Jöran Beel & Béla Gipp

ePass - der neue biometrische Reisepass

Eine Analyse der Datensicherheit, des Datenschutzes sowie der Chancen und Risiken

ePass - der neue biometrische Reisepass

Eine Analyse der Datensicherheit, des Datenschutzes sowie der Chancen und Risiken

Jöran Beel & Béla Gipp

Impressum

Jöran Beel
Zur Salzhaube 3
31832 Springe
epass@beel.org

Béla Gipp
Herzog-Wilhelm-Str. 63
38667 Bad Harzburg
epass@gipp.com

Aktuelle Informationen zum Buch finden sie unter
www.beel.org/epass/
www.gipp.com/epass/

5. Vorbehalte gegen den ePass

5.1 Einleitung

Die vorherigen Kapitel beschreiben den ePass in seiner geplanten Funktionalität. Angeregt durch Kritik von Datenschützern und Sicherheitsexperten am ePass werden in diesem Kapitel weitergehende Aspekte betrachtet. Nach dieser Einleitung wird die Zuverlässigkeit des Systems im Allgemeinen betrachtet. Der Schwerpunkt liegt dabei auf der Zuverlässigkeit der Biometrie und der Haltbarkeit des RF-Chips. Anschließend werden mögliche Angriffsszenarien durch einzelne Individuen auf den störungsfreien Betrieb analysiert. Wege zum Täuschen und Umgehen des Systems werden in Kapitel 5.4 bewertet. Die Gewährleistung des Datenschutzes wird im fünften Abschnitt behandelt, um nach der Betrachtung weiterer Aspekte im siebten Abschnitt eine Zusammenfassung zu geben.

5.2 Zuverlässigkeit des Systems im Allgemeinen

5.2.1 Einleitung

Ein ausgestellter ePass wird, wie auch der bisherige Reisepass, 10 Jahre gültig sein [AA 2005a]. Mussten bisher nur der Reisepass an sich - in Papierform - und das enthaltene Passfoto 10 Jahre halten, gilt diese Anforderung zukünftig auch für den RF-Chip und die darauf gespeicherten biometrischen Merkmale. Ob dies der Fall ist, ist umstritten. Im Folgenden werden die einzelnen Merkmale genauer auf ihre Eignung zum langjährigen Einsatz im ePass betrachtet.

5.2.2 Zuverlässigkeit der Biometrie

Wie in Kapitel 4.3 erwähnt, kommen unterschiedliche Studien zu teils sehr unterschiedlichen Ergebnissen, was die Erkennungsraten bei Biometrischen Systemen betrifft. Die BioPII Studie des BSI untersuchte die Erkennungsleistung der biometrischen Merkmale Gesicht, Finger und Iris und deren Eignung für den Einsatz in Ausweisdokumenten [BIOPII 2005]. Sie kommt zu dem Schluss, dass „Biometrische Verfahren […] die Identitätsprüfung anhand von Personaldokumenten wirksam unterstützen“ können [BIOPII 2005 S.169]. Die Studie führt außerdem an, dass in der Praxis mit besseren Erkennungsraten zu rechnen sei, da „die Nutzer am Erfolg der Verifikation ein unmittelbares Interesse haben“ und sich genauer an Anweisungen etc. halten werden (S.164). Diese Aussage kann kritisch betrachtet werden. So war die Testpopulation – bestehend aus Mitarbeitern des Frankfurter Flughafens - nicht repräsentativ für die deutsche Bevölkerung und somit eine verallgemeinerte Aussage auf den Regelbetrieb schwer möglich (S.10). Zudem gibt es Anhaltspunkte, dass die Erkennungsleistungen im Regelbetrieb eher schlechter ausfallen könnten, als die Studie vermuten lässt. Den Seiten 51ff der BioPII Studie lässt sich entnehmen, dass die Testpopulation zu einem – im Verhältnis zur deutschen Gesamtbevölkerung betrachtet – überproportionalen Teil aus europäischen und männlichen Testpersonen jungen bis mittleren Alters bestand, die mit hoher Bildung eher administrativen Aufgaben nachgehen. Personen mit diesen Eigenschaften sind es, die verhältnismäßig gute Erkennungsraten erzielen (vgl. Kapitel 4.3). So haben Männer in der Regel stärker ausgeprägte Minuzien und größere Finger als Frauen, so dass ein Fingerabdrucksensor den Abdruck eines Mannes besser erkennen kann als den einer Frau. Insbesondere Menschen asiatischer Herkunft haben zudem häufig sehr kleine Finger und sehr feine Fingerlinien, was ein erfolgreiches

Enrolen und Authentifizieren erschwert. Des Weiteren haben Administrativ tätige Personen seltener störende Merkmale an den Händen wie Verletzungen oder starke Hornhaut. Auch ältere Menschen erzielen zum Teil schlechtere Ergebnisse bei Biometrischen Systemen (vgl. Kapitel 4.3). Gänzlich unberücksichtigt bleiben bei der BioPII-Studie körperlich und geistig Behinderte. Diese erzielen signifikant schlechtere Erkennungsraten und können deutlich häufiger nicht enrolt werden [UKPS 2005].

Unabhängig davon ist zu hinterfragen, inwieweit eine repräsentative Aussage in Bezug auf die deutsche Bevölkerung überhaupt wünschenswert ist. Als wichtiger könnte eine entsprechende Repräsentation des Teils der deutschen Bevölkerung beurteilt werden, der tatsächlich einen Reisepass besitzt bzw. diesen voraussichtlich in Zukunft beantragen und nutzen wird. Da seit der Einführung des Reisepasses 1988 nur 65 Millionen Exemplare des Reisepasses ausgegeben wurden (vgl. Kapitel 2.2), ist es offensichtlich, dass nur ein Teil der deutschen Bevölkerung einen gültigen Reisepass besitzt. Es könnte also vermutet werden, dass beispielsweise überwiegend Männer mittleren Alters – Geschäftsreisende – einen Reisepass besitzen oder junge wohlhabende Menschen, die vermutlich eher verreisen, als Ältere mit geringem Einkommen. Allerdings sollte die Einführung des ePasses auch im Zusammenhang mit der Einführung des elektronischen Personalausweises (ab 2007) gesehen werden. Dieser wird für Reisezwecke innerhalb Europas die gleichen Funktionen wie ein ePass aufweisen und muss von jedem deutschen Bürger ab dem 16. Lebensjahr mitgeführt werden. Diesbezüglich wäre eine für die deutsche Bevölkerung repräsentative Studie wünschenswert.

Auch wenn die BioPII Studie zu dem Schluss kommt, dass biometrische Merkmale in Reisepässen die Grenzkontrolle wirksam unterstützen können, empfiehlt sie „eine gründliche Untersuchung der Funktionstüchtigkeit, der Erkennungsleistung und der Überwindungssicherheit“ vor dem endgültigen Echtbetrieb [BIOPII 2005 S.170]. Auf eine schriftliche Nachfrage hin erläuterte das BSI, diese Aussage sei ausdrücklich nicht so zu interpretieren, dass die gründliche Untersuchung vor der Einführung der ePässe zu erfolgen hat sondern „vor Einführung der biometrischen Systeme an den Grenzkontrollen“. Die Einführung der Biometrischen Systeme an den Grenzkontrollen erfolgt erst Anfang 2006 und wird bis 2008 dauern (vgl. Kapitel 3.2). Eine solche Untersuchung seitens der Bundesregierung ist bisher allerdings nicht erfolgt [BUND 2005].

