Der ePass – ein Feldtest

starbug@berlin.ccc.de

Inhalt

Der ePass

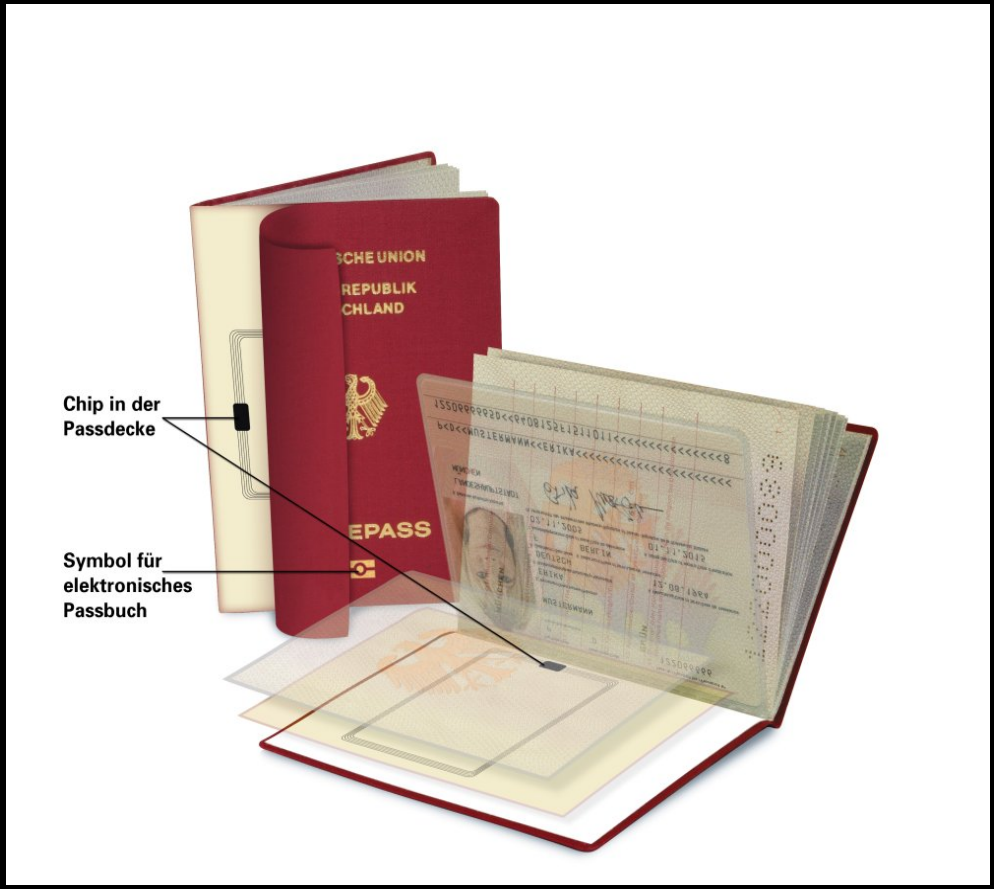
Der RFID-Chip im ePass
- Sicherheitsmechanismen
- Probleme und Gefahren

Die Biometrie im ePass
- Gesichtserkennung
- Fingerabdruckerkennung
- Probleme und Gefahren

Fazit

Der ePass

- aktuelles Paßbuch
- RFID-Chip mit biometrischen Daten



ePass :: offizielle Gründe der Einführung

- RFID und Biometrie als zusätzliches Sicherheitsmerkmal (weniger Paßfälschungen)
- Ist der Besitzer des Dokuments auch der Inhaber?
- Effektivierung von Grenzkontrollen (Computergestützte Verifikation)
- Unterstützung bei Personenfahndungen

ePass :: Timeline Einführung

- 09.01.02 Terrorismusbekämpfungsgesetz
- 26.10.04 Abnahme von Fingerabdrücken und Fotos bei der Einreise in die USA
- 02.12.04 Beschluß des EU-Parlaments (Coelho-Bericht)
- 13.12.04 Beschluß des EU-Rates der Innen- und Justizminister bzw. der Regierungschefs
- 22.06.05 Kabinett beschließt Einführung des ePasses
- 08.07.05 Bundesrat billigt Änderung des Paßgesetzes
- 01.11.05 Einführung des neuen ePasses (Aufnahme eines digitalen Gesichtsbildes)
- 03/ 2007 Aufnahme von Fingerabdrücken in den Paß
- 2007 RFID-Chip und Biometrie auch in Ausweisen

