

**Machen biometrische Reisepässe die EU sicherer?**

# **Sicherheitsrisiko Fingerabdrücke [v 1.0.1]**

27. Juni 2009

David Raison  
<david@hackerspace.lu>

## Wozu Fingerabdrücke im Reisepass?

Der Rat hat am 13. Dezember 2004 nach den Bestimmungen von Art. 67 EGV beschlossen, die, für alle Länder im Schengen-Besitzstand, unmittelbar anwendbare VERORDNUNG (EG) NR. 2252/2004 DES RATES [...] ÜBER NORMEN FÜR SICHERHEITSMERKMALE UND BIOMETRISCHE DATEN IN VON DEN MITGLIEDSTAATEN AUSGESTELLTEN PÄSSEN UND REISEDOKUMENTEN an die Mitgliedstaaten der Europäischen Union zu erlassen. Bereits bei Einführung der ersten Generation von biometrischen Reisepässen in Luxemburg lobte der damalige Außenminister Nicolas Schmit die „besonders sichere[n] Ausweisdokumente [...]“ (Bingenheimer 2006) in der Tagespresse: „Diese neue Generation von Pässen wird - wenn überhaupt - nur mit erheblichem technischen Aufwand zu fälschen sein.“ Überraschenderweise schlug die nationale Datenschutzkommission<sup>1</sup> (CNPD) nicht weniger enthusiastische Töne an und begründet die Einführung der elektronischen Reisedokumente mit dem einführenden Satz „Afin de réduire de façon significative le risque de fraude et de falsification [...]“ (CNPD 2007) um am Ende ihrer Stellungnahme doch auf einige Sicherheitsbedenken hin zu weisen.

Sicherheitsbedenken? Der sogenannte ePass macht doch alles sicherer? Die Beantwortung dieser und ähnlicher Fragen lohnt es sich zu verfolgen, bevor man seine persönlichen Daten, allen voran das Gesichtsfoto und ab 28. Juni 2009 nunmehr auch die Fingerabdrücke der beiden Zeigefinger in einen unscheinbaren Funkchip übertragen lässt. Das erschreckende ist, dass viele Menschen noch nicht einmal wissen, dass sich ein solcher in ihrem Reisepass befindet. Vor allem die Fingerabdrücke, die man vor der Konzipierung dieses Reisepasses nur straffällig gewordenen, sowie umstrittenerweise auch Visa- und Asyl-Bewerbern abgenommen hat, sollen die EU vor Terrorismus und Kriminalität bewahren.

Die Fälschung der Pässe soll so vereitelt und die Zuordnung des jeweiligen Passes zu seinem Besitzer eindeutig feststellbar werden. So soll Identitätsklau unmöglich gemacht werden und niemand mehr unter falscher Identität reisen können.

## Fingerabdrücke sind diskriminierend.

Fingerabdrücke sind für jede Person einzigartig und ändern sich ein Leben lang nicht. Damit wird zumindest die Aufnahme dieser biometrischen Merkmale in den Reisepass begründet. Doch die Minuzien und Pappilaren, die die Struktur der Finger so einzigartig machen, sind besonders von äußeren Bedingungen beeinflussbar. Das soziale Umfeld und der natürliche Alterungsprozess eines Menschen bedingen die Qualität seiner Fingerabdrücke.

Internationale und deutsche Studien belegen so zum Beispiel, dass über 10 Prozent der Senioren keine ausreichend erfassbaren Fingerabdrücke besitzen. In Luxemburg macht

---

<sup>1</sup>Commission Nationale pour la Protection des Données

die Gruppe der Senioren derzeit satte 14 Prozent der Bevölkerung aus. Rund 39.000 Personen<sup>2</sup> wären also von dieser Problematik betroffen (Statec 2008, s.9).

Doch von diesen Schwierigkeiten sind nicht nur Senioren betroffen. Menschen mit Behinderungen und jene die schwere körperliche Arbeit mit ihren Händen verrichten, werden durch die neuen Reisepässe inklusive Fingerabdrücken ebenfalls stigmatisiert. Die Personen, die dazu physisch nicht in der Lage sind und ein Attest ihres Arztes vorweisen können, sind zwar von der Abgabe ausgenommen, das bedeutet aber nicht, dass man ihnen auch bei der Passkontrolle entgegenkommt. Betroffen sind folglich auch bei dieser Maßnahme wieder größtenteils sozial schwache Schichten der Bevölkerung.

