



Die Anforderungen der ICAO an Reisedokumente mit Biometrie

Vortrag im Seminar
„Biometrische Systeme“

Alexander Klink

klink@mathematik.tu-darmstadt.de

25.01.2005

Überblick

- Wer ist eigentlich die ICAO?
- Der ePassport
- Public Key Infrastruktur
- Stand der Dinge
- Mögliche Probleme
- Diskussion



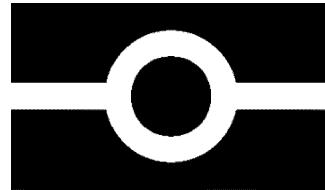
- International Civil Aviation Authority
- Teilorganisation der UN
- 188 Mitgliedsstaaten
- arbeitet seit 1978 an maschinenlesbaren Reisedokumenten



ICAO (2)

- MRTD: „Machine Readable Travel Document“
- TAG/MRTD, NTWG
- MRP: „Machine Readable Passport“ (ca. 120)
- MRV: „Machine Readable Visa“ (ca. 30)
- MRZ: „Machine Readable Zone“ (OCR-B)
- MRTD + Biometrie = ePassport

Der ePassport



- Berlin/New-Orleans Resolution:
 - Gesicht (+ Fingerabdruck, Iris)
 - Kontaktlose ICs als Speichermedium
- TAG/MRTD entwickelt Standard



Der ePassport: Anwendungen

- Während des Enrolments:
 - Biometrisches Template mit anderen Datenbanken vergleichen
 - beim Abholen Identität des Antragstellers verifizieren
 - Identität der Mitarbeiter beim Enrolment verifizieren

Der ePassport: Anwendungen (2)

- An der Grenze:
 - Test: Identität \leftrightarrow biometr. Daten im Reisedokument
 - 2-Wege-Test: biometr. Daten jetzt \leftrightarrow im Reisedokument
 - 3-Wege-Test: 2-Wege \leftrightarrow Biometrie in Enrolment-Datenbank
 - 4-Wege-Test: 3-Wege + visueller Vergleich Foto auf Chip \leftrightarrow Foto im Pass



Der ePassport: Ausgestaltung

- Bilder: ca. 15-20K (Gesicht), 10K (Fingerabdruck), 30K (Iris)
- Rohdaten, Templates nur optional
- Kontaktloser IC, Lese-Reichweite 0-10cm, Kapazität mindestens 32K, 512K empfohlen
- Position im Pass: Datenseite, in der Mitte, Innenseite des Covers (vorne oder hinten)



Der ePassport: Ausgestaltung (2)

- Gesichtsbild: entweder identisch zur Datenseite, evtl. Ausschnitt
- MRZ ist im Chip enthalten, lesen optional
- Haltbarkeit des Chips 10 Jahre, evtl. 5 Jahre
- Digitale Signatur bzw. Verschlüsselung von Daten
- Lesegeräte nach ISO14443 + x



Public Key Infrastruktur

- Was ist eine Public Key Infrastruktur?
- Zertifikat: Public Key + digitale Signatur einer Certificate Authority (CA)
- Certificate Revocation Lists (CRLs)
- Country Signing CA (Certificate)
- Document Signer Certificate
- ICAO Public Key Directory (PKD)
- Passive Authentifizierung (braucht keinen Prozessor im IC)



Stand der Dinge

- EU: Gesichtsbild & Fingerabdruck
- Deutschland
 - Gesichtsbild bis Herbst (wg. Visa Waiver Programm der USA)?
 - Fingerabdruck & digitale Signatur ab 2007
 - Kosten für den Antragsteller?



Mögliche Probleme

- Implementierungen noch in Entwicklung begriffen (vgl. auch Ergebnisse der BioP-Studie von BSI und BKA)
- Kaum Langzeittests (> 10 Jahre)
- Wenig Erfahrung mit Identifikation 1:n mit $n = |\text{Passinhaber eines Staates}|$
- Datenschutzvorgaben, Gesetze zum Schutz der Privatsphäre, kulturelle Praktiken



Mögliche Probleme (2)

- Wie wird Nichterkennung behandelt?
- Grenzverkehr auf dem Landweg
- Kosten (Schätzung des Büros für Technikfolgen–Abschätzung beim Deutschen Bundestag: ca. 669 Millionen € einmalig, ca. 610 Millionen € jährlich)
- Begehrlichkeiten anderer möglicher Nutzer (Banken, etc.)



Noch Fragen ...?

Diskussionsanregungen

- Kosten/Nutzen?
- Forderungen des Chaos Computer Clubs:
 - öffentliche Debatte & Aufklärung
 - aktive Teilnahme der Personen bei Überprüfung
 - Haftungsfragen klären
 - keine Speicherung in Datenbanken
 - keine Speicherung von Rohdaten
 - keine Diskriminierung von einzelnen Personen/-gruppen
 - Test durch unabhängige Organisationen, Feldtests sowie wissenschaftliche Begleitung des Einsatzes
 - strenge Zweckbindung der Daten
 - Verzicht auf RFID-Technologie