Biometrie - Stand der Technik

Christoph Busch

Fraunhofer IGD / Hochschule Darmstadt / Gjøvik University College

BITKOM
Konferenz Biometrie im betrieblichen Einsatz

5. Mai 2010

Fraunhofer IGD

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES
fbmd FACHBEREICH MEDIA

HØGSKOLEN I GJØVIK

Zur Person

Biometrische Aktivitäten

- Convenor der ISO/IEC JTC1 SC37 WG3 Biometric Data Interchange Formats
- Sprecher der GI Fachgruppe BIOSIG
- Leiter der Arbeitsgruppe Biometrie im TeleTrust e.V.
- Mitglied des International Biometrics Advisory Council des European Biometric Forum

Aktuelle Forschungsprojekte

- Hochschule Darmstadt
  - FP6-IP 3D Face http://www.3dface.org
  - LOEWE CASED http://www.cased.de
  - BSI BioKeyS
- GUC:
  - FP7-IP TURBINE http://www.turbine-project.eu
  - FP7-TN BEST http://www.best-nw.eu

3D Face Biometric Research

CASED

TURBINE

BEST NETWORK

Überblick

- Biometrie
  - Stand der Technik
  - Projekte 3D-Face, TURBINE, HIDE, BEST, BioKeyS
- Forschungsthemen
  - Sicherheit für Biometrie
    - Sensor Sicherheit (Finger, 3D-Face am Laptop, Venen)
    - Erkennungsleistung (Sample Quality Metric - VIS)
    - Template Protection - Pseudonyme Identifikatoren
  - Biometrie für Sicherheit
    - Duplicate Enrolment Check (DEC)
    - Mobile Sicherheit
      - Nebenläufige Authentisierung
    - Online Transaktionen
      - Online-Banking
  - Gesellschaftliche Fragestellungen
    - Usability von Biometrie (das bezahlt keiner...)
    - Warum verkaufen natürliche Personen biometrische Daten

Einführung

Was ist Biometrie?

Die Vermessung („Metrik“) von Charakteristiken des menschlichen Körpers zum Zweck der Wieder-Erkennung.

Identität

„busch“

Identifikation - Verifikation

Identifikation:

- Wiedererkennung einer Person (1:n - Vergleich)

staff identity = „busch“

Verifikation:

- Prüfung einer Identitätsbehauptung (1:1 - Vergleich)


similarity: „71%“

(Comparison-Score)

Warum Biometrie?

Personen-Authentisierung durch:

- Wissen: Passwort, PIN, sonstiges Geheimnis
- Besitz: Magnet- oder Chipkarte, Schlüssel
- Körper: biometrische Charakteristik

Wissen oder Besitz kann man leicht verlieren,vergessen oder weitergeben, biometrische Charakteristika nicht ohne weiteres.

Vorteile

- Für den Betreiber:
  - Sicherheitspolitik kann nicht durch Delegation umgangen werden!
- Für die betroffene Person:
  - Identitätsmissbrauch wird erschwert

Password - Statistik

Password Statistik basierend auf 32 Millionen Einträgen

- System-Fehler bei www.rockyou.com
- 20% Namen und triviale Passworte
- Top 5 passwords

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622

Source: Imperva

Stand der Forschung

Forschungsaktivitäten

- National
  - BSI-Livefinger
  - BSI-BioKeyS
  - BKA-AGES
  - LOEWE-CASED
- International
  - 3D-Face
  - HUMABIO
  - TURBINE
  - HIDE
  - BEST
  - BioP@ss
- Ergebnisse
  - Fusion, Erkennungsleistungen, Interoperabilität

FP6 Integrated Project 3D-Face

- Authentisierung mit ePass und
  - 2D Gesichterkennung (Frankfurt easyPASS)
  - Fingerbilderkennung

- Multi-Biometrische System versprechen
  - eine bessere biometrische Erkennungsleistung
  - mehr Sicherheit gegenüber Replikaten einer biometrischen Charakteristik