Der RFID-Chip im ePass

ePass :: RFID

- ISO 14443 - 13,56 Mhz
- Proximity Card – Reichweite 10 cm
- kryptographischer Coprozessor
- Infineon SLE 66CLX641P (64 kB)
- Philips Smart MX P5CT072 (72 kB)

ePass :: gespeicherte Daten

- verpflichtende Datengruppen
  - DG 1: Daten der Maschinenlesbaren Zone
    - PassID
    - Geburtsdatum
    - Ablaufdatum
  - DG 2: Gesichtsbild
- optionale Datengruppen
  - DG 3: Fingerbilder (ab März 2007 verpflichtend)
  - DG 4: Irisbilder
  - DG 15: public Key (aktive Authentifikation)

ePass :: Sicherheitsmechanismen

Verpflichtend in Deutschland:
1- zufällig generierte RFID-Chip-ID
2 - passive Authentifikation
3 - Basic Access Control

Optional:
- aktive Authentifikation
- Extended Access Control

Sicherheitsmechanismen :: passive Authentifikation

- *sichert Authentizität und Integrität der gespeicherten Daten*
- Algorithmen: RSA, DSA oder ECDSA
- global interoperable PKI
  - Country Signing CA (BSI) signiert den public Key des Document Signers (256 Bit ECDSA)
  - Document Signer (Bundesdruckerei) signiert die Daten auf dem Paß (224 Bit ECDSA)
- Schlüssel werden regelmäßig ausgetauscht
  - 3 - 5 Jahre für Country Signing CA Keys
  - 3 Monate für Document Signer Keys

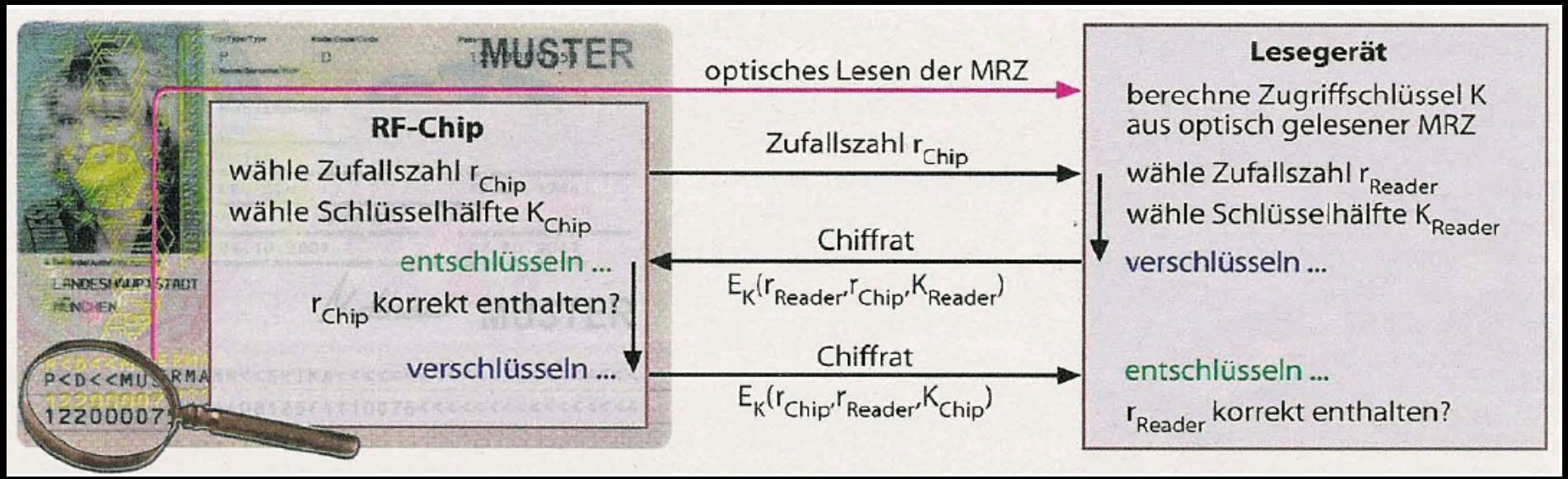
Sicherheitsmechanismen :: aktive Authentifikation

