

Die geplanten Pässe haben und schaffen ernste Sicherheitsprobleme:

- A. Fingerabdrücke in Pässen fördern Kriminalität mehr,
als sie zu bekämpfen**
- B. Grundsatzüberlegungen zu Biometrie**
- C. Sicherheitsprobleme von und durch RFIDs**

Prof. Dr. Andreas Pfitzmann

TU Dresden, Fakultät Informatik, D-01062 Dresden
Tel.: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, <http://dud.inf.tu-dresden.de/>

23. April 2007

A. Fingerabdrücke in Pässen helfen Kriminellen ...

... und erschweren polizeiliche Ermittlungen – also keine Fingerabdrücke in Pässe!

- Die Aufnahme des biometrischen Merkmals „Fingerabdruck“ in Pässe und seine **Prüfung** werden Menschen daran gewöhnen, ihre **Fingerabdrücke an** von ihnen **nicht kontrollierbaren Geräten abzugeben**.
- Damit werden **Fingerabdrücke** (unabhängig vom Schutz innerhalb der Pässe) **vielen Akteuren zugänglich** – insbesondere auch fremden Geheimdiensten und Kriminellen.
- Digitale Fingerabdrücke können dazu verwendet werden, **Fingeroberflächen nachzubilden** und so **an Tatorten falsche Spuren zu hinterlassen** – sei es um die Ermittlungen durch falsche Fährten zu erschweren (ein lohnendes Ziel für Kriminelle) oder als Agent Anzuwerbende in eine Notsituation zu bringen (ein lohnendes Ziel für fremde Geheimdienste).

B. Grundsatzüberlegungen zu Biometrie

Biometrie – wie einsetzen und wie keinesfalls?

Wie umgehen mit Sicherheitsproblemen von Biometrie und Sicherheits- und Datenschutzproblemen durch Biometrie?

Grundsatzüberlegungen zu Biometrie (Gliederung)

1. Was ist Biometrie?
2. Wozu Biometrie?
 - Authentifizieren vs. Identifizieren
3. Sicherheitsprobleme von Biometrie
 - FMR vs. FNR
4. Sicherheitsprobleme durch Biometrie
 - Entwertung klassischer forensischer Techniken
 - Safety-Problem: Fingerdiebstahl, um Auto stehlen zu können
 - Enttarnbarkeit gewünschter Mehrfachidentitäten
5. Datenschutzprobleme durch Biometrie
 - Sensible persönliche Daten, z.B. Netzhaut-Scan oder Fingerabdruck
 - Auswertung ohne Information des Betroffenen, z.B. Gesichtserkennung
6. Wie einsetzen und wie keinesfalls?
 - Nur zwischen Mensch und seinen Geräten!
7. Ausblick

1. Was ist Biometrie ?

Körper- oder Verhaltensmerkmale werden gemessen,

z.B.:

- Gesicht(sform)
- Temperaturverteilung Gesicht
- Fingerabdruck
- Handgeometrie
- Venen-Muster der Netzhaut
- Muster der Iris
- DNS
- ...
- Dynamik des eigenhändigen Schreibens (u.a. bei Unterschrift)
- Sprechweise
- Gangbewegung
- ...

2. Wozu Biometrie ?

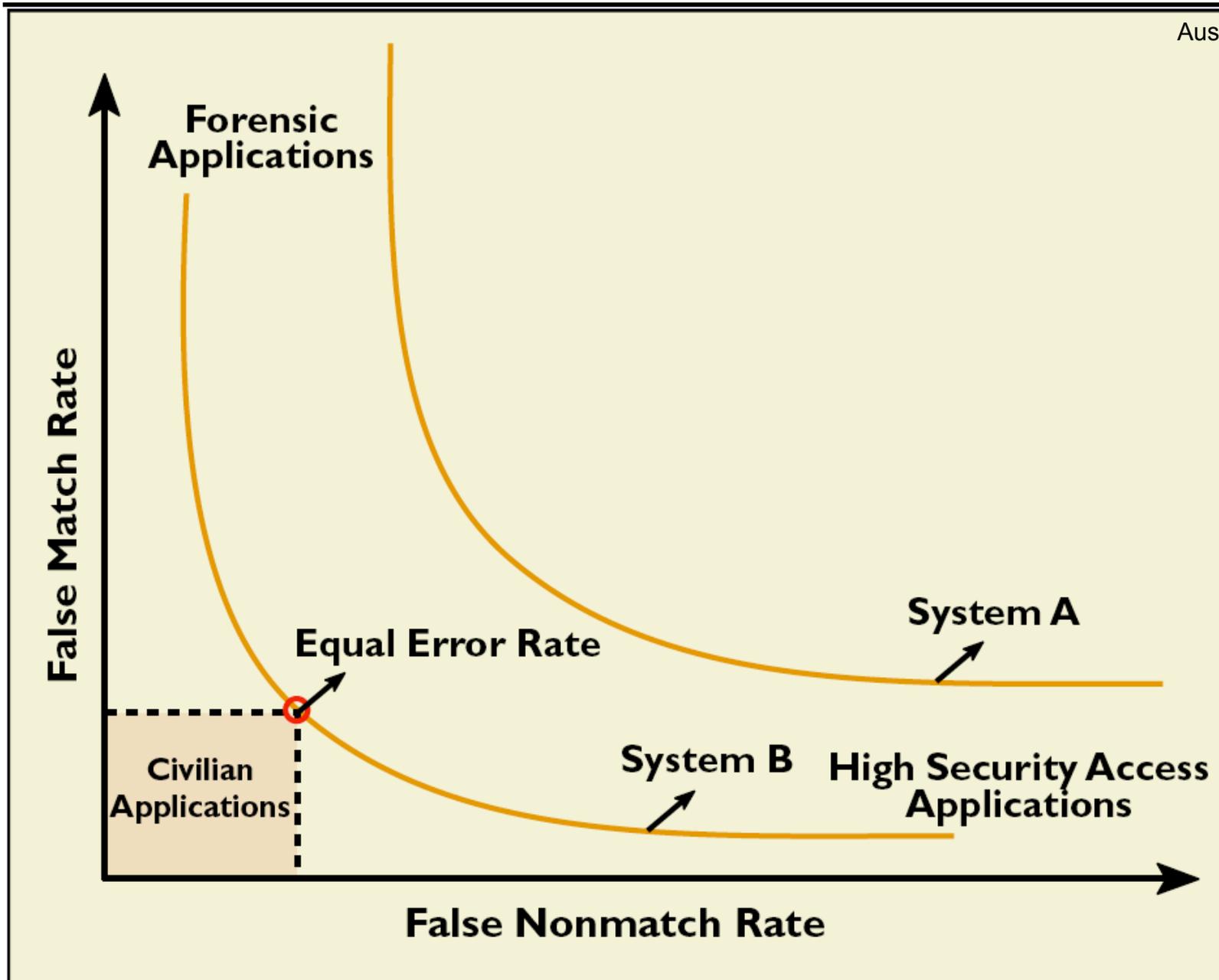
Körper- oder Verhaltensmerkmale werden gemessen, um durch Vergleich mit Referenzwerten Menschen zu

- **Authentifizieren** (Ist dies der, der er behauptet zu sein?)
oder gar zu
- **Identifizieren** (Wer ist das?).