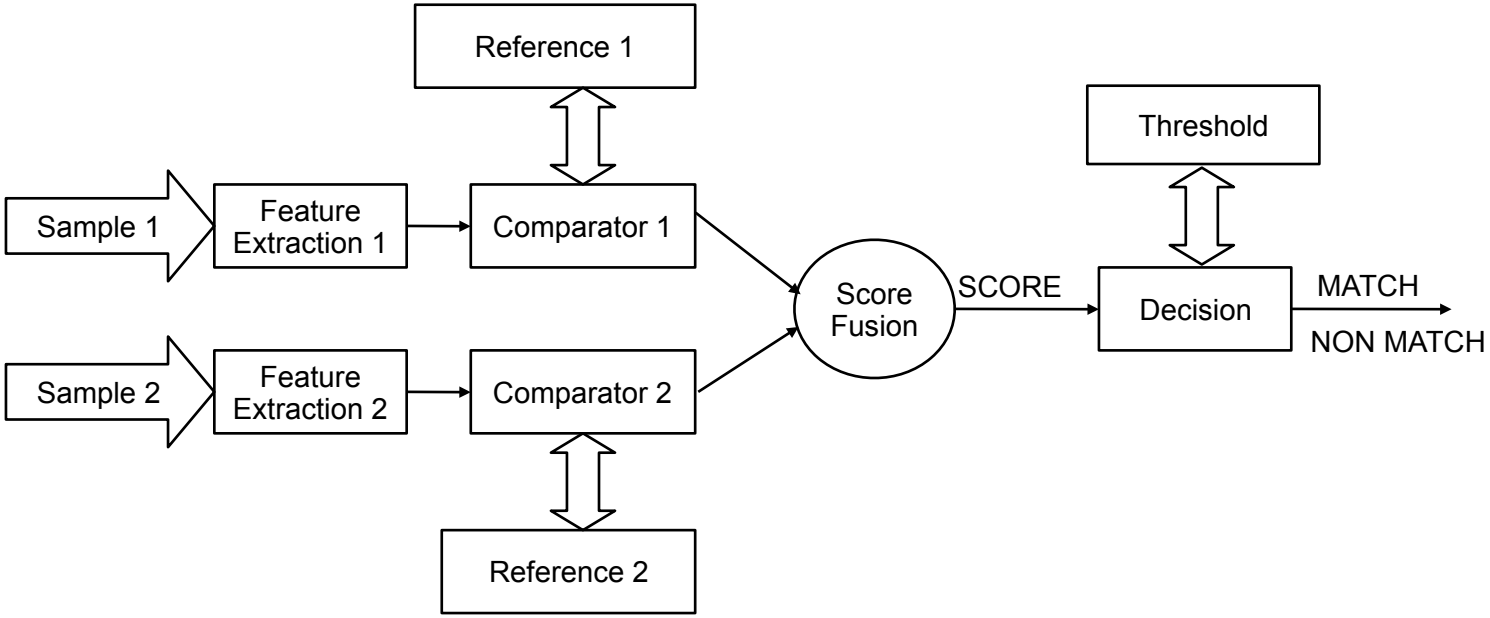
Unbeaufsichtigte Grenzkontrolle kann nur erreicht werden, wenn nicht-flüchtige Chrakateristika gemessen werden

