

# **Komfortable sichere Biometrie: Von der Wegfahrsperre für den PC zum universellen Sicherheitstoken**

## **Informatikunterricht der Zukunft**

3. März 2006, Jena

Henning Arendt

**@bc<sup>®</sup>**

[www.atbc.de](http://www.atbc.de)

Dipl.-Ing. Henning Arendt, Arendt Business Consulting Idstein

## **Komfortable sichere Biometrie:**

### **Von der Wegfahrsperre für den PC zum universellen Sicherheitstoken**

Die inflationäre Zunahme von PINs und Passwörtern für die unterschiedlichsten Anwendungen vom PC-Login über die ebay-Anmeldungen bis zum Geldautomaten ist weder benutzerfreundlich noch besonders sicher: Kaum jemand kann sich diese Fülle der Zugangsdaten merken. Entweder stehen die Daten auf Zetteln oder es werden die gleichen Namen und Passwörter verwendet. Beispielhaft werden sichere Lösungen aufgezeigt, bei denen sich der Nutzer biometrisch authentifiziert. Neben dem hohen Komfort erfolgt auch gleichzeitig eine viel stärkere Bindung an die Person. Ebenfalls lassen sich die Forderungen von Daten- und Verbraucherschützern realisieren: Die biometrischen Referenzdaten bleiben beim Nutzer und werden ausschließlich von ihm kontrolliert.

# Biometrie: Spracherkennung

Wenn nun einer von den Flüchtlingen Ephraims sprach: Lass mich hinübergehen!, so sprachen die Männer von Gilead zu ihm: Bist du ein Ephraimter? Wenn er dann antwortete: Nein!, ließen sie ihn sprechen: **Schibbolet**. Sprach er aber: **Sibbolet**, weil er's nicht richtig aussprechen konnte, dann ergriffen sie ihn und erschlugen ihn an den Furten des Jordans, so dass zu der Zeit von Ephraim fielen zweiundvierzigtausend.

Richter 12, Vers 6

Wegfahrsperre von ABS-Jena



- Messung („Metrik“) individuell charakteristischer, personengebundener Lebensmerkmale.
- Gleichzeitige Prüfung des Legitimationsmittels und seines Eigentums.
- Vorteile biometrischer Merkmale im allgemeinen:
  - schwer zu stehlen und zu kopieren
  - komfortabel zu nutzen
  - können nicht vergessen werden

## Physiologisch

- einzigartig
- unveränderbar
- nicht übertragbar

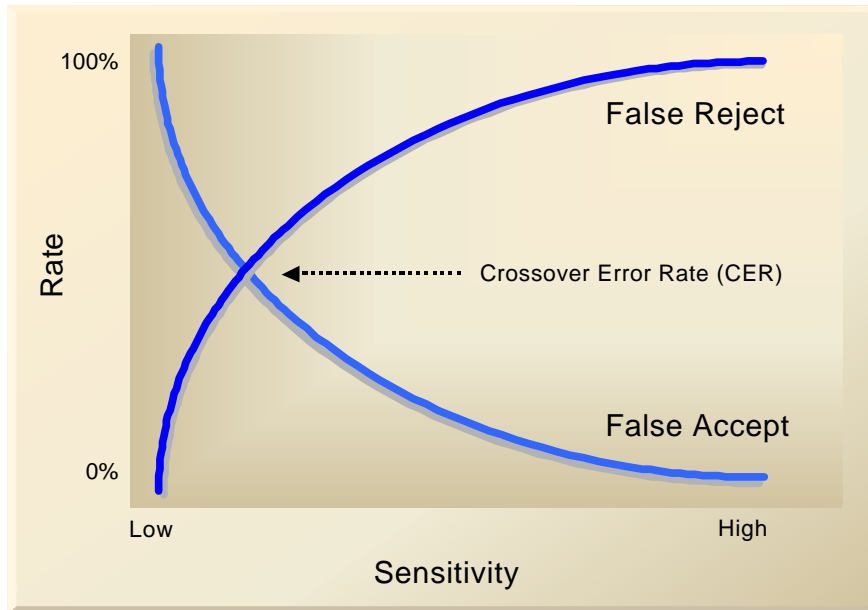
Beispiele:	Nutzung
■ Fingerbild	- 49%
■ Hand	- 10%
■ Gesicht (Iris)	15%+6%
■ Venenmuster (NEU)	

