

10. Veranstaltung - Biometrie

- Warum biometrische Verfahren
- Begriffe
- Biometrische Erkennung
- Fehlerraten
- Einsatzfelder
- Risiken
- ePersonalausweis

Biometrische Verfahren

Die Bedeutung biometrischer Verfahren:

- **Die biometrische Durchdringung des Alltags wird uns in naher Zukunft begegnen bei Zugangskontrollen (Gesichtserkennung bei Zugangskontrollen und auf Reisen), beim Starten von Pkws, am Arbeitsplatz, beim Geldabheben und Bezahlen in Restaurants**
- **Ziel ist eine verbesserte Identitätsprüfung, die über den bloßen Besitz eines Ausweises hinausgeht**
 - In einer vermehrt elektronisch kommunizierenden Welt wächst das Bedürfnis nach vertrauenswürdiger und automatischer Personenidentifikation
 - Körperliche Merkmale sind im Gegensatz zu Wissens- und Besitzelementen unmittelbar personengebunden
 - Eine zweifelsfreie Erkennung ist anhand der Individualität von Menschen möglich, weil sich bestimmte körperliche Merkmale nur einem bestimmten Menschen zuordnen lassen

Quelle: BSI (Hrsg.): Faltblatt Biometrie, o.D., download: www.bsi.de/literat/faltbl/F23Biometrie.htm

Biometrische Verfahren



Die politische Forderung nach verstärktem Einsatz biometrischer Identifikationsverfahren

- *wird regelmäßig mit der Bekämpfung des Terrorismus begründet*
- *2003 wird „Eurodac“, die erste zentrale biometrische Datenbank Europas in Betrieb genommen*
- *2005 bis 2007 wird schrittweise der ePass in Deutschland eingeführt*
- *Ab 2008 werden an deutschen Flughäfen Computer zur Gesichtserkennung eingesetzt*
- *2009 ist die Einführung des ePersonalausweises geplant, über entsprechende Führerscheine wird noch diskutiert*

These: Eine einmal erfolgte biometrische Merkmalerfassung ist unwiderrufbar. Die biometrische Erfassung (Stand:2008) hat Schwächen, ist teuer und die zusätzliche Sicherheit ist kaum nachzuweisen, statt dessen werden neue riskante Datenschutzrisiken generiert

Biometrische Verfahren



Was ist Biometrie?

- *Die automatische Identifikation von Personen auf Grund von persönlichen Merkmalen*
- *Einziges Mittel, die Identität einer Person unwiderlegbar festzustellen, ist die automatische Erkennung persönlicher Eigenschaften. Wir bezeichnen diese als **biometrische Eigenschaften**, die Technik dieser Erkennung als **Biometrie***

Die zwei Hauptkategorien der biometrischen Verfahren:

1. **Identifikation**
 - *Wer bin ich? [1:n]*
2. **Authentifikation (Verifikation)**
 - *Bin ich die Person, für die ich mich ausbebe? [1:1]*

Biometrische Verfahren



Sinn und Zweck von Biometrie:

- **Ziel einer biometrischen Erkennung ist stets, die Identität einer Person zu ermitteln (Identifikation) oder eine behauptete Identität zu bestätigen oder zu widerlegen (Verifikation)**
- **Authentizität ist neben Vertraulichkeit, Integrität und Verfügbarkeit eines der herausragenden Sicherheitsziele im informationstechnologischen Zusammenhang**

Quelle: BSI (Hrsg.): Faltblatt Biometrie, o.D., download: www.bsi.de/literat/faltbl/F23Biometrie.htm

Biometrische Verfahren



Welche Anforderungen sind an biometrische Merkmale für Authentifikationszwecke zu stellen:

- Bei der Entwicklung biometrischer Identifikationsverfahren geht es darum, Körper- und Verhaltensmerkmale zu finden und zur Erkennung zu nutzen,
 - die möglichst eindeutig sind, d. h. sich bei keiner weiteren Person wiederholen: **Eindeutigkeit**
 - bei möglichst vielen Personen vorkommen: **Universalität**
 - sich zeitlich möglichst wenig verändern: **Konstanz**
 - mit möglichst einfachen technischen Mitteln erfassbar sind: **Messbarkeit**
 - deren Erfassung für den Anwender bequem durchführbar ist: **Anwenderfreundlichkeit**

Vgl.: <http://www.bromba.com/faq/biofaqd.htm#Verfahren>

Biometrische Verfahren



Definitionen Biometrie:

- **System zur biometrischen Erkennung:** ein System der Informationstechnik, das Personen durch Messungen von körperlichen Merkmalen erkennt
- **Verifikation** bedeutet „Bestätigung der Identität“
- **Identifikation** bedeutet „Feststellung der Identität“
- **Authentifizierung/Authentifikation** bedeutet „Bezeugung der Echtheit“
- **Autorisierung** bedeutet „Ermächtigung, Bevollmächtigung.“

Quelle: TeleTrust Deutschland e.V. Arbeitsgruppe 6: Biometrische Identifikationsverfahren: Kriterienkatalog V. 2.0, 10.07.2002, S. 4f., www.teletrust.de

Biometrische Verfahren



Wie entstehen biometrische Merkmale?

- **Genotypisch**
 - Biometrische Merkmale sind genetisch bedingt und damit teilweise vererbbar
- **Randotypisch**
 - Biometrische Merkmale entstehen in einer embryonalen Phase auf der Basis von Zufallsprozessen und bleiben ein Leben lang erhalten
- **Konditioniert**
 - Biometrische Merkmale sind verhaltensgesteuert, können teilweise anerzogen und geändert werden

Jedes biometrische Merkmal besitzt alle drei Anteile

Biometrische Verfahren



Was ist ein biometrisches System?

