

# Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren

## - Kriterienkatalog -

Version 2.0

Stand: 10.07.2002

**TELETRUST Deutschland e.V.**

Arbeitsgruppe 6:  
Biometrische Identifikationsverfahren

Redaktion:  
Dr. G. Laßmann

---

© **TELETRUST Deutschland e.V.**  
Verein zur Förderung der Vertrauenswürdigkeit von Informations- und  
Kommunikationstechnik  
<http://www.teletrust.de>

Geschäftsstelle:  
Chamissostraße 11  
D-99096 Erfurt  
Tel: 0361 / 3 46 05 31  
Fax: 0361 / 3 45 39 57  
E-Mail: [info@teletrust.de](mailto:info@teletrust.de)

## Vorwort

Der mit diesem Dokument neu vorgelegte Kriterienkatalog zur Bewertung der Vergleichbarkeit biometrischer Verfahren ist von der Arbeitsgruppe 6 „Biometrische Identifikationsverfahren“ von TeleTrusT erarbeitet worden und als Hilfsmittel für die sachbezogene Arbeit potentieller Anwender oder Betreiber von biometrischen Identifikationsverfahren gedacht. Mit diesem Papier soll durch Versachlichung der Diskussion der sinnvolle Einsatz von biometrischen Verfahren gefördert werden.

Bereits der erste, 1998 vorgelegte Kriterienkatalog hatte diese Aufgabe erfüllt und ist von vielen als Einstiegslektüre in die komplexe Thematik benutzt worden.

In den neuen Kriterienkatalog sind neben der Fortschreibung der technischen Entwicklung und der rechtlichen Aspekte auch die Erfahrungen aus mehreren Tests und Feldversuchen eingeflossen. Das TeleTrusT-Projekt "BioTrusT" beispielsweise lieferte viele Impulse.

Ergänzend zum Kriterienkatalog ist die Einrichtung einer Kolumne (FAQ) mit häufig gestellten Fragen auf der TeleTrusT-Website ([www.teletrust.de](http://www.teletrust.de)) geplant.

Fragen, Kritik und weitere Anregung sammelt Dr. G. Laßmann, T-Systems Nova GmbH, unter der Mail-Adresse: [gunter.lassmann@t-systems.com](mailto:gunter.lassmann@t-systems.com)

Berlin, den 10.Juli 2002

Dr. Gunter Laßmann, Redakteur

Folgende Mitglieder der AG6 haben mitgewirkt:

Astrid Albrecht, Rechtsanwältin	Verbraucher- zentrale Bundes- verband e.V.	aalbrechtlaw@aol.com
Dr. Christoph Busch	Fhg-IGD	busch@igd.fhg.de
Claus Freytag	Bundesdruckerei	freytag@bdr.de
Hans-Joachim Giesecke	T-Systems Nova	hans-joachim.giesecke@t- systems.com
Horst Kalo	T-Systems Nova	horst.kalo@t-systems.com
Marcus Klische		marcus.klische@ieee.org
Dr. Gunter Laßmann	T-Systems Nova	gunter.lassmann@t-systems.com
Axel Munde	BSI	axel.munde@bsi.bund.de
Andrew Pretzel	BKA	andrew.pretzel@bka.bund.de
Dr. Thomas Probst	Unabhängiges Landeszentrum für Datenschutz	ld32@datenschutzzentrum.de
Prof. Richard Roth	FH Gießen	richard.w.roth@t-online.de
Dr. Christiane Schmidt	Softpro	csc@softpro.de
Dr. Dirk Scheuermann	FhI-SIT	dirk.scheuermann@sit.fraunhofer.de
Stephan Schertel	GAD	Stephan.Schertel@GAD.de
Berthold Weghaus	TÜViT	b.weghaus@tuvit.de
Franz Veit	Dipl. sc. Pol.	veit5555@gmx.de

## Zielsetzung

Dieses Dokument erläutert exemplarisch die Begriffe und Möglichkeiten der Biometrie. Dem potentiellen Anwender/Betreiber werden Kriterien zur Verfügung gestellt, die es ihm ermöglichen, biometrische Verfahren zu vergleichen und ein für seine Applikation geeignetes Verfahren auszuwählen. Diese Bewertungskriterien umfassen

- technische,
- juristische und
- anwendungsbezogene

Aspekte.

# Inhaltsverzeichnis

<b>1</b>	<b>ALLGEMEINE EINFÜHRUNG .....</b>	<b>1</b>
1.1	Erläuterung der biometrischen Vorgehensweise .....	1
1.2	Beispielhafte Anwendungsszenarien .....	1
1.2.1	PC-Zugang, Ersatz oder Ergänzung der PIN .....	1
1.2.2	Sicherung einer Tür mit biometrischem System (Zutrittskontrolle).....	2
1.2.3	Zugang zu geschützten Ressourcen, Freischalten einer elektronischen Signatur...2	
1.3	Prinzipieller Ablauf einer biometrischen Erkennung .....	2
1.4	Definitionen .....	4
<b>2</b>	<b>EIGENSCHAFTEN DES VERWENDETEN BIOMETRISCHEN MERKMALS.....</b>	<b>6</b>
2.1	Verwendete Merkmalsart .....	6
2.2	Merkmalseigenschaften.....	7
2.2.1	Einzigartigkeit des Merkmals .....	7
2.2.2	Konstanz .....	7
2.2.3	Möglichkeit zur willentlichen Beeinflussbarkeit durch den Nutzer .....	7
2.2.4	Merkmalsverbreitung.....	7
<b>3</b>	<b>FEHLERRATEN .....</b>	<b>9</b>
3.1	Grundsätzliches zu Fehlerraten .....	9
3.2	Prinzipielle Herleitung der Fehlerraten .....	9
3.2.1	Prüfung gegen die Daten einer erfassten Testperson.....	9
3.2.2	Die False Rejection Rate (FRR) .....	10
3.2.3	Prüfung gegen Daten von nichterfassten Testpersonen.....	11
3.2.4	Die False Acceptance Rate (FAR) .....	11
3.2.5	Die Equal Error Rate (EER) .....	13
3.2.6	Berechnung der Fehlerraten in der Praxis.....	14
3.2.7	Failure to Enrol Rate.....	15
3.3	Statistische Signifikanz.....	16
<b>4</b>	<b>TECHNISCHES SYSTEM .....</b>	<b>18</b>
4.1	Merkmalerfassung im System.....	18
4.2	Anforderungen aufgrund möglicher Einsatzorte .....	19
4.3	Sicherheitsanforderungen nach Einsatzort bzw. Anwendung .....	19
4.4	Toleranz des biometrischen Verfahrens bzw. Systems .....	19
4.5	Mobilität .....	20
4.6	Einsatzfelder.....	20
4.6.1	Zutrittsmechanismen.....	20
4.6.2	Zugriff / Zugang zu elektronischen Geräten/Daten .....	20
4.6.3	Weitere Einsatzfelder.....	20
4.7	Art der Überprüfung .....	21
4.8	Technische Spezifikation des Systems.....	21
4.9	Zertifizierung und Prüfzeichen .....	21

<b>4.10</b>	<b>Produktausprägung</b> .....	<b>23</b>
<b>4.11</b>	<b>Voraussetzungen an das Trägersystem</b> .....	<b>23</b>
4.11.1	Hardware.....	23
4.11.2	Software .....	23
<b>5.</b>	<b>SICHERHEITSQUALITÄT</b> .....	<b>25</b>
<b>5.1</b>	<b>Merkmalskriterien</b> .....	<b>25</b>
<b>5.2</b>	<b>Ermittlung der Qualitätskennzahlen</b> .....	<b>25</b>
5.2.1	Fehlerrate .....	25
5.2.2	Versuchsanordnung .....	25
5.2.3	Natürliche Variabilität der Referenzdaten .....	25
5.2.4	Qualität der Referenzdaten .....	26
5.2.5	Art der Erhebung der Falschakzeptanzrate .....	26
<b>5.3</b>	<b>Ausspähbarkeit des Merkmals</b> .....	<b>27</b>
<b>5.4</b>	<b>Schutz des Systems vor Angriffen</b> .....	<b>27</b>
<b>5.4.1</b>	<b>Aufwand eines Angriffs</b> .....	<b>27</b>
5.4.2	Allgemeine Systemrisiken .....	28
5.4.3	Beispiele für biometricspezifische Angriffsszenarien .....	28
<b>6.</b>	<b>NICHT-TECHNISCHE ASPEKTE</b> .....	<b>30</b>
<b>6.1</b>	<b>Juristische Aspekte</b> .....	<b>30</b>
<b>6.2.</b>	<b>Datenschutz</b> .....	<b>30</b>
6.2.1.	Einleitung.....	30
<b>6.3</b>	<b>Problemfelder bei der Verwendung biometrischer Daten</b> .....	<b>31</b>
6.3.1	Datenvermeidung und -sparsamkeit .....	31
6.3.2	Keine unbemerkte Erhebung der biometrischen Daten .....	32
6.3.3	Informationsgehalt der biometrischen Daten.....	32
6.3.4	Rückschließbarkeit auf die hinter den biometrischen Daten stehende natürliche Person.....	32
6.3.5	Dauerhaftigkeit der Bindung zwischen biometrischen Daten und Personen.....	33
6.3.6	Ort der Speicherung der biometrischen Daten.....	33
<b>6.4</b>	<b>Konkrete Empfehlungen beim Einsatz biometrischer Verfahren aus datenschutzrechtlicher Sicht</b> .....	<b>33</b>
6.4.1	Allgemeine Anforderungen .....	33
6.4.2	Biometrische Daten als personenbezogene Daten .....	34
<b>6.5</b>	<b>Weitere juristische Fragen</b> .....	<b>36</b>
6.5.1	Anwendung biometrischer Merkmale bei elektronischen Signaturen .....	36
6.5.2	Verwendung einer qualifizierten elektronischen Signatur.....	37
6.5.3	Personaldokumente .....	37
6.5.4	Strafrechtliche Relevanz .....	38
6.5.5	Haftung des Betreibers für das biometrische System .....	39
6.5.6	Allgemeine Geschäftsbedingungen beim Einsatz biometrischer Merkmale .....	40
6.5.7	Betrieblicher Einsatz, insbesondere: Betriebsvereinbarungen.....	41
<b>6.6</b>	<b>Verbrauchersicht</b> .....	<b>43</b>

<b>7</b>	<b>BETREIBERSICHT .....</b>	<b>45</b>
<b>7.1</b>	<b>Produktreife / Produktverfügbarkeit.....</b>	<b>45</b>
<b>7.2</b>	<b>Installation .....</b>	<b>45</b>
<b>7.3</b>	<b>Systembetrieb .....</b>	<b>45</b>
<b>7.4</b>	<b>Administrationsaufwand.....</b>	<b>46</b>
7.4.1	Regelfall.....	46
7.4.2	Sonderfälle (Aufwand relativ zum Normalfall).....	46
<b>7.5</b>	<b>Investitionssicherheit .....</b>	<b>46</b>
7.5.1	Zukunftssicherheit .....	46
7.5.2	Abhängigkeit vom Anbieter.....	47
7.5.3	Abhängigkeit vom Technologielieferanten .....	47
<b>7.6</b>	<b>Integrationsfähigkeit .....</b>	<b>47</b>
7.6.1	Systemintegration .....	47
7.6.2	Lösungsintegration / Integration in das Sicherheitskonzept .....	47
<b>7.7</b>	<b>Kosten .....</b>	<b>48</b>
7.7.1	Einmalige Kosten.....	48
7.7.2	Laufende Kosten .....	48
<b>7.8</b>	<b>Unterschiedliche Nutzergruppen.....</b>	<b>48</b>
<b>8.</b>	<b>BENUTZERAKZEPTANZ.....</b>	<b>49</b>
<b>8.1</b>	<b>Relevanz der Benutzerakzeptanz zur Bewertung biometrischer Identifikationssysteme .....</b>	<b>49</b>
<b>8.2</b>	<b>Allgemeine Haltung und Nutzungstypen.....</b>	<b>49</b>
<b>8.3</b>	<b>Informationstransparenz .....</b>	<b>50</b>
<b>8.4</b>	<b>Enrolment und Benutzerführung.....</b>	<b>50</b>
<b>8.5</b>	<b>Diskriminierungsfreier Einsatz .....</b>	<b>51</b>
8.5.1	Ausgrenzung durch das verwendete Merkmal.....	51
8.5.2	Ausgrenzung aufgrund personenbezogener Besonderheiten .....	51
8.5.3	Notwendigkeit von Ersatzverfahren .....	51
8.5.4	Kosten für Nutzer.....	51
<b>8.6</b>	<b>Handhabung der Verfahren .....</b>	<b>52</b>
8.6.1	Einfachheit und Bequemlichkeit.....	52
8.6.2	Schnelligkeit .....	52
8.6.3	Ergonomie der Anwendergeräte .....	52
8.6.4	Übertragbarkeit von Zugangsberechtigungen im Arbeitsalltag.....	53
<b>8.7</b>	<b>Bedenken und Befürchtungen .....</b>	<b>53</b>
8.7.1	Physische und moralische Unversehrtheit .....	53
8.7.2	Kriminelle Handlungen Dritter und Datenmissbrauch .....	53
8.7.3	Erzwungene Nutzung.....	53
8.7.4	Nutzung für Zwecke der Strafverfolgung.....	54
8.7.5	Scheu und Scham.....	54
<b>8.8</b>	<b>System- und Merkmalsausfall .....</b>	<b>54</b>

<b>9</b>	<b>ANHANG .....</b>	<b>55</b>
<b>9.1</b>	<b>Referenzen .....</b>	<b>55</b>
<b>9.2</b>	<b>Weiterführende Literatur .....</b>	<b>56</b>
<b>9.3</b>	<b>Abkürzungsverzeichnis / Glossar .....</b>	<b>57</b>

# 1 Allgemeine Einführung

## 1.1 Erläuterung der biometrischen Vorgehensweise

Neben der Sicherung von Datenintegrität, der Garantie von Vertraulichkeit und der Gewährleistung von Nachweisbarkeit gehören Authentifikationsmethoden zu den wichtigsten Sicherheitsdiensten, die u.a. mit biometrischen Verfahren realisiert werden können.

Traditionelle Authentifikationstechniken beruhen darauf, dass der Benutzer über ein bestimmtes, nur ihm bekanntes Wissen verfügt (Verifikation der Identität durch Wissen) oder einen persönlichen Berechtigungsschlüssel besitzt (Verifikation der Identität durch Besitz). Herkömmlich erfolgt der Zugangsschutz zu verschiedenen PC- oder Netzwerkelementen mittels Abfrage von Benutzername und Passwort bzw. Persönlicher Identifikationsnummer (PIN). Die damit verbundenen Handhabungsprobleme sind hinlänglich bekannt: ein Passwort oder eine PIN können ausgespäht, gestohlen, notiert oder weitergegeben werden. Der Einsatz eines biometrischen Verfahrens kann hier Abhilfe schaffen, um tatsächlich nur autorisierte Personen zuzulassen.

Die Biometrie verwendet physiologische oder verhaltenstypische Merkmale zur Authentifikation des Benutzers. Es werden somit personengebundene und nicht nur personenbezogene Merkmale erfasst. Biometrische Merkmale haben den Vorteil, dass sie im Allgemeinen nicht gestohlen und nur schwer kopiert werden können. Bei Passwort- oder Chipkartensystemen kann zwar überprüft werden, ob die Karte oder der Schlüssel gültig ist, es wird jedoch nicht überprüft, ob der aktuelle Benutzer auch der berechtigte Besitzer dieses Legitimationsmittels ist. Mit biometrischen Verfahren kann dieses Sicherheitsmanko behoben werden. Die herausragende Charakteristik der Biometrie ist die Möglichkeit der Überprüfung des zu identifizierenden Merkmals zusammen mit dessen zulässigen Besitz. Biometrische Verfahren können bezüglich Kosten und Leistungsfähigkeit eine Alternative zu anderen Sicherungsmechanismen darstellen oder diese ergänzen. Durch den Einsatz von biometrischen Systemen kann auch eine neuartige Sicherheitsqualität erreicht werden.

## 1.2 Beispielhafte Anwendungsszenarien

In diesem Abschnitt sollen dem Anwender / Betreiber anhand von Beispielen die praktische Anwendung biometrischer Identifikationsverfahren nahegebracht werden.

### 1.2.1 PC-Zugang, Ersatz oder Ergänzung der PIN

Allgemein bekannt ist der Zugangsschutz zu verschiedenen PC- oder Netzwerkelementen mittels Abfrage von Benutzername und Kennwort. Die damit verbundenen Handhabungsprobleme sind hinlänglich bekannt.

Der Einsatz eines biometrischen Verfahrens kann hier Abhilfe schaffen, um tatsächlich nur autorisierte Personen zuzulassen.

Verschiedenste biometrische Merkmale (z.B. Fingerbild, Gesicht, Iris, Sprache) für die Authentifizierung einer Person kommen in den zur Zeit auf dem Markt angebotenen biometrischen Systemen für PC-Login zum Einsatz.

### 1.2.2 Sicherung einer Tür mit biometrischem System (Zutrittskontrolle)

Für den Zutritt zu einem abzusichernden Bereich kann für den bis heute üblichen Einsatz einer Chipkarte oder die Verwendung eines Passwortes auch ein biometrisches System zur Anwendung kommen. Es sind zwischenzeitlich Produkte auf dem Markt, die verschiedenste biometrische Merkmale (z.B. Fingerbild, Gesichtserkennung, Iriserkennung, Sprache, kombinierte Verfahren) für die Authentifizierung einer Person ausnutzen. Die bis jetzt zum Einsatz gekommenen biometrischen Systeme werden im überwiegenden Maß zur Verifikation (1:1-Vergleich siehe Abs.1.4) des Nutzers eingesetzt und in wenigen Fällen auch als Identifikationssystem (1:n-Vergleich siehe Abs.1.4) genutzt.

### 1.2.3 Zugang zu geschützten Ressourcen, Freischalten einer elektronischen Signatur

Als weiterer Einsatzbereich eines biometrischen Verfahrens kommt die sogenannte qualifizierte elektronische Signatur in Betracht. Zum Freischalten des Signaturmechanismus wird ein Besitzelement, herkömmlich eine Signaturkarte, benötigt, die in aller Regel in einem Kartenlesegerät mittels einer PIN freigeschaltet wird. Nach den im Jahr 2001 novellierten gesetzlichen Grundlagen zur elektronischen Signatur können zur Freischaltung des Signaturmechanismus auch ein oder mehrere biometrische Merkmale anstelle der PIN verwendet werden<sup>1</sup>: „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“ (§ 15 Absatz 1 Satz 1 SigV). Weiterhin muss „Bei Nutzung biometrischer Merkmale hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben ist“ (§ 15 Absatz 1 Satz 3 SigV). Die Verknüpfung mit einem Besitzelement muss also auch beim Einsatz biometrischer Merkmale erfolgen. In technischer Hinsicht wird in der Anlage zur SigV auf die Common Criteria bzw. ITSEC verwiesen.

## 1.3 Prinzipieller Ablauf einer biometrischen Erkennung

Ein System zur biometrischen Erkennung verarbeitet die erfassten biometrischen Daten einer Person mit dem Ziel, mit Hilfe von vorher erfassten Referenzdaten die Identität dieser Person zu bestätigen oder zurückzuweisen.

Alle biometrischen Systeme enthalten generell die Komponenten *Datenaufnahme*, *Vorverarbeitung*, *Merkmalsextraktion*, *Klassifikation* und *Referenzbildung*. Für die Anpassung an Veränderungen des biometrischen Merkmals kann ein *adaptives Verfahren* eingesetzt werden.

In Bild 1-1 und Bild 1-2 ist der grundsätzliche Aufbau eines biometrischen Systems dargestellt. Mit Hilfe eines Sensors werden die Eingabedaten aufgenommen. Sie werden vor oder während des Mustervergleichs vorverarbeitet und normalisiert. Zur Klassifikation können entweder die vorverarbeiteten Daten oder daraus extrahierte Merkmale verwendet werden. Diese Eingangsdaten werden dabei mit den entsprechenden Referenzdaten verglichen. Zur Auswahl der Referenzdaten aus der Referenzdatenbank kann der Benutzer z. B. seine persönliche Identifikationsnummer angeben. Alternativ dazu können die Referenzdaten auch auf einem im Besitz des

<sup>1</sup> Insbesondere §§ 17 Absatz 1 Satz 1 SigG (vom 17.05.2001) in Verbindung mit 15 Absatz 1 Satz 1-3 und Anlage I SigVO (vom 22.11.2001)

Nutzers befindlichen Speichermedium (z.B. Chipkarte) gespeichert sein. Bei adaptiven Verfahren können die erhaltenen Bewertungen im Fall einer positiven Klassifikation zur Aktualisierung der Referenzdaten verwendet werden.

