Biometrie

puts the “e” in ePass

Biometrie

Definition

allgemein: Vermessung biologischer Merkmale

klassische Biometrie

- Biostatistik, Medizin, z.B. BMI ...

modernde Biometrie

- Erfassung möglichst eindeutiger biologischer menschlicher Merkmale

Ziele

Identifizierung

- one-to-many Vergleich

Verifizierung

- one-to-one Vergleich, z.B. Passkontrolle

Methoden

- Augen: Iris oder Retina
- Fingerabdruck
- Foto, bzw. Gesichtserkennung
- Handschrift
- genetischer Fingerabdruck
- ...

Anforderungen

besonders im Bereich Passkontrolle

- Minimierung der Falschrückweisungsrate und Falschakzeptanzrate
- Erfasste Merkmale müssen *stabil* bleiben
- Niedriger Bedienungsaufwand bei Massenanwendung
- Einfaches *Enrollment* (erstmalige Erfassung und Speicherung), im Rahmen bisherigen Zeitbedarfs
- Kosten

Fingerabdruck

- Mittelwert aus drei Messungen
- Match-on-card oder Datenbank
- Probleme im Enrollment in ca. 2%
- Verletzungen oder übermässige Abnutzungen der Finger beeinflussen Stabilität (kritisch laut TAB)
- FAR nur mit besonderem Aufwand niedrig

Gesichtserkennung

- Besondere Anforderungen an Fotos für Enrollment
- FRR teilweise ca. 20% (BSI BioP II)
- Stabilität “ausreichend” (TAB), notfalls neues Enrollment
- Hohe Erkennungsrate laut TAB

Handgeometrie

- Unterscheidbarkeit für Verifizierung nur in kleinen Szenarien brauchbar

- Stabilität erst ab Alter >20 ausreichend

Iriserkennung

- Keine umfangreichen Studien zur Erkennungsleistung in Großanwendungen.
- Geringe Akzeptanz
- Hohe Anforderungen an Bedienung
  - Besondere Verhaltensvorschriften
  - Einlernzeit