- *Folgende Komponenten sind in allen System enthalten:*
 - *Sensor zur Aufnahme des biometrischen Merkmals*
 - *Recheneinheit zur Verarbeitung und evtl. zur Speicherung des biometrischen Merkmals*
 - *Anwendung, für die der Anwender die Berechtigung nachweisen möchte*
- Die Verarbeitungseinheit setzt sich im Detail zusammen aus:
 - *Merkmalsextrahierer, der aus den vom Sensor gelieferten Rohdaten die Einmaligkeitsdaten herausfiltert und in einem Anfragetemplate zusammenfasst,*
 - *"Matcher", der das Anfragetemplate mit einem oder mehreren Referenztemplates vergleicht und das Ergebnis als "Score"-Werte weitergibt,*
 - *Entscheider, der den oder die Scorewerte in Bezug zu einem Schwellwert setzt und daraus in der Regel eine zweiwertige Entscheidung ableitet (berechtigt oder nicht berechtigt).*

Quelle: <http://www.bromba.com/faq/biofaqd.htm#Verfahren>

Biometrische Verfahren



Grundprinzip der biometrischen Erkennung in allen Systemen gleich!

- *Folgende Komponenten sind unabhängig von dem individuellen technologischen Aufbau in allen System enthalten:*
 1. *Personalisierung oder Registrierung des Nutzers im System (Enrolment)*
 2. *Erfassung der biometrisch relevanten Eigenschaften einer Person*
 3. *Erstellung von Datensätzen (Templates)*
 4. *Vergleich der aktuell präsentierten mit den zuvor abgespeicherten (Matching)*

Biometrische Verfahren



Grundprinzip einer biometrischen Wiedererkennung:

- Das jeweilige **biometrische Merkmal** wird mit Hilfe eines **Sensors** erfaßt
- Die unmittelbaren Aufnahmen [Bild des Originalmerkmals] nennt man **Rohdaten**
- Aus den Rohdaten wird in einem technischen Verfahren ein **Template**, das heißt ein kleiner Datensatz erzeugt. - I.d.R. mit einem **herstellerspezifischen! Algorithmus**
- Bei der **ersten Benutzung** eines Aufnahmegerätes, dem „**enrolment**“ wird derart das individuelle biometrische Merkmal eingelernt
- **Identifikation** zielt auf einen **Abgleich** des Template des aktuellen Benutzers mit allen **eingelernten Templates** in einem System
- Als **Ergebnis** wird eine **Nutzererkennung**, z.B. der Name des Betroffenen ausgeworfen
- **Alle existierenden Systeme weisen noch beträchtliche Fehlerraten auf!**

Biometrische Verfahren



Prinzipieller Ablauf einer biometrischen Erkennung:

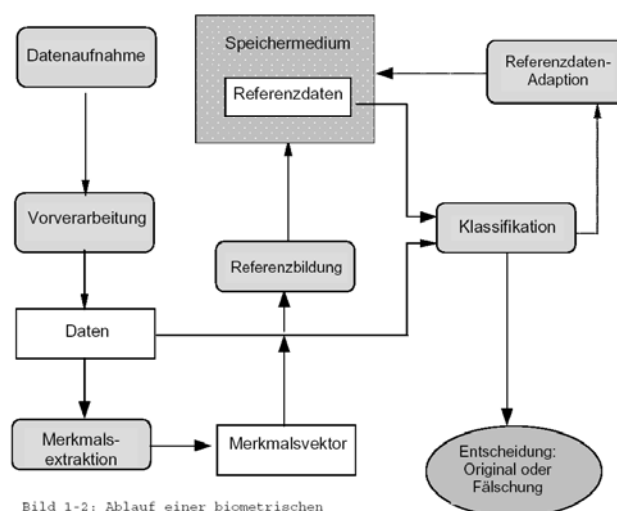


Bild 1-2: Ablauf einer biometrischen Verifikation

Biometrische Verfahren



Messtechnische Erfassung biometrischer Merkmale:

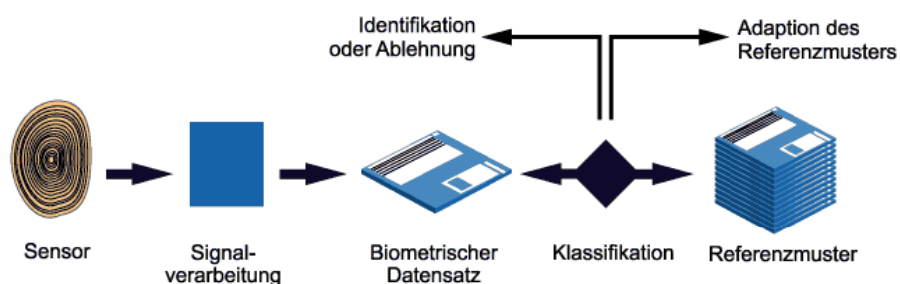
- **optische Erfassung mit Kamera[s]**
- **Abtastung mit Laserstrahl**
- **Erfassung von Wärme, Druck**
- **Ultraschall**
- **Elektrische Verfahren**
- **Mikrophon**

Quelle: Brüderlein, R.: Was ist Biometrie?

