Jöran Beel & Béla Gipp

ePass - der neue biometrische Reisepass

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

ISBN 3-8322-4693-2

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/

Wir danken

Bundesamt für Sicherheit in der Informationstechnik
Michael Dickopf
Dr. Marian Margraf
Fabian Schelo

Bundesdruckerei GmbH
Dipl.-Ing. Ute Eberspächer

Bundesregierung
Ulla Burchardt, SPD

EMPA Zürich
Dipl.-Ing. Peter Jacob

Fraunhofer Institut Berlin
Dipl.-Ing. Jan Krissler

Otto-von-Guericke Universität Magdeburg
Dr. Martina Engelke

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Dr. Thilo Weichert

Weitere
Felix Alcala
Stefanie Deichsel
Anja Gipp
Christian Hentschel
Birgit Lautenbach
Ivo Rössling

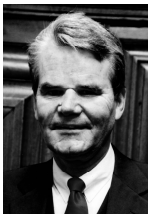
Inhaltsverzeichnis

Abkürzungen

BAC	Basic Access Control Sicherheitsmechanismus um den Datenschutz zu gewährleisten
BioPII	Studie des BSI zur Leistungsfähigkeit von biometrischen Verifikationssystemen
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
ECDSA	Elliptic Curve Digital Signature Algorithm Verschlüsselungsalgorithmus den Deutschland im ePass einsetzt
ePass	Elektronischer Reisepass Ein Reisepass auf dem biometrische Merkmale wie Gesicht und Finger elektronisch gespeichert werden
FAR	False Acceptance Rate Wahrscheinlichkeit, dass ein Biometrisches System einen Benutzer fälschlicherweise akzeptiert
FRR	False Rejection Rate Wahrscheinlichkeit, dass ein Biometrisches System einen Benutzer fälschlicherweise zurückweist
FTE	Failure To Enrole Prozentualer Anteil der Personen. bei denen ein biometrisches Merkmal nicht enrolt werden kann
ICAO	International Civil Aviation Organization Verantwortliche Organisation für die Empfehlungen, auf deren Basis der ePass entwickelt wurde
MRZ	Machine Readable Zone Der Bereich eines Reisepasses, welcher maschinenlesbar ist

RF-Chip	Radio Frequency Chip Ein Bestandteil von RFID
RFID	Radio Frequency IDentification Eine Methode zum kontaktlosen Speichern und Lesen von Daten auf einem Mikrochip. Wird häufig zum Identifizieren von Objekten genutzt.

Vorwort von Henning Arendt



Der ehemalige IBM-Manager Dipl.-Ing. Henning Arendt beschäftigt sich als Inhaber der @bc® Arendt Business Consulting und Projektleiter von BioTrusT intensiv mit der Biometrie sowie deren Eignung für die neuen Reisepässe.

Deutschland führt zum 1. November als einer der ersten Staaten den elektronisch lesbaren Pass ein, bei dem das Gesichtsbild und die Pass-Referenzdaten auf einem im Pass integrierten Chip abgespeichert sind. Die Daten lassen sich daraus nur mit einem für die Behörden verfügbaren Sicherungsverfahren auslesen, wenn der Pass auf ein spezielles Lesegerät gelegt wird.

Man stelle sich die gewaltige Herausforderung vor: ein ausgegebener ePass soll innerhalb seiner Gültigkeitsdauer von üblicherweise 10 Jahren in 189 Ländern (Anzahl der ICAO-Mitgliedsstaaten) biometrische Identifikation ermöglichen.

Seit Jahren wirke ich aktiv in nationalen und internationalen Projekten mit, bei denen es um die zuverlässige, aber auch für den Benutzer komfortable Identifizierung durch biometrische Verfahren geht. Seit 1999 nutzt auch meine Familie biometrische Verfahren im täglichen Gebrauch: als Zutrittssicherung zu unserem Haus und als Zugang zu Informationen. Ich leitete seit 1999 das mehrjährige Projekt BioTrusT (gefördert durch das Bundeswirtschaftsministerium, die Sparkassenorganisation und TeleTrusT), bei dem wir alle wesentlichen

biometrischen Verfahren auf die breite Nutzungsmöglichkeit im Banken-Umfeld untersucht haben.

Im Rahmen von BioTrusT entstanden die inzwischen international verbreiteten Empfehlungen des Daten- und Verbraucherschutzes für den Einsatz der Biometrie. Dazu gehört die Kontrolle der biometrischen Daten durch den Benutzer, wie sie jetzt auch im ePass durch deutsche Initiative realisiert wurde. Jeder hat seine biometrischen Daten im Pass, nicht in einem zentralen Datenspeicher.

Durch deutsche Initiative wurde auch die Verschlüsselung der elektronisch im Pass gespeicherten Referenzdaten international akzeptiert und in dieser ersten Stufe implementiert. Die erste Stufe, bei der lediglich das Bild zusätzlich elektronisch auslesbar im ePass verfügbar ist, ist sicherlich weniger kritisch, da ein Foto ja auch bisher schon in jedem Ausweisdokument für jeden erkennbar vorhanden ist.

Mit dem eingesetzten Verschlüsselungsverfahren soll verhindert werden, daß Unbefugte dieses elektronisch gespeicherte Bild, das dem Foto entspricht, auslesen können. Die nächste Stufe, in der Fingerabdruckdaten elektronisch gespeichert werden, erfordert weitaus höhere Hürden, um diese für einen Menschen einzigartigen Referenzdaten zu schützen. Anders als bei dem Gesichtsbild, sind die Fingerprint-Referenzdaten bisher nicht erfaßt worden.

Der Schutzwürdigkeit dieser persönlichen Daten sollte allen, die Verantwortung für den ePass tragen, bewußt sein. Der volkswirtschaftliche Schaden wäre enorm, wenn Unbefugte an die Referenzdaten von bestimmten Personen kämen und sich so die biometrische Identität von Bürgern beschaffen könnten. Das gilt besonders natür-

lich auch für die unzähligen Zutritts- und Zugangssysteme in Firmen und Behörden mit Fingerbild-Erkennungssystemen, die genutzt oder geplant werden.

Historisch hat es sich gezeigt, daß nur die kritische Auseinandersetzung dazu führt, bessere Systeme zu entwickeln. Damit hat sich die deutsche Industrie bisher hervorragend international positionieren können.

Deswegen empfehle ich dieses Buch allen, die sich als mündige Bürger informieren wollen, besonders aber den Verantwortlichen für die nächsten Stufen des ePasses. Vielleicht kann es dazu beitragen, deutsche Sicherheitstechnologien und speziell biometrische Lösungen besser international durchzusetzen.

Daher freut es mich, daß Ihnen die jungen und kompetenten Autoren dieses Buchs schon wenige Wochen vor Einführung des ePasses einen solchen tiefen, aber auch kritischen Einblick in die Details ermöglichen. Ich würde mich freuen, wenn die kritische Auseinandersetzung zu besseren biometrischen Systemlösungen führen würden, die weltweit eingesetzt werden und den Bürgern komfortables Reisen ermöglichen: ein weiterer wichtiger Beitrag des Biometrie-Standorts Deutschland.

Henning Arendt

Über die Autoren

Jöran Beel[1] und Béla Gipp[2] studierten Wirtschaftsinformatik an der Otto-von-Guericke Universität in Magdeburg. Der Schwerpunkt ihres Studiums lag in der IT-Sicherheit und biometrischen Anwendungssystemen. Beide Autoren besitzen mehrjährige berufliche Erfahrung in diesen Bereichen und arbeiteten mit Unternehmen wie Siemens oder der AOK zusammen. Béla Gipp arbeitet zudem für die Working Group ISO/IEC JTC1/SC17/WG8 welche sich mit der Normung von RFID-Technik beschäftigt.

Dieses Buch stellt die dritte Publikation von Jöran Beel und Béla Gipp dar. Für ihre bisherigen wissenschaftlichen Arbeiten erhielten die Autoren zahlreiche Auszeichnungen. Unter anderem von der Heinz und Gisela Friederichs Stiftung für „außerordentliche Leistungen auf dem Gebiet der Technik“ und von Bundeskanzler Gerhardt Schröder für „herausragende wissenschaftliche Leistungen“. Auf Einladung der Bundesministerin für Bildung und Forschung, Edelgard Bulmahn, stellten Jöran Beel und Béla Gipp ihre Forschungsergebnisse auf der Hannovermesse 2003 vor.

[1] http://www.beel.org
[2] http://www.gipp.com

1. Einleitung

Zum 1. November 2005 wird in Deutschland ein elektronischer Reisepass eingeführt. Im Vergleich zu dem bisherigen Reisepass werden zusätzlich das Gesichtsbild und später auch die Fingerabdrücke in digitaler Form gespeichert. Der Name des neuen Reisepasses lautet ‚ePass'. Die Einführung des ePasses basiert auf einer Entscheidung des Rates der EU. Diese Entscheidung sieht vor, dass spätestens ab Mitte 2006 alle Mitgliedsstaaten nur noch elektronische Reisepässe ausstellen dürfen.

Ein elektronischer Reisepass wird sich äußerlich wenig von den bisherigen Pässen unterscheiden. Zusätzlich zu dem Papierteil wird er einen Radio Frequency Chip enthalten. Auf diesem werden die digitalen Daten des Gesichts und der Finger gespeichert. Zudem ermöglicht er, dass die Daten kontaktlos an ein Lesegerät bei der Grenzkontrolle übertragen werden können. Dort kann dann, zur Unterstützung der Grenzbeamten, eine automatische biometrische Erkennung erfolgen. Diese vergleicht die in dem Reisepass gespeicherten Daten mit der sich ausweisenden Person.

Im Grunde ändert sich an dem bisherigen Ausweisverfahren wenig. Bisher führten die Grenzbeamten einen Vergleich des Passfotos mit dem Gesicht des vermeintlichen Passinhabers durch. Zukünftig wird dies zusätzlich computergestützt geschehen, wobei neben dem Gesichtsbild auch die Fingerabdrücke mit einbezogen werden.

Dennoch kritisieren einige Datenschützer und Sicherheitsexperten die Einführung des ePasses. Sie sehen die Gefahr, dass Unbefugte

die Daten aus den Reisepässen unbemerkt auslesen können. Auch die unklaren Kosten werden kritisiert sowie Ungewissheit ob die Leistungsfähigkeit Biometrischer Erkennungssysteme ausreicht, um die reibungslose Funktionalität des ePasses zu gewährleisten.

Dieses Buch gibt in sechs Kapiteln einen umfassenden Überblick über den ePass, dessen Einführung zum 1. November 2005 geplant ist, und beschäftigt sich ebenfalls mit der Kritik. Das 1. Kapitel ist diese Einleitung. Im 2. Kapitel werden Informationen zum bisherigen Reisepass gegeben. Das 3. Kapitel erläutert den ePass in seiner grundsätzlichen Funktionalität und den geplanten Verlauf der Einführung. Weitere Details, mit Schwerpunkt auf den biometrischen Merkmalen und den Sicherheitsaspekten, werden in Kapitel 4 behandelt. Kritische Punkte wie Möglichkeiten zum Umgehen der Sicherheitsmaßnahmen, Probleme bei der Zuverlässigkeit Biometrischer Systeme oder der Haltbarkeit des ePasses werden in Kapitel 5 behandelt. Kapitel 6 gibt einen zusammenfassenden Überblick.

Die Informationen in diesem Buch basieren im Wesentlichen auf den folgenden Dokumenten:

> [ICAO 2004a-i]
> Die Internationale Zivilluftfahrt-Organisation (ICAO) hat eine Empfehlung für elektronische Reisepässe mit biometrischen Merkmalen veröffentlicht. Diese Empfehlung, die aus mehreren Dokumenten besteht, ist laut EU-Ratsbeschluss [EU 2004] die Grundlage für die Entwicklung und Einführung des ePasses in Europa.

[BMI 2002a-b/2005a-i] & [BSI 2003a-b/2004a-b/2005a-c]
Die Dokumente des Bundesministeriums des Innern (BMI) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) enthalten grundlegende Informationen zum ePass und dessen Einführung in Deutschland.

[BIOPII 2005]
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in Zusammenarbeit mit dem Bundeskriminalamt (BKA) und der secunet GmbH die Studie „Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II“ herausgegeben. Diese Studie beschäftigt sich mit der Eignung der biometrischen Merkmale Gesicht, Finger und Iris in Bezug auf deren Verwendung in elektronischen Reisepässen. Der Schwerpunkt der Studie lag darin, zu untersuchen, inwieweit eine zuverlässige Verifikation mit den genannten Merkmalen möglich ist. Zudem wurde die Akzeptanz und Benutzbarkeit untersucht. Zwar war die in der Studie untersuchte Testpopulation nicht repräsentativ für die deutsche Bevölkerung [BIOPII 2005 S.56], dennoch kann sie als guter Anhaltspunkt dienen, da die Vorgaben der ICAO als Rahmenbedingungen genommen wurden [BIOPII 2005 S.10]. Insgesamt nahmen rund 2000 Personen an der Studie teil [BIOPII 2005 S.51].

[UKPS 2005]
Der „UK Passport Service“ (UKPS) hat in Kooperation mit dem „Home Office Identity Cards Programme“ und der „Driver and Vehicle Licensing Agency“ (DVLA) mit 10.000 Teilnehmern von April bis Dezember 2004 eine Studie

> durchgeführt. Diese Studie, der „Biometrics Enrolment Trial“, untersuchte, wie ausgereift Biometrische Systeme sind. Dabei wurde der Schwerpunkt auf das Enrolment und die Verifikation gelegt. Zudem wurde untersucht, inwieweit Menschen mit Behinderungen für die Teilnahme an Biometrischen Systemen geeignet sind. Die Studie ist nicht repräsentativ für die Bevölkerung Großbritanniens [UKPS 2005 S.8].

Die Dokumente werden an entsprechender Stelle referenziert, ebenso wie weitere Quellen, die sich gesammelt im Literaturverzeichnis befinden.

Auf Abbildungen des ePasses muss in diesem Buch leider verzichtet werden. Die Rechte sämtlich bisher verfügbarer Bilder liegen bei dem Bundesministerium des Innern und dieses hat eine Nutzung der Bilder in diesem Buch ausdrücklich untersagt.

2. Der aktuelle Deutsche Reisepass

2.1 Einleitung

In diesem Buch ist die Frage nach der Sicherheit des aktuellen deutschen Reisepasses und der daraus resultierenden Notwendigkeit für ein neues System von Belang. Die Fragen der Datensicherheit – wichtig für den Staat – und des Datenschutzes – wichtig für den Passinhaber – sollen in diesem Kapitel erörtert werden. Nach einer kurzen Einleitung mit allgemeinen Informationen zu dem aktuellen Reisepass wird die Datensicherheit des Reisepasses betrachtet. Dann folgt eine Analyse des Datenschutzes und in der darauf folgenden Zusammenfassung eine erste Einschätzung der Sicherheit des aktuellen Reisepasses und der Notwendigkeit eines neuen Reisepasses.

2.2 Grundlegende Informationen

Mehr als 65 Millionen Exemplare des roten deutschen Reisepasses produzierte die Bundesdruckerei[3] seit seiner Einführung 1988 [BMI 2005a]. Das auch als Europapass bezeichnete Dokument besitzt eine Gültigkeit von 10 Jahren. Wenn das Alter des Antragstellenden 26 Jahre unterschreitet, ist die Gültigkeit auf 5 Jahre beschränkt [AA 2005a].

Personenbezogene Informationen über den Passinhaber werden derzeit sowohl in maschinenlesbarer (OCR) als auch von Menschen lesbarer Schrift auf dem Reisepass festgehalten. Der so genannte vorläufige Reisepass, mit einjähriger Gültigkeit, war bisher nicht

[3] http://www.bundesdruckerei.de

maschinenlesbar, wird dies aber ab dem 1. Januar 2006 sein [AA 2005b]. Allerdings werden nicht gleich alle Behörden in der Lage sein, diese Dokumente auszustellen [AA 2005a].

