



# 7. Berner Tagung für Informationssicherheit 2004

## Identity Management: Chancen und Risiken für Bürger, Wirtschaft und Staat



# Verbessertes Identity Management mit Biometrie

-

## ein Feldtest


**Klaus J. Keus, Dipl. Mathematiker**  
**Referatsleiter „Schlüsseltechnologien“**

**Dr. Astrid Albrecht**

**Referat II 2.1 – Schlüsseltechnologien**  
**Bundesamt für Sicherheit in der Informationstechnik**

- **BSI in Kürze**
- **Elektronisches Identitätsmanagement - einige Anmerkungen**
- **Einführung in die Biometrie einschl. Definitionen**
- **Funktionsprinzip der Biometrie**
- **BSI Aktivitäten zum Thema Biometrie**
- **Biometrie im Feldtest BioP II**
- **Kontakt**

# BSI - Zahlen und Hintergründe

- 
- ❏ Unabhängige und neutrale Behörde für IT-Sicherheit
  - ❏ Oberste Bundesbehörde, unterstellt dem Bundesministerium des Inneren
  - ❏ gegründet 01. Januar 1991
  - ❏ ca. 400 Mitarbeiter
  - ❏ Budget: ca. 51 Million €

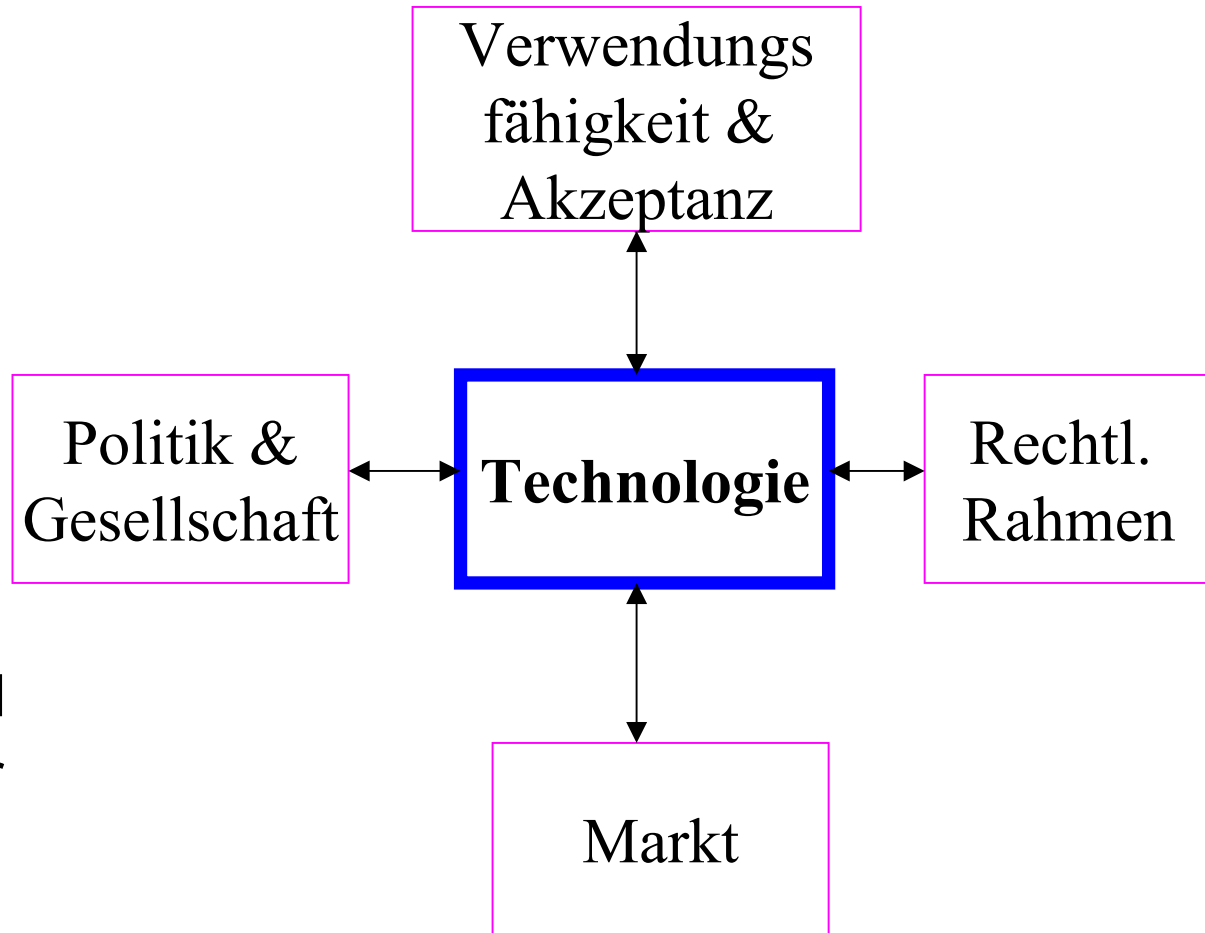
# Aktuelle Hauptschwerpunkte des BSI

- ✎ Internet Sicherheit
- ✎ sicheres E-Government
- ✎ Grundschutz
- ✎ Nationale / internationale Sicherheits-Kooperationen
- ✎ Krypto-Innovationsprogramm
- ✎ Biometrie
- ✎ Abstrahlsicherheit
- ✎ Awareness Kampagnen zu IT-Sicherheit
- ✎ Zertifizierung und Zulassung
- ✎ Schutz kritischer Infrastrukturen

- ✎ **Grundlagenarbeit** im Bereich der Biometrie als eine Schlüsseltechnologie
  - Standardisierung
  - Labor: Evaluierung bzgl. Performance, Funktionalität, Sicherheit (Penetrationstests)
- ✎ **wissenschaftl. Projekte** (Theorie und Praxis) für verschiedene Biometrieverfahren
- ✎ **Feldversuche / Pilotierungen** mit unterschiedlichem Fokus und Anwendungsfeldern
- ✎ **grundlegende juristische Arbeiten** z.B. Datenschutz
- ✎ **Kooperationen mit Wissenschaft und Industrie** auf nationaler, europäischer und internationaler Ebene

## **bedeutsame Einflußfaktoren:**

- Hochsicherheit
- nachgewiesener  
Level von  
Vertrauen
- anwendbar
- akzeptabel
- rechtl. bindend
- politisch vertretbar





# Elektronisches Identity Management – was ist das?



## Generelles, allgemeines Ziel von Elektronischem Identity Management (eIDM):

*Wer* darf *was* in *welchen* definierten / implementierten  
elektronischen Prozessen und Geschäftsmodellen im  
E-Government?

# eIDM – Definitionen I

eIDM :

- ein **Schlüsselbeitrag** zur Errichtung und zum Betrieb eines benutzerfreundlichen und administrablen globalen E-Government
- **mehr als** eine Form eines im Kontext von Applikationen eindeutigen und verifizierbaren **Informationswertes**
- und somit mehr als eine Technologie

eIDM:

**mehr als die digitale Identität** einer Person, sondern:  
digitale Identität einer Person  
+ Zugangs-Management  
+ Administrations-Management von Bürgern

eIDM ist unterteilt in **3 Hauptphasen**:

- Directory Dienste (für Identifikation, Registrierung, Enrolment und Revokation, Modifizierung und Benutzerverwaltung)
- Authentication Management
- Zugriffs-Management

eIDM bietet eine **Infrastruktur** für:

- die Erstellung
- den Betrieb
- die Benutzung von digitalen Identitäten

eIDM öffnet Möglichkeiten für eine **starke und klare Relation** zwischen Identitäts-Management und E-Government Zielen

⇒ eIDM ist eher gedacht für **prozessorientierte** Ansätze

⇒ eIDM hat **direkte Beziehung** zum Strategie- /  
Geschäftsmodell E-Government

## Rollen von Benutzern von Identitäten:

- Bürger
- Mitarbeiter einer Behörde
- Mitarbeiter ausserhalb einer Behörde : A2A (Behörde-zu-Behörde, national / cross border)
- Kunde / Kontraktor
- etc.

⇒ eIDM hat ***natürliche und legale Identitäten*** für unterschiedl. Zwecke, Anwendungen und Bereiche zu berücksichtigen

## eIDM und Biometrie:

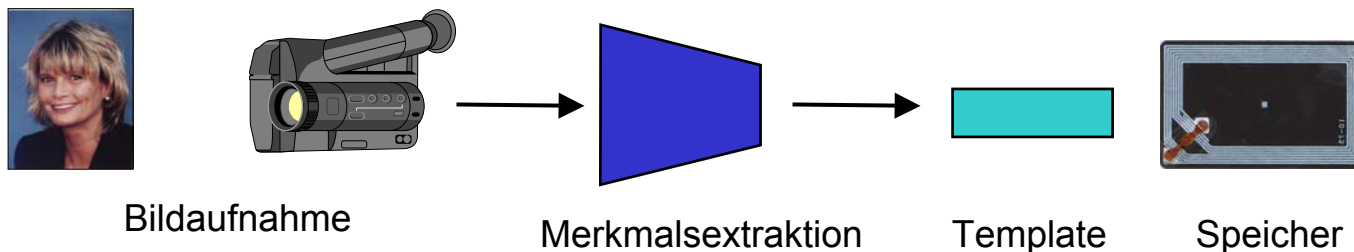
Biometrie leistet eine ***zusätzliche eindeutige***  
***Beziehung*** (Identifikation / Verifizierung) zu ***einer***  
***natürlichen Person*** (Individuum) und seiner Daten

# Einführung: Biometrie – was ist das?

- ↯ Automatisierte Methoden, eine Person basierend auf physischen oder Verhaltens-Merkmalen zu messen
  
- ↯ Merkmale sind z.B.
  - ✓ Gesicht, Fingerabdruck, Handgeometrie, Iris, Retina
  - ✓ Handschrift, Stimme, Gang,
  - ✓ Venenmuster, Körpersalze, Geruch ...
  