3. Sicherheitsprobleme von Biometrie

Aus: Anil Jain, Lin Hong,
Sharath Pankanti:
Biometric
Identification;
Communications of
the ACM 43/2
(2000) 91-98

**Kleine FMR
bedingt
große FNR
und
umgekehrt !**



4. Sicherheitsprobleme durch Biometrie (1)

- **Entwertung klassischer forensischer Techniken**
 - Beispielsweise **erleichtern Datenbanken mit Fingerabdrücken oder weit verbreitetes „Abgeben“ des eigenen Fingerabdrucks** den Nachbau von „Fingern“ und damit das **Hinterlassen falscher Fingerabdrücke am Tatort** erheblich.
 - Werden mittels Fingerabdruck-Biometrie große Werte gesichert, wird eine **Finger-Nachbau-„Industrie“** entstehen.
 - Da Infrastrukturen z.B. für Grenzkontrollen weniger schnell upgradebar sind als einzelne Maschinen zum Fingernachbau, ist **insgesamt ein Sicherheitsverlust** zu erwarten.
- **Diebstahl von Körperteilen** (Safety-Problem der Biometrie)
 - Bsp.: **Finger abgeschnitten**, um S-Klasse Mercedes zu stehlen.
 - Selbst eine **temporäre** (oder auch nur **vermeintliche**) **Verbesserung** der „Sicherheit“ durch Biometrie ist nicht unbedingt ein Fortschritt, sondern gefährdet die körperliche Unversehrtheit der Betroffenen.
 - Sollte biometrische **Lebenderkennung** funktionieren, dürfte **Entführung oder Erpressung** an die Stelle von Diebstahl von Körperteilen treten.

4. Sicherheitsprobleme durch Biometrie (2)

- **Auch gewünschte Mehrfachidentitäten könnten leichter enttarnbar werden:**
 - **Geheimdienstagenten** – jeder Staat wird personenbezogene Biometriedatenbanken zumindest für alle „fremden“ Staatsbürger anlegen.
 - **Verdeckte Ermittler** und **Personen in Zeugenschutzprogrammen** – insbesondere die organisierte Kriminalität wird personenbezogene Biometriedatenbanken anlegen.

5. Datenschutzprobleme durch Biometrie

- **Sensible persönliche Daten**, z.B.
Netzhaut-Scan liefert u.a. Daten über Alkoholkonsum,
Fingerabdruck möglicherweise über Homosexualität
- Auswertung **ohne Information des Betroffenen**, z.B.
Gesichtserkennung
- **Erfassung mehrerer biometrischer Merkmale**, um die
Unsicherheit einzelner Merkmale zu kompensieren,
vervielfacht das Datenschutzproblem (vgl. Mosaiktheorie
des Datenschutzes).

Datenschutz durch Löschen von Daten funktioniert im Internet nicht, da man *alle* Kopien erwischen müsste. Also muss bereits die Erfassungsmöglichkeit der Daten vermieden werden.

6. Wie einsetzen und wie keinesfalls ? (1)

- Zwischen **Mensch** und **seinen Geräten**
 - Authentifizierung durch Besitz und/oder Wissen *und* Biometrie
 - Keine Entwertung klassischer forensischer Techniken
 - Keine Datenschutzprobleme durch Biometrie
 - Aber: Safety-Problem bleibt bestehen
⇒ ggf. Abschaltmöglichkeit der Biometrie nach erfolgreicher biometrischer Authentifizierung vorsehen
- **Aktive Biometrie** (d.h. Mensch tut etwas explizit) in Pässen und/oder gegenüber „fremden“ Geräten kann und sollte vermieden werden!
- **Passive Biometrie** durch fremde Geräte ist leider kaum zu verhindern.

6. Wie einsetzen und wie keinesfalls ? (2)

- **Visa mit Biometrie** sind bzgl. Datenschutz deutlich weniger gefährlich als **Reisepässe mit Biometrie**.
 - **Fremde Länder** werden versuchen, über Besucher personenbezogene **Biometriedatenbanken** aufzubauen – wir sollten es ihnen weder erleichtern noch durch Maschinenlesbarkeit unserer Reisepässe verbilligen.
 - Die **organisierte Kriminalität** wird versuchen, personenbezogene **Biometriedatenbanken** aufzubauen – wir sollten es ihr nicht erleichtern, indem wir das Abgeben biometrischer Merkmale an „fremden“ Geräten zur Normalität erklären oder gar noch durch unkontrollierte Maschinenlesbarkeit unserer Reisepässe unterstützen (vgl. Unsicherheit der RFID-Chips gegen unautorisiertes Auslesen).
 - **Unterschiedliche Messungen** und damit **unterschiedliche Werte** biometrischer Merkmale eignen sich – da biometrisches Identifizieren bei weitem nicht perfekt klappt – **weniger als Personenkennzeichen** als ein über 10 Jahre konstanter digitaler Referenzwert im Reisepass. Dies gilt natürlich nur, wenn die unterschiedlichen Messergebnisse zumindest nicht immer von einem konstanten Personenkennzeichen wie der Passnummer „begleitet“ werden.

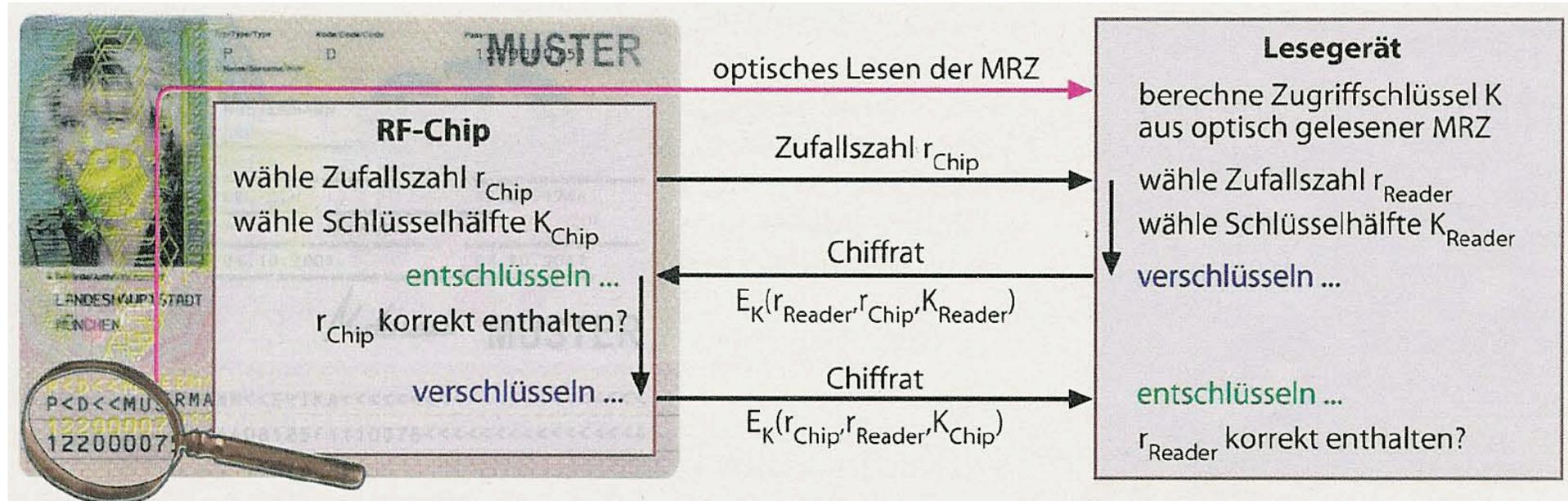
7. Ausblick

- **Balancierung** sollte nicht nur innerhalb einzelner Anwendungen, sondern **über Anwendungen hinweg** erfolgen.
- **Genomdatenbanken** werden möglicherweise die **Sicherheit von Biometrie**, die **ererbte Körpermerkmale** misst, untergraben.
- **Genomdatenbanken** und **Ubiquitous Computing** (= pervasive Computing = Rechner in allen Dingen und deren Vernetzung) werden **Datenschutz in der physischen Welt weitgehend untergraben**.
- **Freiräume in der digitalen Welt sind möglich** (und wohl auch notwendig, Bsp. Jugendgruppe Kirchengemeinde) **und sollten geschaffen werden** – anstatt mit hohen Kosten unsinnige (im Sinne einer Balancierung über Anwendungen hinweg) Vorratsdatenspeicherung anzustreben.

