# Die neuen EU-Pässe

Versuch einer Zusammenfassung

CCC-Ulm - Chaosseminar 11.4.05
Stefan Schlott und Frank Kargl

# Quellen

- Vortrag “Security mechanisms of the biometrically enhanced passport” von Dr. Dennis Kügler (BSI)
- “Risiko Reisepass?” - c't 5'05
- http://www.icao.int/mrtd/
- http://www.icao.int/icao/en/atb/fal/mrtd/tagmrtd15/Docs/TagMrtd15_WP010_en.pdf
- http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf

# Wie es dazu kam…

- 13.12.2004: EU-Rat beschließt Reisepässe mit darin gespeicherten biometrischen Daten
- Maßgebliches Gremium: ICAO (International Civil Aviation Organization)
  - Veröffentlicht Rahmenspezifikationen für Pässe
    - Logical data structure, digital signatures, biometric deployment
  - Dr. Kügler (BSI) arbeitet an den ersten beiden mit
  - …war Referent auf der SPC 2005
  - …und da waren auch wir :-)

# (Kryptographische) Designziele

- Fälschungssicherheit
  - PKI-Zertifikate
- Kopierschutz
  - Verwendung eines SmartCard-Chips
- Zugriffskontrolle
  - Gegenseitige Authentisierung der beteiligten Geräte
- (möglichst) patentfrei

# Aufbau des Passes

- Herkömmlicher Reisepaß
  - Physikalische Sicherheitsmerkmale
  - Daten wie bisher
- ...zuätzlich: RFID-Chip
  - Daten der machine readable zone (MRZ)
  - Encoded face (JPEG)
- Paß auch ohne RFID gültig!


# Aufbau des Passes

- DG1 und DG2 zwingend
- Mögliche weitere Daten:
  - Weitere biometrische Merkmale
  - Visa-Informationen, Reisevermerke (DG17+)
  - "persons to notify"
  - ...

| | | | |
|---|---|---|---|
| Detail(s) Recorded in MRZ | DG1 | Document Type | |
| | | Issuing State or organization | |
| | | Name (of Holder) | |
| | | Document Number | |
| | | Check Digit - Doc Number | |
| | | Nationality | |
| | | Date of Birth | |
| | | Check Digit - DOB | |
| | | Sex | |
| | | Date of Expiry or Valid Until Date | |
| | | Check Digit - DOE/VUD | |
| | | Optional Data | |
| | | Check Digit - Optional Data Field | |
| | | Composite Check Digit | |
| Encoded Identification Feature(s) | GLOBAL INTERCHANGE FEATURE | DG2 | Encoded Face |
| | Additional Feature(s) | DG3 | Encoded Finger(s) |
| | | DG4 | Encoded Eye(s) |
| Displayed Identification Feature(s) | DG5 | Displayed Portrait | |
| | DG6 | Reserved for Future Use | |
| | DG7 | Displayed Signature or Usual Mark | |
| Encoded Security Feature(s) | DG8 | Data Feature(s) | |
| | DG9 | Structure Feature(s) | |
| | DG10 | Substance Feature(s) | |
| | DG11 | Additional Personal Detail(s) | |
| | DG12 | Additional Document Detail(s) | |
| | DG13 | Optional Detail(s) | |
| | DG14 | Reserved for Future Use | |
| | DG15 | Active Authentication Public Key Info | |
| | DG16 | Person(s) to Notify | |

# RFID

- Radio Frequency Identification
- Für passive RFIDs: Stromquelle = Trägerwelle
- Auslese-Entfernung: 10-15 cm
  - ...aber Abhören mit geeigneten Antennen auch mehrere Meter
  - Geplante USA-Schutzvorrichtung: Metallfolie im Paß
- Ansprechen der Chips über deren ID
  - Unique Identifier!

# Zugriffsschutz

- Zu Beginn: Chip gesperrt
  - Chip wählt zufällige ID für Kommunikation
- Basic access control
  - Optische Infos vom Ausweis benötigt
  - Zugang zu Daten der MRZ plus Bild
- Extended access control
  - Besteht aus Chip authentication und Terminal authentication
  - Zugang zu sensitiven Daten (z.B. Fingerabdruck)

# Verwendete Verfahren

- Secret Key: 3DES
- Hashfunktionen: SHA1, SHA256, SHA512
- Public Key:

| | Länderebene | Herstellerebene |
|---|---|---|
| RSA/DSA | 3072 | 2048 |
| ECDSA | 256 | 224 |

- Signaturen: “Card verifiable signatures”

# Basic access control

Zugriffschlüssel k auf Karte vorhanden

Wähle Zufallszahl $r_{chip}$

$r_{chip}$ korrekt erhalten?