- ↯ Merkmale können sein
  - ✓ Konditioniert - Schriftzug, Sprache, ....
  - ✓ Zufällig - Fingerabdruck, Iris, ...
  - ✓ Genetisch bedingt - Gesicht, DNA, ...

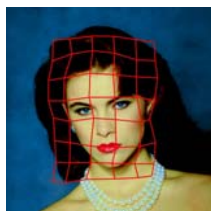
- **Technische Biometrie, was kann sie leisten?**
  - **Identifikation (1:n Vergleich):** Die individuellen Merkmale einer Person können gegen die bekannten Merkmale einer Referenzmenge abgeglichen werden. (Frage: Wer bist du?)
  - **Verifikation (1:1 Vergleich):** Die individuellen, frisch aufgezeichneten Merkmale einer Person werden gegen ein vorab bereitgestelltes Referenzmuster verglichen. (Frage: Bist du der, für den du dich ausgibst?)

# Funktionsprinzip



## Enrolment

### Verifikation

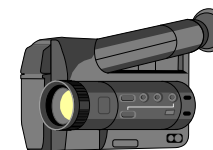


**Input:** Name, Live Merkmal und Template

- Merkmalsextraktion
- Vergleich mit Template

**Output:** Bei hinreichender  
Übereinstimmung: **OK**  
sonst: **NOK**

### Identifikation



**Input:** Live Merkmal

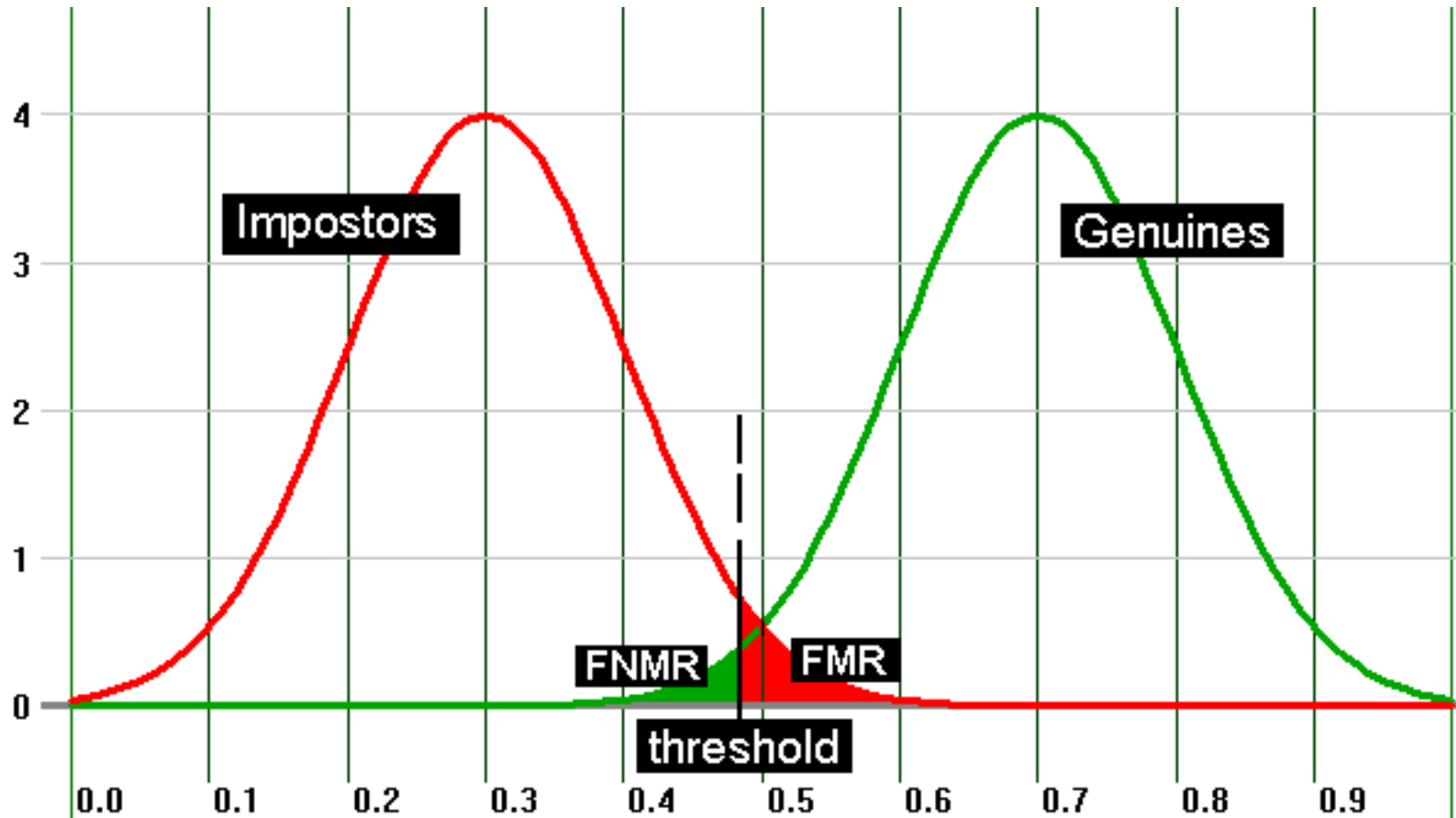
- Merkmalsextraktion
- Vergleich mit allen Templates einer DB

**Output:** Bei hinreichender  
Übereinstimmung mit einem Template:  
**Ausgabe des Namens**  
**(oder Hitliste von Namen)**

# Funktionsprinzip / Fehlerraten

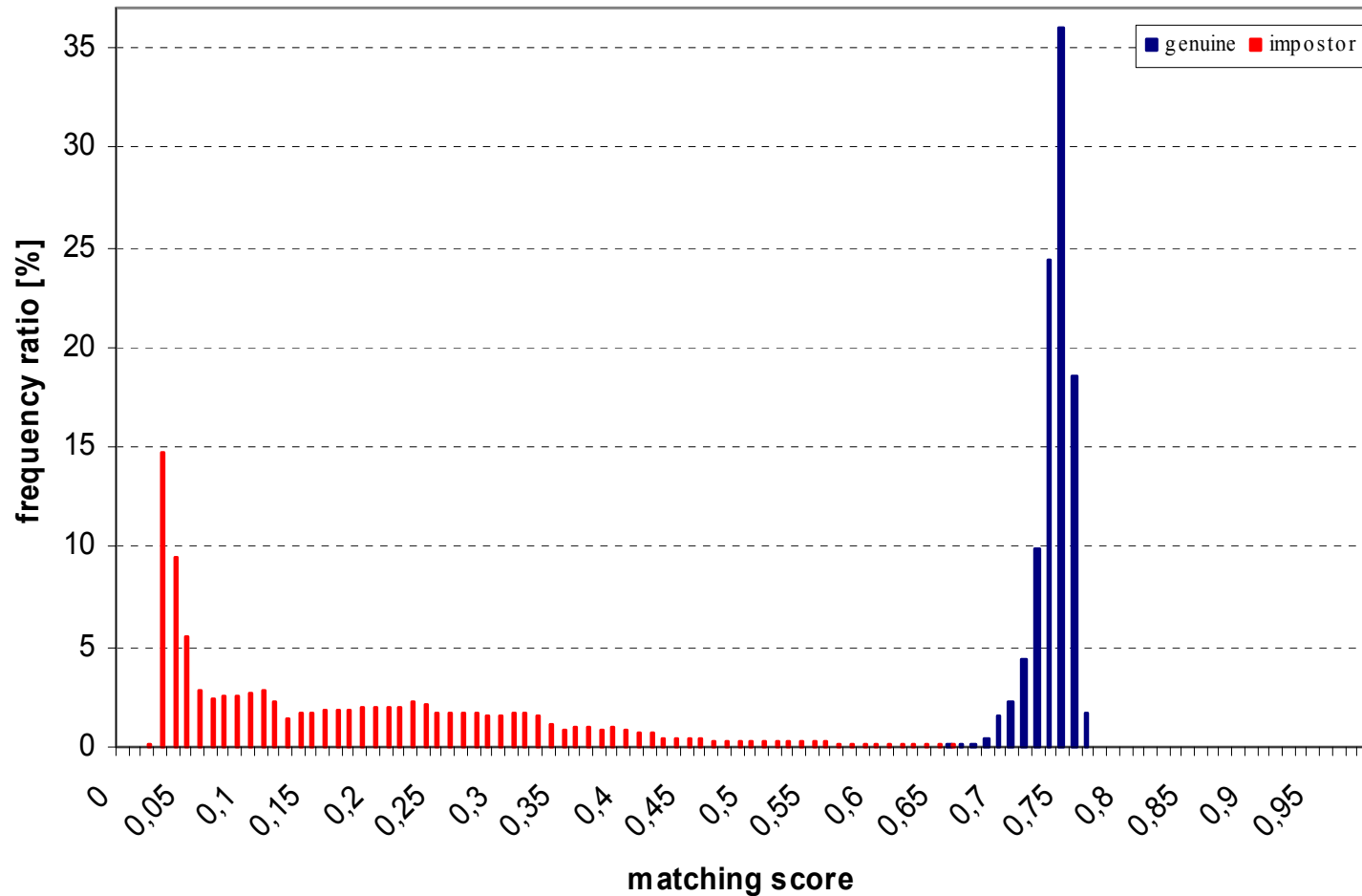
- Verschiedene Aufnahmen des gleichen Merkmals liefern immer unterschiedliche Rohdaten.
- Also: statistischer Vergleich
- Konsequenz: Mögliche Fehlentscheidungen!
  - **False Match**: Ein Life Merkmal eines anderen (Imposter) wird fälschlich als passend zur Referenz bewertet, also sicherheitsrelevant (Bezeichnungen: FMR, FAR)
  - **False Non Match**: Ein Life Merkmal der korrekten Person (Genuine) wird fälschlich als nicht zur Referenz passend bewertet, also akzeptanzrelevant. (Bezeichnungen: FNMR oder FRR)
- Die zugehörigen Fehlerraten sind nicht unabhängig