C. Sicherheitsprobleme von und durch RFIDs

- **RFIDs in Reisepässen** (ab Herbst 2005 in Deutschland) **und Personalausweisen** (ab 2008) **unterstützen** nicht nur das Erstellen von Bewegungsprofilen, sondern auch **den Bau von personenspezifischen Bomben**, die genau dann explodieren, wenn ein bestimmter Pass(inhaber) ganz in der Nähe ist.
- Die **Verbesserung von BSI et al. bzgl. der Sicherheit der RFIDs in europäischen Pässen (basic access control)** ändert daran nichts:
Wer immer Zugriff auf den Papierteil hatte (ausstellendes Land; Grenzposten bei Ein- oder Ausreise; Hotels; Händler, die z.B. Mobilfunkverträge verkaufen und dabei eine Papierkopie des Passes erhalten) oder die Kooperation von so jemand, kann das RFID auslesen, wenn immer es in der Nähe ist.

Sicherheit von RFIDs vom BSI et al. ungenügend verbessert



Das Lesegerät muss sich gegenüber dem RF-Chip auf den neuen Ausweisen authentisieren. Dafür benötigt das Lesegerät einen geheimen Zugriffsschlüssel, der sich aus der maschinenlesbaren Zone des Reisepasses berechnet.

Aus:
 Dr. Dennis Kügler:
 Risiko Reisepass?
 Schutz der
 biometrischen Dater
 im RF-Chip; ct
 5/2005, Seite 88

Was bringt PKI für Lesegeräte ?

Lesegerät identifiziert sich gegenüber RFID-Chip (z.B. signiert Challenge und sendet PKI-Zertifikat für seinen Public Key), bevor RFID-Chip irgendetwas Chip-Spezifisches überträgt.

- Wenn PKI nur für Zugriff auf **manche Passdatenfelder** benutzt, bringt PKI bzgl. der Verhinderung von Bewegungsprofilen und personenspezifischen Bomben **wenig bzw. nichts** ([extended access control](#)).
- Wenn ***PKI für jeden Zugriff*** und ***kein Klonen von Lesegeräten möglich*** und ***kein Schurkenstaat beteiligt*** (was wegen der universellen Gültigkeit des Passes praktisch bedeutet: kein Schurkenstaat auf Erden), dann **RFID-Zugriffsproblem gelöst**.
- Sehr wünschenswert: **Anzeige durch Pass** oder (unfälschbar!) durch Lesegerät, ob Biometriemerkmale dem Lesegerät vom Menschen gegeben werden soll.

Resultierende politische Forderungen

- **Biometrie** sollte nicht gepushed, sondern **allenfalls sehr behutsam und umsichtig eingeführt** werden.
- Die Erfassung und Speicherung biometrischer Merkmale **außerhalb des Verfügungsbereichs des Betroffenen** stellt ein **hohes Sicherheits- und Datenschutzrisiko** dar und sollte deshalb möglichst vermieden werden.
- Vor der Aufnahme von maschinenlesbaren biometrischen Merkmalen in **Reisepässe und Personalausweise** ist eine nachvollziehbare **Kosten-/Nutzenanalyse** vorzulegen. Ggf. sind die Biometriepläne zu revidieren.
- **RFIDs in Reisepässen und Personalausweisen gefährden** selbst in den bzgl. Sicherheit vom BSI et al. verbesserten Fassungen ([basic/extended access control](#)) **Leib und Leben ihrer Träger**. RFIDs in Pässen müssen deshalb entweder komplett vermieden oder z.B. durch physische Schirmung des Passes mittels einer entsprechenden Schutzhülle gegen unbemerktes Auslesen geschützt werden.