevens (Nederlands)

Het onderstaande schema geeft een goede indruk van de datastructuur op de chip; welke data erin te vinden zijn.



Uit: Logical Data Structure(LDS) version 1.7 , *pag 16. Data group* nummering 1-16 toegevoegd.

Nota bene: het onderste deel uit het schema, bruin omlijnd, behoort tot een volgende specificatie (vs. 2.0), die er o.a. in gaat voorzien dat, behalve Nederland als uitgever, ook ontvangende staten gegevens in uw paspoort mogen gaan bijschrijven. Het is mij onbekend wanneer versie 2.0 gebruikt gaat worden.

Het paspoort is te klonen en te kopiëren.

http://www.pcworld.com/article/151734/article.html
http://www.youtube.com/watch?v=5IttUi67XmE Video praktisch klonen en vervalsen.

De data zijn niet veilig opgeslagen en kunnen worden gestolen en misbruikt.

http://www.dexlab.nl/epassports.html

Met een eenvoudige scanner is de chip op 10 cm uitleesbaar door derden.
Met betere apparatuur tot op meters uitleesbaar.
http://simplyrfid.typepad.com/simplyrfid1/2008/07/read-range-how-far-can-we-track-you-with-passive-rfid.html
Met gesofistikeerde apparatuur gaat de grens al een kilometer voorbij.
http://www.youtube.com/watch?v=HjT7wJusuW4&feature=related vanaf de 27ste minuut.

Visa's komen op de chip en zijn door de drager niet te verwijderen.

In een latere specificatie zullen aan het biometrisch paspoort ook (elektronische) visa worden toegevoegd (zie Datastructuur op de chip). Welnu, de oudere lezer zal zich nog wel herinneren, dat, in de periode van de Koude Oorlog, een visum voor Rusland altijd op een apart vel werd uitgegeven en geniet op een bladzijde in het paspoort: als het visum namelijk fysiek IN het paspoort werd gestempeld, kwamen we Amerika niet meer (of moeilijker) in. Ik heb het zelf meegemaakt voor de val van het ijzeren gordijn. Dit fenomeen bestaat nog steeds (Arabische landen/Israël) of kan weer opduiken. In vroeger tijden haalde je het nietje los en klaar, geen haan die er meer naar kraaide: met de visa in een chip kan dat (zeer waarschijnlijk) niet.

Een personen traceersysteem wordt mogelijk gemaakt.

Hier wordt het iets schimmiger, uw paspoort kan gebruikt worden als een onzichtbaar identificatiemiddel: een Staat, een bedrijf of een misdadiger kan overal sterke zenders ophangen die constant registreren (en in een database opslaan) dat u in de buurt bent. Men kan niet gemakkelijk de gegevens uit uw paspoort lezen (die zijn in uw jaszak "redelijk" beschermd), maar er bestaan toch genoeg momenten waarop een derde wel de link tussen uw naam en uw chip kan leggen. En het vervelende is dat, als er maar één keer die relatie tussen nummer en identiteit in de database gelegd is, u op basis van dat nummer - draadloos en argeloos - identificeerbaar bent, totdat u een nieuw paspoort krijgt.

Deze angst is niet uit de lucht gegrepen. Wat te denken bijvoorbeeld van een rapport van Europese Commissie uit februari 2004 over 'a programme to advance European security through Research and Technology', waarin men het volgende project noemt:
"Demonstration of the appropriateness and acceptability of tagging, tracking and tracing devices by static and mobile multiple sensors that improve the capability to locate, identify and follow the movement of mobile assets, goods and persons, including smart documentation (e.g. biometrics, automatic chips with positioning) and data analysis techniques (remote control and access)." . Bron: com2004_0072en01.pdf, hoofdstuk 2.2.A.
Vaak wordt hier weliswaar tegenin gebracht dat zoiets alleen opgaat als de houder zijn paspoort op zak heeft en dat de houder dit 'scannen' kan bestrijden door z'n paspoort als boterham te vermommen: wikkel hem in aluminiumfolie. (de 'kooi van Farraday'). Echter, met de stringente nationale identificatie-wetgeving is het niet meer zo ondenkbaar dat men het paspoort (of een nationale identiteitskaart met dezelfde chip) altijd op zak MOET hebben. Dan zult u uw paspoort steeds vaker uit z'n folie-hulsje moeten halen en ja, dan begint het paspoort weer dat nummer uit te zenden. In de Tax Free shop moet ik bijv. ook m'n paspoort en instapkaart tonen, dat nummer kan dan opgevangen worden en opgeslagen in de database. Ook minder vergezochte voorbeelden zijn er te over: om vanaf het vliegveld in de aansluitende trein plaats te kunnen nemen, moet u eerst door een tourniquet, dat alleen opengaat als u even uw paspoort opendoet ('anti-terrorisme'). Om in de trein een lunch te kunnen afrekenen met uw creditcard, moet u even uw paspoort opendoen ('tegen creditcard-fraude'). De angst is dus, dat die chip bedacht is als middel om fraude met reisdocumenten tegen te gaan, maar allengs meer en meer gebruikt zal gaan worden voor allerlei andere toepassingen, die allemaal het beste met u voor hebben, maar wel een enorm spoor van data over u achterlaten.