Biometrische Verfahren



Identifikationsverfahren / Merkmalerfassung im System:



© tecChannel.de

Biometrische Verfahren



Sollen Messung und Vergleich mit vorher gespeicherten Daten automatisch erfolgen, so sind folgende Anforderungen an diese biometrischen Eigenschaften zu stellen :

- **Invarianz der Eigenschaften**
- **Erfassbarkeit**
- **Einzigartigkeit**
- **Akzeptanz**
- **Reduzierbarkeit**
- **Zuverlässigkeit**
- **Datenschutz**

Biometrische Verfahren



Auswertbare Merkmale:

- **Finger- und Handflächenabdruck**
- **Handvenenmuster**
- **Handgeometrie**
- **Ohr- und Iris (Regenbogenhaut)- und Retinamuster**
- **Gesichtsgeometrie**
- **Stimme**
- **Lippenbewegungen**
- **Körpergeruch**
- **DNA**
- **auch dynamische Vorgänge / Bewegungen**
 - *Gang, Lippen, Gestik/Mimik beim Sprechen*
 - *Unterschrift, Schreibverhalten*
 - *Gesamtkörper, Sprechverhalten*
 - *Tipverhalten auf der Tastatur*

Biometrische Verfahren



Sollen Messung und Vergleich mit vorher gespeicherten Daten automatisch erfolgen, so sind folgende Anforderungen an diese biometrischen Eigenschaften zu stellen:

Eigenschaft	Erfassung	Invarianz	Einzigartigkeit	Akzeptanz
Handgeometrie	Optisch (IR)	gut	1:1000	sehr gut
Zwei-Finger-geometrie	Optisch (IR)	gut	1:1000	sehr gut
Augennetzhaut	Optisch (Laser)	sehr gut	1:1 Million	nicht gut
Augeniris	Optisch	sehr gut	1: 6 Millionen	nicht gut
Venen Handoberfläche	Optisch (IR)	gut	unbekannt	sehr gut
Unterschrift	Dynamisch (Druck)	nicht gut	1:10000	sehr gut
Stimme	Elektroakustisch	nicht gut	1:10000	gut
Gesicht	Optisch oder IR	gut	unbekannt	gut
Fingerabdruck	Optisch, kapazitiv etc.	sehr gut	1:1 Million	gut

Quelle: Brüderlein, R.: Was ist Biometrie?

Prozessoptimierung mit RFID

Leibniz Universität Hannover Institut für Wirtschaftsinformatik

Dr. Günter Wohlers | 04.07.2008 | Folie 17/46

Biometrische Verfahren



Beurteilung von biometrischen Systemen:

- **Zeitbedarf der Erstregistrierung**
- **Zeitbedarf einer Verifikation**
- **Falsche Akzeptanz (Falsch-Akzeptanz-Rate [False Acceptance Rate])**
- **Falsche Rückweisung (Falsch-Rückweisungs-Rate [False Rejection Rate])**
- **Gleichfehlerpunkt (Equal Error Rate)**
- **Failure to enrol rate gibt den Prozentsatz der potentiellen Nutzer an, bei denen das Enrolment nicht erfolgreich durchgeführt werden kann**

Das ideale biometrische Verfahren für alle Anwendungen gibt es nicht!

Quelle: Brüderlein, R.: Was ist Biometrie?

Prozessoptimierung mit RFID

Leibniz Universität Hannover Institut für Wirtschaftsinformatik

Dr. Günter Wohlers | 04.07.2008 | Folie 18/46

Biometrische Verfahren

Beurteilung von biometrischen Systemen:

- Je mehr Lebend-Erkennung, desto komplexer wird die Erfassung
- Je höher die Komplexität der Erfassung, desto schwieriger ist das Erreichen guter Erkennungsleistungen
- Und: desto teurer wird das biometrische System! Fraglich wird dann, ob es für einen Massenmarkt geeignet ist?
- Ein weiteres Problem stellt die Alterung des Referenzmuster (Templat-Aging) dar
- Es gibt für jedes Merkmal so genannte Problemuser, die nicht eingelernt werden können oder Schwierigkeiten mit der Erfassung des Merkmals haben

Biometrische Verfahren

Herleitung von Fehlerraten:

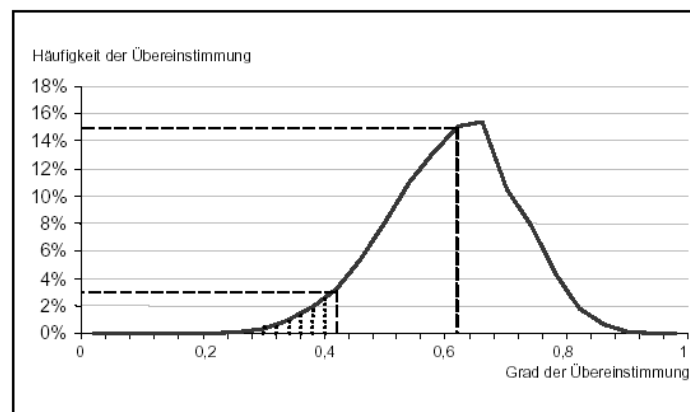


Bild 3-1: Verteilung der Anzahl der übereinstimmenden Merkmale

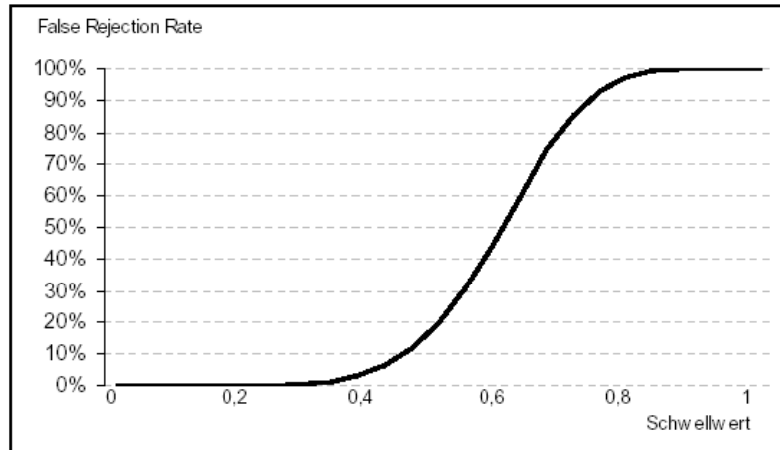
Quelle: TeleTrust Deutschland e.V. Arbeitsgruppe 6: Biometrische Identifikationsverfahren: Kriterienkatalog V. 2.0, 10.07.2002, S. 9f., www.teletrust.de

