

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

Inhaltsverzeichnis

Inhaltsverzeichnis	1
Abkürzungen.....	4
1. Einleitung.....	6
2. Der aktuelle Deutsche Reisepass	10
2.1 Einleitung.....	10
2.2 Grundlegende Informationen.....	10
2.3 Datensicherheit	11
2.4 Datenschutz.....	14
2.5 Zusammenfassung	15
3. Der ePass – eine allgemeine Betrachtung.....	16
3.1 Einleitung.....	16
3.2 Grundlagen	16
3.3 Ziele des ePasses.....	19
3.4 Der ePass in der Praxis	20
3.5 Zusammenfassung	25
4. Der ePass im Detail – Detaillierte Technische Funktionsweise und Biometrie	26
4.1 Einführung	26
4.2 RFID	26
4.3 Biometrie	30
4.3.1 Einleitung.....	30
4.3.2 Biometrische Verfahren im Überblick.....	31
4.3.3 Gesichtserkennung.....	35
4.3.4 Fingerabdruckerkennung	37
4.3.5 Iriserkennung	39
4.3.6 Speicherung der biometrischen Daten	41
4.3.7 Zusammenfassung	44
4.4 Sicherheitsmerkmale.....	44
4.4.1 Basic Access Control.....	44
4.4.2 Extended Access Control.....	48
4.4.3 Digitale Signatur (Datensicherheit)	49

4.5 Zusammenfassung	51
5. Vorbehalte gegen den ePass	52
5.1 Einleitung.....	52
5.2 Zuverlässigkeit des Systems im Allgemeinen	52
5.2.1 Einleitung.....	52
5.2.2 Zuverlässigkeit der Biometrie.....	53
5.2.3 Haltbarkeit des ePass	56
5.2.4 Zusammenfassung	58
5.3 Störung des Regelbetriebs durch einzelne Individuen.....	59
5.3.1 Einleitung.....	59
5.3.2 Störsender & Blockertags.....	59
5.3.3 Zerstören durch Fremdeinwirkung	60
5.3.4 Demonstrationen und Sabotage	61
5.3.5 Zusammenfassung	61
5.4 Täuschen und Umgehen des Systems.....	61
5.4.1 Einleitung.....	61
5.4.2 Echter ePass mit falschen Papieren	62
5.4.3 Gefälschte Pässe aus Ländern, die keinen ePass nutzen..	63
5.4.4 Einreise über schlecht bewachte Grenzen	63
5.4.5 Verändern der Daten auf dem Chip / Austauschen des Chips / Komplettfälschung	64
5.4.6 Klonen eines ePasses / Nutzen des gleichen Passes durch mehrere Personen	65
5.4.7 Überwindungssicherheit der biometrischen Merkmale ...	66
5.4.8 Zerstören des RFID-Chips durch Passinhaber.....	68
5.4.9 Unkenntlich-Machen der biometrischen Merkmale	69
5.4.10 Zusammenfassung	69
5.5 Gewährleistung des Datenschutzes.....	70
5.5.1 Einleitung.....	70
5.5.2 Unautorisiertes physikalisches Auslesen der Daten	71
5.5.3 Kryptographische Sicherheit von Basic Access Control .	71
5.5.4 Umgehen von Basic Access Control	77
5.5.5 Kryptographische Sicherheit von Extended Access Control	78
5.5.6 Umgehen von Extended Access Control	78

5.5.7 Zentrale Datenbanken	79
5.5.8 Bewegungsprofile & personenbezogene Bomben.....	79
5.5.9 Verbesserung des Datenschutzes	80
5.5.10 Zusammenfassung	81
5.6 Weitere Aspekte.....	82
5.6.1 Einleitung.....	82
5.6.2 Unklare Kosten und ungewisser Nutzen.....	82
5.6.3 Vorschnelle Einführung.....	83
5.6.4 Informationspolitik	86
5.6.5 Politische Herausforderungen.....	87
5.6.6 Zusammenfassung	87
5.7 Zusammenfassung	88
6. Fazit	90
7. Quellenverzeichnis	96
Anhang A: Zerstören eines RF-Chips.....	108