# Funktionsprinzip



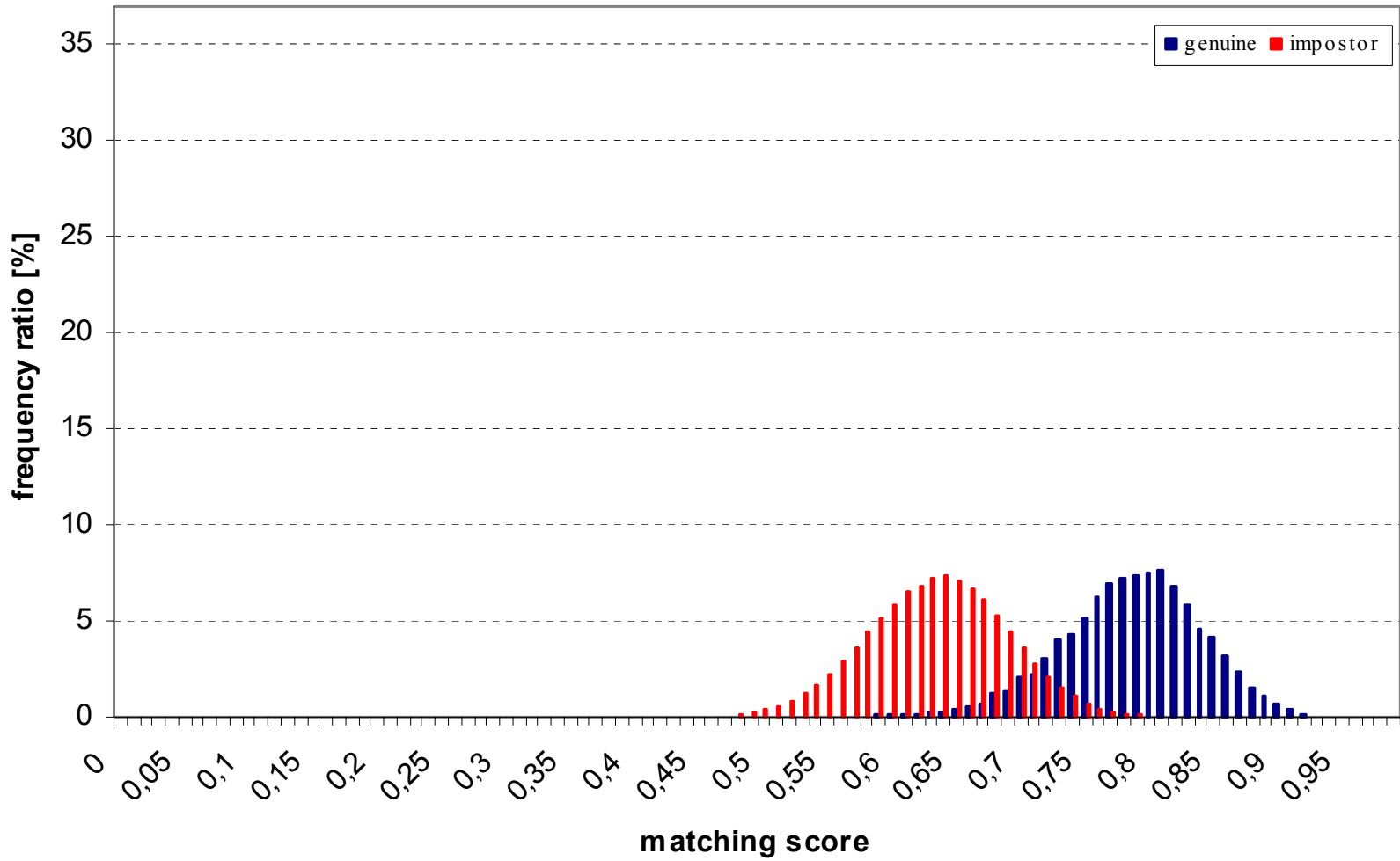
Typische Verteilungsfunktion für Genuines + Imposters

# Funktionsprinzip



Beispiel aus dem echten Leben 1: gute Trennung

# Funktionsprinzip



Beispiel aus dem echten Leben 2: schlechte Trennung

# Strategie des BSI zum Thema „Biometrie“

## Grundlagenprojekte

- Projektreihe **BioFace** - Vergleichende Untersuchung von Gesichtserkennungssystemen
- Projektreihe **BioFinger** - Vergleichende Untersuchung von Verfahren zur Fingererkennung