## Verhaltenstypisch

- Eingebaute Bewegungsabläufe aufgrund von Kinematik und Motorik

Beispiele:	Nutzung
■ Unterschrift	3%
■ Stimme	4%
■ Lippenbewegungen	<1%
■ Tippverhalten	<1%

# Biometrische Begriffe



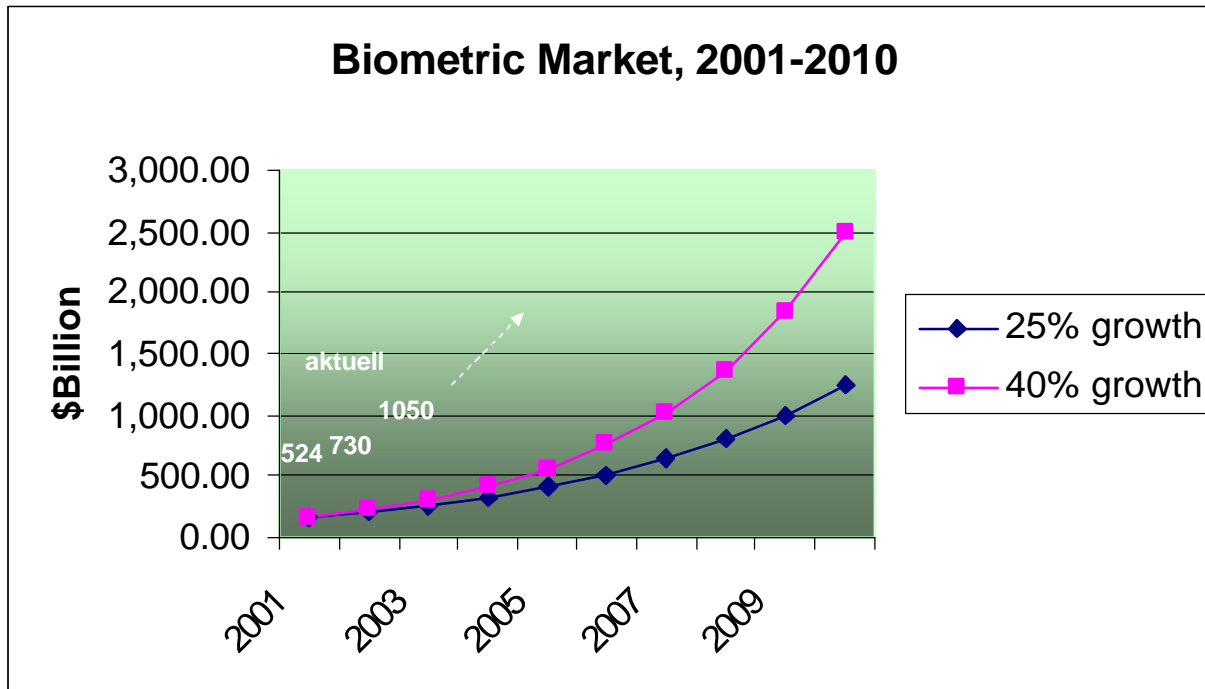
**False Reject Rate (FRR)**

**Equal Error Rate (EER)**

**False Accept Rate (FAR)**

**Failure to Enroll (FTE)**

# Der Biometriemarkt

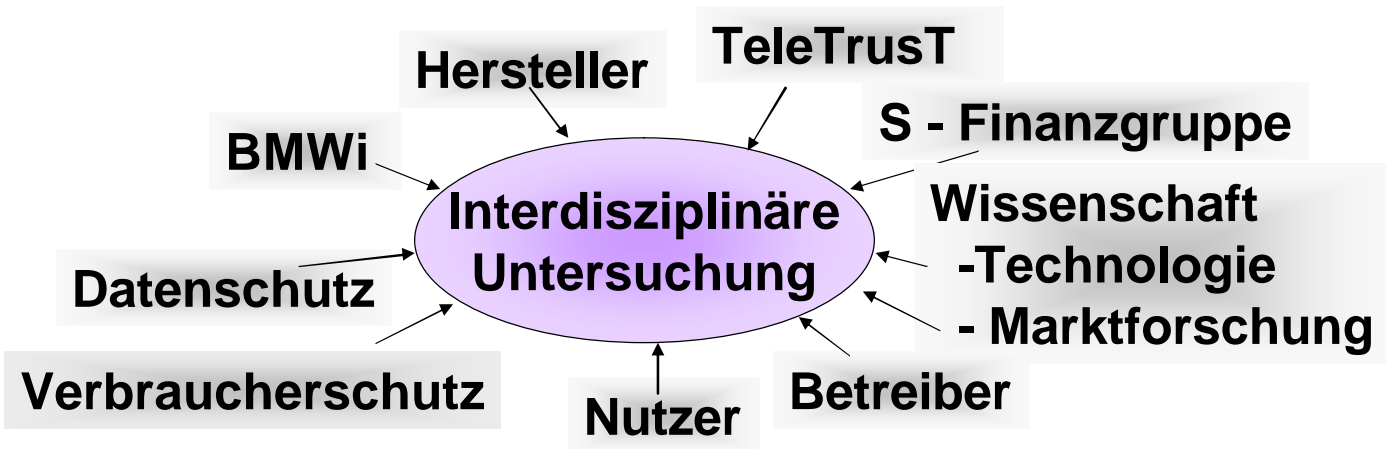




## Die Idee

Viele Hersteller unterschiedlicher biometrischer Verfahren wollen in den Markt

Eine Fülle von offenen Fragen lassen sich nur durch einen Massentest untersuchen





# Partner

- BioTrust Betreiberstellen: 13
- BioTrust Hersteller: 8/15
- BioTrust Forschung, VZBV, ULD, FhG, Consulting, Schnittstellen: 7
- BioTrust Sponsoren: 3