Die Fingerabdrücke können aber ebenso auf Krankheiten hinweisen. Die Einnahme eines Medikamentes<sup>3</sup> zur Unterstützung der Krebs-Therapie führt bei den Patienten zu Entzündungen der Hautflächen an Händen und Füßen. Es kommt zu Schuppenbildung, Blutungen und Blasenbildung und die Patienten verlieren dadurch die Profile ihrer Finger. In den USA musste ein Flugreisender 4 Stunden den Einreisebehörden Rede und Antwort stehen. (vgl. BBC 2009)

Bedenkt man, dass all jene Menschen in Zukunft bei Einreise- und Passkontrollen mit verschärften Kontrollen und längeren Wartezeiten rechnen müssen, kann man wohl nicht mehr von einer Vereinfachung und Beschleunigung des Prozedere durch die neuen Reisedokumente sprechen.

## **Sind Fingerabdrücke verhältnismäßig?**

Eine grundlegende Frage bei der Einführung repressiver Maßnahmen zur Bekämpfung der Kriminalität oder auch des Terrorismus ist ihre Verhältnismäßigkeit gegenüber der Problematik. Die Einhaltung dieser Relation zwischen Problem und scheinbarer Lösung wird im Protokoll 30 des EG-Vertrags gefordert. Der Europäische Rat bezeugt in der Präambel zur Verordnung CE2252/2004 in Grund 9 die Verhältnismäßigkeit der Maßnahmen, kann sich dabei aber vermutlich nicht auf eine bedeutende Anzahl wissenschaftlicher Studien über die Auswirkungen von Biometrie auf die Bevölkerung stützen, da jene, bis auf vereinzelte Ausnahmen erst ab dem Jahre 2005 entsteht. Unerklärt blieb bisher aber auch, wie der Fingerabdruck in Ausweisdokumenten denn in der Tat Terrorismus vorbeugen soll. Gewußt ist einzig und allein, dass Spanien seit 1940, damals unter Diktator Franco, die Fingerabdrücke seiner Bürger erfasst und im Ausweis hinterlegt. Doch offensichtlich konnten weder die Terroranschläge 2004 in Madrid, noch die unzähligen Anschläge der baskischen Untergrundorganisation Euskadi Ta Askatasuna (ETA) dadurch verhindert werden. (vgl. Bommarius 2004)

Auf Anfrage der Fraktion DIE LINKE hat das deutsche Bundesinnenministerium bekannt gegeben, dass im Zeitraum zwischen 2001 und 2006 nachweislich lediglich sechs deut-

---

<sup>2</sup>Ausgehend von einer Bevölkerungszahl von 277.900 Luxemburgern. (vgl. Statec 2008, s. 9)

<sup>3</sup>Hierbei handelt es sich um das Präparat Capecitabine

sche Reisepässe gefälscht wurden (vgl. Bundesregierung 2007). Man darf sich die Frage stellen, inwiefern diese Zahl die Einführung eines wesentlich umstritteneren Reisepasses aus Sicherheitsgründen rechtfertigt.

Noch fragwürdiger erscheint allerdings die Verpflichtung, Kindern ab 12 Jahren einen biometrischen Reisepass inklusive Fingerabdrücken auszustellen. Ist die Aufhebung der Unschuldsvermutung, sogar bei erst 12-jährigen Kindern zur Bekämpfung des Identitätsklaus und des internationalen Terrorismus als verhältnismäßig zu bewerten? Wann hat zuletzt ein 12 bis 15-jähriger Terrorist mit einem gefälschten Pass eine Grenze der EU passiert?

## **Sind Fingerabdrücke unfehlbar?**

In den Vereinigten Staaten haben seit 1999 mehr als 40 Richter ihre Zweifel an der Beweislastigkeit von Fingerabdrücken geäußert. Die Wahrscheinlichkeit, dass sie wissenschaftlichen Anforderungen, wie z.B. dem DAUBERT-TEST<sup>4</sup> genügen, sei eher anzuzweifeln (vgl. Mnookin N.d.).