Neben Unterschrift und Lichtbild werden die folgenden Informationen zur Identifizierung des Passinhabers gespeichert [PaßG 1986, §4]:

- Familienname und ggf. Geburtsname
- Vornamen
- Doktorgrad
- Ordensname/Künstlername
- Tag und Ort der Geburt
- Geschlecht
- Größe
- Farbe der Augen
- Wohnort
- Staatsangehörigkeit

2.3 Datensicherheit

Für den Staat spielt die Datensicherheit des Reisepasses eine wichtige Rolle. Die Daten des Reisepasses bzw. der Reisepass selbst sollen möglichst nicht oder nur unter hohem Aufwand gefälscht werden können. Nur so kann die Gefahr eines Passmissbrauchs, beispielsweise zur Einreise unter falscher Identität, gesenkt werden. Seit November 2001 beinhaltet der Reisepass acht zusätzliche und komplett neu entwickelte Sicherheitsmerkmale, welche durch die Bundesdruckerei und das Deutsche Kriminalamt erarbeitet wurden [BMI 2002a] & [BDR 2005b].

Die neuen Merkmale sind:

1. Holographisches Portrait
2. 3D-Bundesadler
3. Kinematische Bewegungsstrukturen
4. Makroschrift und Mikroschrift
5. Kontrastumkehr
6. Holographische Wiedergabe der maschinenlesbaren Zeilen
7. Maschinell prüfbare Struktur
8. Oberflächenprägung

Die folgenden drei Sicherheitsmerkmale wurden von dem alten Reisepass übernommen:

9. Sicherheitsdruck mit mehrfarbigen Guillochen
10. Laserbeschriftung
11. Wasserzeichen

Aufgrund der genannten Sicherheitsmerkmale gilt der deutsche Reisepass weltweit als eines der sichersten und am schwersten zu fälschenden Reisedokumente [BMI 2005a], [BMI 2005b]. In einem Interview mit dem Spiegel äußert sich Deutschlands derzeitiger Innenminister Otto Schily, der maßgeblich an der Einführung des ePasses beteiligt ist, dahingehend, dass es eine ganze Reihe von Fälschungen deutscher Ausweise und Reisepässe gebe [SPIEGEL 2001]. Konkret wurden im Jahr 2002 von der Grenzschutzdirektion 7700 Reisepässe untersucht [BUND 2005]. Dabei waren 290 Pässe Totalfälschungen aus EU-Staaten (93 aus Nicht-EU-Staaten), 394 Pässe inhaltlich veränderte Originalpässe aus EU-Staaten (1086 aus Nicht-EU-Staaten) und in 91 Fällen handelte es sich um entwendete

Blankovordrucke von Reisepässen, wobei hier keine Unterscheidung zwischen EU und Nicht-EU-Staaten vorliegt. Bei den 35 untersuchten deutschen Reisepässen handelte es sich hauptsächlich um Fälschungen vorläufiger Pässe, also nicht um Fälschungen des normalen Reisepasses, genaue Zahlen darüber fehlen jedoch. Wie das Bundeskriminalamt feststellte, liegt der Schwerpunkt gefälschter Pässe auf denen der Länder Italien, Frankreich, Spanien, Griechenland, Portugal und Belgien [BMI 2005b]. Bei diesen Zahlen handelt es sich nur um die Daten der Grenzschutzdirektion. Laut Otto Schily sollen die Strafverfolgungsbehörden in Deutschland eine nennenswerte Zahl weiterer Fälschungen sichergestellt haben [SPIEGEL 2001]. Darunter seien auch Fälschungen deutscher Reisepässe.

Der Schluss liegt nahe, dass zumindest auf europäischer Ebene ein Verbesserungspotenzial bezüglich der Fälschungssicherheit besteht.

2.4 Datenschutz

Das Paßgesetz [PaßG 1986] und die Meldegesetze der jeweiligen Bundesländer verpflichten die Bürger, ihre personenbezogenen Daten bei der zuständigen Meldebehörde anzugeben. Das Bundesdatenschutzgesetz sieht vor, personenbezogene Daten direkt bei dem Betroffenen zu erheben und zwar mit seiner Kenntnis [BDSG 2003, §4]. Zudem muss der Betroffene selbst über die Preisgabe und Verwendung seiner Daten entscheiden können [BVerfGE 1983, S.43ff]. Dazu gehört auch, dass die Daten nicht heimlich erhoben bzw. von unbefugten Dritten gelesen und verwendet werden können [ULDSH 2003].

Um den Datenschutz beim Reisepass zu gewährleisten, bestimmt das Paßgesetz [PaßG 1986, §16], dass die personenbezogenen Daten des Passinhabers nur bei der zuständigen Passbehörde gespeichert werden dürfen – und im Pass selbst. Eine Speicherung an anderer Stelle ist unzulässig und auch die Bundesdruckerei GmbH – Hersteller der Reisepässe – ist verpflichtet, die Daten umgehend nach der Passerstellung zu löschen. Allerdings ist es der Bundesdruckerei gestattet, eine zentrale Datenbank mit den eindeutigen Seriennummern der Reisepässe zu führen, wenngleich „ausschließlich zum Nachweis des Verbleibs der Pässe“ [PaßG 1986, §16]. Diese Datenbank kann zusätzlich von der jeweils zuständigen Passbehörde und Polizeibehörden des Bundes und Landes verwendet werden (Details siehe [PaßG 1986, §16]).

Unbefugtes Auslesen der Daten durch Dritte scheint nur schwer möglich. Der Passinhaber behält die Kontrolle über seine Daten, sofern er den Pass nicht verliert oder aus den Händen gibt und sich die offiziell berechtigten Stellen (siehe vorheriger Absatz) an die geltenden Gesetze halten.

2.5 Zusammenfassung

Der aktuelle deutsche Reisepass ist eines der fälschungssichersten Ausweisdokumente der Welt. Der Datenschutz wird bei den deutschen Reisepässen gewährleistet. Fälschungen von Reisepässen anderer, auch europäischer Länder kommen allerdings häufiger vor. Die Forderung nach einer Erhöhung der Sicherheit auf europäischer Ebene scheint somit grundsätzlich gerechtfertigt.

3. Der ePass – eine allgemeine Betrachtung

3.1 Einleitung

Zur Erhöhung der Dokumentenbindung zwischen Passinhaber und Reisepass sowie der Fälschungssicherheit führen die Mitgliedsstaaten der EU und ein paar weitere Länder einen elektronischen Reisepass ein. Dieser wird die biometrischen Merkmale Gesicht und Finger des Passinhabers enthalten. Die erhöhte Fälschungssicherheit und Dokumentenbindung sollen unter anderem ein wirksames Mittel gegen den Terrorismus, Organisierte Kriminalität und illegale Einwanderer darstellen. Dieses Kapitel gibt einen Überblick über die Grundlagen des ePasses, dessen Ziele und Einsatz in der Praxis. Abschließend erfolgt eine Zusammenfassung.

3.2 Grundlagen

Am 13. Dezember 2004 beschloss der Rat der Europäischen Union die Einführung eines neuen Reisepasses – verbindlich für alle Mitgliedsstaaten der EU [EU 2004]. Kernpunkt der Verordnung ist die Pflicht zur elektronischen Speicherung biometrischer Daten in den Reisepässen – konkret die Daten des Gesichts und der Fingerabdrücke. Dabei sollte sich an die Empfehlungen der Internationalen Zivilluftfahrt-Organisation (ICAO[4]) gehalten werden. Deutschland ist in der ICAO durch das Innenministerium vertreten, mit technischer Unterstützung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt (BKA) [BMI 2005d].

[4] http://www.icao.org

Während die ICAO empfiehlt, nur das Gesichtsbild verbindlich zu speichern und weitere biometrische Merkmale wie Fingerabdrücke oder Iris optional [ICAO 2004e S.15], sieht die EU Verordnung vor, dass alle Mitgliedsstaaten ab Mitte 2006 das Gesichtsbild speichern und ab Anfang 2008 zusätzlich Fingerabdrücke [EU 2004]. Das Bundesministerium des Innern begründet die Entscheidung der EU wie folgt

> *„Die Festlegung der EU auf zwei biometrische Merkmale war erforderlich, um Flexibilität bei der Kontrolle zu ermöglichen. An Stellen, an denen die Gesichtserkennung nicht praktikabel ist (z.B. bei schlechten Beleuchtungsverhältnissen oder bei Massenandrang), soll eine Verifikation durch Fingerabdrücke möglich sein"* [BMI 2005e].

Neben den Mitgliedern der EU werden auch Japan, die USA, Australien, Russland und die Schweiz Pässe entsprechend der ICAO Empfehlung ausstellen [BMI 2005c].

Deutschland wird den ePass früher einführen, als es die Verordnung der EU vorsieht. Am 8. Juli 2005 billigte der Bundesrat als letzte Instanz die Entscheidung der Bundesregierung, bereits ab dem 1. November 2005 ausschließlich biometriegestützte Reisepässe auszugeben [BR 2005]. Auf diesen wird in erster Stufe das Gesichtsbild des Passinhabers in elektronischer Form gespeichert. Dieses Bild soll identisch mit dem auf dem Datenblatt gedruckten Foto sein [ICAO 2004d S.33]. Digitale Fingerabdrücke werden dann ab März 2007 in die Reisepässe aufgenommen [BMI 2005c]. Es ist nicht vorgesehen, die Fingerabdrücke auch in den Papierteil des ePasses zu drucken[5].

[5] Laut telefonischer Auskunft des BSI

Alte Reisepässe ohne biometrische Merkmale und ePässe lediglich mit elektronisch gespeichertem Gesichtsbild behalten ihre zehnjährige Gültigkeit, auch wenn neue Pässe ab 2007 nur noch mit Gesichtsbild und Fingerabdruck ausgegeben werden [EU 2004, Artikel 6]. Die notwendigen Änderungen der Gesetze zur Aufnahme biometrischer Merkmale in den Reisepass erfolgten bereits im Jahr 2002 im Rahmen des Terrorismusbekämpfungsgesetzes [BMI 2002b]. Eine flächendeckende Ausstattung der Grenzposten mit entsprechenden Lesegeräten soll Anfang 2006 beginnen und bis 2008 abgeschlossen sein [BSI 2005a].

Laut EU-Beschluss [EU 2004] darf jedes Land die Reisepässe nur von einer Stelle produzieren lassen. Diese Stelle ist in Deutschland die Bundesdruckerei GmbH. Die Philips AG und Infineon Technologies AG liefern dabei die RF-Chips, auf denen die biometrischen Daten gespeichert werden [BMI 2005c]. Das BSI und das BKA unterstützten die Bundesdruckerei bei der Entwicklung der Sicherheitsstandards [BMI 2005d]. Die Flexsecure AG stellt die Software für den Betrieb der Country Signing Certification Authority (CSCA) zur Verfügung. Wer die Lesegeräte für die Passkontrolle produziert, ist uns nicht bekannt (vgl. Kapitel 5.4.7).

Von verschiedenen Seiten gibt es starke Kritik an der Einführung des ePasses. Dabei wird unter anderem die Art der Entscheidungsfindung sowohl auf europäischer als auch auf Bundesebene kritisiert. Kapitel 5.6.3 setzt sich mit dieser Kritik auseinander.

3.3 Ziele des ePasses

Durch das Speichern biometrischer Merkmale im Reisepass soll die Dokumentenbindung zwischen einer Person und ihrem Reisepass verstärkt werden [BSI 2005c]. Es kann somit mit höherer Wahrscheinlichkeit gesagt werden, ob eine Person wirklich die Person ist, welche in dem Reisepass ausgewiesen wird. In Kombination mit digitalen Signaturen wird zudem die Fälschungssicherheit der Pässe erhöht [BSI 2005c]. Durch höhere Dokumentenbindung und Fälschungssicherheit wird es schwerer, sich eine falsche Identität zu verschaffen und damit beispielsweise unberechtigt nach Deutschland einzureisen. So soll der ePass ein wirksames Mittel gegen den Terrorismus, das Organisierte Verbrechen und illegale Einwanderer darstellen [BMI 2002b]. Da der ePass europaweit eingeführt wird, verstärkt sich der Zugewinn an Sicherheit nochmals, da bisher überwiegend Pässe aus dem europäischen Ausland gefälscht wurden [BMI 2005b]. Für „vertrauenswürdige Personen“ ergibt sich zudem ein Zeitgewinn bei der Grenzkontrolle [BMI 2005b].

Der derzeitige Bundesinnenminister Otto Schily erwähnt in [BMI 2005c] eine Stärkung der deutschen Wirtschaft und die Möglichkeit zu zeigen, „dass Deutschland das Know-how und die Innovationskraft hat, um im jungen Sektor Biometrie Standards zu setzen.“. Eine Studie der Europäischen Kommission führt weiterhin auf, dass ein erfolgreiches Nutzen der Biometrie im ePass dazu führt, dass Ängste in der Bevölkerung gegenüber der Biometrie abgebaut werden [EU 2005]. Damit würde sich die Biometrie schneller in anderen Bereichen des Lebens durchsetzen. Es scheint plausibel, dass gleiches für den Einsatz von RFID gilt, welches als Speichermedium und zur Datenübertragung in den ePässen dienen wird. Umgekehrt liegt der

Schluss nahe, dass größere Probleme bei der Einführung des ePasses dazu führten, dass Ängste und Vorbehalte in der Bevölkerung gegenüber der Biometrie und RFID verstärkt würden und ein Schaden für die Wirtschaft entstünde. Eine Betrachtung, inwieweit eine hohe Verbreitung von Biometrie oder RFID in anderen Bereichen als elektronischen Ausweisdokumenten überhaupt wünschenswert ist, ist nicht Gegenstand dieses Buches.

Ob die Ziele, die laut Otto Schily im „ureigenen deutschen Interesse" [BMI 2005b] liegen, tatsächlich mit der Einführung des ePasses erwartungsgemäß erreicht werden, wird von manchen Kritikern bezweifelt (siehe auch Kapitel 5).

3.4 Der ePass in der Praxis

Der deutsche ePass wird sämtliche Sicherheitsmerkmale des alten Reisepasses behalten[6]. Zusätzlich wird er einen Radio Frequency Chip (RF-Chip) enthalten [BSI 2005a]. Dieser dient als Speichermedium und zur Datenübertragung für das Gesichtsbild und zwei Fingerabdrücke des Passinhabers. Zudem werden die bisherigen Daten des Reisepasses wie Wohnort und Geburtsdatum auf dem Chip gespeichert [BSI 2005b]. RF-Chips sind von der Funktionsweise mit den Chips auf Geldkarten oder Telefonkarten vergleichbar, lassen sich aber kontaktlos auslesen. Welche Daten im Detail auf dem Chip gespeichert sind, lässt sich durch den jeweiligen Passinhaber – entsprechend der EU Verordnung [EU 2004] – jederzeit in der Meldestelle mit dort aufgestellten Lesegeräten überprüfen.

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

Für den Bürger wird sich auf den ersten Blick mit der Einführung des ePasses zum 1. November 2005 nicht viel ändern. Der Ablauf der Beantragung eines Reisepasses bei der zuständigen Passstelle ist quasi identisch zu dem bisherigen Ablauf. Lediglich das Passfoto muss zukünftig frontal aufgenommen sein anstatt wie bisher im Halbprofil. Diese Änderung basiert auf den Vorgaben der ICAO [ICAO 2004c] und der Tatsache, dass die automatisierte Gesichtserkennung am besten mit frontal aufgenommenen Gesichtsbildern funktioniert [BIOFACE 2003]. Eine Prüfung des Passbildes durch Mitarbeiter der Passbehörde auf ausreichend viele biometrische Merkmale soll nicht stattfinden [HEISE 2005e]. Das Passfoto soll in der Standardgröße mit einer Auflösung von mindestens 600dpi eingereicht werden.

Wie auch der bisherige Reisepass wird der ePass eine Gültigkeit von 10 Jahren aufweisen [BSI 2005a]. Die Kosten werden bei 59 Euro für den Antragssteller liegen bzw. bei 37,50 Euro für einen 5 Jahre gültigen Pass, den Personen unter 26 Jahren erhalten. Vorläufige Reisepässe mit einer Gültigkeit von weniger als 12 Monaten müssen laut EU Verordnung [EU 2004] nicht zwangsläufig mit RF-Chip und biometrischen Daten ausgestattet werden. Gleiches gilt für Personalausweise. Deutschland wird zu Anfang 2007 aber auch Personalausweise mit biometrischen Daten ausstellen [BUND 2005].