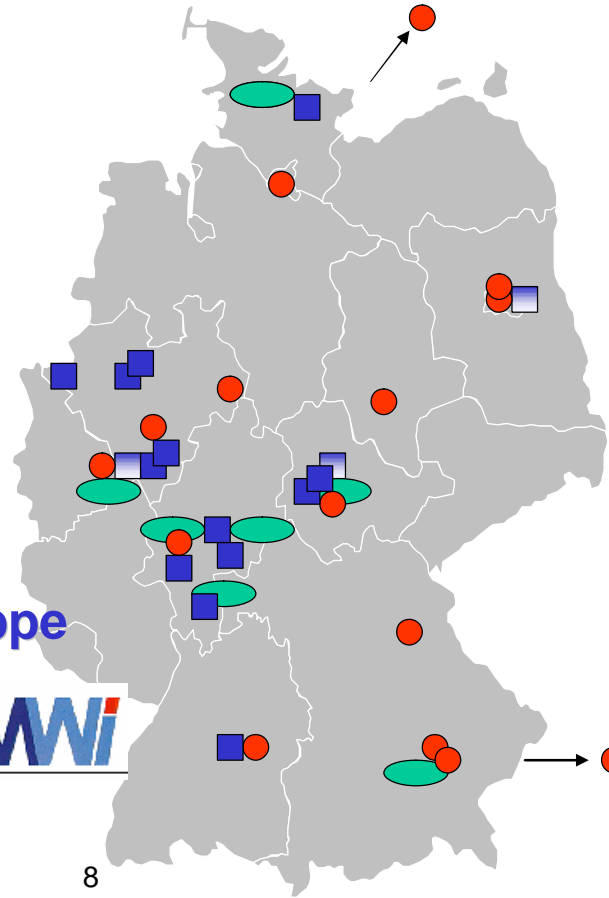


- Finanzgruppe



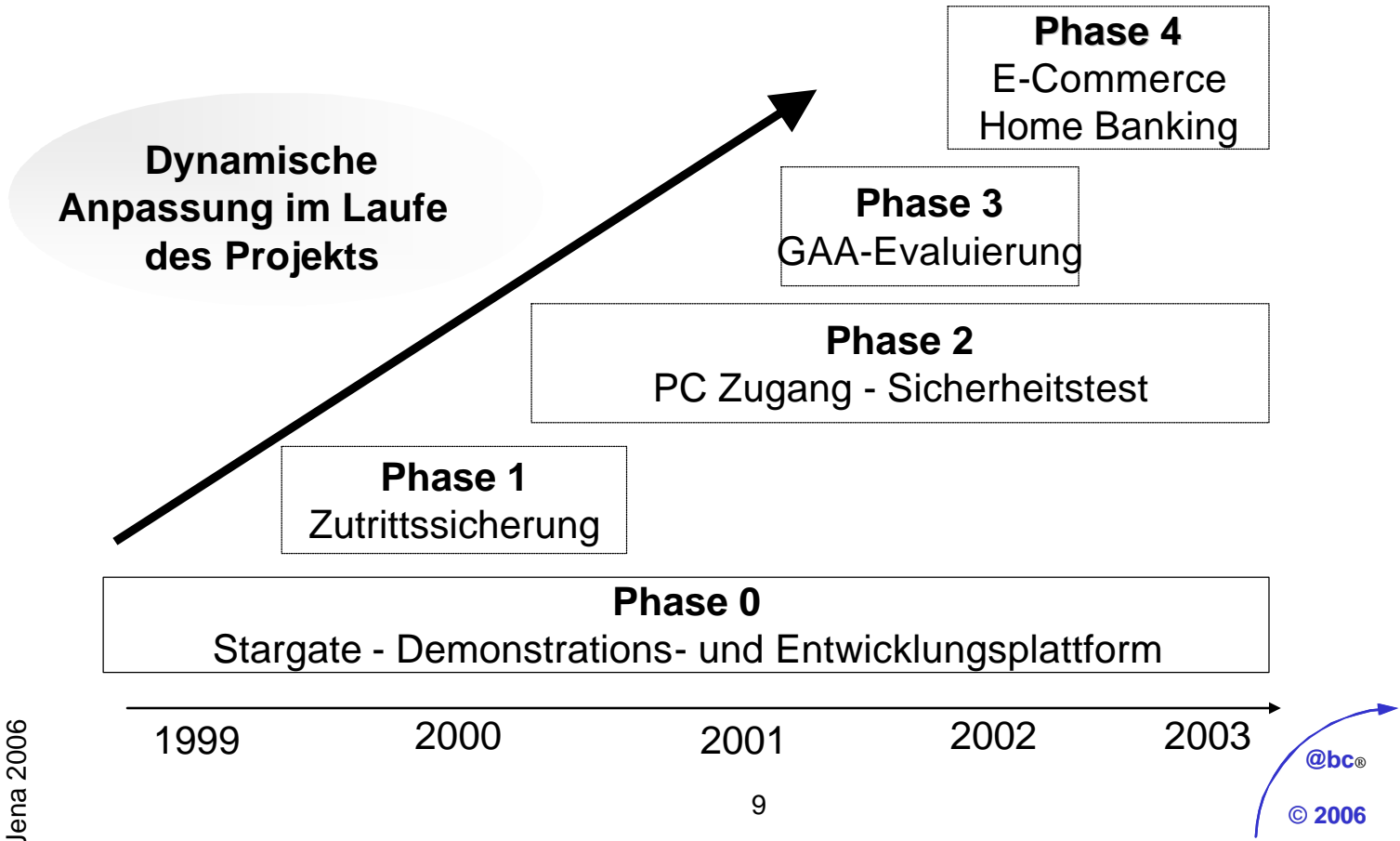
Bundesministerium für Wirtschaft und Technologie