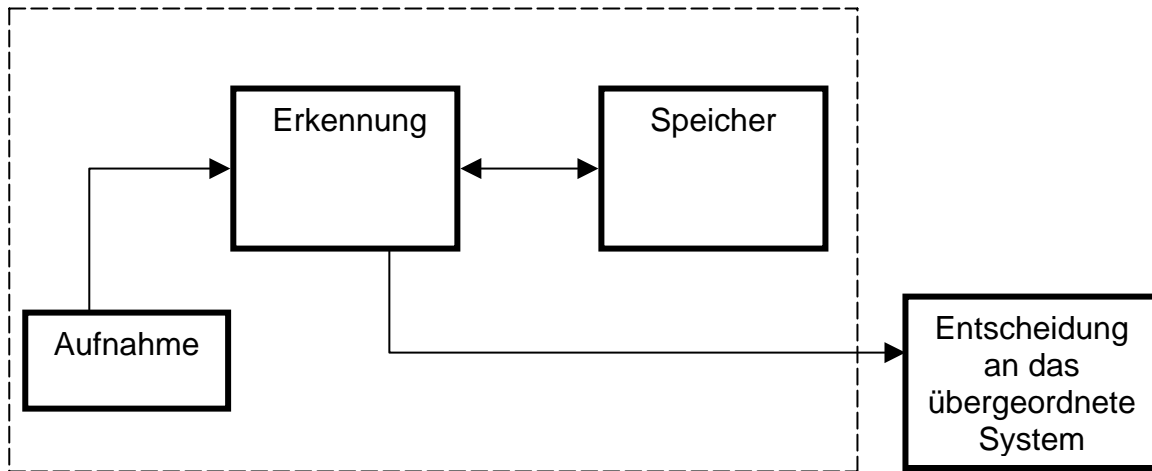


Bild 1-1 Ablauf eines biometrischen Verfahrens

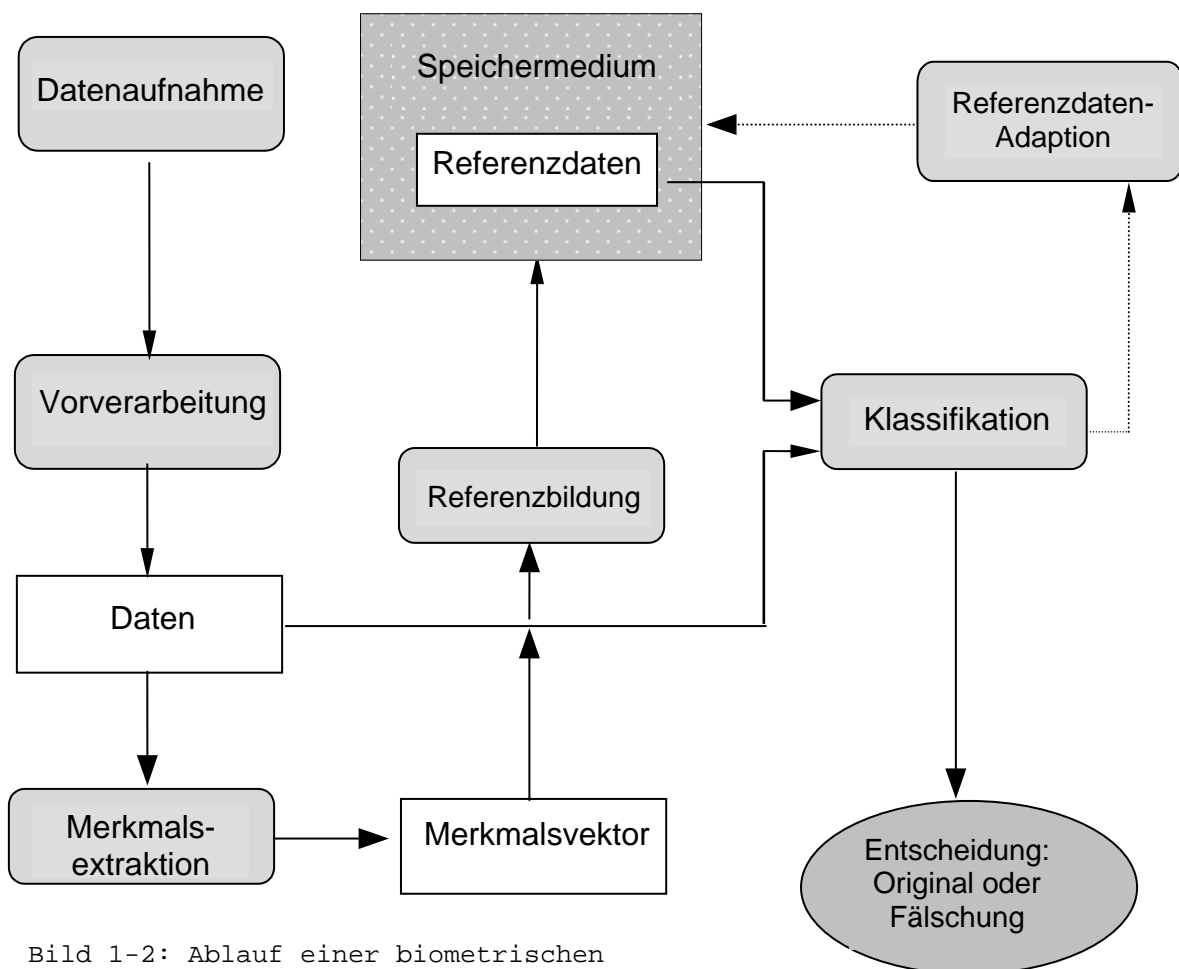


Bild 1-2: Ablauf einer biometrischen Verifikation

## 1.4 Definitionen

<b>Betreiber (Anwender)</b>	Unternehmen oder Organisationen, die ein IT-System mit bestimmten Anwendungen (Applikationen) betreiben und dabei biometrische Verfahren anwenden wollen.
<b>Hersteller</b>	Ein Unternehmen, das komplette biometrische Produkte, die Integration von biometrischen Komponenten zu biometrischen Systemen, oder biometrische Erkennungssoftware auf dem Markt anbietet.
<b>Nutzer (Benutzer)</b>	Die Person, deren biometrische Merkmale geprüft werden sollen.
<b>System zur biometrischen Erkennung</b>	Ein System der Informationstechnik, das Personen durch Messungen von körperlichen Merkmalen erkennt.
<b>Verifikation</b> genauer: Verifikation einer Person durch ein biometrisches Verfahren	<p>Verifikation bedeutet „<u>Bestätigung</u> der Identität.“ Die Personenverifikation entscheidet die Frage, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt.</p> <p>In der Biometrie werden bei der Verifikation die aktuellen biometrischen Daten einer Person erfasst und mit den im Vorfeld erfassten biometrischen Referenzdaten desjenigen Individuums verglichen, als das sich die Person ausgibt (1:1-Vergleich). Es findet ein Vergleich zweier Datensätze statt. Stimmen die beiden Datensätze innerhalb der gewählten Toleranzgrenzen miteinander überein, so wird bestätigt, dass es sich bei der Person um diejenige handelt, für die sie sich ausgibt.</p>
<b>Identifikation</b> genauer: Identifikation einer Person durch ein biometrisches Verfahren	<p>Identifikation bedeutet „Feststellung der Identität.“ Bei der Personenidentifikation wird festgelegt, um welche Person es sich handelt.</p> <p>In der Biometrie werden bei der Identifikation die aktuellen biometrischen Daten einer Person erfasst und mit den im Vorfeld erfassten biometrischen Referenzdaten einer Vielzahl von Individuen verglichen (1:n-Vergleich). Diese Referenzdaten sind beispielsweise in einer Datenbank gespeichert. Es findet somit eine Vielzahl von Vergleichen statt. Die Person wird als dasjenige Individuum identifiziert, dessen biometrischer Referenzdatensatz mit dem aktuellen biometrischen Datensatz der Person innerhalb der gewählten Toleranzgrenzen übereinstimmt.</p>

**Authentifizierung/  
Authentifikation**

genauer:  
Authentifizierung/  
Authentifikation einer  
Person durch ein  
biometrisches  
Verfahren

Authentifizierung/Authentifikation bedeutet „Bezeugung der Echtheit.“ Bei der Authentifizierung mittels eines biometrischen Systems erfolgt eine Identifikation oder Verifikation.

**Autorisierung**

Autorisierung bedeutet „Ermächtigung, Bevollmächtigung.“  
Nach erfolgreicher Authentifikation (Identifikation oder Verifikation) mittels eines biometrischen Systems wird die Person ermächtigt, gewisse Handlungen durchzuführen oder bestimmte Dienste zu nutzen.

## 2 Eigenschaften des verwendeten biometrischen Merkmals

### 2.1 Verwendete Merkmalsart

Bei biometrischen Verfahren unterscheidet man zwischen physiologischen und verhaltensbasierten Merkmalen. Physiologische Merkmale sind Körpermerkmale einer Person, die sich nicht oder nur sehr geringfügig über einen längeren Zeitraum verändern. Verhaltensbasierte Merkmale einer Person sind Merkmale, die sich zeitlich verändern und bei jeder neuen Erfassung anders ausfallen können. Im folgenden sind Beispiele für biometrische Merkmale angeführt.

Physiologisches Merkmal (auch passives Merkmal genannt)

Zum Beispiel:

- Gesicht
- Iris
- Retina
- Finger
- Handgeometrie
- Venenmuster auf dem Handrücken
- Ohr
- Geruch

Verhaltensbasiertes Merkmal (auch aktives Merkmal genannt)

Zum Beispiel:

- Unterschrift
- Sitzverhalten
- Gang
- Gesamtkörper
- Tippverhalten an der Tastatur
- Gestik / Mimik beim Sprechen
- Schreibverhalten
- Stimme / Sprechverhalten

### Merkmalskombination

Zum Beispiel:

- Erfassung des Gesichts und der Gesichtsdynamik beim Sprechen kombiniert mit Stimmerkennung

## 2.2 Merkmalseigenschaften

Körperliche Merkmale sollten, um für eine biometrische Erkennung geeignet zu sein, folgende Mindestvoraussetzungen erfüllen.

### 2.2.1 Einzigartigkeit des Merkmals

Ein Merkmal muss, um für ein biometrisches Verfahren geeignet zu sein, einzigartig in dem Sinne sein, dass es für unterschiedliche Menschen hinreichend verschieden ist.

### 2.2.2 Konstanz

Ein Merkmal sollte, um für ein biometrisches Verfahren geeignet zu sein, sich im Laufe der Zeit möglichst wenig ändern. Kleinere Änderungen können adaptive biometrische Verfahren ausgleichen.

Die Gefahr des Verlustes oder der Unverwendbarkeit des Merkmals sollte stets berücksichtigt werden.

### 2.2.3 Möglichkeit zur willentlichen Beeinflussbarkeit durch den Nutzer

Biometrische Systeme unterscheiden sich auch dadurch, dass verschiedene Merkmale ein unterschiedliches Aktivitätsniveau erfordern: so kann z.B. ein Gesichtserkennungssystem auch ohne Zutun des Nutzers eine Erkennung durchführen, während z.B. bei Unterschriftenerkennungssystemen der Nutzer stets aktiv seine Unterschrift leisten muss.

Einige biometrische Merkmale bieten dem Nutzer zudem die Möglichkeit, eine zusätzliche Information abzugeben. So besteht bei Fingerabdruckverfahren grundsätzlich die Möglichkeit, mehrere Finger im System einzulernen und je nach Wahl des entsprechenden Fingers dem System eine Zusatzinformation zu geben. Bei der Stimmerkennung oder Unterschriftsdynamik, die typisch mit einem festen, frei wählbaren Schlüsselwort kombiniert sind, besteht ebenfalls die Möglichkeit, durch Anlernen und Speichern verschiedener Schlüsselwörter eine Steuerinformation an das System zu geben. Diese Eigenschaft gewinnt besondere Bedeutung in Anwendungsszenarien, in denen mit einer Erpressung des Merkmalsträgers gerechnet werden muss. Hieraus ergibt sich die Chance, durch den erpressten Merkmalsträger einen stillen Alarm ohne Erkennbarkeit für den Erpresser abzugeben.

### 2.2.4 Merkmalsverbreitung

Ein Merkmal sollte, um für biometrische Verfahren geeignet zu sein, bei möglichst vielen potentiellen Nutzern vorhanden sein. Es gibt jedoch Personen, die gewisse Merkmale gar nicht aufweisen oder bei denen die Merkmale in einer für die Erfassung und Auswertung nicht ausreichenden Ausprägung vorhanden sind. Bei jedem biometrischen Verfahren gibt es einen gewissen Prozentsatz von Individuen, die überhaupt nicht im System erfasst werden können (sog. failure-to-enrol-Rate, siehe dazu in Kap. 3.2.3). So besitzt zum Beispiel ein kleiner Bevölkerungsanteil keine ausgeprägten Fingerabdruckstrukturen. Ferner ist die Verwendung mancher Merkmale für andere Gruppen nicht geeignet. In diesem Fall muss ein alternatives Verfahren zur Verfügung gestellt werden

**„Merkmalsakzeptanz“**

Zusätzlich zu den in 2.2.1. bis 2.2.4. genannten Basisanforderungen muss das biometrische Merkmal von den potenziellen Nutzern und Betreibern schließlich auch akzeptiert werden. Ein Merkmal, das aufgrund mangelnder Akzeptanz in einer Anwendung praktisch nicht benutzt wird, ist für diese Anwendung nicht geeignet. Merkmale werden von den potenziellen Nutzern in unterschiedlicher Art und Weise akzeptiert. Welche Faktoren die Akzeptanz beim Nutzer positiv oder negativ beeinflussen können, wird in Kap. 7 näher erläutert.

## 3 Fehlerraten

Eine rein theoretische Abschätzung der Sicherheit, wie man sie aus der Kryptographie oder der Diskussion um die PIN kennt, gibt es in der Biometrie nicht. Einer der Gründe dafür ist, dass die biometrischen Fehlerraten empirisch zu ermitteln sind. Empirisch ermittelte Fehlerraten können nur mit großem Testaufwand kleine Werte annehmen. Ist z.B. in der Kryptographie aufgrund theoretischer Überlegungen die Fehlerwahrscheinlichkeit sehr gering, so trifft dies nicht auf die aus dem praktischen Versuch ermittelten oberen Schranken der Fehlerraten zu, die in der Regel um mehrere Größenordnung größer sind. Die empirisch ermittelte obere Schranke einer Fehlerrate kann z. B. nie Null sein, sondern sich diesem Wert (bei einer sehr großen Zahl von Testpersonen) nur annähern.

### 3.1 Grundsätzliches zu Fehlerraten

Da in der Praxis bei der Messung biometrischer Daten niemals dieselben Bedingungen herrschen und die Messobjekte (z.B. Finger) natürlichen Schwankungen unterliegen, werden die aktuell erfassten Messdaten und die abgelegten Referenzdaten nie ganz übereinstimmen sondern nur eine gewisse „Ähnlichkeit“ erreichen.

Bei der Überprüfung wird daher getestet, ob die Messdaten in einem vorab festzulegenden „Toleranzbereich“ enthalten sind und den vorher bestimmten Übereinstimmungsgrad erreichen.

Jedes biometrische System hat also immer eine unvermeidbare Restfehlerquote. Diese Fehlerquote lässt sich aber nur sehr schwer objektiv ermitteln, da sie stark von der Vorauswahl der Versuchspersonen und den jeweiligen Versuchsbedingungen abhängt. Die Fehlerraten weichen in der Praxis nicht selten von den Angaben des Herstellers ab. Um die Fehlerraten der Hersteller beurteilen zu können, sind konkrete Angaben über Versuchsanordnung und Versuchsbedingungen notwendig. Erst die individuelle Anpassung des Systems an die Anforderungen des einzelnen Betreibers ermöglicht Aussagen über die Verwendbarkeit des Systems in der konkreten Anwendung.

### 3.2 Prinzipielle Herleitung der Fehlerraten

#### 3.2.1 Prüfung gegen die Daten einer erfassten Testperson

Von einer Testperson werden Referenzdaten generiert und abgelegt. Anschließend werden von der nun erfassten Testperson zahlreiche neue Datensätze erstellt. Von den einzelnen Datensätzen werden jeweils die Übereinstimmungsgrade bezüglich der Referenzdaten ermittelt. In Bild 3-1 sind die Häufigkeiten der Übereinstimmungen in Abhängigkeit vom Grad abgebildet. So werden z.B. 15% der Datensätze mit einer Übereinstimmung mit den Referenzdaten von 0,62 ermittelt, wobei „0“ keine und „1“ die identische Übereinstimmung bedeutet. Obwohl es im Beispiel so aussieht, muss die Verteilung mit steigender Zahl der Messungen nicht in eine Normalverteilung übergehen. Starke Abweichungen von der Normalverteilung, etwa ein ausgeprägter Doppelgipfel, sind aber als Hinweis auf systematische Fehler bei der Erfassung zu beachten.

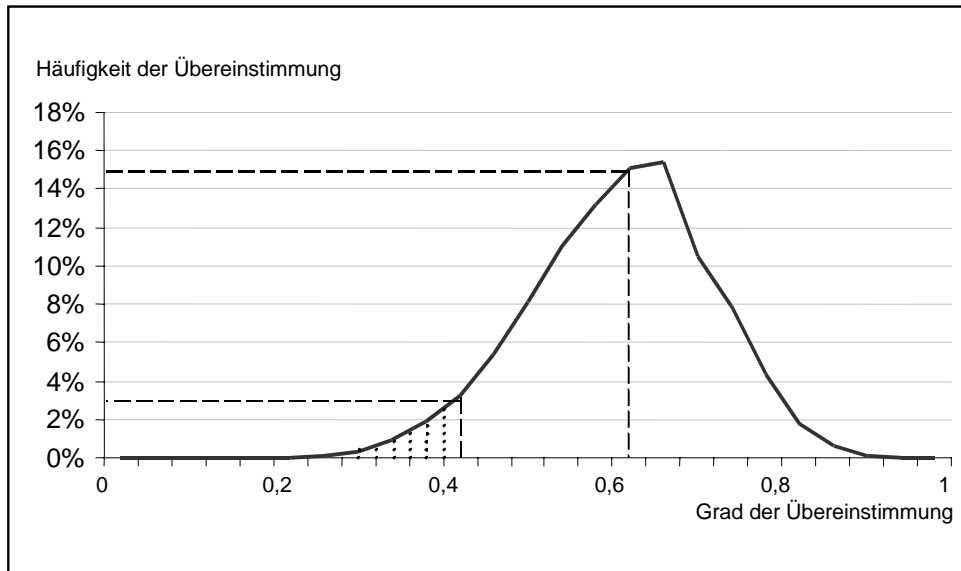


Bild 3-1: Verteilung der Anzahl der übereinstimmenden Merkmale

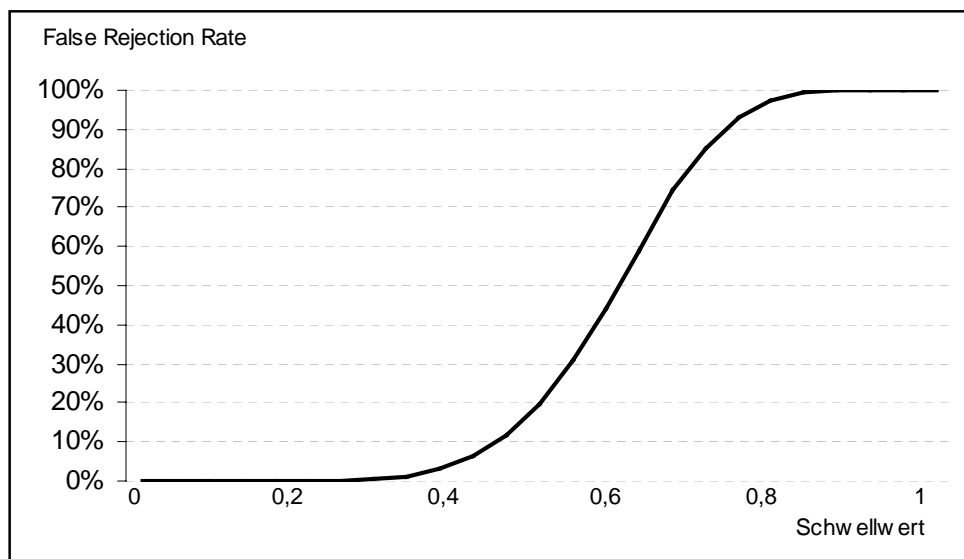


Bild 3-2: Verteilung des Anteils der zu Unrecht Abgewiesenen (FRR) in Abhängigkeit vom Schwellwert

### 3.2.2 Die False Rejection Rate (FRR)

Wird nun im biometrischen System vom Administrator ein bestimmter Schwellwert, z.B. im Bild 3-1 der Grad 0,42 eingestellt, so werden alle Personen mit Übereinstimmungsgrad weniger als 0,42 haben vom System abgelehnt. Aufgrund der Verteilung kann man nun abschätzen, wie groß in diesem Fall die Wahrscheinlichkeit ist, dass die zugelassene Testperson abgelehnt wird: Dies ist genau der Anteil der Fälle bei denen die Testperson nur mit dem Übereinstimmungsgrad 0,41 oder weniger erfasst wurde. Das sind im Beispiel 3,14 %. Der prozentuale Anteil fälschlich zurückgewiesener Berechtigter, die sogenannte *false rejection rate (FRR)*, entspricht also jeweils dem Flächenanteil unter der Kurve vom Ursprung bis zum Schwellwert.

Damit kann die zu erwartende Fehlerrate *FRR* in Abhängigkeit vom Schwellwert angegeben werden. In Bild 3-2 ist die Abhängigkeit aufgrund der Datensätze aus dem Beispiel aus Bild 3-1 angegeben. Je größer der Schwellwert und damit der geforderte Übereinstimmungsgrad eines Datensatzes mit dem Referenzdatensatz gewählt wird, je größer wird die Zahl der unrechtmäßigen Zurückweisungen.

### 3.2.3 Prüfung gegen Daten von nichterfassten Testpersonen

Das aus den vorangegangenen Abschnitten bekannte Beispiel weiterführend, werden von möglichst vielen weiteren Testpersonen neue Datensätze erstellt und auf Übereinstimmung mit dem Datensatz der erfassten Testperson geprüft. In Bild 3-3 sind dazu die Häufigkeiten der Übereinstimmungen in Abhängigkeit vom Übereinstimmungsgrad dargestellt. Wie man bei Übereinstimmungsgrad 0 sieht, kommt es bei diesem biometrischem System durchaus vor, dass eine nicht zuvor im System eingelernte Person gar kein Merkmalskriterium erfüllt. Das ist der erwünschte Fall. Jedoch ist damit zu rechnen, dass es Personen gibt, deren Merkmal eine hohe Übereinstimmung mit den Referenzdaten der erfassten Testperson besitzen können.

### 3.2.4 Die False Acceptance Rate (FAR)

Wird nun im biometrischen System vom Administrator ein bestimmter Schwellwert, z.B. mindestens 0,42 eingestellt, so werden alle Personen die einen Übereinstimmungsgrad weniger 0,42 haben, vom System abgelehnt.

Aufgrund der Verteilung kann man nun abschätzen, wie groß in diesem Fall die Wahrscheinlichkeit ist, dass eine nichterfasste Testperson zugelassen wird: Dies ist genau der Anteil der Fälle bei denen die nichterfasste Testperson einen Übereinstimmungsgrad gleich oder größer 0,42 hatte. Der prozentuale Anteil fälschlich zugelassener Unberechtigter, die sogenannte *false acceptance rate (FAR)*, entspricht also jeweils dem Flächenanteil unter der Kurve vom Schwellwert bis zum Übereinstimmungsgrad. In Bild 3-4 ist diese Abhängigkeit aufgrund der Datensätze aus Bild 3-3 angegeben. Je kleiner der Schwellwert und damit der geforderte Übereinstimmungsgrad eines Datensatzes mit dem Referenzdatensatz gewählt wird, je größer wird die Zahl der Falsch-Akzeptanzen.