Ab März 2007 werden zwei Fingerabdrücke in neu ausgestellten ePässen gespeichert. Da der Herstellungsaufwand durch das Hinzufügen der Fingerabdrücke – durch zusätzlichen Erfassungsaufwand und erhöhte Sicherheitsanforderungen – offensichtlich steigt, scheint auch eine weitere Preissteigerung wahrscheinlich. Denn die „Ausstellungskosten für die Reisepässe werden, wie auch jetzt schon, in

vollem Umfang auf die Passgebühr umgelegt“ [BUND 2005]. Zu den Ausstellungskosten zählen die Herstellungskosten für das Passbuch, den Speicherchip, die Erfassung der biometrischen Daten und die Aufnahme derselben in den ePass [BSI 2005a]. Wie hoch die Kosten für Mitarbeiterschulungen, Lesegeräte und Einrichtung der ca. 6500 Meldestellen ausfallen werden, steht noch nicht fest, so dass die Gesamtkosten für den ePass derzeit unbekannt sind [BUND 2005].

Bei der Grenzkontrolle wird sich im Idealfall ebenfalls wenig für den Reisenden ändern. Die Kontrolle wird weiterhin von Grenzbeamten durchgeführt. Die biometrischen Merkmale werden den Grenzbeamten bei seiner Arbeit lediglich unterstützen [BUND 2005]. Auch ein ePass mit beschädigtem RF-Chip, bei dem die biometrischen Daten nicht ausgelesen werden können. wird seine Gültigkeit behalten [BSI 2005a], ebenso wie Ausweisdokumente, die vor Einführung des e-Passes ausgestellt wurden [EU 2004, Artikel 6]. Im Falle eines defekten RF-Chips muss die entsprechende Person allerdings mit einer „intensiveren“ Prüfung rechnen [CCC 2005]. Abbildung 3.4a zeigt den Ablauf einer Passkontrolle an der Grenze.

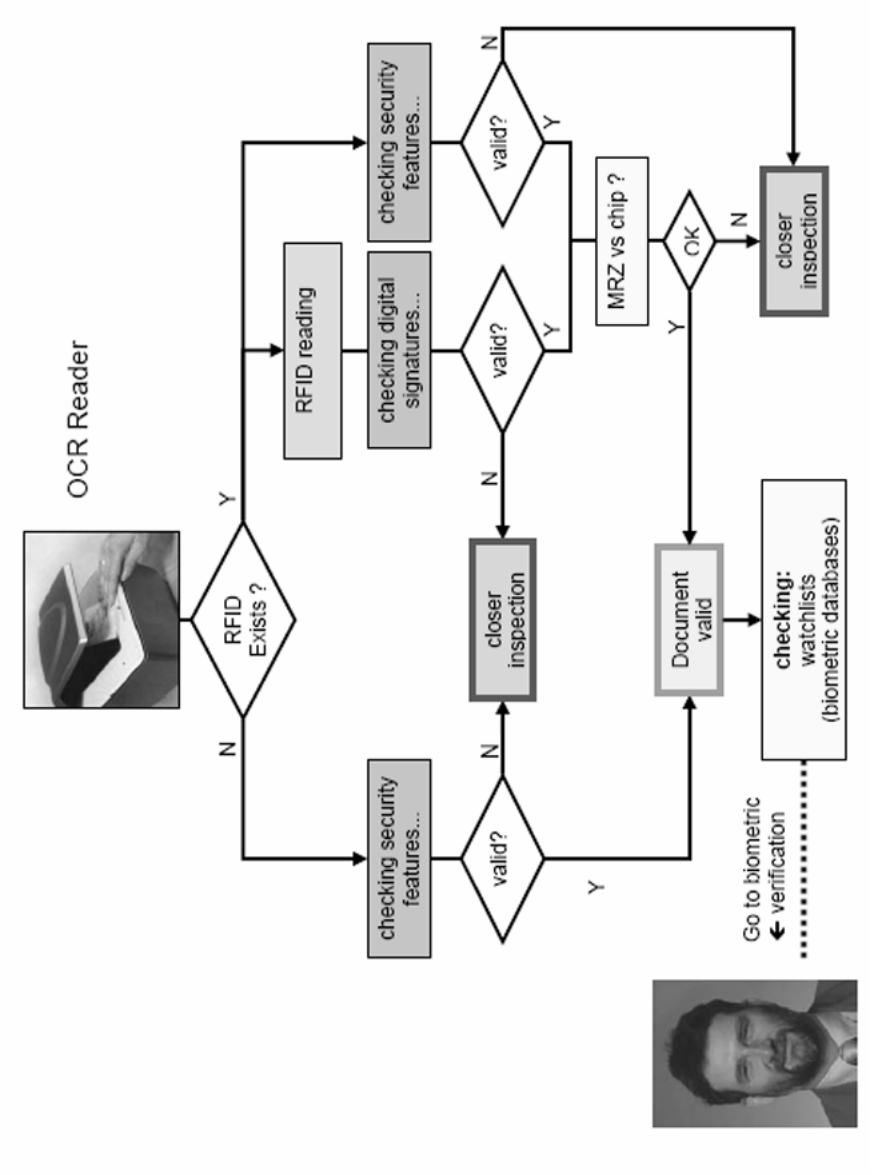


Abbildung 3.4a, Ablauf einer Passkontrolle
Übernommen aus [ICAO 2004d S.44]

Für den Schutz der Daten auf dem RF-Chip vor unbefugtem Auslesen und Mitlesen des Gesichtbildes und der Fingerabdrücke (falls zusätzlich vorhanden) hat die ICAO die beiden Verfahren Basic Access Control und Extended Access Control definiert [ICAO 2004a]. Die Basic Access Control sorgt dafür, dass die biometrischen Daten im Regelfall nur nach einem optischen Lesen der MRZ ausgelesen werden dürfen. Die Datenübertragung erfolgt dabei verschlüsselt, so dass ein unbefugtes Mitlesen der Daten nicht ohne weiteres möglich ist. Der erweiterte Zugriffsschutz auf die biometrischen Daten, die Extended Access Control, greift auf eine Public Key Verschlüsselung zurück, welche ein unbefugtes Lesen der Daten praktisch unmöglich macht. Details zum Zugriffsschutz finden sich im nächsten Kapitel. Die Empfehlung der ICAO regelt überdies, dass nur das Gesichtsbild auf dem Pass für alle Länder bei der Grenzkontrolle zugänglich sein muss. Weitere biometrische Merkmale können mittels Verschlüsselung und Zertifikaten nur für bestimmte Staaten freigegeben werden. Für welche Länder Deutschland den Fingerabdruck freigeben wird, scheint derzeit noch nicht festzustehen [CCC 2005]. Hieraus resultierende Probleme werden in Kapitel 5.6.5 behandelt.

3.5 Zusammenfassung

Zum 1. November 2005 wird in Deutschland der elektronische Reisepass, der ePass, eingeführt. Dieser wird in der ersten Stufe auf einem RF-Chip das Gesichtsbild des Passinhabers speichern. Ab März 2007 werden zusätzlich zwei Fingerabdrücke gespeichert. Der Preis wird für einen 10 Jahre gültigen Pass von 26 Euro auf 59 Euro erhöht. Sofern Einführung und Betrieb des ePasses wie geplant verlaufen, wird sich grundsätzlich für die Passinhaber wenig ändern. Kritik am ePass wird ausführlich in Kapitel 5 betrachtet.

4. Der ePass im Detail – Detaillierte Technische Funktionsweise und Biometrie

4.1 Einführung

Der ePass wird neben dem Papierteil einen RF-Chip enthalten. Dieser speichert die biometrischen Daten und sorgt für die Datenübertragung und die Verschlüsselung eben dieser Daten. Dieses Kapitel betrachtet die grundlegende Funktionsweise der RF-Chips, gibt eine Übersicht über die ausgewählten biometrischen Merkmale und deren Eignung für den Einsatz im ePass. Darauf folgt ein Überblick über die Sicherheitsmaßnahmen zum Schutz der Daten. Das Kapitel endet mit einer Zusammenfassung der wichtigsten Informationen.

4.2 RFID

Im Wesentlichen machen zwei Komponenten ein RFID-System aus: der Transponder und das Lesegerät [RFID 2002]. Der Transponder stellt den eigentlichen Datenträger dar, auf dem Daten gespeichert sind und mittels Mikroprozessor auch verarbeitet werden können.

Im Falle des ePasses ist der Transponder der in den Pass integrierte Radio Frequency Chip (RF-Chip). Auf diesem werden die biometrischen Daten gespeichert und der Mikroprozessor bietet die nötige Funktionalität, um die in den folgenden Abschnitten beschriebenen Sicherheitsfunktionen gewährleisten zu können. Die ICAO hat sich in ihrer Empfehlung für RF-Chips gemäß dem Standard ISO/IEC 14443 ausgesprochen [ICAO 2004b]. Dieser Chip arbeitet mit einer Frequenz von 13,56 MHz und bietet laut ICAO verschiedene Vortei-

le gegenüber anderen Standards und Technologien. So sei das Frequenzband um 13,56 MHz in jedem Land der Welt nutzbar. Zudem könne die Frequenz nicht durch Wasser oder einen menschlichen Körper gedämpft werden, ließe sich aber durch Metall komplett abschirmen. Chips dieses Standards sind seit vielen Jahren im Einsatz und haben sich bewährt. Außerdem bieten sie genügend Speicherkapazität, eine ausreichend hohe Datentransferrate und die Möglichkeit, mehrere Pässe gleichzeitig auszulesen. Weiterhin ermögliche die Bauart eine Implementierung in die Reisepässe, ohne deren Format grundsätzlich ändern zu müssen, und die Chips bieten genügend Leistung, um die notwendigen Verschlüsselungs- und Identifizierungsfunktionen auszuführen. Durch die geringe Lesereichweite von im Normalfall bis zu 10 cm wird zudem ein unberechtigtes Aus- und Mitlesen der Daten erschwert, im Gegensatz zu anderen Standards, deren verwendete Frequenzen und Sendeleistung ein Auslesen aus einigen Metern Entfernung ermöglichen [ICAO 2004b].

Das Lesegerät an den Grenzübergängen wird in der Lage sein, den RF-Chip mittels Induktion mit Energie zu versorgen und die Daten aus dem RF-Chip kontaktlos auszulesen. Auf eine detaillierte Darstellung der physikalischen Grundlagen wird in diesem Buch verzichtet. Diese Informationen finden sich ausführlich beschrieben in [RFID 2002]. Wichtig ist die Tatsache, dass die Kommunikation zwischen Lesegerät und Transponder (ePass) kontaktlos erfolgt und der ePass keine eigene Energiequelle wie beispielsweise eine Batterie benötigt.

Da die Daten bei RFID kontaktlos übertragen werden, besteht ein grundsätzliches Risiko, dass die Daten von nicht autorisierten Dritten mitgelesen werden könnten. Um zu verhindern, dass Dritte die Daten

lesen können, werden diese verschlüsselt übertragen (vgl. Kapitel 4.4). An der Sicherheit der verwendeten Verschlüsselung wird von einigen Seiten Kritik geübt (vgl. Kapitel 5.5). Beispielsweise fordert der Bundesdatenschutzbeauftragte Peter Schaar, dass ein 3D Barcode anstelle der RFID Technik verwendet werden solle, um dem Datenschutz gerecht zu werden [HEISE 2005]. Tabelle 4.2a stellt die gängigsten Alternativen gegenüber.

Die ICAO hat sich in ihrer Empfehlung mit verschiedenen Alternativen auseinandergesetzt und den RFID Standard ISO 14443 – wie oben beschrieben – als für am besten geeignet befunden. Maßgeblich entscheidend war laut [ICAO 2004d S.35] die Tatsache, dass RFID als einzige Technologie die nötigen Anforderungen in den Bereichen Benutzerfreundlichkeit, Datenkapazität und Performance erfüllt. Zwar könnten kontaktbehaftete Chipkarten ähnliches leisten, allerdings bezweifelt die ICAO, dass ein kontaktbehafteter Chip auch nach 10 Jahren noch einwandfrei funktioniert, da dieser dann Verschleißerscheinungen aufweise und beispielsweise durch Oxidation die Kontakte beschädigt sein könnten. Zudem sei es schwierig bis unmöglich, diese Chips in Pässe der üblichen Bauart zu implementieren.

Tabelle 4.2a: Eigenschaften ausgewählter Auto-ID-Systeme im Vergleich

Parameter/System	Barcode	OCR	Chipkarte	RFID
Typische Datenmenge (Byte)	1 ~ 100	1 ~ 100	16 ~ 64k	16 ~ 64k
Datendichte	gering	gering	sehr hoch	sehr hoch
Maschinenlesbarkeit	gut	gut	gut	gut
Lesbarkeit durch Personen	bedingt	leicht	unmöglich	unmöglich
Einfluss von Schmutz/ Nässe	sehr stark	sehr stark	möglich (Kontakte)	kein Einfluss
Einfluss von (opt.) Abdeckung	totaler Ausfall	totaler Ausfall	möglich	kein Einfluss
Einfluss von Richtung und Lage	gering	gering	sehr hoch (eine Steckrichtung)	kein Einfluss
Abnutzung/ Verschleiß	bedingt	bedingt	bedingt	kein Einfluss
Anschaffungskosten/ Leseelektronik	sehr gering	mittel	gering	mittel
Unbefugtes Kopieren/ Ändern	leicht	leicht	schwierig	schwierig
Lesegeschwindigkeit (inkl. Handhabung des Datenträgers)	gering ~ 4s	gering ~ 3s	gering ~ 4s	sehr schnell ~ 0,5s
Maximale Entfernung zwischen Datenträger und Lesegerät	0-50cm	<1cm	direkter Kontakt	0-5m

Übernommen aus [BSI 2004 S.90]

4.3 Biometrie

4.3.1 Einleitung

Der Hauptgrund für die Einführung des ePasses liegt neben der Erhöhung der Fälschungssicherheit in der Möglichkeit, anhand der im Pass gespeicherten biometrischen Merkmale besser beurteilen zu können, ob die sich ausweisende Person tatsächlich der rechtmäßige Passinhaber ist [BSI 2005c]. In diesem Abschnitt werden biometrische Verfahren vorgestellt und deren Vor- und Nachteile für die Verwendung im ePass erläutert.

Der Begriff „Biometrie“ leitet sich ab aus den griechischen Wörtern „Bios“ (das Leben) und „Métron“ (das Maß) [DUDEN 2005]. Unter biometrischen Merkmalen eines Menschen versteht man messbare und möglichst individuelle Körpermerkmale, die sich idealerweise im Leben eines Menschen nur geringfügig verändern.

Neben den biometrischen Verfahren existieren zwei weitere Möglichkeiten zur Authentisierung von Personen. Zum einen kann man sich über Wissen, beispielsweise ein Passwort, authentisieren, und zum anderem kann dies über einen speziellen Besitz, beispielsweise einen Autoschlüssel, geschehen. In beiden Fällen erfolgt jedoch keine feste Personenbindung, was zu erleichtertem Missbrauch führen kann und daher nicht zur Verifikation des rechtmäßigen Benutzers von Ausweisdokumenten geeignet ist [BSI2005a].

4.3.2 Biometrische Verfahren im Überblick

Nicht jedes Körpermerkmal eignet sich gleichermaßen für den Zweck der biometrischen Authentifizierung. Folgende Kriterien sollten erfüllt sein [BROMBA 2005a+b]:

1. Akzeptanz: Das Verfahren sollte von den Benutzern akzeptiert sein und den Menschen nicht in seiner Würde oder Gesundheit verletzen.

2. Beständigkeit: Das biometrische Merkmal sollte sich im Laufe der Zeit nicht über einen für den eingesetzten Zweck spezifischen Toleranzbereich hinaus verändern.

3. Disponibilität: Das Merkmal sollte bei allen Benutzern vorhanden sein

4. Messbarkeit: Die Merkmale sollten mit vertretbarem technischen Aufwand erfassbar sein.

5. Einzigartigkeit: Nicht jedes Merkmal ist einzigartig. Am besten geeignet sind Merkmale, die sich in der embryonalen Phase auf der Basis von Zufallsprozessen (radotypisch) entwickelt haben. Ein Beispiel hierfür ist die individuelle Struktur der Iris oder des Fingerabdrucks, welche auch bei eineiigen Zwillingen unterschiedlich ist. Weniger gut geeignet sind Merkmale die verhaltensgesteuert und damit erlernbar oder genotypisch, also vererbbar sind. [BSI2005a]

Eine Übersicht über biometrische Merkmale, die den genannten Kriterien weitgehend entsprechen, sind in der folgenden Tabelle 4.3.2a dargestellt.