Bei den Daten, die auf den Reisepässen gespeichert werden, handelt es sich noch nicht einmal um die Abbildungen der Fingerabdrücke, sondern lediglich um logarithmisch errechnete Hash-Werte (vgl. Krempl and Briegleb 2007). Das verhindert zwar einerseits, dass die Fingerabdrücke aus den Reisepässen entnommen und missbraucht werden können, es erhöht aber auch die Fehleranfälligkeit. Die Hashes dürfen nämlich nicht zu genau sein, um die Fingerabdrücke nicht bei den geringsten Abweichungen vom ursprünglichen Abdruck, wie zum Beispiel Unreinheiten oder Verletzungen, abzuweisen. Andererseits erhöht sich dadurch aber auch die Wahrscheinlichkeit, dass die ansonsten so einzigartigen Fingerabdrücke zwei verschiedener Personen als gleich wahrgenommen werden. BIOMETRISCHE ZWILLINGE sind Fingerabdrücke von unterschiedlichen Fingern, die ausreichend Ähnlichkeiten untereinander aufweisen um diese Abdrücke für biometrische Systeme schwer unterscheidbar machen. Die meisten Zutrittskontrollsysteme verfügen nicht über die notwendige Musterklassifizierung um solche Abdrücke voneinander zu unterscheiden (vgl. BSI and Bundeskriminalamt 2004, s. 82), doch wie schaut es mit den Systemen aus, die für die biometrischen Pässe verwendet werden?

Eine „BioFinger“ betitelte Studie des deutschen Bundesamtes für Sicherheit in der Informationstechnik zur „Evaluierung biometrischer Systeme Fingerabdrucktechnologien“ ergab, dass die Hälfte der geprüften Testsysteme bis zu zehn Prozent der zu kontrollierenden Personen fälschlich abwies (vgl. Jakobs 2009). Die Studie belegt zudem, dass durch Alterungseffekte nach ungefähr 10 Jahren nur mehr rund 70% aller Fingerabdrücke als mit den gespeicherten Daten übereinstimmend erkannt werden (vgl. BSI and Bundeskriminalamt 2004, s. 88f). Die Kommission für Datenschutz hat aufgrund dieser und weiterer Schwierigkeiten mit Fingerabdrücken glücklicherweise durchsetzen können, dass die

---

<sup>4</sup>[http://en.wikipedia.org/wiki/Daubert\\_test](http://en.wikipedia.org/wiki/Daubert_test)

Gültigkeitsdauer luxemburgischer Pässe auf 5 Jahre beschränkt wurde. Das erhöht zwar unter Umständen die Kosten für den Bürger, verringert aber auch die Wahrscheinlichkeit von Unannehmlichkeiten an den Einreise-Kontrollen und erhöht darüber hinaus, wie wir weiter unten sehen werden, die Sicherheit der Dokumente.

## **Die zweite Generation der biometrischen Pässe. Endlich sicher?**

Die biometrischen Reisepässe der ersten Generation ließen sich mit Kenntnis der Daten, die auf der sogenannten maschinen-lesbaren Zone (MRZ) aufgedruckt sind, also dem Geburtsdatum des Inhabers sowie der Nummer und dem Ablaufdatum des Passes, auslesen. Die nötige technische Kompetenz und ein handelsübliches Lesegerät vorausgesetzt konnte ein jeder seinen eigenen Reisepass zu Hause auslesen und sich davon überzeugen, dass die abgedruckten mit den abgespeicherten Daten übereinstimmen.

In den Niederlanden wurden die Pässe sogar mit linear aufsteigenden Nummern ausgegeben, so dass sie sich der Maschinencode in Abhängigkeit vom Ausstelldatum relativ leicht erraten ließ. Wenngleich es sich hierbei um eine rein theoretische und keinesfalls praktische Aussage handelt<sup>5</sup>, läßt sich der Zugangscod zum Funkchip so mit einem heute üblichen Notebook in etwa 3 Stunden errechnen. Das Problem dabei? Diese Daten stehen nicht ausschließlich auf dem Reisepass. Hotels, Flughäfen und Banken speichern solche Informationen, ja sogar der Stromlieferant, die Fahrzeugzulassungsstelle<sup>6</sup>, der Mobilfunkbetreiber und die Videothek um die Ecke wissen um die Matrikelnummern ihrer Kunden<sup>7</sup>, und einige Notare scheuen nicht einmal davor zurück, diese in den Tageszeitungen zu veröffentlichen<sup>8</sup>. In Luxemburg wurden die Passnummern auf Drängen der Datenschutzkommission jedoch von Anfang an zufällig vergeben (vgl. CNPD 2007).

Die Reisepässe der zweiten Generation führen nicht nur den digitalen Fingerabdruck ein, sie werden zudem mit der EXTENDED ACCESS CONTROL (EAC) besser vor nicht autorisierten Zugriffen geschützt. Damit der neue Pass irgendeine Information preisgibt, muss das Lesegerät sich ihm gegenüber erst anhand eines Zertifikats authentifizieren.

„Fingerprint-based document authentication cannot occur without diplomatic and technical agreements with each issuing country, which may lag behind EAC date.“ (Coleman 2008)

Das Zertifikat muss also erst vom jeweiligen Ausstellungsland den anderen Staaten zur Verfügung gestellt werden. Im Verzeichnis der internationalen Behörde für zivile Luftfahrt

---

<sup>5</sup>Unpraktisch ist dies deshalb, weil einem Hacker selten die Möglichkeit gegeben sein wird, mehr als 3 Stunden an der Hosentasche seines Opfers zu kleben.

<sup>6</sup>Schriftliche Anfrage N°377 des Abgeordneten Mars di Bartolomeo vom 19. Mai 1993

<sup>7</sup>Schriftliche Anfrage N°387 des Abgeordneten Robert Garcia vom 3. Juni 1997

<sup>8</sup>Schriftliche Anfrage N° 2901 des Abgeordneten Claude Adam vom 14. Oktober 2008 (Q-2008-O-E-2901-01)

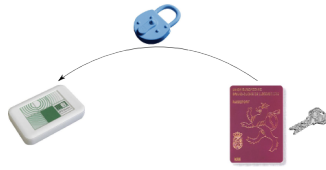


Abbildung 1: Schritt 1: Der Pass übermittelt den öffentlichen, nicht-geheimen Teil seines Schlüssels an das Lesegerät.

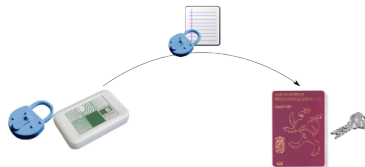


Abbildung 2: Schritt 2: Das Lesegerät verschlüsselt mit diesem Schlüssel eine Botschaft die nur mit dem, auf dem Funkchip befindlichen, privaten Schlüssel dekodiert werden kann.

(ICAO) befinden sich (Stand: April 2009) jedoch nur 9 öffentliche Zertifikate. Die allermeisten Staaten haben also, selbst wenn sie bereits über die nötigen Geräte verfügen, noch gar keine Gelegenheit, die biometrischen Merkmale der neuen ePässe zu überprüfen. Die um einiges teurer gewordenen (vgl. MAE 2009) Dokumente den allermeisten Reisenden überhaupt keine praktischen Vorteile bieten können.

Neben EAC verfügt der neue Reisepass noch über weitere Mechanismen, die beispielsweise verhindern sollen, dass er kopiert oder geklont werden kann. Das ACTIVE ACCESS (AA) genannte Verfahren besteht aus einem im Reisepass enthaltenen, privaten und nicht exportierbaren Schlüssel, der das Klonen und Fälschen der Pässe verhindern soll. Die Abbildungen 1 bis 3 erläutern dieses Verfahren.

Doch wie so oft stimmt die Theorie nicht mit der Realität überein: Grenzposten und Einreisekontrolleure werden erst jetzt mit BAC-fähigen Lesegeräten ausgestattet und EAC wird frühestens 2019 „fully effective“ sein, wenn auch der letzte Reisepass mit BAC seine Gültigkeitsdauer überschritten hat (vgl. van Beek 2009).