Multi-Biometrie

Mult-Sensor, Multi-Modal, Multi-Algorithmen, Multi-Instance

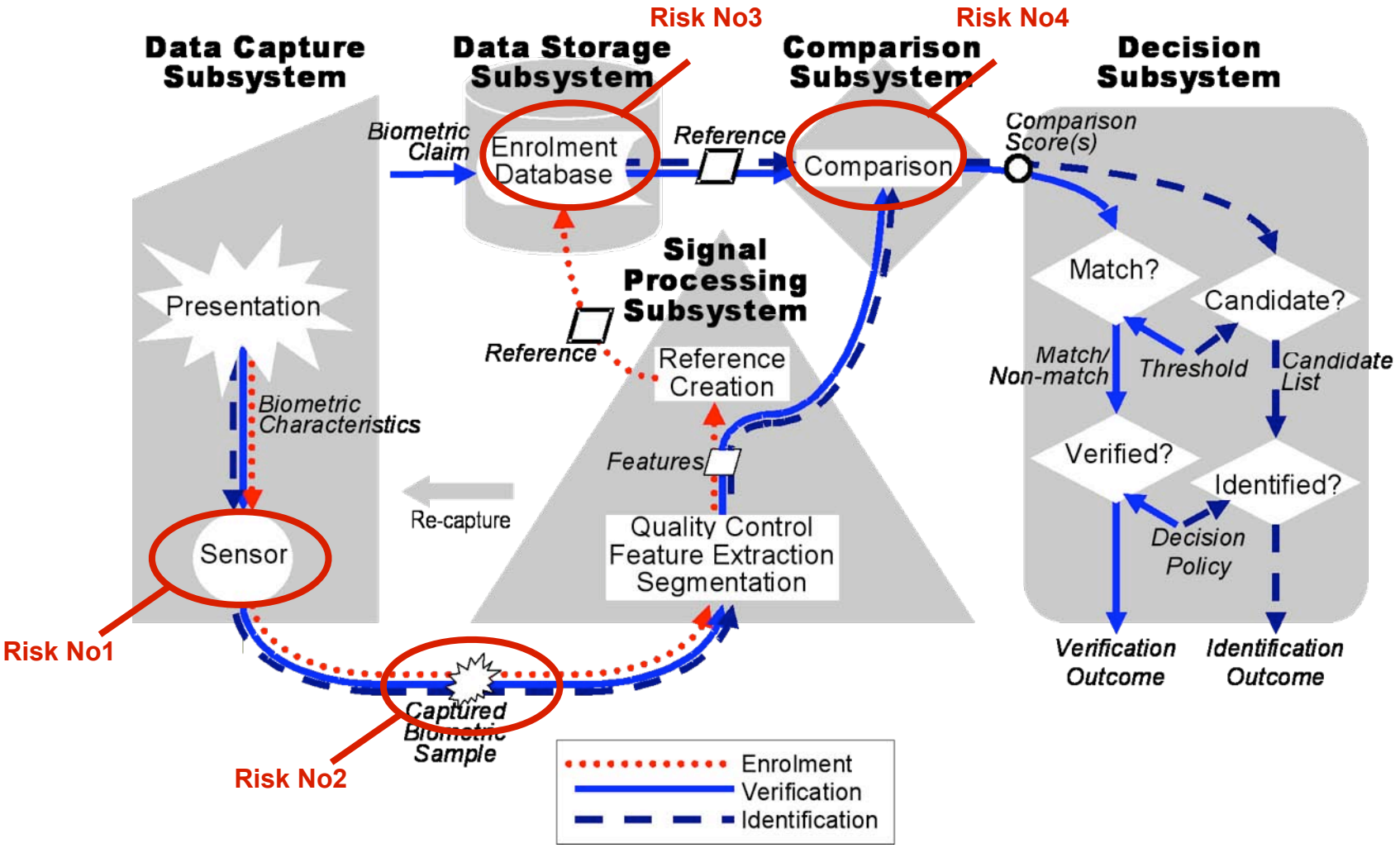
Fusionsmethoden (score-level fusion, decision-level fusion)

- Jede biometrische Komponente liefert einen comparison score.
  - Der Fusion Porzess integriert die Score-Werte
  - Nur der fusionierte score wird mit dem Schwellwert verglichen



Sicherheit für Biometrie

Risiken in Biometrischen Systemen



Source: ISO/IEC JTC1 SC37 SD11
Reference Architecture

Sicherheit von Sensoren

Gummi-Finger

SKorean fools finger printing system at Japan airport: reports

AFP

Thu Jan 1, 2:57 pm ET

Buzz Up | Send | Share | Print

AFP/File – A woman uses a biometric scanner at an airport. A South Korean woman barred from entering Japan last ...

TOKYO (AFP) – A South Korean woman barred from entering Japan last year passed through its immigration screening system by using tape on her fingers to fool a fingerprint reading machine, reports said Thursday.

The biometric system was installed in 30 airports in 2007 to improve security and prevent terrorists from entering into Japan, the Yomiuri Shimbun said.

The woman, who has a deportation record, told investigators that she placed special tapes on her fingers to pass through a fingerprint reader, according to Kyodo News.

Japan spent more than four billion yen (44 million dollars) to install the system, which reads the index fingerprints of visitors and instantly cross-checks them with a database of international fugitives and foreigners with deportation records, the Yomiuri Shimbun said.

Yahoo News am 1. Januar 2009

Sicherheit eines Fingerprint Sensors

Ist das eine überraschende Nachricht?

- Ein optischer oder kapazitiver Sensor misst die Papilliarleisten der Epidermis - die tote Hautoberfläche!