- *verhindert das Cloning*
- public – private Key
- 1024 Bit RSA
- private Key nicht auslesbar

Sicherheitsmechanismen :: Basic Access Control :: 1

- *Schützt weniger sensitive Daten gegen unauthorisiertes Auslesen*
  - Gesichtsbild
  - Daten der MRZ
- Schlüsselgenerierung aus prüfsummengesicherten Teilen der MRZ (max. 56 Bit)
  - PassID (10^9)
  - Geburtsdatum (100*365)
  - Ablaufdatum (10*365)

Sicherheitsmechanismen :: Basic Access Control :: 2



- Sessionkey aus K_{Reader} und K_{chip}
- 112-Bit-Triple-DES
- Dauer ca. 5 s

Sicherheitsmechanismen :: Extended Access Control

- *Schützt sensitivere Daten*
  - Fingerabdruck
  - Iris

- Public Key Infrastruktur
- Aussteller entscheidet über Leseberechtigung der Länderlesegeräte

- Chip verifiziert Zertifikat des Lesegerät
- Zertifikat beinhaltet Rechte des Lesegeräts
- Dauer ca. 10 s

Probleme und Gefahren :: RFID + Crypto

- Lebensdauer von Chip und Crypto
- MRZ (Schlüssel) nicht wechselbar
- Auslesen der RFID-Chips
  - aktives Abhören bis zu 10 m
  - passives Abhören bis zu 30 m
- Brechen der BAC Verschlüsselung möglich
  - Reduzieren des Schlüsselraumes
  - Parallelisieren des Brute Force Angriffs
- Grandmaster Chess Attacke
- gezieltes Tracking von Personen (RFID-Bomben)

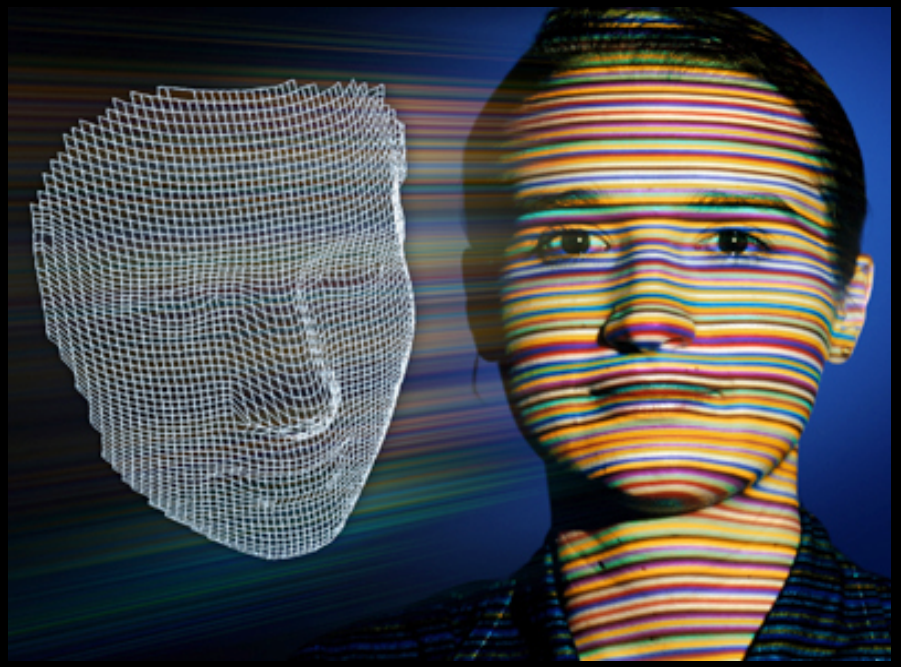
Probleme und Gefahren :: RFID :: Gegenmaßnahmen

- Verhindern des Auslesens
  - Aluminiumfolie
  - Kollision durch andere Chips
  - 13,56 MHz Störsender
- Zerstören des Chips
  - Mikrowelle
  - Schweißtrafo
- Abtrennen der Antenne

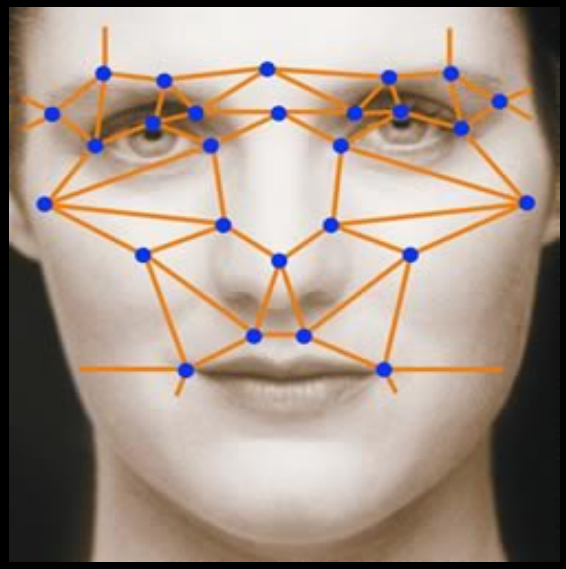
Die Biometrie im ePass

Gesichtserkennung :: Funktion

- Aufnahmevarianten
  - 2-dimensional
  - 3-dimensional

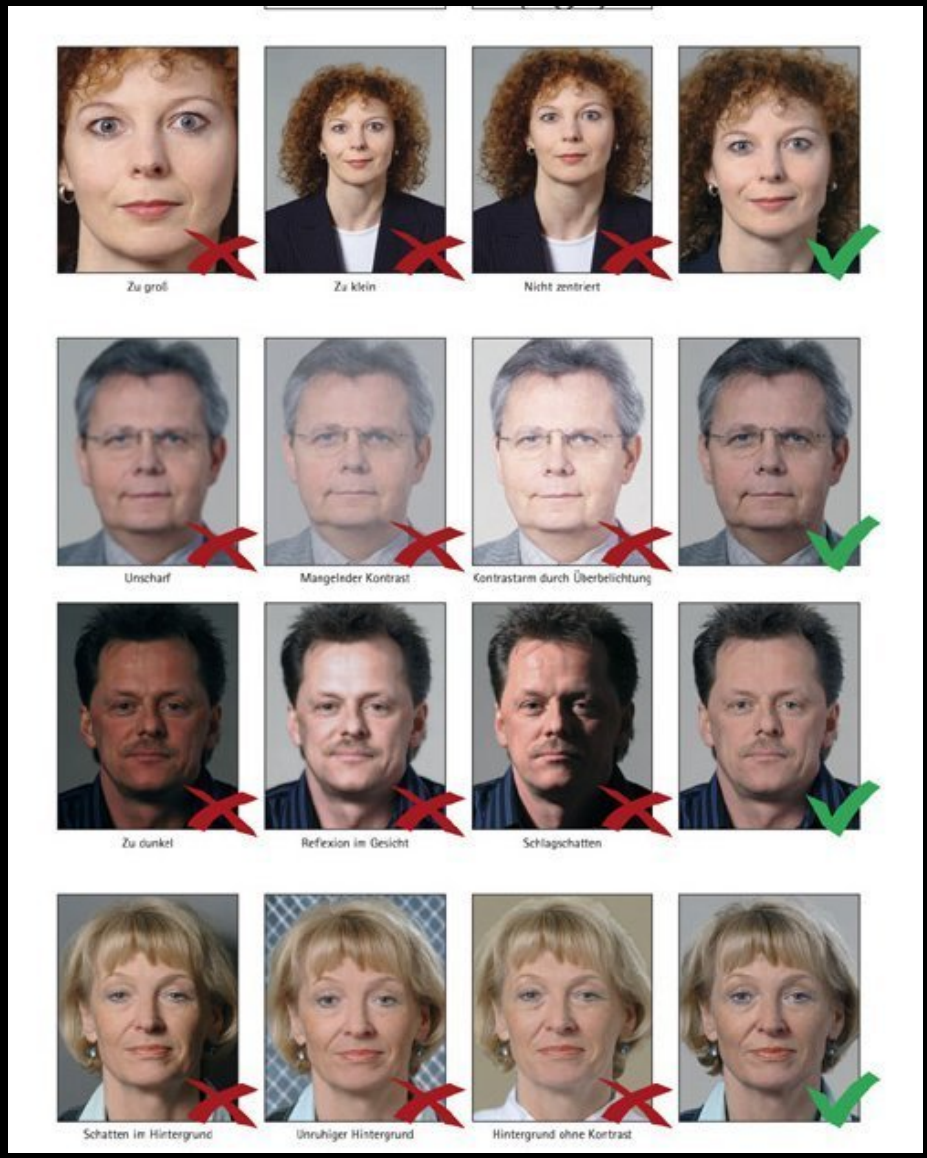


- Auswertealgorithmen
  - Gesichtsmetrik
    (Elastic Graph Matching)
  - Eigenface



ePass :: Mustertafel :: 1

- Format
  - Gesicht zentrisch
  - 32 – 36 mm
  - Kinn bis Haaransatz
- Kontrast
- Ausleuchtung
- Hintergrund
  - einfarbig hell
  - Kontrast zum Gesicht
  - keine Muster oder Schatten

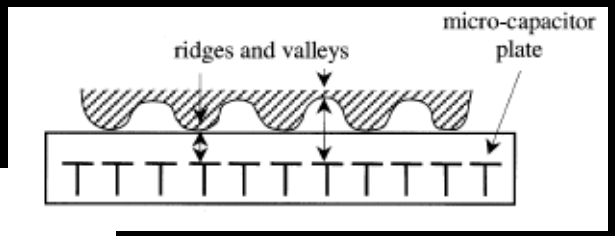


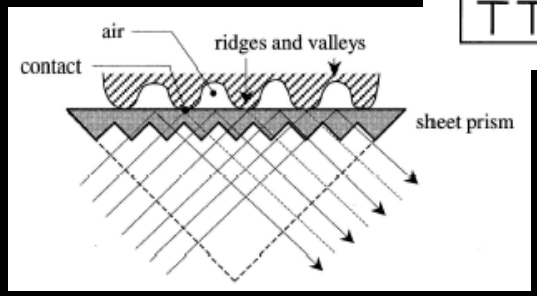
ePass :: Mustertafel :: 2

- Gesichtsausdruck
  - neutral
  - geschlossener Mund
- Kopfhaltung
- Augen
  - Augen sichtbar und in die Kamera gerichtet
- keine Kopfbedeckung
  - außer religiöse Gründe
  - Gesicht sichtbar
  - keine Schatten

Fingerabdruckerkennung :: Funktion

- Aufnahmevarianten
  - kapazitiv
  - optisch
  - Ultraschall





- Auswertealgorithmen
  - musterbasiert
  - minutienbasiert
  - Position der Schweißporen

Probleme mit biometrischen Systemen :: 1

- Merkmale sind nicht konstant
- Aufnahmebedingungen sind nicht identisch

-> **Nur eine Wahrscheinlichkeit der Übereinstimmung**

- Merkmal sind nicht verfügbar oder erfaßbar (körperliche oder kulturelle Einschränkungen)

-> **Ausweichmerkmale oder separate Prüfung**

Probleme mit biometrischen Systemen :: 2

- Gesicht
  - starke Abhängigkeit von Umwelteinflüssen
  - starke Veränderung des Merkmals
  - hohe Anforderungen an das Paßbild
  - FTE von ca. 10%

- Fingerabdruck
  - hygienische Vorbehalte
  - erkennungsdienstliche Behandlung
  - große Problemgruppe (Senioren, Arbeiter)
  - FTE von ca. 2%

Überwindungsworkshop

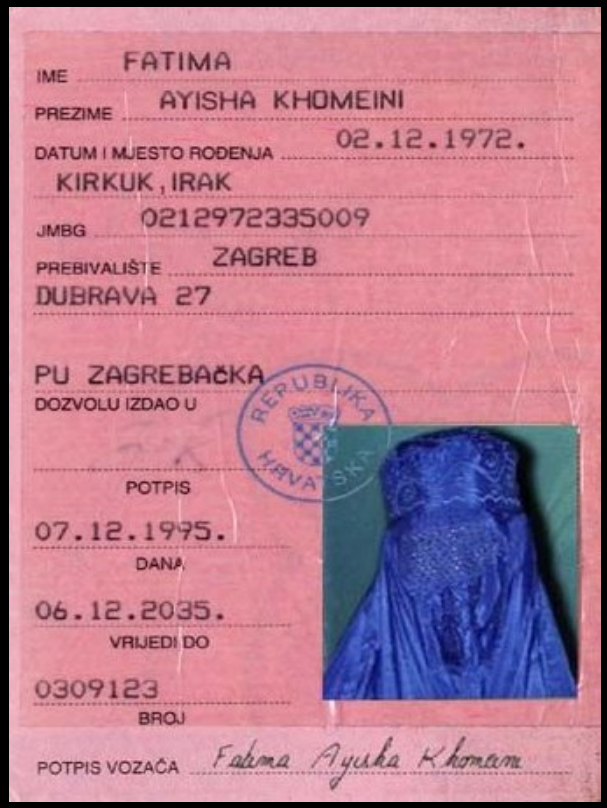
Workshop zur Überwindung biometrischer Systeme

Tag 2
21 Uhr

Workshop Area

Gesichtserkennung :: Verhinderung der Erkennung

- (Sonnen)brille
- falscher Bart
- viel Make up
- Schielen oder Lachen
- Verstecken des Gesichts (Haare oder Burka)



Fingerabdruck :: Verhinderung der Erkennung

- Sekundenkleber
- harte Arbeit :)
- Abschleifen
- Verätzen
- Verbrennen

Probleme mit biometrischen Systemen :: 4

- Manipulation von Template und Kommunikation
  - Löschen / Unterdrücken
  - Hinzufügen
  - Verändern

22. Chaos Communication Congress

Der ePass

Der ePass :: Kosten

- 59 Euro Standardpaß (37,50 Euro bzw. 91 Euro)
- 6500 Meldestellen, 400 Grenzkontrollpunkte, Polizeireviere
- Hardware + Wartung, Software + Konfiguration + Updates, Umbauten, Personal + Schulungen
- TAB-Bericht
  - einmalig 669 Mio Euro
  - laufend 610 Mio Euro

Der ePass :: Fazit

- alter Reisepaß bleibt weiterhin gültig
- **flächendeckende ED-Behandlung**
- Feldtest mit unausgereifter Technik und der gesamten Bevölkerung
- hohe Kosten für minimalen Sicherheitsgewinn
- keine Effektivierung der Grenzkontrollen
- Kein Sicherheitsgewinn, da der Paß auch bei defektem Chip gültig bleibt
- **Der ePass bietet keinen Schutz vor Terroristen!**

Der ePass :: Schreckensvisionen

- Einführung von Personalausweisen mit RFID und Biometrie für jeden Bürger
- Zentralisieren oder Vernetzen der Datenbanken
- Verwenden der Daten zu Fahndungszwecken
- Leaken sensitiver Daten oder kryptographischer Schlüssel
- Bugs im Betriebssystem der RFID-Karten
- technische Weiterentwicklung mit noch größerem Überwachungspotential (funktionierende Identifikation per Gesichtserkennung)

Informationen und Kontakt

starbug@berlin.ccc.de

https://www.ccc.de/epass
https://berlin.ccc.de/index.php/Biometrie