Tabelle 4.3.2a

Biometrisches Merkmal	***Beschreibung***
Fingerabdruck	Fingerlinienbild, Porenstruktur
Unterschrift (dynamisch)	Schriftzug mit Druck- und Geschwindigkeitsverlauf
Gesichtsgeometrie	Abstände der gesichtsbestimmenden Merkmale (Augen/ Nase/Mund)
Iris	Irismuster
Retina	Augenhintergrund (Muster der Adernstruktur)
Handgeometrie	Maße der Finger und des Handballens
Fingergeometrie	Fingermaße
Venenstruktur der Handrückseite	Venenstruktur der Handrückfläche
Ohrform	Abmessungen der sichtbaren Ohrbestandteile
Stimme	Klangfarbe
Geruch	Chemische Zusammensetzung der menschlichen Geruchs
Tastenanschlag	Rhythmus des Tastenanschlags (PC- oder sonstige Tastatur)

Übernommen von http://www.bromba.com

Die ICAO hält – basierend auf dem Biometrics Selection Technical Report der New Technology Working Group (NTWG) – die Merkmale Gesicht, Finger und Iris für die Nutzung in Ausweisdokumenten für geeignet [ICAO 2004d]. Die Empfehlung der ICAO sieht vor, dass die Aufnahme des digitalen Gesichtsbildes in den elektronischen Reisepass verpflichtend ist und weitere biometrische Merkmale optional [ICAO 2004e] sind. Ungeachtet dieser Empfehlung hat die EU beschlossen, nicht nur das Gesichtsbild, sondern auch die Fingerabdrücke verpflichtend für alle Mitgliedsstaaten in dem Pass zu speichern [EU 2004]. Die Aufnahme der Iris wird in dem Beschluss nicht erwähnt. Die Bundesregierung sieht derzeit von einer Aufnahme der Iris ab [BUND 2005]. Laut einem Bericht der c't befürwortet Bundesinnenminister Otto Schily langfristig allerdings eine Aufnahme der Irisdaten in den ePass [HEISE 2005f]. Auch eine Rede von Otto Schily zur Einführung des ePasses legt die Vermutung nahe, dass er die Iris als für Ausweisdokumente geeignet hält [BMI 2005b].

Im Folgenden werden die drei biometrischen Merkmale Gesicht, Finger und Iris in Bezug auf ihre Eignung für die Verwendung im ePass betrachtet. Dabei wird jedes Merkmal hinsichtlich der Disponibilität erläutert bzw. inwieweit ein Enrolment stattfinden kann hinsichtlich der Erkennungsleistung bei der Verifikation und inwieweit Faktoren wie Alter, Geschlecht oder ethnische Herkunft die Erkennungsleistung beeinträchtigen. Für alle biometrischen Merkmale gilt, dass die Auswirkung von Alterungsprozessen auf die Erkennungsleistung bisher nur unzureichend untersucht wurde [BIOPII 2005 S. 170]. Es ist damit schlecht abschätzbar, wie gut die Erkennungsleistung mit heute aufgenommenen Merkmalen in zehn Jahren sein wird. Für alle drei Merkmale gilt zudem, dass die Erkennungsleistung bei

Referenzbildern, wie von der ICAO vorgeschlagen, zum heutigen Zeitpunkt um 1 bis 2,5 Prozentpunkte schlechtere Erkennungsleistung liefert als bei der Verwendung von Templates[7] [BIOPII 2005 S.165]. Die Verwendung von Rohdaten[8] bietet aber den Vorteil, dass auf proprietäre Templates verzichtet werden kann, die unter Umständen nicht mit allen Lesegeräten kompatibel sind [ICAO 2004d]. In den folgenden Abschnitten werden die Begriffe FAR, FRR und FTE Verwendung finden. Deren Bedeutung ist wie folgt:

False Acceptance Rate (FAR): Die False Acceptance Rate gibt die relative Häufigkeit an, dass eine Person von einem Biometrischen System erfolgreich verifiziert, wird obwohl die Verifikation hätte fehlschlagen müssen, da die biometrischen Merkmale der Person nicht mit denen der Referenzdaten übereinstimmen [ICAO 2004d S.10].

False Rejection Rate (FRR): Die False Rejection Rate gibt die relative Häufigkeit an, dass eine Person von einem Biometrischen System nicht erfolgreich verifiziert wird, obwohl die Verifikation hätte erfolgreich sein sollen [ICAO 2004d S.10]

Failure To Enrol Rate (FTE): Die Failure to Enrol Rate repräsentiert die relative Häufigkeit erfolgloser Enrolments aufgrund von unzureichend ausgeprägten bzw. nicht vorhandenen biometrischen Merkmalen [SKVK 2005].

[7] Proprietäre Templates sind herstellerspezifische Datenformate, welche nur die für die Erkennung relevanten Daten beinhalten und im Vergleich zu den Rohdaten lediglich einen Bruchteil des Speicherplatzes benötigen.
[8] Rohdaten sind unbearbeitete Ausgangsdaten wie beispielsweise das Gesichtsfoto im JPEG-Format.

4.3.3 Gesichtserkennung

Ab November 2005 soll das Gesichtsbild in elektronischer Form in dem Reisepass gespeichert werden (vgl. Kapitel 3). Die ICAO sieht in der Verwendung des Gesichts als biometrischem Merkmal einige Vorteile [ICAO 2004d S.17]. So enthüllen Gesichtsfotos keine Informationen, die nicht auch sonst durch das Zeigen des Gesichts der Öffentlichkeit preisgegeben werden. Gesichtsfotos werden international für die Verwendung in Ausweisdokumenten akzeptiert. Zwischen Gesicht und Lesegerät sind kein Kontakt und keine direkte Interaktion notwenig. Zudem sind für das Enrolment in der Regel keine teuren Spezialgeräte nötig. Für die Gesichtserkennung spricht weiter, dass das Gesicht als Merkmal bei praktisch allen Menschen vorhanden ist und einfach enrolt werden kann [BIOPII 2005 S.12] & [UKPS 2005 S. 9]. In seltenen Fällen scheint es aber möglich, dass ein Enrolen des Gesichtes nicht möglich ist. Die Studie [UKPS 2005 S. 196] berichtet von einem Teilnehmer mit so dunkler Hautfarbe, dass es auch nach sieben Versuchen nicht möglich war, ein erfolgreiches Enrolment durchzuführen. Seine Haut wurde von dem System fälschlicherweise als nicht belichtete Fläche erkannt.

Gegen die Gesichtserkennung spricht, dass schon kleine Änderungen der Beleuchtungsverhältnisse zu starken Änderungen der Erkennungsleistung führen [BIOPII 2005 S.16]. Dieser Nachteil tritt nicht bei der 3D Gesichtserkennung auf. Das BSI führt Tests zu deren Praxistauglichkeit durch [BSI 2005e]. Da 3D Gesichtserkennung aber weder in den ICAO Dokumenten noch in dem Beschluss der EU Erwähnung findet, wird die 3D Gesichtserkennung in diesem Buch nicht weiter betrachtet.

Zahlen über die genaue Erkennungsleistung der Gesichtserkennung schwanken sehr stark, abhängig von der jeweiligen Studie. Während die Studie BioFace aus dem Jahre 2003 eine FRR von 50% angibt [BIOFACE 2003 S.10], kommt die Studie BioPII aus dem Jahr 2005 auf eine FRR von 2% bis 10% bei einer FAR von 0,1% [BIOPII 2005 S.12]. Dieser Unterschied kann sicherlich mit der Weiterentwicklung der Technik in den zwei Jahren erklärt werden. Die Studie der Britischen Passbehörde, ebenfalls aus dem Jahr 2005, kommt jedoch auf eine FRR von rund 31%, wobei die FAR nicht angegeben wird [UKPS 2005 S.10].

Der Einfluss der Berufstätigkeit auf die Erkennungsleistung ist unklar [BIOPII 2005 S.127]. Ein Einfluss des Geschlechts scheint weniger durch die Biometrie vorgegeben als mehr durch die verwendeten Lesegeräte bestimmt. BioPII stellte für einige Geräte eine Geschlechtsabhängigkeit fest, bei der Frauen mit einer höheren FRR rechnen mussten [BIOPII 2005 S.126]. Bei anderen Geräten konnte keine Abhängigkeit festgestellt werden. In [UKPS 2005 S. 240] konnte ebenfalls keine Abhängigkeit entdeckt werden. Der Einfluss der ethnischen Herkunft ist unklar [UKPS 2005 S. 239], ein Zusammenhang wird aber vermutet [BIOFACE 2003]. Das Alter spielt bei der Erkennungsleistung eine Rolle. So stellt [UKPS 2005 S. 241] fest, dass die Erkennungsleistung bei über 60-Jährigen abnimmt. [BIOPII 2005 S.127] spricht zwar davon, dass die Erkennungsleistung unabhängig vom Alter sei, allerdings lag der Anteil der Teilnehmer über 60 Jahren auch nur bei rund 2%, womit kaum eine allgemeingültige Aussage getroffen werden kann [BIOPII 2005 S.53].

4.3.4 Fingerabdruckerkennung

Ab März 2007 sollen zwei Fingerabdrücke in den ePass aufgenommen werden (vgl. Kapitel 3). Der Prozess der Fingerabdruckanalyse wird in der BSI-Studie „BioFinger“ in sechs Stufen unterteilt [BIOFINGER 2004]. Als erstes muss ein Abbild des Fingerabdrucks erstellt werden. Dies kann mit Hilfe eines Abdrucks z.B. auf Papier oder mit Hilfe eines Sensors erfolgen. Es existieren unter anderem kapazitiv, optisch und thermisch arbeitende Sensoren, welche verschiedene Vor- und Nachteile haben [BROMBA 2005b].

Nachdem das Bild des Fingerabdrucks digital vorliegt, wird zunächst mit Hilfe verschiedener bildverarbeitender Algorithmen die Bildqualität verbessert. Anschließend erfolgt die Bildaufarbeitung. In der Musterklassifizierung werden verschiedene Grobmerkmale wie Wirbel, Schleife oder Tanne identifiziert.

Tanne Schleife Wirbel

Abbildungen 4.3.4a/b/c, Quelle: [WATSON 2005]

In der Phase der Merkmalsextraktion werden die Fingerabdruck-Feinmerkmale, die so genannten Minuzien, lokalisiert. Diese ergeben sich aus dem Vorhandensein von Verzweigungen und Endungen. Die relative Position der Minuzien zueinander macht Fingerabdrücke für die Algorithmen einmalig und vergleichbar. Der Quantitative Faktor

gibt die Anzahl gefundener Minuzien an. In der abschließenden Verifikationsphase wird der Grad der Übereinstimmung bestimmt und je nach benutztem Schwellwert der Fingerabdruck als identisch oder nicht identisch klassifiziert.

Sowohl in [UKPS 2005 S. 221] als auch [BIOPII 2005 S.12] konnten die Fingerabdrücke von knapp 1% der Teilnehmer nicht erfolgreich enrolt werden. Die Erkennungsleistung wird in [BIOPII 2005] als sehr gut angegeben mit einer FRR von 1% bis 7% bei einer FAR von 0,1%. Auch eine etwas ältere Studie aus dem Jahr 2004 gelangte zu dem Ergebnis, dass die FRR um 2% liege bei einer FAR von 0,1% [BIOFINGER 2004 S.3]. Hingegen kommt [UKPS 2005] zu dem Ergebnis, dass die FRR rund 20% beträgt, leider ohne Angabe der FAR. Einig sind sich die beiden Studien, dass die Erkennungsleistung vom Alter der Personen abhängt [UKPS 2005 S. 249] & [BIOPII 2005 S.127]. So ist bei jungen Menschen eine geringere FRR zu erwarten, bei älteren Personen eine höhere. Auch der Alterungsprozess des Merkmals selbst scheint hoch zu sein. So soll sich die FRR bei dem Vergleich mit einem vor 10 Jahren aufgenommenen Fingerabdruck verdoppeln [BIOFINGER 2004 S.3]. Die Erkennungsleistung ist ebenfalls vom Geschlecht abhängig. Männer erzielen aufgrund ihrer größeren Hände bessere Ergebnisse [UKPS 2005 S. 251] & [NIST 2002 S.7]. Ob die Erkennungsleistung von der ethnischen Herkunft beeinflusst wird kann nicht klar gesagt werden. [UKPS 2005 S. 247] hält es für möglich.

4.3.5 Iriserkennung

Die Aufnahme der Irisdaten in den Reisepass ist derzeit nicht geplant. Die Eigenschaften werden an dieser Stelle dennoch betrachtet, da eine spätere Aufnahme als wahrscheinlich angenommen werden kann (vgl. Kapitel 4.3.2).

Die Irisstruktur eignet sich als biometrisches Merkmal, weil sie wie der Fingerabdruck radotypisch ist, also in der embryonalen Phase auf der Basis von Zufallsprozessen entwickelt und daher auch bei Zwillingen unterschiedlich ausgeprägt ist. Ein weiterer Vorteil besteht in der Komplexität der Strukturen. So lassen sich ca. 250 eindeutige Merkmale bei einem Irisscan identifizieren, was dazu führt, dass die theoretische Wahrscheinlichkeit von zwei unterschiedlichen Personen das gleiche Iris-Template zu errechnen, bei $1:10^{78}$ liegt [GES 2005]. Beim Fingerabdruck sind demgegenüber je nach Qualität des Bildes und der Ausprägung nur ca. 50 Merkmale identifizierbar [WDR 2005]. Als weiterer Vorteil für die Iriserkennung gegenüber der Fingerabdruckerkennung wird auch die Möglichkeit des kontaktlosen Erfassens aufgeführt, welches aus hygienischen Gründen wünschenswert ist.

Die FRR liegt laut [UKPS 2005 S.10] bei ca. 4% und laut [BIOPII 2005 S.164] zwischen 2% und 25% bei einer FAR von 0,1%. Die große Schwankung bei der BioPII Studie liegt daran, dass dort zwischen Wenig- und Vielnutzern unterschieden wurde. Während Nutzer, die häufig über die Iris identifiziert wurden (mehr als 120 Betätigungen), eine niedrige Falschrückweisung auswiesen, wurden Nutzer mit wenig Kontakt (weniger als 10 Betätigungen) häufiger als falsch zurückgewiesen [BIOPII 2005 S.12+167]. Dies deckt sich mit

der Aussage der BioPII Studie, dass die Iriserfassungs- und Erkennungssysteme verbesserungsfähig bzgl. ihrer Benutzerfreundlichkeit seien. Es sei davon auszugehen, dass die Erkennungsleistung sich bei Wenignutzern stark verbessern werde, wenn die Benutzerfreundlichkeit der Systeme erhöht werde [BIOPII 2005 S.13].

Mit der schlechten Benutzerführung lässt sich auch die sehr hohe Failure To Enroll Rate von 10% erklären [UKPS 2005 S.9]. Die Erfassungsgeräte gaben teilweise kein Feedback bei einem Fehlschlag, und stark Sehgeschädigte konnten ohne ihre Sehhilfe einen Punkt nicht fixieren, dessen Fixierung für ein erfolgreiches Enrolment nötig gewesen wäre [BIOPII 2005 S.94] & [UKPS 2005]. Zudem konnten Personen, die kleiner als 1,55m waren, schwer bis gar nicht enrolt werden, da auf Grund der Bauweise der Testsysteme die Kamera die Iris dieser Personen nicht erfassen konnte [BIOPII 2005 S.94].

Die Erkennungsleistung scheint vom Geschlecht unabhängig zu sein [UKPS 2005 S.245]. Eine Abhängigkeit beim Alter dagegen konnte festgestellt werden. So sinkt die Erkennungsleistung bei Personen unter 20 Jahren und über 50 Jahren merklich ab [UKPS 2005 S.244] & [BIOPII 2005 S.127]. Bei operativ Arbeitenden ist die Erkennungsleistung schlechter als bei administrativ Tätigen [BIOPII 2005 S.128].

Gegen die Verwendung der Iris als biometrisches Merkmal sprechen Akzeptanzprobleme [BIOPII 2005] & [UKPS 2005]. Durch einen Irisscan könnten theoretisch gesundheitliche Informationen erfasst werden. Inwieweit diese Daten jedoch für wissenschaftlich fundierte Diagnosen verwertbar wären, gilt als ungewiss [AOK 2005], [AETNA 2005].

4.3.6 Speicherung der biometrischen Daten

Üblicherweise werden zur biometrischen Erkennung so genannte Templates eingesetzt [BIOPII 2005]. Diese werden aus den Bildern, den so genannten Rohdaten, der biometrischen Merkmale erzeugt. Für die Erzeugung dieser Templates gibt es keine verbindlichen Standards, sodass Hersteller von Lesegeräten unterschiedliche Templates verwenden, die zueinander weitgehend inkompatibel sind. Damit der elektronische Reisepass jedoch von allen Ländern mit verschiedenen Lesegeräten gelesen werden kann, empfiehlt die ICAO die Verwendung von Rohdaten anstelle von proprietären Templates [ICAO 2004a S.17]. Templates können für nationale Zwecke zusätzlich auf dem RF-Chip gespeichert werden. Da normale digitale Bilder unter Umständen eine sehr hohe Speicherkapazität benötigen, hat die ICAO dazu Untersuchungen durchgeführt mit welcher Bildgröße welche Ergebnisse bei der biometrischen Erkennung erzielt werden können [ICAO 2004f] & [ICAO 2004g]. Abbildung 4.3.6a zeigt die Erkennungsleistung der Gesichtserkennung bei JPEG-komprimierten Bildern in Abhängigkeit von der Bildgröße.

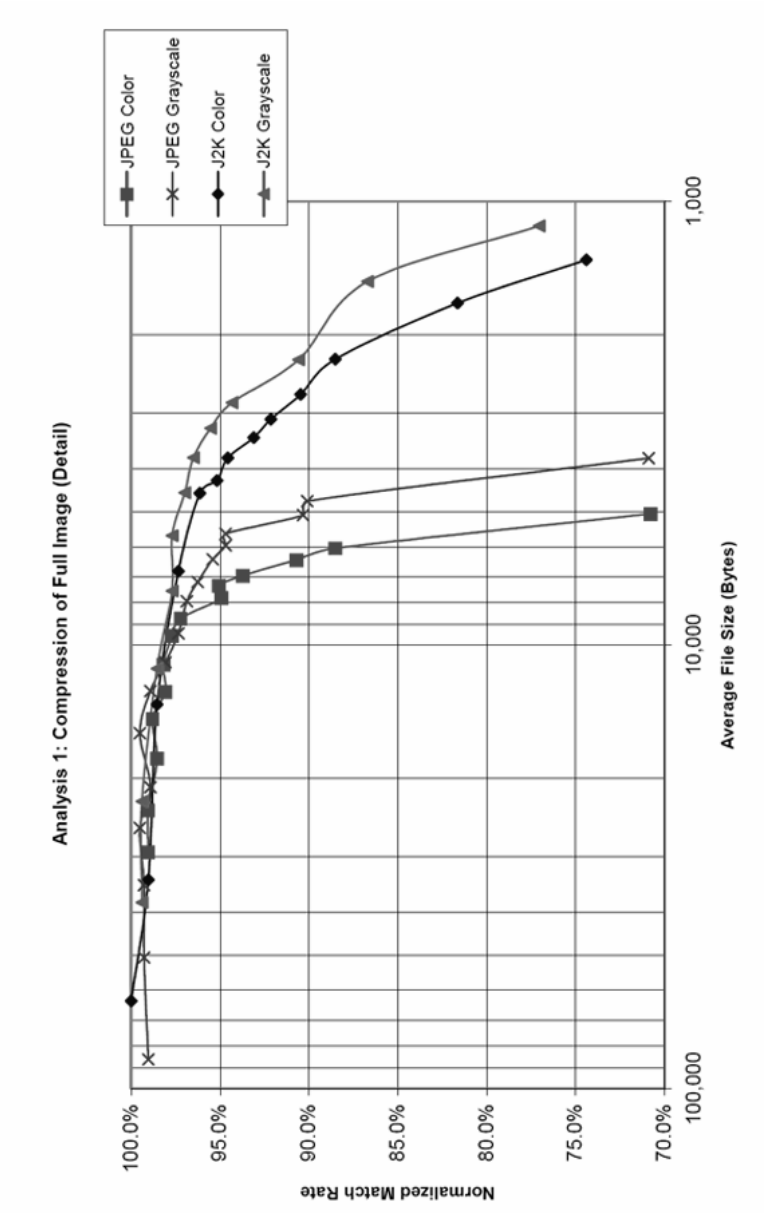


Abbildung 4.3.6a, Übernommen aus [ICAO 2004f S.14]

Die ICAO kommt zu dem Schluss, dass ein Bild des Gesichts mit der Breite 420 Pixel und der Höhe 525 Pixel im JPEG-Format mit einer Dateigröße zwischen 15 und 20KB, ein optimales Verhältnis zwischen Speicherbedarf und Erkennungsleistung darstellt [ICAO 2004h S.31] & [ICAO 2004d S.36]. Soll ein Passfoto, auf welchem die Gesichtshöhe 25mm beträgt, eingescannt werden, empfiehlt die ICAO eine Auflösung von 300dpi [ICAO 2004h S.31].

Durch die unterschiedliche Kompressionsrate beim JPEG-Format kann es bei gleichem Kompressionsfaktor allerdings zu sehr unterschiedlichen Dateigrößen kommen. Das BSI hat in seiner Studie BioPII mit Gesichtsbildern gearbeitet, die eine durchschnittliche Größe von 13,6KB erreichten [BIOPII 2005 S.30]. Die minimale Dateigröße betrug allerdings nur 9,7KB, die maximale lag bei 25,9KB.

Um das Bild einer Iris zu speichern, empfiehlt die ICAO eine Dateigröße von 30KB und für einen Finger 10KB [ICAO 2004d S.32]. Das BSI kommt für das Irisbild auf etwas höhere Werte. So betrug die durchschnittliche Größe zweier Irisbilder 100,6KB [BIOPII 2005 S.34]. Die durchschnittliche Dateigröße von zwei Fingerabdrücken betrug 21,4KB [BIOPII 2005 S.32].

Aus diesen Ergebnissen resultierend empfiehlt die ICAO eine Mindestspeicherkapazität von 32KB für die RF-Chips, sofern lediglich das Gesichtsbild zzgl. weiterer nicht-biometrischer Informationen gespeichert werden soll [ICAO 2004d S.36]. Sollen zwei Fingerabdrücke gespeichert werden, sei eine Speicherkapazität von mindestens 64KB notwendig.

Dementsprechend sieht die Bundesdruckerei vor, für die Einführung des ePasses Chips mit Speicherkapazitäten zwischen 32KB und 72KB zu verwenden [BDR 2005 S.6].

4.3.7 Zusammenfassung

Die Entscheidung der ICAO, das Gesichtsbild als erstes und einzig verpflichtendes biometrisches Merkmal in den ePass aufzunehmen, scheint nachvollziehbar. Das Gesicht kann bei praktisch jeder Person enrolt werden. Das Enrolment ist verhältnismäßig günstig. Zudem hat sich das Gesichtsbild als Foto im Reisepass bereits bewährt und es ist mit einer hohen Akzeptanz zu rechnen. Die Erkennungsraten sind allerdings mäßig.

4.4 Sicherheitsmerkmale

4.4.1 Basic Access Control

Beim alten Reisepass hat der Besitzer durch Aushändigen des Passes indirekt eingewilligt, dass die dort enthaltenden Daten ausgelesen werden können. Um beim ePass ein Auslesen der auf dem RF-Chip befindlichen Daten per Funk ohne Wissen des Passeigentümers zu verhindern, wird beim ePass das Authentifizierungsverfahren Basic Access Control (BAC) eingesetzt. Dieses Verfahren erlaubt die Übertragung der Daten über die kontaktlose Schnittstelle erst dann, wenn zuerst mit einem optisch arbeitenden Lesegerät Daten aus der Innenseite des ePasses ausgelesen wurden, was ein vorheriges Aufklappen des ePasses voraussetzt.

Die Funktionsweise des Basic Access Control ist von der ICAO standardisiert worden und wird im Technical Report [ICAO 2004a]

beschrieben. Die folgende Beschreibung der Funktionsweise basiert auf dem erwähnten ICAO Dokument und einem Dokument des BSI [BSI 2005d].

Als erstes muss der ePass aufgeschlagen werden, um die dann sichtbar werdende Machine Readable Zone (MRZ) mittels Optical Character Recognition (OCR) zu erfassen. In der MRZ sind Daten des Passes wie der Name, die Dokumentennummer, die Nationalität, das Geburtsdatum und das Geschlecht kodiert [ICAO 2004e S.20). Alternativ können die Daten auch manuell – beispielsweise durch Eingabe mit einer Tastatur – erfasst werden, wenn eine automatische Erfassung nicht möglich ist.

Die Dokumentennummer, das Geburtsdatum und das Ablaufdatum werden, ähnlich wie bei einer Hashwertberechnung, für die Berechnung des Zugriffsschlüssels verwendet, mit dem anschließend die gegenseitige Authentisierung zwischen dem RF-Chip und dem Lesegerät erfolgt. Man benutzt nur diese drei Bestandteile der MRZ, weil nur sie durch Prüfsummen abgesichert sind und somit Fehler beim Einlesen per OCR erkannt werden können.

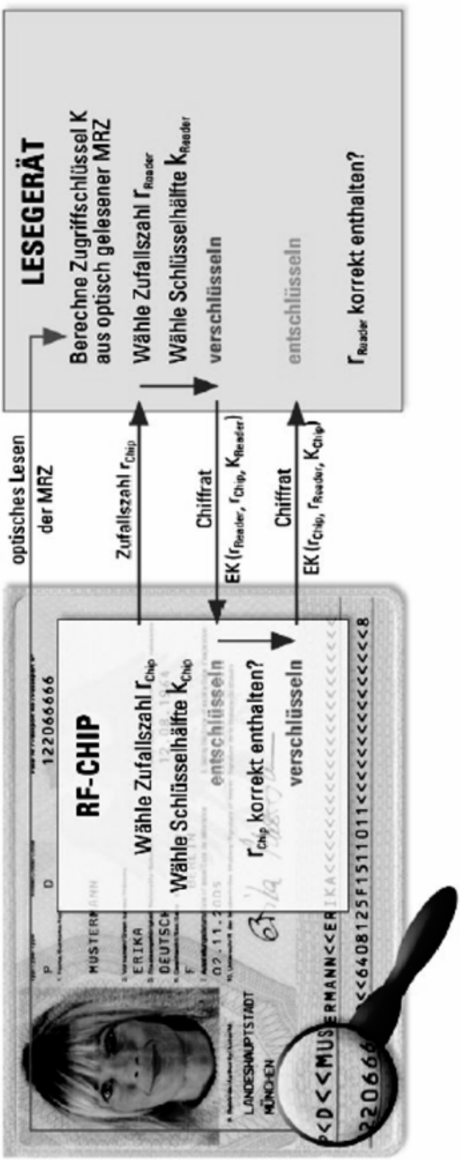
Die ICAO und das BSI bewerteten die Stärke des Zugriffsschlüssels mit maximal 56 Bit, was der Stärke eines normalen DES-Schlüssels entspricht [BSI 2005d] & [ICAO 2004a S.56]. Die ICAO erwähnt ebenfalls, dass sich die Stärke des Schlüssels unter bestimmten Bedingungen verringern lässt. Auf diesen Punkt wird in Kapitel 5.5.3 eingegangen.

Der Authentifizierungsprozess erfolgt in mehreren Schritten: Zuerst wird eine Zufallszahl (r_{Chip}) von dem RF-Chip an das Lesegerät ge-

sendet. Anschließend werden zwei Chiffrate ausgetauscht, die mit dem Zugriffsschlüssel verschlüsselt werden: Das vom Lesegerät an den RF-Chip gesendete Chiffrat besteht neben der eigenen Zufallszahl (r_{Reader}) und der Zufallszahl des RF-Chips (r_{Chip}) noch aus der eigenen Hälfte des späteren Sitzungsschlüssels (K_{Reader}). Nun kann der RF-Chip wiederum mit dem Zugriffsschlüssel das Chiffrat entschlüsseln und überprüfen, ob die vorher an das Lesegerät gesendete Zufallszahl (r_{Chip}) in dem Chiffrat vorhanden ist. Wenn dies der Fall ist, wird ein Chiffrat mit der Zufallszahl des RF-Chips (r_{Chip}), der Zufallszahl des Lesegeräts (r_{Reader}) sowie der eigenen Hälfte des zukünftigen Sitzungsschlüssels (K_{Chip}) an das Lesegerät gesendet. Nun wird das Chiffrat vom Lesegerät entschlüsselt und überprüft, ob die beiden Zufallszahlen korrekt enthalten sind. Wenn dies der Fall ist, wird aus den beiden Schlüsselhälften der neue Sitzungsschlüssel ermittelt, mit dem die nun folgende Kommunikation verschlüsselt wird. Die Integrität der Daten ist somit ebenfalls sichergestellt.

Abbildung 4.4.1a veranschaulicht die Funktionsweise der Basic Access Control.

Abbildung 4.4.1a, Basic Access Control



Quelle: [BSI 2005d S.3]

In der deutschen Version des ePasses erfolgt anschließend eine mit 112-Bit-Triple-DES verschlüsselte Kommunikation zwischen dem ePass und dem Lesegerät [BSI 2005d]. Da der Zugriffsschlüssel mit maximal 56 Bit jedoch weniger stark ist, wäre ein Brute-Force-Angriff bei vollständiger Aufzeichnung im Nachhinein theoretisch denkbar. Das BSI bewertet das Sicherheitslevel jedoch als ausreichend, da durch Basic Access Control keine besonders sensiblen Daten wie beispielsweise der Fingerabdruck geschützt werden.

4.4.2 Extended Access Control

Um auch besonders sensible Daten wie den Fingerabdruck vor unbefugten Zugriff zu schützen, ist ab März 2007 im Zusammenhang mit der Einführung der zweiten Stufe des ePasses die auf einem Public-Key Authentisierungsmechanismus basierende Extended Access Control vorgesehen. Dieses zur Zeit noch in der Spezifikationsphase befindliche Sicherheitskonzept, welches die Basic Access Control erweitert, verwendet zusätzlich einen über Public-Key-Kryptographie ausgehandelten Sitzungsschlüssel (Diffie-Hellman-Schlüsselaustausch [DIHE 1976]) und bietet auch die Möglichkeit einer engen Zweckbindung [BORCHERS 2005] & [BMI 2005d]. Nur Lesegeräte die über einen geheimen Authentisierungsschlüssel verfügen, der über eine Zertifikatskette bestätigt werden muss, können auf die durch Extended Access Control geschützten Daten zugreifen. Daher kann das den ePass herausgebende Land mit Hilfe der im nächsten Abschnitt beschriebenen Digitalen Signaturen bestimmen, welche Daten von welchen Ländern abgerufen werden können.

4.4.3 Digitale Signatur

Um die Authentizität und Integrität der im ePass gespeicherten Daten sicherstellen zu können, sind diese mit einer Digitalen Signatur versehen. Demzufolge kann überprüft werden, ob die signierten Daten von einer berechtigten Stelle ausgestellt wurden und ob die Daten nachträglich manipuliert wurden. Die folgende Beschreibung basiert auf den Dokumenten [BSI 2005d] und [ICAO 2004a].

Alle am ePass mitwirkenden Länder bauen zu diesem Zweck eine global interoperable Public Key Infrastruktur (PKI) auf. In Deutschland bildet das Bundesamt für Sicherheit in der Informationstechnik (BSI) die zentrale nationale Stelle für die Schlüsselverwaltung und erzeugt dazu eine zweistufige PKI, welche aus der so genannten Country Signing CA (Certification Authority) und mindest einem Document Signer besteht.

Country Signing CA:
Die Country Signing CA stellt die oberste Zertifizierungsstelle eines jeden Landes dar. Ihre Aufgabe ist es die Document Signer zu zertifizieren.

Document Signer:
Die Document Signer sind zum Ausstellen der Ausweisdokumente berechtigte Stellen wie beispielsweise die Bundesdruckerei in Deutschland. Mit dem privaten Schlüssel werden die im ePass gespeicherten Informationen (Document Security Objects (DSO) digital signiert und somit vor Manipulationen geschützt. Die Document Signer Schlüsselpaare müssen vor unberechtigtem Zugriff geschützt werden. Der private Schlüssel wird regelmäßig durch neue ersetzt,

um im Falle einer Kompromittierung den Schaden zu begrenzen. Die Dokument Signer Certificate werden an die ICAO übermittelt und über ein Public Key Directory (PKD) allen teilnehmenden Staaten zur Verfügung gestellt. Die Zertifikate können auch im ePass gespeichert werden.

Sowohl für den privaten Schlüssel der Country Signing als auch für den privaten Schlüssel des Document Signers ist eine bestimmte Verwendungsdauer festgelegt. Für den Fall einer Kompromittierung hat dies den Vorteil, dass nur die Echtheit bestimmter Pässe in Zweifel gezogen werden muss. Die ICAO empfiehlt eine Verwendungsdauer von 3 bis 5 Jahren [ICAO 2004a] für den privaten Schlüssel der Country Signing CA und eine Verwendungsdauer von max. 3 Monaten für den privaten Schlüssel des Document Signers. Hieraus ergibt sich für das Country Signing bei einer Gültigkeitsdauer von 10 Jahren für den ePass eine Gültigkeitsdauer des öffentlichen Schlüssels von 13 Jahren und 3 Monaten bzw. 15 Jahren und 3 Monaten, je nachdem, ob die Verwendungsdauer des privaten Schlüssels 3 oder 5 Jahre beträgt. Der öffentliche Schlüssel des Document Signers hat analog dazu eine Gültigkeitsdauer von 10 Jahren und 3 Monaten.

Für den Fall einer Kompromittierung sieht die ICAO die so genannten Certificate Revocation Lists (CRL) vor, die in regelmäßigen Abständen veröffentlicht werden sollen, damit auch andere Länder möglicherweise gefälschte Signaturen identifizieren können [ICAO 2004a].

Für die Digitale Signatur wird in Deutschland der Signaturalgorithmus ECDSA (Elliptic Curve Digital Signature Algorithm) verwendet werden. Für den Country Signing CA Schlüssel wird von der ICAO eine Schlüssellänge von 256 Bit und für den Document Signer Schlüssel eine Länge von 224 Bit empfohlen. Ebenfalls zugelassen sind RSA und DSA.

4.5 Zusammenfassung

Die Entscheidung, einen RF-Chip für den ePass zu verwenden, ist nachvollziehbar. Bis auf eine kontaktbehaftete Smartcard bietet keine andere Alternative eine vergleichbare Speicherkapazität und die Möglichkeit, durch einen Mikroprozessor aktive Sicherheitsmaßnahmen zu implementieren. Die Smartcard hat gegenüber der RFID Technologie den Nachteil, dass ihre Kontakte den Belastungen mit hoher Sicherheit nicht 10 Jahre standhalten würden. Eine Betrachtung der Haltbarkeit von RF-Chips findet gesondert in Kapitel 5.2 statt.

Die Biometrie hinterlässt einen zwiespältigen Eindruck. Die Erkennungsleistungen haben sich in den letzten Jahren verbessert und es gibt keinen Grund anzunehmen, dass in den nächsten Jahren nicht weitere Verbesserungen stattfinden. Trotzdem bedeuten FRRs von 2 bis 10% bei der Gesichtserkennung, dass 2 bis 10 Personen von 100 Reisenden nicht erfolgreich verifiziert würden. Eine weitere kritische Betrachtung der Biometrie findet sich in Kapitel 5.2.2.

Die Sicherheitsmaßnahmen zur Gewährleistung des Datenschutzes sind auf den ersten Blick überzeugend. Zur kritischen Betrachtung siehe Kapitel 5.

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.

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 erfolg-

reiches 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]. Bilder der Bundesdruckerei lassen vermuten, dass das Inlay mit RF-Chip und Antenne entweder im äußeren Umschlag des ePasses oder in der Datenseite implementiert wird. 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 bei begründetem Zweifel an der Robustheit des Chips und der Antenne bzgl. des Stempelns, das Inlay in den oberen Umschlag eingebettet wird.

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 „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

Zusammenfassend kann gesagt werden, dass Stempeln und Schmutz vermutlich keine Gefahr für den ePass darstellen. Sofern bei der Herstellung entsprechende Maßnahmen ergriffen werden, sollte auch ein Schaden durch Biegen oder Knicken weitestgehend verhindert werden können. Ungewiss aber scheint, ob die RF-Chips tatsächlich bis zu 10 Jahre lang ihre Daten zuverlässig speichern werden. Sollte sich herausstellen, dass die Haltbarkeit des ePasses allgemein nicht den Anforderungen entspricht und es häufig zu defekten RF-Chips kommt, ist davon auszugehen, dass der ePass kaum noch einen Sicherheitsgewinn mehr gegenüber dem alten Reisepass böte. Schließlich könnten die Grenzbeamten nicht unterscheiden, welcher Chip durch das Alter oder andere Belastungen Schaden nahm und welcher mutwillig zerstört wurde.

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[9]:

- 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.

[9] 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

Theoretisch denkbar ist ein Szenario, bei dem Gegner des ePasses durch Demonstrationen oder gezielte Anschläge und Sabotageakte hohe Kosten verursachen, so wie es bei Aktionen von Atomkraftgegnern vorkommt [WELT 2004]. Der Nutzen des ePasses würde fraglich erscheinen, wenn bedingt durch seine Einführung Menschen oder Objekte zu Schaden kämen. Schließlich wird die Einführung des ePasses mit der erhöhten Inneren Sicherheit begründet [BMI 2005c]. In der Praxis scheint die Wahrscheinlichkeit solcher Aktionen eher gering. Die Einführung des ePasses ist seit längerem bekannt und auch wenn teils starke Kritik am ePass geübt wird, zeichnet sich unseres Wissens nach keine Bewegung ab, die auf radikale und gewaltbereite Tendenzen schließen lässt.

5.3.5 Zusammenfassung

Zwar gibt es theoretische Szenarien, bei denen der Regelbetrieb durch Maßnahmen einzelner Personen gestört werden könnte. Diese erscheinen aber nicht wahrscheinlich und können kaum als Argument gegen die Einführung des ePasses angebracht werden.

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 inwieweit 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[10]. Somit ist das Beantragen eines echten ePasses mit falschen Daten schwer möglich und auch nur für Personen, die sich schon in Deutschland befinden.

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

5.4.3 Gefälschte Pässe aus Ländern, die keinen ePass nutzen

Solange eines der Schengenländer keinen ePass einführt, wird es möglich sein, Pässe aus diesem Land zu fälschen und so in Deutschland einreisen zu können, ohne sich einem Vergleich biometrischer Merkmale auszusetzen. Weiterhin wird es möglich sein, Pässe aus anderen Nicht-Schengen-Ländern zu fälschen, die keinen ePass einsetzen. Hier würden die jeweiligen Einreisebestimmungen zusätzlich greifen, so dass beispielsweise ein Visum beantragt werden müsste, was in Zukunft auch mit der Speicherung und dem Vergleich biometrischer Merkmale einhergeht [BMI 2002b]. Eine ausführliche Betrachtung wäre zu umfangreich und kann in diesem Buch nicht erfolgen. Festzuhalten bleibt, dass wohl kaum gänzlich ausgeschlossen werden kann, dass Reisepässe anderer Länder ohne biometrische Merkmale gefälscht werden und somit eine illegale Einreise nach Deutschland ermöglicht wird.

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

Das Duplizieren eines ePasses kann in dem seltenen Fall eine Rolle spielen, dass ein eineiiger Zwilling mit der Identität des anderen Zwillings reisen möchte bzw. beide gleichzeitig mit der Identität des anderen. Solange in dem ePass nur das Gesichtsbild als biometrisches Merkmal gespeichert wird, ist davon auszugehen, dass Zwillinge mit demselben Pass reisen können. Sofern das technische Know-how vorliegt, ist auch das Erstellen einer 1:1 Kopie theoretisch möglich [ICAO 2004a S.17&55]. Sobald jedoch auch die Fingerabdrücke in dem ePass gespeichert werden, ist eine eindeutige Identifizierung möglich, da auch eineiige Zwillinge unterschiedliche Fingerabdrücke besitzen [PHILIPS 2005]. Auch wenn es bei Fingerabdrücken und Gesichtsbildern so genannte „Biometrische Zwillinge“ gibt [BSI 2003 S.7] liegt die Vermutung nahe, dass die Wahrscheinlichkeit für Biometrische Gleichheit bei Gesicht *und* Finger vernachlässigbar gering ist.

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 komplet-

ten 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 Innern 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[11] 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.

[11] 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[12]. Es liegt im Ermessen der Beamten eine Lösung zu finden.

5.4.10 Zusammenfassung

Es ist unklar, ob mit dem Geld für die Einführung des ePasses die angestrebten Ziele nicht auf anderem Wege besser hätten erreicht werden können. Die Überwindungssicherheit der Biometrischen Systeme ist unzureichend. Hier muss allerdings berücksichtigt werden, dass bei einer nicht automatisierten Grenzkontrolle sehr gute Voraussetzungen vorhanden sind, dass der Grenzbeamte bei einer Prüfung Manipulationsversuche mit einem Foto oder Gummifingerabdruck

[12] Laut persönlicher Nachfrage bei der Grenzkontrolle

leicht erkennen kann. Offen ist, ob tatsächlich bei jedem Reisenden eine entsprechende Prüfung stattfindet und die Lesegeräte so gut einsehbar sind, dass Manipulationsversuche zuverlässig erkannt werden. Die Tatsache, dass ein ePass auch mit defektem RF-Chip weiterhin gültig bleibt, könnte dazu führen, dass die Sicherheit des ePasses nicht über die Sicherheit des bisherigen Reispasses hinausgeht.

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

In [BSI 2004, S.48] wird erwähnt, dass mittels „Focused Ion Beam“ RF-Chips schrittweise in atomare Schichten zerlegt und ausgelesen werden können. Hierfür ist ein hoher technischer Aufwand und direkter Zugriff auf den ePass nötig. Es scheint wahrscheinlich, dass der Aufwand, einen fremden Pass in seinen Besitz zu bringen und diesen mit komplizierten technischen Verfahren zu analysieren, höher ist als der Aufwand auf anderem Wege an das Gesichtsbild und die Fingerabdrücke einer speziellen Person zu gelangen. Zudem werden die Daten bereits verschlüsselt auf dem Chip gespeichert[13]. Von daher scheint eine Gefährdung des Datenschutzes durch das Verfahren „Focused Ion Beam“ nicht möglich.

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.

[13] Laut Telefonischer Auskunft von Herrn Unger, Mitarbeiter des BSI

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[14]. Dies reduziert den Faktor von 365x10 auf 253 x 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

[14] 8 bis 12 gesetzliche Feiertage in Deutschland, abhängig vom Bundesland.

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 mögli-

chen 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, diese Zeit 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[15].

Das Aufzeichnen eines Kommunikationsvorgangs bei einer bestimmten Person hingegen wäre leichter zu bewerkstelligen, vorausgesetzt

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

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 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

Grundsätzlich gelten asymmetrische Verschlüsselungsalgorithmen wie das beim ePass verwendete ECDSA als sehr sicher. Da von der ICAO jedoch noch keine Empfehlung und kein Standard für die Extended Access Control veröffentlicht wurden, scheint eine Analyse der exakten Sicherheit kaum möglich. Eine allgemeine Betrachtung findet in Kapitel 4.4.1 statt.

5.5.6 Umgehen von Extended Access Control

Auch ohne genaue Kenntnisse, wie die Extended Access Control im Detail arbeiten wird, kann gesagt werden, dass ein Sicherheitsrisiko bestünde, sobald „Schurkenstaaten“ an dem System beteiligt würden

und die entsprechen Zugangsschlüssel erhielten. Diese hätten damit die Möglichkeit, auf die Daten ggf. eingeschränkt zugreifen zu können, und es bestünde die Gefahr, dass diese Staaten den Schlüssel weitergäben oder selbst missbräuchlich nutzten. Allerdings ist Deutschland nicht verpflichtet, die Zugangsschlüssel an andere Staaten weiterzugeben. Laut ICAO-Empfehlung muss lediglich das Gesichtsbild jedem Staat zugänglich sein.

5.5.7 Zentrale Datenbanken

Das Speichern der biometrischen Daten in einer zentralen Datenbank ist per Gesetz verboten [PaßG 1986, §4 Absatz 4] und eine Änderung des Gesetzes ist von der derzeitigen Regierung nicht geplant [BUND 2005]. Aus diesem Grund soll an dieser Stelle nicht eingehender auf Vor- und Nachteile einer bundesweiten Datenbank eingegangen werden. Die Möglichkeit, dass andere Staaten zentrale Datenbanken mit biometrischen Merkmalen von einreisenden Deutschen erstellen könnten, wird in Abschnitt 5.6.5 erörtert.

5.5.8 Bewegungsprofile & personenbezogene Bomben

In [PFITZ 2005] wird als Risiko des ePasses erwähnt, dass das Erstellen von Bewegungsprofilen und personenbezogenen Bomben[16] ermöglicht werde durch Schwachstellen bei der Basic und Extended Access Control (vgl. Kapitel 5.5.4 und Kapitel 5.5.6).

[16] Als personenbezogene Bombe wird eine Bombe betrachtet, die automatisch zündet, wenn sich eine bestimmte Person in einem bestimmten Umkreis der Bombe befindet.

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 ausge-

schlossen 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

Das Gesichtsbild und weitere persönliche Daten wie Name und Geburtsdatum werden durch die Basic Access Control geschützt. Die Fingerabdrücke durch die erweiterte Extended Access Control. Die Basic Access Control erweist sich unter genauerer Betrachtung als nicht so sicher, wie die Dokumente des BSI angeben [BMI 2005d] & [BSI 2005c]. Zwar mag der Schutz immer noch ausreichend sein, die

Frage aber bleibt offen, warum nicht ein wirksamerer Schutz, wie in Kapitel 5.5.9 vorgeschlagen, gewählt wurde. So hätte mit dem Einbau einer Metallfolie vielen datenschutzrechtlichen Bedenken vorgebeugt werden können.

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 werden neben dem Gesichtsbild die Fingerabdrücke erfasst. Dann 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]. Auch Bundestagsabgeordnete wie Ulla Burchardt (SPD) kritisieren die Entscheidung zur Einführung des ePasses, die „auf einer fragwürdigen rechtlichen Grundlage und […] trotz ungeklärter technischer, rechtlicher und finanzieller Fragen“ getroffen worden sei [Anhang B]. 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 Deutschland 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 nichtbiometrischen 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 Innern 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

Sowohl auf europäischer Ebene als auch in Deutschland fühlten sich Politiker und Parlament bzw. Bundesrat bei der Entscheidungsfindung nicht genügend eingebunden. Die Einführung des ePasses wurde beschlossen, ohne die genauen Kosten zu kennen. Pilottests oder Studien, die die Reife des ePasses bescheinigen oder einen realen Nutzen belegen, liegen nicht vor. Die Informationspolitik der Bundesregierung und ihrer Stellen ist in manchen Punkten fragwürdig.

5.7 Zusammenfassung

Von den im Vorhergehenden dargestellten Vorbehalten gegenüber dem ePass erscheinen einige angebracht.

So bleibt unklar, ob die RF-Chips tatsächlich 10 Jahre lang ihre Daten speichern werden. Die Tatsache, dass ein ePass mit defektem Chip dauerhaft ein gültiges Reisedokument bleibt, wirft die Frage auf, ob die Bundesregierung selbst an der dauerhaften Haltbarkeit des ePasses zweifelt. Würden defekte Speicherchips nur sehr selten vorkommen, spräche unserer Ansicht nach nichts gegen einen kostenlosen Austausch, der innerhalb eines bestimmten Zeitraumes nach Bekanntwerden des Defektes stattfinden muss.

Die Falschrückweisungsraten bei Gesichts- und Fingerabdruckserkennung liegen derzeit im Bereich einiger Prozent. Das BSI bezeichnet dies als ausreichend für eine Unterstützung bei der Personenkontrolle. Gleichzeitig merkt es aber an, dass weitere Untersuchungen für einen Praxisbetrieb notwendig sind. Die Überwindungssicherheit der Biometrischen Systeme kann als unzureichend betrachtet werden, wobei unklar bleibt inwiefern bei Grenzkontrollen von den Grenzbeamten auf Manipulationsversuche geachtet wird.

Die Basic Access Control stellt sich als nicht so sicher wie angegeben heraus. Der Schutz wird vermutlich ausreichen. Trotzdem stellt sich die Frage, warum auf den Einsatz einer metallischen Schutzfolie verzichtet wird. Dies hätte viele datenschutzrechtliche Bedenken ausgeräumt und zu einer höheren Akzeptanz in der Bevölkerung geführt.