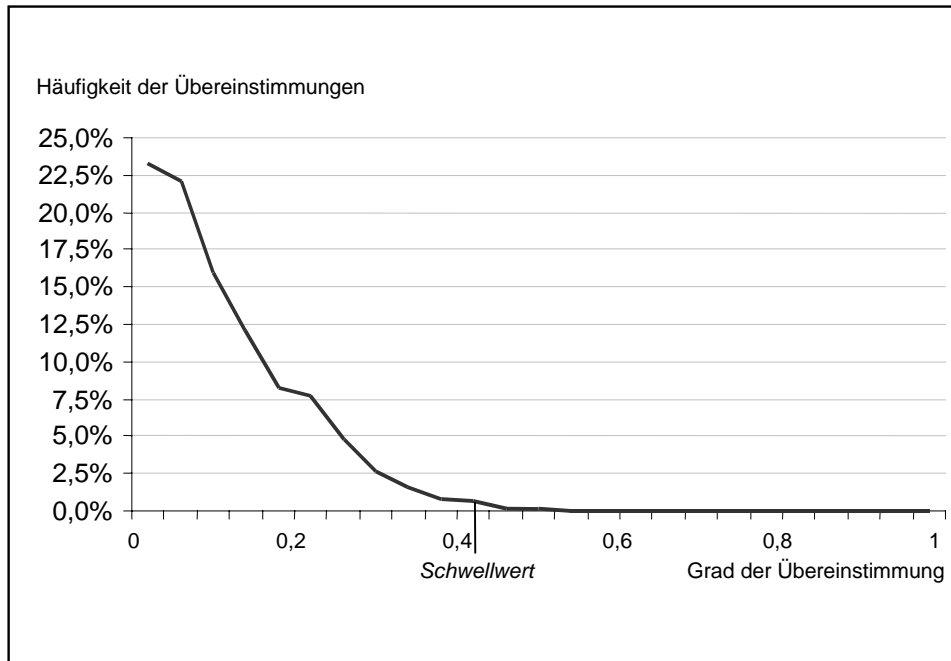


Bild 3-3: Verteilung der Anzahl der übereinstimmenden Merkmale

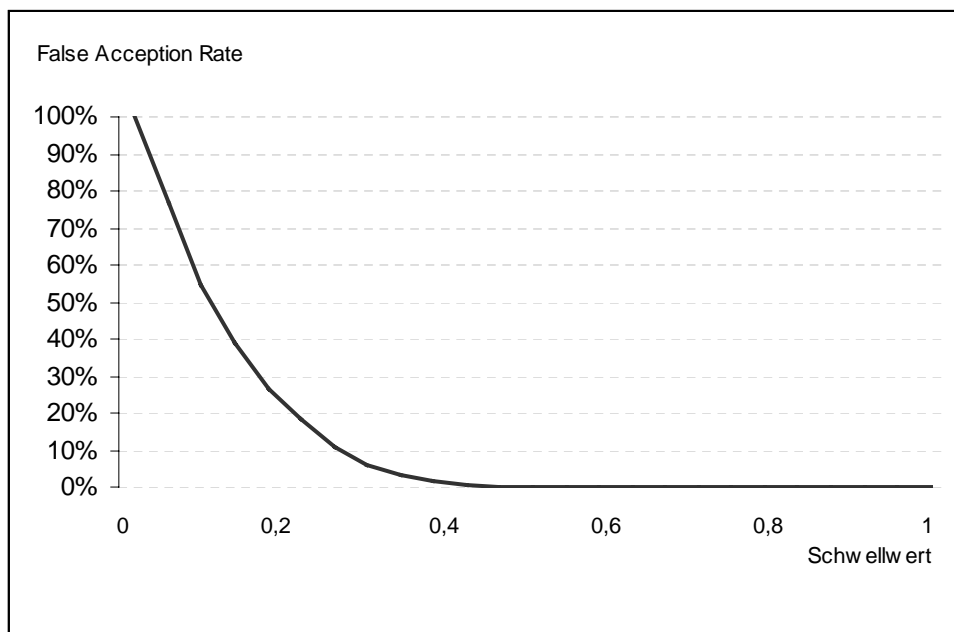


Bild 3-4: Verteilung des Anteils der zu Unrecht Zugelassenen (FAR) in Abhängigkeit vom Schwellwert

### 3.2.5 Die Equal Error Rate (EER)

Die Aufgabe des Administrators eines biometrischen Systems ist es, bei der Wahl des Schwellwertes *Sicherheit* (geringe *FAR*) und *Komfort* (geringe *FRR*) abzuwägen. Maßgeblich sollten dabei die Anforderungen an die konkrete Anwendung sein.

Einen Maßstab für die Möglichkeiten eines biometrischen Systems liefert die *EER*, die sogenannte *equal error rate*. Das ist die Fehlerrate, bei der *FRR* und *FAR* gleich sind. In Bild 3-5 liegt die *EER* für das hier benutzte Beispiel bei 2%. Wird der Schwellwert erhöht und damit die Prüfung strenger, so steigt die *FRR* und fällt die *FAR*. Sinkt der Schwellwert, so fällt die *FRR* und mit steigender *FAR* kann eine steigende Zahl unberechtigter Personen durch die Kontrolle schlüpfen. Eine idealisierte Grafik ist noch einmal in Bild 3-6 angegeben.

Mit der *EER* ergibt sich ein Maß für die allgemeine Trennfähigkeit zwischen erfassten und nichterfassten Nutzern eines Systems. Im Idealfall läge die *EER* eines Systems bei Null, was jedoch in biometrischen Systemen in der Regel nicht der Fall ist. In diesem Fall wären die beiden Verteilungen vollkommen getrennt.

Man beachte, dass diese Fehlerrate nicht für die betrachtete Biometrie allgemein gilt, sondern lediglich für die eingelernte Datenbasis. Genau genommen gelten dieselben Fehlerraten auch nur dann, wenn wiederum dieselben Unberechtigten versuchen, in das System zu kommen.

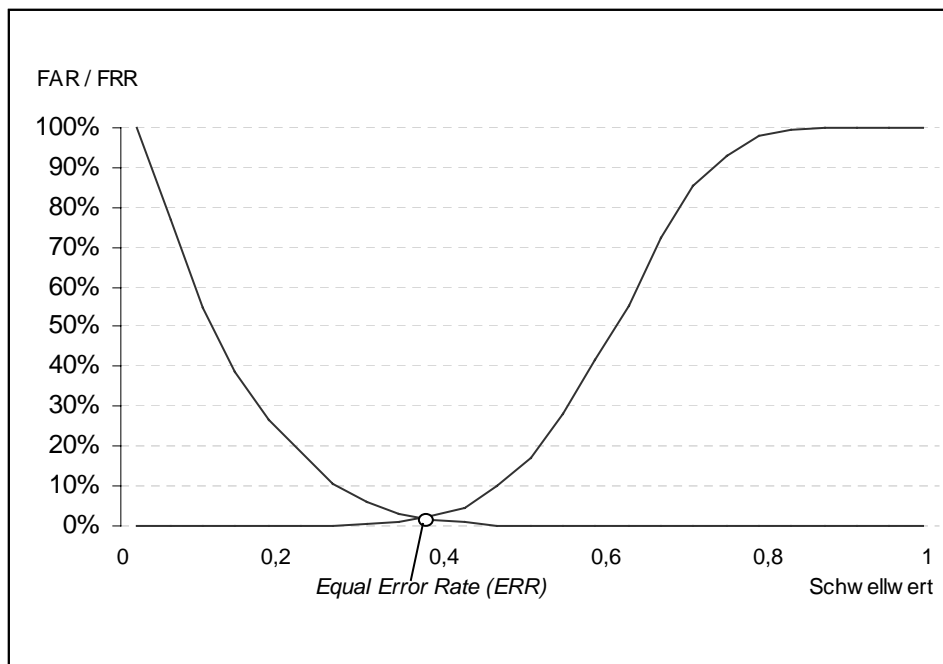


Bild 3-5: Verhältnis FRR und FAR

### 3.2.6 Berechnung der Fehlerraten in der Praxis

Die Raten  $FAR$  und  $FRR$  (in Prozent) ergeben sich wie folgt:

$$FAR = \frac{NFA}{NIA} \cdot 100\% \quad , \quad FRR = \frac{NFR}{NEA} \cdot 100\% \quad ,$$

wobei die Abkürzungen folgende Bedeutung besitzen:

- $NFA$ : die Anzahl fälschlicher Akzeptanzen (*number of false acceptances*),
- $NIA$ : die Gesamtanzahl unberechtigter Zutrittsversuche (Identifikation oder Verifikation, *number of imposter attempts*),
- $NFR$ : die Anzahl fälschlicher Rückweisungen (*number of false rejections*),
- $NEA$ : die Gesamtanzahl berechtigter Zutrittsversuche (Identifikation oder Verifikation, *number of enrollee attempts*).

Das Bild 3-6 zeigt den typischen idealisierten Verlauf biometrischer Fehlerkurven. Je höher der Schwellwert (d.h. je höher die Sicherheit) ist, desto weniger nichterfasste Nutzer wird das System akzeptieren. Ist hingegen der Schwellwert relativ niedrig eingestellt (d.h. hoher Komfort), so werden zwar wenig bis keine erfassten Nutzer zurückgewiesen, dafür jedoch um so mehr nichterfasste Nutzer akzeptiert.

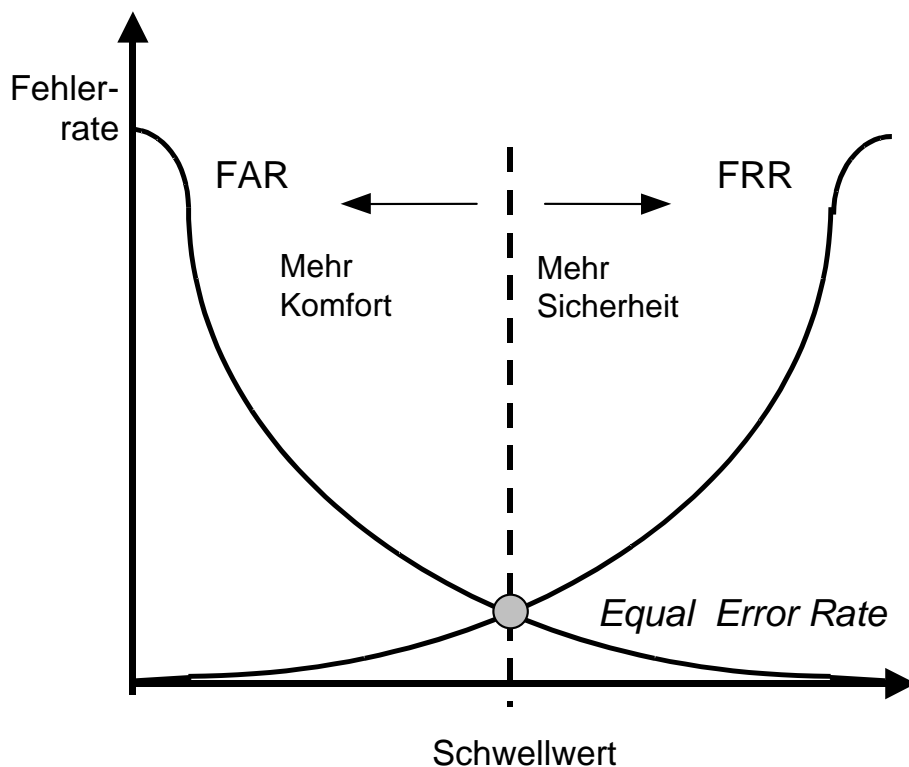


Bild 3-6: Typische Fehlerkurven bei biometrischen Verfahren

Die *EER* befindet sich gerade im Schnittpunkt der beiden Kurven der Fehlerraten *FAR* und *FRR*. Die Bestimmung der *EER* ist nur im Falle klassifizierter erfasster und nichterfasster Testpersonen als theoretische Evaluierung der Leistungsfähigkeit eines Systems möglich. Beim tatsächlichen Systemeinsatz muss der einzustellende Schwellwert entsprechend den gewünschten Fehlerraten aus den konkreten Referenzdaten geschätzt und gegebenenfalls adaptiert werden. Es ist dann zu prüfen, wie weit die tatsächlichen Fehlerraten von den theoretischen abweichen.

In einem praktischen System ist die Suche nach der idealen Wahl des Schwellwerts schwierig, wenn die Klassifikationswerte für erfasste und nichterfasste Nutzer zu nahe beieinander liegen. Dies wird z.B. mit einem zunehmend komplexeren Applikationsszenario wahrscheinlicher und kann dazu führen, dass die Einzelfehlerraten *FAR* und *FRR* bei nur kleinen Abweichungen von dem optimalen Schwellwert signifikant von der theoretischen *EER* abweichen können. Bei gleicher *EER* können also verschiedene Systeme in ihrem Verhalten um diesen idealen Punkt niedrigster Fehlerrate signifikant voneinander abweichen. Besitzen beispielsweise die *FAR*- und *FRR*-Kurve gemeinsam ein großes Tal, so wird dieses System im praktischen Einsatz eine kleinere Fehlerrate aufweisen als eines, bei dem *FAR* und *FRR* rechts und links neben dem idealen Schwellwert signifikant ansteigen. Zur Charakterisierung eines Systems müssen daher *FRR* und *FAR* im Bereich um den idealen Schwellwert herum betrachtet werden. Es wird daher neben der Angabe der *EER* als eindeutige Kenngröße des Systems die gleichzeitige gemeinsame Darstellung der charakteristischen *FAR*- und *FRR*-Fehlerkurven vorgeschlagen, so dass das Verhalten um den kritischen Punkt visualisiert werden kann.

### 3.2.7 Failure to Enrol Rate

Wie in Kapitel 2.2.4. dargelegt, kann das ausgewählte Verfahren ein biometrisches Merkmal verwenden, das keine 100%ige Verbreitung hat, nicht bei allen Nutzern innerhalb der Organisation des Betreibers vorhanden ist und somit nicht ausgewertet werden kann. Mit der *failure to enrol rate (FER)* wird der Prozentsatz der potentiellen Nutzer angegeben, bei denen das Enrolment nicht erfolgreich durchgeführt werden konnte. Als mögliche Ursachen sind die folgenden Aspekte zu berücksichtigen:

- Merkmal fehlt (Finger, Iris, etc..)
- Einschränkung in der Erfassung (Brille, Kontaktlinse, schwache Ausprägung des Merkmals)
- Fehlendes oder unzureichendes technisches Verständnis (Person beherrscht den Gebrauch auch nach Einführung nicht)
- Systemprobleme z.B. Sensorqualität, Algorithmen
- Fehlende Akzeptanz des Verfahrens (z.B. aus gesundheitlichen Bedenken)

Die FER ergibt sich wie folgt:

$$FER = \frac{NNE}{NPU} \cdot 100\% ,$$

wobei die Abkürzungen folgende Bedeutung besitzen:

- *NNE*: die Anzahl der Personen, bei denen das Enrolment nicht durchgeführt werden konnte  
(*number of not enrolled person*),
- *NPU*: die Gesamtanzahl (Population) der potentiellen Nutzer innerhalb der Organisation des Betreibers  
(*number of potential users*).

### 3.3 Statistische Signifikanz

Die Genauigkeit der Fehlerkurven zu einem Datensatz wird durch die Größe des Datensatzes bestimmt. Geht man von einer ungefähren statistischen Normalverteilung der Fehlerrate aus, so ergibt sich aus der Größe des verwendeten Datensatzes und einer festzulegenden Irrtumswahrscheinlichkeit die Genauigkeit der Fehlerrate. Jedoch wird in der Praxis die Fehlerrate durch die konkrete Anwendung und die umzusetzende Sicherheitsanforderung vorgegeben. Ein Betreiber eines biometrischen Systems muss sicher gehen, dass die wirkliche Fehlerrate, z.B. die FAR, mit hoher Wahrscheinlichkeit unterhalb einer bestimmten oberen Grenze liegt. Es ist demnach folgende Frage zu beantworten:

Wieviele Datensätze werden benötigt, um mit einer bestimmten Sicherheit sagen zu können, dass die Fehlerrate eines gegebenen biometrischen Systems unterhalb der bestimmten oberen Grenze gemäss der gewählten Sicherheitsanforderung liegt?

Statistisch gesprochen entspricht das der Anzahl benötigter Beobachtungen  $n_\tau$  zur Schätzung einer relativen Häufigkeit bei bekannter Varianz  $h$ , Irrtumswahrscheinlichkeit  $\tau$  und Genauigkeit  $\delta$ .

Das heißt für

- eine Sicherheit von 95% ( $\tau = 0.05$ ), d.h.  $Z_\tau = 1,96$  (siehe unten)
- eine FAR von 10% ( $h = 0,1$ ) sowie für
- eine maximale Abweichung der realen von der geschätzten Fehlerwahrscheinlichkeit von 5% ( $\delta = 0,05$ )

benötigt man nach der Formel

$$n_\tau = \frac{Z_\tau^2}{\delta^2} \cdot h \cdot (1-h)$$

mindestens 138 Datensätze (siehe auch Bild 3-7)<sup>2</sup>.

Der interessierte Leser sei z.B. auf das Buch von L. Sachs<sup>2</sup> verwiesen. Weitere

<sup>2</sup> Lothar Sachs, *Statistische Methoden: Planung und Auswertung*, Springer-Verlag Berlin Heidelberg New York, 7. Auflage, 1993.

wichtige Schranken der standardnormalverteilten Zufallsvariablen  $Z_\tau$  für den zwei-seitigen Test sind  $Z_\tau = 2,58$  (für  $\tau = 0.01$ ) und  $Z_\tau = 2,24$  (für  $\tau = 0.025$ ).

In Bild 3-7 sind Mindestzahlen  $n_\tau$  von Testpersonen angegeben mit  $Z_\tau = 1,96$ , die für eine bestimmte Sicherheitsklasse und  $FAR$  notwendig sind. Die Messung der  $FAR$  eines biometrischen Systems für die Sicherheitsklasse „sehr stark“ kann mehrere tausend Testpersonen erfordern. Es ist zu beobachten, dass die Anzahl der Testpersonen für ein biometrisches System wesentlich von der Differenz zwischen Sicherheitsanforderung (obere Grenze) und typischer Fehlerrate abhängt. So braucht ein Verfahren mit einer typischen  $FAR$  von 0,7% deutlich weniger Testpersonen für die Erreichung der Sicherheitsanforderung von 1,0% als ein Verfahren mit einer  $FAR$  von 0,8%, um der selben Sicherheitsanforderung zu genügen.

Wesentlich für die hier geführten Betrachtungen sind neben der Zahl der Messungen auch die Zahl der verschiedenen Personen, an denen gemessen wurde, sowie der Zeitraum, über den die Messungen durchgeführt wurden. Die Merkmale müssen also hinreichend verschieden sein.

Sicherheits- klasse	obere Grenze ( $FAR + \delta$ )	$\delta$	$FAR$	$n_\tau$
Schwach	15,0%	5,0%	10,0%	138
	10,0%	2,0%	8,0%	707
	5,0%	1,0%	4,0%	1475
Mittel	4,9%	0,9%	4,0%	1821
	3,6%	0,6%	3,0%	3105
	2,5%	0,5%	2,0%	3012
Stark	1,9%	0,4%	1,5%	3547
	1,5%	0,5%	1,0%	1521
	1,0%	0,3%	0,7%	2967
Sehr stark	1,0%	0,2%	0,8%	7622
	0,5%	0,1%	0,4%	15305
	0,3%	0,1%	0,2%	30671

Bild 3-7: Anzahl benötigter Testpersonen zur Bestimmung der  $FAR$  zu einer Sicherheitsklasse

## 4 Technisches System

Bei der Betrachtung der technischen Aspekte muss zwischen dem eigentlichen biometrischen Produkt (meist ein Sensor mit Zusatzsoftware), das das biometrische Merkmal erfasst, und dem Trägersystem (evtl. ein herkömmlicher Personalcomputer), das die erfasste Information weiterverarbeitet und auch den zugehörigen Datenspeicher verwaltet, differenziert werden.

### 4.1 Merkmalerfassung im System

#### a) Erfassung

- Enrolment: Die Aufnahme der ersten biometrischen Datensätze, die später bei der Identifizierung oder Verifikation des Nutzers als Grundlage der Referenzdaten herangezogen werden, muss mit großer Sorgfalt erfolgen. Das Enrolment ist daher von geschultem und erfahrenem Personal durchzuführen, das die Qualität des aufgenommenen Templates hinreichend beurteilen kann. Unmittelbar im Anschluss an das Enrolment sollte ein erster Probelauf erfolgen, um die Qualität des erstellten Templates zu überprüfen und ggf. eine neue Erfassung vorzunehmen.
- Einmalige, zeitpunktbezogene Erfassung, die nur aufgrund veralteter Daten nach einem längeren Zeitraum der Nutzung des biometrischen Systems wiederholt werden könnte.

#### b) Adaption

Bei der Adaption passt sich das System bei einer permanenten Erfassung den Änderungen des biometrischen Merkmals an, indem in der Datenbank die abgelegten Referenzdaten bei jeder Benutzung des Systems aktualisiert werden. Es besteht die Gefahr, dass nicht in der Datenbank enthaltene Personen nach mehreren Überwindungsversuchen durch die ständig erfolgende Adaption als eine in der Datenbank erfasste Person akzeptiert werden.

#### c) Erfassung mit / ohne Wissen des Benutzers

Bei einem großen Teil der Systeme erfolgt die Datenerfassung (Enrolment) der Benutzer mit ihrem Wissen. Eine bereits praktizierte Form der Erfassung ohne Wissen des Benutzers ist relativ einfach bei der Gesichtserkennung zu realisieren. Eine unbemerkte Erfassung sollte jedoch aus Gründen des Datenschutzes die absolute Ausnahme sein (siehe Kap.6.1.2 zu Datenschutzaspekten).

#### d) Anzahl der notwendigen Einzelerfassungen, bis ein Referenzdatensatz erstellt werden kann.

Für die Bildung des Referenzdatensatzes benötigen die verschiedenen biometrischen Systeme eine unterschiedliche Anzahl von Einzelerfassungen, die mit einer Erfassung beginnt und bis zu 15 und mehr Erfassungen ansteigen kann.

#### e) Überprüfung der Lebendigkeit des Benutzers, die sogenannte „Lebenderkennung“ wie z.B. bei der Fingerbildererkennung die Durchblutung des Fingers.

Systeme ohne Lebenderkennung können durch Nachbildungen überwunden werden und erfordern deshalb eine besondere Überwachung der Echtheit des Merkmals und damit auch des Systems.

- f) Sichere Übertragung der biometrischen Daten mit Verschlüsselung und mit Prüfung der Unversehrtheit der Daten.

## 4.2 Anforderungen aufgrund möglicher Einsatzorte

(nach Norm DIN EN 50133-veröff. 1998 und CC99 / ISO IS 15408)

Je nach Einsatzort des biometrischen Systems können die Anforderungen zur sicheren und störungsfreien Funktion des biometrischen Systems sehr unterschiedlich sein. Im Folgenden werden mögliche Einsatzorte biometrischer Verfahren genannt.

- a) Innenraum, aber eingeschränkt auf Wohn- / Büroumgebung
- b) Innenraum allgemein
- c) Im Freien, aber geschützt vor direktem Regen und Sonnenschein, oder Innenräume mit extremen Umweltbedingungen
- d) Im Freien ohne Schutz vor Witterungseinflüssen.

## 4.3 Sicherheitsanforderungen nach Einsatzort bzw. Anwendung

Die Sicherheitsanforderungen an biometrische Systeme unterscheiden sich erheblich nach Einsatzort bzw. Anwendungsfall. Für die Auszahlung eines Geldbetrages am Geldautomaten oder den Zutritt zu einem Hochsicherheitstrakt werden vollkommen andere Anforderungen an die Sicherheit des biometrischen Systems gestellt werden als z.B. bei einer Zutrittskontrolle zu einer ganz normalen Büroumgebung oder dem Login an einem Rechner zur Erledigung allgemeiner Büroaufgaben. Im Folgenden sind einige, hinsichtlich der Sicherheitsanforderungen sehr unterschiedliche Anwendungsfälle aufgeführt.