Auch die Zertifikate der Lesegeräte sind nicht unfehlbar. Sollte ein solches Zertifikat einmal an die Öffentlichkeit gelangen, kann jeder alle entsprechenden Reisepässe bis zum Ablauf ihrer Gültigkeit auslesen. Denn die Pässe wissen nicht um das Bekanntwerden des

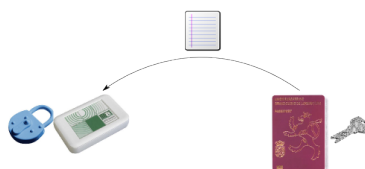


Abbildung 3: Schritt 3: Der RFID-Chip übermittelt die entschlüsselte Botschaft zurück an das Lesegerät. Damit ist sichergestellt, dass es sich um einen echten Reisepass handelt.

Zertifikats.

Daneben kann kein Staat kontrollieren was andere mit den Zertifikaten machen. Wer darf die Daten dort auslesen? Werden sie möglicherweise gespeichert? (vgl. Lischka 2007) Die Verordnung des Rates hat diese Punkte absichtlich offen gelassen um den nationalen Regierungen möglichst viel Spielraum in der Handhabung der Daten zu lassen<sup>9</sup>. Expertengruppen äußern schon seit längerem Bedenken über die mangelnde Sicherheit der Reisepässe. Die FUTURE OF IDENTITY IN THE INFORMATION SOCIETY<sup>10</sup> (FIDIS) bezeichnet in ihrer Budapest Declaration EAC bereits als unzureichend (vgl. FDIS 2006).

### **Die neuen Reisepässe, a Hacker's delight?**

Je mehr Sicherheitsfunktionen einen solcher Reisepass mit sich bringt, desto mehr Angriffsfläche bietet er für Kriminelle, aber auch für gutmütige Hacker, die die Sicherheitsmängel und Unzulänglichkeiten des Dokumentes aufzeigen. So hat der Sicherheitsexperte MARC WITTEMAN (vgl. Witteman 2005; Krempl and Briegleb 2007) rasch festgestellt, dass sich der AA Schlüssel durch Analyse des Stromverbrauchs<sup>11</sup> erraten lässt.

Es geht noch viel einfacher. Der Sicherheitsexperte JEROEN VAN BEEK hat 2008 (vgl. van Beek 2009) gezeigt, dass man die zusätzlichen Sicherheitsfunktionen, wie AA, einfach umgehen kann, indem man ihr Vorhandensein aus der Verzeichnis-Datei des Funkchips entfernt. Wenn das Lesegerät nicht weiß, dass es sich um einen Chip mit AA handelt, lässt es die Funktion einfach ungenutzt.

LUKAS GRUNWALD, ein weiterer Sicherheitsexperte, hat bereits im Sommer 2007 auf der Sicherheitskonferenz DEFCON 15 in Las Vegas, USA gezeigt, wie man Reisepässe mit EAC unbrauchbar macht und dabei auch noch die entsprechenden Lesegeräte lahmlegt. Grunwald gibt sich überzeugt, dass er durch diese Lücke auch eigenen Programm-Code in die Lesegeräte einschleusen könnte (vgl. Grunwald 2007; Bachfeld 2007).

Doch nicht nur die Sicherheitsvorkehrungen sind mangelhaft, auch die Lesegeräte für Fingerabdrücke lassen sich viel zu einfach manipulieren. Der Mathematiker Tsutomu Matsumoto hat bereits 2002 gezeigt, dass man mit dem Hauptbestandteil von Gummibärchen, Gelatine, in 80% der Versuchsfälle Lesegeräte überlisten kann. Lesegeräte, deren Hersteller ihnen höchste Sicherheit bescheinigen, lassen sich also mit Haushaltswaren im Wert von nur 10 US Dollar austricksen (vgl. Schneier 2002). Und dabei muss nicht einmal ein richtiger Finger vorhanden sein um diesen täuschend echten Abdruck zu erstellen. Der Chaos Computer Club zeigt<sup>12</sup>, wie man latente Fingerabdrücke, also solche auf Gegenständen wie Gläsern, in funktionierende Attrappen verwandeln kann.

Zudem ist nach Augenzeugenberichten von deutschen Sicherheitsexperten die Übertragungstechnik der Fingerabdrücke von den Lesegeräten zu den PCs der Behörde nicht

---

<sup>9</sup>Siehe Grund 4 der Verordnung CE2252/2004

<sup>10</sup><http://www.fidis.net/>

<sup>11</sup>Der Funkchip verwendet für die AA Funktion Multiplikation und Quadrat-Rechnung.