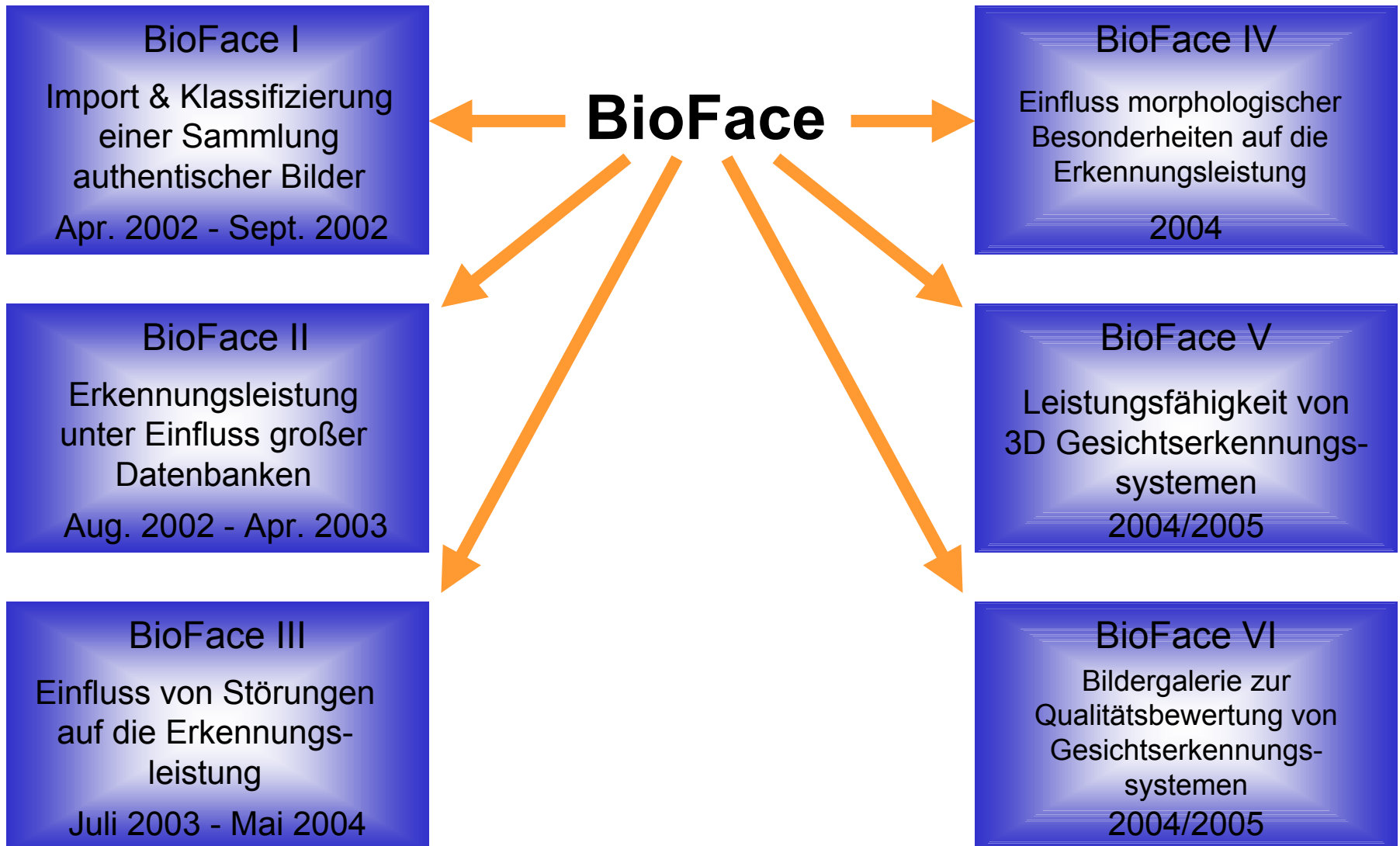
## Anwendungsprojekte

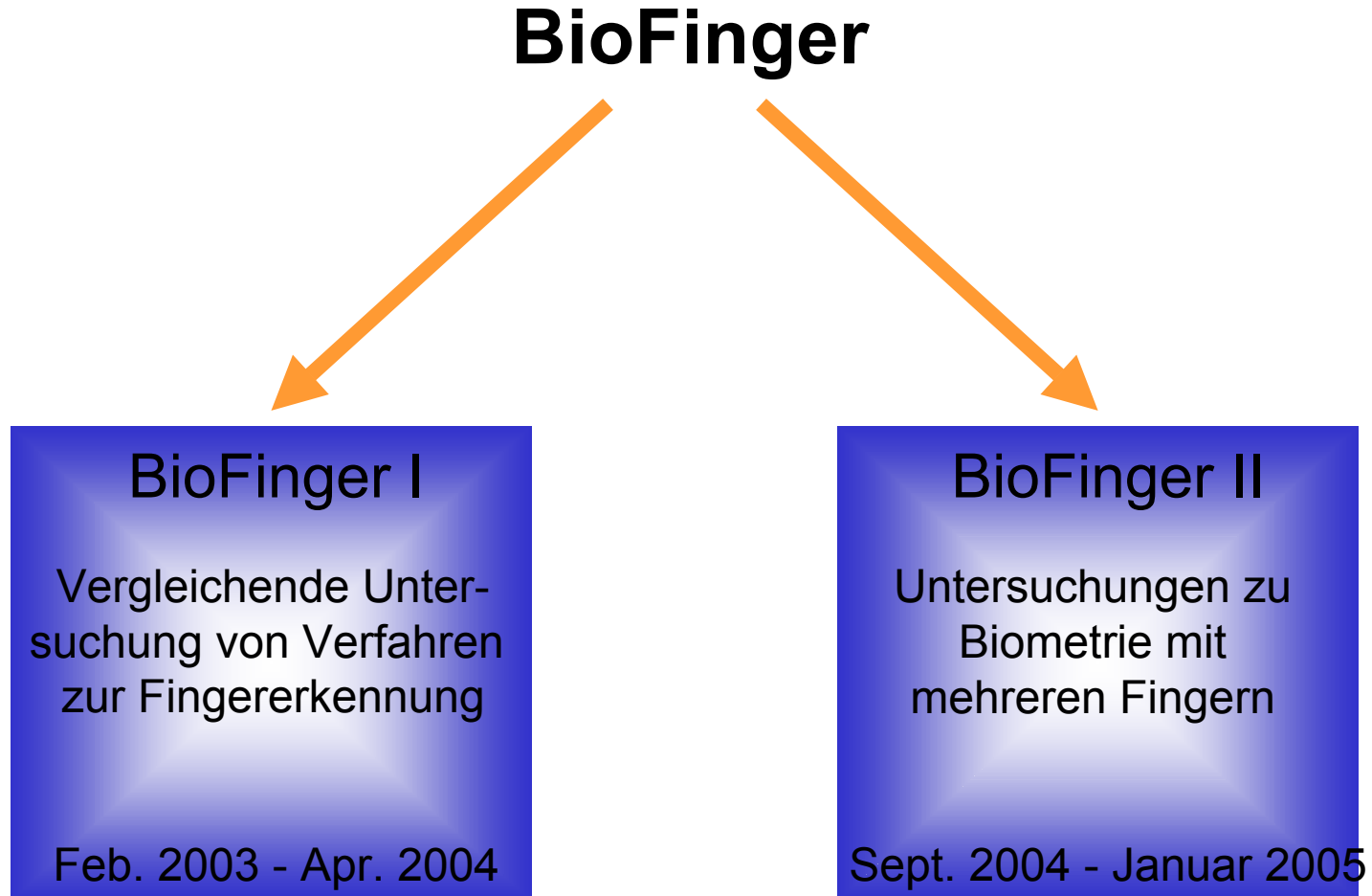
- Projektreihe **BioP** ( Biometrie in Personaldokumenten )

## Standardisierung

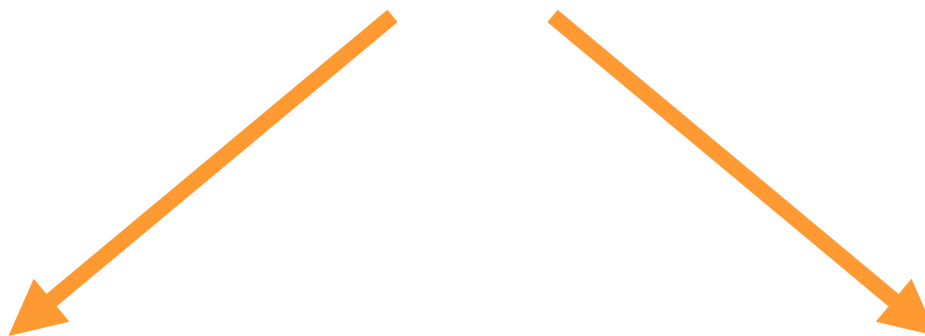
- Projekt **ILSE** ( ICAO LDS and Security Evaluation )
- ICAO
- ISO

## BSI Biometrie Labor





## Bimetrie in Personaldokumenten **BioP**



### BioP I

Untersuchung der Leistungsfähigkeit  
von Gesichtserkennungssystemen  
zum geplanten Einsatz in  
Personaldokumenten

Nov. 2002 - Dez. 2003

### BioP II

Untersuchung der Leistungs-  
fähigkeit von biometrischen  
Verifikationssystemen

Okt. 2003 - Dez. 2004

# Hintergrund für BioP - Studie (1)

- ❏ Zunehmende Aktivitäten im internationalen Terrorismumumfeld erfordern *neue Mechanismen* um die Sicherheit der Bürger zu gewährleisten bzw. zu verbessern
- ❏ Beitrag der Biometrie für die *internationale Sicherheit*:
  - ☑ Prüfung vorgelegter Identitäten,
  - ☑ Vermeidung geheimgehaltener Identitäten,
  - ☑ Beispiele: gefälschte Personaldokumente, gefälschte VISA, Kreditkartenmissbrauch.
- ❏ *Strategie*:
  - ☑ Dialog mit Sicherheitsbehörden wie BSI und BKA zur Ausschöpfung von Möglichkeiten zur Verbesserung der Sicherheit mit Hilfe der Biometrie
  - ☑ gezielte und sensible Implementierung von Biometrie um den Sicherheitsstand in Deutschland zu verbessern

## 🕒 Anti-Terrorismusgesetz von Januar 2002

### ☑ Änderungen von Gesetzen

- Bzgl. Personalausweise und Passports mit dem Ziel, Biometrieinsatz rechtlich zu ermöglichen
- Bzgl. der Erfassung von Ausländerdaten, insbes. für „kritische Staaten“
- Bzgl. Asylantragsteller für Möglichkeiten des automatischen Fingerabgleichs durch Strafverfolgungsbehörden

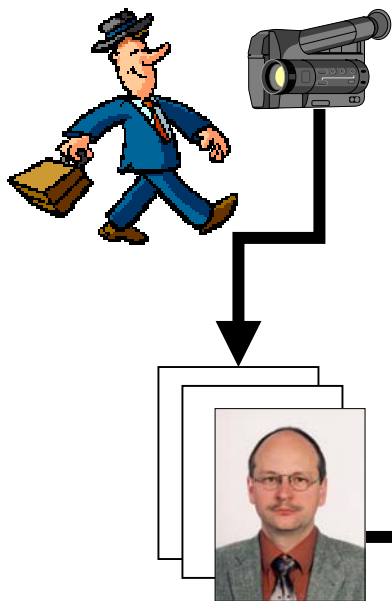
## 🕒 Praktische Implementierungen

- ☑ Neue VISA ab Jjanuar 2003 (Photo eingebunden)
- ☑ verschiedene große Pilotierungen und Projekte durch BSI & BKA
- ☑ Nationale Standardisierungsanstrengungen durch das BMI in enger Abstimmung mit BMWA, BSI, TeleTrust, BITKOM und DIN
- ☑ Machbarkeitsstudien bzgl. elektronischer ID-Karten einschl. elektronischer Signatur und Biometrie

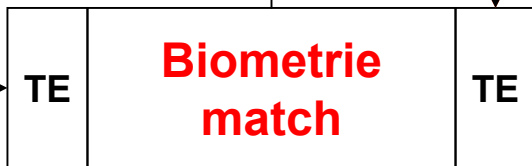
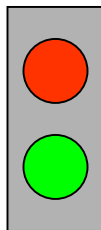
## Vergleichende Untersuchung von Gesichtserkennungssystemen

- Verifikations- bzw. Reisedokumentszenario
- 2 Systeme
- 3 Algorithmen
  - ohne Eye-Finder-Extension
  - mit Eye-Finder-Extension
- Feldtest mit 241 Teilnehmern
  - Teststandort BKA in Wiesbaden

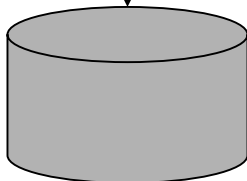
# BioP I - Setup



Anzeige



ok/nok, Matchscore  
und andere Daten



Ergebnis DB  
nur **User-ID**

Schnittstelle

Scanner  
(File)

Scanner  
(direkt)

Scanner  
(File)

File

File

File

File

## Referenz-DB



(1)  
portrait photo  
(image file,  
front)



(2)  
displayed  
portrait from  
ID-card



(3)  
displayed  
portrait from  
new visa  
(image file)



(4)  
portrait photo,  
compressed  
(image file)



(5)  
portrait photo  
(image file, profile)