**BMWi**





# BioTrust - Phasen



# Phase 0 “Stargate“

## Demonstrations und Entwicklungsplattform



- ← Licht
- ← Kamera
- ← Nutzerführung
- ← Biometrische Sensoren

### Stargate Plattform

- **Demonstration biometrischer Verfahren**
- **Offen für neue Technologie**
- **Test der Schnittstellen**
- **Entwicklung des Personalisierungsverfahrens**
- **Verfügbar für die gesamte Projektlaufzeit**

Quelle:  
Sparkassen Informatik



**Einzigartige Testumgebung mit ca. 400 Probanden  
und über 75.000 (!) Nutzungen (Stand 10/2002)**

Quelle:  
FH Friedberg

# Phase 1 (Voruntersuchung)

## Zutrittssicherung - Robustheitstest

### Gesichtserkennung

ZN  
Plettac

Informatik Kooperation  
SKW

### Fingererkennung

Atair  
Bergdata  
G&D

SKW  
Informatik Kooperation  
DSV

### Spracherkennung

ABS

FH

### Iriserkennung

SNI

DSV

### Multimodal

DCS

FH



Quelle: Sparkassen Informatik

**Empirische Studie mit wissenschaftlicher Auswertung durch  
Prof. Behrens and Prof. Roth FH Giessen-Friedberg**

### Empfehlungen von

- Verbraucherschutz, VZBV
- Datenschutz, ULD



## Phase 2

### PC Zugang - Sicherheitstest

#### Zielsetzung

- Entwicklung einer Standardschnittstelle (BioAPI)
- Test mehrerer biometrischer Systeme
- Entwicklung eines verteilten Systems zur
- Ermittlung des Nutzerverhaltens
- 3 Test Serien

BioAPI 1.0 Templates on the local PC

BioAPI 1.1 Templates on the local PC

BioAPI 1.1 Templates on a smart card

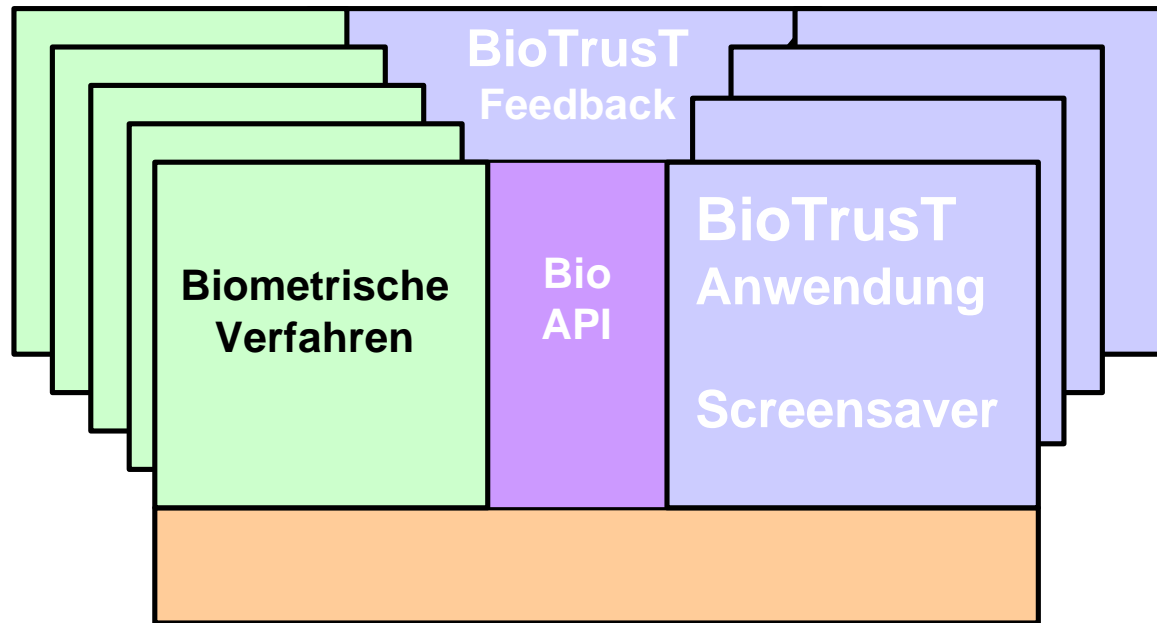
#### BioAPI Implementierung

Fingerabdruck:	Dermalog, Ikendi
Signatur:	Softpro, Wondernet/Dr. Fehr
Iris:	Iridian
Multimode:	BioID
Anwendung:	Omnikey