Die Art der Einführung und deren Geschwindigkeit wurden sowohl auf europäischer als auch auf nationaler Ebene stark kritisiert. Es scheint unverständlich, warum sich nicht ausreichend Zeit genommen wurde, Ängste und Vorbehalte der Kritiker zu diskutieren. Zudem fehlen Studien und Pilottest, die die Wirksamkeit des ePasses und dessen ausreichende Funktionsfähigkeit nahe legen.

Mit einem echten „Hi-Tech-Desaster in der Tradition der Autobahn-Maut“, wie es der Chaos Computer Club befürchtet, ist allerdings keinesfalls zu rechnen [CCC 2005b]. Denn auch wenn ab 1. November 2005 ausschließlich ePässe ausgestellt werden, so beginnt die Ausstattung der Grenzübergänge mit entsprechenden Kontrollsystemen erst Anfang 2006 und wird bis 2008 andauern (vgl. Kapitel 3.2). Das bedeutet, selbst wenn die Biometrischen Systeme in der Praxis unzuverlässig arbeiten sollten, wird dies anfangs nur wenige Reisende betreffen und die Behörden können entsprechend reagieren. Also entweder die Systeme nachbessern oder im ungünstigsten Fall zeitweise auf biometrische Kontrollen verzichten.

6. Fazit

Der aktuelle deutsche Reisepass ist eines der fälschungssichersten Ausweisdokumente der Welt. Fälschungen von Reisepässen anderer, auch europäischer Länder kommen allerdings häufiger vor. Die Forderung nach einer Erhöhung der Sicherheit auf europäischer Ebene scheint somit grundsätzlich nachvollziehbar (vgl. Kapitel 2).

Aus diesem Grund ist die Entscheidung der EU, einen elektronischen Reisepass verpflichtend für alle Mitgliedsstaaten einzuführen, grundsätzlich zu begrüßen (vgl. Kapitel 3). In Deutschland wird der neue Reisepass zum 1. November 2005 unter dem Namen „ePass“ eingeführt. Dieser wird in der ersten Stufe auf einem RF-Chip das Gesichtsbild des Passinhabers speichern. In einer zweiten Stufe – ab März 2007 – werden zusätzlich zwei Fingerabdrücke gespeichert. Der Preis wird für einen 10 Jahre gültigen Pass von 26 Euro auf 59 Euro erhöht. Sofern Einführung und Betrieb des ePasses wie geplant verlaufen, wird sich für die Passinhaber wenig ändern.

Unter Berücksichtigung der geforderten Leistungen, wie Nutzung biometrischer Merkmale und aktive Sicherheitsfunktionen sowie der daraus resultierenden Anforderungen an Speicherkapazität und Übertragungsgeschwindigkeit, erscheint die Entscheidung, einen RF-Chip zu verwenden, sinnvoll (vgl. Kapitel 4.2). Auch der Entschluss, Gesicht und Finger als biometrische Merkmale zu verwenden, ist nach aktuellen Kenntnissen nachvollziehbar (vgl. Kapitel 4.3). Die Sicherheitsmechanismen Basic Access Control und Extended Access Control zeigen, dass bei der Entwicklung an den Datenschutz gedacht wurde (vgl. Kapitel 4.4.1 & 4.4.2). Neben der Biometrie sorgt

die Digitale Signatur für eine hohe Datensicherheit und damit einen hohen Schutz vor Fälschungen bzw. Passmissbrauch (vgl. Kapitel 4.4.3).

Wie in Kapitel 5 aufgezeigt, sind viele in der Vergangenheit dem ePass gegenüber geäußerte Bedenken unbegründet. So kann das Erstellen von Bewegungsprofilen praktisch ausgeschlossen werden (vgl. Kapitel 5.5.8). Ebenso scheint ein massenhaftes unbefugtes Auslesen von ePässen kaum möglich (vgl. Kapitel 5.5.4). Mechanische Einflüsse wie Stempeln und vermutlich auch Knicken werden sich nicht maßgeblich auf die Haltbarkeit des ePasses auswirken (vgl. Kapitel 5.2.3).

Andererseits sind jedoch einige Kritikpunkte am ePass berechtigt. So ist fraglich, ob der verwendete RF-Chip 10 Jahre lang seine Daten speichern wird (vgl. Kapitel 5.2.3). Zudem sind Alterungseffekte auf Biometrische Systeme bisher nur unzureichend untersucht worden. So ist unklar, ob in zehn Jahren eine Person anhand ihrer heute aufgenommenen biometrischen Merkmale mit ausreichender Genauigkeit authentifiziert werden kann (vgl. Kapitel 5.2.2).

Auch die heutige Leistungsfähigkeit der Biometrischen Systeme ist nicht endgültig geklärt. Die BSI-Studie BioPII kommt zwar zu dem Ergebnis, dass „Biometrische Verfahren […] die Identitätsprüfung anhand von Personaldokumenten wirksam unterstützen“ können, allerdings wurde in diesem Buch aufgezeigt, dass in der Praxis die Ergebnisse sowohl besser als auch signifikant schlechter ausfallen können (vgl. Kapitel 5.2.2). Des Weiteren zeigt die Studie, dass die Überwindungssicherheit Biometrischer Merkmale zum heutigen Zeitpunkt keinesfalls gewährleistet ist. Die BioPII Studie empfiehlt

„eine gründliche Untersuchung der Funktionstüchtigkeit, der Erkennungsleistung und der Überwindungssicherheit“ vor dem endgültigen Echtbetrieb der biometrischen Systeme an den Grenzkontrollen. Eine solche Untersuchung ist bisher nicht erfolgt.

Als ebenfalls kritisch könnten sich unerwartete Fortschritte in der Kryptoanalyse erweisen, die dazu führen könnten, dass der Datenschutz mit den eingesetzten Algorithmen nicht weiter gewährleistet werden kann (vgl. Kapitel 5.4.5).

Auf Grund der genannten Unsicherheiten bzgl. der Haltbarkeit der RF-Chips, in der Biometrie und in der Kryptographie legt die ICAO – nach deren Empfehlung der ePass entwickelt wurde – eine Gültigkeit der elektronischen Reisepässe von fünf Jahren nahe. Deutschland hat sich dennoch entschlossen, die Gültigkeit der Reisepässe im Regelfall bei 10 Jahren zu belassen (vgl. Kapitel 5.2.2).

Weiterhin wurde verdeutlicht, dass der Sicherheitsmechanismus Basic Access Control architekturbedingte Schwachstellen aufweist (vgl. Kapitel 5.5.3). Diese können unter bestimmten Voraussetzungen dazu führen, dass die Stärke des Zugriffsschlüssels anstelle von 56 Bit nur 28 Bit oder weniger beträgt. Zudem kann die Basic Access Control von Personen komplett umgangen werden, die einmal Zugriff auf den Papierteil des ePasses hatten. Also von Grenzbeamten, ggf. aber auch von Banken oder Mobilfunkhändlern, denen eine Kopie des Reisepasses vorliegt. Selbst wenn es unwahrscheinlich erscheint, kann auf Grund dieser Schwachstellen beispielsweise der Bau einer personenbezogenen Bombe, nicht gänzlich ausgeschlossen werden.

Zur Verbesserung des Datenschutzes wurden drei Möglichkeiten aufgezeigt (vgl. Kapitel 5.5.9).

- 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.

- 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.

- Die ICAO erwähnt die Möglichkeit in den ePass eine Metallfolie einzubauen. Diese würde komplett verhindern, dass ein Lesen der Daten bei geschlossenem Pass möglich ist.

Die Tatsache, dass ein ePass auch mit defektem RF-Chip weiterhin gültig bleibt, könnte dazu führen, dass die Sicherheit des ePasses kaum über die Sicherheit des bisherigen Reispasses hinausgeht (vgl. Kapitel 5.4.8). Sollte sich herausstellen, dass viele RF-Chips nach wenigen Jahren altersbedingt fehlerhaft oder gar nicht mehr arbeiten, könnten Grenzbeamten vermutlich nicht unterscheiden, welche RF-Chips mutwillig zerstört und welche altersbedingt funktionsunfähig sind. Somit könnte eine Person, die verhindern will, dass die biometrischen Daten des Chips genutzt werden, diesen einfach zerstören.

Die vielfach geäußerte Kritik an den unklaren Kosten, dem ungewissen Nutzen und der Art der Einführung scheint ebenfalls gerechtfertigt (vgl. Kapitel 5.6). So wurde die Einführung des ePasses beschlossen, ohne die genauen Kosten der Einführung zu kennen. Studien darüber, inwieweit der ePass seine angestrebten Ziele erreichen kann, existierten ebenfalls nicht. Sowohl auf europäischer als auch auf Bundesebene wird von Politikern verschiedener Parteien Kritik geübt. Der Bundesrat bemängelt, dass die Länder „in dem bisherigen Verfahren zur Einführung biometrischer Merkmale erst sehr spät und nur unzureichend von der Bundesregierung einbezogen worden“ sind.

Allgemein kann die Informationspolitik des Bundes kritisiert werden (vgl. Kapitel 5.6.4). Die offiziellen Informationsseiten zum ePass vermitteln den Eindruck, es handele sich um eine ausgereifte und risikofreie Technologie. So spricht beispielsweise das Bundesministerium des Innern von „technisch perfekten Lösungen“ die „ausreichend getestet“ seien. 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.

Darüber hinaus sagt die BioPII-Studie zwar aus, dass die Überwindungssicherheit der Biometrischen Systeme weiter getestet werden müsse. Ihre eigenen Ergebnisse durchgeführter Tests wurden bisher aber nicht veröffentlicht.

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.*

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

Insgesamt bestehen kaum Zweifel, dass ein elektronischer Reisepass mit gespeicherten biometrischen Merkmalen des Passinhabers wirkungsvoll gegen Passfälschungen und Identitätsmissbrauch sein kann. Die Art der Einführung und einige Teile der technischen Umsetzung des ePasses werden in der Öffentlichkeit jedoch zu Recht kritisiert. Dies betrifft insbesondere die aufgezeigte Schwachstelle bei der Basic Access Control; das Ignorieren der ICAO welche eine 5jährige Gültigkeit der Reisepässe nahe legt; die Ungewissheit, ob Biometrische Systeme tatsächlich bereits praxistauglich sind; und die Informationspolitik der für den ePass zuständigen öffentlichen Stellen. Dennoch ist wohl nicht mit einem „Hi-Tech-Desaster in der Tra-

dition der Autobahn-Maut“ zu rechnen, wie es der Chaos Computer Club befürchtet [CCC 2005b]. So wird im Gegensatz zur Maut der ePass sukzessive eingeführt. Ab 1. November 2005 werden ePässe ausgestellt. Die Ausstattung der Grenzübergänge mit entsprechenden Kontrollsystemen beginnt allerdings erst Anfang 2006 und wird bis 2008 andauern. Das bedeutet, anfängliche Fehler im System werden nur wenige Reisende betreffen und die zuständigen Stellen können entsprechend reagieren.

7. Quellenverzeichnis

[AA 2005a] Auswärtiges Amt: Gibt es verschiedene deutsche Reisepässe, ist der vorläufige Reisepass für die Einreise in alle Länder gültig? http://www.auswaertiges-amt.de/www/de/aamt/buergerservice/faq/kat9/F2

[AA 2005b] Auswärtiges Amt: Was ist ein Kinderausweis? http://www.auswaertiges-amt.de/www/de/aamt/buergerservice/faq/kat9/F10

[AA 2005c] Auswärtiges Amt: Was ist ein maschinenlesbarer Pass? http://www.auswaertiges-amt.de/www/de/aamt/buergerservice/faq/kat9/F4

[AETNA 2005] Aetna: Iridology. http://www.intelihealth.com/IH/ihtIH/WSIHW000/8513/34968/358826.html?d=dmtContent

[AOK 2005] Allgemeine Ortskrankenkasse AOK: Irisdiagnose. http://www.aok.de/bund/rd/136183.htm

[BDR 2005] Bundesdruckerei: ePassport – die Zukunft sicherer Reisedokumente

[BDR 2005b] Bundesdruckerei: Personalausweis/Reisepass: Sicherheitsmerkmale der Personalausweiskarte. http://www.bundesdruckerei.de/de/iddok/2_1/2_1_6.html

[BDS 2005] Bundesbeauftragter für den Datenschutz: Entschließung zwischen der 69. und 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder. 1. Juni 2005

[BDSG 2003] Bundesdatenschutzgesetz.
http://www.bfd.bund.de/information/BDSG.pdf

[BGSJRS 2005] Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, Michael Szydl: Security Analysis of a Cryptographically-Enabled RFID Device. The Johns Hopkins University Information Security Institute Baltimore. 28. Januar 2005

[BIOFACE 2003] Bundesamt für Sicherheit in der Informationstechnik: BioFace – Vergleichende Untersuchung von Gesichtserkennungssystemen, Öffentlicher Abschlussbericht BioFace I & II Version 2.1. Juni 2003

[BIOFINGER 2004] Bundesamt für Sicherheit in der Informationstechnik: Evaluierung biometrischer Systeme Fingerabdrucktechnologien – BioFinger Version 1.1 06.08.2004

[BIOPII 2005] Bundesamt für Sicherheit in der Informationstechnik: Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II

[BM 2005] Berliner Morgenpost: Studie: In Berlin leben bis zu 200 000 Illegale, 4. Juli 2005

[BMI 2002a] Bundesministerium des Innern: Innenpolitischer Bericht 1998 – 2002. Dr. Bernd Heimbüchel

[BMI 2002b] Bundesministerium des Innern: Der 11. September 2001 und seine Folgen. 1. März 2002

[BMI 2005a] Bundesministerium des Innern: Weiterentwicklung der Fälschungssicherheit von Pässen und Personalausweisen. http://www.bundesdruckerei.de/de/support/download/ident_72.pdf

[BMI 2005b] Bundesministerium des Innren: Bundesinnenminister Otto Schily zur Einführung des ePass und zur Biometrie. http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Nachrichten/Reden/2005/06/ePass.html

[BMI 2005c] Bundesministerium des Innern: Bundesinnenminister Schily stellt den neuen Reisepass mit biometrischen Merkmalen vor, 1. Juni 2005, http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2005/06/ePass.html

[BMI 2005d] Bundesministerium des Innern: Hintergrundinformation zum ePass: Technik & Sicherheit. http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/Biometrie/Hintergrundinfo__ePass.html

[BMI 2005e] Bundesministerium des Innern: Fragen und Antworten zum ePass. http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/Biometrie/Biometrie__FAQ.html

[BORCHERS 2005] Detlef Borchers: „Biosig 2005: Ein Pass, der passt“. 22.7.2005. http://www.heise.de/newsticker/meldung/61964/

[BORCHERS 2005b] Technologie mit Augenmaß: Der biometrische Pass in der Schweiz. 2.9.2005
http://www.heise.de/newsticker/meldung/63499

[BR 2005] Bundesrat: Drucksache 510/1/05, 8. Juli 2005

[BROMBA 2005a] Bromba: Bioidentifikation. 17.9.2005.
http://www.bromba.com/faq/biofaqe.htm#Grundlagen

[BROMBA 2005b] Bromba: Fingerabdruckerkennung. 23.7.2005.
http://www.bromba.com/knowhow/fingerprint.htm

[BSI 2003] Bundesamt für Sicherheit in der Informationstechnik: GSM-Mobilfunk, Gefährdungen und Sicherheitsmaßnahmen
http://www.bsi.de/literat/doc/gsm/gsm.pdf

[BSI 2004] Bundesamt für Sicherheit in der Informationstechnik: Risiken und Chancen des Einsatzes von RFID-Systemen, ISBN 3-922746-56-X

[BSI 2004b] Bundesamt für Sicherheit in der Informationstechnik: Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen zum geplanten Einsatz in Lichtbilddokumenten – BioP I

[BSI 2005a] Bundesamt für Sicherheit in der Informationstechnik: Häufig gestellte Fragen http://www.bsi.de/fachthem/epass/faq.htm

[BSI 2005b] Bundesamt für Sicherheit in der Informationstechnik: BSI gewährleistet technische Sicherheit des elektronischen Reisepasses http://www.bsi.de/presse/pressinf/020605epass.htm

[BSI 2005c] Bundesamt für Sicherheit in der Informationstechnik: Digitale Sicherheitsmerkmale im elektronischen Reisepass. 01.06.2005

[BSI 2005d] Bundesamt für Sicherheit in der Informationstechnik: Digitale Sicherheitsmerkmale im ePass. 1.6.2005. http://www.bmi.bund.de/cln_028/Internet/Content/Common/Anlagen/Themen/Informationsgesellschaft/DatenundFakten/Sicherheitsmerkmale__ePass,templateId=raw,property=publicationFile.pdf/Sicherheitsmerkmale_ePass.pdf

[BSI 2005e] Bundesamt für Sicherheit in der Informationstechnik: Biometrie - Gesichtserkennung http://www.bsi.de/fachthem/biometrie/ dokumente/Gesichtserkennung.pdf

[BUND 2005] Deutsche Bundesregierung: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Ulrike Flach, Rainer Funke, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 15/4457 –, http://dip.bundestag.de/btd/15/046/1504616.pdf

[BVerfGE 1983] Bundesverfassungsgericht: BVerfGE 65, 1 – Volkszählung vom 15. Dezember 1983

[CCC 2004] Chaos Computer Club: Wie können Fingerabdrücke nachgebildet werden? 9.10.2004. http://www.ccc.de/biometrie/fingerabdruck_kopieren

[CCC 2005] Chaos Computer Club e.V.: Auskunft des Bundesinnenministeriums, http://www.ccc.de/epass/stellungnahme-bmi?language=de

[CCC 2005b] Chaos Computer Club e.V.: Biometrische Verfahren in der Praxis ungeeignet, http://www.ccc.de/epass/biopii?language=de

[DDP 2000] ddp Nachrichtenagentur (Deutsche Depeschen Presse): Immer mehr Illegale kommen über Schengen-Binnengrenzen. 14 Dezember 2000

[DH 2003] Professor Dr. Michael Ronellenfitsch: Zweiunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, http://www.datenschutz.hessen.de/Tb32/K18P06.htm

[DIHE 1976] W. Diffie und M. E. Hellman: New directions in cryptography. IEEE Trans. Inform. Theory, IT-22(6), pp. 644-654, November 1976.

