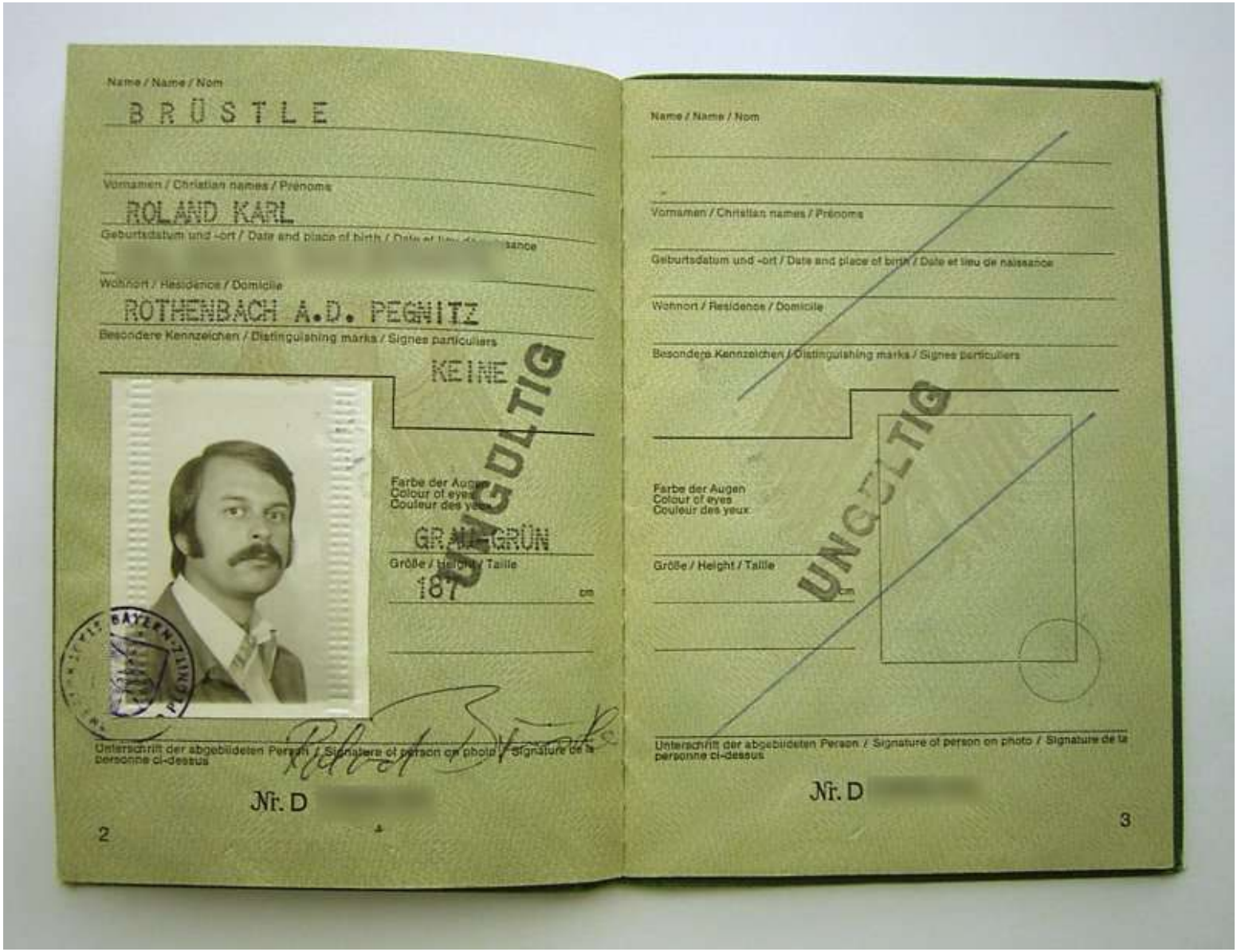
# Reisepaß mit Chip

Matthias Brüstle
<m@mbsks.franken.de>


Kommunikationsnetz Franken e.V.