Die BioPII-Studie sagt weiterhin aus, dass Alterungseffekte auf biometrische Merkmale bisher unzureichend untersucht worden seien. So sei schwierig abzuschätzen, ob heute aufgenommene biometrische Merkmale in 10 Jahren noch zuverlässig für eine Verifikation genutzt werden können (S.170). Diese Aussage deckt sich mit der Empfehlung der ICAO. Die ICAO empfiehlt, die Gültigkeit von biometrischen Reisepässen auf 5 Jahre zu begrenzen, da die Entwicklung in der Biometrie schnell voranschreitet und die Erkennungsleistung mit alten Merkmalen über die Zeit abnimmt [ICAO 2004d S.47]. Dennoch wird der deutsche ePass im Regelfall 10 Jahre gültig sein [AA 2005a].

Zusammenfassend kann gesagt werden, dass angesichts der Fortschritte der Biometrie in den letzten Jahren kaum Zweifel daran bestehen können, dass langfristig gute Erkennungsleistungen erzielt werden sollten. Fraglich bleibt aber, wie zuverlässig die Biometri-

schen Systeme bei der Einführung des ePasses am 1. November 2005 funktionieren werden. Ebenso fraglich bleibt, ob die biometrischen Merkmale robust genug gegen Alterungseffekte sein werden, so dass auch in einigen Jahren eine reibungslose Funktionalität der ePässe gewährleistet ist.

5.2.3 Haltbarkeit des ePass

In der Praxis ist der ePass vier Hauptbelastungen ausgesetzt. Dem Stempeln, dem Knicken bzw. Biegen, Schmutz und normalen Alterungsprozessen des RF-Chips. Der bisherige Reisepass gilt als sehr robust [BSI 2004b, S.91]. Leider existieren keine uns bekannten Studien, die sich explizit mit der Haltbarkeit von RF-Chips in Ausweisdokumenten beschäftigen, so dass sich Experten derzeit uneins sind, ob der ePass zehn Jahre lang den Belastungen standhalten wird [BSI 2004, S.73].

Stempeln sollte sich in der Praxis kaum als Problem erweisen. Die ICAO macht sehr flexible Vorschläge, wo der RF-Chip in den ePass implementiert werden kann [ICAO 2004d S.41]. Abbildung 3.4a lässt vermuten, dass die Bundesdruckerei plant, das Inlay mit RF-Chip und Antenne entweder im äußeren Umschlag des ePasses oder in der Datenseite zu implementieren. Ist das Inlay in dem oberen ePass-Umschlag implementiert, wird durch das Stempeln kein Druck auf den Chip oder die Antenne ausgeübt, der schädlich sein könnte. Befindet sich das Inlay in der Datenseite, wäre dies theoretisch möglich. Es scheint wahrscheinlich, dass, wenn begründete Zweifel an der Robustheit des Chips und der Antenne bzgl. des Stempelns bestünden, das Inlay in den oberen Umschlag eingebettet würde.

Allgemein gilt, dass RF-Chips – je nach Bauart – durch Knicken beschädigt werden können [BSI 2004, S.45]. Auch Dipl.-Ing. Jan Krissler vom Fraunhofer Institut Berlin meint auf den ePass bezogen, dass „Häufiges Knicken […] der Verbindung zwischen Chip und Antenne garantiert schaden“ wird [KRISSLER 2005]. Die ICAO hält das Biegen und Knicken des ePasses ebenfalls für eine realistische Gefährdung und empfiehlt, den ePass an den kritischen Stellen mit einem steifen nicht-metallischen Material zu verstärken [ICAO 2004b S.21]. Die Vermutung liegt nahe, dass Bundesregierung und Bundesdruckerei dieser Empfehlung nachkommen und die Haltbarkeit des ePasses auch langfristig als gewährleistet betrachten. Diesbezügliche Anfragen per Email an die Bundesdruckerei, das Innenministerium und das BSI brachten jedoch keine Antworten hervor.

Da RF-Chips als resistent gegen Schmutz gelten [BSI 2004a], ist davon auszugehen, dass dieser Faktor keinen störenden Einfluss haben wird.

Inwieweit normale Alterungsprozesse die Funktionsfähigkeit des RF-Chips innerhalb von 10 Jahren beeinträchtigen, ist unklar. So handelt es sich bei dem RF-Chip um ein elektromagnetisches Speichermedium. Auf diesen Speichermedien lassen sich nicht unbegrenzt lange Daten speichern. Die ICAO spricht von einer normalen Haltbarkeitserwartung bei RF-Chips und Smartcards von 2 bis 3 Jahren [ICAO 2004d S.47]. Laut einer Pressemitteilung von Philips sind die im ePass verwendeten RF-Chips „extrem zuverlässig“ und „die Daten bleiben deutlich länger als bei branchenweit üblichen Anforderungen erhalten“ [PHILIPS 2005b]. Die ICAO macht diesbezüglich unklare Aussagen. In [ICAO 2004d S.47] spricht sie davon, dass es ungewiss sei, ob RF-Chips nach 5 bis 10 Jahren noch zuverlässig arbeiten

würden, und empfiehlt daraufhin, die Gültigkeit eines Reisepasses auf 5 Jahre zu begrenzen. An anderer Stelle schreibt sie

> *„There are now estimated to be in excess of 100 million Contactless ICs in circulation which conform to the ISO standards. The inherent durability of the Contactless ICs specified here is not in question. “*

allerdings ohne Angabe einer konkreten Zahl, wie lange die Chips nun „zweifellos“ halten [ICAO 2004d S.7]. In [ICAO 2004b S.17] wird erwähnt, dass die RF-Chips ihre Daten mindestens 10 Jahre behalten – allerdings bei einer Lagerung von 25°C. Es ist offensichtlich, dass in der Praxis ein ePass nicht zehn Jahre lang durchgängig bei 25° Celsius aufbewahrt wird. Die Frage nach der langfristigen Haltbarkeit der RF-Chips bleibt also offen.

5.2.4 Zusammenfassung

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.3 Störung des Regelbetriebs durch einzelne Individuen

5.3.1 Einleitung

Da Diskussionen über den ePass teils sehr emotional und unsachlich geführt werden [HOF 2005] ist die Möglichkeit zu betrachten, inwieweit einzelne Individuen den Betrieb des ePasses mutwillig stören könnten. Würde sich eine „Anti-ePass“ Bewegung bilden, die ansatzweise mit der Anti-Atomkraft Bewegung zu vergleichen wäre, und bestünde die Möglichkeit, ePässe beispielsweise über größere Distanz mit hoher elektromagnetischer Strahlung zu beschädigen, könnten hohe Kosten und ein Verlust von Sicherheit entstehen. In den folgenden Abschnitten werden mögliche Angriffsszenarien beschrieben und bewertet.

5.3.2 Störsender & Blockertags

Störsender und Blockertags stören die Kommunikation zwischen Lesegerät und ePass, so dass ein Auslesen der Daten erschwert oder unmöglich gemacht werden könnte [BSI 2004a]. Auf eine nähere Betrachtung wird an dieser Stelle verzichtet. Sollte sich herausstellen, dass tatsächlich einige technisch versierte ePass-Gegner mobile Störsender entwickeln, kann diesem leicht entgegen gewirkt werden, indem die Bereiche um die Lesegeräte abgeschirmt werden, so dass eine ungestörte Kommunikation zwischen ePass und Lesegerät möglich bleibt [BSI 2004a].