- a) Fest eingebautes, gesichertes Spezialgerät (z. B. Geldautomat)
- b) Gesicherte Umgebung mit Zutrittskontrolle (z.B. Rechenzentrum )
- c) Büroumgebung mit Zutrittskontrolle
- d) Zugangs- und Zugriffskontrolle zu Rechnern und Ressourcen (z.B. Login am PC)

## 4.4 Toleranz des biometrischen Verfahrens bzw. Systems

- a) auf verändertes Benutzerverhalten. Es kann durchaus vorkommen, dass ungeübte Nutzer bzw. solche, die das System bewusst provozieren, durch zu enge Toleranzgestaltung Probleme bei der Nutzung des Systems bekommen. Die Parameter des Verfahrens bzw. Systems müssen so ausgelegt sein, dass einerseits keine Falschakzeptanzen für Nichtberechtigte zustande kommen, aber andererseits auch bei verändertem Benutzerverhalten die Erkennung noch funktioniert und die Falschrückweisungsrate in vertretbaren Grenzen gehalten wird.
- b) auf Veränderung des Merkmals selbst. Über einen längeren Zeitraum unterliegen auch physiologische biometrische Merkmale Veränderungen, bzw. es können durch bestimmte Umstände auch zeitweilige Veränderungen dieser Merkmale auftreten (z.B. kann sich das Fingerbild durch handwerkliche Tätigkeiten fast von einem Tag zum anderen so stark verändern, dass der Erkennungsprozess nur noch sehr problematisch oder gar nicht mehr vollzogen werden kann). Auch verhaltensbasierte biometrische Merkmale sind durch bestimmte Ereignisse

Veränderungen unterworfen (z.B. die Stimme bei Erkältung). Die Toleranz der Verfahren und Systeme sollte daher möglichst so ausgelegt werden, dass nicht jede Veränderung des Merkmals zur Abweisung des berechtigten Benutzers führt, aber auch gleichzeitig die Falschakzeptanzrate so klein wie möglich gehalten wird.

- c) auf veränderte Umweltbedingungen (z.B. geänderte Beleuchtung oder geänderte Temperatur). Beim Einsatz biometrischer Systeme kann es zu sehr wechselhaften Umweltbedingungen und beim Einsatz im Freien auch zu den unterschiedlichsten Witterungsbedingungen kommen. Das muss zur Folge haben, dass der Toleranzbereich eines biometrischen Systems, dass für alle denkbaren Bereiche einsetzbar sein soll, auch in diesem Fall bestimmte Veränderungen zulassen können muss.

## 4.5 Mobilität

- a) Stationäre Lösung  
z. B.: Stationäre Lösung aufgrund der erforderlichen Hardwarevoraussetzung
- b) Mobile Lösung  
z. B.: Einsatz im Notebook, Palmtop, Mobiltelefon, Smartcards. Systeme mit eigenem Prozessor, auf dem die Referenzdaten abgelegt werden und auf dem gleichzeitig das Matching erfolgt.

## 4.6 Einsatzfelder

Biometrische Verfahren können in den verschiedensten Anwendungen zum Einsatz kommen und dabei für die Erhöhung der Sicherheit sorgen.

### 4.6.1 Zutrittsmechanismen

- Als „elektronischer Pförtner“ für die Zutrittskontrolle zu Gebäuden
- Zutrittskontrolle mit Zeiterfassung und Verweildauerkontrolle
- Zutrittskontrolle zu Sicherheits- und Hochsicherheitsbereichen

### 4.6.2 Zugriff / Zugang zu elektronischen Geräten/Daten

- Integration eines biometrischen Systems in bestimmten Applikationen, um damit den Zugriff auf sensitive Unternehmensdaten zu schützen.
- Zugang zum Computer (anstelle der Passworteingabe) oder zu Netzen bzw. Netz-Segmenten.
- Zugriff auf Geldautomaten (in Verbindung mit EC-Karte)
- Zugang zu Internetdiensten
- Zugang zum Mobiltelefon bzw. zu anderen sicherheitssensiblen Geräten
- Zugriff auf den Signiermechanismus bei der elektronischen Signatur (zur Vornahme elektronischer Transaktionen)

### 4.6.3 Weitere Einsatzfelder

- Quittierung eines Vorgangs anstelle einer Unterschrift oder einer Paraphe.

## 4.7 Art der Überprüfung

Grundsätzlich erfolgt die Überprüfung biometrischer Merkmale in zwei Betriebsarten, entweder durch eine Verifikation, bei der der Vergleich der neu erfassten Daten mit den Referenzdaten eins zu eins erfolgt oder durch eine Identifikation, bei der die übereinstimmenden Referenzdaten aus n Datensätzen herausgesucht werden müssen. (Weitere Erläuterungen siehe Kap. 1.4)

## 4.8 Technische Spezifikation des Systems

- a) Technische Systemarchitektur
- b) Beschreibung des Erfassungsterminals
- c) Maximale Anzahl von Nutzern / Referenzmustern in der Datenbank (Populationsgröße)
- d) Größe des abgespeicherten Referenzmusters
- e) Erfüllung bestehender Normen
- f) Portabilität auf andere Systemumgebungen / Betriebssysteme (allg.: Kompatibilität zu anderen Systemen / Kombination)
- g) Physikalische Angaben
  - Größe (B x H x T)
  - Gewicht
  - Stromaufnahme
  - Wärmeabgabe
  - weitere wichtige Angaben für die jeweilige Anwendung

## 4.9 Zertifizierung und Prüfzeichen

Wie alle Systeme der IT-Sicherheit sollten auch biometrische Systeme geprüft werden. Es gibt informelle, semiformale und formale Prüfungen.

Formale Evaluierungen gemäß den Common Criteria (CC) dürfen nur von akkreditierten Prüf- und Zertifizierungsstellen durchgeführt werden. Mit den CC steht ein international anerkannter Katalog von Kriterien zur Verfügung um IT-Sicherheitsmaßnahmen festzulegen. Daneben liefern die CC Vorgaben für die Prüfung und Bewertung von Sicherheitsanforderungen. Der Idee einer unabhängigen Analyse der Sicherheit wird also Rechnung getragen. Evaluationen laufen im Rahmen eines Zertifizierungsschemas ab, das aber außerhalb der CC liegt. Eine detaillierte Evaluationsmethodologie beschreibt die „Common Methodology for Information Technology Security Evaluation (CEM)“.

Die CC unterscheiden nicht nach der Korrektheit der Implementierung und der Wirksamkeit der Mechanismen, sondern sie führen sieben Vertrauenswürdigkeitsstufen (EAL1 - EAL7) ein. Je höher die Vertrauenswürdigkeitsstufe ist, um so höher ist auch das geforderte Qualitätsniveau. Verknüpft ist damit ein erhöhtes Vertrauen des Anwenders in die vom Hersteller angegebenen Sicherheitsmaßnahmen. Es bedeutet aber auch die Zunahme des erforderlichen Aufwandes für den erfolgreichen

---

Abschluss einer Evaluation, insbesondere des Umfangs der zu erstellenden Dokumentation.

In den CC wird das stark strukturierte Konzept der Klassen, Familien, Elemente und Komponenten verwendet. Der Katalog von Anforderungen berücksichtigt auch Abhängigkeiten von Komponenten untereinander und ist klassenübergreifend und vollständig. Folgende Funktionale Sicherheitsanforderungsklassen stehen zur Verfügung:

- Klasse FAU: Sicherheitsprotokollierung
- Klasse FCO: Kommunikation
- Klasse FCS: Kryptographische Unterstützung
- Klasse FDP: Schutz der Benutzerdaten
- Klasse FIA: Identifikation und Authentisierung
- Klasse FMT: Sicherheitsmanagement
- Klasse FPR: Privatsphäre
- Klasse FPT: Schutz der EVG-Sicherheitsfunktionen
- Klasse FRU: Betriebsmittelnutzung
- Klasse FTA: EVG-Zugriff
- Klasse FTP: Vertrauenswürdiger Pfad/Kanal

Vergleichbar zu obigen Ausführungen ist auch bei den Anforderungen an die Vertrauenswürdigkeit eine Struktur von Klassen, Familien, Komponenten und Elementen definiert. Folgende Liste zeigt im Überblick die in den CC festgelegten Klassen:

- Klasse ACM: Konfigurationsmanagement
- Klasse ADO: Auslieferung und Betrieb
- Klasse ADV: Entwicklung
- Klasse AGD: Handbücher
- Klasse ALC: Lebenszyklus-Unterstützung
- Klasse ATE: Testen
- Klasse AVA: Schwachstellenbewertung
- Klasse AMA: Erhaltung der Vertrauenswürdigkeit

Bei den Vertrauenswürdigkeitselementen unterscheidet man Anforderungen an den Entwickler, Inhalt und Form der Nachweise und Evaluatoren.

Insgesamt existieren ca. 30 Vertrauenswürdigkeitsfamilien, ca. 100 Komponenten der Vertrauenswürdigkeit und eine noch viel größere Zahl von Elementen. Um unter diesen Bedingungen Evaluationen besser miteinander vergleichen zu können, ist es sinnvoll, bestimmte Komponenten und Elemente zu gruppieren und in spezielle Pakete zusammenzufassen. Spezielle Pakete von Vertrauenswürdigkeitskomponenten bilden die EAL, von EAL1 – "funktionell getestet", bis EAL7 – "formal verifizierter Entwurf und getestet".

Durch solche „normierten“ Stufen der Vertrauenswürdigkeit und die unabhängige Überprüfung der gedachten und umgesetzten Gegenmaßnahmen, wie sie die CC ermöglichen, lässt sich eine Aussage zum Grad des Vertrauens treffen, das man in das geprüfte System haben kann.

In Rahmen des Projekts BIOKRIT werden zurzeit Prüfkriterien nach CC für zwei exemplarische biometrische Verfahren erarbeitet. Exemplarische "Protection Profiles" zu den CC wurden bisher in Großbritannien bei der Biometrics Working Group unter Mitarbeit von AG6-Mitgliedern erarbeitet.

## 4.10 Produktausprägung

Die Untersuchungen der T-Systems zeigten, dass nicht eine einzige reine Hardwarelösung existiert. Für den Matching-Prozess ist immer Software nötig. Bei allen Produkten, die als reine Evaluierungsverfahren vorlagen, wurde auch immer Hardware benötigt (z.B. Unterschriftsprüfung – Grafiktablett oder Stimme – Mikrofon und letztendlich zählt ja der Rechner, auf der die Software implementiert wird, auch als Hardware).

Es gibt auch Firmen, die Komplettlösungen anbieten, in denen Soft- und Hardware von unterschiedlichen Herstellern integriert wurde

- Sensor (Hardware)
- Sensorsoftware
- Erkennungssoftware
- Entwicklungstools
- Komplettlösung
- Integrierte Anwendung
- standalone Lösungen

## 4.11 Voraussetzungen an das Trägersystem

### 4.11.1 Hardware

Bei den auf dem Markt angebotenen biometrischen Systemen, die auf den verschiedensten biometrischen Merkmalen basieren, werden unterschiedliche Voraussetzungen an die Hardware gestellt. Viele Systeme kommen mit Standardhardware, also mit Rechnern, die im freien Handel angeboten werden, aus. Es sind aber auch (noch) Systeme auf dem Markt, die spezielle Hardware benötigen und z.B. zur weiteren Verarbeitung der mit dem Sensor erfassten Daten zusätzlich Videokarten verlangen und erhebliche Ressourcen des Rechners belegen.

- a) Hardwaresystem (Prozessor, Speicher, Bussystem)
- b) Zusatzkarten für Schnittstellen
- c) Standardhardware / Spezialhardware

### 4.11.2 Software

- a) Betriebssystem

Die für biometrisches Systeme bereitgestellte Software wird in vielen Fällen für alle Windowssysteme (Windows 9X, NT, 2000) angeboten, während einige Systeme aber auch bestimmte Betriebssysteme nicht bedienen. Eher selten kann die Software auch unter UNIX installiert werden.

- b) Einbindung des biometrischen Systems

Des weiteren ist von Interesse, ob und wie das biometrische System in übergeordnete System integriert werden kann. Der Hersteller sollte beschreiben, ob und mit welchem Aufwand die Integration erfolgen kann und ob zur Steuerung der biometrischen Komponente eine international standardisierte Schnittstelle zur Verfügung steht.

c) Applikationssoftware

Für jedes biometrische System muss eine Applikationssoftware zur Verfügung stehen, die für verschiedene Anwendungen einsetzbar sein kann wie z.B. Evaluationssoftware, Login oder Zugang, Zutrittskontrolle.

## 5. Sicherheitsqualität

### 5.1 Merkmalskriterien

- Grad der Einzigartigkeit des Merkmals
- Grad der Einzigartigkeit der extrahierten Daten
  - a) Fehlerraten und Trennschärfekriterien
  - b) False Acceptance Rate (*FAR*)
  - c) False Rejection Rate (*FRR*)
  - d) Equal Error Rate (*EER*)
  - e) Failure to Enroll Rate (*FER*)
  - f) Untersuchung der *FAR* / *FRR* in Abhängigkeit von einem Sicherheitsniveau
  - g) Untersuchung der Verteilung der Fehlerraten (Perzentilen / Varianzen)

### 5.2 Ermittlung der Qualitätskennzahlen

#### 5.2.1 Fehlerrate

False Acceptance Rate (*FAR*)

- a) Wurde die *FAR* im „true-vs-true“-Verfahren ermittelt?  
Bei der Bestimmung von Fehlerraten (*FAR*, *FRR*, etc.) ist die Verwendung von simulierten Daten zum Beispiel als Ergebnis von Hochrechnungen oder Interpolationen nicht zulässig. Es sind reine „wirkliche“ gemessene Daten zu verwenden.
- b) Wurden echte Angriffe zur Bestimmung der *FAR* unternommen?

#### 5.2.2 Versuchsanordnung

- a) Art des durchgeführten Versuches (Feldtest oder Labortest)
- b) Erfahrungsbericht
- c) Anzahl der Probanden
- d) Anzahl der durchgeführten Versuche
- e) Zusammensetzung der Testgruppe (ethnische Unterteilung, evtl. besondere Fähigkeiten wie Schreibmaschinenkenntnisse usw.)
- f) Gesamtdauer des Tests (Tage / Wochen / Monate)
- g) Motivation der Probanden

#### 5.2.3 Natürliche Variabilität der Referenzdaten

Biometrische Verfahren werden in verhaltensbasierte und physiologische Verfahren unterschieden. Verhaltensbasierte Verfahren, die auf dem Verhalten des Menschen beruhen, wie z.B. Unterschriftsverifikation, Tippdynamik oder Sprecherverifikation, unterliegen immer natürlichen Schwankungen, die, unabhängig von Schwankungen in der Datenaufnahme, immer zu unterschiedlichen Beispielcharakteristiken führen. Physiologische Eigenschaften des Menschen hingegen, wie z.B. Retinamuster oder Fingerabdruck, verändern sich hingegen meist nur über äußere Einwirkungen oder Schwankungen, die im Datenaufnahmeprozess begründet liegen. In beiden Fällen

sind im Vergleich zu den Referenzdaten unterschiedlich variable Datensätze die Folge. Diese natürliche Variabilität wird allerdings zusätzlich u.a. durch die Applikationsrandbedingungen und die Testpopulation verändert.

#### 5.2.4 Qualität der Referenzdaten

Schwankungen in der Qualität der Referenzdaten können auf folgenden Aspekten beruhen:

- Natürliche Referenzdatenvariabilität
- Applikationsszenario
- Sensorbedingte Variabilität - durch die Sensor-Mensch-Schnittstelle erzeugte Variabilität

Untersuchungen zur Erkennungsleistung (FRR, FAR) sollten möglichst alle relevanten Referenzdatenvariabilitäten abdecken bzw. zumindest den diesbezüglichen Wertebereich beschreiben. Für den praktischen Einsatz sollten insbesondere natürliche Variationen an den Referenzdaten nicht zur Verwechslung mit Fälschungen führen und daher im Test enthalten sein. Eine Mindestvoraussetzung ist daher die Erfassung der Streuung der Referenzdaten über einen relevanten Zeitraum.

#### 5.2.5 Art der Erhebung der Falschakzeptanzrate

Um die Falschakzeptanzrate zu bestimmen, müssen die Daten nicht erfasster Personen, biometrisch mit den Daten erfasster Personen verglichen werden. Dies kann durch Anwendung des Erkennungsalgorithmus auf eine Datenbank oder auch durch Testen von fertigen biometrischen Produkten durch reale Testpersonen geschehen. Die Höhe der Falschakzeptanzrate hängt maßgeblich davon ab, in welcher Art und Weise die biometrischen Daten der nicht erfasster Personen gewonnen wurden. Dabei werden zwei Arten unterschieden:

- **Zufällige biometrische Daten nicht erfasster Personen:**

Dies ist typischerweise der Fall, wenn die Daten aus einer biometrischen Datenbank genommen werden. Im Wesentlichen gibt ein solcher Test nichts anderes als die Klassifikationsleistung eines Systems wieder, d.h. inwieweit das System in der Lage ist, zwischen verschiedenen Personen zu unterscheiden.

- **Geübte Fälschungen:**

Hier ist den Testpersonen die erfasste biometrische Kennung bekannt und sie versuchen, diesen bestimmten erfassten Originalen so ähnlich wie möglich zu sein. Mit geübten Fälschungen erzeugte Fehlerraten werden im Normalfall wesentlich schlechter als solche mit zufälligen biometrischen Daten nichterfasster Personen sein. Geübte Fälschungen sind jedoch nicht für alle Verfahren möglich, sie erfordern manchmal extrem hohen Aufwand (z.B. einen künstlichen Ersatzkopf) oder abwegige, in der Regel praktisch nicht durchführbare Szenarien (z.B. abgeschnittener Finger). Insbesondere bei biometrischen Systemen, die mit verhaltensbasierten Merkmalen arbeiten, ist jedoch die Nachahmung durchaus praktikabel. Solche Fälschungen sollten auch verwendet werden, da ein seriöser Test eine pessimistische Abschätzung für den realen Einsatz liefern muss.

### 5.3 Ausspähbarkeit des Merkmals

Bei der Bewertung eines biometrischen Systems spielt die Aussage zur Ausspähbarkeit des biometrischen Merkmals eine wesentliche Rolle. Viele Merkmale sind als öffentliche Merkmale einzustufen. Sie werden ohne ausdrückliche initiative der Person hinterlassen bzw. sind passiv erfassbar - d.h. es kann auch keine Willensbekundung damit assoziiert werden. Dazu zählt beispielsweise der Fingerabdruck, den eine Person an vielen Orten unbeabsichtigt hinterlässt (Beispiel Glas). Derartige Merkmale sind als offen oder leicht verdeckt einzustufen und können die einem biometrischen System unterstellte Sicherheitsvermutung gegebenenfalls wesentlich einschränken.

- **offen** - Dieses Merkmal kann ohne weitere Hilfsmittel beobachtet werden. (z. B. Gesicht)
- **leicht verdeckt** - Ein Nebestehender kann dieses Merkmal beobachten (z. B. Fingerabdruck)
- **verdeckt** - Dieses Merkmal kann nur mit Hilfe eines bestimmten Detektors erfasst werden. (z. B. Retina-Muster)
- **diskret / schwer verdeckt** - Das Merkmal ist nicht direkt beobachtbar, sondern das Ergebnis, welches eine (geheime) Funktion aus dem Personenverhalten analysiert. Das Abhören von Messdaten bringt keine auswertbare Information.

### 5.4 Schutz des Systems vor Angriffen

#### 5.4.1 Aufwand eines Angriffs

Abgeleitet aus dem entstehenden Aufwand für einen Angreifer können verschiedene Klassen eines Angriffs festgelegt werden, die sich auf Angreiferklassen aus dem Umfeld der Elektrotechnik beziehen:

Klasse „niedrig“: Damit die Mindeststärke eines kritischen Mechanismus als **niedrig** eingestuft werden kann, muss erkennbar sein, dass er Schutz bietet gegen zufälliges unbeabsichtigtes Eindringen, d.h. geringer Aufwand der Angreifer, ohne Vorkenntnisse, mit einfachen Mitteln und ohne größeren Zeitaufwand, während er durch sachkundige Angreifer überwunden werden kann.

Klasse „mittel“: Damit die Mindeststärke eines kritischen Mechanismus als **mittel** eingestuft werden kann, muss erkennbar sein, dass er Schutz bietet gegen Angreifer mit beschränkten Gelegenheiten, d.h. alle allgemein zugänglichen Informationen als Vorkenntnisse und einige Stunden bis Tage als Zeitaufwand.

Klasse „hoch“: Damit die Mindeststärke eines kritischen Mechanismus als **hoch** eingestuft werden kann, muss erkennbar sein, dass er nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, d.h. auch Insider-Kenntnisse über das System und einige Wochen Zeitaufwand, Gelegenheiten und Betriebsmittel verfügen.

## 5.4.2 Allgemeine Systemrisiken

Zur Manipulation bzw. Überwindung eines biometrischen Systems durch einen unbefugten Eindringling sind prinzipiell die beiden folgenden Arten von Systemattacken zu unterscheiden:

- Direkte Täuschung des biometrischen Sensors
- Einspielung von Daten unter Umgehung des biometrischen Sensors

Die Möglichkeiten der direkten Täuschung des biometrischen Sensors hängen sehr vom individuellen biometrischen Verfahren ab.

In Bezug auf die Beschaffung in das System einzuspielender Daten gibt es für den Angreifer wiederum verschiedene Möglichkeiten:

Zum einen gibt es die sogenannten *Replay-Angriffe*, bei denen Daten (eventuell einschließlich kodierter Lebendigkeitsinformationen) aus dem Datenspeicher ausgelesen oder von der Übertragungsleitung abgehört und später wieder eingespielt werden. Darüber hinaus haben einige biometrische Verfahren die Eigenschaft, dass die biometrischen Merkmale eines Benutzers öffentlich verfügbar sind; hier besteht die Gefahr eines *Daten-Akquisitions-Angriffs*, bei dem sich ein Angreifer die biometrischen Merkmale verschafft, eigens digitalisiert und anschließend als Verifikationsdaten in das biometrische System einspielt.

Besonders zu beachten sind auch:

- a) Vandalismus
- b) Diebstahl
- c) Manipulation / Attrappe
- d) Insiderattacken
- e) Denial-of-Service Angriffe

## 5.4.3 Beispiele für biometricspezifische Angriffsszenarien

Im Folgenden werden beispielhaft denkbare Angriffsmodelle mit verschiedenem Aufwand auf biometrische Systeme vorgestellt.

### Biometrisches Merkmal Fingerabdruck

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

### Biometrisches Merkmal Stimme

- geringer Aufwand der Angreifer: Nachsprechen eines zugelassenen Nutzers
- mittlerer Aufwand der Angreifer: Hochwertiges Abhören und Wiedereinspielen
- hoher Aufwand der Angreifer: Erstellen eines akustischen Profils.

### Biometrisches Merkmal Unterschrift

- geringer Aufwand der Angreifer: Nachschreiben der Unterschrift
- mittlerer Aufwand der Angreifer: Schriftzug beobachten, mit hohem Aufwand Üben und Fälschen der Unterschrift
- hoher Aufwand der Angreifer: Eigenschaften des Erkennungsalgorithmus berücksichtigen, systematische Konstruktion eines Schreibmodells. Nutzung von Unterschriftensimulatoren.