# Früher



Name / Name / Nom

BRÜSTLE

Vornamen / Christian names / Prénoms

ROLAND KARL

Geburtsdatum und -ort / Date and place of birth / Date et lieu de naissance

Wohnort / Residence / Domicile

ROTHENBACH A.D. PEGNITZ

Besondere Kennzeichen / Distinguishing marks / Signes particuliers

KEINE

UNGÜLTIG

Farbe der Augen
Colour of eyes
Couleur des yeux

GRAU-GRÜN

Größe / Height / Taille

187 cm

Unterschrift der abgebildeten Person / Signature of person on photo / Signature de la personne ci-dessus

Nr. D

2

Name / Name / Nom

Vornamen / Christian names / Prénoms

Geburtsdatum und -ort / Date and place of birth / Date et lieu de naissance

Wohnort / Residence / Domicile

Besondere Kennzeichen / Distinguishing marks / Signes particuliers

UNGÜLTIG

Farbe der Augen
Colour of eyes
Couleur des yeux

Größe / Height / Taille

Unterschrift der abgebildeten Person / Signature of person on photo / Signature de la personne ci-dessus

Nr. D

3

# ICAO

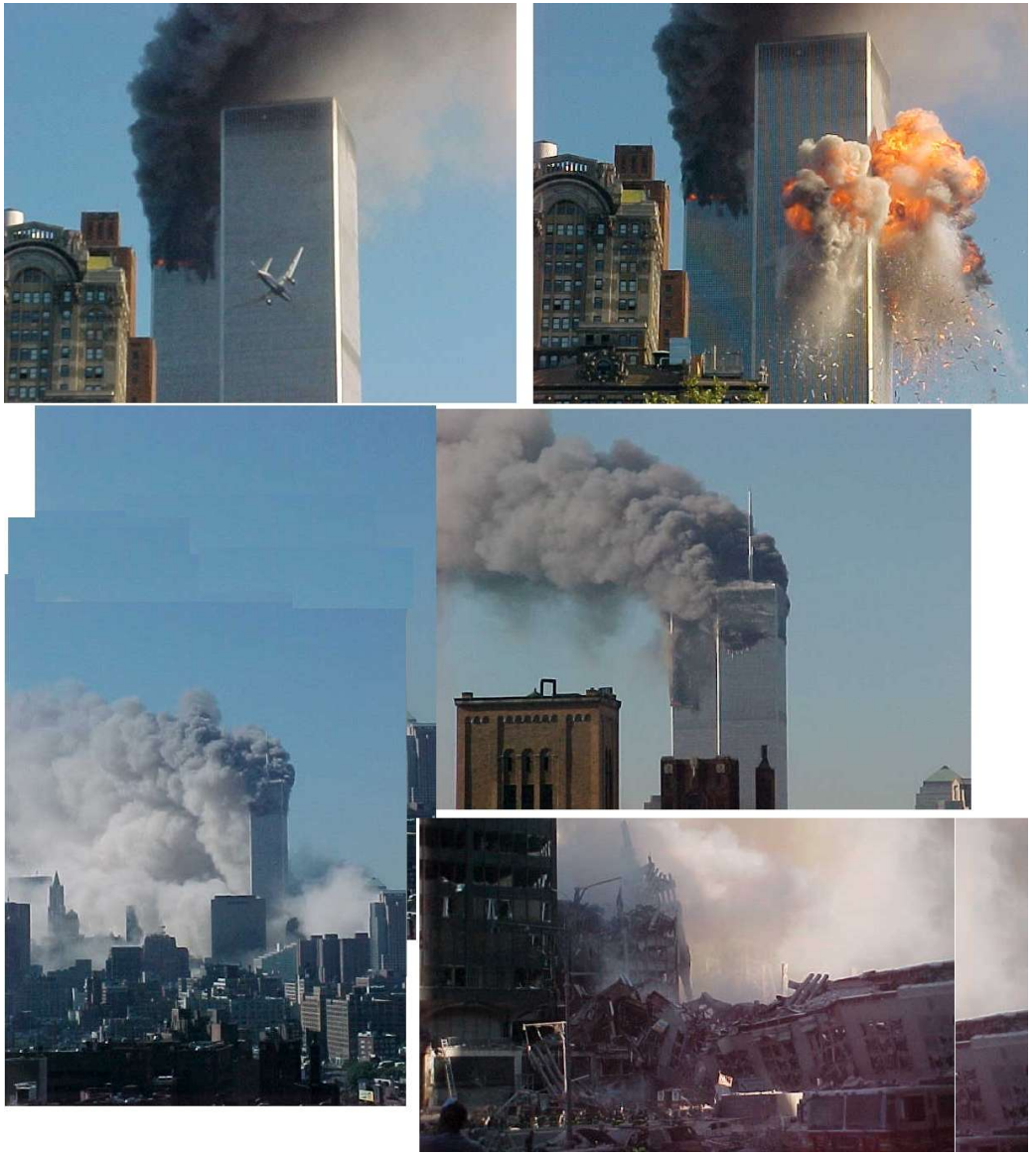
## International Civil Aviation Organization