Biometrische Verfahren



FRR: die False Rejection Rate

Verteilung des Anteils der zu Unrecht Abgewiesenen in Abhängigkeit vom Schwellenwert



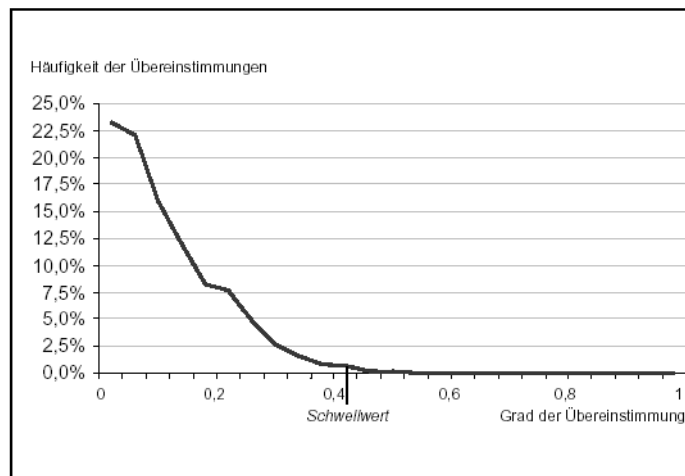
Quelle: TeleTrust Deutschland e.V. Arbeitsgruppe 6: Biometrische Identifikationsverfahren: Kriterienkatalog V. 2.0, 10.07.2002, S. 9f., www.teletrust.de

Biometrische Verfahren




FAR: die False Acceptation Rate

Verteilung der Anzahl der übereinstimmenden Merkmale



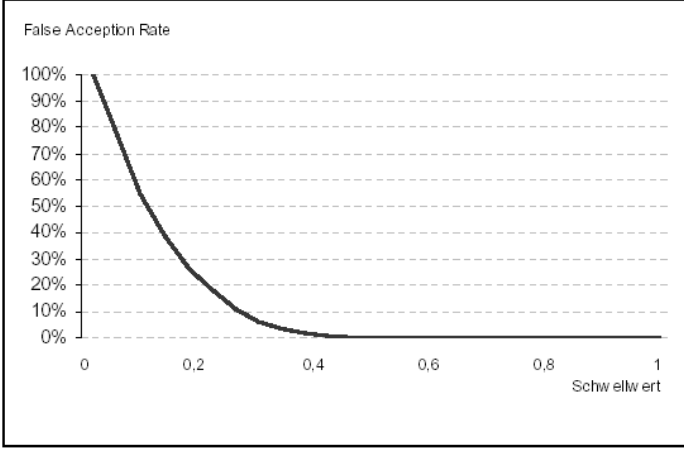
Quelle: TeleTrust Deutschland e.V. Arbeitsgruppe 6: Biometrische Identifikationsverfahren: Kriterienkatalog V. 2.0, 10.07.2002, S. 12, www.teletrust.de

Biometrische Verfahren



FAR: die False Acceptance Rate


Verteilung des Anteils der zu Unrecht Zugelassenen in Abhängigkeit vom Schwellenwert



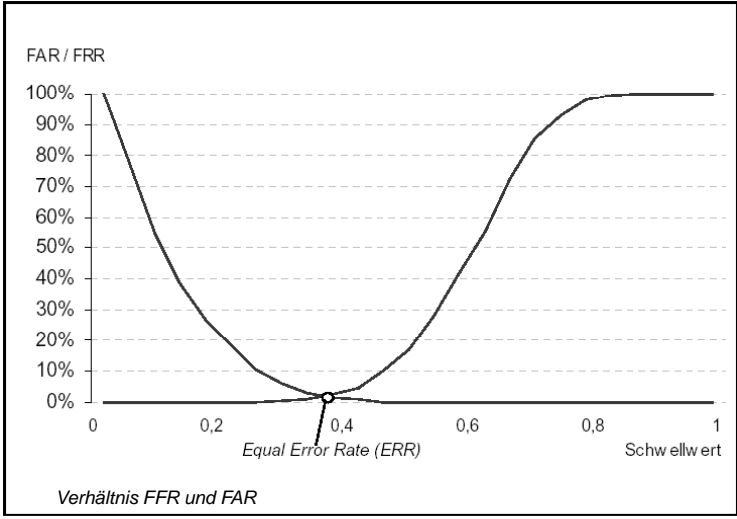
Quelle: TeleTrust Deutschland e.V. Arbeitsgruppe 6: Biometrische Identifikationsverfahren: Kriterienkatalog V. 2.0, 10.07.2002, S. 12, www.teletrust.de

Prozessoptimierung mit RFID
Leibniz Universität Hannover Institut für Wirtschaftsinformatik
Dr. Günter Wohlers | 04.07.2008 | Folie 23/46