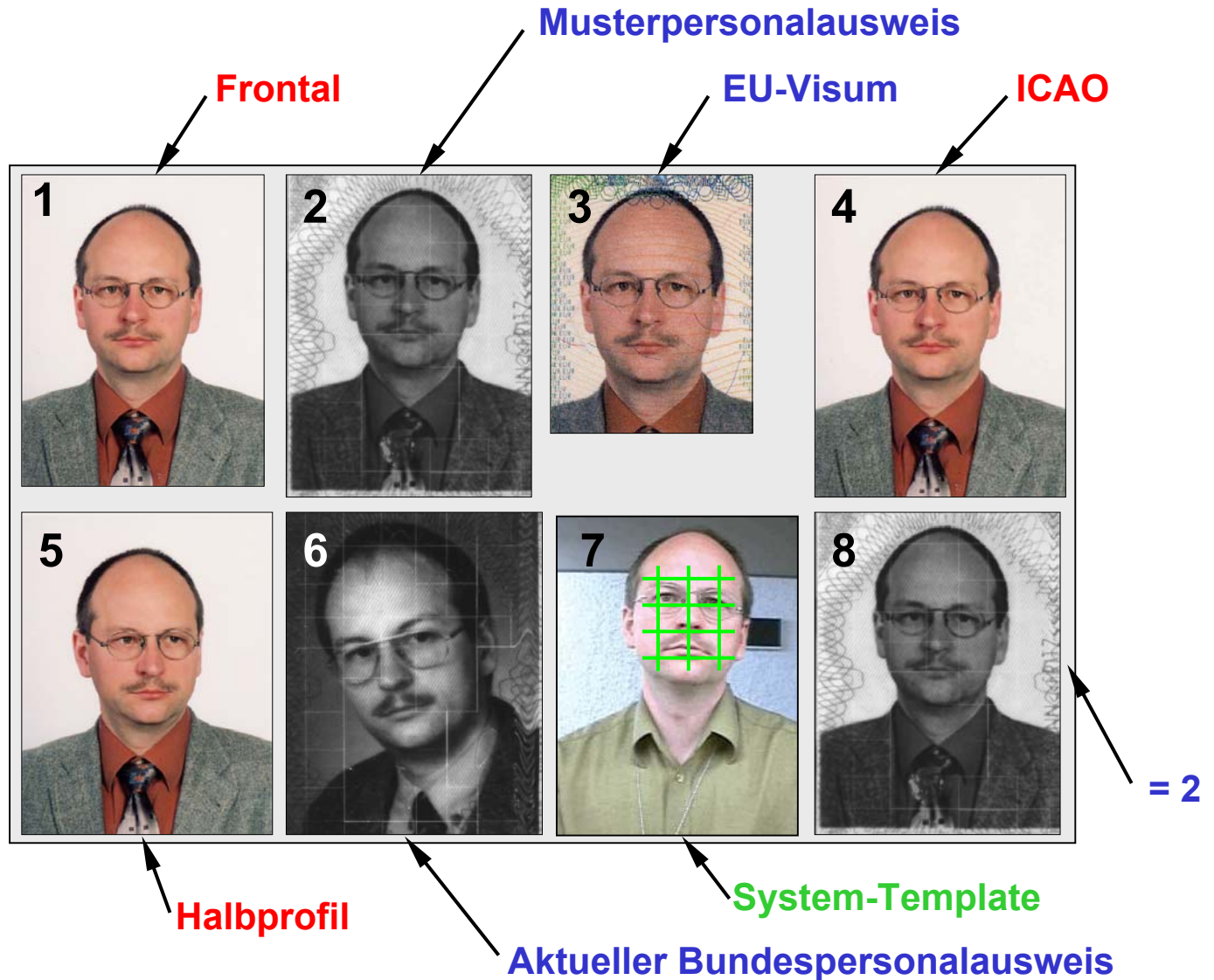
(6)  
portrait photo,  
old ID-card  
(image file)

00101010

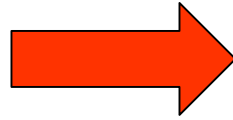
(7) proprietary template  
from enrolment

# BioP I

## Referenzbasen



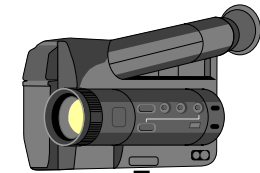
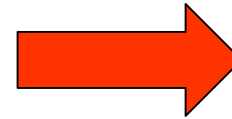
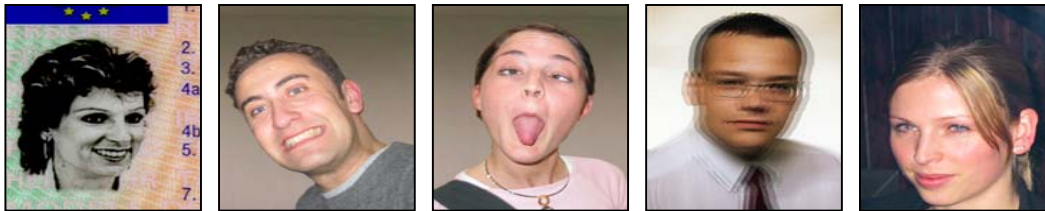
# 1. Presentation des Dokuments, lesen der ID-No. und Anzeige Portrait



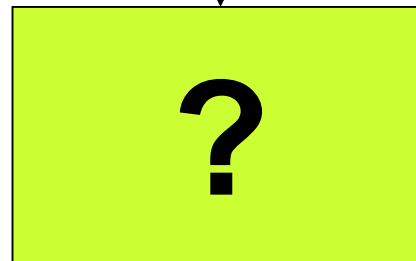
User-ID = 0001



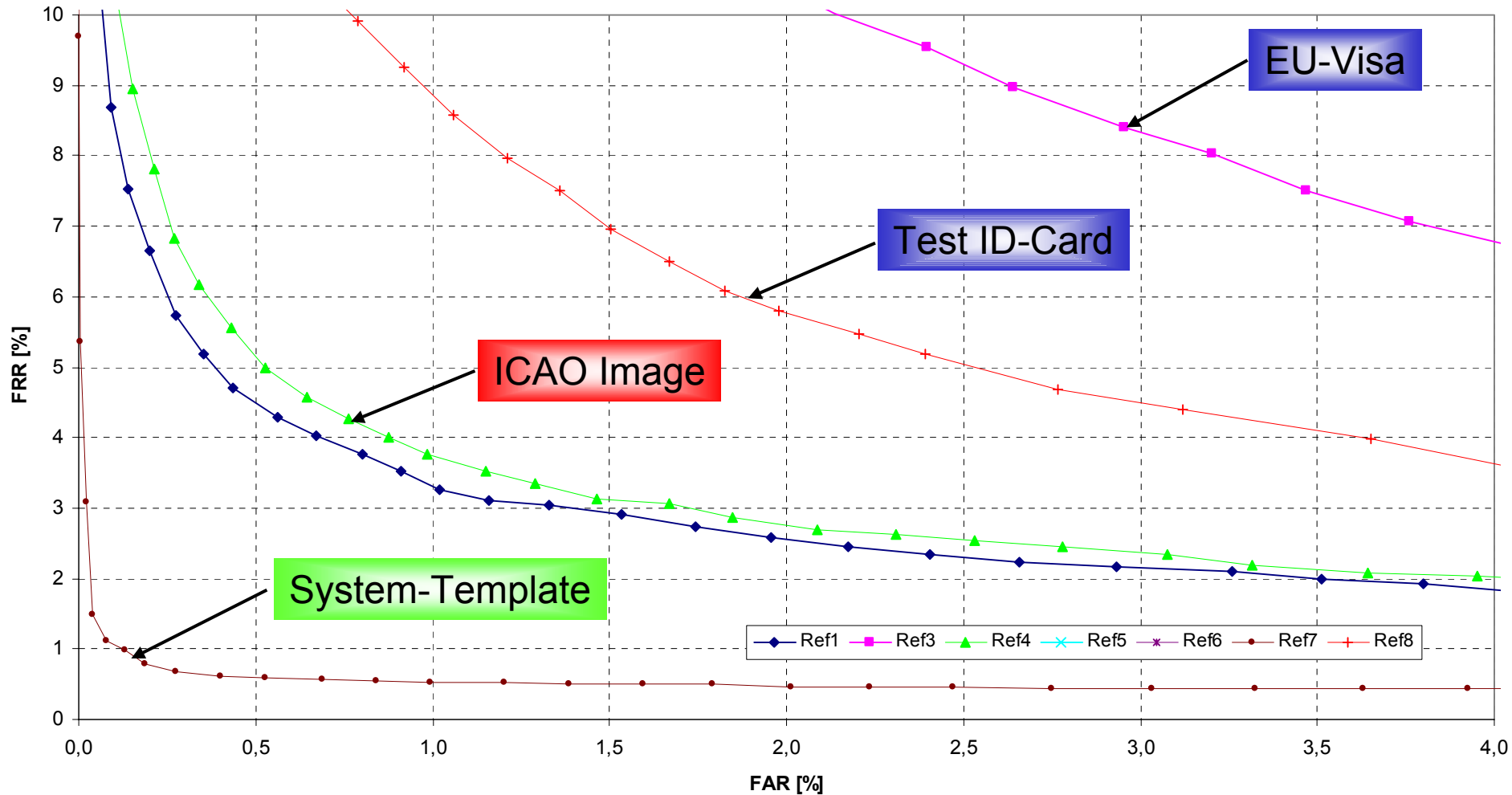
## 2. Erfassung Livebild



## 3. Biometrie Match / Imposter



## - ROC der unterschiedlichen Referenzen



# BioP I - Ergebnisse (1)

Scanning des Portraits aus dem MRTD



aktuelle ID Card

neue ID Card

EU Visa

Referenz Daten

Bild Datei

frontal

Profile

komprimiert  
Nicht  
komprimiert

Digitale Daten



System Template 

- verwendbar**
- eingeschränkt  
verwendbar**
- sehr eingeschränkt  
verwendbar**
- nicht verwendbar**



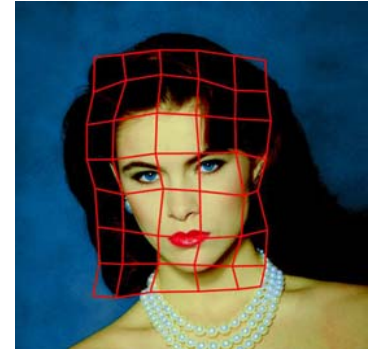


- ❏ Gesichtserkennung ist im Prinzip einsetzbar um die durch ICAO definierten Aufgaben zu erreichen.
- ❏ Anforderungen an deutsche Dokumente (und alle MRTD)
  - ✓ Einbindung eines digitalen Speichermediums
  - ✓ Neue Photovorgaben durch ICAO
- ❏ Anforderungen für Gesichtserkennungssysteme
  - ✓ Verbesserungen hinsichtlich möglicher Penetrationsangriffe
  - ✓ Optimierung der Algorithmen, tuning der Bilddaten vs. Templates
  - ✓ Alterungsrobustheit (weiterer Research notwendig)
- ❏ Anforderungen an das Umfeld
  - ✓ Benutzung von Gesichtserkennung nur in Verbindung mit manueller Begleitung (Grenzbeamter)
  - ✓ kontrollierte Beleuchtung



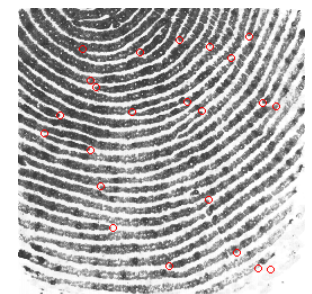
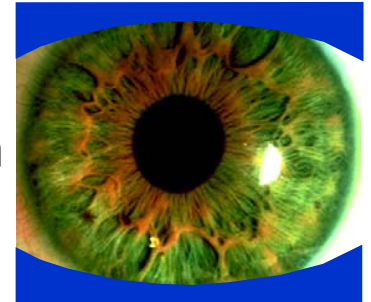
## BioP I

- ✓ Bester Performance des Algorithmus
- ✓ Bestes Performance des Systems
- ✓ Test-Methodologie



## BioP II

- ✓ Evaluierung von (mehr) „real life“ Performanz durch Vergrößerung der Anzahl und Hintergrundwechsel der Teilnehmer
- ✓ Vergleich mit anderen biometrischen verfahren (Iris und Finger)
- ✓ Evaluierung der RFID Technologie in MRTDs
- ✓ Studie zu Benutzbarkeit und Akzeptanz



# BioP II

## Fragestellung & Zielsetzung

*Welches der biometrischen Verfahren zur Gesichts-, Iris- und Fingerabdruckerkennung eignet sich am ehesten hinsichtlich der technischen Leistungsfähigkeit für einen Einsatz in Anwendungsszenarien wie Personal- oder Reisedokumente für eine große Benutzergruppe (>2000 Benutzer) unter Verwendung der ICAO-Empfehlungen (z.B. hinsichtl. Bilder, RFID-Chip / LDS)*

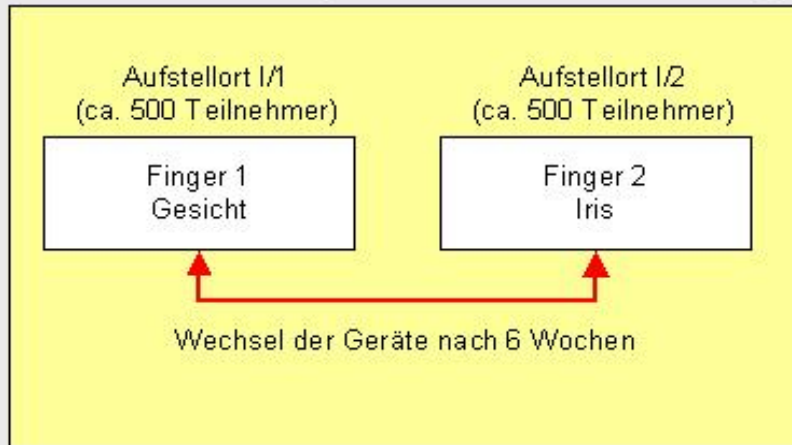
**➔ Vergleichende Untersuchung der Verfahren im Rahmen eines Feldtests\* bzgl.:**

- **Leistungsfähigkeit**
- **Sicherheit**
- **Nutzerakzeptanz**

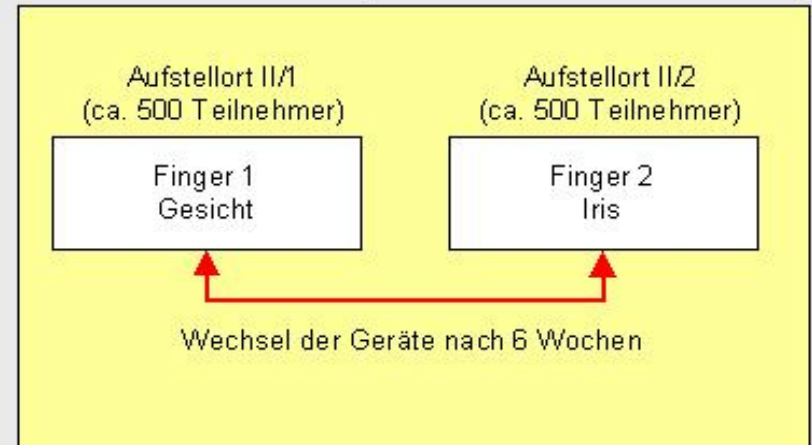
\*Feldtestklasse III gemäß den technischen Evaluierungskriterien des BSI (> 2000 Nutzer)

### Standort Flughafen Frankfurt

#### Lufthansa (mind. 1000 Teilnehmer)



#### Fraport (mind. 1000 Teilnehmer)



- insges. vier Aufstellorte (Container)
- zwei unterschiedliche Systeme pro Container
- geplant sind zwei Besuche pro Tag
  - ➡ vier Verifikationsversuche pro Tag und Teilnehmer
  - ➡ insges. ca. 500.000 Verifikationsdatensätze über den gesamten Feldtest

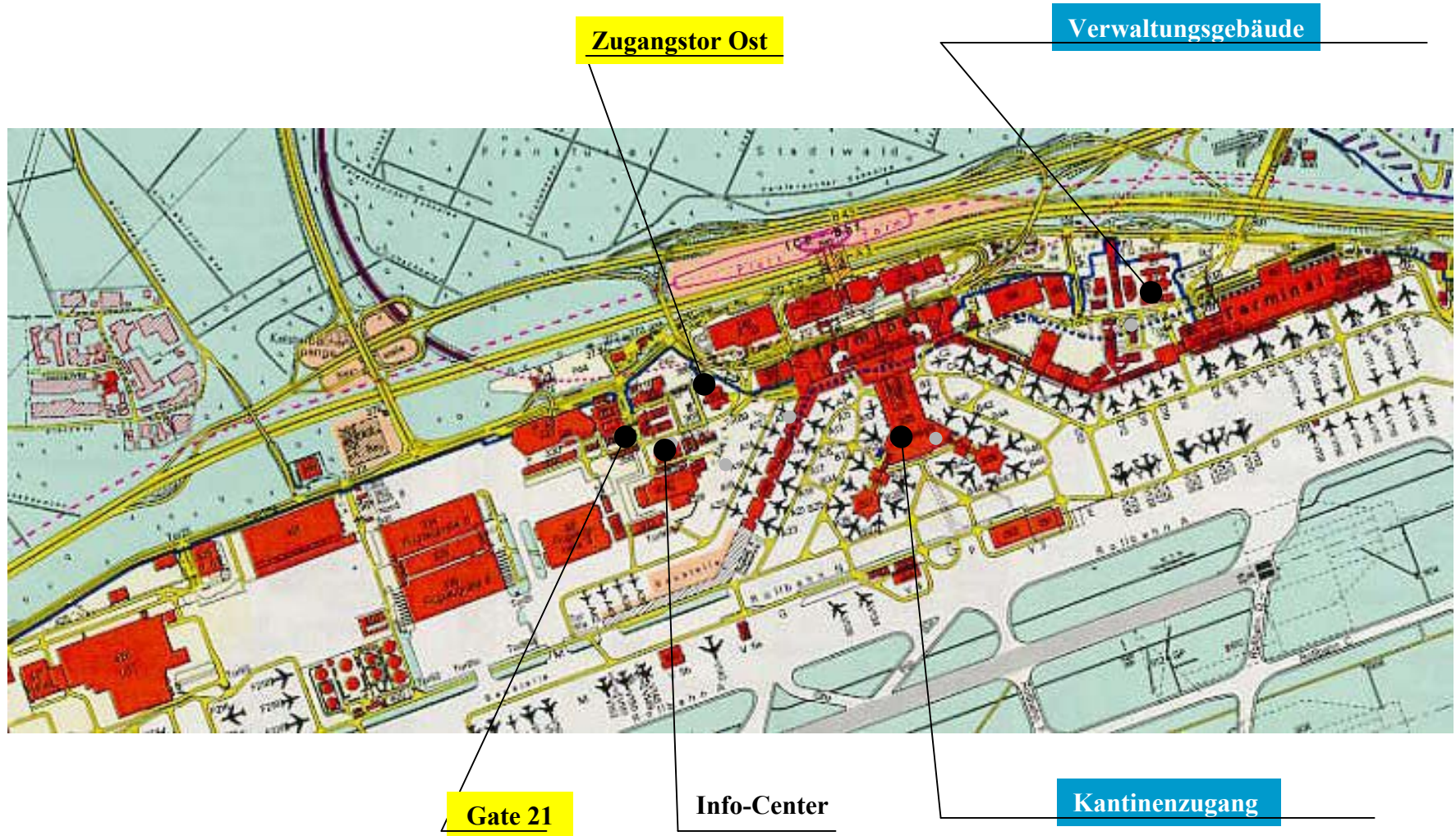
## Fakten

- 7. Größter Flughafen weltweit und größter Frachtflughafen in Kontinentaleuropa in 2003 mit:
  - 158 Airlines
  - 304 Zielen
  - 458.865 Bewegungen
  - 48.4 Mio. Passagiere
  - 1.65 Mio. Tonnen Fracht
- Heimatbasis von Lufthansa und somit wichtigster europäischer Drehpunkt der Star Alliance