5.3.3 Zerstören durch Fremdeinwirkung

Grundsätzlich gibt es drei Möglichkeiten einen RF-Chip auf nicht-mechanische Weise, d.h. nicht durch Knicken oder Ähnliches zu zerstören[5]:

- Der Speicherinhalt des EEPROM wird durch sehr starke E- und/ oder B- Felder gelöscht.
- Durch das Anlegen einer sehr hohen Spannung an die beiden Anschlusspins, an welcher die Spule angeschlossen ist, wird der RF-Chip zerstört.
- Durch elektrostatische Aufladungen erfolgt ein "Blitzeinschlag" in die Chipoberfläche und der RF-Chip wird zerstört.

Der Aufwand zur Entwicklung einer mobilen Sendeanlage, mit der sich RF-Chips auf ePässen aus einigen Metern Entfernung zerstören bzw. löschen ließen, ist hoch und mit technischen Problemen verbunden. Ein solches Gerät wäre sehr groß und auch die Energieversorgung wäre „problematisch“ [Anhang A]. Die beiden anderen genannten Möglichkeiten lassen sich für einen Angreifer nur realisieren, wenn er zumindest temporär direkten physischen Kontakt zu dem ePass hat.

[5] Basierend auf der Aussage von Dipl. Ing. Peter Jacob, Mitarbeiter der EMPA, Abteilung „Zentrum für Zuverlässigkeitstechnik“ (ehemals das Institut für Baumaterialprüfung der ETH Zürich). Der genaue Wortlaut der Email von Dipl. Ing. Peter Jacob kann Anhang A entnommen werden.

5.3.4 Demonstrationen und Sabotage

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.3.5 Zusammenfassung

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.4 Täuschen und Umgehen des Systems

5.4.1 Einleitung

Damit die Ziele des ePasses erreicht werden können (vgl. Kapitel 3.3) muss gewährleistet werden, dass das System weder getäuscht noch umgangen werden kann. Interessant ist der Vergleich zum derzeitigen Reisepass und in wieweit der ePass eine Verbesserung oder gar Verschlechterung darstellt.

Da der ePass auf dem alten Reisepass basiert und sämtliche Sicherheitsmerkmale des alten Reisepasses beinhaltet (vgl. Kapitel 3.4) sowie durch den RF-Chip mit den biometrischen Informationen ein zusätzliches Sicherheitsmerkmal erhalten hat, ist grundsätzlich davon auszugehen, dass der ePass zumindest die gleiche Sicherheit wie der alte Reisepass bietet. Die folgenden Szenarien kommen in Betracht zum Täuschen oder Umgehen des Systems.

5.4.2 Echter ePass mit falschen Papieren

Basierend auf [ROSS 2005] stellt sich die Frage, ob es möglich sein wird, einen echten ePass mit gefälschten Dokumenten zu bekommen. Meldet man seinen Personalausweis und Reisepass als gestohlen, können neue Ausweisdokumente auch mit einem Identitätsnachweis – beispielsweise mit einer Geburtsurkunde oder einem Führerschein – beantragt werden [SKBS 2005]. Sollten überhaupt keine Ausweisdokumente mehr vorhanden sein, kann der Identitätsnachweis auch mit einem Zeugen erfolgen [SKBS 2005]. Es scheint offensichtlich, dass Geburtsurkunde oder Führerschein im Vergleich zu einem (biometrischen) Personalausweis oder Reisepass verhältnismäßig leicht zu fälschen sind und auch ein „falscher Zeuge“ mit entsprechendem Aufwand beschafft werden kann. Zu bedenken gilt, dass dem jeweiligen Einwohnermeldeamt sämtliche Daten der ursprünglichen Ausweisbeantragung vorliegen und somit beispielsweise ein Vergleich des vorliegenden Fotos mit der beantragenden Person erfolgen kann[6]. Somit ist das Beantragen eines echten ePasses mit falschen Daten schwer möglich und auch nur für Personen, die sich schon in Deutschland befinden.

5.4.3 Gefälschte Pässe aus Ländern, die keinen ePass nutzen

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

[6] Dies wird auch durchgeführt, laut Auskunft der Leiterin des Einwohnermeldeamtes/Bürgerbüros Magdeburg

5.4.4 Einreise über schlecht bewachte Grenzen

Laut Bundesgrenzschutz wurden im 1. Halbjahr 2000 insgesamt 15.217 illegale Einwanderer festgenommen [DDP 2000]. Es scheint offensichtlich, dass weitere illegale Einwanderer nicht festgenommen wurden und sich nun in Deutschland befinden. Laut [BM 2005] sollen sich rund eine Million Menschen ohne gültige Aufenthaltserlaubnis in Deutschland aufhalten. Dass auch mit Einführung des ePasses weiterhin illegale Einwanderer über schlecht bewachte Grenzen nach Deutschland kommen, scheint offensichtlich. So stellt eine Studie der London School of Economics & Political Science fest, dass das Geld für biometrische Ausweispapiere unter anderem besser in verstärkte Grenzkontrollen gesteckt werden solle, um einen wirksameren Terrorismusschutz zu erzielen [LSE 2005]. Diese Studie bezieht sich allerdings auf Großbritannien und wird von der britischen Regierung als fehlerhaft betrachtet [UK 2005]. Inwieweit das Geld für den ePass tatsächlich wirksamer in andere Maßnahmen gegen Terrorismus und Illegale Einwanderung hätte gesteckt werden können bleibt offen.

5.4.5 Verändern der Daten auf dem Chip / Austauschen des Chips / Komplettfälschung

Die verwendeten RF-Chips in den ePässen können nach ihrer Herstellung und erstmaligem Beschreiben kein weiteres Mal beschrieben oder geändert werden [BSI 2005a]. Somit ist ein einfaches Ändern der Daten auf den Chips nicht möglich. Es scheint wahrscheinlich, dass der RF-Chip so in den Papierteil oder den Umschlag des ePasses implementiert ist, dass ein Austauschen des Chips nicht möglich sein wird, ohne den Pass dabei merklich zu beschädigen.

Die Daten auf dem Chip werden zudem durch eine digitale Signatur mit 224 bzw. 256 Bit geschützt (vgl. Kapitel 4.4.3). Schwachstellen in der Architektur des Algorithmus könnten die Sicherheit allerdings gefährden. So geschehen bei dem Hash-Algorithmus SHA-1 der auch von ECDSA für die digitalen Signaturen eingesetzt wird. Seit einiger Zeit sind Schwachstellen des Algorithmus bekannt, die ermöglichen die Komplexität eines Angriffs von 2^80 (Brute Force) erst auf 2^69 [WYY 2005] und mittlerweile auf 2^63 zu verringern [SCHNEIER 2005]. Es gibt keinen Grund anzunehmen, warum die Komplexität durch weitere Untersuchungen nicht noch weiter verringert werden können sollte [SCHNEIER 2005]. Diese Sicherheitslücke betrifft den ePass nicht direkt. Sie kommt nur zum Tragen, wenn man versucht eine Kollision zweier beliebiger Zahlen bzw. Bilder zu finden. Für den Reisepass hingegen wäre es wichtig, eine Kollision zu einer bestimmten anderen Zahl bzw. einem bestimmten anderen Bild zu finden. Die erwähnte Sicherheitslücke soll lediglich verdeutlichen, dass es schwer vorhersagbar ist, wie sicher ein kryptographischer Algorithmus in einigen Jahren sein wird. Die ICAO legt den Staaten mit einer zehnjährigen Passgültigkeit deshalb nahe, die Gültigkeit auf 5 Jahre zu begrenzen. So könne flexibler auf Fortschritte bei Angriffen auf die Algorithmen reagiert werden [ICAO 2004d S.47].