Source: Heise

Sicherheit eines Fingerprint Sensors

Angriff ohne Mithilfe oder Mitwissen der eingelernten Person

- Abnehmen eines Fingerabdrucks von glatter Fläche
  - z.B. Glas, CD-Hülle, Hochglanz-Zeitschrift mittels handelsüblichem Eisenpulver und Klarsicht-Klebeband
- Einscannen in den Rechner und nachbearbeiten:
  - Offensichtliche Fehler durch Abnahme/Scannen berichtigen, Bild invertieren
- Auf Folie ausdrucken
- Platine mit der Folie belichten und ätzen
- Platine mit Silikonkautschuk abformen

Lebenderkennung / Plagiaterkennung

Forschungsthemen

- 3D-Gesichterkennung - photogrammetrisch
  - Mit sechs eingebauten Laptop-Webcams
- Fingerbild-Sensoren, die „unter die Haut“ gehen
  - Bildgebende Verfahren aus der Medizin (z.B. Ultraschall)
  - Ergänzende Venen-Erkennung
- Schwachstellenanalyse
  - Machbarkeitsanalyse mit Plagiaten biometrischer Charakteristika und Einsatz
    - in (nicht-)kooperativen Anwendungen
    - in nicht-überwachten Anwendungen
- Zertifizierte Sensorsicherheit
  - Common-Criteria Prüfung von Sensoren und biometischen Systemem

Sicherheit bedingt Zuverlässigkeit der Sensorik

Forschungsziel:
Überwindungssichere Sensoren

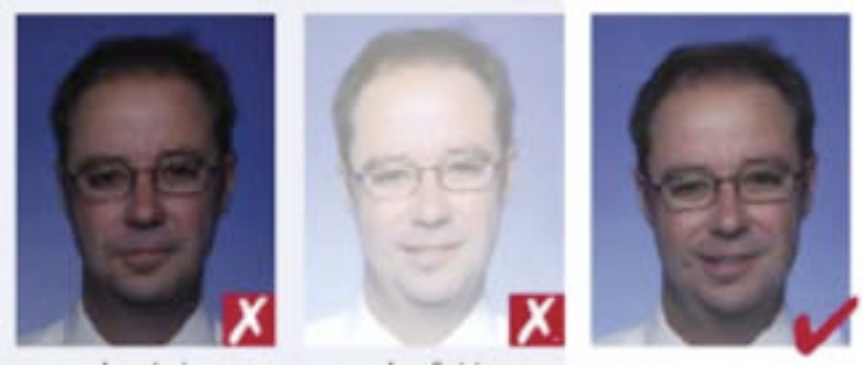
Sample Quality Metric

Signal-Qualität beim Enrolment ist
kritischer Faktor für die Leistung eines Biometrie-System

- Erfahrungen im ViS (EU DG JLS) und BioDev

Forschungsthemen

- Prädiktive Qualitätsmetriken, die
  einen zuverlässigen Vergleich ermöglichen
- Modalitäten: Gesichtsbild, Fingerbild, Irisbild
- Kalibrierung von Metriken
- Ground Truth Datenbanken



Die Zuverlässigkeit beginnt bei
der biometrischen Erfassung

Forschungsziel:

Objektive Metriken zur Bewertung biometrischer Samples

Biometrie und Datenschutz

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vom 7. März 2002)

- *„Es dürfen nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist“ - nicht diskriminierende rasche Aufklärung*
- Bei der Anwendung von biometrischen Verfahren können Zusatzinformationen anfallen (Krankheitsbilder etc.)
  „Die gespeicherten und verarbeiteten Daten dürfen keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben“
- *„Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten, sind abzulehnen“*
- Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit Ausweisinhaber übereinstimmen.
  „Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen“

Template Protection

Mögliche Angriffe auf Referenzdaten

- Diebstahl von biometrischen Referenzbildern
  - keine Bilder hinterlegen
- Cross-Matching: Identische Templates können personenbezogene Querbezüge zwischen verschiedenen Datenbanken herstellen
  - Anzahl der direkten Abbilder einer biometrischen Charakteristik ist begrenzt
  - Diversifikation der Referenzen aus einer Quelle
- Die biometrische Charakteristik selbst ist nicht erneuerbar
  - Rückrufbarkeit der biometrischen Referenz
- Überschussinformation
  - Referenz als reinen pseudonymen Identifikator (PI) ausbilden