# Frankfurt Airport - Systembereiche (Lokationen)

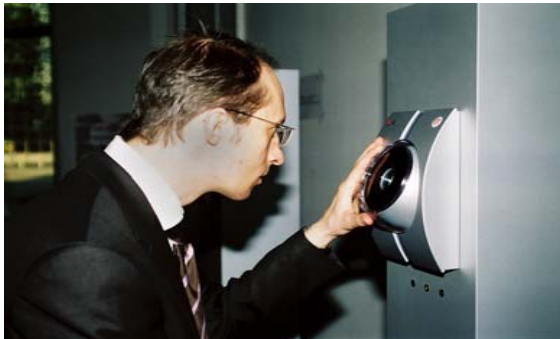




**Face** Cognitec Systems



**Fingerprint 1** Bundesdruckerei/NEC



**Iris** SD Industries



**Fingerprint 2** DERMALOG Identifikation System

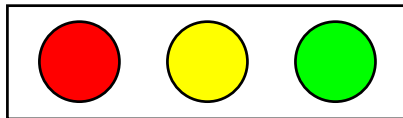
- gemeinsames Interface (ICAO LDS), kontaktlos Smart-Card-Leser, gemeinsames Benutzerfeedback

## Systeme im Test

- Gesicht: Cognitec
- Iris: SD Industries
- Finger1: Bundesdruckerei/NEC
- Finger2: Dermalog

## Ausstattung/Erweiterung der Systeme

- BioP II Datenbankschnittstelle (ICAO LDS)
- SmartCard-Leser (kontaktlos) zur Identifikation der Testpersonen
- Einheitliches Benutzer-Feedback



# BioP II

## Weiterführende Untersuchungen

- **FAR Bestimmung**
  - Verifikation / Identifikation
- **Überwindungssicherheit**
  - Zero-effort Attempt
  - Manipulation Gesamtsystem
- **Umweltbedingungen**
  - Temperatur
  - Luftfeuchtigkeit
  - Beleuchtung
- **Langzeitstabilität**
  - Systeme / Sensoren
  - Biometrische Merkmale
- **Nutzerakzeptanz**

## **Enrolment**

- Antragsformular (Papier oder Online)
- Produktion der UserID / Versand an Teilnehmer (Papier oder online)
- Enrolment Station: Übergabe des kontaktlosen Tokens (RFID-basiert)
- Enrolment:  
Erstellung der verschiedenen Templates / Bilder, Speicherung in DB
- Bildererfassung durch Spezialkameras (Gesicht) gem. ICAO-Anforderungen und Sensoren (Finger)
- Erfassung von 2 verschiedenen Aufnahmen für Iris und Finger (1:1, 1:2)

## **Kommunikations Konzept**

- E-basiert (Intranet, online) und offline: Transparenz und Datenschutz
- aktive Begleitung durch Datenschutzbeauftragte und Personalräte
- Leistungsprämien

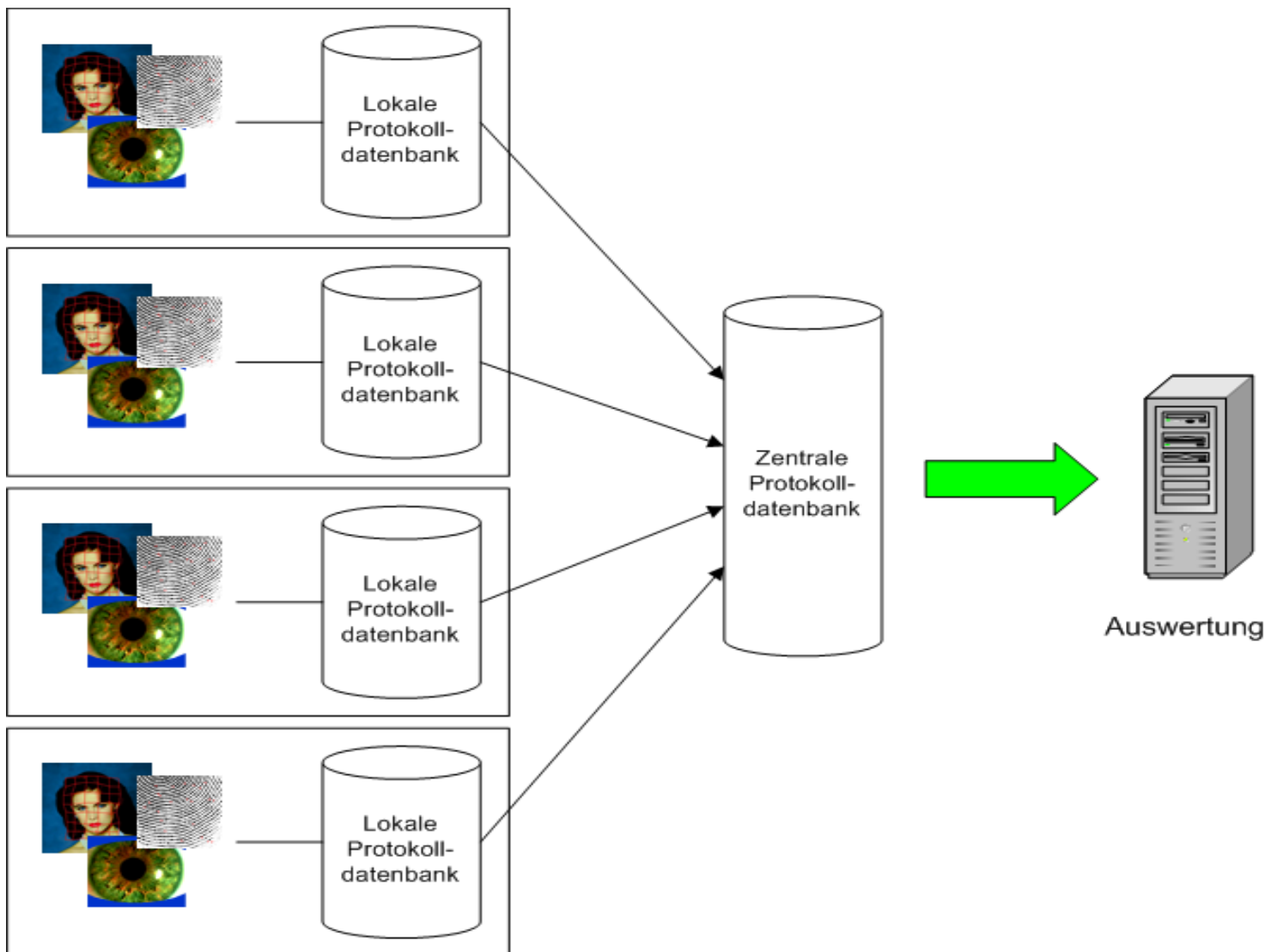
## **Benutzerverteilung**

- Lufthansa und Fraport separat
- Exclusive administriert und begleitet durch die beiden Firmen
- User-ID
- Personal-Informationen (Name, Tel.No., E-mail Adresse etc.)