<sup>12</sup>[http://www.ccc.de/biometrie/fingerabdruck\\_kopieren](http://www.ccc.de/biometrie/fingerabdruck_kopieren)

abgesichert. Ob das auch in Luxemburg der Fall ist wird sich erst noch zeigen müssen, Informationen darüber und über die Kontrolle der Lesegeräte sind zumindest in den öffentlichen Medien dürftig. Die Verschlüsselung der Daten ist angeblich deswegen nicht möglich, da die Scans der Fingerabdrücke beim Antrag eines Reisepasses von den Beamten überprüft werden müssen. Anschließend werden die biometrischen Daten des Antragstellers allerdings verschlüsselt an das Passamt übertragen (vgl. deGuichet 2009).

Die erwähnten Sicherheitsexperten sind sich sicher, dass sie aufgrund der unverschlüsselten Übertragung der Daten vom Lesegerät zum Behörden-Rechner die Fingerabdrücke mitlesen und manipulieren könnten. So wäre es unter anderem möglich, die eigenen Fingerabdrücke in den Reisepass einer anderen Person einzuschleusen und so unerkannt zu reisen. (vgl. Hahn 2009) Die biometrischen Daten werden erst einen Monat nach Ausstellen eines Passes vom Rechner des Passbüros gelöscht (vgl. CNPD 2007). So lange besteht die Möglichkeit eines Hacker-Angriffs.

Es steht zudem die berechtigte Frage im Raum, ob in jeder luxemburgischen Gemeinde, in der man Pässe beantragen kann, das nötige Know-How vorhanden ist um die nötige Sicherheit zu gewährleisten.

### **Schützen Fingerabdrücke vor Terrorismus?**

Es stellt sich die berechtigte Frage, ob sich durch den biometrischen Pass und die Aufnahme von Fingerabdrücken wirklich terroristische Anschläge verhindern lassen? Unter welchen Annahmen wäre dies der Fall? Wie oben bereits erwähnt, wurde auch in vorbiometrischer Vergangenheit keine bedeutende Anzahl an deutschen und baugleichen luxemburgischen Reisepässen gefälscht. Warum geht man eigentlich davon aus, dass (potentielle) Terroristen unter falscher Identität reisen? Oder dass es sich dabei zwangsläufig um prominente Personen handelt, die wegen ihres Bekanntheitsgrades dazu gezwungen sind Identitätsklau zu betreiben? In jüngster Vergangenheit hat sich vielmehr gezeigt, dass terroristische Anschläge von unbekanntem und bisher unauffälligen Personen ausgeführt wurden, die keine gefälschten europäischen Reisepässe benötigen, sondern ganz normal mit ihren eigenen, offiziellen Reisedokumenten reisen.

Obschon diese Fragen zumindest im Augenblick unbeantwortet bleiben nimmt der Ruf nach mehr biometrischer Datenerhebung kein Ende. Weil Fingerabdrücke aus den oben erwähnten Gründen nicht immer eindeutig zugeordnet werden können, schlägt die britische BIOMETRICS ASSURANCE GROUP (BAG) vor, als Rückversicherung auch Scans der Iris durchzuführen (vgl. Heath 2008). Auch das zeigt: Die teure Einführung der Fingerabdrücke wird auf Teufel komm raus forciert, obwohl Studien und Erfahrungswerte bereits jetzt nachweisen, dass sie nicht verlässlich sind. Wie lange wird es dauern, bis erst alle 10 Finger, dann auch die Iris und die Stimme gescannt werden, um die Mängel der jeweils vorherigen Reisedokumente zu beseitigen? (vgl. Jakobs 2009)

Die biometrischen Reisepässe sollen dem Identitätsmissbrauch vorbeugen, doch in der Praxis dürfte sie eher dem Identitätsdiebstahl durch Kriminelle mit dem nötigen techni-

schen Fachwissen Vorschub leisten (vgl. Krempf and Ziegler 2007).