Template Protection

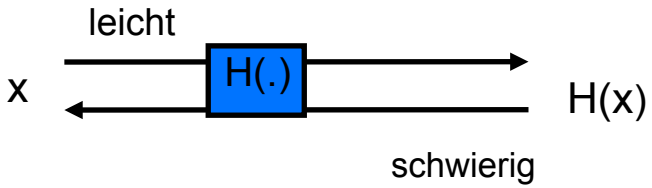
Ansatz analog zur UNIX Password Authentisierung

- Öffentlich zugängliche Datei: /etc/passwd

  `id:<login_name>:hash(password)`

- Authentisierung:

  `hash(input) =?= hash(password)`



Template Protection

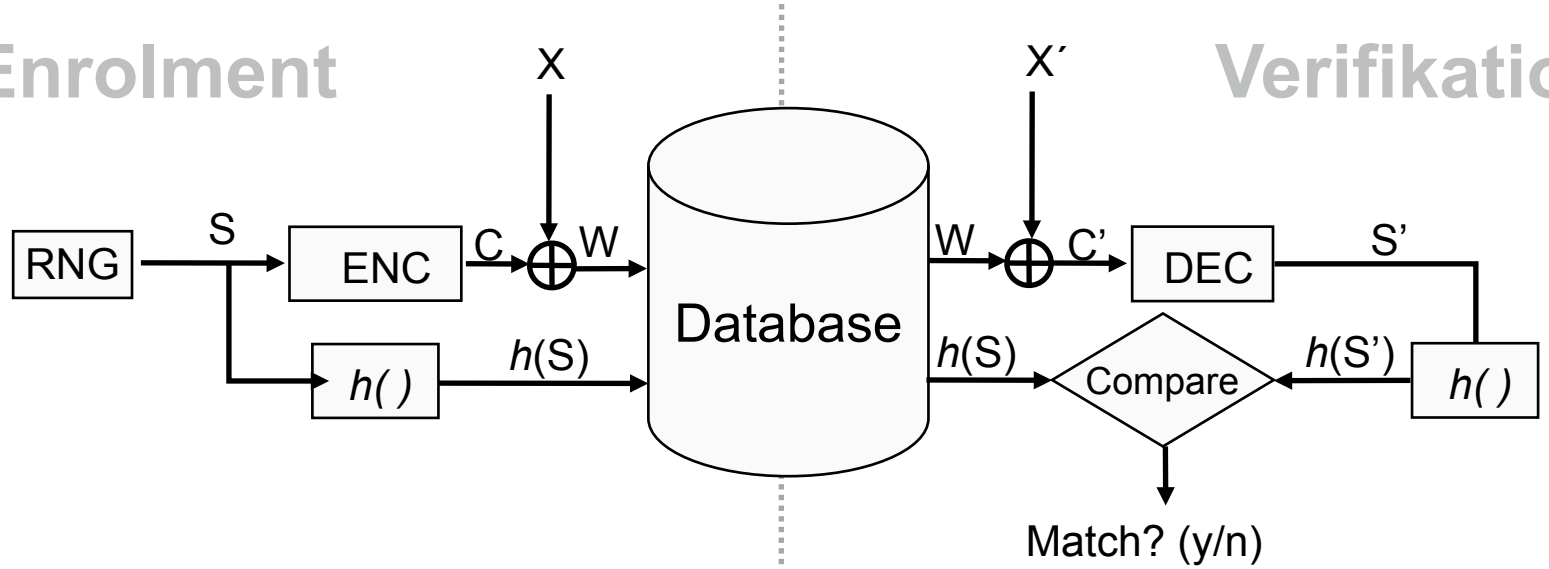
Herausforderung: Unterschied zwischen Passworten und biometrischen Samples

- Biometrische Messungen sind von Rauschen beeinflusst
- Kryptographische Einwegfunktionen sind extrem sensitiv gegenüber kleinsten Änderungen in den Eingabedaten

