Biometrische Identifikationssysteme

Sachstandsbericht
Inhalt

Zusammenfassung .................................................................................................................. 3

I. Einleitung ......................................................................................................................... 15

II. Biometrie: Merkmale, Verfahren und Systeme .......................................................... 17
   1. Allgemeines zu biometrischen Verfahren ............................................................ 17
   2. Biometrische Systeme im Einzelnen ..................................................................... 22
      2.1 Fingerbild ........................................................................................................ 22
      2.2 Handgeometrie ............................................................................................ 26
      2.3 Iris ................................................................................................................ 27
      2.4 Retina ............................................................................................................ 30
      2.5 Gesicht ........................................................................................................... 31
      2.6 Unterschrift/Handschrift ............................................................................... 33
      2.7 Stimme .......................................................................................................... 34
      2.8 Kombinationen ............................................................................................. 35
      2.9 Entwicklungslinien im Frühstadium .............................................................. 35
   3. Vorzüge und Nachteile der Systeme im Überblick ............................................... 36

III. Forschungs- und Entwicklungsaktivitäten ................................................................. 41
   1. Pilotprojekte und Entwicklung von Testkriterien .............................................. 42
      1.1 BioIS-Projekt .............................................................................................. 42
      1.2 BioTrusT (TeleTrusT Deutschland e.V.) ..................................................... 46
      1.3 Standardisierung und Evaluierung biometrischer Systeme ....................... 48
   2. FuE-Projekte in Deutschland und international .................................................. 50

IV. Biometrische Verfahren in der Praxis .......................................................................... 61
   1. Anwendungsfelder und -beispiele ....................................................................... 61
      1.1 Benutzerzugangssicherung ......................................................................... 62
      1.2 Personenidentifikation ............................................................................... 63
      1.3 Gerätezugangskontrolle ............................................................................. 66
      1.4 Elektronischer Zugang zu Informationen und Dienstleistungen .................. 67
Inhalt

1.5 Conveniencebereiche ........................................................................................................ 68
1.6 Internetanwendungen und das Problem der Referenzdaten ........................................ 70
2. Markteinschätzung .............................................................................................................. 71

V. Verbraucherpolitik, Recht, Datenschutz ........................................................................... 75
1. Verbraucherpolitische Anforderungen an die Biometrie .............................................. 75
2. Elektronische Signaturen und Biometrie - rechtliche Aspekte ................................ 80
3. Datenschutz ....................................................................................................................... 85
   3.1 Biometrische Daten als personenbezogene Daten .................................................. 86
   3.2 Grundrechtsbezug biometrischer Daten und Verfahren ........................................ 89
   3.3 Folgerungen für rechtliche Regelungen und die Praxis
       biometrischer Verfahren .......................................................................................... 90
4. Das Terrorismusbekämpfungsgesetz ......................................................................... 93

VI. Perspektiven der weiteren Entwicklung - Forschungs- und
Handlungsbedarf .................................................................................................................. 97

Literatur .................................................................................................................................. 105
1. Vergebene Gutachten ........................................................................................................ 105
2. Weitere Literatur ................................................................................................................ 105

Anhang ................................................................................................................................ 109
1. Tabellenverzeichnis ........................................................................................................... 109
2. Abbildungsverzeichnis ...................................................................................................... 109
3. Biometrie und Internet - Projekte und Produkte ............................................................ 110
4. Marktabschätzungen zur Biometrie ............................................................................... 112
Zusammenfassung


Merkmale, Verfahren und Systeme


Konventionelle Systeme können verwendete Passwörter oder PIN-Chipkarte nicht daraufhin überprüfen, ob der Nutzer, der die korrekten Daten liefert, auch deren rechtmäßiger Inhaber ist. Da biometrische Verfahren mit personenge-
Zusammenfassung

**bundenen Merkmalen** (die weder verloren noch vergessen und auch nicht so leicht gestohlen werden können) arbeiten, versprechen sie neue Qualitäts-, Komfort- und Sicherheitsdimensionen bei der Personenaufentferenzierung.

**Leistungsfähigkeit biometrischer Verfahren**


Insbesondere dann, wenn es um einen weit reichenden, große Nutzergruppen - ob freiwillig oder verpflichtend - einbeziehenden Einsatz biometrischer Systeme geht, z.B. im Rahmen der Ausrüstung von Ausweispapieren, müssen höchste Ansprüche an eine substanzierte Evaluation der infrage kommenden Systeme gestellt werden. Eine **regelmäßige Berichterstattung zum Stand der laufenden Pilotprojekte und der** (internationalen) **Standardisierungsbemühungen** wäre als **Basis für die weitere politische Behandlung** des gesamten Themenkomplexes sicherlich nützlich.
Zusammenfassung

FuE-Aktivitäten

Der Stand der Forschung und Entwicklung im Bereich biometrischer Systeme konnte für Deutschland etwas umfassender erhoben werden, ebenso auch die Förderaktivitäten der EU, allenfalls exemplarisch jedoch auf internationaler Ebene. Gerade im nordamerikanischen und asiatischen Raum gibt es eine kaum überschaubare Vielzahl von Aktivitäten im privatwirtschaftlichen und öffentlichen Sektor.

Von besonderem Interesse sind die sog. "Pilotprojekte" zur Evaluierung biometrischer Systeme, die sowohl technische Fragestellungen als auch Verbraucher- und Datenschutzaspekte untersuchen. In Deutschland waren bzw. sind dies insbesondere das u.a. vom BMWi geförderte Projekt BioTrust und das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geförderte BioIS-Projekt (Kap. III.1).


Anwendungen biometrischer Verfahren

Es existiert eine große und ständig wachsende Zahl von Berichten über konkrete Nutzungen in zahlreichen Einsatzfeldern, insbesondere aus den USA, aber auch aus europäischen und asiatischen Ländern. Der Einsatz biometrischer Identifikationssysteme erfolgte bis vor einigen Jahren fast ausschließlich zu Sicherheitszwecken, bevor nach und nach weitere Anwendungsfelder in Unternehmen und Behörden erschlossen wurden. Bisherige und absehbare Einsatzfelder können in fünf Gruppen eingeteilt werden (Kap. IV.1):

– Benutzerzugangssicherung
– Personenidentifikation
Zusammenfassung

- Gerätezugangskontrolle
- elektronischer Zugang zu Dienstleistungen (E-Banking und E-Commerce)
- sonstige "Conveniencebereiche".

Markteinschätzung

Vorliegende ökonomische **Daten und Einschätzungen** zum Einsatz biometrischer Systeme wirken häufig sehr **punktuell und zufällig** (Kap. IV.2). In der Regel sind sie wenig transparent, auf keinen Fall geben sie ein vollständiges Bild. Allerdings ist es **methodisch auch schwierig**, den eigentlichen "biometrischen" Anteil einer Gesamtleistung zu definieren, abzugrenzen und wertmäßig zu beziffern. Auch die Daten der amtlichen Statistiken liefern keine Grundlage, um relevante Kennziffern für biometrische Produkte und Dienstleistungen (Produktionsumfang, Umsätze, Beschäftigte u.ä.) zu erhalten. Darüber hinaus verfolgen die beteiligten Firmen oft eine eher restriktive Informationspolitik. Der Stand der Diffusion, der Umsätze und der Marktanteile (national wie international) bleibt daher äußerst unscharf.


Im Hinblick auf eine mögliche gezieltere Förderung im Bereich Biometrie wären genauere Daten vonnöten. Voraussetzung hierfür wäre allerdings die **Entwicklung von Konzepten und Methoden zur besseren Erfassung relevanten wirtschaftlichen Kennziffern**, differenziert nach eigentlichem biometrischen System, peripheren Geräten sowie Art und Umfang der Anwendung.

Verbraucherschutz

Die weltweiten Forschungs- und Entwicklungsaktivitäten sowie die zunehmend erkennbare Ausweitung von Einsatzfeldern signalisieren die Möglichkeit, dass

Will man die Chancen der Biometrie nutzen und die Risiken beherrschen, so müssen Gestaltung und Anwendung biometrischer Systeme bestimmte Kriterien erfüllen. Dazu zählen vor allem hohe Sicherheit, umfassende Vertrauenswürdigkeit, ausreichende Nutzerfreundlichkeit sowie weitgehende Sozialverträglichkeit (Kap. V.1).

*Sicherheit und Vertrauenswürdigkeit*


Um eine möglichst große Vertrauenswürdigkeit zu erreichen, wird beispielsweise vorgeschlagen, Vertrauensinstanzen einzurichten, die - fachlich kompetent, unabhängig und neutral - ein im Zusammenwirken von Nutzern, Herstellern, Betreibern und Staat vereinbartes Sicherheitsniveau umfassend prüfen und gewährleisten.

Nutzerfreundlichkeit und Sozialverträglichkeit

Ausreichende Nutzerfreundlichkeit biometrischer Verfahren setzt voraus, dass diese robust und alltagstauglich sind, d.h. im massenhaften Gebrauch über lange Zeit zuverlässig funktionieren. Dies ist häufig noch nicht der Fall. Die Sozialverträglichkeit biometrischer Verfahren wird sich zum einen daran erweisen müssen, dass ihre breite Implementierung nicht zur weiteren "digitalen Spaltung" der Gesellschaft beiträgt, zum andern daran, dass kein "Zwang zur Biometrie" entsteht. Aus verbraucherpolitischer Sicht müssten also Vorkehrungen getroffen werden, die gewährleisten, dass kein Nutzer von biometrischen Anwendungen ausgeschlossen wird, z.B. wären (biometrische und herkömmliche) Ausweichverfahren bereitzustellen.

Einschlägige rechtliche Regelungen

Regelungen, die sich ausdrücklich mit dem Einsatz biometrischer Verfahren befassen, lagen in Deutschland bis vor kurzem nur hinsichtlich ihrer Verwendung im Rahmen elektronischer Signaturen vor (Kap. V.2). Im Mai 2001 trat ein neues Signaturgesetz (SigG) in Kraft, im Juli 2001 folgte das "Formgesetz", mit dem die "qualifizierte elektronische Signatur" wie eine handschriftliche Signatur als formgebundene Erklärung anerkannt wird.

Während das Signaturgesetz bewusst technikoffen formuliert ist, wird in der Verordnung zum Gesetz (SigV) ausdrücklich der Einsatz biometrischer Verfahren ermöglicht: In Bezug auf die Sicherung des Signaturschlüssels hat der Signaturschlüssel-Inhaber die Wahl, sich vor der Anwendung des Schlüssels entweder in herkömmlicher Weise durch "Besitz und Wissen" (etwa Karte und Geheimzahl) oder aber "durch Besitz und ein oder mehrere biometrische Merkmale" zu identifizieren. Ergänzend gibt die Verordnung ein bestimmtes Sicherheitsniveau vor: Bei der Anwendung eines biometrischen Verfahrens muss "hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist, und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein" (§ 15 Abs. 1 SigV).

Aus Verbraucherschutzsicht ist diese vergleichende Bezugnahme auf Verfahren nach dem Prinzip von "Besitz und Wissen" schon seit längerem kritisch kommentiert worden. Dabei wird vor allem auf den Umstand hingewiesen, dass die Sicherheit solcher Verfahren heute weithin umstritten ist.

Mit den genannten Regelwerken gibt es in Deutschland einen gesetzlichen Rahmen für den Einsatz biometrischer Verfahren im Zusammenhang mit der

**Datenschutz**

Insofern biometrische Verfahren auf persönliche körperliche Merkmale zurückgreifen, sind Fragen des Datenschutzes berührt (Kap. V.3).


**Grundrechtsbezug der Biometrie**


Das Grundrecht auf informationelle Selbstbestimmung garantiert die Befugnis des Einzelnen, prinzipiell selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Zugleich sind begrenzte staatliche Eingriffe


Systemdatenschutz

Ob und wieweit eine bestimmte Praxis des Einsatzes biometrischer Verfahren datenschutzrechtlichen Vorgaben genügt, hängt grundlegend ab von der Eingriffsintensität. Hier macht das Datenschutzgesetz Vorgaben, die als Richtschnur für möglichst eingriffsarme Verfahren gelten können:

- Grundsätzlich sind Daten offen zu erheben, unmittelbar beim Betroffenen, unter seiner Mitwirkung und mit seiner Unterrichtung bzw. seiner Kenntnis u.a. bezüglich der Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung (§ 4 Abs. 2 u. 3 BDSG). Unter diesem Gesichtspunkt sind Verfahren, die einen hohen Grad der Mitwirkung bezüglich der Erfassung der Rohdaten verlangen, solchen, die weniger beteiligen oder gar unbemerkt arbeiten, vorzuziehen.

- Gefordert ist, unter dem Stichwort "Datenvermeidung und Datensparsamkeit", schon bei der Auswahl und Gestaltung eines Datenverarbeitungssystems darauf zu achten, dass keine bzw. möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden (§ 3a BDSG).
• Anzustreben ist ferner, zum Zwecke des Datenschutzes, von den Möglichkeiten der **Anonymisierung und Pseudonymisierung** Gebrauch zu machen (§ 3a BDSG).


**Neuere rechtliche Entwicklungen**


Im **Aussländergesetz** wird ebenfalls die Nutzung biometrischer Merkmale in der o.g. Art und Weise als Möglichkeit eröffnet: Einzelheiten bestimmt das Bundesministerium des Innern durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf.

Mit dem "Terrorismusbekämpfungsgesetz" hat der Gesetzgeber **eine parlamentsgesetzliche Grundlage** geschaffen, aus der (auch für den Bürger) Voraussetzungen, Ziel und Umfang des Eingriffes in das Recht auf informationelle Selbstbestimmung klar hervorgehen:

– Die zu nutzenden biometrischen Merkmale werden alternativ explizit genannt.
– Der Zweck der gespeicherten Daten ist ausdrücklich bestimmt.
Zusammenfassung


Perspektiven der weiteren Entwicklung


Die geltenden rechtlichen Rahmenbedingungen (insbesondere das Signaturetgesetz und die Signaturenverordnung) eröffnen der Biometrie im Bereich elektronisch getätigter Transaktionen und Rechtsgeschäfte einen riesigen Markt. Durch das "Terrorismusbekämpfungsgesetz" ist die Tür zum Markt der Sicherheitstechnologien weiter geöffnet worden. Sollte in Deutschland (und Europa) durch staatliche Verfahren ein Masseneinsatz von biometrischen Systemen angesprochen werden, so würde dies voraussichtlich Signalwirkungen für andere Anwendungsfelder in der Wirtschaft und im privaten Bereich haben. Von Verbraucherverbänden und Datenschützern ist die Biometrie zwar stets kritisch, zugleich aber auch positiv bewertet worden: Das Potenzial der Biometrie als verbraucher- und datenschutzfreundliche Technologie wird herausgestritten - allerdings verbunden mit der Aufforderung an Entwickler und Anwender, für technische und organisatorische Lösungen zu sorgen, die den Kriterien eines fortgeschrittenen Daten- und Verbraucherschutzes genügen.
Forschungs- und Handlungsbedarf


I. Einleitung

Im Juni 2000 wurde das TAB durch den Ausschuss für Bildung, Forschung und Technikfolgenabschätzung beauftragt, vorbereitende Untersuchungen zum Thema "biometrische Systeme" in Angriff zu nehmen. Als besonders relevante Fragestellungen wurden

– Diffusionsperspektiven,
– Verlässlichkeit und Manipulationssicherheit,
– Datenschutz und informationelle Selbstbestimmung,
– Verbraucherschutz, Rechtsfragen und die Rolle der Politik


Eine wichtige Informationsgrundlage für den Bericht des TAB bildeten folgende fünf Gutachten:
I. Einleitung

- Stand der verbraucherpolitischen Diskussion zu biometrischen Erkennungsverfahren unter Berücksichtigung der Situation in den USA (Astrid Albrecht; Arbeitsgemeinschaft der Verbraucherverbände [AgV] e.V.), Bonn 2001
- Biometrische Identifikationssysteme: Auf dem Weg vom Labor zum Markt. Eine Bestandsaufnahme - unter Berücksichtigung der USA (Michael Behrens, Richard Roth; TransMIT-Zentrum, Institut für biometrische Identifikationssysteme), Gießen 2001
- Biometrische Systeme - FuE, Diffusionstendenzen und Anwendung. Kommentar- und Ergänzungsgutachten (Jana Dittmann, Astrid Mayerhöfer, Claus Vielhauer; Platanista GmbH), Darmstadt 2001
- Einsatz biometrischer Systeme zur Erhöhung der Sicherheit im Internet - Kurzexpertise (Jana Dittmann, Astrid Mayerhöfer, Claus Vielhauer; Platanista GmbH), Darmstadt 2001


II. Biometrie: Merkmale, Verfahren und Systeme


Biometrie soll dabei neue Qualitäts-, Komfort- und Sicherheitsdimensionen bei der Personenausweisung erschließen und wird häufig als alternativlose Technologie beschrieben, ohne deren Nutzung eine wirklich umfassende Ausdehnung des elektronischen Handels für Endverbraucher nicht vorstellbar erscheint (beispielhaft: Nolde/Leger 2002).

1. Allgemeines zu biometrischen Verfahren

Prinzipielle Anforderungen an Merkmale und Verfahren

Merkmale des Menschen, ob physiologische (passive) oder verhaltensabhängige (aktive), müssten folgende vier Eigenschaften aufweisen, um "biometrisch
II. Biometrie: Merkmale, Verfahren und Systeme


- **Universalität** (bei jedem Menschen vorhanden),
- **Einzigartigkeit** (bei jedem Menschen verschieden),
- **Beständigkeit** (ohne Veränderungen über die Zeit) und
- **Erfassbarkeit** (durch ein technisches System quantitativ messbar).