### Biometrisches Merkmal Gesicht

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

### Biometrisches Merkmal Hand

- geringer Aufwand der Angreifer: Testen von Handgeometrien verschiedener Versuchspersonen
- mittlerer Aufwand der Angreifer : Anfertigen einer Handnachbildung z.B. nach einer Fotografie, Nutzung 2-dimensionaler Nachbildung
- hoher Aufwand der Angreifer: Herstellung und Nutzung 3-dimensionaler Nachbildung

### Biometrisches Merkmal Augen

Von den Möglichkeiten Iris- und Retinaerkennung soll hier vorrangig die Iriserkennung betrachtet werden.

- geringer Aufwand der Angreifer: Einsatz verschiedener Testpersonen, allerdings mit geringen Erfolgsaussichten
- mittlerer Aufwand der Angreifer: Anfertigen von Kontaktlinsen nach Fotografie, Erstellung eines Computer-Programms zur Simulation von Lebendigkeitseigenschaften (Augenzucken)
- hoher Aufwand der Angreifer: Herstellen von speziellen Kontaktlinsen und Augenmodellen.

### Biometrisches Merkmal Tippverhalten

- geringer Aufwand der Angreifer: Direkte Nachahmung des Tippverhalten durch Beobachtung
- mittlerer Aufwand der Angreifer: z.B. Videoaufzeichnung des Tippenden und Einüben der Sequenz
- hoher Aufwand der Angreifer: Nutzung Tippapparat, Unterschieben einer präparierten Tastatur.

## **6. Nicht-Technische Aspekte**

### **6.1 Juristische Aspekte**

Die rechtliche Einordnung einer biometrischen Erkennung und insbesondere die rechtlichen Anforderungen an einen Einsatz biometrischer Verfahren hängen von generellen Prinzipien der einschlägigen nationalen Rechtsordnungen ab. Die folgenden Überlegungen beziehen sich auf vornehmlich deutsche Regelungen. Neben grundsätzlichen Rahmenbedingungen sind auch bereichsspezifische Bedingungen zu beachten, bei denen es auf die ganz konkrete Anwendung ankommt. Zu den generellen Anforderungen unserer Rechtsordnung gehören etwa die Menschenwürde und der Grundsatz der Verhältnismäßigkeit. Die Menschenwürde ist grundsätzlich bei einem Einsatz von Biometrie dadurch betroffen, dass, auf natürliche Weise mit einem Menschen verbundene, körperliche Merkmale und Funktionen zu bestimmten (Erkennungs-)zwecken instrumentalisiert werden. Bedenklich kann dies dann sein, wenn jemand dazu verpflichtet wird, seinen Körper zu Zwecken der Informationsauswertung (für ein biometrisches Verfahren) zur Verfügung zu stellen. Auch die umfassende Katalogisierung der Persönlichkeit durch eine einheitliche Personenkennziffer kann einen Würdeverstoß darstellen, wie das BVerfG in dem bekannten Volkszählungsurteil festgestellt hat. Verhältnismäßigkeit ist überall dort gefordert, wo widerstreitende Interessen auftreten können, hier vor allem die des Betreibers einerseits und die des Nutzers andererseits.

Abhängig vom Anwendungsumfeld sind beim Einsatz biometrischer Verfahren unterschiedliche rechtliche Anforderungen zu beachten. Im staatlichen Bereich können neben verfassungsrechtlichen Grundsätzen straf(prozessuale) Regelungen beim Einsatz durch Strafverfolgungsbehörden, Pass- und Personalausweiswesen, Asylverfahrensregelungen, Grenzkontrollvorschriften (Bundesgrenzschutzgesetz), Sozial(versicherungs)recht eine Rolle spielen. In datenschutzrechtlicher Hinsicht ist bei einem verpflichtenden Einsatz von Biometrie grundsätzlich eine gesetzliche Grundlage erforderlich.

### **6.2. Datenschutz**

#### **6.2.1. Einleitung**

Biometrische Verfahren arbeiten mit spezifischen körperlichen Merkmalen, die bestimmten natürlichen Personen zugeordnet werden. Biometrische Informationen sind daher grundsätzlich personenbezogene Daten. Sie unterliegen damit in aller Regel dem Schutz des informationellen Selbstbestimmungsrechts, das das Bundesverfassungsgericht bereits 1983 im sog. Volkszählungsurteil aus dem verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrecht entwickelt hat. Das informationelle Selbstbestimmungsrecht enthält für die Betroffenen (d.h. die Nutzer) die Befugnis, grundsätzlich selbst über Preisgabe und Verwendung ihrer Daten zu bestimmen.

Konkret bedeutet das für biometrische Anwendungen: Wird die flächendeckende Einführung eines biometrischen Systems im staatlichen Bereich geplant (z. B. zur Kontrolle der Berechtigungen bei staatlicher Leistungsvergabe etc.), so ist dies nur aufgrund eines Gesetzes möglich, das – wie alle Gesetze – dem Verhältnismäßigkeitsgrundsatz entsprechen muss. (Etwas anderes gilt allerdings, wenn Systeme lediglich für die Abwicklung des internen Betriebs bei staatlichen Stellen eingeführt

werden, wie z.B. Zugangssysteme.) Beim Einsatz biometrischer Verfahren im privaten Bereich sind die entsprechenden Vorschriften des Bundesdatenschutzgesetzes über die nicht-öffentlichen Stellen zu beachten.

In das Bundesdatenschutzgesetz (BDSG) von 2001 sind die Grundsätze der Datenvermeidung und Datensparsamkeit als allgemeine Grundsätze aufgenommen worden, die bei der Auswahl von Datenverarbeitungsanlagen beachtet werden müssen. Bei den einzelnen Verarbeitungsschritten, insbesondere Datenerhebung und -verarbeitung, ist dann zu beachten, inwieweit diese Daten überhaupt erforderlich sind. Für den Einsatz eines biometrischen Systems bedeutet dies u.a., dass, wenn alternative Methoden zur Verfügung stehen, die datenschutzfreundlichste Lösung gewählt werden muss, was im Einzelfall auch die Wahl eines nicht-biometrischen Systems bedeuten kann. Beim Einsatz eines biometrischen System aber kommt es vor allem auf die nachfolgend im Einzelnen erwähnten Aspekte an.

Neben etwaigen datenschutzrechtlichen Beschränkungen gibt es auch Vorschriften, die aus Datenschutzsicht für die Einführung (entsprechend gestalteter) biometrischer Verfahren sprechen. So kann vor allen Dingen im Bereich der Datensicherheit ein höheres Niveau erreicht werden. Die Gewährleistung der Datensicherheit umfasst u.a. die Zugangskontrolle, die Benutzerkontrolle und die Zugriffskontrolle und ist nach § 9 BDSG (bzw. den entsprechenden Vorschriften der Länder) geboten.

Optimal ist der Einsatz biometrischer Verfahren dann, wenn datenschutzrechtliche Klippen umschiffen, also rechtliche Anforderungen eingehalten und gleichzeitig Datenschutz und Datensicherheit gefördert werden können; in diesem Fall spricht man von sogenannten *datenschutzfördernden Techniken (privacy enhancing technologies-PET)*.

## 6.3 Problemfelder bei der Verwendung biometrischer Daten

Biometrische Daten weisen im Gegensatz zu anderen personenbezogenen Daten gewisse Besonderheiten auf, die in den folgenden Abschnitten diskutiert werden. Zusätzlich werden Gestaltungshinweise für biometrische Verfahren gegeben, um den aufgeführten Problemen in der Praxis zu begegnen.

### 6.3.1 Datenvermeidung und -sarsamkeit

Das BDSG schreibt vor, bei der Datenerfassung und -speicherung deren Erforderlichkeit genau zu beachten (d.h., sich sparsam zu verhalten).<sup>3</sup> So ist es zum bloßen Feststellen der Identität bzw. Berechtigung in den meisten Anwendungsumgebungen überhaupt nicht erforderlich, die einzelnen Identifikationsvorgänge zu speichern. Wird von vornherein darauf verzichtet, Daten zu erheben und zu speichern, entstehen keine Datenbestände, die dann auch nicht missbraucht werden können. Sollte dennoch eine Datenerhebung, etwa für eine erforderliche Protokollierung, notwendig sein, muss sich diese auf den angemessenen Umfang beschränken. Das bedeutet, dass nur die Daten erhoben und gespeichert werden dürfen, die für die eigentliche Erkennung auch tatsächlich notwendig sind. Zudem müssen (interne) Regelungen getroffen werden, wann, wie und durch wen die Protokolldateien auszuwerten und zu löschen sind. Dazu gehört die vorherige Regelung von Zugriffsrechten, die restriktiv vergeben werden sollten und etwa durch das Vier-Augen-Prinzip zusätzlich beschränkt werden können. Darüber hinaus sollte

<sup>3</sup> Stichwort „Datensparsamkeit“, §3a BDSG

auch geregelt werden, in welchen zeitlichen Abständen Protokolldaten wieder aus der Datenbank gelöscht werden müssen.

### **6.3.2 Keine unbemerkte Erhebung der biometrischen Daten**

Bei biometrischen Verfahren sollte grundsätzlich ausgeschlossen sein, dass ohne Kenntnis der Betroffenen von diesen ein biometrisches Merkmal technisch erfasst wird. Vielmehr sollte in jedem Fall die willentliche Mitwirkung des Nutzers erfolgen. Dies gilt sowohl für die Referenzdatenerfassung als auch für die spätere Überprüfung des biologischen Merkmals des Betroffenen. Eine aktive Mitwirkung des Nutzers macht das Verfahren zudem transparenter, baut daher vermutlich unberechtigte Ängste ab und trägt somit zur Akzeptanz des Systems bei. Wegen Verletzung des Rechts auf informationelle Selbstbestimmung sind daher grundsätzlich solche Installationen abzulehnen, bei denen z.B. beim bloßen Passieren einer bestimmten Stelle, für die Betroffenen unerkennbar, biometrische Merkmale erfasst werden.

### **6.3.3 Informationsgehalt der biometrischen Daten**

Zur Wahrung des informationellen Selbstbestimmungsrechts der Betroffenen sollten biometrische Verfahren eingesetzt werden, bei denen sich aus den Identifikationsdaten kein sog. überschießender Informationsgehalt ergibt, der für den eigentlichen Zweck der Authentisierung nicht notwendig ist. Rückschlüsse auf den gesundheitlichen Zustand des Merkmalsträgers sollten daher von vornherein technisch nicht möglich sein, oder aber jedenfalls nicht ausgewertet werden. Da üblicherweise aus den biometrischen Rohdaten solche Rückschlüsse leichter als aus den Referenzdaten (Templates) gezogen werden können, sollte auf die Speicherung von Rohdaten ganz verzichtet werden. Bei solchen zusätzlichen Informationen unterliegen biometrische Daten als besondere Arten personenbezogener Daten weiteren Beschränkungen in der Verarbeitung<sup>4</sup>.

Hierbei ist auch zu beachten, dass die diesbezüglich technische Machbarkeit einzelner biometrischer Verfahren noch nicht abschließend wissenschaftlich erforscht ist und daher auch mögliche, erst in der Zukunft entdeckte Zusatzinformationen berücksichtigt werden müssen.

### **6.3.4 Rückschließbarkeit auf die hinter den biometrischen Daten stehende natürliche Person**

Die Möglichkeit, aus den Identifikationsdaten unmittelbar auf die dahinterstehende natürliche Person rückschließen zu können, sollte erschwert oder ausgeschlossen werden. So gibt es biometrische Rohdaten, die auch eine manuelle Identifikation zulassen (etwa Bilder von Gesichtern) - diese sollten nicht gespeichert werden, wenn sie nicht unbedingt (etwa für Protokollzwecke) gebraucht werden.

Es sind Verfahren bekannt, die bei der Verarbeitung der biometrischen Eingabedaten für den Vergleich mit den Referenzdaten beispielsweise zusätzlich noch eine Zufallszahl einfließen lassen, die nur auf einer Chipkarte im Besitz des Betroffenen gespeichert ist. Der Rückschluss aus den Referenzdaten alleine auf die natürliche Person ist in diesem Fall nicht möglich, es bedarf vielmehr zusätzlich der Chipkarte. Auch sollte ausgeschlossen werden, dass aus mehreren biometrischen Identifikationen, sozusagen akkumulierend, auf die natürliche Person rückschließen werden kann, etwa indem mit Hilfe des Merkmals mehrere Datenbestände verknüpft werden.

---

<sup>4</sup> nach §3 IX BDSG

### **6.3.5 Dauerhaftigkeit der Bindung zwischen biometrischen Daten und Personen**

Beim Erzeugen von biometrischen Datenbeständen (Referenzdaten, Eingabedaten, Rohdaten) muss bedacht werden, dass die Bindung zwischen den Daten und der Person in den meisten Fällen auf natürliche Weise gegeben ist und dauerhaft anhält. Dadurch ergibt sich eine noch über lange Zeit hinweg wirkende Missbrauchsgefahr der Daten. Abhilfe können hier solche Verfahren schaffen, die bei der Berechnung der Referenzdaten noch weitere, veränderbare Daten mit einbeziehen (etwa Zufallszahlen) oder auf willkürlich veränderbaren biometrischen Merkmalen basieren.

### **6.3.6 Ort der Speicherung der biometrischen Daten**

Werden die biometrischen (Referenz-)Daten beim Nutzer (z.B. auf einer Chipkarte, einem Token oder einer anderen mobilen Speichereinheit) gespeichert, so hat dieser eher die Möglichkeit der Kontrolle über seine Daten. Ein zentraler Datenbestand birgt dagegen Gefahren für das informationelle Selbstbestimmungsrecht, nicht zuletzt wegen der weitgehenden Übermittlungsbefugnisse im Privatbereich und der umfassenden Datenerhebungsbefugnisse der Strafverfolgungsbehörden. Je mehr Daten zentral abgelegt werden und auf diese zumindest theoretisch zugegriffen werden kann, je größer sind die Begehrlichkeiten, die bei Behörden und privaten Stellen entstehen können. Kann auf eine zentrale Speicherung der Referenzdaten auch nach sorgfältiger Abwägung nicht verzichtet werden (etwa weil der Umgang mit individuellen Speichermedien wie Chipkarten bei der betrachteten Anwendung für Nutzer und Betreiber unzumutbar ist), so müssen insbesondere die Zugriffsbefugnisse genau definiert sein. Über etwaige Übermittlung an Dritte müssen die Betroffenen im Allgemeinen informiert werden.

Ein weiteres Problem besteht darin, dass zentrale Datenbestände üblicherweise ohne Wissen (und Zutun) des Benutzers ausgewertet werden können, was ebenso dessen Selbstbestimmungsrecht einschränkt. Der Einsatz identischer Verfahren in unterschiedlichen Anwendungen führt für den Nutzer zu erhöhten Risiken, da sein biometrisches Merkmal als ein (im Gegensatz zu Namen und Adresse) unveränderbares Personenkennzeichen verwendet werden und sein jeweiliges Nutzungsverhalten zu einem umfassenden Profil zusammengeführt werden kann. Eine dezentrale Speicherung ist daher in den allermeisten Fällen vorzuziehen.

## **6.4 Konkrete Empfehlungen beim Einsatz biometrischer Verfahren aus datenschutzrechtlicher Sicht**

### **6.4.1 Allgemeine Anforderungen**

Generell muss darauf geachtet werden, dass die Verfahren für die Nutzer transparent sind, die Revisionsfähigkeit gegeben ist und eine ausreichende Dokumentation der Datenverarbeitung (Software, Hardware, Datenfluss, organisatorisches Umfeld, Sicherheitsmaßnahmen) erfolgt. Dies ergibt sich bereits aus den allgemeinen Anforderungen an IT-Systeme. Werden personenbezogene Daten verarbeitet, finden sich entsprechende Regelungen in den Vorschriften über die Datensicherheit in den Datenschutzgesetzen<sup>5</sup>. Die betrieblichen Datenschutzbeauftragten sollten bei Einführung und Betrieb der Verfahren einbezogen werden; unter bestimmten Voraussetzungen *müssen* sie sogar (im Rahmen einer

<sup>5</sup> s. z.B. Anlage zu §9 Bundesdatenschutzgesetz (BDSG) und die sich daraus ergebenden Pflichten.

sogenannten "Vorabkontrolle") eingebunden werden.<sup>6</sup> Daneben ist der Grundsatz der *Zweckbindung* zu beachten, der eine Nutzung der Daten zu anderen Zwecken als denen, für die die Datenerhebung ursprünglich erfolgte, grundsätzlich nicht zulässt. So dürfen beispielsweise Protokolldaten, die aus Gründen der Datensicherheit angelegt wurden, nur zur Revision der Datenverarbeitung und nicht für andere Zwecke verwendet werden (s. § 31 BDSG).

#### 6.4.2 Biometrische Daten als personenbezogene Daten

Personenbezogene Daten im Sinne von § 3 Abs.1 BDSG liegen immer dann vor, wenn sich die fraglichen Informationen einer bestimmten natürlichen Person zuordnen lassen. Bei biometrischen Datensätzen muss grundsätzlich davon ausgegangen werden, dass ein Personenbezug herstellbar ist. Grundsätzlich sind Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift es erlaubt oder anordnet, oder der Betroffene eingewilligt hat<sup>7</sup>.

##### 6.4.2.1 Rechtsvorschriften als Zulässigkeitstatbestand

Es kommen mehrere Rechtsvorschriften in Betracht, die eine Zulässigkeit für die Datenerhebung, -verarbeitung und -nutzung begründen: Dies können zum einen die Zulässigkeitstatbestände nach § 28 Abs.1 BDSG sein; sie umfassen im Wesentlichen:

- Datenerhebung, -verarbeitung und -nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient<sup>8</sup> (Beispiel: Speicherung von Uhrzeit und Ort bei Abhebungen an Geldautomaten im Rahmen eines Kontoführungsvertrages mit einer Bank, nicht aber der Einsatz eines Gesichtserkennungssystems durch eine Hotelkette, um Hotelgäste bei *weiteren* Besuchen am Empfangstresen namentlich begrüßen zu können),
- Datenerhebung, -verarbeitung und -nutzung zur Wahrung berechtigter Interessen der verantwortlichen Stelle<sup>9</sup>, soweit diese erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Beispiel: Interessen eines Arbeitgebers an der Absicherung eines Systems zur Vermeidung von Schäden, etwa in Rechenzentren, zum Diebstahlschutz etc. Allerdings müssen hier immer die schutzwürdigen Interessen der Arbeitnehmer abgewogen werden; zusätzlich müssen deren Mitbestimmungsrechte beachtet werden, siehe Abschnitt Mitbestimmungsrechte).

Nach § 28 Abs.1 S. 2 BDSG muss zudem beachtet werden, dass bei einer Datenerhebung stets die Zwecke, für die die Daten verarbeitet oder genutzt werden, konkret festzulegen sind; eine nachträglich Zweckänderung ist nur in Ausnahmefällen möglich. Dies bedeutet beispielsweise, dass bei der Einführung eines biometrischen Systems durch einen Arbeitgeber als Zutrittskontrolle eine gleichzeitige Verwendung der Daten zur Zeiterfassung für die spätere Lohnabrechnung im Vorfeld geregelt sowie dem Arbeitgeber mitgeteilt werden muss.

<sup>6</sup> s. §4d Abs. 5 BDSG.

<sup>7</sup> § 4 Abs.1 Bundesdatenschutzgesetz (BDSG)

<sup>8</sup> § 28 Abs.1 Nr. 1 BDSG

<sup>9</sup> § 28 Abs.1 Nr. 2 BDSG

Als weitere Rechtsvorschrift kommt insbesondere beim Einsatz biometrischer Verfahren am Arbeitsplatz neben einem Tarifvertrag auch eine Betriebsvereinbarungen in Betracht, die dann sowohl die Berücksichtigung der Arbeitnehmerrechte regelt (siehe auch Abschnitt Mitbestimmungsrechte) als auch die Rechtsgrundlage für die Datenverarbeitung darstellt. Um eine Datenverarbeitung im Sinne von § 4 Abs. 1 BDSG legitimieren zu können, werden allerdings an Form und Inhalt einige Anforderungen gestellt:

- Zum einen muss sie die Verarbeitung personenbezogener Daten *ausdrücklich* für zulässig erklären.
- Aus ihr müssen sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Arbeitnehmer erkennbar ergeben ("Gebot der Normenklarheit").
- Der Grundsatz der Verhältnismäßigkeit muss beachtet werden (Abwägung der widerstreitenden Interessen).
- Schließlich darf sie nicht wesentlich zu Lasten des Arbeitnehmers von den Vorschriften des Bundesdatenschutzgesetzes abweichen.

Umsetzungsprobleme können meist bei der Interpretation von zivilrechtlichen Altverträgen (etwa Verträgen mit Bankkunden) entstehen, wenn nämlich diese bei neuen Sachverhalten (etwa die Neueinführung eines biometrischen Verfahrens) daraufhin überprüft werden müssen, ob die bestehenden Verträge die neue Anwendung ebenfalls abdecken. Häufig schaffen eine Vertragsänderung bzw. der Abschluss eines Neuvertrages oder aber Vereinbarungen, die für alle Nutzer gültig sind, mehr Klarheit.

#### 6.4.2.2 *Einwilligung der Betroffenen*

In der Neufassung des BDSG 2001 wurden die Anforderungen an einen datenschutzrechtlich wirksame Einwilligung<sup>10</sup> präzisiert: Sie muss *freiwillig, informiert* und *bestimmt* sein. Dies bedeutet im Einzelnen: Sie muss auf der freien Entscheidung des Betroffenen beruhen, den Zweck und Umfang der vorgesehenen Datenverarbeitung festlegen und ausreichende (und verständliche) Informationen über diese enthalten, damit der Betroffene in etwa die Tragweite seiner Entscheidung absehen kann. Daneben gibt es gewisse formale Vorschriften, etwa dass eine datenschutzrechtliche Einwilligung im äußeren Erscheinungsbild von anderen Erklärungen hervorgehoben sein muss und grundsätzlich schriftlich zu erfolgen hat.

Insbesondere die Anforderungen an eine informierte Entscheidung setzen voraus, dass dem Betroffenen der Gang der Datenverarbeitung, der Ort der Speicherung etc. verständlich, d.h. unkompliziert und ohne verwirrende technische Details, vermittelt wird. Da eine umfassende Aufklärung üblicherweise hilft, Ängste abzubauen, wird eine ausreichende Transparenz voraussichtlich auch die Akzeptanz der Nutzung des Verfahrens steigern. Hinzu kommt, dass die Bedienung und Handhabung erfahrungsgemäß gerade bei biometrischen Systemen leichter fällt, wenn die Arbeitsweise des Systems bekannt ist.

Zu beachten ist, dass der Zweck und Umfang der Datenverarbeitung zum Zeitpunkt der Einwilligung festgeschrieben wird und ohne erneute Einwilligung nur noch marginal, nicht aber in wesentlichen Punkten geändert werden darf. Insbesondere darf ohne Einwilligung keine Datenübertragung an Dritte erfolgen, sofern nicht gesetzlich zugelassene Gründe vorliegen. Vor einer solchen Datenübermittlung ist zu

---

<sup>10</sup> § 4 a BDSG

prüfen, inwieweit schutzwürdige Belange des Betroffenen überwiegen. Ist dies der Fall, ist eine solche Übertragung zu unterlassen; ggf. müssen die Betroffenen von der Übermittlung benachrichtigt werden.