[DP 2005] Die Presse.com: Österreich Musterschüler beim "ePass" http://www.diepresse.com/Artikel.aspx?channel=c&ressort=c&id=492412

[DUDEN 2005] Der Duden: Das große Fremdwörterbuch

[EU 2004] Amtsblatt der Europäischen Union vom 29.12.2004: VERORDNUNG (EG) Nr. 2252/2004 DES RATES vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten

[EU 2005] European Commission: Technical Report of Biometrics at the Frontiers - Assessing the Impact on Society. EUR 21585 EN. Februar 2005

[FK 2004] Thomas Finke, Harald Kelter: Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, Whitepaper des BSI http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf

[GES 2005] Gesundheit.com: Iriserkennung am Flughafen. http://www.gesundheit.com/gc_detail_11_gc05070411.html

[HEISE 2004] Heise Online: EU-Rat nickt Verordnung für Biometriepässe ab 15.12.2004. http://www.heise.de/newsticker/meldung/54277

[HEISE 2005] Heise Online: Datenschützer verschärft Kritik an E-Pässen http://www.heise.de/newsticker/meldung/60536

[HEISE 2005b] Heise Online: What the Hack: Hacken zwischen Kultur und Kurzschluss http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/62253

[HEISE 2005c] Heise Online: Deutschland setzt internationale Standards bei Biometrie-Reisepässen
http://www.heise.de/newsticker/meldung/59512

[HEISE 2005d] Heise Online: Kritik am Biometriepass: "Zu früh, zu teuer und zu unsicher"

[HEISE 2005e] Heise Online: Biosig 2005 - Ein Pass, der passt
http://www.heise.de/newsticker/meldung/61964

[HEISE 2005f] Heise Online: Infineon und Philips liefern Chips für deutsche Biometriepässe
http://www.heise.de/newsticker/meldung/60211

[HEISE 2005g] Heise Online: RFID im Reisepass kein Sicherheitsmerkmal. http://www.heise.de/newsticker/meldung/64002

[HOF 2005] Heise Online Forum: Biometriepass soll 59 Euro kosten
http://www.heise.de/newsticker/foren/go.shtml?list=1&forum_id=79524

[ICAO 2004a] International Civil Aviation Organisation: Technical Report - PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1. 1. Oktober 2004

[ICAO 2004b] International Civil Aviation Organisation: Annex I - Use of Contactless Integrated Circuits In Machine Readable Travel Documents Version 4.0. 5. May 2004

[ICAO 2004c] International Civil Aviation Organisation: Annex A - Photograph Guidelines

[ICAO 2004d] International Civil Aviation Organisation: Technical Report - Biometrics Deployment of Machine Readable Travel Documents Version 2.0. 21.Mai 2004

[ICAO 2004e] International Civil Aviation Organisation: Technical Report - Machine Readable Travel Documents Development of a Logical Data Structure - LDS for Optional Capacity Expansion Technologies Revision 1.7. 18.05.2004

[ICAO 2004f] International Civil Aviation Organisation: Facial Image Optimal Storage Size Study #1.

[ICAO 2004g] International Civil Aviation Organisation: Facial Image Optimal Storage Size Study #2.

[ICAO 2004h] International Civil Aviation Organisation: Biometric Data Interchange Formats — Part 5: Face Image Data

[ICAO 2004i] International Civil Aviation Organisation: Supplement 9303 Version: 2005-4 V3.0. 12. Juni 2005

[KREMPL 2005] Stefan Krempl: Biometrie statt Demokratie. In c't 26/2004, S. 54.

[KRISSLER 2005] Dipl.-Ing. Jan Krissler in die tageszeitung: „Am besten in Alufolie einpacken“, 16. Juni 2005

[LSE 2005] The London School of Economics & Political Science: The Identity Project, An assessment of the UK Identity Cards Bill & its implications

[MMYH 2002] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino: Impact of Artificial "Gummy" Fingers on Fingerprint Systems. SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, Thursday-Friday 24-25 January 2002

[NIST 2002] NIST: Standards for Biometric Accuracy, Tamper Resistance, and Interoperability 13.11.2002

[PaßG 1986] Das Deutsche Paßgesetz

[PFITZ 2005] Prof. Dr. Pfitzmann, Andreas: Biometrie – wie einsetzen und wie keinesfalls? http://dud.inf.tu-dresden.de/literatur/BiometrieRFID.pdf

[PHILIPS 2005] Philips Electronics: Für eine schnelle und bequeme Passkontrolle http://www.philips.de/pv_article-17511.htm

[PHILIPS 2005b] Philips Electronics Pressemitteilung: Deutsche Regierung verwendet für elektronische Reisepässe hochsicheren kontaktlosen Chip von Philips. 3. Juni 2005

[RFID 2002] RFID-Handbuch, Klaus Finkenzeller

[ROSS 2005] Philip E. Ross: Passport to Nowhere. IEEE Spectrum. January 2005. S.54-44

[SCHNEIER 1996] Bruce Schneier: Angewandte Kryptografie. 1996

[SCHNEIER 2005] Bruce Schneier: New Cryptanalytic Results Against SHA-1. 17. August 2005. http://www.schneier.com/blog/archives/2005/08/new_cryptanalyt.html

[SKBS 2005] Stadt Karlsruhe Bürgerservice und Sicherheit: Reisepass, http://www.karlsruhe.de/Stadt/BuS/bb06.htm

[SKVK 2005] S. Schimkea, S. Kiltza, C. Vielhauera, T. Kalkerb: Security Analysis for Biometric Data in ID Documents. Otto-von-Guericke-Universität Magdeburg. SPIE-IS&T/ Vol. 5681

[SPIEGEL 2001] Der Spiegel: Ausgabe Nr. 44/2001 vom 29. Oktober 2001

[TAB 2003] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag: Biometrie und Ausweisdokumente, Zweiter Sachstandsbericht. Arbeitsbericht 93

[TKZ 2002] Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler: Biometric Access Protection Devices and their Programs Put to the Test. In c't 11/2002

[UK 2005] Home Office United Kingdom: Home Office Response to The London School of Economics' ID Cards Cost Estimates & Alternative Blueprint

[UKPS 2005] UK Passport Service: Biometrics Enrolment Trial. Mai 2005

[ULDSH 2003] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf

[WATSON 2005] Craig Watson 17.8.2005. http://www.nist.gov/srd/fing_img.htm

[WDR2005] West Deutscher Rundfunk: Sicherheits-Check per Irisabtastung. http://www.wdr.de/themen/politik/deutschland/iriserkennung/index.jhtml

[WELT 2004] Die Welt: Höhn ruft zum Kampf gegen Trittin, 1. April 2004, http://www.welt.de/data/2004/04/01/259042.html

[WYY 2005] X. Wang, Y. Yin, and H. Yu. Collision Search Attacks on SHA1, 2005. http://theory.csail.mit.edu/?yiqun/shanote.pdf

Anhang A: Zerstören eines RF-Chips

Eine Email von Dipl.-Ing. Peter Jacob, Mitarbeiter der EMPA, Abteilung „Zentrum für Zuverlässigkeitstechnik“ (ehemals das Institut für Baumaterialprüfung der ETH Zürich) zum Thema Zerstören von RF-Chips:

Eine Zerstörung eines RFID-Chips kann grundsätzlich auf drei Arten erfolgen:
1) Anlegen einer sehr hohen Spannung an die beiden Anschlusspins, an welcher die Spule angeschlossen ist
2) "Blitzeinschlag" in die Chipoberfläche durch die Chip-Passivierung hindurch infolge elektrostatischer Aufladungen
3) Löschung des EEPROM-Memoryinhalts durch Einbringen extrem starker E- und/ oder B- Felder bzw. gezielte Manipulation über Schreib/ Lesegerät.

Nun zu den einzelnen Punkten im Detail:
zu 1. Das RFID-Chip ist in der Karte oder im Transpondergehäuse mit einer Antennen-Spule oder einer kleinen Dipolantenne (je nach Frequenzbereich) verbunden. Über diese Antenne erfolgt sowohl der Informationsaustausch via Funkstrecke mit dem Lese-/ Schreibgerät als auch die Speisung des Chips. Je nach Abstand des RFID vom Lesegerät wird durch die Antenne eine sehr unterschiedliche Versorgungsspannung erreicht. Aus diesem Grund haben RFID Chips neben der integrierten Spannungsgleichrichtung der aus der Antenne zugeführten Wechselspannung auch eine Spannungs-Stabilisierungsschaltung oder zumindest -Begrenzung eingebaut. Dadurch wird die interne Betriebsspannung des Chips auf einen Festwert zwischen 2-5 Volt - je nach Chiptechnologie - begrenzt. Die

überschüssige Spannung wird dabei meist durch begrenzende Diodenstrecken, etwa vergleichbar den bekannten Zenerdioden, in Wärme umgesetzt. Übersteigt die Eingangsspannung den möglichen Abregelbereich, so erfolgt nach kurzer Zeit eine Zerstörung des Chips infolge EOS (Electrical Overstress), z.B. durch Abschmelzen der Versorgungsleiterbahn. Mit normalen Lesegeräten wird diese kritische Spannung nicht erreicht. Eine gewollte Zerstörung könnte aber beispielsweise durch Annähern der Transponderkarte an eine entsprechend bestromte "Primär"-Induktionsspule (mit wenigen Windungen aber hoher Wechselspannung) erfolgen. Bei Dipolantennen-Transpondern würden überhöhte Elektromagnetische Felder des entsprechenden Frequenzbereichs den gleichen Effekt bewirken. Ein solcher Effekt kann zum Beispiel durch starke Funkeninduktoren ungewollt eintreten. An der Empa haben wir solche Effekte festgestellt, als RFID-Chips elektrisch getestet wurden und ein Funkeninduktor in der Nähe betätigt wurde. Durch diesen wurden in der Testzuleitung des Chips Spannungsspikes erzeugt, denen das Chip nicht über längere Zeit (>1 Min) gewachsen war.
zu 2. Generell haben Mikrochips, so auch RFID-Chips, an den elektrischen Aussenverbindungen (Pins) Schutzstrukturen eingebaut, die vor kurzzeitigen, meist elektrostatisch verursachten Spannungsspikes bis etwa maximal 2kV schützen. Anders verhält es sich aber bei elektrostatischen Entladungen, welche direkt auf die Chip-Oberfläche einwirken (Oberflächen-ESD, ESDFOS). Dabei wird die etwa 1um dicke Chip-Passivierung durchschlagen und es entstehen Kurzschlüsse zwischen den beiden oberen Metall-Leiterbahnebenen. Dieser Fehlermechanismus ist als "Produktkiller" bei den Eingehäusungsprozessen der Chips in Plastikgehäuse, Karten, Glaskapseln usw. bekannt. Im gehäusten Zustand ist der Chip hingegen gut geschützt gegen einen direkten Einschlag. Würde

man jedoch eine bewusste Zerstörung herbeiführen wollen, so könnte etwa ein gezielter Blitzeinschlag, welcher die Karte durchschlägt und die Chipoberfläche trifft, etwa mit Hilfe eines Van-de-Graaf-Generators, Influenzmaschine oder Funkeninduktors oder dgl. die Zerstörung des RFID-Chips bewirken.
zu 3. Sofern ein entsprechendes Schreibgerät mit Zugangscodes vorliegt, könnte durch Löschen/ Überschreiben der Daten des im RFID befindlichen EEPROMS eine Manipulation des Chips gemacht werden. Eine Änderung des EEPROM-Inhalts durch starke elektrische und/ oder magnetische Felder sowie auch durch UV- und radioaktive alpha- Strahlung ist physikalisch zwar grundsätzlich möglich, aber nur bei Ansatz jeweils extrem starker Einwirkung. Im Bewusstsein dieser prinzipiellen Möglichkeit werden RFID-Chips im Rahmen ihrer Qualifikation auf ihre Resistenz gegen diese Einwirkungen mustergeprüft. (Dafür gibt es auch einen Standard, ich habe diesen allerdings leider gerade nicht zur Hand, könnte diesen aber evtl. herausfinden) Bei Magnetfeldern werden solche Prüfungen beispielsweise bis in den Tesla-Bereich geführt, wobei es bei den mir bekannten RFID-Baumustern bisher zu keinen Ausfällen gekommen ist.

Anhang B: Email von der Bundestagsabgeordneten Ulla Burchardt (SPD)

Sehr geehrter Herr Beel,

haben Sie vielen Dank für Ihre E-Mail vom 14. September 2005 zum Thema Biometrie. Wie Sie zutreffend schreiben, habe ich mich bereits mehrfach gegen die geplante Einführung biometrischer Merkmale in Pässen ausgesprochen.

Meine Kritik am Verfahren lässt sich in wenigen Sätzen zusammenfassen: Der Bundestag hätte nach geltendem Gesetz über die Einführung beschließen müssen, wozu es aber nicht kam, weil eine Beschlussfassung auf europäischer Ebene mittels einer EU-Verordnung herbeigeführt wurde.

Auf europäischer Ebene wiederum kam das so genannte „Anhörungsverfahren“ zur Anwendung, das Europäische Parlament hatte also keine Möglichkeit, seine mannigfachen Änderungswünsche gegenüber dem allein maßgeblichen EU-Ministerrat durchzusetzen. Im Übrigen wurde der Verordnungsentwurf nach Abschluss der Beratungen im federführenden Ausschuss des Europäischen Parlaments vom Ministerrat noch gravierend abgeändert. Und schließlich: Die EU darf nur dann tätig werden, wenn sie eine ausdrückliche Kompetenz dafür hat. Genau das aber ist beim biometriegestützten Reisepass zumindest umstritten.

Fazit: Faktisch blieben die Parlamente bei einem so bedeutsamen Thema wie dem ePass außen vor, beschlossen hat der EU-Ministerrat auf einer fragwürdigen rechtlichen Grundlage und das trotz ungeklärter technischer, rechtlicher und finanzieller Fragen.

Gerne können Sie sich im Falle weiterer Fragen mit meinem Berliner Büro in Verbindung setzen. Im Übrigen würde ich mich freuen, wenn Sie mir das genaue Thema und die Fragestellung Ihrer Arbeit in einer kurzen E-Mail noch etwas näher erläutern würden.

Ich wünsche Ihnen auf Ihrem weiteren Studienweg viel Erfolg und verbleibe

mit freundlichen Grüßen

gez. Ulla Burchardt