5.4.6 Klonen eines ePasses / Nutzen des gleichen Passes durch mehrere Personen

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.4.7 Überwindungssicherheit der biometrischen Merkmale

Die Sicherheit des ePasses hängt maßgeblich von der Überwindungssicherheit der biometrischen Merkmale ab. Wäre es möglich, mit einem entsprechend geschminktem Gesicht die Gesichtserkennung zu täuschen, mit einem Gummifinger die Fingererkennung oder mit einer entsprechenden Kontaktlinse die Iriserkennung, dann würde die Sicherheit und damit der Nutzen des ePasses in Frage gestellt.

Bisherige Studien zu diesem Thema brachten überwiegend negative Ergebnisse hervor. In [TKZ 2002] wird gezeigt, wie die gängigen Biometrischen Systeme alle erfolgreich überlistet werden können. Auch Fingerabdruck-Erkennungssysteme mit Lebenderkennung scheinen sich überlisten zu lassen [MMYH 2002] und [CCC 2004] demonstriert ebenfalls, wie sich mit einfachen Mitteln Fingerabdruck-Erkennungssysteme überlisten lassen.

Auch neuere Studien zeigen schlechte Ergebnisse der Biometrischen Systeme bezüglich ihrer Überwindungssicherheit. Die Studie BioPI des BSI kommt zu dem Ergebnis, dass sich die am Test „beteiligten biometrischen Systeme mit geringem Aufwand durch Kopien des biometrischen Merkmals Gesicht in Form von Fotos überwinden lassen“ [BSI 2004b S.11].

Die Nachfolgestudie BioPII lässt ähnliche Ergebnisse für Gesicht, Finger und Iris vermuten. In der Studie wurde, neben den eigentlichen Testzielen, die Überwindungssicherheit der beteiligten Systeme im Labor der secunet AG getestet [BIOPII 2005 S.11]. Die kompletten Ergebnisse wurden bisher nicht veröffentlicht. Auf Seite 161 der Studie findet sich in einer Tabelle allerdings der Hinweis, dass 3 der

4 Testsysteme mit der Note 4 bezüglich der Überwindungssicherheit getestet wurden. Die Note 4 erhielten Systeme deren „Überwindung mit mittlerem Aufwand erfolgreich (mit Zugriff auf das Merkmal eines Berechtigten)“ war [BIOPII 2005 S.158]. Ein System erhielt die Note 2, was daran lag, dass eine Lebenderkennung eingesetzt wurde. Dieses System erzielte jedoch schlechtere Erkennungsleistungen, da allgemein gilt, dass eine Lebenserkennung für signifikant höhere Falschrückweisung sorgt [BIOPII 2005 S.63]. Auch bietet eine Lebenderkennung keinen hundertprozentigen Schutz. In [TKZ 2002] wurde beispielsweise die Lebenderkennung des Gesichts umgangen, indem ein Wasserbeutel vor ein Foto gehalten wurde.

Eines des mit der Note 4 bewerteten Systems wird von der Bundesdruckerei und NEC produziert. Da sich die Studie direkt auf den ePass bezieht, lag die Vermutung nahe, dass dieses System auch tatsächlich – unter Umständen mit Nachbesserungen – bei den Passkontrollen eingesetzt werden soll. Eine schriftliche Nachfrage beim BSI ergab jedoch, dass NEC zwar einige der Testgeräte lieferte, jedoch nicht der Produzent für die offiziellen Grenzkontrollstationen ist.

Unklar ist, inwieweit an den Grenzkontrollen Vorkehrungen getroffen werden, um ein Täuschen der Systeme zu verhindern. Es scheint offensichtlich, dass ein Täuschen mit Fotos oder Wasserbeuteln kaum möglich sein wird, da die Passkontrollen nicht vollautomatisch sondern auch weiterhin durch Grenzbeamte durchgeführt werden. Um Gummifinger oder ähnliches zu bemerken, bedürfte es aber einer verhältnismäßig genauen Kontrolle der Reisenden. Inwieweit eine solche stattfinden wird, ist unklar.

Die BioPII Studie kommt zu dem Schluss, dass vor dem Echtbetrieb eine gründliche Untersuchung der Überwindungssicherheit sinnvoll und notwendig ist [BIOPII 2005 S.170].

5.4.8 Zerstören des RFID-Chips durch Passinhaber

Wird der RF-Chip des ePasses (mutwillig) beschädigt und sind somit die biometrischen Merkmale nicht lesbar, behält der ePass trotzdem seine Gültigkeit [BSI 2005a]. Das bedeutet, auch wenn kein Vergleich der biometrischen Merkmale stattfinden kann, ist eine Einreise nach Deutschland möglich. Diese Tatsache stellt den Nutzen des ePasses in Frage. Was bringt die Einführung des ePasses, wenn ein Einreisen auch mit defektem RF-Chip und somit ohne Vergleich der biometrischen Merkmale möglich ist? Laut Auskunft des Bundesministeriums des Inneren wird im Fall eines defekten RF-Chips „mit den klassischen Verfahren die Identität geprüft, wobei dies sicher Anlass zu besonders intensiver Prüfung wäre“ [CCC 2005]. Wie eine solche intensive Prüfung aussehen wird, ist unklar. Da die Fingerabdrücke des Passinhabers nur digital auf dem RF-Chip gespeichert und nicht in den Papierteil des Passes gedruckt[7] oder in einer zentralen Datenbank gespeichert werden (vgl. Kapitel 5.5.7), scheidet ein Vergleich der Fingerabdrücke mit Referenzdaten vermutlich aus. Hier sollte in Erwägung gezogen werden, ob eine zusätzliche Aufnahme der Fingerabdrücke in den Papierteil sinnvoll wäre. Vielleicht wäre es auch möglich, die Fingerabdrücke der zu überprüfenden Person mit den Daten im zuständigen Melderegister abzugleichen. Inwieweit dies möglich und rechtlich zulässig ist, können wir nicht einschätzen.

[7] Laut telefonischer Auskunft von Michael Dickopf, Pressesprecher des BSI

5.4.9 Unkenntlich-Machen der biometrischen Merkmale

Einen ähnlichen Effekt wie das Zerstören des RF-Chips hätte das Unkenntlichmachen der biometrischen Merkmale, also des Gesichts und der Finger, so dass kein Vergleich mit den auf dem Pass gespeicherten Daten stattfinden kann. Hier gelten die gleichen Punkte wie beim Zerstören des RF-Chips durch den Passinhaber. Ein Einreisender, bei dem weder Gesicht noch Finger zur Verifikation genutzt werden können, würde mit besonders hoher Aufmerksamkeit bei der Grenzkontrolle geprüft. Hier stellt sich die Frage, welche Möglichkeiten die Grenzbeamten haben, eine Prüfung durchzuführen, wenn Gesicht und Finger unkenntlich sind. Das gleiche Problem tritt bereits jetzt auf, wenn das Gesicht eines Reisenden unkenntlich und damit ein Vergleich mit seinem Passfoto nicht möglich ist. Laut Auskunft zweier Grenzbeamter des Flughafens Berlin Schönefeld gibt es keine genauen Richtlinien für diesen Fall[8]. Es liegt im Ermessen der Beamten eine Lösung zu finden.

5.4.10 Zusammenfassung

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

[8] Laut persönlicher Nachfrage bei der Grenzkontrolle

5.5 Gewährleistung des Datenschutzes

5.5.1 Einleitung

Datenschützer kritisieren die Einführung des ePasses als „verfassungsrechtlich höchst problematisch“ und sehen den Datenschutz durch den ePass gefährdet [HEISE 2005]. Dieser Abschnitt führt die geäußerten Bedenken auf und analysiert sie. Dabei wird unterschieden zwischen den Möglichkeiten, gezielt Daten einer bestimmten Person zu erhalten, und Möglichkeiten zum massenhaften Auslesen der ePässe vieler verschiedener Personen. In ersterem Fall ist zu beachten, dass Gesichtsbild und Fingerabdrücke einer Person in der Regel auch ohne ePass mit entsprechendem Aufwand zu bekommen sind. Von daher liegt der Schwerpunkt der Betrachtung auf der Frage, inwieweit massenhaftes Auslesen der Daten verschiedener Personen möglich ist.

5.5.2 Unautorisiertes physikalisches Auslesen der Daten

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.5.3 Kryptographische Sicherheit von Basic Access Control

Der Schlüssel für die Basic Access Control setzt sich aus Ablaufdatum des Passes, Geburtsdatum des Passinhabers und der Passnummer zusammen. Hieraus ergibt sich eine maximale Schlüssellänge von 56 Bit (vgl. Kapitel 4.4.1). Tatsächlich aber kann der Schlüssel als schwächer als 56 Bit eingestuft werden. Abhängig davon, ob nur die Daten einer einzelnen Person abgehört werden sollen oder das massenhafte Auslesen angestrebt wird, lassen sich die Wertebereiche der drei Faktoren, aus denen der Schlüssel gebildet wird, mehr oder weniger stark einschränken, wodurch die effektive Schlüssellänge sinkt.

In den ersten 10 Jahren nach Einführung des ePasses liegt die Anzahl der Möglichkeiten, für das Ablaufdatum des ePasses nicht bei 365x10 Möglichkeiten sondern nach dem ersten Jahr der Einführung bei 365x1, nach dem 2. Jahr der Einführung bei 365x2 etc. Berücksichtigt man Wochenenden und Feiertage, an denen die Ausgabestellen nicht geöffnet haben, reduziert sich die Anzahl der Möglichkeiten weiter, und zwar um 52 Wochenenden à 2 Tagen sowie mindestens 8 Feiertage pro Jahr[9]. Dies reduziert den Faktor von 365x10 auf 253 x

[9] 8 bis 12 gesetzliche Feiertage in Deutschland, abhängig vom Bundesland.

10 (rund 10^3) bzw. entsprechend weniger in den ersten 10 Jahren nach der Passeinführung.

Wird berücksichtigt, dass junge und alte Menschen weniger häufig verreisen und somit seltener an Grenzübergängen anzutreffen sind bzw. Kleinkinder keinen Reisepass besitzen können [AA 2005b], reduziert sich die Anzahl der Möglichkeiten der Geburtsjahre von 100x365 auf 49x365 (rund 10^4) unter der Annahme, dass der Wertebereich auf das Alter zwischen 16 und 65 Jahren eingeschränkt wird. Soll das Auslesen der Pässe nicht vollautomatisch erfolgen, sondern könnte das Alter grob geschätzt werden, reduzieren sich die Möglichkeiten auf 10x365 (rund 10^3) Möglichkeiten (geschätztes Alter plus minus 5 Jahre). Wird das Geburtsdatum als bekannt angenommen, da man die Daten einer bestimmten und persönlich bekannten Person auslesen will, reduziert sich die Länge dieses Teilschlüssels auf die Länge eins.

Die Passnummer besteht - zumindest in Deutschland - aus 9 Zahlen, womit sich 10^9 theoretische Möglichkeiten ergeben. Werden diese Zahlen zufällig bzw. nach einem dem Angreifer nicht bekannten Muster vergeben, kann der Wertebereich nicht weiter eingeschränkt werden. Dies macht deutlich, dass die Sicherheit des Gesamtschlüssels stark von der Passnummer abhängt, die im Idealfall mit 10^9 Möglichkeiten einen weitaus größeren Faktor darstellt als das Ablaufdatum (10^3 Möglichkeiten) oder das Geburtsdatum (zwischen 1 und 10^4 Möglichkeiten).

Werden die Passnummern fortlaufend oder nach einem bekannten Muster vergeben, lässt sich die Anzahl der Möglichkeiten einschränken. So werden in den Niederlanden die Passnummern fortlaufend

vergeben. Dies soll bereits dazu geführt haben, dass Basic Access Control gebrochen werden konnte [HEISE 2005b], allerdings unter optimalen Bedingungen mit bekanntem Geburtsdatum und einem 5 Jahre gültigen Pass.

In Deutschland wird die Passnummer ebenfalls nicht zufällig vergeben [PaßG 1986 §4]. Jede der ca. 6500 Passbehörden hat eine eindeutige Behördenkennzahl. Diese vierstellige Zahl stellt die ersten Ziffern der Seriennummer dar. Die verbleibenden 5 Stellen werden von der Behörde als Passnummer fortlaufend vergeben. Eine eventuell vorhandene 10. Zahl kann vernachlässigt werden, sie stellt lediglich eine Prüfziffer dar. Es ist offensichtlich, dass die ohnehin schon eingeschränkte Schlüsselstärke bei Kenntnis der Behördenkennzahl nochmals stark reduziert werden kann. Bei bekannter Behördenkennzahl und unbekannter fünfstelliger Passnummer ergeben sich statt 10^9 nur noch 10^5 Möglichkeiten für die Seriennummer.

Die Tabellen 5.5.3a/b geben eine Übersicht, als wie stark der Schlüssel von Basic Access Control angesehen werden kann unter den jeweiligen Bedingungen. Tabelle 5.5.3.a geht dabei von 10^9 möglichen zufälligen Passnummern aus, Tabelle 5.5.3.a von einer Einschränkung auf 10^5 Möglichkeiten und stellt damit den Fall dar, dass die Behördenkennzahl dem Angreifer bekannt, die Passnummer aber unbekannt ist.

Tabelle 5.5.3a: Tatsächliche Schlüssellänge von Basic Access Control bei 10^9 zufälligen Passnummern [Bit]

	Ausstellungs-tage pro Jahr*	Geburtsdatum bekannt	Geburtsdatum geschätzt (+-5 Jahre)	Geburtsdatum beschränkt (16-65 Jahre)	Geburtsdatum nicht bekannt (100 Jahre)
1 Jahr nach Einführung	365	38	50	53	54
	253	38	50	52	53
2 Jahre nach Einführung	365	39	51	54	55
	253	39	51	53	54
5 Jahre nach Einführung	365	41	53	55	56
	253	40	52	54	55
10 Jahre nach Einführung	365	42	54	56	57
	253	41	53	55	56

* 253 Tage pro Jahr unter der Annahme, dass an Wochenenden und Feiertagen keine Pässe ausgestellt werden, 365 sonst

Tabelle 5.5.3b: Tatsächliche Schlüssellänge von Basic Access Control bei 10^5 zufälligen Passnummern [Bit]

	Ausstellungs-tage pro Jahr*	Geburtsdatum bekannt	Geburtsdatum geschätzt (+-5 Jahre)	Geburtsdatum beschränkt (16-65 Jahre)	Geburtsdatum nicht bekannt (100 Jahre)
1 Jahr nach Einführung	365	25	37	39	40
	253	25	36	39	40
2 Jahre nach Einführung	365	26	38	40	41
	253	26	37	40	41
5 Jahre nach Einführung	365	27	39	42	43
	253	27	39	41	42
10 Jahre nach Einführung	365	28	40	43	44
	253	28	40	42	43

* 253 Tage pro Jahr unter der Annahme, dass an Wochenenden und Feiertagen keine Pässe ausgestellt werden, 365 sonst

Ist die Passnummer in etwa abschätzbar, lässt sich die Schlüssellänge noch weiter einschränken.

Nachdem gezeigt wurde, dass die tatsächliche Schlüssellänge von der theoretischen Schlüssellänge abweichen kann, stellt sich die Frage, ob die kürzere Schlüssellänge dennoch als ausreichend betrachtet werden kann um den Datenschutz zu gewährleisten.

Der Datenschutzbeauftragte von Hessen empfiehlt einen 56 Bit langen Schlüssel für den

> „Einsatz bei nicht sensiblen personenbezogenen Daten oder in solchen Fällen, in denen ein Angriff mit hohem Aufwand aus anderen Gründen unwahrscheinlich ist (z. B. geschlossenes Netz). Zukünftige Sicherheitsprobleme sind jedoch zu erwarten“ [DH 2003].

Einen 40 Bit langen Schlüssel hingegen nur als „Schutz gegen zufällige Kenntnisname“ und für den

> „Einsatz bei nicht sensiblen personenbezogenen Daten, wenn ein gezielter Angriff unwahrscheinlich ist.“ [DH 2003]

Diese Empfehlung, die auch von anderen Datenschützern und Sicherheitsexperten geteilt wird, bezieht sich jedoch nicht direkt auf den ePass. Es liegt die Vermutung nahe, dass der Mikroprozessor eines RF-Chips nicht die Leistungsfähigkeit besitzt wie ein handelsüblicher PC oder ein System, das auf Entschlüsseln spezialisiert ist und somit eine Brute-Force Attacke ungleich länger dauert. Dennoch haben es Forscher aus den USA geschafft, einen mit 40 Bit verschlüsselten RF-Chip innerhalb einer Stunde zu knacken [BGSJRS 2005]. Sie vermuten, die Zeit mit weiterer Forschung auf wenige Minuten senken zu können. Der Versuchsaufbau gleicht allerdings nicht der Situation wie sie beim ePass vorzufinden ist. Zudem müsste sich ein Angreifer für eine ‚Live-Brute-Force-Attacke’ permanent in unmittelbarer Nähe zu dem ePass befinden. Selbst wenn die Chips langfristig um ein vielfaches leistungsstärker werden und ein Brute Force Angriff in wenigen Sekunden möglich würde, könnte man diesen leicht unterbinden, indem der Chip erst nach einer kurzen

Verzögerung antwortet. Durch diese Verzögerung würde das Ausprobieren aller möglichen Kombinationen praktisch unmöglich gemacht, da die Zeitspanne zu groß wäre.

Anders sieht es bei der Sicherheit von aufgezeichneten Daten aus. Hat ein Angreifer die Kommunikation zwischen ePass und Lesegerät aufzeichnen können, kann er die verschlüsselten Daten nachträglich entschlüsseln und so an die biometrischen Daten gelangen.

Doch auch in diesem Fall ist die Wahrscheinlichkeit abzuwägen. Um einen Kommunikationsvorgang zwischen Lesegerät und ePass aufzeichnen zu können, muss man sich innerhalb weniger Meter vom ePass befinden. Damit scheint das massenhafte Aufzeichnen unwahrscheinlich, da ein Kommunikationsvorgang nur direkt an einem Grenzübergang stattfindet und ein Aufzeichnungsvorgang über längere Zeit schnell bemerkt würde, sofern nicht der Grenzbeamte selbst der Angreifer ist. Zudem kann ein Aufzeichnen der Kommunikation zwischen Lesegerät und RF-Chip wirksam unterbunden werden, wenn die Zonen um die Lesegeräte entsprechend abgeschirmt sind [BSI 2004a]. Allerdings ist dies zurzeit nicht geplant[10].

Das Aufzeichnen eines Kommunikationsvorgangs bei einer bestimmten Person hingegen wäre leichter zu bewerkstelligen, vorausgesetzt es erfolgt keine Abschirmung. Doch gilt zu bedenken, dass durch die Basic Access Control lediglich das Gesichtsbild geschützt wird. Ein Angreifer der in der Lage ist, den Kommunikationsvorgang aufzuzeichnen und diesen zu entschlüsseln sollte mit weniger Aufwand in

[10] Laut telefonischer Auskunft von Michael Dickopf, Pressesprecher des BSI

der Lage sein, auch unbemerkt ein Gesichtsbild der Zielperson aufzunehmen.

5.5.4 Umgehen von Basic Access Control

Prof. Dr. Andreas Pfitzmann, tätig an der TU Dresden, erwähnt in [PFITZ 2005], dass die Basic Access Control datenschutzrechtlich bedenklich sei. Selbst wenn die technische Seite als vollständig sicher eingestuft werden könne, hätten zu viele Personen Zugriff auf die MRZ des ePasses und könnten von da an den RF-Chip auslesen. Als Beispiel für Personen mit Zugriff auf die MRZ – und damit auf den kompletten Schlüssel - führt er die ausstellende Behörde, Mitarbeiter der Bundesdruckerei und Grenzposten an, aber auch Unternehmen, denen gegenüber man sich mit dem Ausweis bzw. Reisepass oder einer Kopie desselben identifizieren muss (Banken oder Mobilfunkhändler).

Diese Kritik scheint im Grundsatz richtig. Es stellt sich jedoch die Frage, inwiefern es als kritisch angesehen werden kann, wenn eine Person mit direktem optischen Zugriff auf die MRZ später das digitale Gesichtsbild des ePasses erneut auslesen kann. Unter der Annahme, dass digitales und „echtes“ Passfoto keine relevanten Unterschiede enthalten, ist in dem Moment, in dem der optische Zugriff auf die MRZ gewährt wird, ebenfalls der Zugriff auf das im ePass enthaltene Passfoto möglich, so dass ein Angreifer auch später keine Daten erhalten kann, die er nicht schon beim Zugriff auf die MRZ erhalten konnte.

Pfitzmann führt als daraus resultierende Risiken das Erstellen von Bewegungsprofilen und personenbezogener Bomben an. Diese Risiken werden gesondert in Kapitel 5.5.8 betrachtet.