Ein weiteres Problem dabei ist, dass sich das blinde Vertrauen in die Technik, und so auch in die Reisepässe, schon so weit eingebürgert hat, dass wir den Daten eines Lesegeräts eher vertrauen, als dass wir einer Person glauben schenken, die beteuert unschuldig zu sein, obschon ihre Fingerabdrücke nicht mit jenen im Pass übereinstimmen (vgl. Hahn 2009). Biometrische Verfahren geben daneben auch Anlass zu anderen Besorgnis erregenden neuen Konstruktionen von Normen (vgl. Raison 2008, s. 23ff).

Es stellt sich weiterhin die Frage wieso die neuen Pässe der EU überhaupt per Funktechnik auslesbar sein müssen. Welche Beweggründe, außer einer offensichtlichen Forcierung von RFID-Technologie<sup>13</sup>, hat es gegeben um diese Art von Reisepässen einzuführen? Warum gehen die Bestimmungen in der Verordnung der EU über jene der ICAO hinaus? Auf welche Art und Weise bietet der Reisepass gefühlte Sicherheit? Warum werden Experten von der Politik bei diesem Thema ignoriert? Es lohnt sich also unbedingt, dieses Thema noch ausführlicher zu untersuchen.

Matthias Merx, Produktionschef der BUNDESDRUCKEREI GMBH hat wohl recht wenn er sagt: „Die Sicherheit hat sich [mit diesem Reisepass D.R.] um Quanten erhöht.“ (vgl. Middendorf 2007) Allerdings wohl offensichtlich nicht im umgangssprachlichen, sondern im physikalischen Sinn von Quanten, dem kleinsten messbaren Objekt.

### **Auf der Suche nach mehr Informationen?**

Eine Linksammlung und mehr Infos zum Thema, besonders zu den Angriffsmöglichkeiten, finden sich auf [https://www.hackerspace.lu/wiki/Topics#Biometric\\_Passports](https://www.hackerspace.lu/wiki/Topics#Biometric_Passports)

---

<sup>13</sup>Alleine in Luxemburg wurden 3 Millionen Euro in entsprechende Ausrüstung investiert (vgl. lesfrontaliers.lu 2006)

## Literatur

Bachfeld, Daniel. 2007. "Scan mich, dann krieg ich dich!".

**URL:** <http://www.heise.de/newsticker/Scan-mich-dann-krieg-ich-dich-/meldung/93723>

BBC. 2009. "Cancer drug erases fingerprints."

**URL:** <http://news.bbc.co.uk/2/hi/health/8064332.stm>

Bingenheimer, Volker. 2006. "Unsichtbarer Chip auf allen neuen Pässen." *Lëtzebuenger Wort*. last accessed: June 15, 2009.

**URL:** [http://www.groussbus.lu/egocms/data/groussbus\\_/passeport%20Wort%2020060822.pdf](http://www.groussbus.lu/egocms/data/groussbus_/passeport%20Wort%2020060822.pdf)

Bommarius, Christian. 2004. "Hat Franco wirklich Recht gehabt?". last accessed on June 22, 2009.

**URL:** <http://www.berlinonline.de/berliner-zeitung/archiv/.bin/dump.fcgi/2004/0319/meinung/0061/index.htm>

BSI and Bundeskriminalamt. 2004. Evaluierung biometrischer Systeme Fingerabdruck-technologien – BioFinger. Technical report Bundesamt für Sicherheit in der Informationstechnik.

**URL:** <http://www.bsi.de/literat/studien/BioFinger/index.htm>

Bundesregierung. 2007. "Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen."

**URL:** <http://dip21.bundestag.de/dip21/btd/16/117/1611796.pdf>

CNPD. 2007. "Le passeport électronique et biométrie."

**URL:** [http://www.cnpd.lu/fr/dossiers/passeport\\_electronique/index.html](http://www.cnpd.lu/fr/dossiers/passeport_electronique/index.html)

Coleman, David. 2008. "Developing an EU Member State's e-Passport, Biometrics, and Border Control Program."

**URL:** <http://biometrics.org/bc2008/presentations/157.pdf>

deGuichet. 2009. "A partir du 29 juin 2009 : introduction des passeports biométriques deuxième génération."

**URL:** <http://www.guichet.public.lu/fr/citoyens/actualites/2009/06/9-passeport-biometrique-empreintes-digitales/index.html>

FDIS. 2006. Budapest Declaration on Machine Readable Travel Documents. Technical report Future of Identity in the Information Society.