Tab. 1: Derzeit vorrangig genutzte "biometrische Merkmale" des Menschen

<table>
<thead>
<tr>
<th>erfasstes Merkmal</th>
<th>gemessene Charakteristik</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>physiologisch (passiv)</strong></td>
<td></td>
</tr>
<tr>
<td>Fingerbild (Muster der Hautleisten auf der Fingerkuppe)</td>
<td>Verzweigungs- und Endpunkte der Fingerlinien (&quot;Minuzien&quot;)</td>
</tr>
<tr>
<td>Handgeometrie</td>
<td>Länge, Dicke und Abstand der Finger, Profil der Hand, evtl. Venenmuster</td>
</tr>
<tr>
<td>Iris</td>
<td>Muster des Gewebes um die Pupille</td>
</tr>
<tr>
<td>Retina</td>
<td>Muster der Blutgefäße im Augenhintergrund</td>
</tr>
<tr>
<td>Gesicht</td>
<td>typische geometrische Merkmale des Gesichts (Augen, Kinn, Nase, Mund)</td>
</tr>
<tr>
<td><strong>verhaltensabhängig (aktiv)</strong></td>
<td></td>
</tr>
<tr>
<td>Unterschrift (Schreibdynamik)</td>
<td>Schriftbild &amp; Schriftzug, Geschwindigkeit, Druck, Beschleunigung</td>
</tr>
<tr>
<td>Handschrift (Schriftsemantik)</td>
<td>(wie Unterschrift, plus:) Syntax des Schriftbildes</td>
</tr>
<tr>
<td>Stimme</td>
<td>akustisches Spektrum (teils vorgegebene Wörter)</td>
</tr>
<tr>
<td><strong>multimodale/hybride Systeme</strong></td>
<td></td>
</tr>
<tr>
<td>z.B. Gesicht-Mimik-Stimme</td>
<td>akustisches Spektrum und Lippenbewegung</td>
</tr>
</tbody>
</table>

Quelle: Behrens/Roth 2001, S. 4; Platanista 2001a

Die biometrischen **Verfahren** bzw. Systeme wiederum müssen eine Reihe von **Kriterien der Praxistauglichkeit** erfüllen, u.a. (Behrens/Roth 2001, S. 3; Scheuermann et al. 2000, nach Platanista 2001a)

- technische Umsetzbarkeit (Schnelligkeit, Kompatibilität),
1. Allgemeines zu biometrischen Verfahren

– Robustheit (Wartungsaufwand), Empfindlichkeit (Genauigkeit) und Überwindungsresistenz (Sicherheit),
– ökonomische Machbarkeit (vertretbare Kosten für Betreiber) sowie
– Nutzerfreundlichkeit (Zuverlässigkeit, Einfachheit/Komfort, Hygiene/Gesundheit).

Wie im Weiteren gezeigt wird, genügt keines der derzeit genutzten "biometrischen Merkmale" (Tab. 1) bzw. keines der verfügbaren Systeme allen genannten Anforderungen vollständig, zum Teil aus praktischen, zum Teil aus prinzipiellen Gründen. Dennoch sind weltweit zahlreiche Systeme in unterschiedlichen Anwendungskontexten in Betrieb (Kap. IV.1). Ökonomisch bislang am erfolgreichsten sind die Erkennung von Fingerbild, Handgeometrie, Gesicht, Stimme, Iris und Unterschrift/Handschrift (Kap. IV.2).

**Grundlegende Begriffe: Enrolment - Template - Verifikation - Identifikation**

Basis eines jeden biometrischen Verfahrens ist - unabhängig von dem genutzten Merkmal und der angewandten Technik - das so genannte **Enrolment**. Es umfasst das erstmalige Erfassen und (Ver-)Messen des biometrischen Merkmals der zukünftigen Nutzer, die Umwandlung der "Rohdaten" in einen Referenzdatensatz und die Speicherung desselben, des sog. **Templates**. Dieses stellt den Vergleichswert dar, mit dem bei allen darauf folgenden biometrischen Überprüfungen die neuen Messdaten (zumindest zu einem hohen Grad) überestimmen müssen, um den Nutzer identifizieren zu können (s.u.).

An diesen grundlegenden Vorgang des Enrollments müssen folglich sowohl höchste technische Anforderungen (bzgl. Empfindlichkeit und Genauigkeit, damit tatsächlich individuelle, aber auch reproduzierbare Datensätze entstehen) als auch höchste Sicherheitsanforderungen gestellt werden. Der Hauptzweck der Anwendung biometrischer Verfahren, d.i. die Erhöhung der Sicherheit eines Gesamtsystems (z.B. der Geldausgabe am Automaten), kann nur dann erreicht werden, wenn der Referenzdatensatz, das Template, dauerhaft geschützt gespeichert werden kann. Insbesondere im Hinblick auf zukünftige großflächige Einsätze sind noch viele Fragen offen (z.B. welche und wie viele Personen entsprechend qualifiziert werden müssen, um das Enrolment durchzuführen), deren Lösung aller Voraussicht nach mit hohem finanziellen und organisatorischen Aufwand verbunden sein wird (Platanista 2001a; vgl. Kap. IV.1.6).

Bei einer biometrischen Überprüfung der Nutzer werden zwei "Betriebsarten" unterschieden (Behrens/Roth 2001, S. 2):
II. Biometrie: Merkmale, Verfahren und Systeme

- die biometrische **Verifikation**, d.h. die Bestätigung der behaupteten Identität des Individuums (1:1 = die vermessene Person ist tatsächlich die, die sie zu sein behauptet), und
- die biometrische **Identifikation**, d.h. die Erkennung eines Individuums aus einer (definierten) Menge biometrisch registrierter Personen (1:n = die vermessene Person ist XY).

Im Fall der **Verifikation** werden die aktuellen Messdaten verglichen mit den vorhandenen Daten der Einzelperson, die z.B. auf einer Chipkarte oder einem PDA (= Personal Digital Assistant) dezentral (im Besitz der Person) abgelegt sind oder aber, verbunden mit einer vorgegebenen Benutzerkennung, zentral gespeichert sein können. Im Rahmen des Enrolments - z.B. bei einem großflächigen Einsatz für Bankautomaten - wird es oftmals nötig sein, zumindest vorübergehend die biometrischen Daten an einer weiteren zentralen Stelle abzuspeichern, um sie auf die Chipkarte für den entsprechenden Benutzer zu laden ("Personalisierung der Chipkarten"). Dem Vorteil aus der Sicht des Datenschutzes, dass sich bei einer dezentralen Verifikation das Template in der Verfügungsgewalt der Nutzer befindet, stehen Sicherheitsnachteile und damit verbundene mögliche Haftungsprobleme durch Verlust oder Beschädigung gegenüber (Platanista 2001a; vgl. Kap. V.2).

Im Fall der **Identifikation** vergleicht das biometrische System die gemessenen Daten mit den - zentral gespeicherten - Daten aller zuvor Registrierten und prüft, welches Template am besten mit dem des aktuellen Nutzers übereinstimmt. Dadurch entstehen höhere Anforderungen hinsichtlich der benötigten Datenbankgröße und Identifikationszeit. Diese Art der biometrischen Erkennung wird derzeit vor allem in Hochsicherheitsbereichen mit einer geringen Anwenderanzahl oder zu polizeilichen Ermittlungszwecken eingesetzt (Platanista 2001a).

Probleme in der Praxis: Falsche Akzeptanz und falsche Zurückweisung

Idealerweise wäre jeder gewonnene biometrische Datensatz einzigartig für ein menschliches Individuum und diesem eindeutig zuzuordnen - ursprünglich erhobene Referenzdaten (Template) und jeweils gemessener Datensatz wären identisch. In der Praxis resultieren Einschränkungen dieser idealen Einzigartigkeit, Genauigkeit und Reproduzierbarkeit aus verschiedenen Gründen:

– Jeder Messvorgang bedeutet eine starke Informationsreduktion. Aus prinzipiellen (Kapazitäts-)Gründen muss die erhobene Datenmenge begrenzt werden. Hinzu kommt die jeweilige Messgrenze (Empfindlichkeit) und Genauigkeit des Sensors bzw. des Gesamtsystems sowie das nicht zu vermeidende "Rauschen". Die zu speichernde Datenmenge des Templates sollte aus technischen Gründen (Speichergröße, Übertragungsrate) weitestgehend minimiert werden, wodurch aber die Genauigkeit reduziert wird.


– Hinzu kommen störende Umwelteinwirkungen während der Messung, z.B. unterschiedliche Lichtverhältnisse oder Temperaturveränderungen, welche die Leistungsfähigkeit von Sensoren beeinflussen können (Platanista 2001a).

**II. Biometrie: Merkmale, Verfahren und Systeme**

**FAR = False Acceptance Rate** können nicht theoretisch berechnet werden, sondern müssen empirisch ermittelt werden.

FAR und FRR beeinflussen sich dergestalt, dass eine Absenkung der fälschlichen Akzeptanz die falsche Zurückweisung erhöht und umgekehrt. Die **absolute Höhe der Fehlerraten** ist allerdings abhängig von der Empfindlichkeit und Genauigkeit, also der Trennschärfe, des Gesamtsystems und wird daher von der Wahl der o.g. Toleranzschwelle direkt beeinflusst. Weniger präzise Systeme wie die Stimmerkennung werden entweder viele Nutzer fälschlicherweise akzeptieren (bei niedrig eingestellter Toleranzschwelle) oder aber fälschlicherweise zurückweisen. Der Iris-Scan hingegen weist aufgrund seiner großen Trennschärfe sowohl eine niedrige FAR als auch eine niedrige FRR auf. Je nach praktischer Anwendung soll durch die Wahl und Einstellung der Toleranzschwelle des Systems die Rate falscher Ablehnung minimiert werden (meist aus Komfortgründen, d.h. Vermeidung frustrierender Fehlversuche) oder aber die Rate falscher Akzeptanz (vor allem im Hinblick auf eine Sicherheitserhöhung) (Kap. IV.1.5). FAR und FRR gelten als mit den wichtigsten Kenngrößen für die Leistungsfähigkeit eines biometrischen Systems. Bei Gleichheit der Werte spricht man von "EER" = "Equal Error Rate".

Ein selbst in Testszenarien bislang selten behandelter, für die Praxis aber sehr wichtiger weiterer Parameter ist die Rate fehlerhafter Registrierungs- bzw. Enrolmentversuche (**FER = False Enrolment Rate**), die großen Einfluss auf die Nutzerakzeptanz ausüben kann (Vielhauer 2000).

2. **Biometrische Systeme im Einzelnen**

Die folgenden (Kurz-)Beschreibungen der biometrischen Merkmale und Systeme behandeln physiologische, technische, ökonomische und Nutzeraspekte. Eine Gegenüberstellung der Eigenschaften und Kenngrößen der Verfahren (FAR und FRR, Registrierungs- und Verifikationszeit, Templategröße), ihrer Stärken und Schwächen wird in Kapitel II.3 vorgenommen.

2.1 **Fingerbild**

Die Fingerbilder jedes Menschen gelten als völlig einzigartig. Selbst eineiige Zwillinge können anhand der Fingerabdrücke unterschieden werden. Zur Unterscheidung werden entweder das gesamte Graubild ("Pattern Matching") oder die

Bei der kriminaltechnischen (forensischen) Verarbeitung der Fingerabdrücke geht es im Unterschied zu den biometrischen Fingerbild-Erkennungen um die Erfassung der Gesamtbilder, vor allem zu Vergleichszwecken. Das bedeutet, dass die von den Scannern erfassten Bilder als hochwertige Schwarz-Weiß-Bilder mit z.B. 250 KByte (pro Finger!) gespeichert werden, während für die biometrische Identifikation Datensätze verwendet werden, die um den Faktor 250 bis 1.000 kleiner sind und sich auf die zur Unterscheidung benötigten Merkmale reduzieren. Daher kann bei einer biometrischen Identifikation der Fingerabdruck aus den gespeicherten Daten nicht eindeutig rekonstruiert werden, was eine Verwendung vor Gericht kaum möglich macht (Behrens/Roth 2001, S. 10).

Abbildung 1 demonstriert die Gewinnung der biometrischen Fingerbildinformation, des sog. Minuzienbildes. Die einzelnen Schritte sind (Behrens/Roth 2001, S. 8):

– Gewinnung des Original-Graustufenbildes des Fingers (a)
– Berechnung des Richtungsfeldes aus dem Originalbild (b)
– Extraktion des Vordergrundanteils (c)
– Herausfilterung des Hintergrundes (d)
– Berechnung des Skelettes mit den markierten Minuzien (e)
– Überlagerung der Minuzien mit dem Original-Graustufenbild (f)

Derzeit sind drei Technologien im Gebrauch bzw. in der Erprobung: optische Sensoren, Halbleiterlösungen und Ultraschall (Behrens/Roth 2001, S. 6 f.).
II. Biometrie: Merkmale, Verfahren und Systeme

Abb. 1: Gewinnung des Minuzienbildes bei der Fingerbilderkennung

Quelle: Behrens/Roth 2001, S. 9, nach GMD/Infineon Technologie AG

• Immer wichtiger wird die **Halbleiterlösung** (kapazitative Sensoren). Seit einiger Zeit sind Chips verfügbar, die mittels Messung der Gleichstromkapazität zwischen der Chipoberfläche und der Fingeroberfläche digitale Graustufenbilder mit 200 bis 300 Linien - bei einer nutzbaren Fläche von ca. 10 x 15 mm bis max. 13 x 18 mm - mit 8 Bit Auflösung erzielen (Infineon, Sony, ST-Microelectronics, Veridicom). Ein System (des Herstellers Authentec) kann durch eine modifizierte Kapazitätsmessung auch die lebende Schicht des Fingers unter der Oberfläche vermessen, was theoretisch deutliche Vorteile hat, da sich zum Beispiel Verletzungen weniger auswirken. Mit latenten Fingerabdrücken aus der vorhergehenden Benutzung kämpfen allerdings auch viele der Halbleiterlösungen, und wie haltbar und zuverlässig sie sind, ist noch offen. Die Angaben der Hersteller sind viel versprechend, indem sie eine hundertfach bessere Haltbarkeit als bei den optischen Systemen behaupten. Charakteristisch ist eine, durch die relativ kleine Aufnahmefläche bedingte, sehr große Abhängigkeit der Gesamtqualität der Erkennung von der Qualität des Enrolments. Der Benutzer muss immer die gleiche Teilfläche des Fingers wie beim Enrolment benutzen, was eine unrealistische Disziplin des Nutzers erfordert, der oft schon Schwierigkeiten hat, sich daran zu erinnern, welchen Finger er beim Enrolment benutzt hat. Chips zur Fingerbilderfassung werden zukünftig weitaus preiswerter sein und vermutlich immer häufiger eingesetzt werden. Schon jetzt sind sie in Smartcards integriert verfügbar.

• Große Hoffnung wird auf die Verwendung von **Ultraschalltechnologie** gesetzt, wenn auch nur wenige Geräte bisher Marktreife erreicht haben.
II. Biometrie: Merkmale, Verfahren und Systeme


2.2 Handgeometrie


Die Bedienung der Systeme ist einfach, teilweise aber unbequem (wenn z.B. für die richtige Positionierung die Hand fest an starre Anschlagstifte gedrückt werden muss, Abb. 2). Da aufgrund der Dickenmessung dreidimensionale Aufnahmen benötigt werden, sind komplizierte Optiken erforderlich. Die Sensor-technik und mit ihr das Gesamtsystem ist daher meist recht voluminös, so dass die Technik bislang überwiegend bei der räumlichen Zugangskontrolle oder zur Zeiterfassung eingesetzt wurde. Die Templategröße ist mit 10-20 Bytes klein, Angaben zur erzielbaren Genauigkeit schwanken (mittel bis hoch) (Beh-
2. Biometrische Systeme im Einzelnen


Abb. 2: Erfassen der Handgeometrie

Quelle: Michigan State University (http://biometrics.cse.msu.edu/hand,proto.html), nach Behrens/Roth 2001, S. 12

2.3 Iris


Die Einzigartigkeit von Irismustern ist unbestritten. Sie gilt nicht nur für eineiige Zwillinge, sondern sogar für die zwei Augen einer Person. Veränderungen über die Zeit werden als vernachlässigbar eingestuft. Allerdings können Krankheiten des Auges, z.B. Schädigungen der Hornhaut, zu deutlichen Verän-
2. Biometrische Systeme im Einzelnen

Abb. 4: Iris mit Iris-Code


II. Biometrie: Merkmale, Verfahren und Systeme

2.4 Retina

Wie das Fleckenmuster der Iris gilt auch die Anordnung der Blutgefäße in bzw. hinter der Netzhaut oder Retina, also dem lichtempfindlichen Bereich im Augeninneren, als individuell einzigartig (auch bei Zwillingen). Ebenfalls wie das Irismuster bleibt das Adernmuster der Netzhaut weitgehend konstant, kann sich aber durch Krankheiten oder Verletzungen vorübergehend oder andauernd verändern.

Abb. 5: Infrarot-belichtete Retina

[Image: Infrarot-belichtete Retina]


Seit 1985 gibt es (mit dem EyeDentify 7.5) ein Gerät, das mittels Infrarot-Laser die Blutgefäße der Netzhaut scannt. Dabei werden etwa 400 charakteristische Punkte festgehalten (Abb. 5). Relativ aufwendige Spezialtechnik ist erforderlich, um durch die Pupille hindurch die Netzhaut aufzunehmen. Das Auge muss sich sehr nahe an der Aufnahmeoptik befinden (1-2 cm) und während des Scannens ruhig gehalten werden. Der Nutzer blickt dann auf ein rotierendes grünes Licht, während das tatsächlich zum Abtasten benutzte Infrarotlicht für
ihn unsichtbar ist. Die Templates sind mit 40-96 Bytes mittelgroß. Die Zeit für eine Messung beträgt ca. 1,5 Sekunden (Behrens/Roth 2001, S. 17 f.).


2.5 Gesicht


Eigenschaftsanalyse (Feature analysis) ist das wohl verbreitetste System zur Gesichtserkennung. Gegenüber dem Eigengesicht-Verfahren gilt die Methode als vielseitiger, da sie Variationen der Mimik, etwa beim Sprechen oder Lächeln, akzeptiert (Behrens/Roth 2001, S. 21).
Neben diesen beiden dominanten Systemen gibt es eine Reihe weiterer Varianten, die als Neural Network Mapping Technology oder Automatic Face Processing bezeichnet werden, ferner erste Versuche zur Nutzung anderer Parameter, wie dreidimensionales Scannen oder das Erfassen der Wärmeverteilung im Gesicht (Abb. 7) (Behrens/Roth 2001, S. 21 f.).

Äußere Einflüsse, z.B. unterschiedliche Lichtverhältnisse oder Temperaturschwankungen, beeinflussen die Funktionalität der Gesichtserkennung. Ohne Lebenderkennung (z.B. durch Registrierung intrinsischer Mund- oder Augenbewegungen) ist die Überwindung der Systeme äußerst einfach - meist genügen bereits Fotos oder Videos (Breitenstein 2002, S. 45). Vor allem bei Kindern und Jugendlichen, aber auch in späteren Lebensphasen verändert sich das Merkmal relativ stark (Platanista 2001a). Die Templategröße beträgt bis zu 1.300 Bytes.
2. Biometrische Systeme im Einzelnen

Abb. 7: Thermogramm eines Gesichts

Quelle: Michigan State University (http://biometrics.cse.msu.edu/), nach Behrens/Roth 2001, S. 22

Je nach Anwendungszweck und Perspektive (z.B. Komfort vs. Datenschutz) erscheinen zwei Charakteristika der Gesichtserkennung als Vor- oder Nachteil: die Passivität der Nutzer (keine aktive Mitwirkung erforderlich) und die mögliche Kontinuität gegenüber einem Nutzer (permanente Überprüfung der Zugangsberechtigung z.B. während der Benutzung eines PCs).

