ePass - der neue biometrische Reisepass

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

Jöran Beel & Béla Gipp

Berichte aus der Politik

Jöran Beel, Béla Gipp

ePass – der neue biometrische Reisepass

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

Shaker Verlag
Aachen 2005

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

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/

ISBN 3-8322-4693-2
ISSN 0948-437X

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • eMail: info@shaker.de

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

Inhaltsverzeichnis 1
Abkürzungen 4
Vorwort von Henning Arendt 6
Über die Autoren 9
1. Einleitung 10
2. Der aktuelle Deutsche Reisepass 14
  2.1 Einleitung 14
  2.2 Grundlegende Informationen 14
  2.3 Datensicherheit 15
  2.4 Datenschutz 17
  2.5 Zusammenfassung 18
3. Der ePass – eine allgemeine Betrachtung 19
  3.1 Einleitung 19
  3.2 Grundlagen 19
  3.3 Ziele des ePasses 22
  3.4 Der ePass in der Praxis 23
  3.5 Zusammenfassung 27
4. Der ePass im Detail – Detaillierte Technische Funktionsweise und Biometrie 28
  4.1 Einführung 28
  4.2 RFID 28
  4.3 Biometrie 32
    4.3.1 Einleitung 32
    4.3.2 Biometrische Verfahren im Überblick 33
    4.3.3 Gesichtserkennung 37
    4.3.4 Fingerabdruckerkennung 39
    4.3.5 Iriserkennung 41
    4.3.6 Speicherung der biometrischen Daten 43
    4.3.7 Zusammenfassung 46
  4.4 Sicherheitsmerkmale 46
    4.4.1 Basic Access Control 46

4.4.2 Extended Access Control 50
4.4.3 Digitale Signatur 51
4.5 Zusammenfassung 53
5. Vorbehalte gegen den ePass 54
5.1 Einleitung 54
5.2 Zuverlässigkeit des Systems im Allgemeinen 54
5.2.1 Einleitung 54
5.2.2 Zuverlässigkeit der Biometrie 55
5.2.3 Haltbarkeit des ePass 58
5.2.4 Zusammenfassung 60
5.3 Störung des Regelbetriebs durch einzelne Individuen 61
5.3.1 Einleitung 61
5.3.2 Störsender & Blockertags 61
5.3.3 Zerstören durch Fremdeinwirkung 62
5.3.4 Demonstrationen und Sabotage 63
5.3.5 Zusammenfassung 63
5.4 Täuschen und Umgehen des Systems 63
5.4.1 Einleitung 63
5.4.2 Echter ePass mit falschen Papieren 64
5.4.3 Gefälschte Pässe aus Ländern, die keinen ePass nutzen .. 65
5.4.4 Einreise über schlecht bewachte Grenzen 65
5.4.5 Verändern der Daten auf dem Chip / Austauschen des Chips / Komplettfälschung 66
5.4.6 Klonen eines ePasses / Nutzen des gleichen Passes durch mehrere Personen 67
5.4.7 Überwindungssicherheit der biometrischen Merkmale ... 68
5.4.8 Zerstören des RFID-Chips durch Passinhaber 70
5.4.9 Unkenntlich-Machen der biometrischen Merkmale 71
5.4.10 Zusammenfassung 71
5.5 Gewährleistung des Datenschutzes 72
5.5.1 Einleitung 72
5.5.2 Unautorisiertes physikalisches Auslesen der Daten 73
5.5.3 Kryptographische Sicherheit von Basic Access Control . 73
5.5.4 Umgehen von Basic Access Control 79

5.5.5 Kryptographische Sicherheit von Extended Access Control 80
5.5.6 Umgehen von Extended Access Control 80
5.5.7 Zentrale Datenbanken 81
5.5.8 Bewegungsprofile & personenbezogene Bomben 81
5.5.9 Verbesserung des Datenschutzes 82
5.5.10 Zusammenfassung 83
5.6 Weitere Aspekte 84
5.6.1 Einleitung 84
5.6.2 Unklare Kosten und ungewisser Nutzen 84
5.6.3 Vorschnelle Einführung 85
5.6.4 Informationspolitik 88
5.6.5 Politische Herausforderungen 89
5.6.6 Zusammenfassung 89
5.7 Zusammenfassung 90
6. Fazit 92
7. Quellenverzeichnis 99
Anhang A: Zerstören eines RF-Chips 111
Anhang B: Email von der Bundestagsabgeordneten Ulla Burchardt (SPD) 114

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