`h(01000101)` ist ungleich `h(01010101)`

Template Protection

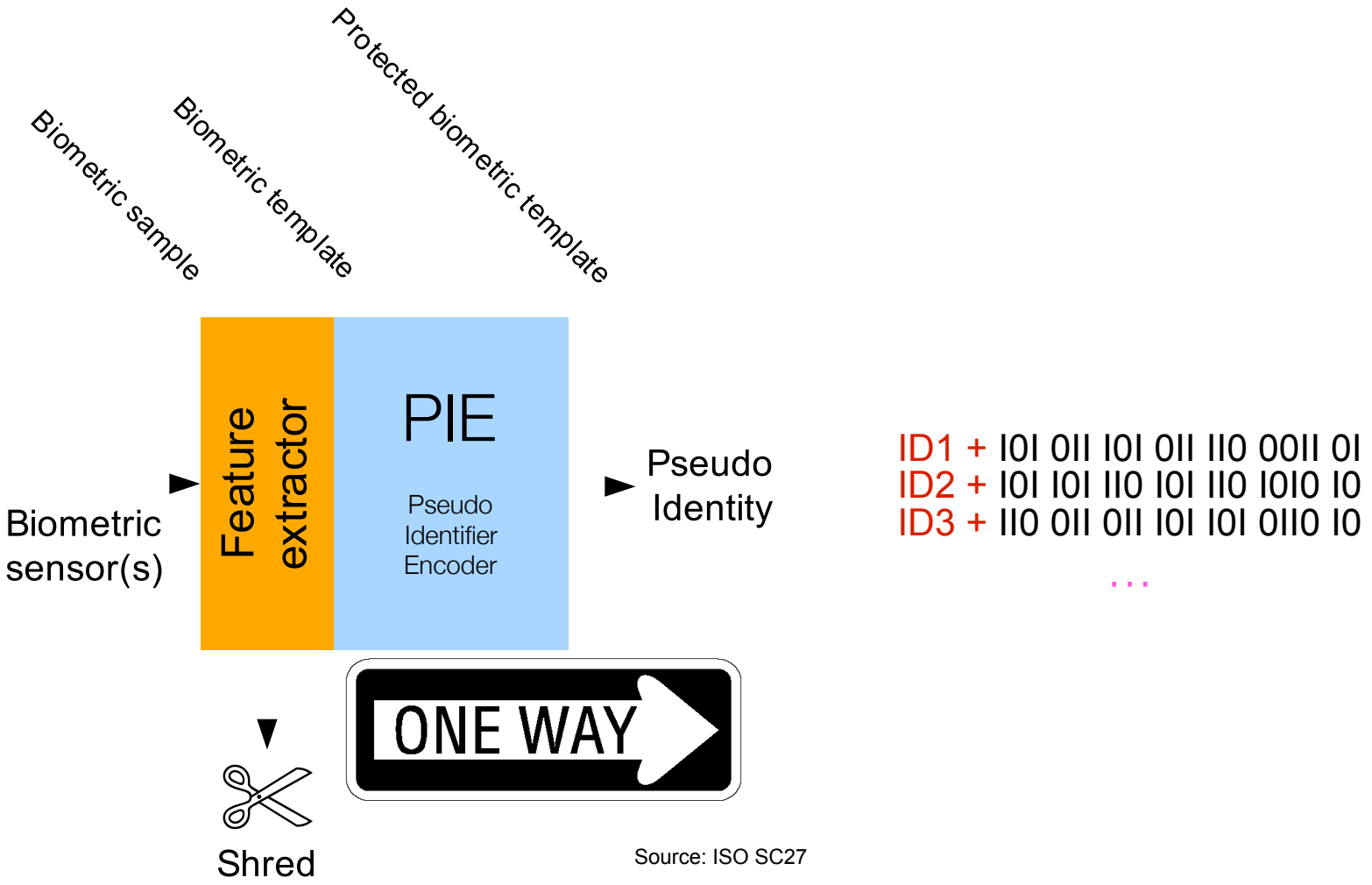
Schutz biometrischer Referenzdaten



- X ist ein binärer Feature Vektor der biometrischen Charakteristik
- C ist ein Codewort, das aus einem Geheimnis S erzeugt wird
- W = C⊕X ist öffenlich und { h(S), W} werden (verteilt) gespeichert
- C'=W⊕X´ wird bei der Verifikation rekonstruiert
  - Hamming Distance zwischen C und C´ innerhalb der Leistungsgrenzen des Fehlerkorrekturverfahrens

Template Protection

Biometrische Pseudonyme Identifikatoren



Sicherheit bedingt Vertrauen
der betroffenen Personen in das biometrische System

Forschungsziel:

Sicherheit und Leistungsfähigkeit von Template Protection

Biometrie für Sicherheit

BIG meeting member:

*„As Germany does **not** have a central database for passport applicants - they offer best conditions for duplicate enrolments“*

Forschungsziel:

Verfahren zum Schutz Biometrischer Referenzdaten und Machbarkeit in großen Identifikationsanwendungen

Mobile Authentisierung

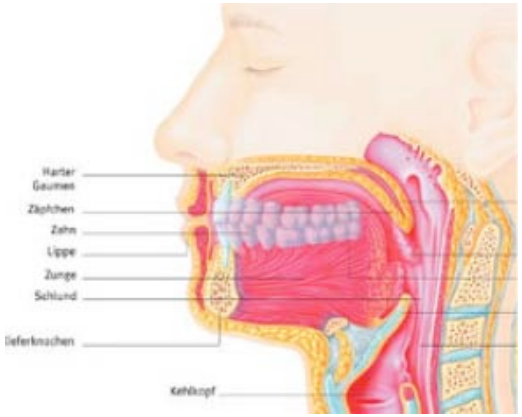
Mobiles Internet bedingt
Verlagerung aller Dienste auf mobile Geräte

- London: 1000 Mobil-Telefone pro Monat in Taxis verloren
- Bei 75% der Mobil-Telefone ist die PIN deaktiviert ...
  .. aus Komfortgründen

Forschungstehmen

- Das Mobil-Gerät „kennt“ seinen Besitzer





Zugangskontrolle zu Mobilen Endgeräten

Forschungsziel:
Biometrische Authentisierung
an persönlichen mobilen Endgeräten

Sonstige Themen

Nutzerakzeptanz und Usability

Verbesserung der Nutzbarkeit biometrischer Geräte

- Ergonomie und Benutzerfreundlichkeit
- Leichte Bedienung, behindertengerechte Systeme (Rollstuhlfahrer, eingeschränkte Sehfähigkeit, …)
- Unabhängigkeit von Umgebungsbedingungen.

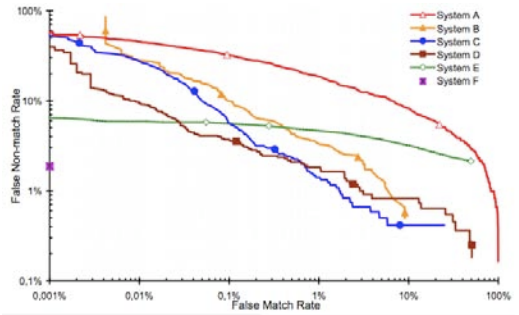
Anpassung auf ethnische Gruppen und Behinderte

- Vermeiden von Failure-to-Enrol oder Performanceverlusten, keine Diskriminierung

Testverfahren

Integrierte Bewertungskriterien eines biometrischen System

- Erkennungsleistung
- Überwindungssicherheit
- Ergonomie
- Umwelteinflüsse
- Konformität zu Standards / Interoperabilität



Themen

- Einheitliche und vergleichbare Methodiken und Kriterien für die strukturierte und methodische Prüfung
- Entwicklung von Teststrategien und Testwerkzeugen

Weitere Informationen

Fachgremien

CAST-Forum
http://www.cast-forum.de

Gesellschaft für Informatik - BIOSIG
Fachgruppe Biometrie und Elektronische Signaturen
http://www.biosig.org