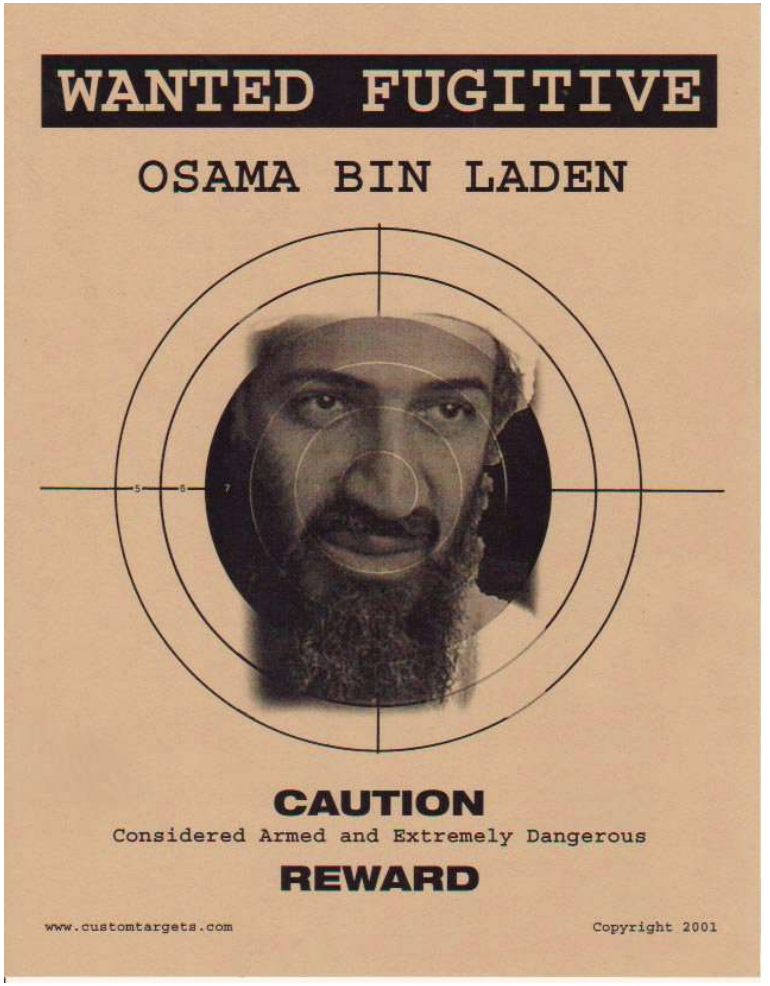
- Standards und empfohlene Vorgehensweisen in der zivilen Luftfahrt:
  - licensing of personnel
  - rules of the air
  - aeronautical meteorology/charts
  - operation of aircraft
  - aeronautical telecommunications
  - air traffic services
  - ...

# Jetzt: Machine Readable Travel Document (MRTD)

- Format
- Layout
- Machine Readable Zone (MRZ)

# 9-11




WANTED FUGITIVE
OSAMA BIN LADEN
CAUTION
Considered Armed and Extremely Dangerous
REWARD
www.customtargets.com
Copyright 2001

# Folgen

- Politischer Aktionismus
- Grund für Gesetze die sich die Innenminister und Staatssicherheiten aller Staaten wünschen
- Chip im Reisepaß

# Biometrie – Was ist das?

- Vermessen biologischer Merkmale
- Hier für:
  - Authentifizierung
  - Identifizierung

# Biometrie – Was gibt es?

- Gesicht
- Fingerabdruck
- Iris
- Retina
- Stimme
- Gang
- Handgeometrie
- ...