Probleme bei der Verwendung von Einwilligungen können sich ergeben, wenn Zweifel an der Freiwilligkeit der Einwilligung auftreten: Dies dürfte etwa im Rahmen bestehender Arbeitsverhältnisse der Fall sein, wenn Arbeitnehmer bei Nichterteilung der Einwilligung (unausgesprochener Weise) mit beruflichen Nachteilen oder sogar Kündigung zu rechnen hätten. Eine Regelung mittels Betriebsvereinbarungen oder Tarifverträgen ist daher einzelvertraglichen Vereinbarungen vorzuziehen.

## 6.5 Weitere juristische Fragen

Soll mittels eines biometrischen Verfahrens z.B. der Signiermechanismus einer elektronischen Signatur freigeschaltet oder ein biometrisches System im elektronischen Rechts- und Geschäftsverkehr im weitesten Sinne eingesetzt werden, stellt sich die Frage, welche zivil- und zivilprozessrechtlichen Voraussetzungen bestehen und welche Rechtsfolgen eintreten können.

### 6.5.1 Anwendung biometrischer Merkmale bei elektronischen Signaturen

Die Anwendung biometrischer Verfahren im Rahmen elektronischer Signaturen ist nach den entsprechenden Vorschriften in SigG und SigV zulässig. Das bedeutet, dass auch bei der sog. qualifizierten elektronischen Signatur, die besondere Voraussetzungen erfüllen muss, biometrische Merkmale zur Identifikation des Signaturschlüssel-Inhabers eingesetzt werden dürfen<sup>11</sup>. Die Besonderheit der qualifizierten Signatur liegt darin, dass zum einen besondere Anforderungen an die technische und organisatorische Sicherheit gestellt werden, wie z.B. an die sog. sichere Signaturerstellungseinheit (in der Regel die Signaturkarte). Zum anderen sind an die Verwendung der qualifizierten elektronischen Signatur bestimmte materielle und prozessuale Rechtsfolgen geknüpft (s. unten) Das biometrische Merkmal darf hier das wissensbasierte Verfahren, also PIN oder Passwort ersetzen, muss aber zusätzlich an ein Besitzelement gekoppelt werden, d.h. die Verwendung eines Besitzelements wie etwa einer Karte ist auch mit Biometrie obligatorisch<sup>12</sup>. Die mit einer biometrisch gesicherten elektronischen Signatur versehene elektronische Willenserklärung hat bei entsprechend technischer Gestaltung und Einhaltung von Sicherheitsanforderungen voraussichtlich einen höheren Beweiswert vor Gericht als eine elektronische Signatur, die nur mit PIN abgesichert wurde.

Auf die Verwendung biometrischer Verfahren angewendet bedeutet dies folgendes: wird das Gericht von einer hohen (Überwindungs-)Sicherheit des biometrischen Verfahrens überzeugt sein, wird A schwerlich beweisen können, dass er die von X vorgelegte Bestellung nicht aufgegeben hat. A muss also für die Bestellung einstehen und zahlen, wenn er nicht nachweisen kann, dass die Verwendung der Signatur ausnahmsweise doch durch einen Dritten möglich war. Kommt das Gericht dagegen zur Überzeugung, dass der (biometrisch geschützte) Zugang zur verwendeten elektronischen Signatur von einem Unberechtigten (theoretisch) überwunden werden konnte, wird die Firma die behauptete Bestellung nicht durchsetzen können, A muss nicht zahlen. Bei der rechtlichen Beurteilung ist also entscheidend, inwieweit das Gericht von der Sicherheit des eingesetzten

<sup>11</sup> §§ 17 Absatz 1 Satz 1 SigG in Verbindung mit 15 Absatz 1 SigV

<sup>12</sup> § 15 Absatz 1 Satz 1 SigV

biometrischen Systems überzeugt werden kann. Zu hohe Technikgläubigkeit kann hier genauso zu ungerechten Ergebnissen führen wie unbegründete Zweifel.

### **6.5.2 Verwendung einer qualifizierten elektronischen Signatur**

Bestimmte formgebundene Rechtsgeschäfte, die früher nur mit der eigenhändigen Unterschrift wirksam waren, können heute auch mit der qualifizierten elektronischen Signatur erfolgen (§ 126a BGB). Eine Bindung an eine bestimmte Form erfolgt stets nur dann, wenn dem Rechtsgeschäft eine besondere Bedeutung zukommt, die Beteiligten sich etwa des besonderen Risikos bewusst werden sollen, das sie eingehen (Warnfunktion mit Übereilungsschutz), oder für den Fall eines späteren Rechtsstreits ein Beweis besonders wichtig ist (Beweisfunktion). Bei der elektronischen Form macht das Gesetz keinen Unterschied danach, ob die Signatur mittels PIN oder Biometrie freigeschaltet wurde. In der Praxis, insbesondere vor Gericht, kann dies aber in Zukunft einen erheblichen Unterschied machen. Aufgrund der bekannten Schwächen einer PIN kann niemals sicher davon ausgegangen werden, dass auch wirklich der berechtigte Signaturinhaber die Signatur abgegeben hat.

Neben dieser elektronischen Form wird der qualifizierten elektronischen Signatur auch in prozessualer Hinsicht ein „Vertrauensvorschuss“ gewährt. Wird diese verwendet, wird per Gesetz nunmehr zunächst vermutet, dass diese auch tatsächlich vom berechtigten Signaturinhaber verwendet wurde (§ 292a ZPO). Der Gesetzgeber hat hierfür einen gesetzlichen Beweis des ersten Anscheins geschaffen. Dies führt dazu, dass der Signaturinhaber, dessen Signatur durch einen unberechtigten Dritten missbraucht wurde, de facto beweisen muss, dass dieser mit seiner PIN und Signaturkarte eine Signatur in seinem Namen und ohne sein Wissen abgeben konnte.

Welche praktischen und rechtlichen Auswirkungen kann nun der Einsatz biometrischer Merkmale bei der qualifizierten Signatur haben?

Beim Einsatz biometrischer Verfahren anstelle der PIN kann grundsätzlich davon ausgegangen werden, dass ein Missbrauch nicht so einfach möglich ist – wenn das biometrische System entsprechend gegen Missbrauch abgesichert ist und die in Kap. 5 dargestellten Überwindungsmöglichkeiten so weit wie möglich ausgeschlossen wurden. Dann würde die Annahme der elektronischen Form sowie der Beweis des ersten Anscheins eher gerechtfertigt sein. Allerdings kommt es auch hier entscheidend auf die tatsächliche und überprüfbare Sicherheit des Systems an. Ist dieses nämlich nur vermutet sicher (ähnlich wie bei der PIN), darf einem Nutzer das „Restrisiko“ nicht zugerechnet werden: dieser würde sonst im Zweifelsfall für eine Signatur haften, die er nicht abgegeben hat, und nur mit erheblichen Schwierigkeiten nachweisen können, dass sein biometrisches Merkmal nachgemacht oder verfälscht wurde. Unberechtigte Technikgläubigkeit würde daher die Situation für alle Beteiligten verschlechtern.

### **6.5.3 Personaldokumente**

Im Bereich von Personaldokumenten können biometrische Merkmale die bisher auf Personalausweis oder Führerschein schon vorhandenen persönlichen Charakteristika ergänzen, indem etwa zusätzlich zum Passfoto ein Fingerbild auf dem Dokument abgelegt wird. Im Gegensatz zu den bisher auf den Dokumenten befindlichen Fotos und Angaben zu Augenfarbe und Körpergröße können biometrische Merkmale automatisiert ausgewertet werden und insofern auch für

dritte Stellen von Interesse sein. Biometrische Verfahren würden dabei an die Stelle des bisher manuell ausgeführten Vergleichs von Ausweis und Ausweisträger treten oder diesen ergänzen. Im Terrorismusbekämpfungsgesetz, das am 01.01.2002 in Kraft getreten ist, wurden die Rechtsgrundlagen für die Aufnahme biometrischer Merkmale in Pässe und Personalausweise geschaffen. Danach dürfen sowohl Pass als auch Personalausweis nunmehr „neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Pass-/Personalausweisinhabers enthalten“. Diese Merkmale dürfen auch in verschlüsselter Form eingebracht werden. Weiter bestimmt das Gesetz, dass die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form sowie die Art ihrer Speicherung, ihrer Verarbeitung und Nutzung durch ein weiteres Bundesgesetz geregelt werden. Schließlich wurde bestimmt, dass eine bundesweite Datei nicht eingerichtet wird.

Darüber hinaus kann ein biometrisches Verfahren auch dazu verwendet werden, die Identität des Antragstellers zweifelsfrei nachzuweisen, um so Missbrauchs- und Betrugsfälle bei der Ausweiserstellung zu minimieren. Dazu ist aber die Speicherung der biometrischen Daten *aller* Ausweisinhaber erforderlich, mit denen die Daten eines neuen Antragstellers abgeglichen werden. Eine solche zentralisierte Datenspeicherung vieler Betroffener ist allerdings sehr bedenklich und widerspricht der grundsätzlichen Forderung nach möglichst dezentraler Datenverarbeitung (s. oben)

Im Rahmen einer großflächigen Einführung muss außerdem bedacht werden, dass wegen der Vielzahl der biometrischen Vergleiche auch bei kleinen Fehlerraten die absolute Anzahl von Fehlentscheidungen recht groß werden kann. Hier sind sinnvolle Regelungen mit dem Umgang von Zurückweisungen durch das biometrische System erforderlich, denn die große Zahl von sowohl berechtigten Zurückweisungen als auch fehlerhaften Entscheidungen kann sowohl zu bedingungslosem Technikglauben ("der Computer hat immer recht" ) als auch zum Vertrauensverlust in die Technik ("der Computer funktioniert mal wieder nicht") verleiten. Zu berücksichtigen sind hierbei vor allem die Rechtsfolgen, die daraus erwachsen können (vgl. dazu auch Abschnitt 6.3.1.2)).

#### **6.5.4 Strafrechtliche Relevanz**

Im strafrechtlichen Bereich können biometrische Verfahren in unterschiedlicher Hinsicht zum Einsatz kommen. Sie können vor allem dazu dienen, die Identität eines Straftäters nachzuweisen, Tatverdächtige zu ermitteln (positiv) und auszuschließen (negativ).

Vor allem bei der strafprozessualen Beweisführung kann der Einsatz biometrischer Erkennungsverfahren insofern relevant sein, als bei vermutet hoher Sicherheit des eingesetzten Verfahrens die Verwendung des körperlichen Merkmals eines Verdächtigen gegen ihn verwendet werden kann. Zu denken wäre hier an kriminelle Handlungen, die nur aufgrund des Zugangs zu einem geschützten Bereich erfolgen können. Auch hier ist wiederum die Sicherheit des Verfahrens entscheidender Maßstab dafür, in welchem Umfang die Verwendung eines biometrischen Merkmals zugunsten oder zulasten des Berechtigten ausgelegt werden wird. Als Beispiel sei hier die DNA-Analyse angeführt, die erst nach langjähriger Prüfung ihrer (technisch begründeten) Aussagekraft als strafprozessuales Beweismittel zugelassen wurde.<sup>13</sup>

<sup>13</sup> vgl. §81g I Stopp und DNA-Identitätsfeststellungsgesetz vom 07.09.1998, BGBl. I S.2646

Dabei ist zu berücksichtigen, dass im Strafprozessrecht aufgrund der verfassungsrechtlich garantierten Unschuldsvermutung stets gesetzlich genau bestimmte Beweisregeln und damit prinzipiell strengere Maßstäbe gelten als etwa im Rahmen der freien Beweiswürdigung im Zivilprozessrecht.

Im Zusammenhang mit Befugnissen der Strafverfolgungsbehörden nach strafprozessualen Regelungen ist davon auszugehen, dass diese unter bestimmten Voraussetzungen die Befugnis haben, auf biometrische Daten zuzugreifen. Dies gilt grundsätzlich sowohl für Daten, die bei Behörden gespeichert sind, als auch für solche, die bei privaten Stellen verwendet werden. Hier können auch Mitwirkungspflichten der Betreiber entstehen, wenn es z.B. darum geht, nicht nur einen biometrischen Datensatz herauszugeben, sondern auch mit einem anderen abzugleichen.

Anerkannte Methoden der erkennungsdienstlichen Behandlung sind die Erhebung und Speicherung biometrischer Rohdaten in Form von Fingerabdrücken und Lichtbildern. Im AFIS-System<sup>14</sup>, das seit 1992 beim BKA eingesetzt wird, werden aus den so gewonnen Rohdaten der Fingerabdrücke Templates erstellt und diese zusammen mit den Rohdaten abgespeichert. Zudem ist die Feststellung sonstiger körperlicher Merkmale wie Tätowierungen, Klang der Stimme oder Schriftproben zulässig und üblich.

Schließlich ist in strafrechtlicher Hinsicht noch zu beachten, dass Rechte anderer nicht in strafwürdiger Weise beeinträchtigt werden dürfen, wenn ein biometrisches Verfahren eingesetzt wird. Soll etwa durch ein Videoüberwachungssystem das eigene Haus abgesichert werden, muss dies im rechtmäßigen Rahmen des Hausrechts erfolgen. So dürfen z.B. von Passanten auf dem angrenzenden Bürgersteig oder Straße ohne konkreten Anlass einer Tatverdächtigung keine Aufnahmen gemacht und gespeichert werden<sup>15</sup>.

### **6.5.5 Haftung des Betreibers für das biometrische System**

Bei dem Betrieb eines biometrischen Systems muss zudem berücksichtigt werden, dass es sich stets um ein technisches System handelt, das bestimmte Funktionen in der konkreten Anwendung übernehmen soll. Hier muss wie bei anderen technischen Systemen auch bedacht werden, in welchem Umfang ein Betreiber für welche Funktionalitäten des Systems einstehen muss. Während dieser auf der einen Seite Ansprüche gegen den Hersteller haben kann, wenn das System nicht die zugesagten Eigenschaften hat, ist er selbst gegenüber seinem (End-)Kunden ebenfalls verpflichtet. Dies gilt auch, wenn eine biometrische Komponente in ein Gesamtsystem integriert wird. So ist etwa beim Schutz des Zugangs zum Online-Banking der Nutzer nur bei ordnungsgemäßer Funktion der biometrischen Zugangskontrolle in der Lage, z.B. Rechnungen fristgerecht zu bezahlen oder Aktienhandel zu betreiben. Systemausfälle oder Funktionsstörungen können hier zur Haftung des Betreibers führen, die dieser auch nicht umfassend in seinen Allgemeinen Geschäftsbedingungen ausschließen kann.

---

<sup>14</sup> Automatisches Fingerabdruck Identifizierungs System

<sup>15</sup> dies folgt u.a. aus §§ 22, 23 Kunsturhebergesetz

### **6.5.6 Allgemeine Geschäftsbedingungen beim Einsatz biometrischer Merkmale**

Die kundenfreundliche Ausgestaltung der Allgemeinen Geschäftsbedingungen, insbesondere der Haftungsfragen, ist bei der Verwendung biometrischer Erkennung im elektronischen Geschäftsverkehr als vertrauensbildende und damit unmittelbar akzeptanzfördernde Maßnahme anzusehen. Kann auf der einen Seite auch mittels Biometrie keine hundertprozentige Sicherheit erlangt werden, sollten die Betreiber biometrischer Verfahren auf der anderen Seite dem Endkunden das verbleibende Restrisiko mittels kundenfreundlicher Geschäftsbedingungen abnehmen.

Nach den rechtlichen Grundsätzen zur Regelung der Allgemeinen Geschäftsbedingungen und der allgemeinen Mitverschuldensregelung im Zivilrecht ist von folgenden Grundsätzen auszugehen:

- Unzulässig wäre eine Abwälzung der Haftung auf den Nutzer im Falle des Missbrauchs eines biometrischen Systems. Grundsätzlich muss der Betreiber für die Sicherheit seines (biometrischen) Systems einstehen, da diese in seiner Sphäre liegt und der Nutzer keinen Einblick oder gar Einfluss darauf hat. Betreiber können sich im Gegensatz zum Kunden mit entsprechenden Versicherungen zudem gegen derartige Risiken absichern.
- Unzulässig wäre die Schaffung von Sorgfaltspflichten, die an einen missbrauchssicheren und störungsfreien Umgang mit dem verwendeten biometrischen Merkmal knüpfen. Viele der in biometrischen Verfahren verwendeten körperlichen Merkmale sind öffentlich zugänglich und können nicht verborgen werden (z.B. der auf dem Weinglas im Restaurant zurückgelassene Fingerabdruck, oder das Gesicht / die Stimme in der Öffentlichkeit). Der Nutzer hat keinen Einfluss darauf, ob ein Dritter (erfolgreich) versucht, seinen Fingerabdruck nachzumachen, sein Gesicht / seine Stimme unbemerkt aufzunehmen etc. Darüber hinaus wäre es nicht zulässig, dem Nutzer bei Veränderungen des Merkmals aufgrund von Verletzungen oder Erkrankungen, aber auch bei „freiwilligen“ Veränderungen z.B. der Frisur ein Mitverschulden aufzubürden, wenn die Erkennung deshalb temporär nicht funktioniert.
- Unzulässig wäre auch eine vollständige Befreiung des Betreibers von Pflichten zur Haftung bei zeitweiligen Beschränkungen und Unterbrechungen des biometrischen Systems. Die Zulässigkeit von Haftungsbeschränkungen wegen technischer Störungen hängt allerdings auch vom konkreten Anwendungsgebiet ab. Grundsätzlich ist ein Betreiber jedoch verpflichtet, geeignete Vorkehrungen für die Funktionsfähigkeit und Betriebssicherheit des eigenen Systems zu treffen. Hier ist zudem zu berücksichtigen, dass bei Schäden, die durch technische Störungen und Funktionsmängel dem Nutzer des Systems entstehen, der Betreiber für diese grundsätzlich Ersatz leisten muss.
- Eine kundenfreundliche Regelung der Beweislastverteilung und damit des Risikos des Prozessverlustes würde schließlich grundsätzlich beinhalten, dass im Schadensfall der Betreiber dem Kunden nachweisen muss, dass dieser für den Schaden verantwortlich ist, und nicht umgekehrt der Kunden beweisen muss, dass er diesen nicht verursacht hat.

## 6.5.7 Betrieblicher Einsatz, insbesondere: Betriebsvereinbarungen

Bei Einführung eines biometrischen Systems in den Betrieb, als Zutritts-, Anwesenheits- und Verweildauerkontrolle oder Zugangs- und Zugriffssicherung etwa zum PC muss ein Arbeitgeber grundsätzlich davon ausgehen, dass eine vorhandene Arbeitnehmervertretung an dem Entscheidungsprozess beteiligt werden muss. Dies dient dem Schutz der Persönlichkeit der Arbeitnehmer. Im Folgenden werden die rechtlichen Voraussetzungen nach den betriebsverfassungsrechtlichen Grundlagen dargestellt und aufgezeigt, in welcher Art und Weise und zu welchem Zeitpunkt der Betriebsrat beteiligt werden muss, was über gesetzliche Pflichten hinaus zu beachten ist und welche (rechtlichen) Konsequenzen das Übergehen eines Mitbestimmungsrechts haben kann.

### 6.5.7.1 Mitbestimmungsrecht des Betriebsrates

Grundsätzlich ist die Zustimmung des Betriebsrats einzuholen, wenn es um die Einführung technischer Einrichtungen geht, sofern diese Einrichtungen zur Überwachung der Leistung oder des Verhaltens des Arbeitnehmers bestimmt sind.<sup>16</sup>

Ein biometrisches System, das im Rahmen der Zeiterfassung oder der Zugangskontrolle eingesetzt wird, stellt grundsätzlich eine technische Einrichtung zur Überwachung dar. Hierbei kommt es nur darauf an, dass das System objektiv für eine Überwachung geeignet ist. Der konkrete Wille des Arbeitgebers, es auch tatsächlich zu Überwachungszwecken einzusetzen, ist hierbei nicht von Bedeutung.

Eine Überwachung liegt allerdings dann nicht vor, wenn auf das Verhalten oder die Leistung des jeweiligen Arbeitnehmers keine Rückschlüsse gezogen werden können. Dies wäre z.B. dann der Fall, wenn das biometrische System lediglich als eine Art Schlüsseleratz eingesetzt wird, um dem Arbeitnehmer den Zutritt zum Betriebsgelände oder den Zugang zum PC zu ermöglichen, und auf die Erhebung von Protokolldaten vollständig verzichtet wird.

Da allerdings in der Regel schon aus Gründen der Revisionssicherheit (s.o.) Daten erhoben werden, ist grundsätzlich vom Eingreifen der hier angesprochenen Mitspracheregelung auszugehen.

### 6.5.7.2 Zeitpunkt der Beteiligung

Sollen biometrische Verfahren als Kontrolleinrichtungen eingesetzt werden, braucht der Betriebsrat zwar nach den gesetzlichen Regelungen noch nicht im Planungsstadium beteiligt zu werden. Zwingend ist der Betriebsrat erst dann zu beteiligen, wenn eine Entscheidung über das Ob, die Anzahl, den Zeitraum, die Zweckbestimmung und Wirkungsweise der Kontrolleinrichtung getroffen werden soll. Jedoch muss der Arbeitgeber den Betriebsrat rechtzeitig, d.h. bereits im Planungsstadium, über die geplante Einführung biometrischer Verfahren unterrichten.<sup>17</sup>

Zum Zwecke des gütlichen Miteinanders von Arbeitgeber und Betriebsrat sowie im Interesse der Arbeitnehmerrechte ist jedoch auch bei fehlendem gesetzlichem Zwang zu empfehlen, den Betriebsrat frühestmöglich mit einzubeziehen. Der Betriebsfrieden wird letztlich nicht unerheblich davon abhängen, ob der Betriebsrat den Arbeitgeber bei Einführung des biometrischen Systems unterstützt, was zu guter

<sup>16</sup> § 87 Abs.1 Nr.6 BetrVG

<sup>17</sup> §§ 90, 111 BetrVG

Letzt auch entscheidenden Einfluss auf die Akzeptanz des biometrischen Systems durch die Arbeitnehmer haben wird. Neben der gesetzlich vorgesehenen Unterrichtung des Betriebsrates können außerdem gemeinsame Ausschüsse von sachverständigen Vertretern der Arbeitgeber- und Betriebsratsseite gebildet werden.<sup>18</sup> Diese können die weiteren Verhandlungen zwischen Arbeitgeber und Betriebsrat erheblich erleichtern.

### 6.5.7.3 *Ausübung des Mitbestimmungsrechts*

Die Zustimmung des Betriebsrates sollte durch eine entsprechende Betriebsvereinbarung erfolgen. Die erforderliche Vereinbarung muss ohnehin schriftlich niedergelegt werden<sup>19</sup>, was auch erheblich zu Rechtssicherheit und Transparenz beiträgt. Die Betriebsvereinbarung beansprucht zudem unmittelbare und zwingende Geltung gegenüber dem Arbeitgeber und der Arbeitnehmerschaft<sup>20</sup>. Ihr kommt daher sog. Rechtsnormcharakter zu, was erhebliche Auswirkungen auf die Rechtsverbindlichkeit und Verstöße gegen die getroffenen Regelungen hat (siehe dazu sogleich).