TeleTrust
Arbeitsgruppe Biometrie
http://www.teletrust.de

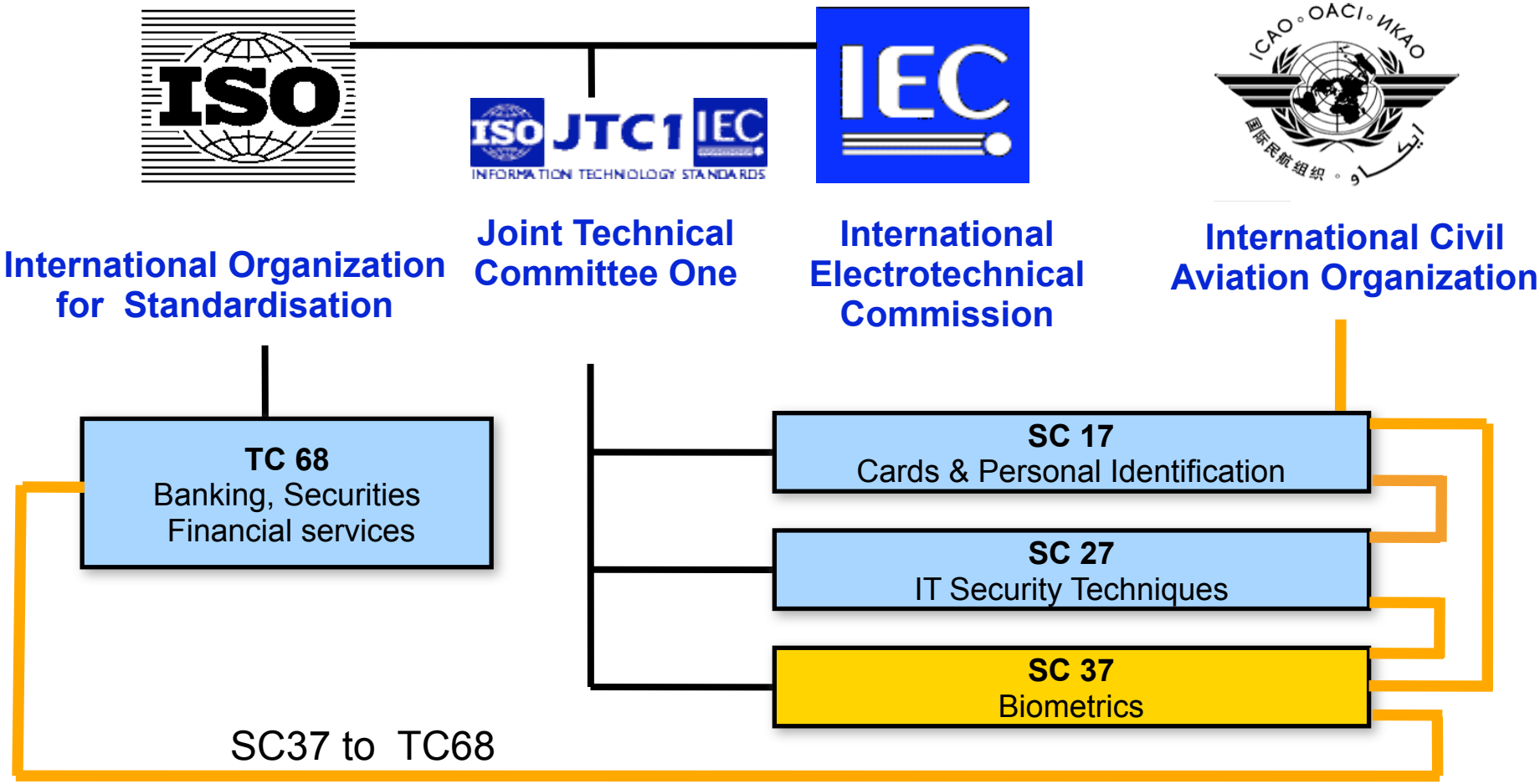
European Biometrics Forum
http://www.eubiometricsforum.com

White Paper Datenschutz in der Biometrie

TeleTrust
publiziert White Paper im Mai 2008:

- „Datenschutz in der Biometrie“
- http://www.teletrust.org/uploads/media/Datenschutz-in-der-Biometrie-080521.pdf
- Ziele der TeleTrust Arbeitsgruppe mit diesem Papier:
  - Information für Betreiber von Biometrischen Systemen,
    - um datenschutzgerechte Lösungen zu installieren
    - Akzeptanz der Systeme durch die Betroffenen herbeizuführen
- Nächste Sitzung der Teletrust - AG Biometrie
  - 08. September 2010
  - Fraunhofer IGD Darmstadt

Biometric Standardisation



- Publizierte Standards
  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on
- Harmonized Biometric Vocabulary verwenden:
  http://www.3dface.org/media/vocabulary.html

Zusammenfassung

- Datenschutz und Biometrie wiedersprechen einander nicht
  - Datenschutzfreundliche Gestaltung von Biometrischen Systemen ist möglich
- Biometrie muss auch in nicht-überwachten Szenarien einsetzbar werden
- Biometrie muss bequem zu nutzen sein
- Identitätsmissbrauch führt zu dramatischen Schäden
  - Return-of-Research-Investment

Kontakt

Prof. Dr. Christoph Busch

Department
Security Technology

Fraunhoferstrasse 5
64283 Darmstadt, Germany
Phone: +49-6151-155-536
christoph.busch@igd.fraunhofer.de
www.igd.fraunhofer.de/~busch