Biometrische Verfahren

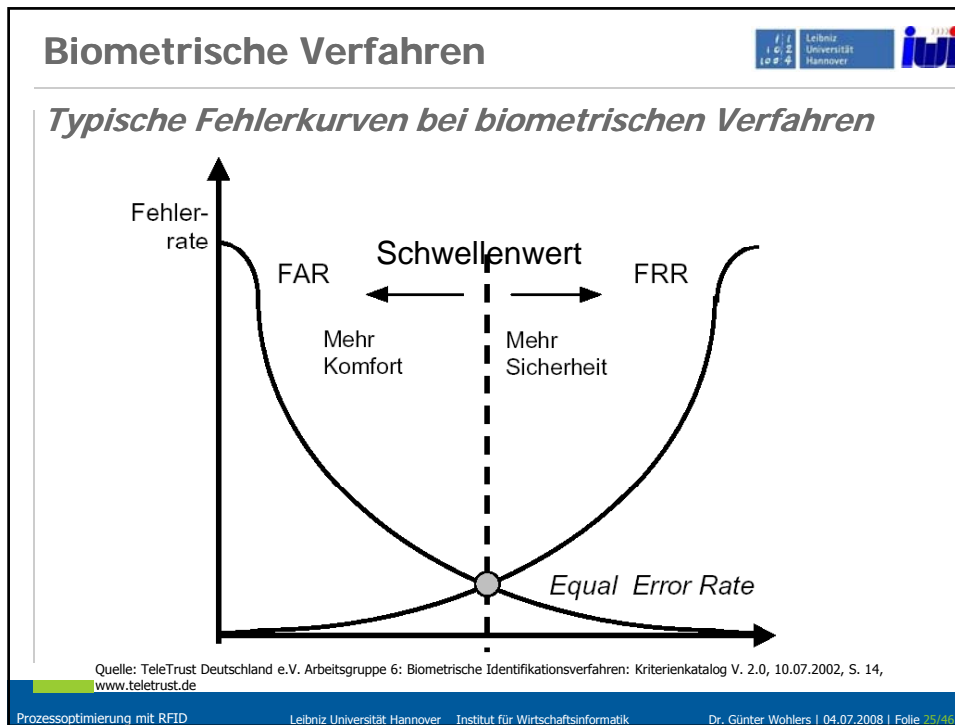


EER: Equal Error Rate




Quelle: TeleTrust Deutschland e.V. Arbeitsgruppe 6: Biometrische Identifikationsverfahren: Kriterienkatalog V. 2.0, 10.07.2002, S. 12, www.teletrust.de

Prozessoptimierung mit RFID
Leibniz Universität Hannover Institut für Wirtschaftsinformatik
Dr. Günter Wohlers | 04.07.2008 | Folie 24/46



Biometrische Verfahren



Einsatzfelder für biometrische Verfahren (lt. Teletrust):

- **Zutrittsmechanismen**
 - Als „elektronischer Pfortner“ für die Zutrittskontrolle zu Gebäuden
 - Zutrittskontrolle mit Zeiterfassung und Verweildauerkontrolle
 - Zutrittskontrolle zu Sicherheits- und Hochsicherheitsbereichen
- **Zugriff / Zugang zu elektronischen Geräten/Daten**
 - Integration eines biometrischen Systems in bestimmten Applikationen, um damit den Zugriff auf sensitive Unternehmensdaten zu schützen.
 - Zugang zum Computer (anstelle der Passworteingabe) oder zu Netzen bzw. Netz-Segmenten.
 - Zugriff auf Geldautomaten (in Verbindung mit EC-Karte)
 - Zugang zu Internetdiensten
 - Zugang zum Mobiltelefon bzw. zu anderen sicherheitssensiblen Geräten
 - Zugriff auf den Signiermechanismus bei der elektronischen Signatur (zur Vornahme elektronischer Transaktionen)
- **Weitere Einsatzfelder**
 - Quittierung eines Vorgangs anstelle einer Unterschrift oder einer Paraphe

Quelle: TeleTrust Deutschland e.V. Arbeitsgruppe 6: Biometrische Identifikationsverfahren: Kriterienkatalog V. 2.0, 10.07.2002, S. 20f., www.teletrust.de

Prozessoptimierung mit RFID Leibniz Universität Hannover Institut für Wirtschaftsinformatik Dr. Günter Wohlers | 04.07.2008 | Folie 26/46

Biometrische Verfahren



Für 7 Euro kann man sich von seinem Fingerabdruck eine Stempel anfertigen lassen:



Quelle: Bromba, M. (Siemens AG – Bereich ICM Biometrics): Biometrie und Sicherheit, www.bromba.com/knowhow/biosich.htm


Biometrische Verfahren



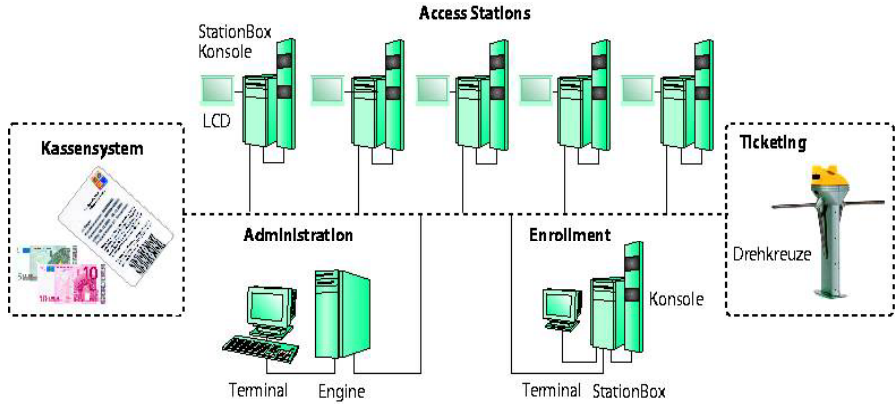
Zoo Hannover: Größte Gesichtserkennungssystem auf dem europäischen Kontinent



