

Jöran Beel & Béla Gipp

ePass - der neue biometrische Reisepass

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



Bei diesem Dokument handelt es sich um einen
Auszug aus dem Originalbuch. Eine Weitergabe
ist nicht gestattet.

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/

© 2005 Jöran Beel & Béla Gipp

Alle Rechte vorbehalten. Eine Vervielfältigung, Verbreitung oder Weitergabe dieses Dokumentes oder Teile desselben ist ausdrücklich nicht gestattet, weder in digitaler noch in einer anderen Form.

© Titelbild: Bundesdruckerei GmbH

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 2005b] 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=dmContent>

[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 Inneren: Innenpolitischer Bericht 1998 – 2002. Dr. Bernd Heimbüchel

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

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

[BMI 2005b] Bundesministerium des Inneren: Bundesinnenminister Otto Schily zur Einführung des ePass und zur Biometrie.
http://www.bmi.bund.de/cIn_028/nn_122688/Internet/Content/Nachrichten/Reden/2005/06/ePass.html

[BMI 2005c] Bundesministerium des Inneren: Bundesinnenminister Schily stellt den neuen Reisepass mit biometrischen Merkmalen vor, 1. Juni 2005,
http://www.bmi.bund.de/cIn_028/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2005/06/ePass.html

[BMI 2005d] Bundesministerium des Inneren:
Hintergrundinformation zum ePass: Technik & Sicherheit.
http://www.bmi.bund.de/cIn_028/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/Biometrie/Hintergrundinfo_ePass.html

[BMI 2005e] Bundesministerium des Inneren: Fragen und Antworten zum ePass.
http://www.bmi.bund.de/cIn_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/biofaq.htm#Grundlagen>

[BROMBA 2005b] Bromba: Fingerabdruckerkenung. 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 Reisepas-
ses <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/cIn_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 Biometripässe 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 Kreml: Biometrie statt Demokratie. In c't 26/2004, S. 54.

[KRISLER 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 Iris-abtastung.
<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>