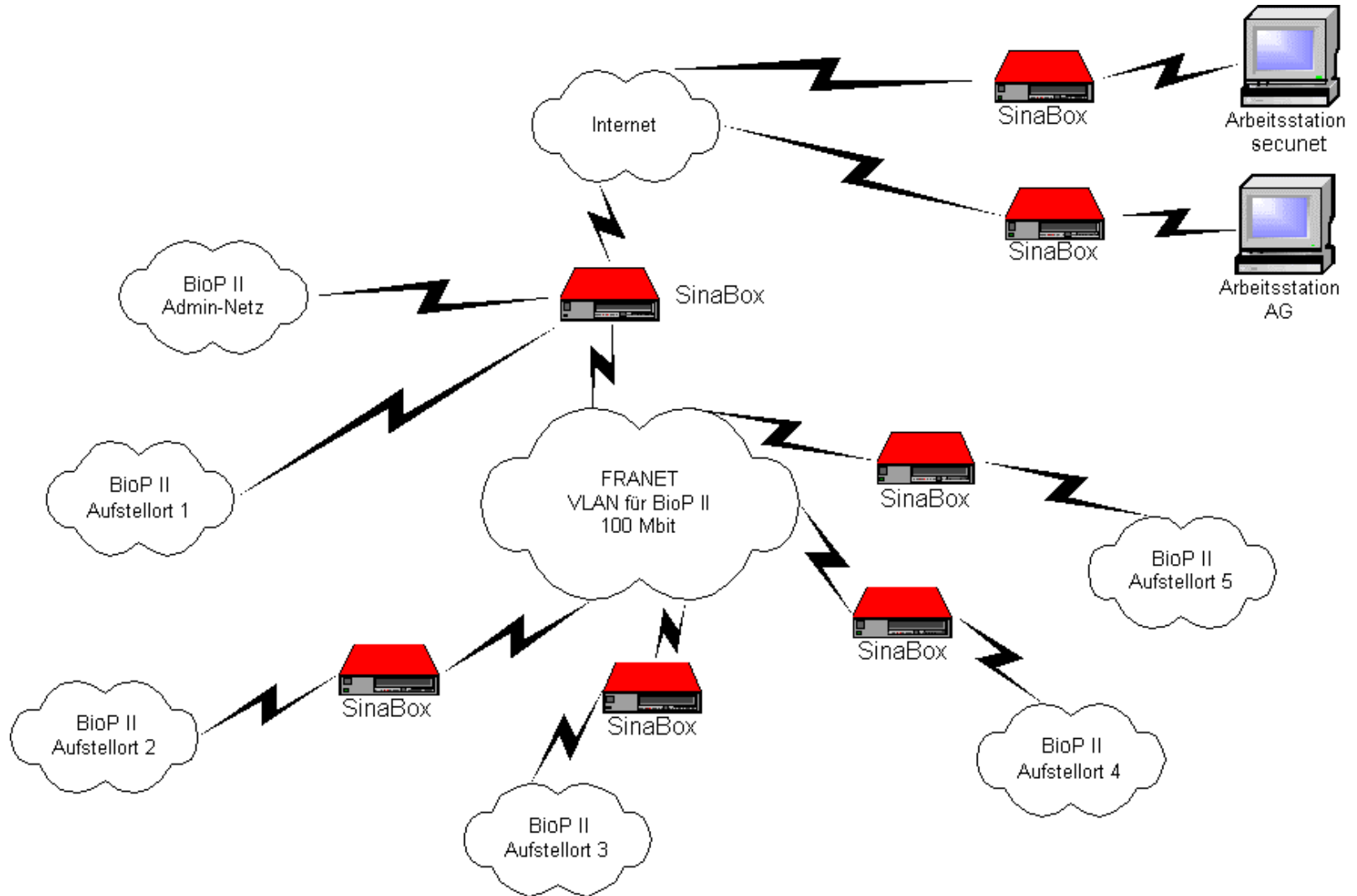
## **Feldtest DB**

- Administratiert durch die Fa. secunet
- User-ID
- Demographische Informationen
- keine Speicherung der Daten auf Biometrie Systemen
- Biometrie Referenz Daten (Bilder und Templates)
- Matching-scores und Lebendbilder

# Datenspeicherung (2)



# BioP II - IT- Infrastruktur



- ✎ Vergleich von **3 verschiedenen biometrischen Verfahren**
- ✎ Vergleich von **2 verschiedenen Fingerprint Systemen**
- ✎ Vergleich **verschiedener Referenz Daten** (Bilder gem. ICAO vs. proprietärer Templates)
- ✎ **Evaluierung der Performanz**
  - ☑ FTE, FRR, FAR
  - ☑ Illustration
    - Genuine-imposter-Verteilungs-Diagramme
    - FAR-FRR-Diagramme
    - ROC-Kurven
- ✎ **Fake-Widerstand**
  - ☑ Lebend-Erkennung
  - ☑ zero-effort-Angriffe
- ✎ **ICAO-Empfehlungen: LDS und Bilder**



## Generell

- hoch komplexer Großfeldversuch bzgl. technischer, administrativer und rechtlicher Aspekte
- Kommunikation mit Benutzern und Transparenz sind kritische Faktoren
- Kommunikation mit Datenschutzbeauftragte und Personal-/ Betriebsräte höchst relevant
- hohe strategische Bedeutung für die beiden Unternehmen

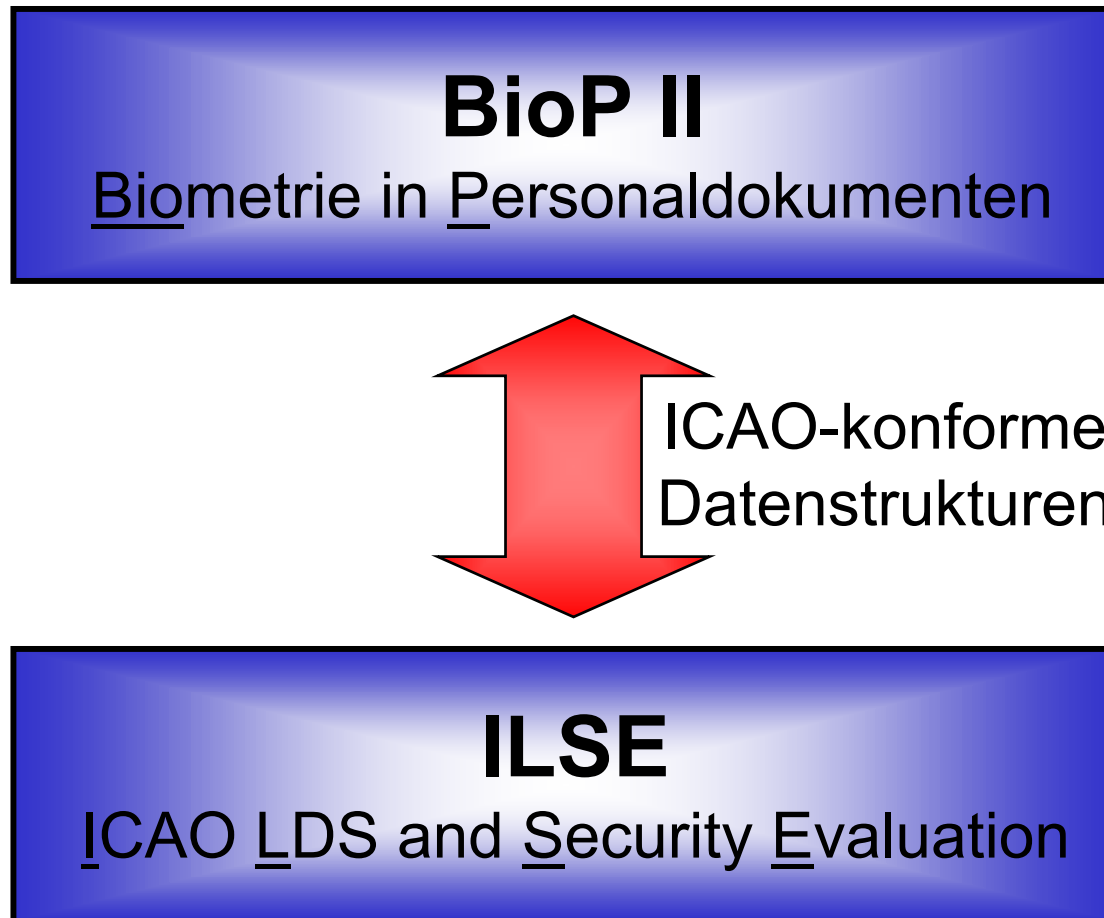
## Details

- Enrolment ist hoch relevant
  - Qualität der Referenzdaten und stabile Lichtbedingungen
- Benutzbarkeit ist abhg. von Systemdesign und Konfiguration
  - Sensor, Zeitverhalten, Feedback (Transparenz)
- Akzeptanz ist abhg. von persönlichen Vorlieben

# Erste Trendaussagen / Empfehlungen zur Einführung

## Generell

- ☑ Unterstützender und überwachter Einsatz sinnvoll
- ☑ Einsatz ICAO-Bilder als Referenz ist möglich
- ☑ neue Passbildrichtlinien gem. ICAO OK
- ☑ hohe Anforderungen an Einsatzumgebung für die Gesichtserkennung
- ☑ Erweiterung Ausweisdokumente um Chip
- ☑ Benutzerfreundliche Systeme sind Pflichtkriterium, Anpassung ggf. notwendig
- ☑ Akzeptanzfördernde Maßnahmen / Aufklärung
- ☑ mögliche Verbesserung von Sicherheit und Erkennungsleistung durch Multimodalität



### Schwachstellenanalyse

- Verifikation / Identifikation als „andere“ Person
- Enrolment unter neuer, veränderter Identität
- „Denial of Service“ : System kann existierendes Merkmal nicht aufnehmen

### Benutzbarkeit biometrischer Systeme

- Leistungsumfang, Eigenschaften und Zweck eines Systems gemäß Dokumentation
- Eigenschaften und Verhalten des Systems in der Realität

### Analyse bzgl. Erkennungsleistung

- FAR
- FRR
- Einfluss spezieller Umwelt- bzw. Operationsbedingungen

- Report BioFace I/II verfügbar jetzt:  
<http://www.bsi.bund.de/literat/studien/bioface/index.htm>
- Report BioFace III verfügbar 1. Q. 2005
  
- Report BioFinger I verfügbar jetzt:  
<http://www.bsi.bund.de/literat/studien/biofinger/index.htm>
- Report BioFinger II verfügbar 2. Q. 2005
  
- Report BioP I verfügbar jetzt:  
<http://www.bsi.bund.de/literat/studien/biop/index.htm>
- Report BioP II verfügbar 1. Q 2005



**Vielen Dank für Ihre  
Aufmerksamkeit**

Bundesamt für Sicherheit in der  
Informationstechnik (BSI)

Dipl. Math. Klaus Keus  
Dr. jur. Astrid Albrecht  
Schlüsseltechnologien  
Godesberger Allee 185-189  
53175 Bonn

Tel: +49 (0)1888-9582-141 / bzw. 371  
Fax: +49 (0)1888-9582-90-141 / bzw. 371

[Klaus.Keus@bsi.bund.de](mailto:Klaus.Keus@bsi.bund.de)  
[Astrid.Albrecht@bsi.bund.de](mailto:Astrid.Albrecht@bsi.bund.de)  
[www.bsi.bund.de](http://www.bsi.bund.de)  
[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)