Biometrische Verfahren



Zoo Hannover: Größte Gesichtserkennungssystem auf dem europäischen Kontinent




Quelle: Ziegler, P.-M.: Adlauge, in: c't 2003 J

Prozessoptimierung mit RFID
Leibniz Universität Hannover Institut für Wirtschaftsinformatik
Dr. Günter Wohlers | 04.07.2008 | Folie 29/46

Biometrische Verfahren




Irisscan am Frankfurter Flughafen:



Prozessoptimierung mit RFID
Leibniz Universität Hannover Institut für Wirtschaftsinformatik
Dr. Günter Wohlers | 04.07.2008 | Folie 30/46

Biometrische Verfahren




Chancen und Risiken der Biometrie:
Personengebundenheit der Merkmale

- **Chancen:**
 - *Höhere Sicherheit*
 - *Größere Rechtsverbindlichkeit*
 - *Einfachere Handhabung / mehr Bequemlichkeit*
- **Risiken:**
 - *Lebenslange und untrennbare Merkmalsverknüpfung mit der Person*
 - *Begrenzte Verfügbarkeit der Merkmale*
 - *Verlässlichkeit der Systeme! (bisher keine 100%-Erkennung erreichbar)*
 - *Datenschutz und –sicherheit (informationelles Selbstbestimmungsrecht)*

Prozessoptimierung mit RFID Leibniz Universität Hannover Institut für Wirtschaftsinformatik Dr. Günter Wohlers | 04.07.2008 | Folie 31/46

Biometrische Verfahren



Maßnahmen:

US-Visa für Mexiko mit Fingerabdruck
Ausweise in Malaysia, Brunei, Ägypten mit biometrischen Merkmalen
ICAO (International Civil Aviation Organisation)

- **Standardisierung von Machine Readable Travel Documents (MRTD), vorwiegend Pässe**
- **Vorauswahl fiel auf Gesichtskennung und Fingerabdruck**
- **Optional zusätzlich weitere freiwillige Merkmale**

Abkommen USA / EU-Kommission über Weitergabe von Passagierdaten auf Transatlantikflügen erstmals 05/2004

Prozessoptimierung mit RFID Leibniz Universität Hannover Institut für Wirtschaftsinformatik Dr. Günter Wohlers | 04.07.2008 | Folie 32/46

Biometrische Verfahren



Maßnahmen:

US-VISIT-Programm

- Betrieben vom Department of Homeland Security an 115 Flughäfen und 14 Seehäfen
- Seit Januar 2004 bereits Erfassung der Zeigefinger (Speicherung: 100 Jahre) und des Gesichts bei Einreise, inzwischen erweitert auf alle 10 Finger
- „Early 2004“ Abgleich der Einreisedaten bei Ausreise
- Abgleich der biometrischen Daten mit bekannten und verdächtigen Terroristen

„MATRIX“

Multistate Anti-Terrorism Information Exchange

Biometrische Verfahren



Maßnahmen:

Die USA forderten im „Visa Entry Reform Act“ (Section 4b) Biometrie im Pass für die Staaten des VISA-Waiver-Programms (überwiegend EU-Staaten) bereits ab dem 26.10.2004



Fingerabdruckerkennung
und Gesichtserkennung
bei der Einreise in die USA

Bildquelle: o.V., Gesichtskennung, dreidimensional,in: Forschung & Lehre 8/06, S. 444



Biometrische Verfahren

Aktuelle Entwicklungen:

Sämtliche ab November 2005 neu ausgestellten Pässe in der EU enthalten biometrische Daten (Gesichtsbild und ab 2007 auch Fingerabdruck).



Im April 2006 wurde das durch die Europäische Kommission geförderte Projekt „3-D Face“ (Entwicklung eines 3-D-Erkennungssystems z.B. für die Grenzkontrollen) begonnen

Quelle: http://www.igd.fraunhofer.de/igd-a8/publications/flyer/3d-face_flyer_deutsch.pdf#search=%223-d%20face%22




Fotos: Fraunhofer Institut





Gesichtserkennungssystem

Prozessoptimierung mit RFID Leibniz Universität Hannover Institut für Wirtschaftsinformatik Dr. Günter Wohlers | 04.07.2008 | Folie 35/46



Biometrische Verfahren

Aktuelle Entwicklungen:


Viisage FaceFINDER®
*Reliably Identify Individuals.
 Protect Privacy.
 Smart screening and surveillance for reliable identification of individuals in real-time (2004)*


„FaceFINDER scans persons in controlled scenarios like border crossing without the actual cooperation of the person“

Quelle: http://www.viisage.com/ww/en/pub/viisage___products/facefinder.htm

**Big Brother im Hauptbahnhof Mainz
 Modellversuch „Fotofahndung“ des BKA
 mit 200 Testpersonen und neuen Kameras –**

Die neue Technik könnte die Polizeifahndung revolutionieren, aber auch den Überwachungsstaat ein Stück näher bringen!