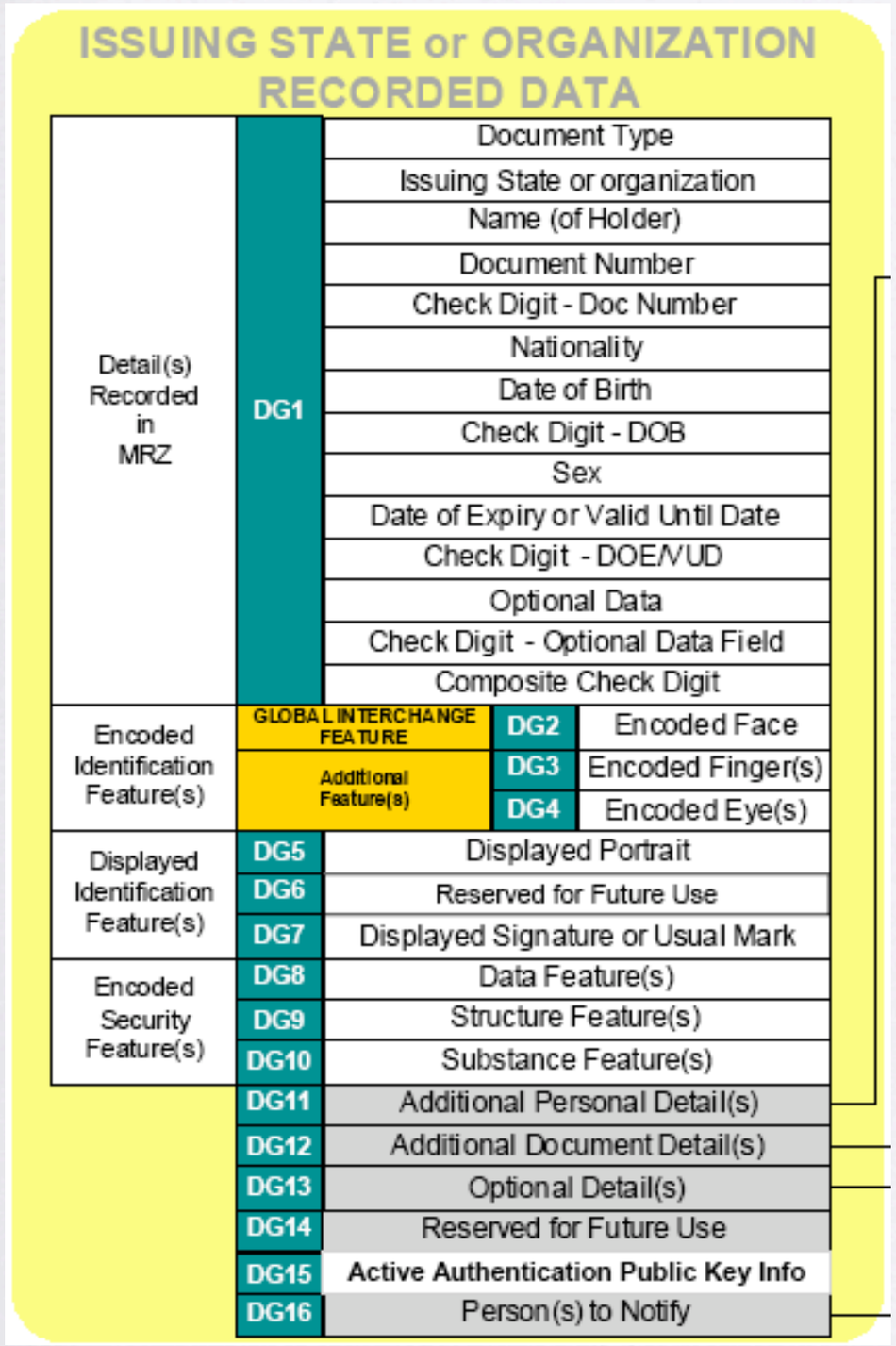
genetischer Fingerabdruck

- Genom ist eindeutig (mod Zwillinge)
- Vollständiger Genomvergleich unmöglich, daher Verwendung von Mirkosatteliten-Polymorphismus
- Teuer, zeitaufwändig.
- Statistische Sicherheit ungleich tatsächlicher Sicherheit

der ePass

- Reisepass seit 1.11.05 mit digitalem Foto
- Ab März 2007 mit digitalen Fingerabdrücken
- Verwendung von RF-Chip
- Reichweite laut Spec 10 cm, Kommunikation ließ sich in Experimenten auch in >2m abhören
- Standard nach ICAO (International Civil Aviation Organization) und EU-Gremium

ePass Details



Maschinenlesbarer Teil Bestandteil auch älterer Pässe

DG2 auf RF-Chip in neuen Pässen

DG3 für Fingerabdrücke

DG15 Public Key Authentication

Was wird gespeichert?

- Laut BSI: Bild als ca. 15 kB JPEG in DG2
- Eventuell 20 Bytes “Facial Informations”
  - Geschlecht, Augenfarbe, Koordinaten ...

Zugriffsschutz

- Daten sind signiert und verschlüsselt.
- Elliptic Curve Digital Signature Algorithm
- Verwendung einer zwei stufigen PKI

