Jöran Beel & Béla Gipp

ePass - der neue biometrische Reisepass

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

ePass - der neue biometrische Reisepass

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

Jöran Beel & Béla Gipp

Impressum

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

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

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

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). Die BioPII Studie empfiehlt zudem „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. Stu-

dien 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 Inneren 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.

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 der ePass langfristig wirkungsvoll gegen Passfälschungen und Identitätsmissbrauch sein wird. Die Art der Einführung und Teile der technischen Umsetzung werden in der Öffentlichkeit jedoch zu Recht kritisiert. Dennoch ist keinesfalls mit einem „Hi-Tech-Desaster in der Tradition 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 (vgl. Kapitel 3.2). Das bedeutet, anfängliche Fehler im System werden nur wenige Reisende betreffen und die zuständigen Stellen können entsprechend reagieren.