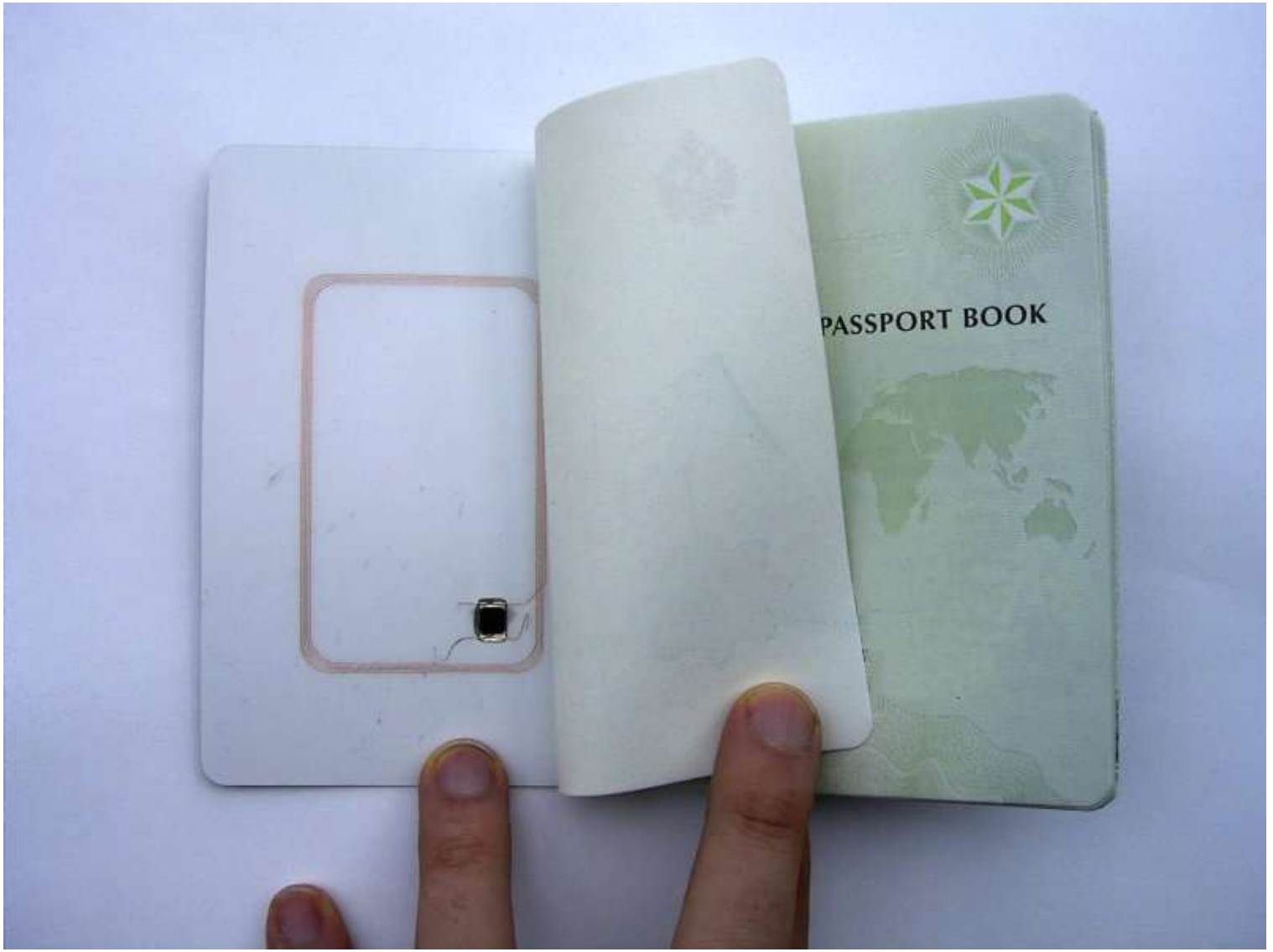
# Biometrie - Kennzahlen

- EER: Equal Error Rate
  - FVC2002 Top 10: 0.2 – 2 %
- FMR: False Match Rate (=FRR)
  - 1%: selten seinen Finger nochmal auflegen
- FNMR: False Non-Match Rate (=FAR)
  - 0.1%: unwahrscheinlich, daß sich ein Terrorist für mich ausgeben kann, aber ...
  - bei 80 Mio. Leuten werden 80000 als identisch erkannt