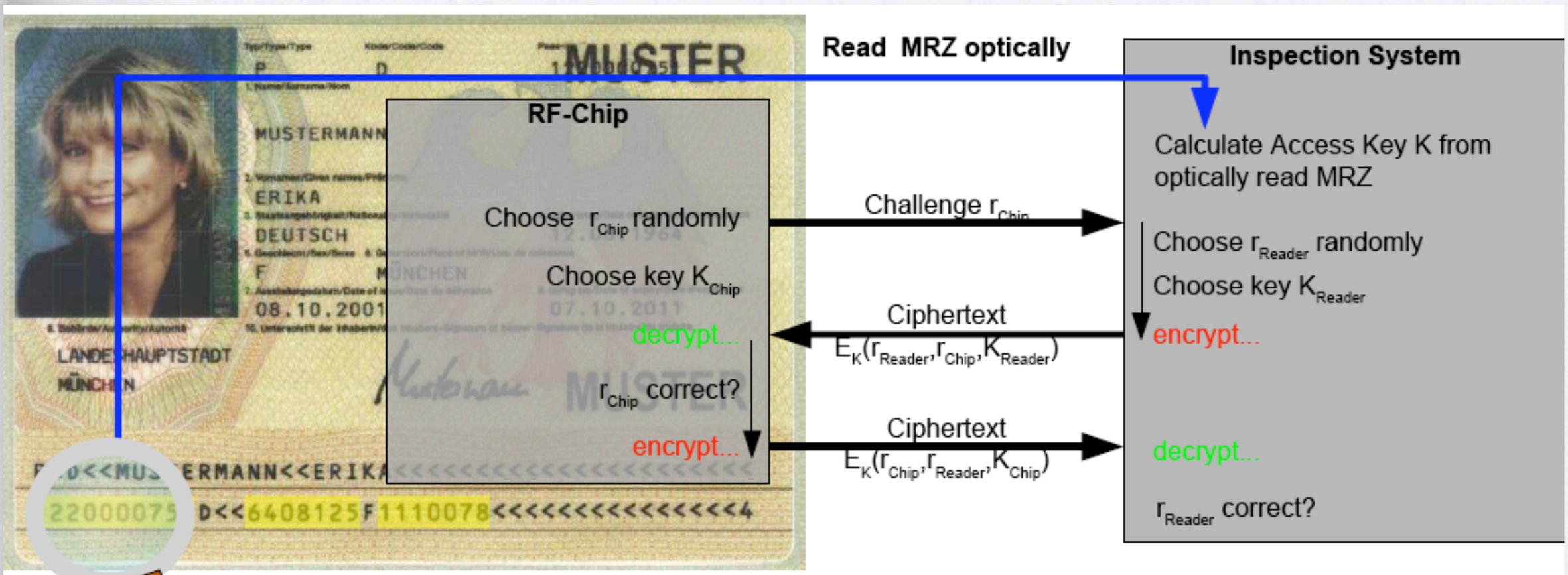
Algorithmus	***Country Signing CA [Bit]***	***Document Signer [Bit]***
RSA / DSA	3072	2048
ECDSA	256	224

Public Key

- Jeder Pass besitzt eigenes Schlüssel Paar
- Public Key in DG15 gespeichert
- Private Key im nicht auslesbaren Teil des Chips

Basic Access Control

für Foto nach DG2



After successful authentication:

- Secure Messaging
- Chips grants access to less-sensitive data

Schlüssel (Theorie)

Zugriffschlüssel wird berechnet durch:

- Passnummer: 109 Möglichkeiten
- Geburtsdatum, ca. 365*102 Möglichkeiten
- Ablaufdatum: 365*10 Möglichkeiten

ca. 56 bit Schlüsselstärke

Schüssel Bewertung

- Kommunikation läßt sich mitschneiden
- Angriff auf Zugriffschlüssel ausreichend, um Datenverkehr lesen zu können.
- Da Foto als “less-sensitive data” angesehen wird, nur 56 Bit

Schlüssel (Praxis)

- Nicht alle Daten zwingend gleichverteilt

- Bei fortlaufenden Nummern Korrelation
  Passnumer <-> Ausgabedatum, bzw. Ablaufdatum