Sitzungsschlüssel aus Schlüsselhälften erz. (xor)

MRZ optisch auslesen
Berechne daraus Schlüssel k

Wähle Zufallszahl $r_{reader}$
und Schlüsselhälfte $K_{reader}$

$E_k(r_{chip}, r_{reader}, K_{reader})$

$E_k(r_{chip}, r_{reader}, K_{chip})$

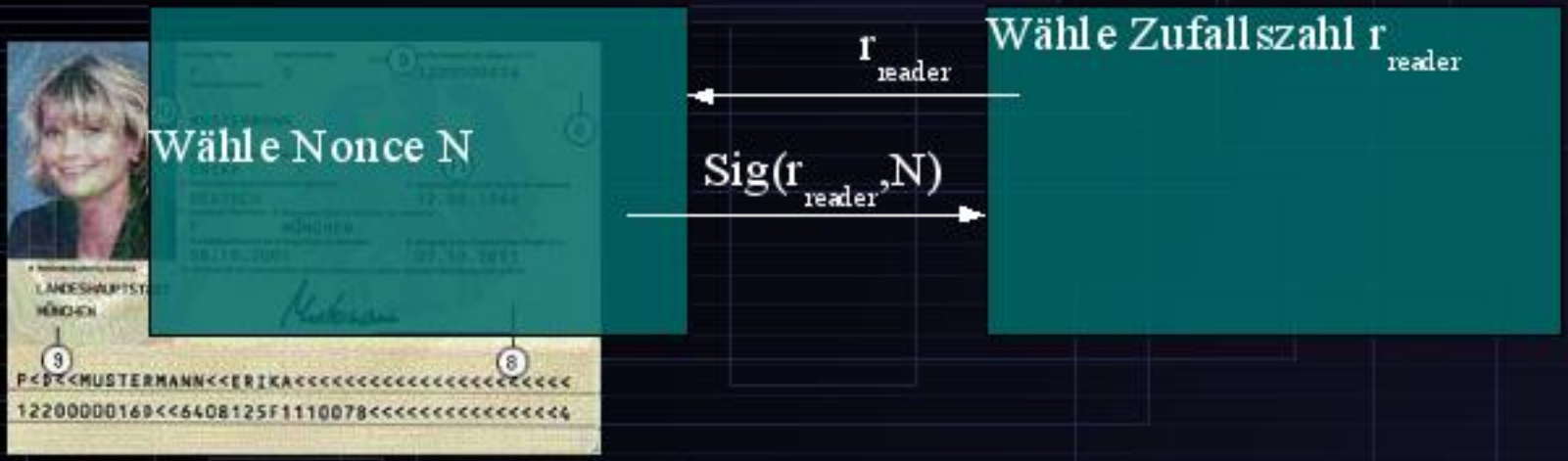
$r_{reader}$ korrekt erhalten?

Sitzungsschlüssel aus Schlüsselhälften erz. (xor)

# Basic access control

- Verwendeter Algorithmus: 3DES
- Problem: Entropie der verwendeten MRZ-Daten:
  - ~56 Bit bei numerischen MRZ-Daten
  - ~73 Bit bei alphanumerischen MRZ-Daten
  - Nur numerische Daten mit Prüfziffer: Bleiben ~40 Bit
- Daher: Nur Zugriff auf Daten, die auch optisch ablesbar wären
- Restliche Daten: Extended access control

# Active Authentication




- Status: Noch nicht standardisiert
- “Anti cloning feature”
- Ohne Basic Authentication: MitM-anfällig

# Extended access control

- Status: Noch nicht standardisiert
- Vorschläge an ICAO:
  - Match on chip
    - Fixiert auf Algorithmen im Chip
    - Chips nicht leistungsfähig genug
  - PIN-basiert
    - Nicht praktikabel
  - PKI-basiert
    - Vorschlag vom BSI
    - “likely to be adopted”

