

---

# Einfachere Nutzung von Ausweisen im Gesundheitswesen durch Verwendung von Biometrie



Dr. Dirk Scheuermann

**Fraunhofer**

Institut  
Sichere Informations-  
Technologie

---

---

# Übersicht

- Ausgangslage und Motivation
- Technische Aspekte und Sicherheitsaspekte beim Einsatz von Smartcards mit Biometrie
- Aktueller Stand: Gesetzeslage, Standardisierung, Datenschutz
- eCard-Initiative

---

## Ausgangslage und Motivation

geschützte  
Anwendungen  
auf Ausweiskarten

stärkere Bindung  
an den  
Ausweisinhaber

einfachere  
Handhabung

- Gesundheitskarte und Heilberufsausweis sind zentrale Bestandteile der Telematikinfrastuktur und sind gegen Missbrauch durch unbefugte Personen zu schützen.
- Aktueller Stand der Spezifikation: Benutzer-Authentisierung mittels PIN.
- Zukünftig mögliche Ergänzung oder Alternative: biometrische Benutzer-Authentisierung: Handhabung ist einfacher, wenn nicht für jeden Vorgang eine PIN-Eingabe notwendig ist!

---

# Biometrische Verfahren

wissensbasierte  
Benutzer-Verifikation

biometrische  
Benutzer-Verifikation

- PIN/Passwort ist **personenbezogen**, biometrisches Merkmal ist **personengebunden** (kann nicht vergessen, verloren oder weitergegeben werden)
- Charakteristische biometrische Merkmale werden aus Rohmessdaten extrahiert (=> zusätzlicher Arbeitsschritt)
- keine exakte Übereinstimmung biometrischer Daten (=> kompliziertere Vergleichsverfahren, notwendige Bestimmung von Toleranzgrenzen)
- Manche biometrischen Daten sind öffentlich (z.B. Fingerabdruck vom Glas, Gesichtsbild von Kamera)



---

## Einsatz von Off-Card und On-Card-Matching \*)

Sicherheitsstatus  
am richtigen Ort  
setzen

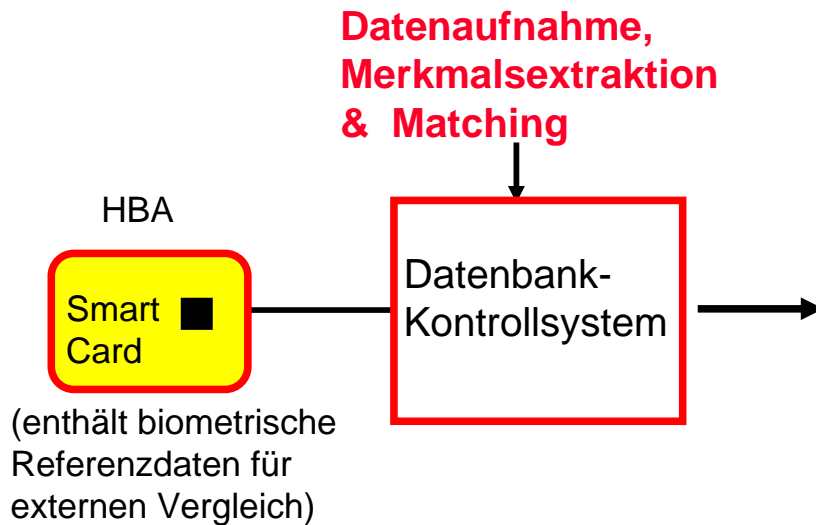
- Wenn das **Service-System** wissen muss, ob die biometrische Benutzer-Verifikation erfolgreich war, dann ist **Off-Card-Matching** angebracht. (=> Karte kann als Datenspeicher genutzt werden!)
- Wenn die **Smartcard** wissen muss, ob die biometrische Benutzer-Verifikation erfolgreich war, dann ist **On-Card-Matching** angebracht.
- mögliche Nutzung von **On-Card-Matching** für Sicherheitsanwendungen **außerhalb der Karte**:
  - Verifikationsergebnis geschützt übertragen
  - „Hybrid-Lösung“: z.B. Freigabe von Authentisierungsdaten

\*) neuer Begriff in der Standardisierung: „On-Card-Comparison“ !