- Geburtsdatum bekannt oder Jahr schätzbar

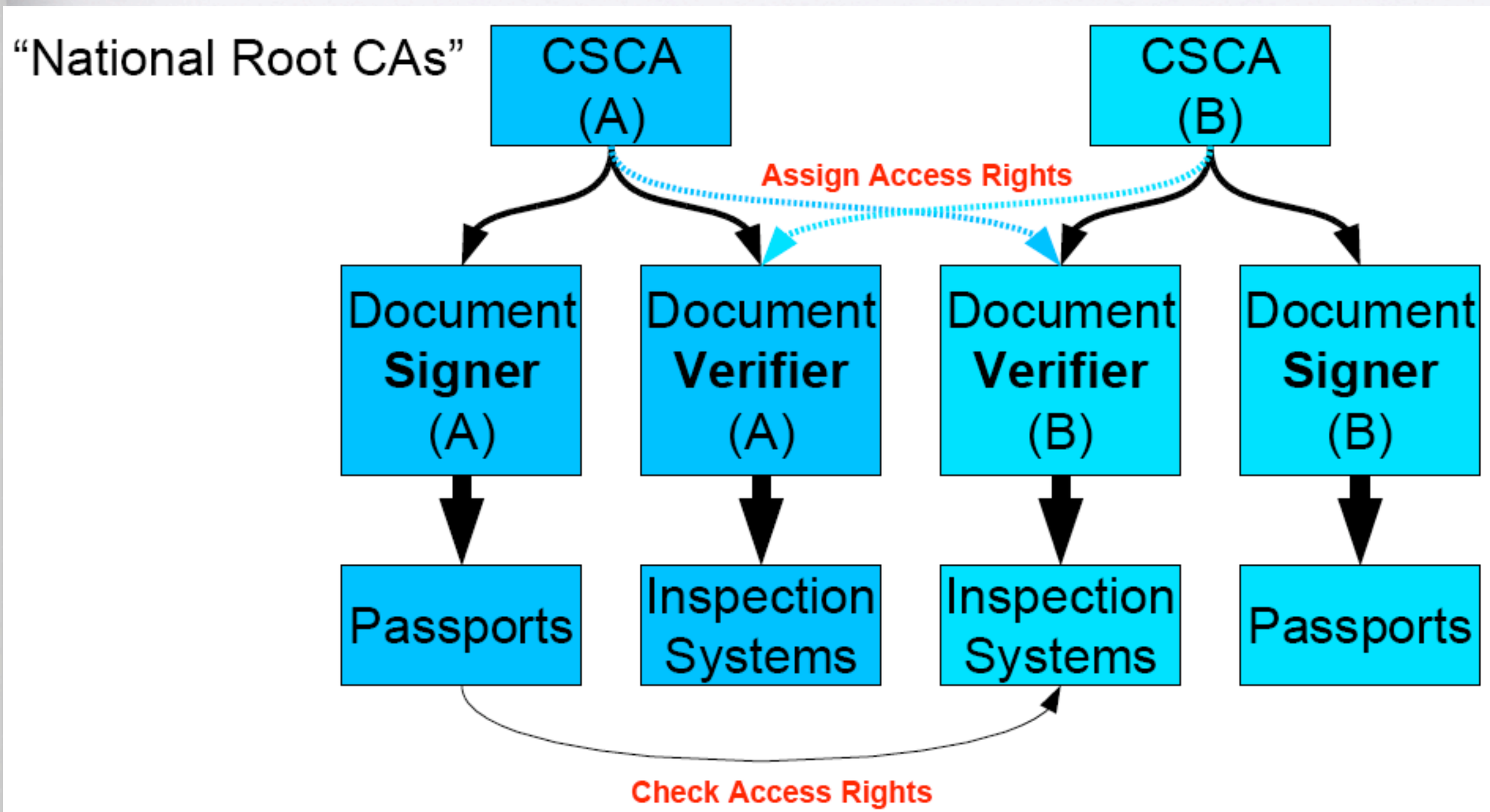
Extended Access Control

- Zusätzlicher Schutz für Fingerabdrücke
- Add-on zu ICAO-Zugriffsschutz
- Public Key Mechanismus
- Lesegerät muß sich identifizieren
- Spezifische Rechte pro Lesegerät
- kryptographischer Coprozessor auf ePass

Details?

- Nach BAC Austausch eines neuen Schlüssels per Diffie-Hellman
- Vergleichbar mit HTTPS mit Client-Zertifikaten
- Zertifikat des Lesegerätes muß vom ePass verifiziert werden
- Genaue Spezifikation steht noch aus

Wer darf was?


"National Root CAs"
CSCA (A)
CSCA (B)
Assign Access Rights
Document Signer (A)
Document Verifier (A)
Document Verifier (B)
Document Signer (B)
Passports
Inspection Systems
Inspection Systems
Passports
Check Access Rights

Probleme

- Was bei gestohlenen Lesegeräten?
    - Etwas Schutz durch BAC
- Certificate Revocation
    - Wie ohne Online-Verbindung des Chips?

Quellen

- c't 5/2005
- Büro für Technikfolgen-Abschätzung am Deutschen Bundestag
- BSI
- Pressestelle des Auswärtigen Amts
- CCC
- ICAO
- Wikipedia