Festzuhalten bleibt, dass architekturbedingt die Basic Access Control – welche dazu dienen soll, das unbemerkte Auslesen der Daten zu verhindern - von Personen umgangen werden kann, sobald diese einmal Zugriff auf die MRZ hatten. Diese Personen sind dann zukünftig in der Lage, unbemerkt vom Passinhaber aus geringer Distanz das auf dem RF-Chip gespeicherte Gesichtsbild sowie die weiteren persönlichen Daten wie Name oder Geburtsort auszulesen. Dabei können im Grunde keine Daten ausgelesen werden, die nicht auch beim optischen Zugriff auf die MRZ hätten gelesen werden können.

5.5.5 Kryptographische Sicherheit von Extended Access Control

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.5.6 Umgehen von Extended Access Control

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.5.7 Zentrale Datenbanken

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.5.8 Bewegungsprofile & personenbezogene Bomben

In [PFITZ 2005] wird als Risiko des ePasses erwähnt, dass das Erstellen von Bewegungsprofilen und personenbezogenen Bomben ermöglicht werde durch Schwachstellen bei der Basic und Extended Access Control (vgl. Kapitel 5.5.4 und Kapitel 5.5.6).

Auch wenn die erwähnten Schwachstellen existieren, scheint zumindest das Erstellen von Bewegungsprofilen in der Praxis ausgeschlossen. Die Reichweite des RF-Chips beträgt unter günstigen Umständen wenige Meter [FK 2004] und es gibt keinen Grund anzunehmen, dass langfristig Lesegeräte flächendeckend und an anderen Orten als Grenzübergängen installiert werden, was für das Erstellen von Bewegungsprofilen notwendig wäre. Doch selbst wenn Lesegeräte in weiten Teilen der Bundesrepublik installiert würden, könnte das Lesegerät nicht bestimmen, welche Personen sich in der Nähe befinden. Ein ePass besitzt keine eindeutige Seriennummer. Somit müsste ein Lesegerät alle in Deutschland vorhandenen MRZs an den in der Nähe befindlichen ePass senden und erst in dem Moment, wo zufällig die richtige MRZ bzw. der richtige Schlüssel gesendet wurde, könnte das Lesegerät den Passinhaber identifizieren. Eine flächendeckende Personenüberwachung mittels ePass scheint also ausgeschlossen, zumal es leichtere Methoden zum Erstellen von Bewegungsprofilen gibt, beispielsweise mittels GSM-Mobilfunknetz [BSI 2003].

Das Erstellen von personenbezogenen Bomben scheint theoretisch möglich. Sofern ein Angreifer im Besitz der MRZ oder eines gültigen Schlüssels für die Extended Access Control ist, könnte dieser mit entsprechendem Know-how ein System bauen, welches bestimmte Aktionen auslöst – also z.B. eine Bombe zündet – wenn der ePass

sich innerhalb eines Radius von wenigen Metern um das Systems befände.

5.5.9 Verbesserung des Datenschutzes

Sämtliche in den vorigen Absätzen beschriebenen Vorbehalte gegenüber dem ePass basieren auf der Tatsache, dass nicht gänzlich ausgeschlossen werden kann, dass Dritte unbemerkt Zugriff auf die Daten des ePasses bekommen. Es stellt sich somit die Frage, ob eine Verbesserung des Datenschutzes erreicht werden kann, indem das unbemerkte Auslesen weiter erschwert oder praktisch unmöglich gemacht wird. Wir sehen folgende Ansatzpunkte.

Die Stärke des Basic Access Schlüssels könnte erhöht werden, wenn ein echter Zufallsschlüssel verwendet würde anstelle eines Schlüssels, der sich aus Faktoren zusammensetzt, die unter Umständen stark eingeschränkt werden können (vgl. Kapitel 5.5.3).

Wäre der Schlüssel der Basic Access Control – in der konkreten Umsetzung des ePasses die MRZ – beispielsweise nur unter UV-Licht sichtbar, ergäbe sich nicht das Problem, dass der Schlüssel auch auf Kopien des ePasses sichtbar ist, die beispielsweise Mobilfunkunternehmen oder Banken erhalten (vgl. Kapitel 5.5.4).

Die ICAO erwähnt die Möglichkeit in den ePass eine Metallfolie einzubauen. Diese würde verhindern, dass ein Lesen der Daten bei geschlossenem Pass möglich ist [ICAO 2004i S.20] & [ICAO 2004b S.14+25].

5.5.10 Zusammenfassung

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.6 Weitere Aspekte

5.6.1 Einleitung

Neben datenschutzrechtlichen Bedenken und Zweifeln an der Zuverlässigkeit bemängeln Kritiker weitere Punkte am ePass, die im Folgenden erörtert werden sollen.

5.6.2 Unklare Kosten und ungewisser Nutzen

Die Einführung des ePasses wurde vom Bundesrat als letzte Instanz beschlossen, ohne zu wissen, wie hoch die endgültigen Kosten sein werden [BR 2005]. Zwar steht der Preis von 59 Euro für den Passinhaber schon fest, wie hoch aber die tatsächlichen Kosten, z. B. für Schulungen von 35.000 Mitarbeitern, Anschaffung der Lesegeräte und Ausstattung der 6.500 Meldestellen sein werden, ist unklar [BUND 2005] & [HEISE 2005c]. Das ‚Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag' (TAB) - aus dem Jahre 2003 und nicht direkt auf den ePass bezogen - geht in einer Schätzung von einmaligen Mehrkosten zwischen 0,18 Mrd. und 0,61 Mrd. Euro aus [TAB 2003, S. 142ff]. Jährliche Mehrkosten entstünden in Höhe von 0,06 Mrd. bis 0,33 Mrd. Euro. Hierbei handelt es sich um eine sehr grobe Abschätzung mit vielen Unsicherheitsfaktoren [TAB 2003, S. 83].

Die London School of Economics & Political Science hat in [LSE 2005] die Effizienz von biometrischen Ausweisdokumenten untersucht. Ergebnis der Studie ist, dass die Einführung der biometrischen Ausweise vermutlich wirksam gegen illegale Einwanderer und Terroristen sein wird, diese Ziele aber auch mit weniger Aufwand erreicht werden können [LSE 2005 S.3]. Zudem wird die mangelnde Zuverlässigkeit von Biometrischen Systemen kritisiert. Die Britische Regierung widerspricht dieser Studie jedoch ausdrücklich in [UK 2005]. Zudem kann die Studie nicht direkt auf Deutschland übertragen werden. Sie beschäftigt sich mit der Einführung von biometrischen Personalausweisen und nicht mit Reisepässen wobei die Ziele vergleichbar sind.

Da in Deutschland die Kosten unklar sind, ist folglich auch keine Kosten-Nutzen-Analyse möglich gewesen. Eine Abschätzung, inwieweit der Nutzen die Kosten rechtfertigt oder inwieweit die verfolgten Ziele (vgl. Kapitel 3.3) auf anderem Wege, beispielsweise durch eine Verstärkung der Grenzkontrollen, hätte erreicht werden können, liegt nicht vor.

Ab 2007, wenn neben dem Gesichtsbild die Fingerabdrücke erfasst werden, ist mit einer weiteren Preissteigerung zu rechnen (vgl. Kapitel 3.4).