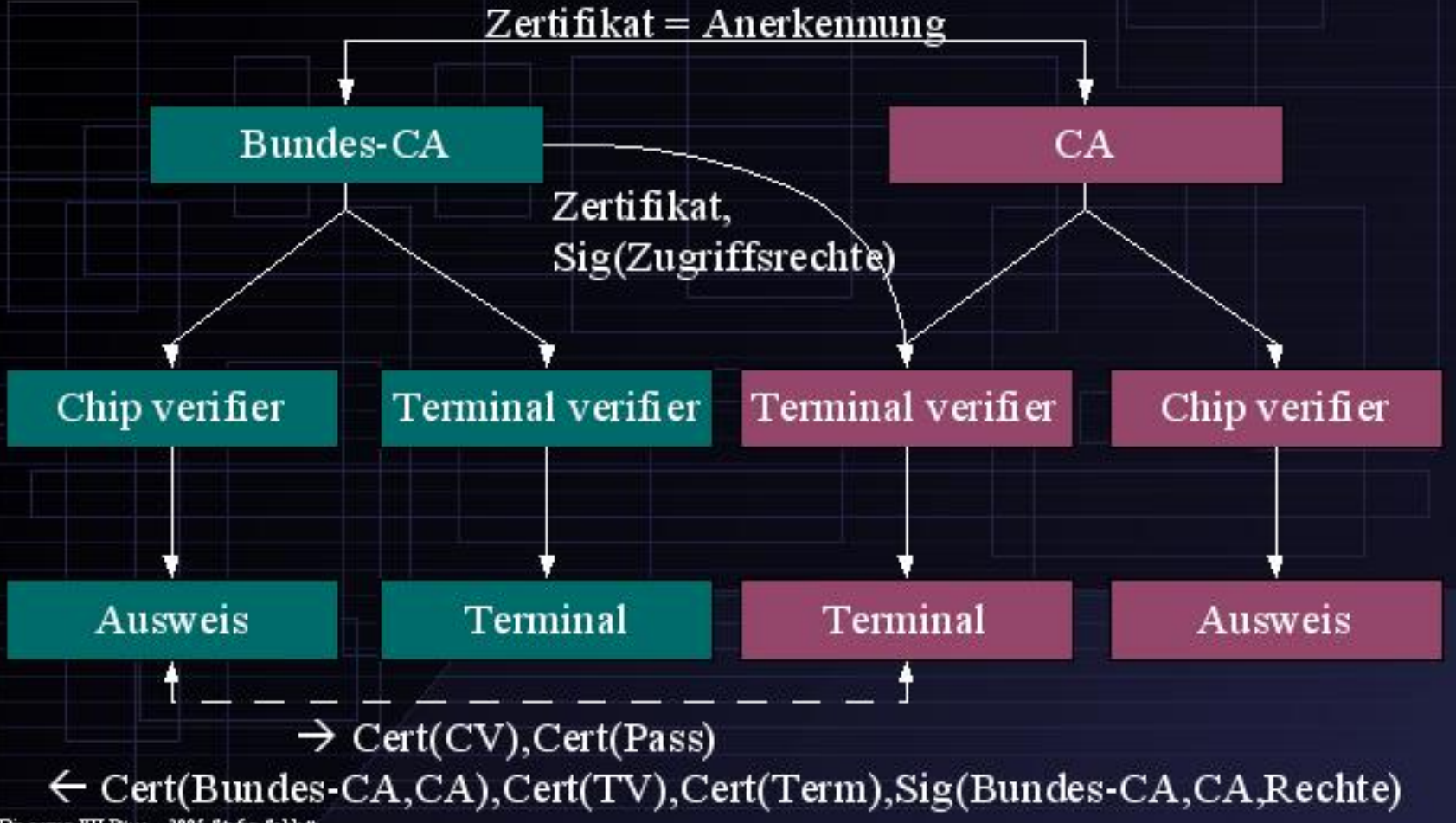
# Chip authentication

- Im Prinzip: Diffie-Hellman-Austausch
- “Cipher-based authentication”: Wenn Daten nach Schlüsselaustausch lesbar, war's wohl der richtige :-)
- Neuer Schlüssel: Nutzt volle Schlüssellänge

# Terminal authentication

- Vermutlich: Einfaches Challenge-Response
- Identität des Terminals wird bestätigt
- Zugriffsrechte für das Terminal werden übertragen

# CA-Struktur


Zertifikat = Anerkennung
Bundes-CA
CA
Zertifikat,
Sig(Zugriffsrechte)
Chip verifier
Terminal verifier
Terminal verifier
Chip verifier
Ausweis
Terminal
Terminal
Ausweis
→ Cert(CV),Cert(Pass)
← Cert(Bundes-CA,CA),Cert(TV),Cert(Term),Sig(Bundes-CA,CA,Rechte)

# Certificate revocation

- SmartCards nie online: Keine revocation lists
- “Revocation” über Expiry Date
- Aber: SmartCards haben auch keine Uhr
  - Creation Date von Zertifikaten lesen
  - Wenn jünger als gespeichertes Datum: Datum ersetzen
- Kurze Gültigkeitsdauer für...
  - Terminals: Gestohlene Terminals nur kurz nutzbar
  - Zugriffsrechte: “Druckmittel” bei Mißbrauch

# Fazit

- Mal von der Politik ("Biometrie") abgesehen: Das Design sieht brauchbar aus
- Standard läßt viele Freiheiten zu – z.B. USA:
  - Feste IDs für RFID-Chip
  - Basic Authentication nicht nötig für Datenzugriff
  - Geringe Entropiemenge in MRZ
- Vieles noch "im Fluß", aber immerhin positiver Eindruck