# Biometrie - Probleme

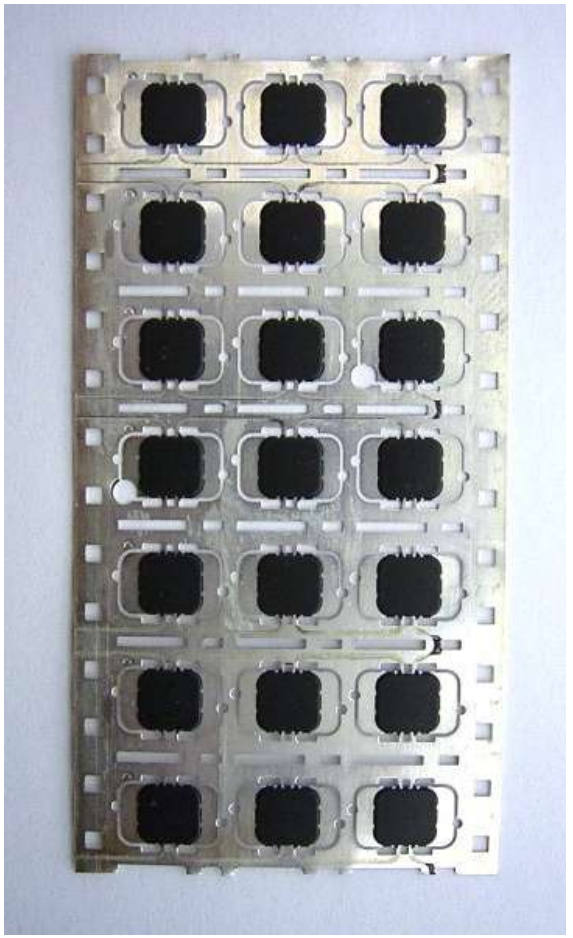
- Allgemeine Probleme
  - Nicht jeder für jedes Merkmal geeignet (permanent/temporär)
  - Verwechslungsgefahr
- Spezifische Probleme
  - Gesicht: keine deutliche Handlung notwendig
  - Fingerabdruck: Verschmutzung
  - Iris: Veränderlichkeit

# Zukunft



# Chip

- Smart Card Chip
- Kontaktloses Interface (ISO/IEC 14443)
- Mind. 32kB EEPROM, besser mind. 64kB



# Daten

- EF.COM: Index
- EF.DG1: Machine Readable Zone
- EF.DG2: Gesichtsfoto
- EF.DG3: Fingerabdruckbilder (optional)
- EF.DG4: Irisbilder (optional)
- EF.SOD: Digitale Signatur
- Weitere Fotos, Unterschrift, persönliche Daten (Geburtsort, Telefonnr., ...), ...

# DG1: **<<M<R<Z<<**

- Dokumententyp
- Land
- Nachname
- Vornamen
- Paßnummer (CD)
- Nationalität
- Geburtsdatum (CD)
- Geschlecht
- Ablaufdatum (CD)
- Zusätzliche Daten (CD)
- Gesamtprüfziffer