5.6.3 Vorschnelle Einführung

Weitere Kritik trifft laut Datenschutzbeauftragten des Bundes und der Länder die vorschnelle Einführung des ePasses [BDS 2005]. So seien die Voraussetzungen für einen reibungslosen Ablauf noch nicht in ausreichendem Maße gegeben. Der Bundesrat moniert in seiner

Entscheidung zur Einführung des ePasses, dass die Länder „in dem bisherigen Verfahren zur Einführung biometrischer Merkmale erst sehr spät und nur unzureichend von der Bundesregierung einbezogen worden“ sind [BR 2005]. Schon auf europäischer Ebene sollen die Volksvertreter „komplett überfahren“ worden sein [HEISE 2004]. Vertreter in Brüssel sollen von „Erpressung“ und einem „hinterhältigem Spiel“ gesprochen haben, und eine britische Parlamentarierin meint, es sei „ein absoluter Skandal, dass dieser Angriff auf unsere Freiheitsrechte ohne jegliche parlamentarische Prüfung durchgeht“ [KREMPL 2005].

Kritisiert wird zudem, dass keine Studien oder Pilottests vor der Entscheidung zur Einführung des ePasses durchgeführt wurden, die Rückschlüsse auf den zu erwartenden Nutzen und die entstehenden Risiken gegeben hätten [BUND 2005]. Des Weiteren wurde die Einführung des ePasses zu einem Zeitpunkt beschlossen, als Studien des BSI die Leistung von Gesichtserkennungssystemen „allenfalls in einem automatisierten Überwachungsszenario [als] ausreichend“ betrachteten, darüber hinaus aber als „nicht akzeptabel“ bezeichneten [BIOFACE 2003 S.10].

Begründet wird die schnelle Einführung mit der erhöhten Dringlichkeit und den Vorgaben aus den USA sowie einem wirtschaftlichen Vorteil (vgl. Kapitel 3.3). Laut EU-Beschluss sind die Reisepässe aber erst zu Mitte 2006 mit dem Gesichtsbild in elektronischer Form zu versehen. Genug Zeit also, die Einführung sorgfältiger zu planen und Bedenken in der Bevölkerung zu zerstreuen. Das wirtschaftliche Argument mag zutreffen – sofern der ePass einwandfrei funktioniert. Sollte das Gegenteil der Fall sein, ist eher mit einem Schaden für die Wirtschaft zu rechnen (vgl. Kapitel 3.3). Darüber hinaus ist Deutsch-

land nicht das einzige Land, welches sich als Vorreiter in Sachen ePass sieht [BMI 2005c]. Österreich betrachtet sich als „Musterschüler“, da das Kompetenzzentrum des deutschen Infineon Konzerns in Graz liegt und die RFID-Technik der holländischen Philips AG im österreichischen Gratkorn entwickelt wird [DP 2005]. Die Bundesdruckerei hätte sicherlich nicht wesentlich weniger von der Einführung des ePasses profitiert, wenn dieser den EU-Vorgaben entsprechend ein wenig später eingeführt würde. So lässt sich die Einführung des ePasses insgesamt mit wirtschaftlichen Vorteilen begründen. Eine Einführung zum 1. November 2005 aber eher nicht. Die Vorgaben aus den USA können ebenfalls nur bedingt als Argument gelten. Abgesehen davon, dass die USA einen biometrischen Reisepass mittlerweile erst zu Oktober 2006 vorschreiben [BioPII 2005 S.7], hätte man den Weg der Schweiz gehen können. Die Schweiz stellt es ihren Bürgern vorerst frei, ob sie einen herkömmlichen oder einen biometrischen Reisepass beantragen [BORCHERS 2005b]. So können Personen, die in die USA reisen, einen ePass beantragen. Andere Personen hingegen bleiben vorerst bei ihrem nicht-biometrischen Reisepass.

Eine hohe Dringlichkeit bezüglich höherer Sicherheitsanforderungen bei Reisepässen kann ebenfalls nicht als Argument für die schnelle Einführung gelten. Eine Aufrüstung der Grenzkontrollstellen mit den notwenigen Lesegeräten beginnt erst Anfang 2006 und wird 2008 abgeschlossen sein [BSI 2005a]. Die bisherigen Reisepässe behalten ihre Gültigkeit, so dass die letzten nicht-biometrischen Reisepässe erst im Jahr 2015 ihre Gültigkeit verlieren. Es wird also noch einige Jahre dauern, bis die zusätzliche Sicherheit der ePässe greift.

5.6.4 Informationspolitik

Die offiziellen Informationsseiten zum ePass [BMI 2005a-e] [BSI 2005a-c] [BUND 2005] vermitteln den Eindruck, es handele sich um eine ausgereifte und risikofreie Technologie. So spricht beispielsweise das Bundesministerium des Inneren von „technisch perfekten Lösungen“ die „ausreichend getestet“ seien [CCC 2005].

Zur gleichen Zeit ergibt eine Studie des Bundesamtes für Sicherheit in der Informationstechnik, „dass der Einfluss von Alterungseffekten auf die Erkennungsleistung Biometrischer Systeme bisher noch nicht ausreichend untersucht ist“ und „vor dem Echtbetrieb in einer konkreten Anwendung eine gründliche Untersuchung der Funktionstüchtigkeit, der Erkennungsleistung und der Überwindungssicherheit sinnvoll und notwendig“ erscheint.

Auf einer Informationsseite zum ePass suggeriert das BSI, ein Lesen der Daten des ePasses sei – wenn überhaupt - nur bis zu einer Entfernung von höchstens 15cm möglich:

> *Ein aktives Auslesen über diese Entfernung* [10cm] *hinaus ist beim für den Reisepass verwendeten RF-Chip durch das Erhöhen der vom Lesegerät verwendeten Feldstärke maximal noch bis ca. 15 cm möglich. Darüber hinausgehende Lesereichweiten sind aufgrund physikalischer Gesetzmäßigkeiten nicht realistisch.* [BSI 2005a]

Unerwähnt bleibt die von Mitarbeitern des BSI durchgeführte Studie [FK 2004], die zeigt, dass das passive Mitlesen einer Kommunikation bis zu einem Abstand von 2 Metern „ohne weiteres“ möglich ist.

5.6.5 Politische Herausforderungen

Auf politischer Ebene ergeben sich neue Herausforderungen. So muss jedes Land mit ihrer PKI regeln, welche anderen Länder Zugriff auf die optionalen biometrischen Merkmale wie den Fingerabdruck erhalten. Solange es sich nicht um eindeutige ‚Schurkenstaaten' handelt, wird es der Politik wohl schwer fallen, einem bestimmten Land den Zugriff zu verweigern, wenn es keine politischen Spannungen wünscht.

Damit stellt sich die Frage, wie verhindert werden kann, dass andere Länder mit den biometrischen Daten der Einreisenden nicht so umgehen, wie es vom ausstellenden Land gewünscht wird. Dass also beispielsweise die Fingerabdrücke deutscher Reisender bei der Einreise in die USA nicht in zentralen Datenbanken gespeichert werden. Dieses Problem ist allerdings nicht nur auf den ePass bezogen, schließlich könnten und wollen die USA auch ohne ePass jedem Einreisenden die Fingerabdrücke abnehmen und speichern [HEISE 2005c]. Durch den ePass wird der Aufwand des Auslesens aber stark verringert und eine Weiterverarbeitung der Daten auch für andere Staaten attraktiver.

5.6.6 Zusammenfassung

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.

5.7 Zusammenfassung

Dieser Teil des Buches ist in diesem Auszug nicht enthalten.