# Phase 2

## PC Zugang - Sicherheitstest





## Phase 2

### Was wurde bisher erreicht:

**Einsatz internationaler Standardschnittstelle (BioAPI)  
Voraussetzung für größere Ausschreibungen wie z. B. für  
das DOD/USA**

**BioAPI-Anwendung (Screensaver) und Implementierung  
durch Hersteller**

**Kooperatives Testen der (komplexen) Schnittstellen**

**Elektronisches Befragungsverfahren für Benutzer (FH)**

**Einfluss auf die weitere Standardisierung durch BioTrust  
(NIST-Vorschlag, Vortrag IEEE AutoID)**

**Kooperation mit BioAPI-Konsortium und  
International Biometric Industry Association (IBIA)**

**Internationales Interesse für BioTrust (USA, EU)**



# Phase 3

## Einsatz am Geldausgabeautomaten

### Zielsetzung

Ermittlung der Bedingungen für einen zukünftigen Einsatz von biometrischer Identifikation als Ersatz der PIN

- Bankspezifische Aspekte
- Verbraucherschutzaspekte
- Datenschutzaspekte
- Allgemeine Rahmenbedingungen



# Zusammenfassung

## **Gemeinsame Arbeitsgruppen:**

Datenschutz - Verbraucherschutz - Wissenschaft  
Gemeinsame Fragelisten für Benutzer, Hersteller, Betreiber  
Auswertung und Empfehlungen individuell

## **Entwicklung von Analyseverfahren der Sicherheit in Kooperation**

BSI, Dt. Telekom, BKA, BioTrust, .....

## **Workshop Präsentationen und Ergebnisse verfügbar im Internet**

- ◆ <http://biotrust.de/ws020328.htm> (Workshop March 28, 2002)
- ◆ <http://biotrust.de/ws050601.htm> (Workshop June 5, 2001)
- ◆ <http://biotrust.de/wsagenda.htm> (Workshop May 3, 2000)

## **Was haben wir gelernt:**

In jeder Gruppe ist jemand, der bei einem Verfahren nicht erfasst wird  
In jeder Gruppe ist jemand, der bei einem Verfahren nicht wieder erkannt wird  
100% Erkennung nicht möglich - Managemententscheidung wer wird akzeptiert?

Biometrie soll/darf nur mit Zustimmung des Besitzers eingesetzt werden

## Beispiele für biometrische Authentisierung

- Automatische Grenzübertritt für Vielflieger in Amsterdam und im Pilotversuch in Frankfurt (Iris/Iridian/SD-Industries/Byometrics)
- Identifizierung der Jahreskartenabbonnenten in Disney Land + Zoo Hannover (Finger/Identix,Gesicht/ZN)
- Bezahlung durch Fingerabdruck im Restaurant und Einzelhandel (digiPROOF/it-Werke)
- Automatisches Single-Sign-On (BioSlimDisk/Dr. Fehr mit AUTHENTION/digitronic)
- Zutrittssicherung und Wegfahrsperr (Fingerprint, Stimmerkennung)
- Passwort-Reset (Stimmerkennung/VoiceTrust) bei Allianz und IBM CSG
- Dynamische Unterschriftserkennung mit dem PDA (Pocket Signer/Fraunhofer-SIT)

## Wußten Sie, daß

- die meisten Menschen sich nicht mehr als 3 Passwörter bzw. PINs merken können, obwohl erwartet wird, daß sie sich 6 und mehr merken sollten?

Quelle: Hurwitz Group, 2000

- Unternehmen für Passwort Management ca. EUR 200- 300 pro Jahr aufwenden?