**URL:** [http://www.fidis.net/fileadmin/fidis/press/budapest\\_declaration\\_on\\_MRTD.en.20061106.pdf](http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.en.20061106.pdf)

Grunwald, Lukas. 2007. Security by Politics - Why it will never work. Technical report DN-Systems GmbH Germany. Paper presented to Defcon 15, Las Vegas, USA.

**URL:** <http://www.dc414.org/download/confs/defcon15/Speakers/Grunwald/Presentation/dc-15-grunwald.pdf>

- Hahn, Sven-Hendrik. 2009. "Fingerabdruckscanner ist unsicher. Reisepass: Hacker können Schwachstellen ausnutzen."  
**URL:** <http://wiso.zdf.de/ZDFde/inhalt/9/0,1872,7510025,00.html>
- Heath, Nick. 2008. "Warning: ID cards face fingerprint errors."  
**URL:** <http://www.silicon.com/publicsector/0,3800010403,39249422,00.htm>
- Jakobs, Joachim. 2009. "Hände weg von den Fingerabdrücken!"  
**URL:** <http://www.heise.de/tp/r4/artikel/30/30109/1.html>
- Krempl, Stefan and Peter-Michael Ziegler. 2007. "Expertenstreit über Fingerabdrücke in Pässen."  
**URL:** <http://www.heise.de/newsticker/Expertenstreit-ueber-Fingerabdruecke-in-Paessen-/meldung/88704>
- Krempl, Stefan and Volker Briegleb. 2007. "'Feuchte Hände' vor Ausgabe der neuen Pässe mit Fingerabdrücken."  
**URL:** <http://www.heise.de/newsticker/Feuchte-Haende-vor-Ausgabe-der-neuen-Paesse-mit-Fingerabdruecken-/meldung/96859>
- lesfrontaliers.lu. 2006. "Pour plus de sécurité, le Luxembourg introduit le passeport biométrique."  
**URL:** [http://www.lesfrontaliers.lu/index.php?p=edito&edito\\_id=2153](http://www.lesfrontaliers.lu/index.php?p=edito&edito_id=2153)
- Lischka, Konrad. 2007. "Experten warnen vor Biometrie-Pass."  
**URL:** <http://www.spiegel.de/netzwelt/web/0,1518,478789,00.html>
- MAE. 2009. "Informations Passeports."  
**URL:** <http://www.mae.lu/fr/content/view/full/14237>
- Middendorf, Fides. 2007. "Zwei Fingerabdrücke für mehr Sicherheit."  
**URL:** <http://www.spiegel.de/reise/aktuell/0,1518,509177,00.html>
- Mnookin, Jennifer L. N.d. "Fingerprints: Not a Gold Standard."  
**URL:** <http://www.issues.org/20.1/mnookin.html>
- Raison, David. 2008. "Terrorbekämpfung und Datenschutz: Gräbt die EU ihr eigenes Grab?" Seminararbeit, eingereicht zum Seminar "Terrorismusbekämpfung in der EU" (402060) im Sommersemester 2007 von Prof. Dr. Heinrich Neisser an der Universität Innsbruck.  
**URL:** [https://www.hackerspace.lu/w/images/2/2e/Terrorismusbekaempfung\\_Raison\\_David.pdf](https://www.hackerspace.lu/w/images/2/2e/Terrorismusbekaempfung_Raison_David.pdf)
- Schneier, Bruce. 2002. "Fun with Fingerprint Readers."  
**URL:** <http://www.schneier.com/crypto-gram-0205.html#5>
- Statec. 2008. Le Luxembourg en chiffres. Technical report Statec Luxembourg.

van Beek, Jeroen. 2009. ePassports reloaded goes mobile. Technical report Black Hat Briefings. Paper presented to BlackHat Europe 2009, Amsterdam.

**URL:** <http://www.blackhat.com/presentations/bh-europe-09/VanBeek/BlackHat-Europe-2009-VanBeek-ePassports-Mobile-slides.pdf>

Witteman, Marc. 2005. Attacks on Digital Passports. Technical report Riscure. Paper presented to WhatTheHack.

**URL:** <http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf>