

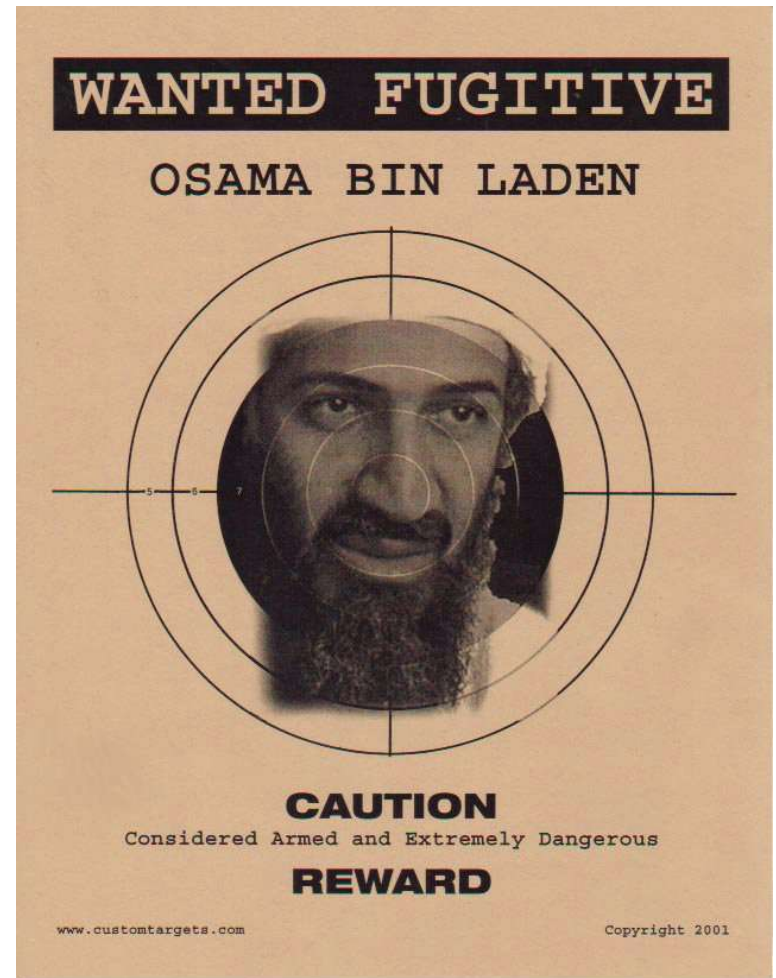
Biometrische Reisepässe in der Einführung

Matthias Brüstle
<m@mbsks.franken.de>



Kommunikationsnetz Franken e.V.

9-11



Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004

- Paß soll ein Speichermedium enthalten
- spätestens ab Mitte 2006: Gesichtsbild im Speichermedium
- spätestens ab Ende 2007: Fingerabdruck im Speichermedium

LogIn Jetzt anmelden ?

- Startseite
- Nachrichten
- Promis, Kino & Musik
- Wetten, dass..?
- Sport
- Volks-Rente
- Volks-Notebook
- Geld & Job
- Auto
- Reise
 - Last Minute
 - Pauschalreisen
 - Billigreisen
 - Baustein-Reisen
 - Ferienflüge
 - Hotel
 - Mietwagen
 - Reisekasse & Recht
- Digital Leben!
- Gesund & Fit
- Bauen & Wohnen
- Fun & Games
- Singles
- Erotik

Er hat einen Chip, kostet 59 Euro Jetzt gibt's den neuen High-Tech-Reisepaß

Er soll mehr Sicherheit für uns alle bringen. Der Reisepaß mit digitalisiertem Foto und Fingerabdruck. Ein echtes High-Tech-Ding. Es soll beispielsweise helfen, Verbrecher aufzuspüren.

Seit gestern gibt es den sogenannten elektronischen Paß, kurz ePaß genannt.

Er kostet 59, ist 33 Euro teurer als der alte und enthält einen Chip, auf dem die persönlichen Daten des Inhabers sowie sein Foto gespeichert werden. Später sollen zudem Fingerabdrücke erfaßt werden.

Hintergrund der Neuerung: Der ePaß soll schwerer zu fälschen sein als sein Vorgänger. Langfristig sollen dank der im Chip gespeicherten Daten die Grenzkontrollen elektronisch ablaufen können.



Bundeminister Otto Schily mit dem neuen Reisepaß

Innenminister Otto Schily (SPD) ist begeistert. Viele Deutsche allerdings stehen dem neuen Paß skeptisch gegenüber. Sie finden ihn nicht nur unnötig teuer, sondern fürchten auch den Mißbrauch der gespeicherten Daten.

Info

Antworten zum neuen Reisepaß – klicken Sie hier!

Urlaub buchen

- Last Minute
- Pauschalreisen
- Billigreisen
- Baustein-Reisen
- Ferienflüge
- Hotel
- Mietwagen

Urlaubswetter

Mallorca 22°

Mein Reiseziel

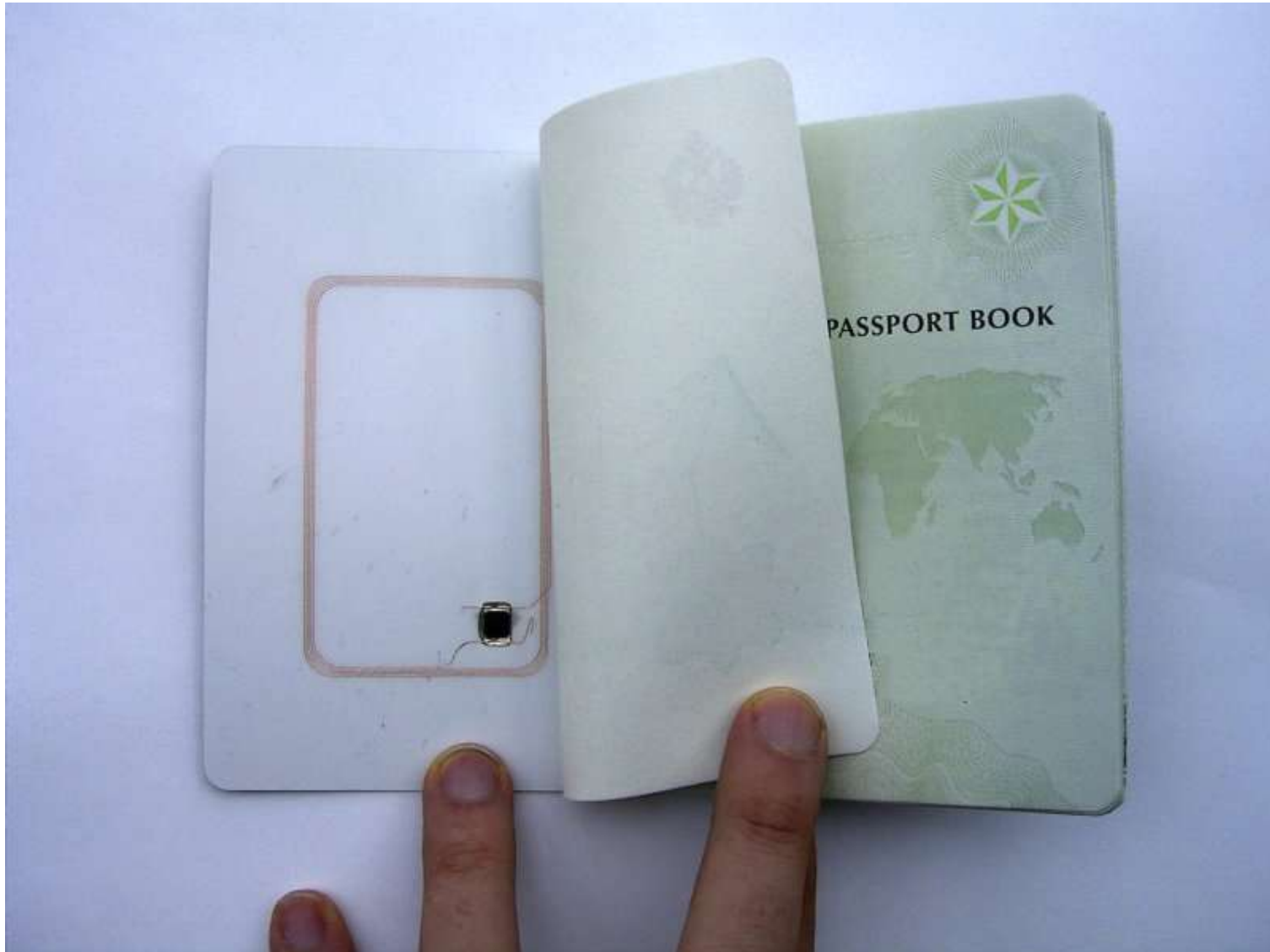
Reise-Services

- Reise-Newsletter
- Luftbilder
- Reiseführer
- Urlaubsplanner
- Welt-Klimakarte
- Reise-Checkliste
- Währungsrechner
- Storno-Rechner

Geld-Service

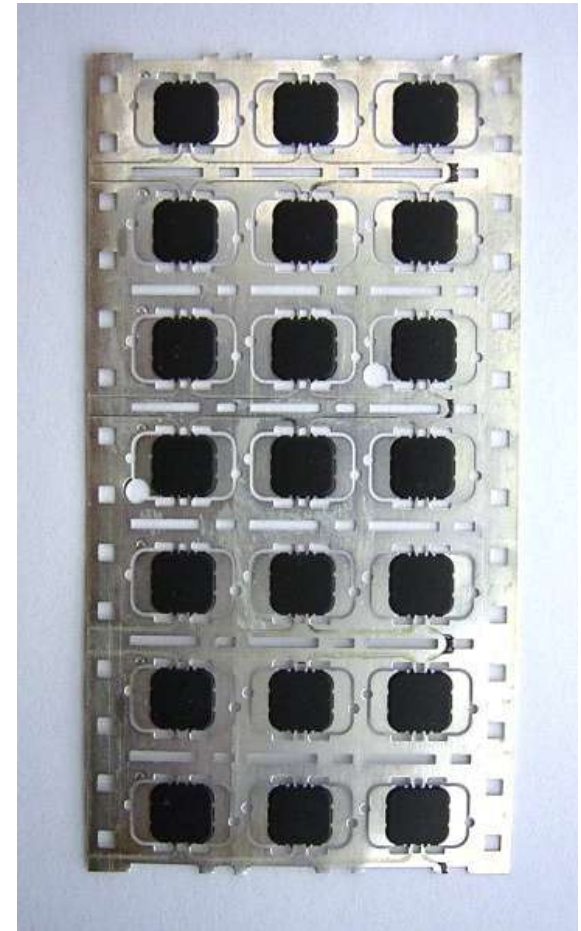
Wie gut sind Online-Kredite?
Kredite: Beratung darf nichts kosten

Speichermedium



Speichermedium: Technik

- Smart Card Chip
- Kontaktloses Interface nach ISO/IEC 14443 (auch Stromversorgung)
- Minimum 32kB EEPROM, besser 64kB, am liebsten noch mehr



Daten

- EF.COM: Index
- EF.DG1: Machine Readable Zone
- EF.DG2: Gesichtsbild
- EF.DG3: Fingerabdruck (in D ab 2007)
- EF.DG4: Irisbild (nicht in D geplant)
- EF.DG15: Public RSA Key (optional)
- EF.SOD: Digitale Signatur
- Weitere Fotos, Unterschrift, persönliche Daten (Geburtsort, Telefonnr., ...), ...

DG2: Gesichtsbild

- Foto
- Datenformat (JPEG, JPEG2000)
- Bildart
- Bildquelle/-qualität
- "Feature Points"
- Haar-/Augenfarbe
- Geschlecht
- Gesichtsausdruck
- "Feature Mask"
- Kopfhaltung (Meßfehler)

DG3: Fingerabdruck

- Fingerabdruckbilder (keine extrahierten Merkmale)
- Fingerposition (Zeigefinger)
- Datenformat (JPEG, JPEG2000, WSQ)
- Datenquelle/-qualität
- Scan-/Bildauflösung

Ablauf in Deutschland

- Antrag im Einwohnermeldeamt
 - 59 EUR
 - Paßfoto nach neuen Richtlinien
- Digitale Übermittlung der Daten zur Bundesdruckerei GmbH nach Berlin
- Druck des Paßes
- Sendung zum Einwohnermeldeamt

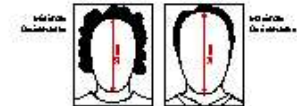
Fotorichtlinien Deutschlands

- 35mm x 45mm
- Gesichtshöhe 32-36mm (ICAO: 29-34mm)
- Gesicht zentriert
- scharf und kontrastreich
- gleichmäßig und schattenfrei ausgeleuchtet
- Hintergrund einfarbig hell mit Kontrast zu den Haaren
- gute Fotoqualität
- farbneutral
- apathischer Gesichtsausdruck und geschlossener Mund
- gerade in die Kamera blicken
- Augen geöffnet und deutlich sichtbar
- Keine Sonnenbrillen und Spiegelungen in Gläsern
- Keine Kopfbedeckung (außer aus religiösen Gründen)

Fotomustertafel

MUSTERFOTO

Das Musterfoto zeigt Passhöhe in vertikaler Ebene und ist als Referenz für die Höhe und Passhöhe im Foto zu verwenden. Die Höhe des Kopfes ist in der Abbildung mit einem vertikalen Maßstab dargestellt. Die Breite des Kopfes ist in der Abbildung mit einem horizontalen Maßstab dargestellt. Die Höhe des Kopfes ist in der Abbildung mit einem vertikalen Maßstab dargestellt. Die Breite des Kopfes ist in der Abbildung mit einem horizontalen Maßstab dargestellt.



FORMAT

Das Format des Fotos ist ein Quadrat mit einer Seitenlänge von 35 mm. Die Höhe des Kopfes ist in der Abbildung mit einem vertikalen Maßstab dargestellt. Die Breite des Kopfes ist in der Abbildung mit einem horizontalen Maßstab dargestellt.



SCHÄRFE UND KONTRAST

Das Foto muss in hoher Schärfe und Kontrast sein. Die Augen müssen scharf und kontrastreich sein. Die Augen müssen scharf und kontrastreich sein.



ABLEUCHTUNG

Das Foto muss gleichmäßig abgeleuchtet sein. Die Augen müssen gleichmäßig abgeleuchtet sein. Die Augen müssen gleichmäßig abgeleuchtet sein.



HINTERGRUND

Der Hintergrund des Fotos muss einfarbig und hell sein. Die Augen müssen einfarbig und hell sein. Die Augen müssen einfarbig und hell sein.



FOTOQUALITÄT

Das Foto muss in hoher Qualität sein. Die Augen müssen in hoher Qualität sein. Die Augen müssen in hoher Qualität sein.



KORPORATION UND GESICHTSAUSDRUCK

Das Foto muss einen neutralen Gesichtsausdruck zeigen. Die Augen müssen einen neutralen Gesichtsausdruck zeigen. Die Augen müssen einen neutralen Gesichtsausdruck zeigen.



AUGEN UND BLICHRICHTUNG

Die Augen müssen direkt in die Kamera blicken. Die Augen müssen direkt in die Kamera blicken. Die Augen müssen direkt in die Kamera blicken.



BRILLENTRÄGER

Die Augen müssen durch die Brillengläser sichtbar sein. Die Augen müssen durch die Brillengläser sichtbar sein. Die Augen müssen durch die Brillengläser sichtbar sein.



KOPFBEDECKUNG

Die Augen müssen durch die Kopfbedeckung sichtbar sein. Die Augen müssen durch die Kopfbedeckung sichtbar sein. Die Augen müssen durch die Kopfbedeckung sichtbar sein.



Symmetrically Challenged: Lichtbildbelehrung für schiefe Gesichter

Hiermit bestätige ich, dass ich von der Ausweisbehörde über die Qualität/Beschaffenheit meines vorgelegten Lichtbildes belehrt wurde.

Ich bestehe auf Annahme dieses Lichtbildes durch die Passbehörde.

Entstehende Schadensersatzansprüche, wegen Abweisung an einer Landesgrenze oder auf Grund polizeilicher Identitätsvorstellungen, kann ich gegenüber der Passbehörde nicht geltend machen. Die Kosten für einen neuen Ausweis habe ich voll zu tragen.

Schutzmechanismen: Passive Authentication

- Daten werden von Document Signing CAs signiert (RSA 2048bit, ECDSA 224bit, Country Signing CA 3072/256bit)
- Schutz vor Veränderung der Daten
- kein Schutz vor Kopie

Schutzmechanismen: Basic Access Control

- Datenzugriff erst nach Authentisierung mit Schlüssel
- Schlüssel wird aus MRZ berechnet (Entropie laut BMI 56bit, Obergrenze in D)
- Auslesen der Daten erst nach Öffnen des Paßes
- Schutz vor unbemerktem Auslesen/
Mitlauschen

Entropie im MRZ

- Paßnummer: 9 Dezimalstellen
- Geburtsdatum: 100 Jahre mit je 365 Tagen
- Ablaufdatum: 10 Jahre mit je 365 Tagen
 - 56 bits
- Paßnummer: Behördenkennzahl + laufende Nummer
 - Bayr. 8752, Erl. 8912, M. 9508-13, N. 8919, R. 8596/7
(www.pruefziffernberechnung.de)
- Geburtsdatum: Alter schätzbar
- Ablaufdatum: Feiertage?

Schutzmechanismen: Active Authentication

- Paß authentifiziert sich mit einem Private Key (1024bit RSA)
- Public Key in EF.DG15, damit zertifiziert
- Schutz vor Kopie

weitere Schutzmechanismen

- Extended Access Control
 - Ähnlich Basic Access Control, aber mit wirklich geheimem Schlüssel
 - Zugriff nur für autorisierte Terminals
- Data Encryption
 - Mit geheimem Schlüssel
 - Zugriff nur für autorisierte Terminals
- Beides nicht spezifiziert

Der Deutsche Weg

- Alternative Active Authentication
 - ECDH
- Extended Access Control für Fingerabdruck
 - Kartenverifizierbare ECDSA-Zertifikatskette
 - ECDH
- Spezifikation noch nicht abgeschlossen

Noch mehr Sicherheit

- Abschirmung: Metallgewebe in einem Paßdeckel (AFAIK nicht in Deutschland geplant)
- DIY-Abschirmung: Alufolie nah am Chip einlegen, eventuell noch besser Mu-Metall

„Was passiert mit meinem ePass, falls der Chip nicht mehr funktioniert?“

„Wenn der Chip nicht mehr funktionieren sollte, bleibt der Reisepass weiterhin ein gültiges Reisedokument, denn die herkömmliche Personenkontrolle kann weiterhin durchgeführt werden.“

Werden in Zukunft Pässe mit kaputtem Chip gefälscht?

Literatur

- www.icao.int
- www.icao.int/mrtd/Home/index.cfm
- www.heise.de/ct/aktuell/meldung/65898

Mahlzeit

Matthias Brüstle
<m@mbsks.franken.de>



Kommunikationsnetz Franken e.V.