**P<UTOBRUESTLE<<MATTHIAS<ROLAND<<<<<<<<<<<<<<<**
**8834000012UTO7306022M1411018<<<<<<<<<<<<<<<2**

# DG2: Gesichtsfoto

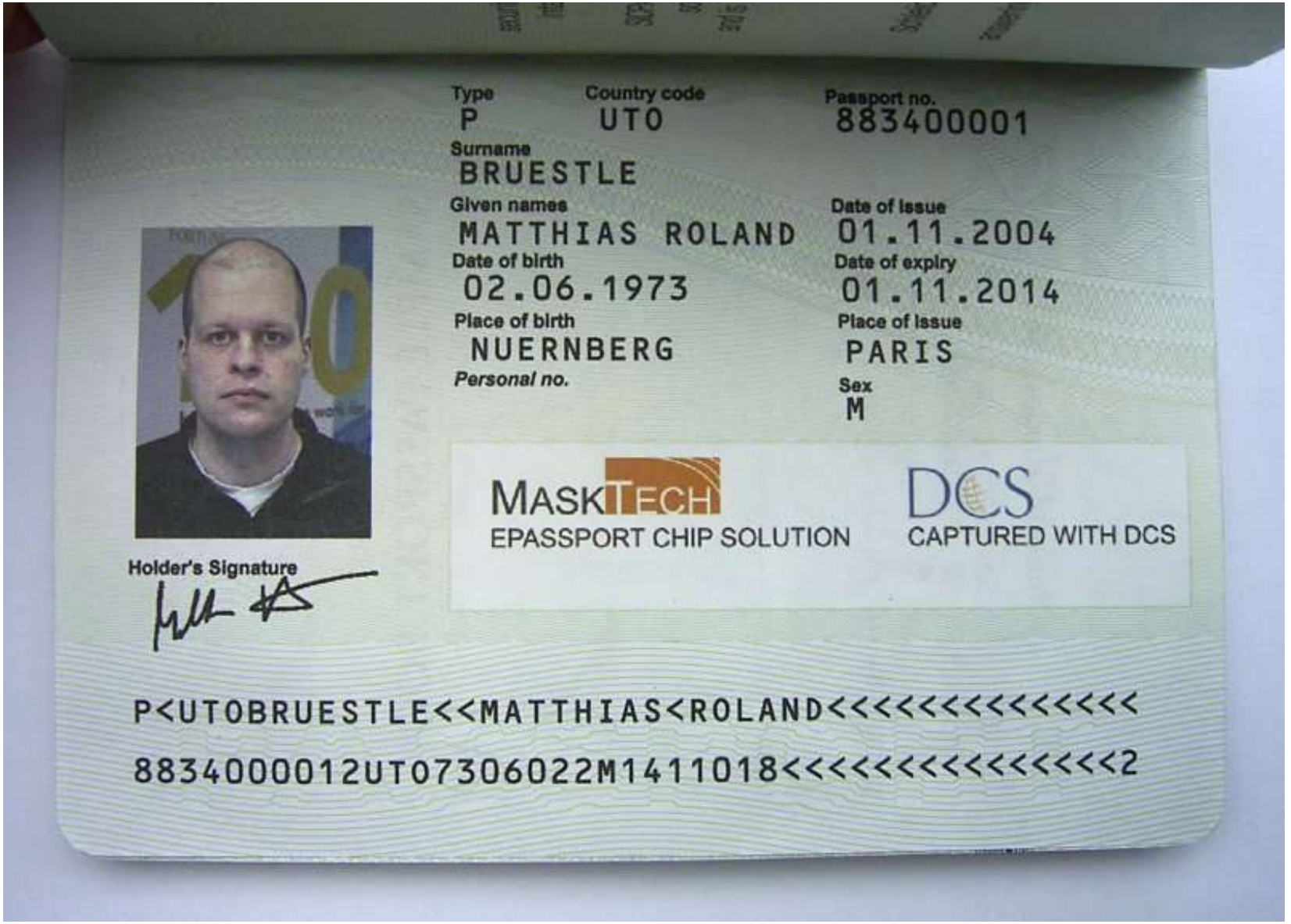
- Foto
- Datenformat (JPEG, JPEG2000)
- Bildart
- Bildquelle/-qualität
- "Feature Points"
- Haar-/Augenfarbe
- Geschlecht
- Gesichtsausdruck
- "Feature Mask"
- Kopfhaltung (Meßfehler)

# DG3: Fingerabdruckbilder

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

# Personalisierung

# Ergebnis


Type
P
Country code
UTO
Passport no.
883400001
Surname
BRUESTLE
Given names
MATTHIAS ROLAND
Date of issue
01.11.2004
Date of birth
02.06.1973
Date of expiry
01.11.2014
Place of birth
NUERNBERG
Place of issue
PARIS
Personal no.
Sex
M
Holder's Signature
MASKTECH
EPASSPORT CHIP SOLUTION
DCS
CAPTURED WITH DCS
P<UTOBRUESTLE<<MATTHIAS<ROLAND<<<<<<<<<<<<<<
8834000012UT07306022M1411018<<<<<<<<<<<<<<<2

# Datenschutz?

- USA: Wurschd!
- Europa: So geht des fei ned!
  (Innenminister: Fingerabdrück mechert mer aber scho!)

# Schutzmechanismen: Passive Authentication

- Daten werden von Document Signing CAs signiert (z.B. RSA)
- Schutz vor Veränderung der Daten
- kein Schutz vor Kopie

# Schutzmechanismen: Basic Access Control

- Datenzugriff erst nach Authentisierung mit geheimem Schlüssel
- geheimer Schlüssel wird aus MRZ berechnet
- Auslesen der Daten erst nach Öffnen des Paßes
- Schutz vor unbemerktem Auslesen/Mitlauschen
- UID fest oder zufällig?

# Schutzmechanismen: Active Authentication

- Paß authentifiziert sich mit einem Private Key (z.B. RSA)
- Schutz vor Kopie

# weitere Schutzmechanismen

- Extended Access Control
  - Wie Basic Access Control nur mit geheimem Schlüssel
  - Zugriff nur für authorisierte Terminals
- Data Encryption
  - Mit geheimem Schlüssel
  - Zugriff nur für authorisierte Terminals
- Beides nicht spezifiziert

# Literatur

- www.icao.int
- www.icao.int/mrtd/Home/index.cfm

# Mahlzeit

Matthias Brüstle
<m@mbsks.franken.de>

Kommunikationsnetz Franken e.V.