Quelle: IDC und Siemens

- ein typischer Benutzer pro Jahr ca. 44 Stunden für Log-On benötigt, um sich bei 4 Anwendungen anzumelden?

Quelle: Studie des Network Application Consortium 1996

# BioSlimDisk™ – der sichere Token



BioSlimDisk Alleinstellungsmerkmale

[www.4trust.de](http://www.4trust.de)

- Patent geschützt
- Gewinnt den NRW IT-Sicherheitspreis 2004
- Authentification von digitronic [www.digitronic.net](http://www.digitronic.net)



# Markterfordernisse für den Einsatz biometrischer Verfahren

## Unterschiedliche Märkte

- ◆ Erhöhte Sicherheit
- ◆ Komfort

## Einsatz im Massenmarkt

- ◆ Signifikanter Vorteil für den Benutzer
- ◆ Pflicht oder Zwang (Verordnung)

## Voraussetzungen

- ◆ Robuste Verfahren
- ◆ Anerkannte Sicherheit
- ◆ Gesellschaftliche Akzeptanz

## Auswahlhilfe

- ◆ Kriterienkatalog der AG6 TeleTrust
- ◆ Download <http://www.teletrust.de/publikat.asp?id=40600>

# Ausblick auf zukünftige Entwicklungen

eine Vision  
für den  
mobilen  
Einsatz  
biometrischer  
Verfahren  
bleibt....



# Ausblick auf zukünftige hoheitliche Entwicklungen

## Reisepass ab 2005 mit Gesicht und ab 2007 mit zwei Fingern

EU-Pässe mit Fingerabdruck und Digitalfoto als biometrische Merkmale

Alle EU-Bürger müssen für einen neuen Reisepass in absehbarer Zeit ihre Fingerabdrücke abgeben. Darauf haben sich die Innenminister der Union in Luxemburg im Grundsatz geeinigt. Wegen Vorbehalten aus Finnland, Österreich und den Niederlanden steht ein formeller Beschluss vorerst aber noch aus.....

Nach dem Beschluss sollen die Pässe einen Speicherchip mit digitalisiertem Foto und Fingerabdrücken erhalten.

Erste Reisepässe mit biometrischen Merkmalen werden in Deutschland seit Herbst 2005 ausgegeben.

Der Bundesbeauftragte für den Datenschutz, Peter Schaar, erneuerte seine Bedenken gegen die Aufnahme biometrischer Merkmale in die Reisepässe: Er warnte vor technischen Kinderkrankheiten und Gefahren für den Datenschutz durch die biometrischen Merkmale.

Der Pass mit biometrischen Merkmalen ist unter anderem eine Voraussetzung dafür, dass EU-Bürger ab Herbst nächsten Jahres weiter ohne Visum in die USA einreisen dürfen. Seit dem 26. Oktober dieses Jahres müssen Reisende aus EU-Ländern einen maschinenlesbaren Pass vorzeigen, um ohne Visum in die USA einreisen zu können. Ab dem 26. Oktober 2005 müssen dann die Pässe von Deutschen und Staatsbürgern aus 26 weiteren so genannten Visa-Waiver-Ländern, die also ohne Visum in die USA einreisen können, zudem biometrische Informationen enthalten.

Quelle: [www.heise.de](http://www.heise.de) 27.10.2004

Später: Dienstausweis -> ID-Karte -> Führerschein?

# Biometrische Grenzkontrolle am Flughafen Frankfurt

Seit Mitte Februar können Passagiere am Flughafen Frankfurt die Grenze übertreten, ohne einem Bundesgrenzschutzbeamten ihren Reisepass vorzeigen zu müssen.



nur vorher registrieren



# Ist Biometrie sicher?

**Sicher ist,  
dass nichts sicher ist,  
selbst das nicht.**

JOACHIM RINGELNATZ

**Blindes Vertrauen  
schenkt man nur  
nach sorgfältigst getroffenen  
Vorsichtsmaßnahmen.**

EMANUEL WERTHEIMER

Jena 2006



  
@bc®  
© 2006

**Vielen Dank für Ihre Aufmerksamkeit**



**www.atbc.de**