Nota bene bij de Nijmeegse Universiteit, zegt prof. Jacobs in het AD van 25 augustus 2006 "Als je een beetje handig bent kan je die chip voor allerlei zaken gebruiken. Op de universiteit hebben we al een systeem ontwikkeld dat je alleen met je paspoort op je computer kan inloggen. Ik denk dat nog wel meer mensen met dat soort gadgets komen" en dat is inmiddels dan ook gebeurd. (Sportscholen, ziekenhuizen, zwembaden enz.)

Nationale databases van bezoekers met o.a. uw paspoortgegevens.

Een andere kwestie zijn de gegevens die geoogst en verzameld worden nadat de chip door de douanier, politieagent of eenieder ander, zijn uitgelezen. Immers, die prachtige Windows-applicatie die al die uitleesapparatuur aanstuurt kan ook die gegevens naar een database schrijven. Zo bouwt elk land een mooie database op van iedereen die ook maar ooit het land binnen of uit is gegaan, een verleiding waar zelfs de meest oprechten niet aan kunnen weerstaan.
En dit is heel goed mogelijk, Er is, technisch gezien, niets wat een land hier van weerhoudt. Het kan. Alles wat op een scherm staat kun je er ook weer vanaf plukken, dat is helemaal geen probleem. Wellicht is dit tegen internationale afspraken in. Maar daar stoort niemand zich aan, want niemand kan het controleren.
Uiteraard kunnen deze gegevens door corrupte douaniers en systeembeheerders doorverkocht worden.
Zelfs de Europese Commissie heeft toegestemd in het verstrekken van passagiersgegevens over vluchten naar Amerika, weliswaar “beperkt” tot 40 velden uit het paspoort. Die worden dan voor elke vlucht naar het land van bestemming gestuurd; gegevens die bijna zeker in een database terecht te komen. Snowden heeft laten zien dat hier veel gevaren en oneigenlijk gebruik kan optreden.
En als ze die foto en vinger afdrukken niet uit uw paspoort halen, dan vraagt de douane u toch alsnog om ze af te staan? Dat gebeurt nu al, bijvoorbeeld in de USA.

Resumerend: de reiziger die per vliegtuig naar het buitenland reist (vooral naar de VS), een hotel heeft geboekt en een auto gehuurd, moet zich met dit paspoort niet al te veel illusies maken over zijn privacy: het staat allemaal in databases en Staten hebben daar ofwel toegang toe (de VS kent bijvoorbeeld geen wetgeving die deze data niet toegankelijk zou maken) of ze krijgen (een deel) van die informatie over en weer aangeleverd met het paspoort en conform bi- of multilaterale verdragen.

Dit alles had/kan gemakkelijk voorkomen worden door een geavanceerde bank digipas en door de uitleessleutel slechts aan de rechtmatige eigenaar, de houder van het paspoort, te verstrekken.
Door dit na te laten betekent het in de praktijk n.l. twee dingen.

- Deze zgn. “Bevriende Staten” kunnen de gegevens, waarvan wij besloten hebben om ze niet op te slaan, juist wél opslaan. Alle argumenten tegen enige vorm van opslag door onze eigen Staat gelden nog steeds.
- Wij staan gegevens c.q. “bevoegdheden”af aan andere Staten.

Elke gegevensuitwisseling moet gepaard gaan met een optimale kwaliteit van zowel ons openbaar bestuur, als ook van het openbaar bestuur van deze vreemde mogendheden.
Uit de geschiedenis weten we dat sterke Staten soms verschrikkelijk ontsporen. Dit betekent dat we altijd de absolute zekerheid moeten hebben dat publieke bevoegdheden corresponderen met de verplichting tot het publiekelijk afleggen van verantwoording. Geen bevoegdheden zonder verantwoordelijkheden, en geen verantwoordelijkheden zonder bevoegdheden. Dat is de alfa en omega voor alle goed bestuur.
De Staat der Nederlanden kan op geen enkele manier garanderen dat andere Staten, al dan niet bevriend, geen misbruik van deze gegevens zullen maken en aldus uw grondrechten geweld aan doen. Bij de paspoortgegevens bezitten “anderen” de sleutels. Door het verstrekken van uw biometrische kenmerken verzwakt uw identiteit tot een identiteit die redelijk eenvoudig gekloond, gestolen en misbruikt kan worden.
De toekomstige misdadigers zullen niet langer met vervalste of gestolen paspoorten rondlopen, neen, ze lopen met uw en met mijn identiteit rond en worden hierdoor niet alleen onvindbaar maar sterker, als u, een onschuldige burger, reeds veroordeeld bent door “onomstootbaar biometrisch bewijs”, zal er niet eens meer naar ze gezocht worden.
De externe toegang, zonder goedkeur van de drager, is ingebakken in de gekozen opslagmethode, met de op afstand uitleesbare chip. De bescherming die art. 1 lid 2 / (EG) nr. 2252/2004 en art. 1 bis zou moeten bieden is ondergeschikt gemaakt aan het gebruiksgemak van de controlerende instanties en overheden.