2.6 Unterschrift/Handschrift

Bei der Unterschrifts- bzw. Handschriftenerkennung ist nicht nur das optische Erscheinungsbild der Signatur (Schriftzug als "Offline-Parameter") entscheidend, sondern es werden Merkmale wie Druck, Geschwindigkeit, Beschleunigung, Auf- und Absetzpunkte sowie Stiftwinkelpositionen beim Schreiben (als "Online-Parameter") gemessen. Aufgenommen wird die Unter/Handschrift heute meistens mit einem handelsüblichen Grafiktablett oder einem PDA bzw. Touchscreen. Alternativ sind auch Spezialstifte mit Sensoren in Verwendung, welche die Parameter bei der Leistung der Unterschrift/Handschrift aufnehmen und zur Auswertung übertragen (Behrens/Roth 2001, S. 22 f.).

Eine Erweiterung der Unterschriftanalyse liefert ein Handschriftensystem, bei welchem nicht allein die Unterschrift, sondern sog. "Semantiken" (Vielhauer 2000) zur handschriftlichen Authentifizierung herangezogen werden. Dies können vordefinierte Wörter, ganze Sätze oder sogar kleine Zeichnungen
II. Biometrie: Merkmale, Verfahren und Systeme


Abb. 8: Online-Handschriften ("Haus von Nikolaus" und vorgegebener Schriftzug)

Quelle: Vielhauer 2000

2.7 Stimme

nikation ein interessantes Anwendungsspektrum, da hier keine zusätzlichen Hardwarekosten für die Nutzer entstehen.

### 2.8 Kombinationen


### 2.9 Entwicklungslinien im Frühstadium


- **Geruchssidentifikation:** Mit "künstlichen Nasen" könnte in Zukunft das einzigartige Geruchsmuster flüchtiger chemischer Substanzen des menschlichen Körpers erfasst und ausgewertet werden. Eine britische Firma, Mastiff Electronic Systems Ltd., arbeitet an einem solchen System mit Namen "Scentinel".
- **DNA-Analyse:** Angesichts der Fortschritte in der DNA-Chip-Technologie ist eine vollautomatisierte DNA-Analyse technisch durchaus vorstellbar. Diese Automatisierung wird in Anwendungsfeldern wie der Medizin oder
II. Biometrie: Merkmale, Verfahren und Systeme

auch der Lebensmittelanalytik intensiv vorangetrieben, und eine Umsetzung in biometrische Systeme dürfte auf längere Sicht technisch kein großes Problem darstellen. Wegen der allseits anerkannten Sensibilität genetischer Daten erscheint jedoch eine Anwendung zur bloßen biometrischen Identifikation auf absehbare Zeit wenig wahrscheinlich.

- **Tastendruckdynamik** (Schreibrhythmus): Das System misst zum einen die sog. Tastenverweildauer, zum anderen die Länge der Zeit, die zwischen zwei Tastenanschlägen liegt. Eine charakteristische Tippdynamik existiert allerdings nur bei geübten Schreibenden.

- **Handflächenerkennung**: Ähnlich der Fingerbilderkennung misst das System das Linienmuster der Handinnenfläche einer Person.

- **Gefäßmuster (vaskuläre Muster)**: Biometrisch erfasst werden kann das charakteristische Venenmuster an verschiedenen Stellen des Körpers, z.B. an Handgelenk und Handrücken oder im Gesicht.


Zunehmend wichtig wird bei allen Systemen die sog. Lebenderkennung, die eine Überwindung der Systeme durch simple Imitate verhindern soll. Als eine verbesserte Technologie für die Lebenderkennung bei Fingerbildsensoren wird z.B. die Pulsoxymetrie verfolgt, also die Messung des Blutsauerstoffgehaltes.

3. Vorzüge und Nachteile der Systeme im Überblick

3. Vorzüge und Nachteile der Systeme im Überblick
t

wichtigsten biometrischen Systeme, wie sie in der Literatur zu finden sind. Tabelle 2 listet die technischen Kennwerte auf (zu FAR/FRR; s. Kap. II.1).

Tab. 2: Technische Angaben zu biometrischen Systemen/Verfahren

<table>
<thead>
<tr>
<th>Merkmal</th>
<th>Templategröße (Bytes)</th>
<th>Verifikations-/Registrierungszeit (sec)</th>
<th>FAR (%)</th>
<th>FRR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerbild (Minuzien)</td>
<td>900-1.200</td>
<td>0,5-20/10-30</td>
<td>0,01-0,0001</td>
<td>1,0-5,0</td>
</tr>
<tr>
<td>Handgeometrie</td>
<td>10-20</td>
<td>2-5/k.A.</td>
<td>0,1-5,0</td>
<td>0,2-5,0</td>
</tr>
<tr>
<td>Iris</td>
<td>bis 512</td>
<td>0,5-10/k.A.</td>
<td>0,01-1,0</td>
<td>0,1-2,0</td>
</tr>
<tr>
<td>Retina</td>
<td>40-96</td>
<td>ab 1,5/bis 30</td>
<td>0,0001</td>
<td>bis 12</td>
</tr>
<tr>
<td>Gesicht</td>
<td>bis 1.300</td>
<td>1-5/bis 30</td>
<td>0,5-2,0</td>
<td>1,0-3,0</td>
</tr>
<tr>
<td>Unter/Handschrift</td>
<td>400-1.500</td>
<td>5-15/30</td>
<td>1,6-20</td>
<td>2,8-25</td>
</tr>
<tr>
<td>Stimme</td>
<td>1.500-3.000</td>
<td>ab 1,5/k.A.</td>
<td>k.A.</td>
<td>k.A.</td>
</tr>
</tbody>
</table>

Quelle: Behrens/Roth 2001; Platanista 2001a

Tab. 3: Vorzüge und Nachteile biometrischer Verfahren/Systeme

<table>
<thead>
<tr>
<th>Merkmal</th>
<th>&quot;Stärken&quot;</th>
<th>&quot;Schwächen&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerbild</td>
<td>- einzigartig</td>
<td>- abhängig von Hautzustand</td>
</tr>
<tr>
<td></td>
<td>- beständig</td>
<td>- Positionierung nötig</td>
</tr>
<tr>
<td></td>
<td>- einfache Bedienung</td>
<td>- Systeminkompatibilitäten</td>
</tr>
<tr>
<td></td>
<td>- preisgünstig</td>
<td>- Lebenderkennung fehlt</td>
</tr>
<tr>
<td></td>
<td>- recht überwindungsresistent</td>
<td>- Assoziation d. Strafverfolgung</td>
</tr>
<tr>
<td>Handgeometrie</td>
<td>- unabhängig von Hautzustand</td>
<td>- nicht sehr charakteristisch</td>
</tr>
<tr>
<td></td>
<td>- niedrige Fehlerrate beim Enrollement (FER)</td>
<td>- beständig nur bei Erwachsenen</td>
</tr>
<tr>
<td></td>
<td>- einfache Bedienung</td>
<td>- Lebenderkennung fehlt</td>
</tr>
<tr>
<td></td>
<td>- schnell</td>
<td>- teuer, da Großgeräte nötig</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Hygieneaspekte</td>
</tr>
<tr>
<td>Iris/Retina</td>
<td>- einzigartig</td>
<td>- Retina: Störung durch Kontaktlinsen u. Astigmatismus</td>
</tr>
<tr>
<td></td>
<td>- beständig</td>
<td>- Positionierung nötig</td>
</tr>
<tr>
<td></td>
<td>- berührungslos</td>
<td>- teuer, da Großgeräte nötig</td>
</tr>
<tr>
<td></td>
<td>- sehr überwindungsresistent (Retina: &quot;nicht offenes&quot; Merkmal)</td>
<td>- Gesundheitsbedenken</td>
</tr>
<tr>
<td>Gesicht</td>
<td>- berührungslos</td>
<td>- unbeständig bei Alterung</td>
</tr>
<tr>
<td></td>
<td>- Standardgeräte verwendbar</td>
<td>- empfindlich gegenüber Licht- und Temperaturveränderungen</td>
</tr>
<tr>
<td></td>
<td>- teils kompatibel zu Papierdokumenten</td>
<td>- teils Positionierung nötig</td>
</tr>
<tr>
<td></td>
<td>- kontinuierliche Kontrolle möglich</td>
<td>- Überwachungsproblematik</td>
</tr>
<tr>
<td>Stimme</td>
<td>- ortsunabhängig</td>
<td>- nicht sehr charakteristisch</td>
</tr>
<tr>
<td></td>
<td>- einfache Bedienung</td>
<td>- unbeständig (Alterung) und störungsanfällig (Krankheit)</td>
</tr>
<tr>
<td></td>
<td>- Standardgeräte verwendbar</td>
<td>- zeitaufwendiges Enrolment</td>
</tr>
<tr>
<td></td>
<td>- Willenserklärung integrierbar, Nutzersteuerung möglich</td>
<td>- leicht überwindbar</td>
</tr>
<tr>
<td>Unter-/</td>
<td>- an konvent. Systeme anschließbar</td>
<td>- nicht sehr charakteristisch</td>
</tr>
<tr>
<td>Handschrift</td>
<td>- akzeptiert, da vertraut</td>
<td>- unbeständig</td>
</tr>
<tr>
<td></td>
<td>- Willenserklärung, Nutzersteuerung</td>
<td>- zeitaufwendiges Enrolment</td>
</tr>
</tbody>
</table>

3. Vorzüge und Nachteile der Systeme im Überblick

Tab. 4: Bewertung biometrischer Verfahren nach Jain et al. 1999

<table>
<thead>
<tr>
<th>Merkmal</th>
<th>Universalität</th>
<th>Einzigartigkeit</th>
<th>Beständigkeit</th>
<th>Messbarkeit</th>
<th>Leistung</th>
<th>Akzeptanz</th>
<th>Resistenzen*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerbild</td>
<td>mittel</td>
<td>hoch</td>
<td>hoch</td>
<td>mittel</td>
<td>hoch</td>
<td>mittel</td>
<td>hoch</td>
</tr>
<tr>
<td>Handgeometrie</td>
<td>mittel</td>
<td>mittel</td>
<td>hoch</td>
<td>mittel</td>
<td>hoch</td>
<td>mittel</td>
<td>hoch</td>
</tr>
<tr>
<td>Iris</td>
<td>hoch</td>
<td>hoch</td>
<td>hoch</td>
<td>mittel</td>
<td>hoch</td>
<td>gering</td>
<td>hoch</td>
</tr>
<tr>
<td>Retina</td>
<td>hoch</td>
<td>hoch</td>
<td>mittel</td>
<td>gering</td>
<td>hoch</td>
<td>gering</td>
<td>hoch</td>
</tr>
<tr>
<td>Gesicht</td>
<td>hoch</td>
<td>gering</td>
<td>mittel</td>
<td>hoch</td>
<td>gering</td>
<td>hoch</td>
<td>gering</td>
</tr>
<tr>
<td>+Thermogramm</td>
<td>hoch</td>
<td>hoch</td>
<td>gering</td>
<td>hoch</td>
<td>mittel</td>
<td>hoch</td>
<td>hoch</td>
</tr>
<tr>
<td>Unterschrift</td>
<td>gering</td>
<td>gering</td>
<td>gering</td>
<td>hoch</td>
<td>gering</td>
<td>hoch</td>
<td>gering</td>
</tr>
<tr>
<td>Stimme</td>
<td>mittel</td>
<td>gering</td>
<td>gering</td>
<td>mittel</td>
<td>gering</td>
<td>hoch</td>
<td>gering</td>
</tr>
<tr>
<td>Handvenen</td>
<td>mittel</td>
<td>mittel</td>
<td>mittel</td>
<td>mittel</td>
<td>mittel</td>
<td>hoch</td>
<td>hoch</td>
</tr>
<tr>
<td>Tastenanschlag</td>
<td>gering</td>
<td>gering</td>
<td>gering</td>
<td>mittel</td>
<td>gering</td>
<td>mittel</td>
<td>mittel</td>
</tr>
</tbody>
</table>

Quelle: Jain et al. 1999, nach Platanista 2001a; *: gegen Überwindungsversuche/Angriffe

Tab. 5: Bewertung biometrischer Verfahren nach Scheuermann et al. 2000

<table>
<thead>
<tr>
<th>Merkmal</th>
<th>Kostenfaktor</th>
<th>Anwenderfreundlichkeit</th>
<th>Wartungsanforderungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerbild</td>
<td>mittel</td>
<td>gering</td>
<td>mittel bis hoch</td>
</tr>
<tr>
<td>Handgeometrie</td>
<td>hoch</td>
<td>mittel</td>
<td>mittel</td>
</tr>
<tr>
<td>Iris</td>
<td>hoch</td>
<td>hoch</td>
<td></td>
</tr>
<tr>
<td>Retina</td>
<td>hoch</td>
<td>hoch</td>
<td></td>
</tr>
<tr>
<td>Gesicht</td>
<td>mittel</td>
<td>hoch</td>
<td></td>
</tr>
<tr>
<td>+Thermogramm</td>
<td>mittel</td>
<td>hoch</td>
<td></td>
</tr>
<tr>
<td>Unterschrift</td>
<td>mittel</td>
<td>gering</td>
<td></td>
</tr>
<tr>
<td>Stimme</td>
<td>gering</td>
<td>gering</td>
<td>gering</td>
</tr>
<tr>
<td>Handvenen</td>
<td>mittel</td>
<td>gering</td>
<td></td>
</tr>
<tr>
<td>Tastenanschlag</td>
<td>gering</td>
<td>gering</td>
<td></td>
</tr>
</tbody>
</table>

Quelle: Scheuermann et al. 2000, nach Platanista 2001a
Bei einer **Gruppierung und Gegenüberstellung der verschiedenen Systeme nach aktiven und passiven Merkmalen** können folgende Einschätzungen zusammengefasst werden (Platanista 2001a):

- **Die passiven, physiologischen Merkmale** sind meist "offen", d.h. von außen erkennbar (Ausnahme: Retina) und daher potenziellen "Angreifern" leichter zugänglich. Sie können anwendungsfreundlich im Sinne von bequem sein, damit verbunden ist dann die Möglichkeit einer unbemerkten, nicht autorisierten Identifikation zum Zweck der Überwachung. Die Erfassung passiver Merkmale kann auch trotz Widerstand durch physische Gewalt erzwungen werden, was z.B. für Zwecke der Strafverfolgung durchaus als Vorteil angesehen werden kann, im Hinblick auf kriminellen Missbrauch aber als Nachteil gelten muss.


III. Forschungs- und Entwicklungsaktivitäten


Auf der internationalen Ebene bereitet es schon Schwierigkeiten, überhaupt einen Überblick zu erlangen. Gerade im nordamerikanischen und asiatischen Raum existiert eine kaum überschaubare Vielzahl von Aktivitäten im privatwirtschaftlichen und öffentlichen Sektor.

Für den Blickwinkel der Technikfolgen-Abschätzung zur Feststellung des politischen Gestaltungsbedarfs sind besonders die sog. "Pilotprojekte" zur Evaluierung biometrischer Systeme von Interesse, die mit Unterstützung öffentlicher Institutionen durchgeführt werden. Sie sind zum einen als vergleichende Untersuchungen verschiedener technischer Systeme angelegt und behandeln zum anderen die gesellschaftlich relevanten Aspekte wie Verbraucher- und Datenschutz.

Im folgenden Kapitel III.1 werden die wichtigsten Ergebnisse der - deutschen - Pilotprojekte vorgestellt, und es wird ein kurzer Überblick zu laufenden Aktivitäten gegeben. Kapitel III.2 fasst zusammen, was zum Stand von FuE durch die Gutachter Behrens und Roth (Behrens/Roth 2001) und die Platanista GmbH (Platanista 2001a) sowie durch die Autoren dieses Berichts v.a. im Internet recherchiert werden konnte. Die Ergebnisse insgesamt sind unvollständig bzw. unsystematisch und bezüglich der einzelnen FuE-Projekte von äußerst unterschiedlichem Informationsgehalt. Dennoch ermöglichen sie zumindest einen ersten, exemplarischen Einblick in die weltweiten Forschungs- und Entwicklungsaktivitäten. Eine systematische Erhebung, einschließlich einer Identifikation von Schwerpunkten und erwartbaren Entwicklungstrends, bleibt eine Aufgabe für die Zukunft.
III. Forschungs- und Entwicklungsaktivitäten

1. Pilotprojekte und Entwicklung von Testkriterien

1.1 BioIS-Projekt


Technische Untersuchung

Überwindungsversuche konnten nur bei sieben Systemen gestartet werden - ein System konnte unter den Versuchsbedingungen gar nicht installiert werden, vier Systeme wiesen auch nach fünf Zugangsversuchen so hohe falsche Ablehnungsraten (FRR) (über 40%, einmal sogar über 60%!) auf, dass ein Test sinnlos gewesen wäre. Von den getesteten sieben Systemen konnten durch Benutzung eines kopierten oder gefälschten biometrischen Merkmals fünf überwunden werden, durch einen "Angriff" auf die Datenverbindung vom Sensor zur Verarbeitungseinheit (Abhören/Abgreifen der übertragenen Daten) sechs (IGD 2000, S. 44 ff.).

Eine Folgerung des IGD aus der technischen Untersuchung war, dass für verbesserte und aussagekräftigere Vergleiche biometrischer Systeme zukünftig ein detaillierter und verbindlicher Kriterienkatalog nötig ist. Entsprechende Aktivitäten sind aufgenommen worden (s.u.).

**Teiluntersuchung Technikfolgen-Abschätzung**


Die **Nutzerbefragung** erbrachte einige überraschende Ergebnisse (WIK 2000, S. 36 ff.):

- 80% der Befragten präferierten nach Abschluss der sechsmonatigen Testphase den Iris-Scan. Gesundheitsbedenken spielten entgegen den Erwartungen keine Rolle, sondern vielmehr die schnelle, bequeme und zuverlässige Handhabung.
- Mit großem Abstand wurden Fingerabdruck (48%), Hand- (36%) und Gesichts-Erkennung (20%) als akzeptabel und geeignet eingeschätzt.
- Das Sprechen mit einer Maschine wurde, insbesondere im Fall notwendiger Mehrfachversuche, als unangenehm bis peinlich empfunden. Hygienische Bedenken (z.B. beim Fingerabdruck) wurden hingegen kaum geäußert.
III. Forschungs- und Entwicklungsaaktivitäten

– Keine/r der Befragten lehnte den Einsatz biometrischer Verfahren prinzipiell ab, wobei berücksichtigt werden muss, dass die Mitarbeiter des IGD sowohl technisch überdurchschnittlich kundig als auch prinzipiell gegenüber Technik eher positiv eingestellt sind.

– Insgesamt dominierten Komfortwünsche deutlich gegenüber Datenschutzaspekten. Diese würden z.B. eine möglichst aktive Teilnahme der Nutzer am Erkennungsprozess nahe legen, um die Gefahr einer unbemerken Überwachung auszuschließen - die Probanden jedoch würden lieber so passiv wie möglich bleiben. Auf allgemeiner, theoretischer Ebene zeigte sich allerdings sehr wohl ein entwickeltes Bewusstsein für Sicherheits- und Datenschutzprobleme (Sicherung der Referenzdaten, Risiko des Merkmalsverlustes, Abhängigkeit vom biometrischen System, "gläserner Mensch").

Die Autoren der WIK-Studie konstatieren insgesamt einen sehr großen Informations- und Aufklärungsbedarf, sowohl im Hinblick auf die zukünftige Akzeptanz als auch auf Daten- und Verbraucherschutz. Für eine fundiertere Analyse spezifischer Nutzungshemmnisse biometrischer Systeme war die Fallgruppe allerdings viel zu klein. Hierzu wäre eine Untersuchung mit mehreren Tausend Nutzern nötig (WIK 2000, S. 39) - dafür wiederum müsste die Biometrie schon eine Massenanwendung gefunden haben.

Die Experteninterviews auf Basis der Literaturanalyse behandelten die Themen Systemische Sicherheit, Daten- und Verbraucherschutz, Grundversorgung und Medienkompetenz. Wichtige Ergebnisse und abgeleitete Gestaltungserfordernisse sind (WIK 2000, S. 40 ff.):

– Biometrische Techniken können potenziell die Authentifizierung verbessern, entscheidend bleibt allerdings die gesamte Sicherheitsarchitektur eines IT-Systems.

– Für einen wirklich aussagekräftigen Vergleich vorhandener Systeme, ob zu Zuverlässigkeit, Bedienungsfreundlichkeit oder Überwindungssicherheit, fehlen bislang die Daten. Unabdingbar ist die Entwicklung international akzeptierter Standardtestverfahren.

– Zentrale Sicherheitsaspekte sind die Lebenderkennung sowie der Schutz vor Manipulation und Missbrauch der Template-Daten. Deshalb sollten die Referenzdaten dezentral, am besten in der Verfügung des Nutzers (z.B. auf

1 Sehr deutlich formuliert wurde die Erwartung der Nutzer an Einfachheit und Zuverlässigkeit des biometrischen Systems durch einen der Befragten (WIK 2000, S. 32 f.): "Ein System wird nur dann akzeptiert, wenn es in der Lage ist, eine nicht ausgeschlafene, zerstreute, eventuell unter Restalkohol stehende Person zu authentifizieren."
1. Pilotprojekte und Entwicklung von Testkriterien


- Niemand darf zur Nutzung biometrischer Systeme gezwungen oder gedrängt werden. Da jedes biometrisch genutzte Merkmal bei überschlägig 5% der Bevölkerung "versagt", müssen alternative Autorisierungsverfahren erhalten bleiben, die für die Nutzer keine Nachteile bedeuten. Im Rahmen einer Verbraucherschutzdiskussion ist zu klären, ob umgekehrt auch die Gewährung von Vorteilen als Anreiz für die Nutzung biometrischer Verfahren unterbunden werden soll und kann.

- Aus Verbrauchersicht wäre eine Umkehrung der Beweislast bei Missbrauch - hin zu den Banken und anderen Betreibern - als Folge der Sicherheitserhöhung zu fordern. Diese Maßnahme würde die Akzeptanz der Kunden sicherlich erhöhen, bedeutet allerdings weitere Kosten für die Betreiber.

- Vor der Einführung biometrischer Verfahren in Massenanwendungen werden umfangreiche Aufklärungsmaßnahmen nötig sein, sowohl in praktischer und technischer Hinsicht als auch zu Verbraucher- und Datenschutz. Die Verteilung der Lasten dieser Aufgabe bleibt zu klären.

**Entwurf: Technische Evaluierungskriterien (TEK)**


Definiert werden drei Prüfungstypen, wobei das Hauptunterscheidungskriterium der Zeitaufwand ist: die generelle Beurteilung (physikalische Robustheit, Hard- und Softwareanforderungen, Erweiterbarkeit), die Zuverlässigkeit der Erfassung (über Feldtests, 3 Klassen à 10, 100 und 1.000 Teilnehmern mit je
III. Forschungs- und Entwicklungsaktivitäten

mindestens 150 Versuchen) bzw. Erkennungsleistung (FAR/FRR) unter verschiedenen Umweltbedingungen sowie die Sicherheit bzw. Überwindbarkeit.


1.2 BioTrusT (TeleTrusT Deutschland e.V.)

Im 1989 gegründeten, gemeinnützigen Verein TeleTrust Deutschland e.V. haben sich Unternehmen, Forschungseinrichtungen, Verbände und öffentliche Institutionen zusammengeschlossen, "um die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik in einer offenen Systemumgebung zu fördern". Aufgabe des Vereins ist es, "die Akzeptanz der digitalen Signatur als Instrument zur Rechtssicherheit einer Transaktion zu erreichen; die Forschung zur Sicherheit des elektronischen Datenaustausches (EDI) und die Anwendung ihrer Ergebnisse sowie die Entwicklung von Standards für dieses Gebiet zu unterstützen; mit Institutionen in anderen Ländern zusammen zu arbeiten, um Ziele und Standards innerhalb der Europäischen Union zu harmonisieren" (http://www.teletrust.de).

Da im Rahmen dieser Zielsetzung biometrische Verfahren eine wichtige Rolle spielen, hat sich eine spezielle Arbeitsgruppe (AG 6) des Themas angenommen. Ziel der AG 6 ist es, "den Einsatz geeigneter biometrischer Identifikationsverfahren zu fördern, die auf körpereigenen biometrischen Merkmalen eines Benutzers basieren, um die erforderlichen Sicherheitsverfahren der Informationstechnik, z.B. das PIN-Verfahren, zu ergänzen bzw. abzulösen. Dazu gehört ganz wesentlich die Information einer breiten Öffentlichkeit über biometrische Verfahren, unterschiedliche Methoden, mögliche Anwendungsgebiete und damit eine Förderung der Akzeptanz für den Umgang mit biometrischen
Identifikationsverfahren im alltäglichen beruflichen und privaten Gebrauch" (http://www.teletrust.de/main/AG/ag6+.htm).

**Kriterienkatalog**


**BioTrusT-Projekt**


Partner des BioTrusT-Projektes sind vier Betreiber, zehn Hersteller und vier "Research Partner", darunter die Fachhochschule Gießen-Friedberg, die folgende Fragestellungen wissenschaftlich bearbeiten soll (Behrens/Roth 2000, S. 329):

- "**Komfort-/Convenience-Aspekte:** Inwiefern bieten die biometrischen Verfahren den Nutzern Vorteile bezüglich Komfort und Bequemlichkeit? Wie bewertet der Benutzer Komfortelemente wie beispielsweise Schnelligkeit oder Einfachheit?

– **Vielfältigkeitenaspekte**: Welche Einsatzfelder sind, vornehmlich im elektronischen Zahlungsverkehr, besonders geeignet für welche biometrischen Verfahren? Gibt es dabei Unterschiede im Akzeptanzniveau bei potenziellen Nutzern?

– **Einsatzempfehlungen**: Die Bedingungsfaktoren für Vor- und Nachteile der einzelnen biometrischen Verfahren sind herauszuarbeiten."


### 1.3 Standardisierung und Evaluierung biometrischer Systeme


gegründet, eine unabhängige und gemeinnützige Forschungs- und Beratungseinrichtung für biometrische Anwender, Hersteller und Regierungsbehörden im asiatisch-pazifischen Raum (Platanista 2001a).


Der European Standard EN 5013 beschreibt Bewertungskriterien für Sicherheitsaspekte biometrischer Methoden und Verfahren, entsprechend den Technischen Evaluationskriterien des BSI in Deutschland (Kap. III.1.1) (Platanista 2001a).

2. FuE-Projekte in Deutschland und international


Deutschland

### Tab. 6: Öffentliche Forschungsaktivitäten zur Biometrie in Deutschland

<table>
<thead>
<tr>
<th>Forschungseinrichtung</th>
<th>biometrisches Thema</th>
<th>Internet-Adresse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fern-Universität Hagen</td>
<td>Tippdynamik</td>
<td><a href="http://ks.fernuni-hagen.de/forschung/datensich/index_Sonja.html">http://ks.fernuni-hagen.de/forschung/datensich/index_Sonja.html</a></td>
</tr>
<tr>
<td>Universität Karlsruhe (+ Robert Bosch GmbH)</td>
<td>Fingerbilderkennung</td>
<td><a href="http://www-iiit.etec.uni-karlsruhe.de/~kroeni/">http://www-iiit.etec.uni-karlsruhe.de/~kroeni/</a></td>
</tr>
<tr>
<td>Universität Tübingen</td>
<td>Gesichtserkennung</td>
<td><a href="http://www-ti.informatik.uni-tuebingen.de/deutsch/publikationen/jahresbericht9596/node40.html">http://www-ti.informatik.uni-tuebingen.de/deutsch/publikationen/jahresbericht9596/node40.html</a></td>
</tr>
<tr>
<td>TU Chemnitz</td>
<td>Bildverarbeitende Überwachungs- und Service-Systeme</td>
<td><a href="http://www.tu-chemnitz.de/~svko/jobpage/Arbeitsgebiete/Bericht.html">http://www.tu-chemnitz.de/~svko/jobpage/Arbeitsgebiete/Bericht.html</a></td>
</tr>
<tr>
<td>TU Ilmenau</td>
<td>Biometrie und Smartcards</td>
<td><a href="http://kb-bmts.rz.tu-ilmenau.de/kb-bmts/Leitprojekte/Komp_kurz.htm">http://kb-bmts.rz.tu-ilmenau.de/kb-bmts/Leitprojekte/Komp_kurz.htm</a></td>
</tr>
<tr>
<td>FH Gießen-Friedberg</td>
<td>BioTrusT-Projekt</td>
<td><a href="http://www.biometrie-info.de">http://www.biometrie-info.de</a></td>
</tr>
<tr>
<td>Fraunhofer-Institut für Integrierte Publikations- u. Informationssysteme (IPSI)</td>
<td>Qualitätsvaluierung, speziell Handschriftenerkennung</td>
<td><a href="http://www.ipsi.fraunhofer.de/mobile/projects/h2o4m/index.html">http://www.ipsi.fraunhofer.de/mobile/projects/h2o4m/index.html</a></td>
</tr>
</tbody>
</table>

Quelle: Behrens/Roth 2001, S. 29 ff.; Platanista 2001a
Tab. 7: Industrielle FuE/Beratung zum Thema Biometrie in Deutschland

<table>
<thead>
<tr>
<th>Unternehmen (Beteiligung an Pilotprojekt)</th>
<th>biometrisches Verfahren oder verwandtes Thema</th>
<th>Internetadresse</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABDA</td>
<td>Smartcard</td>
<td><a href="http://www.abda.de">http://www.abda.de</a></td>
</tr>
<tr>
<td>ABS GmbH (BioTrust)</td>
<td>Stimmerkennung</td>
<td><a href="http://www.abs-jena.de">http://www.abs-jena.de</a></td>
</tr>
<tr>
<td>ACEM GmbH</td>
<td>Fingerbild-Scanner</td>
<td><a href="http://www.acem.de">http://www.acem.de</a></td>
</tr>
<tr>
<td>Add Trust</td>
<td>Digitale Signatur</td>
<td><a href="http://www.addtrust.com">http://www.addtrust.com</a></td>
</tr>
<tr>
<td>AlphaNet Online GmbH (BioIS)</td>
<td>Fingerbild-Scanner, Bio-Mouse</td>
<td><a href="http://www.alphanet.de">http://www.alphanet.de</a></td>
</tr>
<tr>
<td>AMC-Assekuranz Marketing Circle GmbH</td>
<td>Unternehmensberatung</td>
<td><a href="http://www.versicherungen.de/AMC">http://www.versicherungen.de/AMC</a></td>
</tr>
<tr>
<td>Baltimore Technologies</td>
<td>eSecurity</td>
<td><a href="http://www.baltimore.com">http://www.baltimore.com</a></td>
</tr>
<tr>
<td>BERGDATA (BioTrust)</td>
<td>Fingerbild</td>
<td><a href="http://www.bergdata.com">http://www.bergdata.com</a></td>
</tr>
<tr>
<td>BGS Systemplanung</td>
<td>Digitale Signatur</td>
<td><a href="http://www.bgs-ag.de">http://www.bgs-ag.de</a></td>
</tr>
<tr>
<td>CAST-Forum</td>
<td>eSecurity (Consulting)</td>
<td><a href="http://www.castforum.de">http://www.castforum.de</a></td>
</tr>
<tr>
<td>CCI (Competence Center Informatik GmbH)</td>
<td>IT-Consulting, Software</td>
<td><a href="http://www.cci.de">http://www.cci.de</a></td>
</tr>
<tr>
<td>Cherry GmbH (BioIS)</td>
<td>Tastatur-Fingerbild-Scanner</td>
<td><a href="http://www.cherry.de">http://www.cherry.de</a></td>
</tr>
<tr>
<td>CogniTec AG</td>
<td>Gesichtserkennung</td>
<td><a href="http://www.cognitec-ag.de">http://www.cognitec-ag.de</a></td>
</tr>
<tr>
<td>DataDesign AG</td>
<td>digitale Signatur</td>
<td><a href="http://www.datadesignag.de">http://www.datadesignag.de</a></td>
</tr>
<tr>
<td>DCS AG (BioIS, BioTrust)</td>
<td>BioID-Gesichtserkennung, Merkmalskombinationen</td>
<td><a href="http://www.bioid.com">http://www.bioid.com</a></td>
</tr>
<tr>
<td>De-Coda GmbH</td>
<td>digitale Signatur</td>
<td><a href="http://www.de-coda.de">http://www.de-coda.de</a></td>
</tr>
<tr>
<td>Dermalog Identification Systems GmbH</td>
<td>Fingerbild, ID-Cards mit biometrischen Merkmalen</td>
<td><a href="http://www.dermalog.de">http://www.dermalog.de</a></td>
</tr>
<tr>
<td>Dr. Fehr GmbH/Wondernet (BioAPI, BioTrust)</td>
<td>Unterschrift/Handschriften</td>
<td><a href="http://www.drfehr.de">http://www.drfehr.de</a></td>
</tr>
<tr>
<td>Eutelis Consult</td>
<td>Markteinführung</td>
<td><a href="http://www.eutelis.de">http://www.eutelis.de</a></td>
</tr>
<tr>
<td>FAKTUM Softwareentwicklung GmbH</td>
<td>digitale Signatur</td>
<td><a href="http://www.faktum.com">http://www.faktum.com</a></td>
</tr>
<tr>
<td>Fun Communications</td>
<td>digitale Signatur</td>
<td><a href="http://www.fun.de">http://www.fun.de</a></td>
</tr>
<tr>
<td>Gemplus GmbH</td>
<td>Smartcards</td>
<td><a href="http://www.gemplus.com">http://www.gemplus.com</a></td>
</tr>
</tbody>
</table>
Tab. 7: Fortsetzung

<table>
<thead>
<tr>
<th>Unternehmen</th>
<th>Verfahren/Thema</th>
<th>Internetadresse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Giesecke &amp; Devrient GmbH (BioTrust)</td>
<td>Fingerbild</td>
<td><a href="http://www.gdm.de">http://www.gdm.de</a></td>
</tr>
<tr>
<td>IKENDI (BioAPI, BioTrust)</td>
<td>Fingerbild</td>
<td><a href="http://www.ikendi.de">http://www.ikendi.de</a></td>
</tr>
<tr>
<td>INFINEON Technologies AG (BioIS)</td>
<td>Unterschriftenprüfung, Fingerbild</td>
<td><a href="http://www.infineon.com">http://www.infineon.com</a></td>
</tr>
<tr>
<td>INFORA GmbH</td>
<td>IT-Unternehmensberatung</td>
<td><a href="http://www.infora.de">http://www.infora.de</a></td>
</tr>
<tr>
<td>Kesberg, Bütfering &amp; Partner (KB&amp;P)</td>
<td>Markterschließung</td>
<td><a href="http://www.kbp-bonn.de">http://www.kbp-bonn.de</a></td>
</tr>
<tr>
<td>NCR GmbH (BioIS)</td>
<td>Iris-Scanner</td>
<td><a href="http://www.ncr.com">http://www.ncr.com</a></td>
</tr>
<tr>
<td>OMNEYKEY AG</td>
<td>Smartcard-Lesegeräte</td>
<td><a href="http://www.omnikey.de">http://www.omnikey.de</a></td>
</tr>
<tr>
<td>Platanista GmbH (H2O4M)</td>
<td>Handschriften-Software</td>
<td><a href="http://www.platanista.com">http://www.platanista.com</a></td>
</tr>
<tr>
<td>plettac electronics (BioTrust)</td>
<td>Gesichtserkennung</td>
<td><a href="http://www.plettac-electronics.de">http://www.plettac-electronics.de</a></td>
</tr>
<tr>
<td>Rainbow Technologies</td>
<td>eSecurity</td>
<td><a href="http://www.rainbow.com">http://www.rainbow.com</a></td>
</tr>
<tr>
<td>SD Industries GmbH</td>
<td>Iriserkennung</td>
<td><a href="http://www.sd-industries.de">http://www.sd-industries.de</a></td>
</tr>
<tr>
<td>Secorvo Security Consulting GmbH</td>
<td>IT-Consulting</td>
<td><a href="http://www.secorvo.de">http://www.secorvo.de</a></td>
</tr>
<tr>
<td>Secude GmbH</td>
<td>Kryptografie</td>
<td><a href="http://www.secude.com">http://www.secude.com</a></td>
</tr>
<tr>
<td>SOFTPRO (BioAPI, BioTrust)</td>
<td>Unterschriften-Software im Bankenbereich</td>
<td><a href="http://www.softpro.de">http://www.softpro.de</a></td>
</tr>
<tr>
<td>Touchless Sensor Technology AG</td>
<td>Fingerbildsensoren</td>
<td><a href="http://www.tst-ag.com">http://www.tst-ag.com</a></td>
</tr>
<tr>
<td>T-Systems NOVA (BioTrust)</td>
<td>wissenschaftliche Gutachten (Prüfkriterien/siegel)</td>
<td><a href="http://www.t-nova.de">http://www.t-nova.de</a></td>
</tr>
<tr>
<td>Utimaco Safeware</td>
<td>Fingerbild, Smartcard, Sicherheitslösungen</td>
<td><a href="http://www.utimaco.de">http://www.utimaco.de</a></td>
</tr>
<tr>
<td>VoiceTrust AG</td>
<td>Stimmerkennungs-Software</td>
<td><a href="http://www.voicetrust.de">http://www.voicetrust.de</a></td>
</tr>
<tr>
<td>Wincor Nixdorf GmbH &amp; Co KG (BioTrust)</td>
<td>Iriserkennung</td>
<td><a href="http://www.wincornixdorf.com">http://www.wincornixdorf.com</a></td>
</tr>
<tr>
<td>ZN GmbH (BioIS, BioTrust)</td>
<td>Gesichtserkennung</td>
<td><a href="http://www.zn-gmbh.com">http://www.zn-gmbh.com</a></td>
</tr>
</tbody>
</table>

Quelle: Platanista 2001a; http://www.teletrust.de (→ Mitglieder)
Allerdings zeigt die hohe Beteiligung deutscher Institute und Unternehmen an EU-Projekten (Tab. 9) eine zunehmende Aktivität hierzulande. Auch das BMBF hat mit entsprechender Projektförderung begonnen, so im Projekt H2O4M des Fraunhofer-Institutes IPSI in Darmstadt (Tab. 6) mit dem Ziel, digitale Wasserzeichen zum Nachweis der Authentizität und Integrität von Multimediadokumenten und -objekten zu klassifizieren und zu bewerten. Dabei wird auch der Einsatz biometrischer Merkmale zur Benutzerauthentifizierung und damit Erhöhung der Fälschungssicherheit untersucht (Platanista 2001a).


Auf jeden Fall haben auch die industriellen Aktivitäten rund um biometrische Themen in den vergangenen Jahren in Deutschland an Dynamik gewonnen, dabei werden zunehmend die Möglichkeiten von Kooperationen im Rahmen von EU-Projekten genutzt (Tab. 9). Tabelle 7 listet deutsche Herstellerfirmen/ Entwickler biometrischer Systeme und ihre Schwerpunkte auf. Ein großer Teil der Firmen ist Mitglied der AG 6 von TeleTrusT (Kap. III.1.2) und war bzw. ist an den Pilotprojekten BioIS und BioTrusT beteiligt.


Auch in Österreich ist 2001 ein Pilotversuch angelaufen. Die Firma "ekey biometric systems" hat ein 5-stufiges Projekt zur Nutzung des Finger-Scans (Bezahlen am Point of Sale ab 04/01; eTicketing ab 09/01; Business-Transaktionen u. Zahlung im Internet mittels Kreditkarte ab 12/01; eBanking ab Frühjahr 2002) mit mehreren Kooperationspartnern begonnen (http://www.ekey.at).


- Projekt "BANCA - Biometric access control for networked and e-commerce applications" (Ref.-Nr. IST-1999-11159): Unter Benutzung von multimodaler biometrischer Identifikation (Gesicht- und Sprecherverifikation) sollen drei Demonstrationsobjekte aufgebaut werden: Telearbeitsplatz, Home-Banking und ein biometrischer Geldausgabeautomat. Das Projekt wird im Rahmen des IST-Programmes mit 2,55 Mio. € gefördert. Die Laufzeit beträgt 30 Monate ab Januar 2001. Der "Prime-Contractor" ist Matra Nortel Communications S.A, Quimper (F), weitere beteiligte Firmen oder Organisationen sind: Ibermatica S.A., San Sebastian (E), University of Surrey, Guildford (UK), Ecole Polytechnique Fédérale de Lausanne (CH), Banco Bilbao Vizcaya, Bilbao (E), Oscard, Puteaux (F), Institut Dalle Molle d’Intelligence Artificielle Perceptive (CH), Université Catholique de Louvain, Louvain-La-Neuve (B), sowie Thomson CsF Communications, Colombes (F).
### III. Forschungs- und Entwicklungsaktivitäten

Tab. 8: Exemplarische internationale Forschungsstandorte und -themen

<table>
<thead>
<tr>
<th>Forschungseinrichtung</th>
<th>biometrisches Thema</th>
<th>Internet-Adresse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Università di Bologna (I)</td>
<td>Fingerbild, Gesicht, Handgeometrie</td>
<td><a href="http://www2.csr.unibo.it/research/biolab/bio_tree.html">http://www2.csr.unibo.it/research/biolab/bio_tree.html</a></td>
</tr>
<tr>
<td>University of Cambridge (UK)</td>
<td>Iriserkennung</td>
<td><a href="http://www.cl.cam.ac.uk/~jgd1000/">http://www.cl.cam.ac.uk/~jgd1000/</a></td>
</tr>
<tr>
<td>University of Kent at Canterbury (UK)</td>
<td>Gesichts- und Stimmerekennung</td>
<td><a href="http://www.jtap.ac.uk/reports/htm/jtap-038.html">http://www.jtap.ac.uk/reports/htm/jtap-038.html</a></td>
</tr>
<tr>
<td>Ministry of International Trade and Industry MITI (JPN)</td>
<td>National Project of Test and Evaluation for Biometric Technologies</td>
<td><a href="http://www.miti.go.jp">http://www.miti.go.jp</a></td>
</tr>
<tr>
<td>George Mason University (USA)</td>
<td>breitgefächerte Aktivitäten</td>
<td><a href="http://www.cs.gmu.edu">http://www.cs.gmu.edu</a> (search: &quot;biometric&quot;)</td>
</tr>
<tr>
<td>Massachusetts Institute of Technology (USA)</td>
<td>breitgefächerte Aktivitäten</td>
<td><a href="http://www.mit.edu">http://www.mit.edu</a> (search: &quot;biometric&quot;)</td>
</tr>
<tr>
<td>Michigan State University (USA)</td>
<td>diverse Systeme</td>
<td><a href="http://biometrics.cse.msu.edu/">http://biometrics.cse.msu.edu/</a></td>
</tr>
</tbody>
</table>

Quelle: Behrens/Roth 2001, S. 32 ff.; Platanista 2001a
Tab. 9: Laufende Biometrie-Projekte im Rahmen des IST-Programms der EU

<table>
<thead>
<tr>
<th>Name*</th>
<th>Referenz-Nr.</th>
<th>Zahl der Partner*</th>
<th>Fördermittel</th>
<th>Laufzeit</th>
</tr>
</thead>
<tbody>
<tr>
<td>BANCA - Biometric access control for networked and e-commerce applications</td>
<td>IST-1999-11159</td>
<td>9</td>
<td>2,55 Mio. €</td>
<td>01/01-06/03</td>
</tr>
<tr>
<td>BEE - Business environment of biometrics involved in electronic commerce</td>
<td>IST-1999-20078</td>
<td>4</td>
<td>0,55 Mio. €</td>
<td>12/00-05/02</td>
</tr>
<tr>
<td>FINGER_CARD - Biometric matching and authentication system on card</td>
<td>IST-2000-25168</td>
<td>9</td>
<td>1,93 Mio. €</td>
<td>01/01-06/02</td>
</tr>
<tr>
<td>E-POLL - Electronic polling system for remote voting operations</td>
<td>IST-1999-21109</td>
<td>7</td>
<td>1,7 Mio. €</td>
<td>09/00-08/02</td>
</tr>
<tr>
<td>PAIDFAIR - Protecting accumulated intellectual data for accounting in real time</td>
<td>IST-2000-29616</td>
<td>7</td>
<td>1,3 Mio. €</td>
<td>06/01-11/02</td>
</tr>
<tr>
<td>SABRINA - Secure authentication by a biometric rationale and integration into network applications</td>
<td>IST-2000-26273</td>
<td>7</td>
<td>2,09 Mio. €</td>
<td>01/01-12/02</td>
</tr>
<tr>
<td>U-FACE - User friendly face access control system for physical access and healthcare applications</td>
<td>IST-1999-11587</td>
<td>6</td>
<td>0,7 Mio. €</td>
<td>10/00-03/03</td>
</tr>
</tbody>
</table>

* Zu Projektzielen und Namen der Partner s. Text.

Quelle: Behrens/Roth 2001; Platanista 2001a

-- Projekt "**BEE - Business environment of biometrics involved in electronic commerce**" (Ref.-Nr. IST-1999-20078): Aufgabe des Projektes ist es, behindernde und fördernde Elemente der biometrischen Identifikation als Sicherheitselemente innerhalb des E-Commerce zu identifizieren. Dazu soll ein Kosten-Nutzen-Modell entwickelt werden, das alle Aspekte (Technik,
Organisation, Ökonomie, Herstelleraspekte, Standards und Gesetzeslage) berücksichtigt. Das Projekt hat im Dezember 2000 begonnen und soll 15 Monate dauern. Die Fördersumme beträgt 550.000 €. Prime-Contractor ist PriceWaterhouseCoopers N.V., Amsterdam (NL), die weiteren Teilnehmer sind: ATMEL Grenoble (F), die nationale Technische Universität von Athen (G) sowie Expertnet, Athen (G).


2. **FuE-Projekte in Deutschland und international**

Software. Hierdurch soll mehr Vertrauen hinsichtlich der Zahlungsvorgänge für Software- und IP-Content-Verkäufer und ihre Kunden geschaffen werden. Die Authentisierung soll durch biometrische Systeme in Verbindung mit Smartcards realisiert werden. Prime-Contractor ist die Wibu-Systems Aktiengesellschaft, Karlsruhe (D), weitere Teilnehmer sind Neol (F), Native Instruments Software Synthesis Gmbh (D), Hoschar Ag (D), Asknet Ag (D), Compusec N.V. (B) und 2-Tel B.V. (NL).


- **Projekt "U-FACE - User friendly face access control system for physical access and healthcare applications"** (Ref.-Nr. IST-1999-11587): Ziel des Projektes ist es, Gesichtserkennungsalgorithmen im Zusammenhang mit der Nutzung von Smartcards, insbesondere für physikalische Zugangskontrollen im Finanzbereich und für Patientendateien, zu verbessern sowie Prototypen herzustellen. Das Projekt wurde im April 2000 gestartet und dauert 30 Monate, gefördert mit 700.000 €. Prime-Contractor ist die Firma Visual Automation Limited, Manchester (UK), weitere Partner sind Netsmart S.A., Athen (G), Biotrast S.A., Thessaloniki (G), Interactive Labs S.r.l., Florenz (I), die Organisation Social Solidarity, Thessaloniki (G), sowie die Victoria University of Manchester (UK).

Ein weiteres aktuelles EU-Projekt im Rahmen des IST-Programms behandelt den Einsatz einer europäischen Bürgerkarte mit biometrischer Komponente (Smartcard mit Fingerbildsensor), die bei Wohnungwechseln in der EU genutzt werden könnte, nicht aber als Passersatz bzw. Ausweis dienen soll. Das Projekt nennt sich **FASME** ("Facilitating Administrative Services for Mobile Europeans", http://www.fasme.org) und wird von einem Konsortium mehrerer
Städte (Grosseto, Köln, Newcastle), Universitäten (Amsterdam, Köln, Rostock, Zürich) und Firmen (ICL, ZUENDEL & Partner) betrieben.

IV. Biometrische Verfahren in der Praxis


1. Anwendungsfelder und -beispiele


Bisherige und absehbare Einsatzfelder (Tab. 9; Kap. IV.1.5) können grob in fünf Gruppen eingeteilt werden (Behrens/Roth 2001, S. 42 f.):

- Benutzerzugangssicherung
- Personenidentifikation
- Gerätezugangskontrolle
IV. Biometrische Verfahren in der Praxis

– elektronischer Zugang zu Dienstleistungen (E-Banking und E-Commerce)
– sonstige "Conveniencebereiche".  

1.1 Benutzerzugangssicherung

Diese fast schon "klassisch" zu nennende Anwendung der Biometrie reicht von der Zugangssicherung zu einem Gelände oder Gebäude bis hin zu Krankenhausapotheke oder Bankschließfächern.

<table>
<thead>
<tr>
<th>Beispiele für biometrisch gesicherte Bereiche in der Literatur (verschiedene Quellen; &quot;genutztes&quot; Merkmal in [...]</th>
</tr>
</thead>
<tbody>
<tr>
<td>das US-amerikanische <strong>Verteidigungsministerium</strong> [Hand]</td>
</tr>
<tr>
<td>alle 75 <strong>Bundesgefängnisse</strong> der USA sowie Gefängnisse in Großbritannien und den Niederlanden [diverse Systeme]</td>
</tr>
<tr>
<td>Olympisches Dorf in Atlanta 1996 [Hand]</td>
</tr>
<tr>
<td>eine Marinewerft in Indien (gleichzeitig Zeiterfassung) [Gesicht]</td>
</tr>
<tr>
<td><strong>Privatschulen</strong> in Japan und Großbritannien (gleichzeitig Anwesenheitskontrolle von Schülern und Mitarbeitern) [Fingerbild]</td>
</tr>
<tr>
<td><strong>Diskotheken</strong> und Nachtreihen [v.a. Gesicht, auch Fingerbild]</td>
</tr>
<tr>
<td>Mitarbeiter- und Sicherheitszonen in <strong>Flughäfen</strong> weltweit [diverse Systeme, z.B. Fingerbild: Frankfurt/Main; Gesicht: London Heathrow]</td>
</tr>
<tr>
<td>Criminal Justice Information Services Center der US-amerikanischen Bundespolizei FBI [Fingerbild]</td>
</tr>
<tr>
<td>Kernbereiche des Trustcenters bei der <strong>Regulierungsbehörde für Post- und Telekommunikation</strong> (Mainz) [Fingerbild]</td>
</tr>
<tr>
<td>Teilbereiche US-amerikanischer <strong>Hochschulen</strong>, wie Labore, Computerräume oder Wohnheime [diverse Systeme]</td>
</tr>
<tr>
<td>Räume der Geschäftsführung von Unternehmen (Deutsche Bank, Frankfurt am Main) [Gesicht]</td>
</tr>
<tr>
<td><strong>Krankenhausapotheke</strong> (Humana Hospital Aubadon, USA) [Stimme]</td>
</tr>
<tr>
<td><strong>Schließfächer</strong> (Zuger Kantonal Bank, Schweiz) [Fingerbild], (Dresdner Bank, Frankfurt am Main) [Gesicht]</td>
</tr>
<tr>
<td>Biathlonmunition (Olympische Winterspiele 1998, Nagano, Japan) [Iris]</td>
</tr>
</tbody>
</table>


1.2 Personenidentifikation

Bei der eindeutigen Identifikation einer Person werden gegenüber der bloßen Verifikation weitaus höhere Anforderungen an ein biometrisches System gestellt. Es fallen weitaus größere Datenmengen an, die an einer zentralen Stelle gespeichert und verarbeitet werden müssen. Die Anwendungskontexte erfordern z.T. eine Verbindung zu hochsensiblen Informationen z.B. polizeilicher Art, so dass Fragen des Datenschutzes hier eine besondere Rolle spielen. Wegen der Größe der Nutzergruppen und der Bedeutung der Zwecke bzw. der Missbrauchspotenziale sind höchste Anforderungen an die technische Ausgereiftheit der biometrischen Systeme (sowohl niedrige FAR als auch FRR!) zu stellen.

Drei zentrale Zwecke der Personenidentifikation sind die - polizeiliche - Überwachung öffentlicher Orte (zu Abschreckungs- wie zu Fahndungszwecken), die Verbesserung des Identitäts- bzw. Legitimationsnachweises (z.B. Führerschein, aber auch Personalausweise o.ä.) sowie die Kontrolle der Gewährung bzw. die Vermeidung des Missbrauchs von staatlichen (Sozial-)Leistungen oder von Leistungen im Rahmen der Gesundheitsversorgung:

IV. Biometrische Verfahren in der Praxis

Fußballvereinen West Ham United und Manchester United Ende 1999, um bekannte Hooligans zu identifizieren. Mobile Kameras wurden an strategisch wichtigen Punkten außerhalb des Stadions aufgebaut.

- Ein entsprechender Überwachungsvorgang beim American-Football-Finale in den USA ("Superbowl") in Tampa im Februar 2001 hat eine heftige Diskussion in den USA über die Bedrohung von Bürgerrechten durch Biometrie ausgelöst.


1. Anwendungsfelder und -beispiele

Sowohl der hessische als auch der schleswig-holsteinische Datenschutzbeauftragte haben sich klar gegen ein solches Projekt ausgesprochen (Albrecht 2001, S. 13). Bereits jetzt werden auf nationaler Ebene automatische Fingerbild-Identifikations-Systeme (AFIS) bei der Asylbewerbung eingesetzt (u.a. in Deutschland, Belgien, Frankreich), die **EU plant, ein länderübergreifendes System einzurichten** (EURODAC), um doppelte Antragstellung zu vermeiden.

- Die biometrische Ausstattung von **Sozialversicherungsausweisen** bzw. die Nutzung biometrischer Verfahren bei der Auszahlung von Renten und anderen staatlichen Leistungen wird u.a. in vielen US-Bundesstaaten, in Südafrika und auf den Philippinen bereits praktiziert (meist Fingerbilderkennung).

- Die o.g. **europäische Bürgerkarte**, die im Projekt FASME erprobt wird (Kap. III.2), stellt eine Anwendung im Zwischenbereich von Identitätsnachweis, Leistungsgewährung und elektronischem Zugang zu Dienstleistungen (Kap. IV.1.4) dar.


- In den Niederlanden werden Handgeometriesysteme in **Methadonprogrammen** eingesetzt. Die beteiligten drogenabhängigen Patienten können nach erfolgter Authentisierung mehrere Tagesrationen auf einmal erhalten (Albrecht 2001, S. 15 f.).

1.3 Gerätezugangskontrolle

Die biometrische Nutzersicherung von elektronischen und sonstigen Geräten ist gewissermaßen eine Variante der Benutzerzugangssicherung. Eine Verifikation genügt immer, eine Integration in größere Sicherungssysteme ist meist nicht nötig. Weil - verglichen mit o.g. Sicherheitszonen - die Möglichkeit, durch falsch erteilte Zugangsberechtigung Schaden zu verursachen, in der Regel begrenzt ist, kann eine höhere FAR akzeptiert werden, zugunsten einer niedrigen FRR, die für eine verlässliche und komfortable Nutzung nötig ist. Da also die technischen Anforderungen auf einem mittleren Niveau anzusiedeln sind und auch kaum Schwierigkeiten bei der Datenverwaltung (z.B. datenschutzrechtlich) entstehen, finden sich auf diesem Sektor die ausgereiftesten neuartigen, für den privaten Gebrauch konzipierten Biometrie-Anwendungen, z.B. bei:


- **PCs:** Bei hochwertigen Laptops werden zunehmend biometrische Systeme als Missbrauchsenschutz angeboten (Fingerbild- oder Gesichtserkennung); für Desktop-Systeme existiert eine Vielzahl von Lösungen verschiedener Anbieter, die den Rechner bzw. die Tastatur (Fa. Cherry) oder die Maus (Microsoft) v.a. mittels Fingerbilderfassung sichern.

- **Geldausgabeautomaten:** Während in Deutschland bislang nur bankeninterne Pilotversuche durchgeführt worden sind (neben dem o.g. BioTrusT-Projekt z.B. bei einer Filiale der Dresdner Bank), finden sich in den USA Beispiele für "echte" Anwendungen. Die Bank United hat nach eigenen Angaben mit großem Kundenerfolg Iriserkennungssysteme in mehreren Filialen installiert, die Wells Fargo Bank plant in Zusammenarbeit mit "Mr. Payroll", über 1.000 Scheckeinlösungs-Automaten mit Gesichtserkennung aufzustellen. (Die Inkasso-Nahme von Schecks hat in den USA nach
wie vor eine hohe praktische Bedeutung, da laut Schätzungen 37 Mio. US-Amerikaner kein Bankkonto besitzen.)


### 1.4 Elektronischer Zugang zu Informationen und Dienstleistungen

Anwendungen im Bereich E-Commerce werden zwar häufig als Hauptidefrs des zukünftigen Einsatzes biometrischer Systeme genannt, real existieren allerdings nur wenige Anwendungsbeispiele. Ein Grund dafür ist, dass die technischen Anforderungen (gleichzeitig niedrige FAR und FRR) eher hoch sind und die Entwicklung daher kostenintensiv ist. Hinzu kommen Daten- und Verbraucherschutzaspekte, die einer schnelle Verbreitung hinderlich sind.

- **Electronic Banking:** Weltweit werden von vielen Banken biometrische Systeme auf ihre Eignung getestet, bislang meist nur firmenintern (so auch im deutschen BioTrusT-Projekt der S-Finanzgruppe; Kap. III.1.2). Beispiele sind Versuche zum Einsatz von Fingerbilderkennung beim Online-Banking der kanadischen Tochter der niederländischen Bankgruppe ING oder von Sprechererkennung beim Telefon-Banking der britischen Bank "Nationwide" (s. auch das EU-Projekt BANCA; Kap. III.2).

- **Electronic Shopping:** Beim Einkauf via Telefon wird die Anwendung von Sprechererkennung anscheinend genutzt, von "echten" Internet-Händlern sind bislang lediglich konzeptionelle Vorschläge bzw. Überlegungen bekannt (s. auch das EU-Projekt BEE; Kap. III.2).

- **Firmeninterne und -externe Kommunikationssysteme:** Sprechererkennung bildet eine Identifizierungs- und Sicherheitsmaßnahme für umfangreiches Außendienstpersonal, z.B. einer Großbäckerei in den USA, oder bei
IV. Biometrische Verfahren in der Praxis

der Abrufung vertraulicher Informationen durch Flugbesatzungen. Auch andere - z.B. über das Internet verteilte - geschlossene Benutzergruppen (Virtual Private Networks, VPN) können biometrisch autorisiert werden.


1.5 **Conveniencebereiche**


- Heizungs- und Beleuchtungsanlagen,
- Unteralterungselektronik,
- Kraftfahrzeugen (Sitz- und Spiegelinstellungen, Klimaanlage, Radiosender und Autotelefon) oder auch
- einer Kaffeemaschine, die in Abhängigkeit vom identifizierten Nutzer und seinen gespeicherten Vorlieben die Kaffeestärke wählt (Demonstration der Fa. Siemens auf der CeBit).

Noch existieren diese Anwendungsbeispiele zum ganz überwiegenden Teil als Vorschläge, Labormuster oder Messeprototypen.
Tabelle 10 illustriert und charakterisiert in einem Überblick zusammenfassend wichtige Anwendungsbereiche anhand der jeweils vorrangig bestimmenden Optimierungskriterien (FAR oder FRR), nennt die jeweils bevorzugt eingesetzten biometrischen Systeme und deren Verbreitung sowie Beispiele für Einzelanwendungen und Anwender.

**Tab. 10: Biometrische Verfahren in der Praxis**

<table>
<thead>
<tr>
<th>Einsatzbereich</th>
<th>Optimierungsparameter</th>
<th>vorrangig genutzte Verfahren</th>
<th>Verbreitung</th>
<th>Anwendungen und Anwender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bankensektor</td>
<td>FRR (+ FAR)</td>
<td>Fingerbild, Iris, Unterschrift</td>
<td>Pilotprojekte</td>
<td>Kreditkarten, Überweisungen, Geldautomat</td>
</tr>
<tr>
<td>Computer-Sicherheit</td>
<td>FAR</td>
<td>Fingerbild, Gesicht, Handschrift</td>
<td>gering-mittel</td>
<td>PC- u. Netzwerkzugang</td>
</tr>
<tr>
<td>E-Commerce/Internet</td>
<td>FAR (+ FRR)</td>
<td>Fingerbild, Gesicht, Unter- u. Handschrift, Stimme</td>
<td>k.A.</td>
<td>Einzelhandel, Vermittlung, Beratungsdienste</td>
</tr>
<tr>
<td>Recht, öffentliche Sicherheit</td>
<td>FAR</td>
<td>Fingerbild, Gesicht, Unter- u. Handschrift, Iris</td>
<td>Pilotprojekte</td>
<td>Einwanderung, Überwachung, Betrugsvorbeugung, Einreisekontrolle</td>
</tr>
<tr>
<td>Nationale Sicherheit</td>
<td>FAR</td>
<td>Fingerbild, Gesicht, Iris, Handgeometry, Stimme</td>
<td>Pilotprojekte</td>
<td>Militär, Spionage- u. Terrorismusbekämpfung</td>
</tr>
<tr>
<td>Behörden/Unternehmen</td>
<td>FAR</td>
<td>Fingerbild, Gesicht, Handschrift, Stimme</td>
<td>gering-mittel</td>
<td>Finanzamt, Versicherungen, Vielflieger, Arbeitsstätte</td>
</tr>
<tr>
<td>Gesundheit</td>
<td>FRR</td>
<td>Fingerbild, Gesicht, Handschrift</td>
<td>Pilotprojekte</td>
<td>Krankenkassen, Ärzte, Apotheken</td>
</tr>
<tr>
<td>Telekommunikation</td>
<td>FRR</td>
<td>Fingerbild, Stimme</td>
<td>gering</td>
<td>Zugang zu mobilen Endgeräten</td>
</tr>
<tr>
<td>privater Raum</td>
<td>FRR</td>
<td>Fingerbild, Gesicht, Handschrift, Stimme</td>
<td>gering</td>
<td>Zugang zu Auto, Haus, PC</td>
</tr>
</tbody>
</table>

Quelle: Platanista 2001a
1.6 Internetanwendungen und das Problem der Referenzdaten

Bei der Diskussion über die Anwendungsmöglichkeiten biometrischer Verfahren wird regelmäßig auf das Internet, insbesondere auf E-Banking und E-Commerce, verwiesen (Kap. IV.1.4). Dagegen wird bei Einschätzungen und Stellungnahmen zu Sicherheitsproblemen im Internet und deren Lösungen das Thema Biometrie bislang kaum konkret angesprochen. Deshalb wurde die Platanista GmbH durch das TAB beauftragt, im Rahmen einer Kurzexpertise gezielt der Frage "Einsatz biometrischer Systeme zur Erhöhung der Sicherheit im Internet" nachzugehen. Die Recherchen bestätigten den Eindruck, dass das Thema bislang noch recht verhalten diskutiert wird, auch wenn gleichzeitig eine Vielzahl von Firmenaktivitäten erkennbar wurde.

Die Rechercheergebnisse der Platanista GmbH (2001b), v.a. in Form von Projekt- und Produktbeschreibungen, werden in Anhang 3 wiedergegeben bzw. zusammengefasst.

Ein recht weit entwickeltes und zunehmend erfolgreiches Produkt ist das Unterschriftenkennungssystem CyberSIGN, das in den USA u.a. im Gesundheitswesen (Patientendokumentierung, Auftrags- und Terminplanung in Krankenhäusern), als Zugriffsschutz für Regierungsdokumente (z.B. bei der Food and Drug Administration, FDA) und bei E-Banking und E-Commerce zur Authentifizierung eingesetzt wird (Platanista 2001b, S. 16).


Bei zukünftigen Internetanwendungen biometrischer Systeme stellen sich Fragen der Referenzdatenaufnahme, -übermittlung und -verwaltung besonders
intensiv. Schon in klassischen Filialbetrieben wie Banken und Sparkassen ist noch unklar, ob und wie flächendeckend die erforderlichen technischen und personellen Kapazitäten zum sicheren Enrolment (der Referenzdatenaufnahme, Kap. II.1) etabliert werden können oder ob den Kunden dabei zusätzliche und weitere Wege als bislang aufgebürdet werden müssen (Platanista 2001b, S. 17 f.).

Nach erfolgreicher Referenzdatenaufnahme schließen sich z.B. im Fall der Erstellung einer Smartcard (als dezentraler Datenspeicher in der Verfügungsgewalt der Nutzer) zwei weitere problematische Phasen an: zuerst der Transfer der Referenzdaten auf die Smartcard (bzw. den Ort der technischen Einrichtung, in der die Smartcards produziert werden), danach die Auslieferung der Smartcards an die Kunden. In Deutschland schließen die Banken derzeit noch einen Direktversand aus, geeignete Lösungsmöglichkeiten werden noch gesucht (Stand Juni 2001; http://www.biotrust.de/WS050601.htm).


2. Markteinschätzung

Der Begriff "Einschätzung" (im Titel dieses Abschnitts) bezieht sich nicht nur auf die Zukunft, sondern charakterisiert auch die aktuelle Datenlage bei den wirtschaftlichen Kennziffern: Es gibt keine verlässlichen und damit aussage-

• Die Zahl der Firmen, die biometrische Systeme entwickeln/anbieten, betrug im Jahr 2000 ca. 200 (Lockie 2000) und dürfte inzwischen weiter zugenommen haben. Die dominierende Technologie (ca. 40 % der Unternehmen) sind die Fingerbildverfahren, gefolgt von Gesichts- und Sprechererkennung (je ca. 15 %), Unter/Handschrift und Handgeometrie. Bei Iris- und Retina-Scan gibt es nur wenige Anbieter. Sollte die Biometrie in eine fortgeschrittene Diffusionsphase eintreten, wird eine Reduktion der Firmenvielfalt durch Fusionen und Übernahmen erwartet.

• Auch bei den Markterlösen - mit von Quelle zu Quelle und Jahr zu Jahr sehr unterschiedlichen Angaben (Anhang 4, Abb. 10 u. 11) - führt die Fingerbilderkennung (bei steigender Tendenz, mit bis zu 50 % des Gesamtumsatzes) vor der Gesichtserfassung (zunehmende Tendenz) und der Handvermessung (abnehmend), es folgen die Merkmale Stimme (abnehmend), Iris/Retina (zunehmend) und Handschrift.

• Die Angaben zur Verteilung der Umsätze auf die verschiedenen Anwendungsfelder (Anhang 4, Abb. 12 u. 13) sind so widersprüchlich und unklar, dass keine Schlüsse aus ihnen gezogen werden können.

• Zur Verteilung der Umsätze auf Weltregionen findet sich - trotz vorhandener Unterschiede der Quellen bei den Einzelwerten - eine gemeinsame Grundeinschätzung (Anhang 4, Abb. 14 u. 15): Der Markt in Nordamerika dominiert ganz deutlich (60-70 % der weltweiten Umsätze), mit weitem Abstand folgt Europa (10-25 %), danach kommen Asien und Lateinamerika (jeweils 5-10 %).


---

2. Markteinschätzung


- **Daten** über Umsätze und deren Verteilung auf Technologien oder Anwendungsfelder für Deutschland fehlen völlig. Frost & Sullivan (1999 u. 2000a) verorten die Bundesrepublik als größten Markt innerhalb Europas, prognostizieren allerdings für die kommenden Jahre - bei insgesamt steigenden Werten - einen abnehmenden Umsatzanteil gegenüber anderen europäischen Ländern.


V. Verbraucherpolitik, Recht, Datenschutz


1. Verbraucherpolitische Anforderungen an die Biometrie


Die Ambivalenz von Technologien zeigt sich auch im Fall der Biometrie: Biometrische Verfahren können dank der Verwendung personengebundener Merkmale sicheres Erkennen und Identifizieren ermöglichen. Zugleich aber können sie zur Durchleuchtung und umfassenden Überwachung des Bürgers verwendet werden und zur Diskriminierung von Einzelnen oder Bevölkerungs-
gruppen führen. Sollen die Chancen der Biometrie genutzt und die Risiken beherrscht werden, so müssen Gestaltung und Anwendung biometrischer Systeme bestimmte Kriterien erfüllen. Dazu zählen vor allem:

- hohe Sicherheit,
- umfassende Vertrauenswürdigkeit,
- ausreichende Nutzerfreundlichkeit sowie
- weitgehende Sozialverträglichkeit.

Im Folgenden werden anhand dieser Kriterien einige der zentralen Forderungen des Verbraucherschutzes an biometrische Verfahren vorgestellt.

**Sicherheit**


Bei der Ausgestaltung der Sicherheit biometrischer Verfahren geht es übergreifend darum, jede Beschädigung der Menschenwürde, des Allgemeinen Persönlichkeitsrechts und speziell des Rechtes auf "informationelle Selbstbestimmung" zu verhindern. Diese grundsätzliche Perspektive wird weiter unten unter Aspekten des Datenschutzes genauer diskutiert (Kap. V.3). Im Folgenden geht es zunächst um Sicherheit im engeren Sinn, vor allem um die so genannte "Überwindungssicherheit".


Vertrauenswürdigkeit

Für die breite Akzeptanz biometrischer Verfahren ist entscheidend, dass alle Beteiligten sie als vertrauenswürdig einschätzen (Albrecht 2001, S. 46). Um eine möglichst große Vertrauenswürdigkeit zu erreichen, wird beispielsweise vorgeschlagen, Vertrauensinstanzen einzurichten, die - fachlich kompetent, unabhängig und neutral - ein im Zusammenwirken von Nutzern, Herstellern, Betreibern und Staat vereinbartes Sicherheitsniveau zuverlässig gewährleisten. Derartige Vertrauensinstanzen können etwa Zertifizierungsstellen sein, die

Grundsätzlich kommen auch Instanzen infrage, die in der Verantwortung der Anwender stehen - wie bereits bei E-Commerce-Anwendungen. So sind z.B. vier deutscher Großbanken zu gleichen Teilen an dem Hamburger Zertifizierungsunternehmen TC TrusT Center AG beteiligt. Das Eigeninteresse der Akteure ist evident, da für den elektronischen Geschäftsverkehr nicht nur sichere Datenübertragung und Gewissheit bezüglich der Identität der Geschäftspartner essentiell sind, sondern auch, dass Geschäftspartner der gleichen Instanz vertrauen.

Eine Voraussetzung für die Überprüfung und Zertifizierung biometrischer Systeme ist die Entwicklung zuverlässiger Evaluierungskriterien, anhand derer unterschiedliche Verfahren objektiv verglichen werden können, und zwar sowohl unter technischen als auch unter anwendungsbezogenen und rechtlichen Aspekten (Kap. III.1). Mit einem geeigneten und allgemein akzeptierten Kriterienkatalog würden Prüfung und Zertifizierung auf eine solide Basis gestellt; Anwender und Nutzer bekämen einen Leitfaden für die Auswahl eines sicheren Produktes an die Hand; zugleich würde ein Richtschnur für die Entwicklung sicherer, vertrauenswürdiger Systeme geboten. Damit solche Evaluierungskriterien breite Akzeptanz finden, sollten sie von anbieterunabhängigen Stellen entwickelt werden (Albrecht 2001, S. 48).

Nutzerfreundlichkeit

Ausreichende Nutzerfreundlichkeit biometrischer Verfahren setzt voraus, dass diese robust und alltagstauglich sind, d.h. im massenhaften Gebrauch über lange Zeit zuverlässig funktionieren. Um ausreichende Nutzerfreundlichkeit zu erzielen, müssen - so lässt sich aus Pilotprojekten und Befragungen schließen - folgende Kriterien berücksichtigt werden: Wichtig ist bereits die Art und Weise, wie der Benutzer beim ersten Kontakt mit dem Verfahren, dem so genannten Enrolment bzw. der Personalisierung, betreut wird. Ferner spielt die ergonomiche Gestaltung der Anwenderplätze eine ganz erhebliche Rolle. Die Systeme sollten individuell auf den Nutzer einzustellen sein und so auch körperliche Einschränkungen (wie Kleinwüchsigkeit, Rollstuhlgebundenheit, Blindheit etc.) berücksichtigen. Auch sollte das Erkennungsverfahren selbst möglichst einfach und bequem vonstatten gehen, natürlicher Körperhaltung
1. Verbraucherpolitische Anforderungen an die Biometrie


Sozialverträglichkeit


Es liegt auf der Hand, dass die Umsetzung solcher Forderungen sich hart mit den Bedingungen des Marktes stößt. Für die Betreiber würde dies erheblichen organisatorischen Mehraufwand und finanzielle Mehrbelastung bedeuten.

2. Elektronische Signaturen und Biometrie - rechtliche Aspekte

Während die technische Entwicklung der Biometrie voranschreitet, sind die rechtlichen Folgen ihres breiteren Einsatzes weitgehend ungeklärt. Wenig entwickelt ist auch noch die Diskussion der Frage, ob und wie das Recht durch Setzung geeigneter Rahmenbedingungen eine sichere und sozialverträgliche Entwicklung und Nutzung dieser Technik befördern könnte. Regelungen, die sich ausdrücklich mit dem Einsatz biometrischer Verfahren befassen, lagen in Deutschland bis vor kurzem nur hinsichtlich ihrer Verwendung im Rahmen elektronischer Signaturen vor. (Auf neuere Entwicklungen im Zusammenhang mit dem "Terrorismusbekämpfungsgesetz" wird in Kap. V.4 eingegangen.)

Europäische Signaturrichtlinie


Eine fortgeschrittene elektronische Signatur liegt nach Artikel 1 Ziff. 2 der Richtlinie vor, wenn folgende Anforderungen erfüllt sind: Sie

– ist ausschließlich dem Unterzeichner zugeordnet,
– ermöglicht eine eindeutige, zweifelsfreie Identifizierung,
2. Elektronische Signaturen und Biometrie - rechtliche Aspekte

– wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann,
– ist so mit Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.


Signaturgesetz


Verglichen mit dem alten, enthält das neue Gesetz Änderungen insbesondere hinsichtlich des Betriebes von Zertifizierungsstellen sowie der Anforderungen an die elektronische Signatur. Bei beiden Aspekten bezieht sich nicht das (bewusst technologieoffen gehaltene) Gesetz selbst, wohl aber die Begründung zum Gesetzesentwurf auf die mögliche Nutzung biometrischer Verfahren mit dem Ziel der Erhöhung der (Rechts-)Sicherheit im elektronischen Geschäftsverkehr.

Den Anforderungen und Rechtswirkungen, welche die Europäische Signaturrichtlinie mit der "fortgeschrittenen elektronischen Signatur" verbindet, kommt das Signaturgesetz mit den Regelungen zur "qualifizierten elektronischen Signatur" nach. Diese Regelungen implizieren ein bestimmtes Sicherheitsniveau. Um eine "Steigerung des Sicherheitsniveaus" zu ermöglichen und damit "das erforderliche Maß an Sicherheit, Qualität und Vertrauen zu erreichen" (Bundesregierung 2000a, S. 27), eröffnet das Gesetz die Option der "qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung" (§ 15 Abs. 1 Satz 4 SigG). Danach können Anbieter von Zertifizierungsdiensten sich bei der
zuständigen Behörde "akkreditieren", d.h. in Bezug auf die technische und administrative Sicherheit ihrer Arbeit und ihrer Produkte umfassend prüfen und bestätigen lassen. Ein Gütezeichen bringt den "Nachweis" der Sicherheit zum Ausdruck.

Dementsprechend wird in § 15 Abs. 1 Satz 5 SigG den akkreditierten Zertifizierungsstellen erlaubt, "sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit" ihrer Produkte zu berufen. In der Begründung zum Gesetzentwurf heißt es dazu, mit der Feststellung des erbrachten "Nachweises" trete "eine objektive Beschreibung der Sicherheit" an die Stelle der Sicherheitsvermutung in § 1 Abs. 1 SigG 1997. Damit sei zu erwarten, dass der qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung vor Gericht ein besonders hoher Beweiswert zukommen werde, der "im Ergebnis als eine Art 'Sicherheitsvermutung' gewertet werden" könne. An der bisherigen Rechtslage ändere sich somit nichts (Bundesregierung 2000a, S. 28).

Im Fortgang der Begründung kommt u.a. die Frage der sicheren Autorisierung der Signatur zur Sprache. Aufgrund der in Signaturgesetz und -verordnung vorgesehenen Vorkehrungen sei zu vermuten, "dass der im qualifizierten Zertifikat benannte Signaturschlüssel-Inhaber die Signatur erzeugt oder die Erzeugung autorisiert hat, soweit im Einzelfall nicht andere Fakten entgegenstehen". In diesem Zusammenhang wird auf den Einsatz biometrischer Systeme zur Erhöhung der Sicherheit Bezug genommen: "Die mögliche Autorisierung einer anderen Person (z.B. durch Weitergabe der sicheren Signaturerstellungseinheit und PIN) kann ausgeschlossen werden, indem die Signaturerstellungseinheit über die Nutzung biometrischer Merkmale ausschließlich an eine Person gebunden wird" (Bundesregierung 2000a, S. 28).

In § 17 befasst sich das Signaturgesetz mit Produkten für "qualifizierte elektronische Signaturen", speziell mit dem Schutz des Schlüssel-Mechanismus. Vorgeschrieben wird, "sichere Signaturerstellungseinheiten" einzusetzen, die "gegen unberechtigte Nutzung der Signaturschlüssel schützen" (Abs. 1). Technische Komponenten für die Produktion sicherer Signaturerstellungseinheiten müssen so beschaffen sein, dass sie bei der Erzeugung und Übertragung von Signaturschlüsseln deren "Einmaligkeit und Geheimhaltung" gewährleisten und eine Speicherung außerhalb der Signaturerstellungseinheit ausschließen (Abs. 3 Nr. 1). In der Begründung zu § 17 Abs. 1 wird darauf hingewiesen, dass biometrische Merkmale verwendet werden können, um "einer Nutzung von sicheren Signaturerstellungseinheiten durch Unbefugte wirksam vorzubeugen". Deshalb sei die Vorschrift "für die Nutzung biometrischer Merkmale Entwicklungsoffen" (Bundesregierung 2000a, S. 30).
Die damit eröffnete Möglichkeit wird in der Verordnung zum Signaturgesetz aufgegriffen und genauer umrissen.

Verordnung zur elektronischen Signatur

In der Neufassung der "Verordnung zur elektronischen Signatur" (SigV) vom November 2001 werden u.a. die Anforderungen an die technischen Komponenten zur Erzeugung und Prüfung von Signaturschlüsseln näher ausgeführt. § 15 SigV regelt die Erzeugung und Prüfung "qualifizierter elektronischer Signaturen". Er zielt darauf ab, durch technische Anforderungen einen sicheren Nachweis der Integrität elektronisch signierter Dateien sowie der Identität und Berechtigung des Signierenden zu gewährleisten. Hierzu können biometrische Verfahren eingesetzt werden. Dazu heißt es in § 15 Abs. 1 Satz 1 SigV: "Sichere Signaturerstellungseinheiten [...] müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann." Damit wird die Identifikation anhand biometrischer Merkmale alternativ zur Identifikation aufgrund von Wissen ermöglicht. In der Begründung zum Entwurf hieß es hierzu, dies schaffe einen "Anreiz für entsprechende innovative Lösungen" ("Begründung zur Verordnung zur elektronischen Signatur [Entwurf]" vom 16.08.2001).

In § 15 Abs. 1 Satz 1 und 2 der SigV wird speziell für die Nutzung biometrischer Merkmale ein bestimmtes Sicherheitsniveau vorgegeben: Es müsse hierbei "hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist, und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein".

Das "Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr" (Formgesetz) trat im Juli 2001 in Kraft. Mit diesem Gesetz wird - der europäischen Signaturrichtlinie Rechnung tragend - die "qualifizierte elektronische Signatur" wie eine handschriftliche Signatur als formgebundene Erklärung anerkannt (§ 126a BGB). Dadurch ist es möglich, rechtsverbindliche, zuvor an die herkömmliche Schriftform gebundene Erklärungen grundsätzlich auch in elektronischer Form abzugeben.

Mit § 292a des Gesetzes wird in die Zivilprozessordnung (ZPO) eine Beweisregel eingeführt, die an die "qualifizierte elektronische Signatur" anknüpft: "Der Anschein der Echtheit einer in elektronischer Form (§ 126a des Bürgerlichen Gesetzbuches) vorliegenden Willenserklärung, der sich aufgrund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernsthafte Zweifel daran begründen, dass die Erklärung mit dem Willen des Signatschlüssel-Inhabers abgegeben worden ist."

beruhen, die von einer Zertifizierung nicht mit umfasst werden kann. Dies gelte jedenfalls so lange, wie bloß auf die Person bezogene und daher von jedem unberechtigten Dritten verwendbare Nachweise einer Zugangsberechtigung wie Persönliche Identifikationsnummern zum Einsatz kommen.


Hohe, "nachgewiesene Sicherheit" - so die Kritik (am damaligen Entwurf) - gewährleiste nur die "qualifizierte elektronische Signatur mit Anbieter-Akkreditierung", wie sie von der übergeordneten Behörde "akkreditierten" und mit "Gütezeichen" versehenen Zertifizierungsstellen angeboten werde. Allenfalls an diese Signatur könne der Anscheinsbeweis anknüpfen, den § 292a des Formgesetzes an die "qualifizierte elektronische Signatur" anschließe.


Die Praxis wird zeigen, ob dieser Rechtsrahmen ausreicht oder ob vorgetragene Bedenken sich als gerechtfertigt erweisen.

### 3. Datenschutz


Um biometrische Verfahren datenschutzrechtlich beurteilen zu können, ist zum einen eine Betrachtung des Gesamtsystems notwendig, die sowohl technische Aspekte der einzelnen biometrischen Verfahren als auch die konkreten Rahmen-

- **Zur Betrachtung und Beurteilung des Gesamtsystems** gehört ein Blick auf die Art der verwendeten Daten, die Weise ihrer Erhebung, die Spezifika ihrer Verarbeitung sowie die technische Sicherheit und Zuverlässigkeit des Verfahrens insgesamt. Diese umfassende Perspektive ist notwendig, weil sich auf jeder Stufe eines biometrischen Verfahrens Sicherheitsrisiken und Gefährdungen von Rechten ergeben, denen aber auch mit entsprechenden technischen und organisatorischen Maßnahmen begegnet werden kann.


  Insofern biometrische Verfahren auf persönliche körperliche Merkmale zurückgreifen, sind bei ihrer Verwendung **Grundrechte** in ganz besonderer Weise **berührt**. Fragen des Datenschutzes stellen sich speziell und verschärft. Über das Datenschutzrecht hinaus kommen als Maßgaben für die Beurteilung biometrischer Verfahren das Allgemeine Persönlichkeitsrecht und die verfassungsrechtlich besonders geschützte Menschenwürde in Betracht. Ergänzend sollte zur Orientierung die EG-Datenschutzrichtlinie herangezogen werden.

### 3.1 Biometrische Daten als personenbezogene Daten

Das Bundesdatenschutzgesetz sieht den Schutz "personenbezogener Daten" vor. Solche Daten sind im Sinne des Gesetzes dann gegeben, wenn sich "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmmbaren natürlichen Person" zuordnen lassen (§ 3 Abs. 1 BDSG). Ob das der Fall ist, ergibt sich aus dem jeweiligen Kontext: vor allem daraus, ob die
3. Datenschutz


Grundsätzlich generieren Verfahren, die für den Abgleich biometrische Rohdaten verwenden, eher personenbezogene Daten als solche, die mit Templates oder gar templatefrei arbeiten (ULD-SH 2001, S. 15 ff.). Vorgesehen ist der Rückgriff auf Rohdaten häufig bei Gesichtserkennungsverfahren. Da diese an ein im Prinzip für jedermann offen liegendes Merkmal anknüpfen, ist nicht auszuschließen, dass die Daten sich einer bestimmten Person unmittelbar zuordnen lassen. Damit dürften sie in aller Regel als personenbezogene Daten gelten. Bei Rohdaten, die an weniger offen liegende Merkmale, wie z.B. Fingerabdrücke, anknüpfen, wird es im Allgemeinen nicht möglich sein, sie einer bestimmten Person unmittelbar zuzuordnen. Um diese Daten zu personenbezogenen zu machen, müssten sie erst mit anderen Informationen, wie z.B. Name oder Adresse, verbunden werden.

Die aus Rohdaten erzeugten Templatedaten ergeben erst recht nur dann personenbezogene Daten, wenn sie mit geeigneten zusätzlichen Informationen verknüpft werden. Das können zum einen herkömmliche Informationen wie Name oder Adresse sein, zum anderen weitere, aus anderen Rohdaten errechnete Templates. Die Möglichkeiten, Templates unterschiedlicher Provenienz zusammenzuführen, sind zur Zeit noch erheblich eingeschränkt. Datenformate und Algorithmen sind zumeist privates Eigentum, weder offengelegt noch kompatibel. Auf der Ebene der Algorithmen allerdings lassen sich Standardisierungen, die Templates vergleichbar machen, absehen.

Nicht unwichtig für mögliche datenschutzrechtliche Probleme ist die Frage der Vielfalt und Kompatibilität der Systeme. In manchen Bereichen ist damit zu rechnen, dass ein bestimmtes Verfahren sich marktberechtigend durchsetzt. Sollte beispielsweise ein einheitliches System im Bereich der Geldautomaten installiert werden, so wäre ein großer Teil der bundesdeutschen Bevölkerung davon betroffen. In Fällen wie diesen dürfte es nicht allzu schwierig sein, Templates (oder Templates und Rohdaten) so zusammenzuführen, dass sich ein Personenbezug ergibt.

Solche Gefährdungen lassen sich mit templatefreien Verfahren, wie sie zur anonymen und pseudonymen Authentifizierung verwendet werden, vermeiden. In beiden Verwendungen dienen biometrische Daten der sicheren Verschlüs-

**Sensitive Daten**

Im Zusammenhang mit Daten in biometrischen Verfahren ist speziell § 3 Abs. 9 BDSG von Interesse, der in Anlehnung an Art. 8 der EG-Datenschutzrichtlinie "besondere Arten personenbezogener Daten" benennt. Unter diesen Begriff fallen "Angaben über rassische und ethnische Herkunft, über politische Meinungen, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben". Solche "besonderen" oder sensiblen Daten dürfen nur ausnahmsweise erhoben werden und stehen damit unter erhöhtem Schutz.


Nun ist offensichtlich, dass zahlreiche Allerweltsdaten zu den besonders geschützten Daten gehören. Das Portraitfoto eines Betroffenen enthält Informationen über seine rassische Herkunft; oft kann schon der Name Aufschluss über die ethnische Herkunft geben. Um die Geltung des erhöhten Schutzniveaus sinnvoll zu begrenzen, nennt § 13 Abs. 2 Nr. 1-9 BDSG **für den öffentlichen Bereich** eine Reihe von Bedingungen und Zwecken, unter bzw. zu denen sensible Daten eben doch erhoben und verarbeitet werden dürfen. Beispielsweise ist die Datenerhebung zulässig, soweit dies "zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung [...] erforderlich ist" und die Verarbeitung der Daten durch Personen erfolgt, "die einer entsprechenden Geheimhaltungspflicht unterliegen" (§ 13 Abs. 2 Nr. 7 BDSG). Als zulässig gilt die Datenerhebung auch, soweit dies "zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist" (§ 13 Abs. 2 Nr. 6 BDSG).

**Für den nicht-öffentlichen Bereich** sind die Ausnahmen von der prinzipiellen Unterschutzstellung sensibler Daten in § 28 Abs. 6 Nr. 1-4 BDSG geregelt.
3. Datenschutz

3.2 Grundrechtsbezug biometrischer Daten und Verfahren

Datenverarbeitung mittels biometrischer Verfahren greift in einen speziellen Aspekt des Allgemeinen Persönlichkeitsrechts ein: das Recht auf informationelle Selbstbestimmung. Darüber hinaus betrifft sie u.U. weitere Aspekte des Allgemeinen Persönlichkeitsrechts, wie es in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umrissen ist. Auch die Menschenwürde als herausragendes Schutzgut kann betroffen sein.

Menschenwürde


**Allgemeines Persönlichkeitsrecht**


### 3.3 Folgerungen für rechtliche Regelungen und die Praxis biometrischer Verfahren

Soweit mithilfe biometrischer Verfahren personenbezogene Daten erzeugt werden, unterliegen diese Verfahren den Regelungen des allgemeinen Datenschutzes. Das gilt sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich.
Für den öffentlichen Bereich sind darüber hinaus spezielle, bereichsspezifische (auf den jeweiligen Anwendungsbereich bezogene) Regelungen erforderlich.

*(Gesetzliche) Grundlagen*


Teilt man die Einschätzung, dass biometrische Verfahren u.U. über den Bereich des Rechtes auf informationelle Selbstbestimmung hinaus in einen weiteren Bereich des Allgemeinen Persönlichkeitsrechts eingreifen, so folgt daraus, dass die bestehenden gesetzlichen Erlaubnisse zur Datenverarbeitung diesen weiter gehenden Eingriff nicht abdecken. Das heißt in der Konsequenz, dass für die
Implementierung biometrischer Komponenten in staatliche Verfahren


Eingriffsintensität und Systemdatenschutz

Ob und wieweit eine bestimmte Praxis des Einsatzes biometrischer Verfahren datenschutzrechtlichen Vorgaben genügt, hängt grundlegend ab von der Intensität, mit der das verwendete Verfahren den geschützten Bereich des Persönlichkeitsrechts berührt oder in ihn eingreift (ULD-SH 2001, S. 35). Dies wird im Wesentlichen von drei Momenten bestimmt: Entscheidend ist erstens, in welchem Umfang personenbezogene Daten erhoben und verarbeitet werden, zum zweiten, wie aufwendig es ist, einen Bezug zwischen erhobenen Daten und betroffener Person herzustellen, und zum dritten, welcher Grad der Mitwirkung am Geschehen vom Betroffenen verlangt bzw. ihm zugestanden wird. In allen drei Punkten macht das Datenschutzgesetz Vorgaben, die als Richtschnur für möglichst eingriffsarme Verfahren gelten können:

- Grundsätzlich sind Daten offen zu erheben, unmittelbar beim Betroffenen, unter seiner Mitwirkung und mit seiner Unterrichtung bzw. seiner Kenntnis u.a. bezüglich der Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung (§ 4 Abs. 2 u. 3 BDSG). Unter diesem Gesichtspunkt sind Verfahren, die einen hohen Grad der Mitwirkung bezüglich der Erfassung der Rohdaten verlangen, solchen, die weniger beteiligen oder gar unbemerkt arbeiten, vorzuziehen.
- Gefordert ist unter dem Stichwort "Datenvermeidung und Datensparsamkeit", schon bei der Auswahl und Gestaltung eines Datenverarbeitungssystems darauf zu achten, dass keine bzw. möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden (§ 3a BDSG).

Aktive Mitwirkung des Betroffenen, sparsame Erhebung und Verwendung von Daten sowie technikbedingt hohe Sicherheit in der Vermeidung von Personenbezug: Damit sind wichtige Komponenten eines Systemdatenschutzes als (materielle) Grundlage effektiven Datenschutzes benannt. Entscheidend dazu


4. Das Terrorismusbekämpfungsge setz


Ein zukünftiges "besonderes Bundesgesetz" wird diese Vorgaben konkretisieren: Zu regeln sind die "Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form [...]

93
sowie die Art der Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung" (§ 4 Abs. 4 PassG neu, § 1 Abs. 5 PersAuswG neu).

Den Anforderungen des Datenschutzes entsprechen die Neuregelungen in Pass- und Personalausweisgesetz durch die Benennung der Zweckbindung der entstehenden Daten sowie die Normierung der Auskunftsrechte der Betroffenen (§ 16 Abs. 6 PassG neu, § 3 Abs. 5 PersAuswG neu).

Im **Ausländergesetz** (AuslG) wird die Nutzung biometrischer Merkmale in der oben genannten Art und Weise ebenfalls als Möglichkeit eröffnet. Vor allem die Aufenthaltsgenehmigung, aber auch der Ausweisersatz, die Bescheinigung über die Duldung und die "Bescheinigung über die Wirkung [...] [der] Antragsstellung (Fiktionsbescheinigung)" können künftig biometrische Merkmale von Fingern oder Händen oder Gesicht enthalten (§ 5 Abs. 4, § 39 Abs. 1, § 56a, § 69 Abs. 2 AuslG neu). Damit sollen Fälschung und Missbrauch von Dokumenten effektiv verhindert und insgesamt die "Möglichkeiten der Identitätssicherung" erweitert und verbessert werden (Begründung zum Terrorismusbekämpfungsgesetz; SPD/Bündnis 90/Die Grünen 2001, S. 53 u. 36).

Die konkrete Ausgestaltung der so eröffneten Möglichkeiten liegt beim Bundesministerium des Innern und erfolgt durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf (§ 5 Abs. 6, § 39 Abs. 1, § 56a, § 69 Abs. 2 AuslG neu).

Mit dem "Terrorismusbekämpfungsgesetz" hat der Gesetzgeber eine eigene Entscheidung hinsichtlich der Erforderlichkeit und Angemessenheit der Nutzung biometrischer Daten in bestimmten staatlichen Verfahren getroffen. Entsprechend der Rechtsprechung des BVerfG zum informationellen Selbstbestimmungsrecht ist eine **parlamentsgesetzliche Grundlage** geschaffen worden, aus der (auch für den Bürger) Voraussetzungen, Ziel und Umfang des Eingriffes in dieses Recht klar hervorgehen:

- Die zu nutzenden biometrischen Merkmale werden alternativ explizit genannt.
- Der Zweck der gespeicherten Daten ist ausdrücklich bestimmt.
4. Das Terrorismusbekämpfungsgesetz

_Gesetzliche Regelung der Nutzung der Biometrie im Passgesetz, im Gesetz über Personalausweise und im Ausländergesetz_

Das **PassG** wurde durch die Aufnahme folgender Bestimmungen in §§ 4 und 16 (das **PersAuswG** durch Aufnahme der §§ 1 und 3 gleichlautend) wie folgt geändert:

"Der Pass darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. […]

Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form […] sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet."

[…] "Im Pass enthaltene verschlüsselte Merkmale und Angaben dürfen nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Passinhabers ausgelesen und verwendet werden. Auf Verlangen hat die Passbehörde dem Passinhaber Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben zu erteilen."

Das **Ausländergesetz** wurde u.a. durch Einfügungen in § 5 wie folgt geändert:

"Die Aufenthaltsgenehmigung kann neben dem Lichtbild und der eigenhändigen Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Inhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in die Aufenthaltsgenehmigung eingebracht werden."

[…] "Vordruckmuster und Ausstellungsmodalitäten, ihre Einzelheiten sowie ihre Aufnahme und die Einbringung von Merkmalen in verschlüsselter Form bestimmt das Bundesministerium des Innern nach Maßgabe der gemeinschaftsrechtlichen Regelungen durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf."
VI. Perspektiven der weiteren Entwicklung - Forschungs- und Handlungsbedarf


Dem explorativen Charakter der "Vorbereitenden Untersuchung" entsprechend, können die Ergebnisse nur vorläufig sein, zumal sich im Verlauf des Vorhabens gezeigt hat, wie dynamisch sich nicht nur die technologischen, sondern auch die gesellschaftlichen Rahmenbedingungen ändern.

Einige Thesen zu den Perspektiven der Biometrie

Trotz vieler Unsicherheiten insbesondere bei den Rahmenbedingungen ist zu vermuten, dass sich biometrische Systeme und Verfahren weltweit in einer entscheidenden Phase der Diffusion befinden. Nachdem sie lange Zeit vor allem als Zugangssicherung in sicherheitskritischen Bereichen wie Gefängnissen, Kraftwerken oder Rechenzentren zum Einsatz kamen, lassen nun zahlreiche Hinweise ihre Expansion in weitere öffentliche und private Anwendungsfelder erwarten.

– Das Nachfragepotenzial ist seit jeher als immens eingeschätzt worden. Sinnvolle (oder als sinnvoll wahrgenommene) Applikationen sind aber über
lange Zeit nicht in ausreichend großer Zahl vorhanden gewesen. Zudem waren biometrische Systeme technisch anfällig und hochpreisig, so dass sie an der Schwelle der Märkte verblieben. Mittlerweile stellt sich das Angebot preisgünstiger und qualitativ verbessert dar, so dass die Nachfrage besser stimuliert und befriedigt werden kann.


– Die geltenden rechtlichen Rahmenbedingungen (insbesondere SigG und SigV) eröffnen der Biometrie im Bereich elektronisch getätiger Transaktionen und Rechtsgeschäfte einen riesigen Markt. Durch das "Terrorismusbekämpfungsgesetz" ist die Tür zum Markt der Sicherheitstechnologien weiter geöffnet worden. Sollte in Deutschland (und Europa) durch staatliche Verfahren ein Masseneinsatz von biometrischen Systemen angestoßen werden, so würde dies - allen Regeln technologischer Innovationen zufolge - Signalwirkungen für und Auswirkung auf andere Anwendungsfelder in der Wirtschaft und im privaten Bereich haben.

Handlungs- und Forschungsbedarf

Biometrische Verfahren im öffentlichen wie im nicht-öffentlichen Bereich sollten durch gemeinsame Anstrengungen aller Beteiligten so gestaltet werden, dass sie als sicher, vertrauenswürdig, nutzerfreundlich und sozialverträglich gelten können. Handlungsbedarf zeichnet sich hierbei auf verschiedenen Ebenen ab.

Beurteilung der Leistungsfähigkeit biometrischer Systeme und Verfahren

Die Leistungsfähigkeit verfügbarer biometrischer Systeme ist auf der Basis der - oftmals äußerst widersprüchlichen - Informationen, die für den vorliegenden Bericht erhoben werden konnten, nicht seriös einzuschätzen. Für Verwirrung sorgt häufig die unschärfte Trennung zwischen möglichem Potenzial und augenblicklicher tatsächlicher Kapazität.


Trotz erkennbarer Verbesserungen und sicherlich weiter zunehmender technischer Fortschritte ist daher Berichten und Einschätzungen über mittlerweile erreichte hohe Standards bei Genauigkeit und Zuverlässigkeit biometrischer Systeme nach wie vor mit Skepsis zu begegnen.

Insbesondere dann, wenn es um einen weiträumigenden, große Nutzergruppen - ob freiwillig oder verpflichtend - einbeziehenden Einsatz biometrischer Systeme geht, z.B. im Rahmen der Ausrüstung von Ausweispapieren, müssen höchste Ansprüche an eine substantiierte Evaluation der infrage kommenden
VI. Forschungs- und Handlungsbedarf

Systeme gestellt werden. Eine regelmäßige Berichterstattung zum Stand der laufenden Pilotprojekte und der (internationalen) Standardisierungsbestrebungen wäre als Basis für die weitere politische Behandlung des gesamten Themenkomplexes sicherlich nützlich. Eine sinnvolle Ergänzung zu laufenden Aktivitäten könnten Projekte und Verfahren der Technikfolgen-Abschätzung bieten (s.u.).

Beobachtung und Erhebung des Marktgeschehens

Vorliegende Daten und Berichte zum Einsatz biometrischer Systeme wirken häufig sehr punktuell und zufällig. In der Regel sind sie wenig transparent, auf keinen Fall geben sie ein vollständiges Bild. Der Stand der Diffusion, der Umsätze und der Marktanteile (national wie international) bleibt äußerst unscharf.


Im Hinblick auf eine mögliche gezieltere Förderung im Bereich Biometrie wären genauere Daten mit Sicherheit vonnöten. Voraussetzung hierfür wäre allerdings die Entwicklung von Konzepten und Methoden zur besseren Erfassung relevanter wirtschaftlicher Kennziffern, differenziert nach eigenem biometrischen System, peripheren Geräten und der Art und des Umfangs der Anwendung.

Expertendiskurs Biometrie

Eine substanzielle Verbesserung der Informationslage, die gerade angesichts anstehender politischer Entscheidungen zum Einsatz biometrischer Systeme als Folge des "Terrorismusbekämpfungsgesetzes" erforderlich wäre, wird nicht leicht zu erreichen sein. Prägend für die Debatte zur Biometrie ist die geringe Zahl an Experten, die fast immer auch Entwickler sind und sich verständ-
licherweise in diesem jungen, dynamischen Technologiebereich positionieren möchten.

In Ergänzung zu Formen der Sachstandserhebung durch Gutachten oder in Anhörungen könnte die Möglichkeit moderierter Expertenrunden (Stakeholder Workshops) ins Auge gefasst werden, zunächst zu grundsätzlichen Fragen:

– Wie praxistauglich sind die einzelnen biometrische Systeme?
– Was können sie in den verschiedenen Kontexten und hinsichtlich der gewünschten Funktion leisten?

Aufgabe wäre die Erarbeitung gemeinsamer Stellungnahmen, auf die sich Entwickler, Anbieter, regulierende Instanzen, Daten- und Verbraucherschützer einigen sollten, um so die jeweiligen partikulären Perspektiven zu überwinden. Eine enge Anbindung an die Fragestellungen und Entscheidungsnotwendigkeiten der Politik sollte darüber hinaus gewährleistet werden. Hierdurch könnte zum einen deren Informationsbedürfnis klarer herausgearbeitet und direkt in die Expertenrunde hineintransportiert werden, zum andern hätten die Entwickler die Möglichkeit, ihre Erwartungen an die Politik zu verdeutlichen sowie Problemlösungen proaktiv anzubieten.

Aus Sicht der Politik könnte der Expertendiskurs Fingerzeige für Handlungs- und Gestaltungsbedarf liefern, beispielsweise, ob eine stärkere und zielorientiertere Förderung von Forschung, Entwicklung und Pilotprojekten durch BMBF und BMWi erfolgen sollte oder ob Impulse für die Standardisierung der biometrischen Systeme sowie die Vereinheitlichung der Evaluationsverfahren gegeben werden sollten.

**Technikfolgen-Abschätzung Biometrie**

VI. Forschungs- und Handlungsbedarf

Verbraucherschutz


Datenschutz


Eine Konsequenz daraus sollte sein, dass Biometrie in verpflichtend vorgeschriebenen staatlichen Verfahren so zurückhaltend wie möglich angewandt wird. Wird ihr Einsatz als erforderlich und angemessen angesehen, sollte durch entsprechende Technik- und Verfahrensgestaltung sichergestellt werden, dass
VI. Forschungs- und Handlungsbedarf


Biometrische Daten bei der Strafverfolgung


Rechtliche Perspektiven der Technikgestaltung

Mit dem "Terrorismusbekämpfungsgesetz" als gesetzliche Grundlage ist auf breiter Basis die Möglichkeit der Nutzung biometrischer Verfahren eröffnet
worden. Die begonnene Diskussion sollte verstärkt weitergeführt werden. Drei Aspekte seien hierzu genannt:

– Nicht ganz zu überzeugen vermag der Umstand, dass der Gesetzgeber bei den jüngst erfolgten Änderungen im Ausländergesetz andere rechtliche Maßstäbe als im Pass- bzw. Personalausweisgesetz in Bezug auf deutsche Staatsbürger angelegt hat. Hier ist weiterer Diskussions- und Forschungsbedarf nicht zu übersehen, der sich über diese Frage hinaus auch auf die Anforderungen an ein zukünftiges Bundesgesetz zur Biometrie erstreckt.


– In nächster Zeit besonders diskussionswürdig erscheint die mögliche Koppelung von Videoüberwachung und biometrischen Erkennungssystemen. Neben der Tauglichkeit solcher Systeme wären hier auch Rechtsfragen zu prüfen, u.a. deshalb, weil z.B. bei einer Anwendung auf einem Flughafengelände im Passagierbereich die Grenzen zwischen staatlicher Nutzung (Sicherheitsbehörden) und privater Nutzung (Flughafenbetriebsgesellschaft, Stichwort "Passagierlenkung") nicht ganz einfach zu ziehen sind.

Spezifische Rechtsfragen

Die rechtlichen Implikationen der Biometrie sind heute noch weitgehend unklar, eine entsprechende Literatur ist nicht oder kaum vorhanden. Über die genannten rechtlichen Fragen hinaus dürften zahlreiche Einzelaspekte aus juristischer Sicht von hoher Relevanz sein. An dieser Stelle soll exemplarisch nur das Thema "Rechtsfragen der Biometrie am Arbeitsplatz" genannt werden.
Literatur

1. Vergebene Gutachten

ALBRECHT, A. (2001): Stand der verbraucherpolitischen Diskussion zu biometrischen Erkennungsverfahren unter Berücksichtigung der Situation in den USA. Arbeitsgemeinschaft der Verbraucherverbände (AgV e.V.), Bonn


2. Weitere Literatur


BUNDESREGIERUNG (1999): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Angela Marquardt, Dr. Heinrich Fink und der Fraktion der PDS - Drucksache 14/1226 - Förderung biometrischer Verfahren und ihrer datenschutzrechtlichen Begleitung durch die Bundesregierung. Deutscher Bundestag, Drucksache 14/1405, Bonn


FROST & SULLIVAN (2000b): Report 3584 (11/00)


2. Weitere Literatur


MORGAN KEEGAN (Hg.) (2000): Equity Research 08/2000

NEWHAM et al. (1999): The Biometrics Report 1999. SJB Services, Somerset


SPD, BÜNDNIS 90/DIE GRÜNEN (2001): Gesetzentwurf der Fraktionen SPD und Bündnis 90/Die Grünen - Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz). Deutscher Bundestag, Drucksache 14/7386 (neu), Berlin


Anhang

1. Tabellenverzeichnis

Tab. 1: Derzeit vorrangig genutzte "biometrische Merkmale" des Menschen....... 18
Tab. 2: Technische Angaben zu biometrischen Systemen/Verfahren..................... 37
Tab. 3: Vorzüge und Nachteile biometrischer Verfahren/Systeme......................... 38
Tab. 4: Bewertung biometrischer Verfahren nach Jain et al. 1999.......................... 39
Tab. 5: Bewertung biometrischer Verfahren nach Scheuermann et al. 2000........... 39
Tab. 6: Öffentliche Forschungsaktivitäten zur Biometrie in Deutschland .............. 51
Tab. 7: Industrielle FuE/Beratung zum Thema Biometrie in Deutschland............... 52
Tab. 8: Exemplarische internationale Forschungsstandorte und -themen ............... 56
Tab. 9: Laufende Biometrie-Projekte im Rahmen des IST-Programms der EU.......... 57
Tab. 10: Biometrische Verfahren in der Praxis ................................................... 69

2. Abbildungsverzeichnis

Abb. 1: Gewinnung des Minuzienbildes bei der Fingerbilderkennung ................. 24
Abb. 2: Erfassen der Handgeometrie................................................................. 27
Abb. 3: Iris-Muster ............................................................................................ 28
Abb. 4: Iris mit Iris-Code ............................................................................... 29
Abb. 5: Infrarot-belichtete Retina ................................................................. 30
Abb. 6: Einzelbilder der Eigengesichtstechnik .................................................. 32
Abb. 7: Thermogramm eines Gesichts............................................................. 33
Abb. 8: Online-Handsschriften ("Haus von Nikolaus" und vorgegebener Schriftzug) ................................................................................................................. 34
Abb. 9: Zahl der Firmen nach biometrischen Erkennungssystemen ................. 113
Abb. 10: Marktverteilung biometrischer Systeme (1999) weltweit, nach IBG ...... 113
Abb. 11: Marktverteilung biometrischer Systeme weltweit, nach Lockie .......... 114
Abb. 12: Umsatzverteilung biometrischer Systeme nach Anwendungsfeldern ...... 115
Abb. 14: Regionale Umsatzverteilung biometrischer Systeme, nach Lockie ...... 117
Abb. 15: Regionale Umsatzverteilung biometr. Systeme, nach Frost & Sullivan... 117
3. Biometrie und Internet - Projekte und Produkte


- **E-Contract** und **Triton Secure - Zeitfassung** durch Fingerbilderkennung: Die Firma E-Contract nutzt das Fingerbildsystem SAFESITE der Firma
3. Biometrie und Internet - Projekte und Produkte

Triton Secure zur Arbeitszeiterfassung ihrer Vertragsarbeiter. E-Contract "Vertragsfirmen" können auf das Online-Timesheet zugreifen und dieses verwalten. (http://www.tritonsecure.com)


- **Keyware Technologies**: Zugangskontrolle, Webseiteabsicherung mit Fingerabdruck, Spracherkennung, Iriserkennung (http://www.keyware.com)
- **SecuGen**: Onlinebanking mit Fingerabdruck (http://www.secugen.com)
- **Iridian**: Onlinebanking, E-Commerce mit Iris-Scan. (http://www.iriscan.com)
- **SAFLINK Corporation**: Onlinebanking, E-Commerce mit multimodalen Systemen (http://www.saflink.com)
- **Alpha Net Online GmbH**: E-Commerce mit Fingerabdruck (http://www.alphanet.de)
- **Identification Systems Dermalog**: E-Commerce mit Fingerabdruck (http://www.dermalog.de)
- **DCS - BioID**: Onlinebanking, Videokonferenz mit multimodal System (http://www.bioid.com)
- **Identix - BioLogon**: Netzzugriffsschutz, Fingerabdruck (http://www.identix.com)
Anhang

- **Visionics Corporation**: Onlinebanking, E-Commerce mit Gesichtserkennung (http://www.visionics.com)
- **NUANCE Communications**: Telefonbanking mit Stimmerkennung (http://www.nuance.com)
- **Miros**: Onlinebanking, Netzzugriffsschutz (z.B. im Gesundheitswesen) mit Fingerabdruck und Gesichtserkennung (http://www.miros.com)
- **LCI Smartpen**: E-Commerce mit Unterschriftenerkennung (http://www.smartpen.net)
- **Viisage Technology Inc.**: E-Commerce mit Gesichtserkennung (http://www.viisage.com)

4. Marktabschätzungen zur Biometrie


- Die **Zahl der Firmen**, die biometrische Systeme entwickeln/anbieten, beträgt ca. 200 (Lockie 2000); ihre **Aufteilung nach einzelnen Systemtypen** (Fingerbild, Gesicht, Hand, Schrift, Stimme, Auge und übrige) zeigt **Abbildung 9** (Frost & Sullivan 1999; damals ausgehend von 177 Firmen). Es dominieren klar die Fingerbildverfahren (fast 40%), quantitativ das Schlusslicht bilden mit weniger als 3% (5 Firmen) die "Augenverfahren" Iris- bzw. Retina-Scan, was vermutlich auf die Komplexität der Technologie zurückzuführen ist. Sollte die Biometrie in eine fortgeschrittene Diffusionsphase eintreten, wird eine "Marktbereinigung" der Firmenvielfalt durch Fusionen und Übernahmen erwartet.

---

4. Marktabschätzungen zur Biometrie

Abb. 9: Zahl der Firmen nach biometrischen Erkennungssystemen

<table>
<thead>
<tr>
<th>Produkt</th>
<th>Anzahl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerbild</td>
<td>67</td>
</tr>
<tr>
<td>Hand</td>
<td>15</td>
</tr>
<tr>
<td>Auge</td>
<td>5</td>
</tr>
<tr>
<td>Gesicht</td>
<td>30</td>
</tr>
<tr>
<td>Sprecher</td>
<td>30</td>
</tr>
<tr>
<td>Schrift</td>
<td>19</td>
</tr>
<tr>
<td>Andere</td>
<td>11</td>
</tr>
</tbody>
</table>

Quelle: Behrens/Roth 2001, S. 64, nach Frost & Sullivan 1999

Abb. 10: Marktverteilung biometrischer Systeme (1999) weltweit, nach IBG

<table>
<thead>
<tr>
<th>Produkt</th>
<th>Marktanteil</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerbild</td>
<td>34%</td>
</tr>
<tr>
<td>Unterschrift</td>
<td>11%</td>
</tr>
<tr>
<td>Hand</td>
<td>26%</td>
</tr>
<tr>
<td>Auge</td>
<td>15%</td>
</tr>
<tr>
<td>Gesicht</td>
<td>11%</td>
</tr>
<tr>
<td>Stimme</td>
<td>3%</td>
</tr>
</tbody>
</table>

Abb. 11: Marktverteilung biometrischer Systeme weltweit, nach Lockie


4. Marktabschätzungen zur Biometrie

Abb. 12: Umsatzverteilung biometrischer Systeme nach Anwendungsbereichen


Abb. 13: Umsatzentwicklung biometrischer Systeme 1997-2002

Quelle: Behrens/Roth 2001, S. 66, nach Frost & Sullivan 1999; * = prognostizierte Werte


4. Marktabschätzungen zur Biometrie

Abb. 14: Regionale Umsatzverteilung biometrischer Systeme, nach Lockie


Abb. 15: Regionale Umsatzverteilung biometr. Systeme, nach Frost & Sullivan