„Wer sich einen Bart ins Gesicht klebt, wird trotzdem erkannt“: Im Mainzer Hauptbahnhof wird die Fotofahndung getestet. ap

Quelle: Rath, C.: Big Brother im Hauptbahnhof, in: Hannoversche Allgemeine Zeitung, 11.10.2006, S. 3

Prozessoptimierung mit RFID Leibniz Universität Hannover Institut für Wirtschaftsinformatik Dr. Günter Wohlers | 04.07.2008 | Folie 36/46

Biometrische Verfahren



Beispiele für biometricspezifische Angriffs-Szenarien: Biometrisches Merkmal Fingerabdruck

- **geringer Aufwand** der Angreifer: *falsche Finger auflegen, Anhauchen, Befeuchten oder Kühlen (z.B. Wasserbeutel) des Sensors zur Aktivierung von Altabdrücken*
- **mittlerer Aufwand** der Angreifer: *Kunstfinger (z. B. aus Silikon oder Wachs) durch genauen Abguss herstellen, Fingerabdruck von Glas aufnehmen, einscannen und digitalisierte Daten in das System einspielen.*
- **hoher Aufwand** der Angreifer: *Spezialisierten Kunstfinger herstellen, der auch eine Lebend-Prüfung täuscht (Wärmen, Fluoreszenz, Pulssimulation)*

Biometrische Verfahren



Beispiele für biometricspezifische Angriffs-Szenarien: Biometrisches Merkmal Gesicht

- **geringer Aufwand** der Angreifer: *Personenveränderung durch Bart, Brille, Perücke, Make-up u.a.*
- **mittlerer Aufwand** der Angreifer: *Benutzung einer Fotografie oder einer Videosequenz (Abspielen mittels Laptop vor der Kamera, Foto einscannen und digitalisierte Daten in das System einspielen.*
- **hoher Aufwand** der Angreifer: *Erstellung einer Videosequenz und Einspielen in die Datenverbindung, Kunstkopf anfertigen.*

Biometrische Verfahren



Die besonderen Risiken der biometrischen Erkennung liegen:

- in der Erfassung und Erhebung lebenslang gleich bleibender Merkmale, die in die Verfügungsgewalt Dritter gelangen. Hiermit verbunden sind die klassischen Risiken des Datenschutzes
- in der Schaffung ubiquitärer Identifikations- und überwachungsgerechter Infrastrukturen und damit auch der Gefährdung der Anonymität im Alltagsleben
- in der Beschränkung der Freizügigkeit durch die Schaffung erheblicher bürokratischer Hindernisse für den Vorgang des Reisens
- in der Veränderung kultureller Errungenschaften offener und demokratischer Gesellschaften und damit einer unweigerlichen Veränderung des gesellschaftlichen Klimas

Quelle: Humanistische Union, Reader zur Fachanhörung Bündnis 90/Die Grünen vom 19.05.2003 in Berlin: „Mehr Sicherheit durch Biometrie“?

Biometrische Verfahren



Menschen- und bürgerrechtliche Perspektive:

- **Humanistische Botschaft: „Jeder Mensch ist einzigartig“ (Würde, Abkopplung vom Tierreich, freies und autonomes Handeln)**
- **Durch Biometrie materialistisch gewendet: nicht der Geist, sondern die Physiologie verbürgt die menschliche Einzigartigkeit**
- **Der Preis, den die Menschen für eine globalisierte und mobile internationale Gesellschaft zahlen sollen, ist möglicherweise ein Verlust grundlegender Kontrollerfahrungen in Bezug auf die sie betreffenden Informationen**

Biometrische Verfahren



Handelsblatt vom 21.10.2004:

- „Ein Mikrochip unter der Haut kann Patienten im Notfall das Leben retten, aber auch für eine lückenlose Kontrolle missbraucht werden. Nach Prüfung der medizinischen Fragen erhielt das Unternehmen Applied Digital Solutions in Delray Beach, Florida, jetzt die Zulassung der US-Arzneimittelbehörde (FDA) für die Vermarktung ihres „Verichips“. Dieses reiskorngroße Stück Elektronik nutzt die RFID-Technik, um medizinische Daten seines Trägers per Funk zu übertragen... Um das Geschäft in Gang zu bringen, will Applied Digital 200 Schmerzzentren in den USA kostenlos mit einem RFID-Scanner ausstatten, der sonst 650 Dollar (520 Euro) kosten soll. Die Chip-Implantation kostet nach Angaben von Applied-Digital-Sprecherin Angela Fulcher 150 bis 200 Dollar (120 bis 160 Euro). Gedacht wird zuerst vor allem an den Einsatz bei Patienten mit Diabetes oder Alzheimer...Der RFID-Chip steckt Haustieren schon länger unter der Haut. Applied Digital ist in diesem Markt seit 15 Jahren tätig. Rund einer Million Tieren wurde ein solcher Chip eingesetzt und die Firma hat bereits 50 000 Scanner verkauft.“

Biometrische Verfahren

Die bekannten Risiken von MRTDs (Machine Readable Travel Documents):

- *im Unterschied zu traditionellen papiergebundenen Pässen können Daten aus den neuen MRTDs aus Entfernungen bis zu 10 m unbemerkt und ohne Einflussnahme (aus Sicht des Passinhabers) abgehört oder ausgelesen werden*
- *Die bestehende Zugriffssicherung kann gebrochen oder umgangen werden. Damit besteht das Risiko der automatisierten Überwachung (mittels Tracking) von Personen in Situationen, in denen sie MRTDs bei sich tragen, z.B. als Touristen im Ausland*
- *Biometrische Referenzdaten können in der Form, in der sie in MRTDs gespeichert werden, ungehindert auch für andere als den vorgesehenen Zweck verwendet werden. Eine solche Zweckentfremdung verletzt europäisches Datenschutzrecht. Darüber hinaus beruht biometrische Identifizierung auf Wahrscheinlichkeiten – Fehlerkennungen und Fehlzurückweisungen sind unumgänglich und werden europäische Bürger täglich betreffen*

Quelle: fidis: Budapest-Erklärung zu maschinenlesbaren Ausweis-Dokumenten;
download: <http://www.fidis.net/press-events/press-releases/budapest-erklarung/#c1297>

Biometrische Verfahren



Die bekannten Risiken von MRTDs (Machine Readable Travel Documents):