Literatuur en links:

http://eprint.iacr.org/2005/095.pdf
Conclusion: The secrecy requirements for biometric data imply that unauthorized reading of e-passport data is a security risk as well as a privacy risk. The risk will only grow with the push towards unsupervised use of biometric authentication.

http://www.cosic.esat.kuleuven.be/publications/article-1279.pdf

Executive Summary

Wireless RFID networks are getting deployed at a rapid pace and have already entered the public space on a massive scale: public transport cards, the biometric passport, office ID tokens, customer loyalty cards, etc. Although RFID technology offers interesting services to customers and retailers, it could also endanger the privacy of the end-users. The lack of protection mechanisms being deployed could potentially result in a privacy leakage of personal data. Furthermore, there is the emerging threat of location privacy. In this paper, the authors will show some practical attack scenarios and illustrates some of them with cases that have received press coverage.

http://wwwhome.ewi.utwente.nl/~mostowskiwi/papers/nluug2008.pdf

Executive Summary

Passports issued nowadays have an embedded RFID chip that carries digitally signed biometric information. Access to this chip is wireless, which introduces a security risk, in that an attacker could access a person's passport without the owner knowing. While there are measures in place to prevent unauthorised access to the data in the passport, the authors show that it is easy to remotely detect the presence of a passport and determine its nationality. Although all passports implement the same international standard, experiments with passports from ten different countries show that characteristics of each implementation provide a fingerprint that is unique to passports of a particular country.

http://wwwhome.ewi.utwente.nl/~mostowskiwi/papers/nluug2008.pdf

http://www.youtube.com/watch?v=0u4pg_XwNk8 Grappige vervalsing.

http://www.hetverzet.nl/2008/paspoortlek.htm Nederlands verzet

http://frontpage.fok.nl/nieuws/454476/1/1/50/politie-neemt-vingerafdrukken-af-op-straat.html Function creep

Paspoortlek schaadt de privacy

Onderzoekers van de Radboud Universiteit in Nijmegen hebben ontdekt dat de nieuwe generatie paspoorten met draadloze chip hun aanwezigheid verraden en bovendien bij een simpel niet geautoriseerde poging de chip uit te lezen, informatie prijsgeeft door welk land het paspoort is afgegeven. Dit laatste is het gevolg van het beveiligingssysteem dat door het betreffende land wordt toegepast en dat per land verschillend is. In dit verband wordt altijd de zg. paspoortbom genoemd. Terroristen zouden een bom kunnen plaatsen die alleen afgaat als er een bezoeker uit een bepaald land voorbij komt.

http://www.hindawi.com/journals/tswj/2011/403876/abs/

SECURITY AND PRIVACY ISSUES OF THE e-PASSPORT As pointed out in previous paragraphs, the old passport included personal and biometric (photo) data and, in this manner, there was a data loss risk associated with its use. The data risk was restricted to the scope of the authorities. In addition, the classic passport was used as an identification token, for example, in hotels or banks where data could also be retained (e.g., photocopy). The e-Passports include electronic personal information (plus biometrics) that is very easy to read, store, and transmit. This technical characteristic offers an additional method to access and store personal data. The RFID communication method may pose an additional problem for privacy because tracking is possible; even if the 32-bit emitted numbers are random, the first two digits (08) always spot the passport. RFID metal shields can protect this problem, but they ring on metal detectors. As was described in the relative paragraph for the BAC mechanism, it is not based on public key cryptography and this allows online and offline brute force attacks because of the low entropy of the MRZ information. In addition, passive eavesdropping can then lead to an offline brute force attack. The new passport poses a privacy threat in comparison with those of the past since a copy of the paper passport was not evidence of the presence or the involvement of a person in a specific location or a transaction[13]. The passports now, together with the digital information, are a proof since a digital copy of the LDS or the SOD certified can be obtained and retained. Passports are shown in hotels and duty free shops where an employee could create copies of the digital information, which then becomes strong evidence.