Seite 5



## Beispiel für Off-Card-Matching



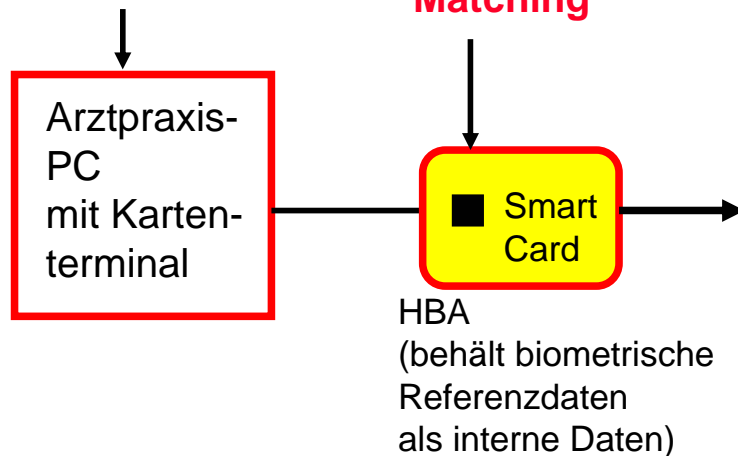
### Geschützter Zugriff auf Patienten-Datenbank

- Wenn Benutzer-Verifikation **erfolgreich**, **ermöglichte** Zugriff auf Datenbank
- Wenn Benutzer-Verifikation **nicht erfolgreich**, **verweigere** Zugriff auf Datenbank

⇒ Kontrollsystem führt biometrischen Vergleich durch und reguliert Zugriff auf Datenbank

# Beispiel für On-Card-Matching

Datenaufnahme,  
Merkmals-  
extraktion



## Signieren elektronischer Rezept

- Wenn Benutzer-Verifikation **erfolgreich**, **ermögliche** Ausführung der Signaturfunktion
- Wenn Benutzer-Verifikation **nicht erfolgreich**, halte Signaturfunktion **gesperrt**

⇒ Karte führt biometrischen Vergleich durch und setzt erforderlichen Sicherheitsstatus

---

## weitere Aspekte bei On-Card-Matching (1)

- Biometrische Referenzdaten verbleiben in der Karte (-> besserer Datenschutz!)
- Begrenzte Kapazität von Smartcards muss berücksichtigt werden.
- Komplettes Verifikationssystem ist nicht auf einem Chip implementierbar – Datenerfassung und Merkmalsextraktion müssen außerhalb erfolgen (extern oder auf anderem Chip)

---

## weitere Aspekte bei On-Card-Matching (2)

- Verifikationsdaten müssen gesichert an die Karte übertragen werden (=> Vermeidung von Replay- und Datenacquisitions-Angriffen)
- Standardisierte Lösungen erfordern **standardisierte Formate** für extrahierte Merkmalsdaten

---

## Stand der Standardisierung

- **Smartcard-Kommandos** nach ISO/IEC 7816-4, -11  
– mit gesicherter Übertragung durch „Secure Messaging“
- Kartenterminals mit biometrischem Sensor nach **MKT-Spezifikation**
- **HPC-Spezifikation** sieht mögliche Nutzung von Biometrie (in späteren Versionen) vor
- Standardisierte Datenformate für **Merkmalsdaten** bisher **nur bei Fingerabdruck** (ISO/IEC 19794-2)
- bisher keinerlei Standards für **Algorithmen** zur Merkmalsextraktion und zum Merkmalsvergleich

---

# Rechtliche Situation

allgemeine Regelungen

- Biometrische Daten sind persönliche Daten
  - unterliegen dem Datenschutz
  - dürfen nur für den vorgesehenen Zweck verwendet werden

anwendungsspezifische Regelungen

- Signaturverordnung erlaubt Biometrie als **komplette Alternative** zur PIN, falls **Mechanismenstärke hoch** erreicht wird – bei **Mechanismenstärke mittel** nur als **Ergänzung** (sekundäre Verifikationsmethode)



---

## eCard Initiative

- Angestrebtes Ziel: Gemeinsamer Standard für Authentisierungs- und Signaturfunktion in **digitalem Personalausweis (ePA)**, **eGK** und **JobCard**
- JobCard-Funktionalität (Signatur) wird in ePA oder eGK integriert (keine separate JobCard!), ePA und eGK sind getrennte Ausweiskarten.
- **eGK-Funktionen** müssen gesondert geschützt werden (-> ggf. weitere biometrische Daten!)

---

## Zusammenfassung und Ausblick

- Entwicklungsstand von Smartcards erfüllt technische Voraussetzungen für On-Card-Matching für verschiedene Biometrien.
- On-Card-Matching ist auch für Zusatz-Funktionen der eGK – u.a. JobCard – geeignet.
- Rechtliche Rahmenbedingungen zum Einsatz von On-Card-Matching für elektronische Signaturen sind gegeben.
- Markt für On-Card-Matching Lösungen ist noch sehr beschränkt.
- Es bestehen noch Lücken im Bereich Testverfahren und Standardisierung.