Der Rechtsnormcharakter der Betriebsvereinbarung hat folgende Auswirkungen:

- Ein Verstoß gegen eine Betriebsvereinbarung bewirkt die Unwirksamkeit der abweichend getroffenen Abrede zwischen Arbeitgeber und dem einzelnen Arbeitnehmer innerhalb des Arbeitsvertrages. Der Arbeitnehmer muss dieser Abrede in diesem Fall nicht Folge leisten, was erheblichen Einfluss auf die Ordnung im Betrieb haben kann.
- Auch bereits zuvor getroffene abweichende Individualvereinbarungen zwischen dem Arbeitgeber und einzelnen Arbeitnehmern treten hinter Betriebsvereinbarungen zurück, verlieren also faktisch ihre Gültigkeit.
- Der Vorrang der Betriebsvereinbarungen gilt auch dann, wenn die Individualvereinbarung eine im Vergleich zur Betriebsvereinbarung für den Arbeitnehmer eigentlich günstigere Regelung trifft.

### 6.5.7.4 *Weitere Schutzpflichten gegenüber dem Arbeitnehmer*

Neben den dargestellten Pflichten, die Rechte der Arbeitnehmer mittelbar über deren Vertretung im Betrieb zu gewährleisten, hat der Arbeitgeber weitere unmittelbare Pflichten zum Schutz der Arbeitnehmer, die bei der Einführung eines biometrischen Systems ebenfalls zu beachten sind.

Der Arbeitgeber hat dafür Sorge zu tragen, dass nicht in unzulässiger Weise in das allgemeine Persönlichkeitsrecht des Arbeitnehmers eingegriffen wird<sup>21</sup>. Dieses gewährt dem Einzelnen nicht nur einen "abgeschirmten Bereich persönlicher Entfaltung", sondern das schon in Kap. 6.1.2 (Datenschutz) angesprochene "Recht auf informationelle Selbstbestimmung".

Durch die Verwendung eines biometrischen Systems wird der Arbeitnehmer zur Überlassung persönlicher Daten an den Arbeitgeber verpflichtet, wodurch in sein allgemeines Persönlichkeitsrecht eingegriffen wird. Aufgrund seiner Schutzpflicht darf der Arbeitgeber ein biometrisches System daher nur dann einführen, wenn dabei die Verhältnismäßigkeit gewahrt bleibt. Dabei kommt es entscheidend darauf an, ob sich

---

<sup>18</sup> § 28 Abs. 3 BetrVG

<sup>19</sup> § 77 Abs. 2 S. 1 BetrVG

<sup>20</sup> § 77 Abs. 4 BetrVG

<sup>21</sup> § 75 Abs. 2 BetrVG

der mit der Einführung verbundene Eingriff in das Persönlichkeitsrecht des Arbeitnehmers im konkreten Fall bei objektiver Würdigung des Einzelfalles als zwingend erforderlich erweist. Hier muss eine sorgfältige Abwägung der Interessen des Arbeitgebers mit denen des Arbeitnehmers erfolgen, wobei die Angemessenheit einer biometrischen Erkennung (im Gegensatz zur bisher verwendeten Erkennungsmethode) und die Geeignetheit für die Zwecke der Zutritts- / Zugangssicherung zu prüfen sind. So ist z.B. der Einsatz von Überwachungskameras gekoppelt mit einem Gesichtserkennungssystem nur dann zulässig, wenn dieser nicht ausschließlich der Kontrolle der Arbeitnehmer dient, sondern eine solche Kontrolle aus besonderen Sicherheitsgründen (wie etwa bei Bankschaltern oder in Atomkraftwerken) geboten erscheint. Auch in diesem Zusammenhang bietet sich wiederum eine frühzeitige Einbindung der Arbeitnehmervertretung an.

## 6.6 Verbrauchersicht

Verbraucher, die Waren und Dienstleistungen aller Art in Anspruch nehmen, können künftig mit Anwendungen biometrischer Verfahren vor allem dort konfrontiert werden, wo eine Überprüfung der Berechtigung erforderlich ist. Dies kann z.B. auf Anwendungen beim Online-Banking zutreffen, wenn es darum geht, sich für den Zugang zum eigenen Bankkonto zu authentifizieren, oder bei der Freischaltung einer Signaturkarte. Der Einsatz von Biometrie im Verbraucheralltag kann bei richtiger Auswahl der Merkmale und Gestaltung der Verfahren zu höherer Sicherheit der jeweiligen Anwendung und zu mehr Bequemlichkeit auf der Nutzerseite führen. Im Interesse der Verbraucher bzw. der Akzeptanz durch die Nutzer sollten beide Aspekte bei der Konzeption gleichberechtigt gewichtet werden, wobei allerdings je nach Anwendung ohne weiteres unterschiedliche Sicherheitsstufen gewählt werden können.

Chancen und Risiken biometrischer Verfahren liegen nicht zuletzt wegen der generell lebenslangen Personengebundenheit biometrischer Merkmale an das jeweilige Individuum nahe beieinander. Auf der einen Seite könnten die Nachteile des im fraglichen Bereich bisher überwiegend angewandten Prinzips von Besitz und Wissen (z.B. Karte und PIN oder Passwort) künftig überwunden werden, da die Sicherheit der Anwendung nicht mehr ausschließlich in der Geheimhaltung der PIN und einer stets sicheren Aufbewahrung der Karte durch den Berechtigten gewährleistet werden muss. Aus dieser Forderung leiten die Anbieter (u.a. insbesondere die Banken) bis heute zum Teil unzumutbare Sorgfaltspflichten für den Verbraucher ab, die wiederum zu einer ungerechten Haftungs- und Beweislastverteilung führen.

Auf der anderen Seite ergeben sich durch den Einsatz von Biometrie bisher nicht bekannte Risiken, die vor allem den Datenschutz und die Datensicherheit betreffen. Daher muss die Sicherheit biometrischer Daten auch in reinen Convenience-Anwendungen gewährleistet sein. Auch muss aus diesem Grunde Sicherheit in Bezug auf Biometrie stets zweiseitig betrachtet werden, und zwar sowohl in Bezug auf die Sicherheit der dabei verwendeten biometrischen als auch auf die mittels Biometrie zu schützenden Daten. Ergänzend dazu ist eine verbraucherfreundliche Gestaltung der, der jeweiligen Anwendung zugrunde liegenden, Allgemeinen Geschäftsbedingungen von entscheidender Bedeutung.

Der praktische Einsatz biometrischer Verfahren im Verbraucheralltag ist nicht nur in solchen Bereichen zu erwarten, in denen sich der Verbraucher frei für oder gegen die Nutzung der Biometrie entscheiden kann. Neben einem möglicherweise verpflichtenden Einsatz im hoheitlichen / staatlichen Bereich, bei dem der

Verbraucher stärker in seiner Eigenschaft als Bürger betroffen ist, könnten auch prinzipiell freiwillige Anwendungen etwa im privatwirtschaftlichen Bereich zu einem faktischen Benutzungszwang führen. Dies kann immer dann der Fall sein, wenn durch die Biometrie das herkömmliche Authentifizierungsverfahren ersetzt werden soll, so zum Beispiel beim Zugang zum Online-Banking oder beim Zutritt zu räumlich geschützten Bereichen (Flugzeug etc.) Die Option, ein biometrisches Verfahren nicht zu benutzen, wäre dann faktisch nicht mehr gegeben.

Auch die Sozialverträglichkeit eines biometrischen Systems ist von besonderer Bedeutung. Nicht alle Menschen können jedes Verfahren nutzen, da sie so verschieden sind wie ihre körperlichen Merkmale voneinander abweichen (s. Kap. 3.2.8 Failure-to-Enrol). Darüber hinaus gehört zu einem nicht-diskriminierenden Einsatz von Biometrie stets die Berücksichtigung derer, die u.a. aus den in Kap. 7 dargestellten Gründen eine biometrische Erkennung ablehnen.

Schließlich sind aus Sicht des Verbraucherschutzes neben den Aspekten des Datenschutzes und der Datensicherheit auch und gerade die Nutzerakzeptanz, die Bedienerfreundlichkeit und die Gestaltung der Einsatzumgebung von entscheidender Bedeutung (s. Kap. 7). Nicht zuletzt muss bei der Auswahl und Konzeption eines biometrischen Systems für eine bestimmte Anwendung hinsichtlich des erforderlichen Nutzens für die Anwender sorgfältig abgewogen werden, ob ein Einsatz von Biometrie tatsächlich dazu führen wird, die gewünschte Aufgabe effizienter und wirtschaftlicher zu lösen und gleichzeitig Sicherheit und Bequemlichkeit für die Nutzer gegenüber einem Verfahren ohne Biometrie mit einem merklichen Mehrwert zu verbessern.

## 7 Betreibersicht

### 7.1 Produktreife / Produktverfügbarkeit

Da am Biometriemarkt ständig neue Entwicklungen und auch neue Start-Ups auftauchen, sollte die Produktreife des angebotenen Produkts abgefragt werden. Das beste System nützt nichts, wenn es sich noch in einer frühen Entwicklungsphase befindet. Die Praxis hat gezeigt, dass teilweise die veröffentlichten Produktinformationen und der tatsächliche Entwicklungsstand nicht übereinstimmen.

Dabei sollte insbesondere darauf geachtet werden, dass vorgelegte Erkennungsraten (FAR, FRR) auf ihre Aussagekraft hinterfragt werden. Erfahrungen aus den durchgeführten Feldversuchen zeigen, dass beispielsweise Identifikationssysteme bei einer kleinen Nutzergruppe (Population kleiner fünf Nutzer) ein sehr gutes Resultat bei der Ermittlung von Fehlerraten erzielen konnten, während bereits bei 40 eingelernten Nutzern die Fehlerraten deutlich absinken.

Es sollte nach Pilot- bzw. Referenzinstallationen gefragt, die benannten Stellen auch wirklich kontaktiert und die Nutzeranzahl beim Referenzbetreiber mit den eigenen Anforderungen verglichen werden.

### 7.2 Installation

Da die Installation biometrischer Systeme immer in ein sehr individuelles Umfeld geschieht, sollte man darauf achten, dass sich das System auch unter den gegebenen Umgebungsbedingungen betreiben lässt. Neben offensichtlichen Voraussetzungen wie Ausleuchtung und Lärmpegel sollten auch Störfaktoren wie beispielsweise Reflexionen, veränderliche Lichtverhältnisse oder ein veränderlicher Hintergrund bei Kameraaufnahmen untersucht werden.

Bei besonderer Beanspruchung der Hardware, wie extreme Temperaturen oder Temperaturänderungen, Feuchtigkeit oder Erschütterungen ist es wichtig, dass der Aufbau des Systems diesen Anforderungen gewachsen ist.

### 7.3 Systembetrieb

- a) Verbrauch von DV-Ressourcen:  
Wird zusätzliche Hardware wie z.B. Rechner, Framegrabber, Grafiktablets, Kamerahardware oder auch spezielle Betriebssystem-Software benötigt?
  - b) Pflege der Erfassungsterminals / Aufwand für die Reinigung:  
Wie häufig muss das Erfassungsterminal des Systems gewartet werden? Sind Reinigungsmaßnahmen an der eingesetzten Hardware nötig und wie oft.?
  - c) Lebensdauer der einzelnen technischen Systemkomponenten
    - MTBF  
(mean time between failures, mittlerer Ausfallabstand, ISO/DIN 40042)
    - MTTR  
(mean time to repair)
-

- d) Aufwand der Systempflege  
Wie häufig muss das Erfassungsterminal des Systems gewartet werden? Sind Reinigungsmaßnahmen notwendig und in welchen Zeitintervallen?
- e) Wartung:  
Wie oft ist beispielsweise durch Templatealterung ein neues Enrolment der Benutzer notwendig?
- f) Änderung
- g) Anpassung bei Änderungen des Trägersystems
- h) Skalierbarkeit Benutzerzahl, offene/geschlossene Benutzergruppen, Gäste, Einmalnutzer
- i) Kosten:  
Neben den Kosten hinsichtlich des Administrationsaufwands sind unter Umständen bei biometrischen Systemen höhere Kosten (Zeitaufwand) einer einzelnen Authentisierung im Vergleich zur Authentisierung mittels Chipkarte zu berücksichtigen.

## 7.4 Administrationsaufwand

Ein wichtiger Aspekt im Zusammenhang mit der Administrierbarkeit sind Werkzeuge zur Qualitätssicherung beim Enrolment. Idealerweise erfolgt eine Bewertung der Güte des erfassten Systems, so dass der Administrator evtl. Problemfälle (siehe FER) schnell erkennen kann.

Sollte sich durch Alterungseffekte (Template-Aging) oder anderen Randbedingungen die Notwendigkeit eines neuen Enrolments ergeben, dann sind bereits gespeicherte Templates aus der Datenbank zu löschen. Dazu sind geeignete Interfaces erforderlich.

### 7.4.1 Regelfall

- a) Registrierung/Löschung neuer Benutzer in der Datenbank
- b) Erzeugung neuer Referenzmuster
- c) Aktualisierung vorhandener Referenzmuster

### 7.4.2 Sonderfälle (Aufwand relativ zum Normalfall)

- a) Aufwand bei False Rejection
- b) Falls man bei einer Person False Acceptance festgestellt hat: Aufwand, um ein künftiges Eindringen zu verhindern

## 7.5 Investitionssicherheit

Mit dem Einsatz eines biometrischen Erkennungssystems müssen auch eventuell auftretende Probleme während der Nutzungsphase betrachtet werden.

### 7.5.1 Zukunftssicherheit

- a) Produktlebensdauer
- b) Ist ein Austausch von Komponenten auf der Basis offener Standards garantiert?

- c) Integrationsfähigkeit in Produkt- und Technologieinnovationen (Chipkarte, Mobiltelefon, neue Anwendungen)
- d) Anwendung der einheitlichen Schnittstelle BioAPI

### **7.5.2 Abhängigkeit vom Anbieter**

- a) Möglichkeit, diverse Sicherheitsparameter selbst zu bestimmen / zu verändern, z.B. die Einstellung einer Akzeptanzschwelle
- b) Möglichkeit, Software/Hardware-Updates selbst durchzuführen. Bei verschiedenen Systemen muss die Installation und die Einspielung von Updates durch den Hersteller vorgenommen werden, es fallen zusätzliche Kosten an.
- c) Können die eigenen Administratoren das System betreiben?

### **7.5.3 Abhängigkeit vom Technologielieferanten**

Existiert ein offener (weltweiter) Markt für die benötigten Hardwarekomponenten?

## **7.6 Integrationsfähigkeit**

### **7.6.1 Systemintegration**

- a) Braucht das System eine eigene IT-Infrastruktur?
- b) Wird die Philosophie „Alles aus einer Hand“ verletzt?
- c) Basiert das System ausschließlich auf Standards oder ist es proprietär?

### **7.6.2 Lösungsintegration / Integration in das Sicherheitskonzept**

- a) Ist das biometrische System in das vorhandene Sicherheitskonzept und die vorhandene Policy integrierbar ?
- b) Wie wird die Anpassung an die unterschiedlichen Sicherheitsanforderungen erzielt? Besteht eine echte Skalierbarkeit über einen Sicherheitsparameter an die Sicherheitsanforderungen, Geräte und Personen.

#### *7.6.2.1 Abdeckungsgrad der verschiedenen Einsatzbereiche*

In welchem Umfang kann das Verfahren die unterschiedlichen, im Unternehmen verstreuten Anwendungsfälle der Authentisierung abdecken?

#### *7.6.2.2 Skalierbarkeit der Sicherheitsanforderung*

- a) Können unterschiedliche Sicherheitsanforderungen abgedeckt werden?
- b) Wie wird die Anpassung an die unterschiedlichen Sicherheitsanforderungen erzielt?
  - Echte Skalierbarkeit über einen Sicherheitsparameter (genauere Beschreibung notwendig)
  - Modifikation der FAR

## 7.7 Kosten

Biometrische Systeme sind je nach Anwendungsfall noch sehr unterschiedlich in den entstehenden Kosten. Bei einem System für einen PC-Zugang kann vorausgesetzt werden, dass nur einmalige und auch relativ geringe Kosten anfallen werden. Dem entgegen muss für die Absicherung des Zutritts zu einem hoch sensiblen Bereich mit einer höheren Investitionssumme und auch mit Kosten z.B. für einen Service gerechnet werden.

### 7.7.1 Einmalige Kosten

- a) Kaufpreis
- b) Installation (Aufwand für evtl. bauliche Maßnahmen)
- c) Schulungsmaßnahmen für das eigene Personal und für die Personen, die das System nutzen sollen (externe Kunden)

### 7.7.2 Laufende Kosten

- a) Hardware-Wartung
- b) Software-Updates / Upgrades
- c) Registrierung neuer Benutzer in der Datenbank
- d) Neu-Personalisierung der Alt-Nutzer bei Merkmalsänderung z.B. durch Alterung (wenn nicht eine Adaption durchgeführt wird)

## 7.8 Unterschiedliche Nutzergruppen

Labor-Bedingungen: technisch absolut versierter Nutzer, der mit dem eingesetzten Verfahren vertraut sowie umfassend über Funktionsweise und Handhabung informiert ist; Ziel der Benutzung: erfolgreiche Erkennung

Moderne Büro-Umgebung: technisch bewanderter und umfassend in die Benutzung des Verfahrens eingeführter „Berufs-Nutzer“, der mit ausführlicher Dokumentation über das Verfahren ausgerüstet ist. Die Benutzung dient dem Zutritt zum Arbeitsplatz oder dem Zugang zum büroeigenen Computer.

Öffentliche Umgebung: nicht-technischer „Allerwelts-Nutzer“, der zuvor eine kurze Einweisung und Anleitung in die Benutzung erhalten hat, aber über keine Dokumentation oder weiteren Hintergrund über biometrische Verfahrensweisen verfügt; die Erkennung dient dem Zugang zu gewünschten Serviceleistungen (z.B. am Geldautomat) oder Informationen (Bürgeramt), oder Zutritt im privaten Bereiche (eigene Haustür, Garagentor, Kfz).

## **8. Benutzerakzeptanz**

### **8.1 Relevanz der Benutzerakzeptanz zur Bewertung biometrischer Identifikationssysteme**

Da bei der biometrischen Erkennung körperliche Merkmale einer Person erfasst und verarbeitet werden, die zu erkennende Person sich daher mit einem Teil ihres Körpers einer Maschine gegenüber präsentieren muss, wird die biometrische Erfassung nach bisherigen Untersuchungen als durchweg intimer und persönlicher aufgefasst als die bloße Eingabe eines künstlich generierten Softwarecodes. Daher sind Fragen der Akzeptanz bei Biometrie von besonderer Bedeutung. Hier werden Fragen der Akzeptanz betrachtet, die sich auf die Technologie im allgemeinen und nicht auf spezielle Anwendungen beziehen.

Zur Orientierung werden im Folgenden die Gesichtspunkte aufgezeigt, die in bisher durchgeführten Pilotprojekten und Nutzerbefragungen für die Benutzer eines biometrischen Systems von Bedeutung waren. Insgesamt zählen für die Einschätzung und Beurteilung eines biometrischen Verfahrens sozio-emotionale ebenso wie technisch-funktionale Kriterien.

Die Nutzer haben nach ersten empirischen Befragungen konkrete Anforderungen an biometrische Verfahren. Der bisherige Trend zeigt deutlich das Verlangen der Nutzer nach einem spürbaren Mehrwert der Biometrie im Vergleich zu herkömmlichen Verfahren.

### **8.2 Allgemeine Haltung und Nutzungstypen**

Ein weitreichendes Basiswissen über Biometrie existiert heute in der Bevölkerung (noch) nicht. Der überwiegende Anteil befragter Personen verbindet keinerlei Vorstellung mit dem Begriff Biometrie. Nach der Nutzung eines biometrischen Verfahrens äußerten sich die bisher befragten Nutzer grundsätzlich positiv, die meisten würden gerne auf ihre PINs / ihre Passwörter verzichten und sehen in der Biometrie eine Möglichkeit dafür. Auf den zweiten Blick herrscht jedoch Skepsis vor, insbesondere im privaten Bereich ist noch kaum jemand bereit, etwaige Schlüssel oder Codes durch biometrische Verfahren zu ersetzen. Folgende Faktoren hatten für die Befragten nach der Nutzung verschiedener Verfahren Priorität: Sicherheit (inkl. Datensicherheit), Einfachheit, technische Zuverlässigkeit, Schnelligkeit und Bequemlichkeit. Die Bewertung der Alltagstauglichkeit des biometrischen Verfahrens, die insbesondere für einen Einsatz im privaten Bereich von hoher Relevanz ist, hängt dabei entscheidend von Robustheit und Zuverlässigkeit des Verfahrens in der praktischen Anwendung ab.

Bei der Implementierung eines biometrischen Identifikationssystems sieht man sich Nutzern gegenüber, die sich in folgende Gruppen untergliedern lassen können.

- **Kooperativer-Nutzer**

Es handelt sich bei diesen Nutzern eher um dem Erkennungssystem gegenüber positiv eingestellte Personen, die durch die Anwendung eines biometrischen Systems einen Vorteil verspüren.

- **Nicht-Kooperativer-Nutzer**  
Es handelt sich bei diesen Nutzern eher um dem Erkennungssystem gegenüber negativ eingestellte Personen, die durch die Anwendung eines biometrischen Systems keinen Vorteil für sich verspüren, sondern sich eher gezwungen sehen, das System zu benutzen.
- **Ablehnender-Nutzer**  
Ablehner stehen entweder der Biometrie oder allen techn. Neuerungen skeptisch gegenüber. Bei Nicht-Funktionieren erfolgt eine Vertiefung der ablehnenden Haltung.
- **Gleichgültiger-Nutzer**  
Nutzer, die der Biometrie gleichgültig gegenüberstehen und sich dem Verfahren anpassen und es korrekt benutzen wollen.

### **8.3 Informationstransparenz**

Die umfassende Aufklärung und Information über Biometrie sowohl hinsichtlich der Chancen als auch der Risiken sowie des konkret eingesetzten Verfahrens sind entscheidende Akzeptanzfaktoren. Dazu gehören Aspekte wie die generelle Funktionsweise biometrischer Verfahren sowie die Erklärung von Wahrscheinlichkeitsraten bei dem eingesetzten körperlichen Merkmal (Individualität). Kurze Informationsschriften, die der Nutzer mit nach Hause nehmen kann, erscheinen hier sinnvoll. Das konkrete Verfahren muss zudem ausführlich erläutert werden. Hierzu zählen Informationen über Ort und Umfang der Datenspeicherung und die Templateverwaltung, Maßnahmen zur Verhinderung von Missbrauch, Zugriffsrechte beim Betreiber, schriftliche Einwilligung in die Erhebung und Verarbeitung der biometrischen Datensätze, Einstellung der (individuellen) Toleranzschwelle und damit verbunden die erreichbare Sicherheit.