- *Biometrische Informationen in MRTDs können derzeit nicht widerrufen werden. Da physische Merkmale wie das Gesicht oder Fingerkuppen nicht einfach geändert werden können, können einmal „gestohlene“ biometrische Merkmale lange Zeit missbraucht werden*
- *Das Schlüsselmanagement bei BAC (Basic Access Control = Zugriffssicherung) ist unzureichend. Der Schlüssel für den Zugang zum RFID-Chip ist auf dem Pass selbst gespeichert und kann maschinell sowie von Personen gelesen werden. Dies bedeutet, dass jeder, der berechtigt oder unberechtigt den ePass in den Zugriff bekommt, den Schlüssel kopieren, speichern und für den Zugriff auf die Daten im RFID-Chip nutzen kann*
- *RFID-Chips in MRTDs konnten bereits kopiert (geklont) werden*
- *Die Lesbarkeit der RFID-Chips in Pässen aus der Entfernung könnte genutzt werden, um z.B. personenspezifisch Bomben auszulösen*

Quelle: fidis: Budapest-Erklärung zu maschinenlesbaren Ausweis-Dokumenten;
download: <http://www.fidis.net/press-events/press-releases/budapest-erklaerung/#c1297>

Biometrische Verfahren



Biometrischer Personalausweis: überflüssig oder sicher?

(Auszüge aus einem Interview mit Peter Schaar, 1.7.2006)

- *Kloiber: Worin besteht denn der große Eingriff in meine informationelle Selbstbestimmung? Ein Bild ist doch bislang auch auf meinem Personalausweis, und jetzt ein Fingerabdruck, ist das so schlimm?*
- *Schaar: [...]Es kann gegebenenfalls, wenn dann auch zentrale oder auch dezentrale Dateien geführt werden, in denen die biometrischen Daten gespeichert werden, dazu kommen, dass solche Systeme gekoppelt werden mit Videoüberwachungsanlagen und dann entsprechend die einzelnen Personen identifiziert werden, wo sie sich dann jeweils aufhalten. Bei den Fingerabdrücken haben wir bisher eine Begrenzung auf erkennungsdienstliche Sammlung. Das heißt, nur wer ein Verbrechen begeht oder eine sonstige schwere Straftat, wird erfasst - nicht jedermann! Eine erkennungsdienstliche Erfassung der gesamten Bevölkerung halte ich doch für ziemlich problematisch.*
- *Kloiber: Nun gibt es ja einen sehr starken internationalen Druck, um biometrische Merkmale in Passdokumente einzuführen, die amerikanischen Behörden verlangen das mittlerweile.*
- *Schaar: Interessant ist ja, dass die US-Behörden die biometrischen Merkmale nur von den einreisenden Ausländern verlangen, aber nicht von den US-Amerikanern. Und zweitens ist es so, dass die US-Behörden für ihre eigenen Bürger auch keine entsprechenden Personalpapiere einführen. Die haben ja bisher nicht mal einen Personalausweis und werden auch in Zukunft keinen Personalausweis haben. Schon von daher stellt sich natürlich die Frage, ob man nach dem Reisepass, der durch internationale Vorgaben normiert ist, auch noch einen Biometrie gestützten Personalausweis wirklich braucht.*

Quelle: www.bfdi.bund.de/cdn_030/nn_531474/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2006/Interview_20dradio_20biometrPerso.html__nnn=true

Biometrische Verfahren

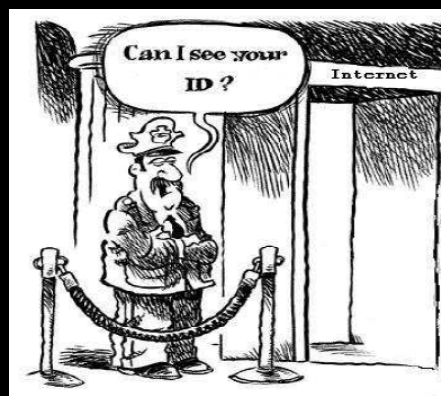
Biometrischer Personalausweis = ePersonalausweis

- Die Feinspezifikation soll bis zum 4. Quartal 2009 abgeschlossen sein
- Die ersten Ausweise sollen Ende 2009 ausgegeben werden
- Vorgesehen ist Scheckkartengröße, gespeichert wird: ein sichtbares digitales Foto, unsichtbar zwei Fingerabdrücke des linken und rechten Zeigefingers und ein PIN-Code
- Wie die elektronische Gesundheitskarte soll auch der ePersonalausweis für die qualifizierte Signatur vorbereitet sein
- Der Ausweis soll kontaktlos arbeiten
- Der Ausweis soll ein zusätzliches ID-System enthalten, auf das zertifizierte Firmen und Institutionen über das Web zugreifen können
- Personalausweise mit derart umfangreichen Funktionen gibt es bisher noch nicht!
- Nach Angaben des BKA wurden in den vergangenen sieben Jahren 216 Fälschungsfälle registriert, davon 88 Totalfälschungen
- Die Einführung eines zentralen Fingerabdruckdatei ist zur Zeit von der Regierung nicht vorgesehen!

Vgl.: [http://www.heise.de/security/Elektronischer-Personalausweis-Wenn-das-Web-den-Ausweis-sehen-will--/news/meldung/108208;](http://www.heise.de/security/Elektronischer-Personalausweis-Wenn-das-Web-den-Ausweis-sehen-will--/news/meldung/108208)
http://phillipbanse.de/wp/2008/03/13/pb_06-elektronischer-personalausweis-im-deutschlandfunk/

UbiComp - Biometrie

Vielen Dank für Ihre Aufmerksamkeit!



Quelle: <http://userpage.fu-berlin.de/~bendrath/Identity-Privacy-RB-04-2007.pdf>