### **8.4 Enrolment und Benutzerführung**

Die Aufnahme der ersten biometrischen Datensätze, der später bei der Identifikation / Verifikation des Nutzers als Grundlage der Referenzdaten herangezogen wird, muss mit großer Sorgfalt erfolgen (s.o.). Die Datenersterfassung (Enrolment) ist daher von geschultem und erfahrenem Personal durchzuführen, das die Qualität des aufgenommenen Templates hinreichend beurteilen kann. Wichtige Bestimmungsfaktoren des Enrolment sind der Ort der Daten(erst)erfassung (dies ist insbesondere wichtig, wenn Umgebungsbedingungen auf die Qualität der Identifikation einwirken, wie z.B. die Lichtverhältnisse bei der Gesichtserkennung) sowie der Zeitaufwand, der durch eine ergonomische Ablaufplanung des Enrolments optimiert werden sollte. Ebenso sind Nachpersonalisierungsoptionen in die Planung des Enrolments mit einzubeziehen. Unmittelbar im Anschluss an das Enrolment sollte ein erster Probelauf erfolgen, um die Qualität des erstellten Templates zu überprüfen und ggf. eine neue Erfassung vorzunehmen.

Wegen der allein schon aus Datenschutzsicht zu fordernden aktiven Kooperation des Nutzers ist eine genaue Einweisung in den Umgang mit dem Verfahren erforderlich. Dazu zählt auch die Handhabung des Endgeräts. Zusätzlich sollte eine schriftliche Kurzanleitung am Gerät mit den wichtigsten Verhaltensregeln sowie ein permanenter Ansprechpartner etwa über eine Telefon-Hotline bereitgestellt werden. Hilfreich sind z.B. auch FAQs, anhand derer sich der Nutzer jederzeit noch einmal aktuell

informieren kann.

## **8.5 Diskriminierungsfreier Einsatz**

Es gibt kein körperliches Merkmal, das bei allen Menschen überhaupt oder in gleich starker Ausprägung vorkommt. Nachfolgend sind die wichtigsten Diskriminierungs-Aspekte aufgeführt.

### **8.5.1 Ausgrenzung durch das verwendete Merkmal**

Nicht oder nicht in ausreichender Ausprägung vorhandene körperliche Merkmale können genetisch bedingt, aber auch die Folge von starker Beanspruchung der entsprechenden Körperpartien (z.B. durch körperliche Arbeit) sein. Bereits das Enrolment kann daher unmöglich sein (sog. Failure-to-Enroll, s. Abschnitt 3.2.8). In der späteren Anwendung kann ein schwach ausgeprägtes Merkmal zu einer höheren Falschzurückweisungsrate (FRR) führen. Dies kann z.B. im Bereich der Zutritts-sicherung im Betrieb zu sozialer Diskriminierung des Betroffenen gegenüber seinen Kollegen führen. Im Dienstleistungsbereich kann dadurch der Service für den Betroffenen schlechter werden. Hier sind geeignete Maßnahmen zu treffen, damit dem Nutzer keine Nachteile entstehen.

### **8.5.2 Ausgrenzung aufgrund personenbezogener Besonderheiten**

Körperliche Besonderheiten und Behinderungen sowie Erkrankungen können ebenso dazu führen, dass eine Person das Verfahren nicht anwenden kann. Vorkommende Behinderungen sind etwa Blindheit, Taubheit, Stummheit, aber auch verkürzte oder nicht vorhandene Gliedmaßen (z.B. Conterganschäden) sowie Kleinwüchsigkeit. Rollstuhlfahrer sind ebenfalls verbreitet anzutreffen. Körperliche Einschränkungen sind daneben z.B. Sehschwächen, die das Tragen einer Sehhilfe (Brille, Kontaktlinsen) erfordern. Analphabetismus verhindert die Eingabe von Passwörtern und Zahlen sowie das Lesen von Anleitungen.

### **8.5.3 Notwendigkeit von Ersatzverfahren**

Wegen der aufgeführten Ausgrenzung unterschiedlicher Bevölkerungsgruppen ist dem Nutzer stets ein Ersatzverfahren anzubieten. Das ist nicht zuletzt deshalb notwendig, um neben der ungewollten auch die gewollte Nichtnutzung biometrischer Verfahren zu berücksichtigen: die Nutzung muss stets freiwillig erfolgen können. Das bedeutet auch, dass den Personen, die ein biometrisches Verfahren nicht nutzen möchten, keine Nachteile etwa im Service entstehen dürfen. Neben der (parallelen) Beibehaltung des herkömmlichen Verfahrens kommt hier auch ein weiteres biometrisches Verfahren in Betracht, das mit einem anderen Merkmal arbeitet.

### **8.5.4 Kosten für Nutzer**

Das Kostenargument ist für den Großteil der Bevölkerung voraussichtlich ein weiterer entscheidender Akzeptanzfaktor. Bei Befragungen, die den Einsatz im privaten Bereich betrafen, sprach sich der überwiegende Teil der Nutzer auch wegen der heute zu erwartenden hohen Kosten gegen einen Erwerb aus. Die biometrischen Systeme sollten daher prinzipiell für jeden Bürger erschwinglich sein. Beim Einsatz am Geldautomaten etwa dürfen dem Bankkunden keine zusätzlichen Kosten entstehen, wenn er sich zur Erhöhung der Sicherheit für die Anwendung der biometrischen Erkennung entscheidet. Für den privaten Bereich etwa bei der Türsicherung oder auch im PC-Bereich sind die bisher durch herkömmliche Verfahren entstehenden Kosten im Vergleich zu beachten, nicht zuletzt aus Gründen

der ansonsten vermutlich nicht erreichbaren Akzeptanz. Während die Nutzer möglicherweise noch bereit sein werden, für den besseren Schutz etwa ihres Eigenheims etwas mehr auszugeben als für ein herkömmliches Türschloss, ist im PC-Bereich nicht mit der Akzeptanz höherer Kosten zu rechnen, da bisherige PINs, TANs oder Passwörter z.B. für Zwecke des Home- und Internetbanking in der Regel kostenlos vergeben werden.

## **8.6 Handhabung der Verfahren**

Bei der Handhabung der Verfahren sind neben den regelmäßigen Anforderungen eines Großteils der Benutzer auch diejenigen zu berücksichtigen, die bei den unter „Ausgrenzung“ genannten Personengruppen besondere Relevanz haben.

### **8.6.1 Einfachheit und Bequemlichkeit**

Die Bedienung des Endgeräts mit dem biometrischen Sensor sollte intuitiv und selbstverständlich erfolgen können. Unnatürliche und gekünstelte Bewegungen oder Körperhaltungen sind zu vermeiden, da sie extra eingelernt und deshalb auch eher „falsch“ gemacht werden können. Die Nutzer scheinen wenig Verständnis dafür zu haben, wenn sie trotz Verwendung des „richtigen“ Merkmals nicht erkannt werden. An Geldautomaten etwa werden voraussichtlich nicht mehr als drei Fehlversuche toleriert werden (vgl. mit der jetzigen Situation vor Einziehen der EC-Karte).

Relevant ist etwa bei der Zutrittssicherung auch die Platzierung des Erkennungsgeräts zu der abgesicherten Raum- oder Gebäudetür. Als lästig wird hier bereits ein minimaler Abstand angesehen, der zusätzlich zum Hindurchgehen bewältigt werden muss.

Ein Feedback des Geräts etwa in Form einer Anzeige auf einem Monitor (z.B. des aufgenommenen Gesichts bei der Gesichtserkennung, des Auges bei der Iriserkennung oder Abbildung der abgeglichenen Minutien bei der Fingerbilderkennung) dient einer problemloseren und damit einfacheren Anwendung durch den Nutzer.

### **8.6.2 Schnelligkeit**

Der Zeitfaktor ist ein erhebliches Argument für den Nutzer. Im Regelfall soll die Nutzung eines biometrischen Verfahrens kürzer, auf keinen Fall aber länger dauern als das bisher benutzte herkömmliche Verfahren. Relevanz hat dabei der gesamte Zeitraum vom „Vor-das-Gerät-Treten“ (also die „Kontaktaufnahme“) bis zur gewünschten Anwendung (Öffnung der Tür, Ausschalten des Bildschirmschoners, Zugang zu elektronischen Daten etc.).

### **8.6.3 Ergonomie der Anwendergeräte**

Die ergonomische Ausgestaltung des Endgeräts sollte häufig vorkommende körperliche Einschränkungen (s. auch unter Ausgrenzung) berücksichtigen. Die behindertengerechte Gestaltung gehört dazu z.B. durch die Möglichkeit, auch mit einem Rollstuhl nah genug an eine Anwendersäule heranfahren zu können. Denkbar sind hier auch akustische Signale für Blinde sowie ein ertastbares Tastatur-/Sensorfeld oder das mögliche Ausweichen auf ein einzutippendes Passwort bei einem sonst notwendigen gesprochenen Passwort. Die variable Höhe der Bedieneroberfläche wird nicht nur kleinwüchsigen Menschen die Bedienung ermöglichen, sondern auch anderen diese erleichtern. Neben der Körpergröße ist auch die variable Größe der verwendeten körperlichen Merkmale zu berücksichtigen:

die Dicke des Fingers etwa oder die Größe der Hand.

#### **8.6.4 Übertragbarkeit von Zugangsberechtigungen im Arbeitsalltag**

Als Nachteil biometrischer Verfahren wird der Umstand erlebt, dass im Gegenteil zu PIN und Passwort ein biometrischer Code nicht an Vorgesetzte oder Untergebene weitergegeben werden kann. Die Praktikabilität im Büroalltag wird dementsprechend bezweifelt. Hierauf könnte reagiert werden, indem Mehrfachzugangsberechtigungen vorgesehen und technisch ermöglicht werden.

### **8.7 Bedenken und Befürchtungen**

Der Einsatz von biometrischen Identifikationssystemen kann bei Anwendern aufgrund der z.T. als sehr sensibel empfunden Datengenerierung der körpereigenen bzw. verhaltensbezogenen Merkmale Bedenken und Befürchtungen hervorrufen. Nachfolgend werden diese Bedenken näher erörtert.

#### **8.7.1 Physische und moralische Unversehrtheit**

Die Verwendung körpereigener Merkmale führt bei den Nutzern zu besonderen subjektiven Befürchtungen. Die Nutzung des eigenen Körpers für die Durchführung einer (Wieder-)Erkennung wird sensibler betrachtet als eine künstlich generierte PIN. Durch sachliche Aufklärung über die Verfahrensweise und den genauen Ablauf der biometrischen Erkennung lassen sich unbegründete Ängste abbauen. Durch die transparente und nachvollziehbare Gestaltung der Anwendergeräte, z.B. die Verwendung von auf Anhieb selbsterklärlichen Bedienelementen, können subjektive Befürchtungen entkräftet und in sachliche Argumente umgewandelt werden. Bei den moralischen Bedenken handelt es sich z.B. um Vorbehalte, die auf einem religiösen Hintergrund beruhen. Es ist darauf zu achten, die kulturellen und religiösen Gegebenheiten der jeweiligen Nutzergruppe zu berücksichtigen.

#### **8.7.2 Kriminelle Handlungen Dritter und Datenmissbrauch**

Die physische Unversehrtheit kann auch durch kriminelle Handlungen Dritter bedroht sein, wenn es dem Täter nämlich darum geht, Zugang zu dem geschützten Bereich zu erhalten und er vor Körperverletzungen oder –verstümmelungen nicht zurückschreckt, z.B. Abtrennen des Fingers/der Hand/des Ohrs, etc. Um dies zu verhindern, muß eine entsprechende Lebenderkennung des Sensors vorgesehen werden. In Betracht kommt u.a. die Messung der (Körper-)Temperatur oder der Blutzirkulation. Aus präventiven Gründen ist schließlich am Anwendungsgerät selbst ein deutlicher Hinweis auf eine vorhandene Lebenderkennung angebracht. Ein solcher Hinweis dient zudem der Information der Nutzer und dem Abbau von diesbezüglichen Ängsten.

Auch die Gewährleistung der Sicherheit der Daten beim Betreiber (keine Weitergabe an Dritte, strenge Reglementierung der Zugriffsrechte z.B. Vier-Augen-Prinzip) sowie die Angst vor Missbrauch beim Vorgang der Registrierung bzw. der Datenerfassung oder der Benutzung des Systems (Datenmissbrauch) können Nutzungshindernisse darstellen

#### **8.7.3 Erzwungene Nutzung**

In allen Einsatzbereichen biometrischer Verfahren ist eine erzwungene Nutzung des Verfahrens mit krimineller Absicht denkbar. Um das für den Nutzer damit verbundene Risiko zu minimieren, kommt der Einbau eines stillen Alarms in Betracht, bei dem

dieser z.B. einen anderen Finger als üblich auf den Sensor legt und dadurch einen für den Täter nicht bemerkbaren Alarm bei einer Polizeidienststelle auslöst. Ob eine solche vorbeugende Maßnahme in jedem Anwendungsbereich sinnvoll ist, muss individuell für jeden einzelnen Einsatzort geprüft werden.

#### **8.7.4 Nutzung für Zwecke der Strafverfolgung**

Aufgrund der möglichen Nutzung von biometrischen Daten für Strafverfolgungszwecke, können sich negative Assoziationen bei den Nutzern zu einer erkenntnisdienlichen Behandlung ergeben.

#### **8.7.5 Scheu und Scham**

Bei der Benutzung von biometrischen Identifikationssystemen kann es bei den Anwendern zu Scheu- oder Schamgefühlen kommen, z.B. beim Sprechen eines Passwortes bei der Sprecherverifizierung im Beisein Anderer (Angst vor Versagen des eigenen Körpers am System) oder die Scheu vor der Kamera bei der Gesichtserkennung.

### **8.8 System- und Merkmalsausfall**

Die Funktionalität des Systems stellt einen entscheidenden Akzeptanzfaktor für biometrische Identifikationssysteme dar. Für den Fall eines Systemausfalls ist die Bereitstellung einer Fall-Back-Lösung zu bedenken, die die Identifikation jederzeit ermöglicht. Ebenso können Probleme auftreten, wenn das biometrische Merkmal des Anwenders, z.B. aufgrund eines Schnittes im Finger, nicht einsetzbar ist. Auch in diesem Fall sollte der Nutzer die Möglichkeit besitzen, sich auf eine andere Weise oder mittels eines anderen biometrischen Merkmals zu identifizieren. Auch im fehlerfreien Regelbetrieb ist immer mit einer Nichtakzeptanz von Berechtigten zu rechnen.

Eine ständige Kontrolle der False Acceptance Rate sowie der False Rejection Rate geben Hinweise auf die Funktionalität des Systems. Mögliche Zeitverzögerungen, die sich daraus ergeben, können die Nutzungsmotivation der Anwender herabsetzen oder mögliche Nach-Enrolments erforderlich machen.

## 9 Anhang

### 9.1 Referenzen

- [BDSG] Bundesdatenschutzgesetz vom 22.05.2001, BGBl. 2001 Teil I Nr. 23, Seite 904 ff.  
<http://www.datenschutz-und-datensicherheit.de/dudserver/dsrecht.htm>
- [CC99] Common Criteria for Information Technology Security Evaluation.  
Part 1: Introduction and General Model, 1999, Version 2.1.  
Part 2: Security Functional Requirements, 1999, Version 2.1.  
Part 3: Security Assurance Requirements, 1999, Version 2.1.
- [CM99] Common Methodology for Information Technology Security Evaluation.  
Part 1: Introduction and General Model, 1997, Version 0.6.  
Part 2: Evaluation Methodology, 1999, Version 1.0.
- [BSigV] Begründung zur Verordnung zur digitalen Signatur,  
vom 16. November 2001  
<http://www.iid.de/iukdg/gesetz/index.html>
- [SigV] Verordnung zur digitalen Signatur (SigV) vom 16. November 2001,  
BGBl. 2001 Teil 1, Nr. 59 vom 21.11.2001, S. 3074-3084  
<http://www.datenschutz-und-datensicherheit.de/dudserver/signatur.htm>
- [SigG] Signaturgesetz vom 22. Juli 1997 (BGBl. I S. 1872) und Änderung vom  
16. Mai 2001, BGBl. 2001 Teil 1 Nr. 22 vom 21.05.2001, S. 876-884  
<http://www.datenschutz-und-datensicherheit.de/dudserver/signatur.htm>
- [TAB] TAB-Arbeitsberichte Nr. 76 *Biometrische Identifikationssysteme*,  
TAB Büro für Technikfolgenabschätzung beim Deutschen Bundestag,  
2002  
<http://www.tab.fzk.de/de/arbeitsberichte.htm>
- [W 1] B. Wirtz, *Technische Evaluierung biometrischer Systeme*,  
Leicher Trendforum 97
- [W 2] B. Wirtz, D. Lotter, *Dynamische Unterschriftenverifikation: Verfahren und Applikationsszenarien zur Chipkartensicherung Siemens AG*,  
GMD-SmartCard Workshop, 1/97
- [W 3] B. Wirtz, *Technical Evaluation of Biometric Systems*,  
Proc. of the ACCV'98, Hong Kong
- [BWG] Biometric Working Group: *Best Practices in Testing and Reporting Performance of Biometric Devices*, Version 1.0, 12.01.2000,  
<http://www.cesg.gov.uk/technology/biometrics/media/Best%20Practice.pdf>  
(Stand: 24.06.2002)

---

## 9.2 Weiterführende Literatur

- Nolde, Veronika / Leger, Lothar: Biometrische Verfahren, Deutscher Wirtschaftsdienst, ISBN 3-87156-464-8
- Behrens, Michael / Roth, Richard: Biometrische Identifikation, DuD-Fachbeiträge, Vieweg & Sohn Verlagsgesellschaft mbH, ISBN 3-528-05786-6
- Albrecht, Astrid / Probst, Thomas: Biometrische Verfahren im Einklang mit Verbraucher- und Datenschutz?, AgV-Forum 01/2001, S. 32 ff.
- Jain, A. / Bolle, R. / Pankati, S.: Biometrics: Personal Identification in Networked Society, Norvell 1999,
- Ashbourn, Julian: Biometrics – Advanced Identity Verification, Springer 2000, und: Bantam, Biometric Users Charter
- Albrecht, Astrid: Biometrie, digitale Signatur und elektronische Bankgeschäfte zum Nutzen für Verbraucher, hrsg. von der Arbeitsgemeinschaft der Verbraucherverbände (AgV e.V.), Bonn 1999
- Nanavati, Samir / Thieme, Michael / Nanavati, Raj: Biometrics – Identity Verification in a Networked World, John Wiley & Sons, Inc. New York u.a., 2002
- Borking, John J.: Privacy Enhancing Technologies (PET), DuD 2001, S. 607 ff.
- Borking, John J. / Verhaar, Paul: Biometrie und Datenschutz – Bedrohungen und Privacy-Enhancing Technologies, DuD 1999, S. 138 ff.
- Köhntopp, Marit: Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren, S. 177 ff., in: Horster,

### 9.3 Abkürzungsverzeichnis / Glossar

Adaption	(automatische) Anpassung/Aktualisierung der gespeicherten Referenzdaten bei der Benutzung des Systems
ARE	Maß zur Beschreibung der Trennfähigkeit eines biometrischen Systems zwischen Originalen und Fälschungen.
Authentifizierung/ Authentifikation	Authentifizierung/Authentifikation bedeutet „ <u>Bezeugung</u> der Echtheit.“ Bei der Authentifizierung mittels eines biometrischen Systems erfolgt eine Identifikation oder Verifikation.
Autorisierung	Nach erfolgreicher Authentifikation (oder Identifikation oder Verifikation) mittels eines biometrischen Systems wird die Person ermächtigt, gewisse Handlungen durchzuführen oder bestimmte Dienste zu nutzen.
Betreiber (Anwender)	Firma, die ein IT-System mit bestimmten Anwendungen (Applikationen) betreibt und dabei biometrische Verfahren anwenden will. Der vorliegende Katalog der Bewertungskriterien soll dem Betreiber bei der Auswahl geeigneter Verfahren helfen.
BDSG	Bundesdatenschutzgesetz
Biometrisches Produkt	Bei einem biometrischen Produkt handelt es sich um ein Hardware- und/oder Softwarepaket, das konzipiert worden ist, biometrische Verfahren zum Zwecke der Identifikation/Verifikation in einer Vielzahl von Systemen anzuwenden.
Biometrisches System	Ein biometrisches System ist eine spezielle IT-Installation, die biometrische Verfahren zum Zwecke der Identifikation/Verifikation in einer bestimmten Einsatzumgebung durchführt. (Vom Standpunkt der Sicherheit liegt also der Hauptunterschied zwischen Systemen und Produkten in der unterschiedlichen Kenntnis bezüglich ihrer Einsatzumgebung.)
Biometrisches Verfahren	Methode bestimmte Eigenschaften von körperlichen Merkmalen auszunutzen, um auf technischem Wege die Identität einer Person zu verifizieren oder die Person als zugehörig zu einer Gruppe zu erkennen.
BVerfG	Bundesverfassungsgericht
DV	Datenverarbeitung
EER	Maß für die allgemeine Trennfähigkeit zwischen Originalen und Fälschungen (equal error rate), d.h. die Fehlerrate, bei der FRR und FAR gleich sind.
FAR:	Falschakzeptanzrate (false acceptance rate), auch: false match

FRR:	Falschrückweisungsrate (false rejection rate), auch: false non-match
Identifikation	Identifikation bedeutet „ <u>Feststellung</u> der Identität.“ Bei der Personenidentifikation wird festgelegt, um welche Person es sich handelt.
IT	Informationstechnik
IT-Produkt	Bei einem IT-Produkt handelt es sich um ein Hardware- und/oder Softwarepaket, das „von der Stange“ gekauft und in eine Vielzahl von Systemen eingebaut werden kann.
IT-System	Ein IT-System ist eine spezielle IT-Installation mit einem definierten Zweck und einer bekannten Einsatzumgebung.
Hersteller	Eine Firma, die ein System zur biometrischen Identifikation auf dem Markt anbietet.
MTBF	mean time between failures, mittlerer Ausfallabstand, ISO/DIN 40042
MTTR	mean time to repair, mittlere Ausfallzeit.
NEA:	die Gesamtanzahl berechtigter Zutrittsversuche (Erkennung oder Verifikation, number of enrollee attempts)
NFA:	die Anzahl fälschlicher Akzeptanzen (number of false acceptances)
NFR:	die Anzahl fälschlicher Rückweisungen (number of false rejections)
NIA:	die Gesamtanzahl unberechtigter Zutrittsversuche (Erkennung oder Verifikation, number of imposter attempts)
Nutzer (Benutzer)	Kunde des Betreibers, der das biometrische Verfahren benutzen soll.
Referenzdaten	Von einem Nutzer erfasste und für die Verifikation oder Identifikation in der Datenbank abgelegter Datensatz
SigG	Signaturgesetz vom 22.Mai 2001
SigV	Verordnung zur digitalen Signatur vom 22.November 2001
Template	Datensatz, der aus biometrischen Rohdaten extrahiert wird
Verifikation	Verifikation bedeutet „ <u>Bestätigung</u> der Identität.“ Die Personenverifikation entscheidet die Frage, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt.