TELETRUST Deutschland e.V.

Verein zur Förderung
der Vertrauenswürdigkeit
von Informations- und
Kommunikationstechnik

Kriterienkatalog

Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren

information
security
solutions

Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren

- Kriterienkatalog -

TeleTrusT Deutschland e.V.

Arbeitsgruppe 6:

Biometrische Identifikationsverfahren

Redaktion:
Dr. G. Laßmann

Version 3.0

Stand: 18.08.2006

Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik

http://www.teletrust.de

Geschäftsstelle:

Chamissostraße 11
D-99096 Erfurt

Tel: +49 361 346 05 31
Fax: +49 361 345 39 57

Folgende Mitglieder der AG6 haben bei der dritten Version mitgewirkt:

Dr. Albrecht, Astrid	BSI	astrid.albrecht@bsi.bund.de
Biermann, Heinz	BfDI	Heinz.Biermann@bfdi.bund.de
Freytag, Claus	Bundesdruckerei	Claus.Freytag@bdr.de
Giesecke, Hans-Joachim	T-Systems	Hans-Joachim.Giesecke@ t-systems.com
Hartwich, Kai	TeleTrusT	kai.hartwich@teletrust.de
Junghanns, Jürgen	Interflex	Juergen_Junghanns@eu.irco.com
Kalo, Horst	Aucoteam	Horst.Kalo@t-online.de
Dr. Laßmann, Gunter	T-Systems	Gunter.Lassmann@t-systems.com
Dr. Quiring-Kock, Gisela	Der Hessische Daten-schutzbeauftragte	G.Quiring-Kock@ datenschutz.hessen.de
Dr. Scheuermann, Dirk	FhG, SIT	dirk.scheuermann@sit.fraunhofer.de

Einführende Inhaltsangabe

Die Entwicklung des mit diesem Dokument zum dritten Mal neu vorgelegten Kriterienkatalogs spiegelt die Entwicklung der Biometrie in der Wahrnehmung der Öffentlichkeit wider. Die erste Version war eine viel gelesene Erstinformation über ein neues exotisches Technologiegebiet, die zweite Version enthielt schon Erfahrungen aus Feldversuchen und Praxistests, und während der Laufzeit dieser dritten Version wird die Biometrie Einzug in den Alltag halten. Ab dem 1.November 2005 hat beispielsweise die viele Bundesbürger betreffende Ausgabe der neuen, biometriegestützten deutschen Reisepässe begonnen, in denen zunächst ein digitales Gesichtsbild gespeichert wird. Ab März 2007 werden zusätzlich zwei Fingerabdruckbilder aufgenommen.

Ziel des Kriterienkatalogs der Arbeitsgruppe 6 „Biometrische Identifikationsverfahren“ von *TELETRUST* Deutschland e.V. bleibt es, die interessierte Öffentlichkeit und den potentiellen Anwender oder Betreiber nachvollziehbar und möglichst objektiv über biometrische Identifikationsverfahren zu informieren. Mit diesem Papier soll durch Versachlichung der Diskussion der sinnvolle Einsatz von biometrischen Verfahren gefördert werden.

Im ersten Kapitel werden die Prinzipien der Biometrie an einführenden Beispielen erläutert und die grundlegenden Definitionen und Abläufe erklärt.

Kapitel 2 stellt dar, welche körpereigenen Merkmale in aktuellen biometrischen Systemen verwendet werden und auf was bei der Auswahl eines biometrischen Merkmals für den eigenen Anwendungszweck zu achten ist.

Im Kapitel 3, das von „Fehlerraten und Qualität“ handelt, werden die wichtigsten Fehlerraten hergeleitet und erläutert sowie welche Größen wichtig sind, um die Güte eines biometrischen Systems beurteilen zu können. Für die wichtigsten Merkmalsarten werden die bekanntesten Angriffe erklärt.

Der Einfluss des zugrunde liegenden technischen Systems wird in Kapitel 4 behandelt.

Im Kapitel 5 werden einige Datenschutz-Anforderungen für biometrische Systeme bis hin zu konkreten Empfehlungen erläutert.

Das Kapitel 6 behandelt weitere juristische Aspekte biometrischer Verfahren. Dazu gehören der Einsatz bei qualifizierten elektronischen Signaturen, biometriegestützte Ausweisdokumente, strafrechtliche Aspekte, Haftungsfragen und Allgemeine Geschäftsbedingungen beim Einsatz biometrischer Systeme im kommerziellen Bereich. Weiter werden die Rahmenbedingungen des betrieblichen Einsatzes biometrischer Systeme dargestellt. Abschließend erfolgt ein Blick auf die Verbrauchersicht sowie einige Erkenntnisse aus Untersuchungen zur Benutzerakzeptanz.

Was der Betreiber eines biometrischen Systems zu beachten hat, wird in Kapitel 7 dargestellt.

In den neu hinzugekommenen Kapiteln 8 und 9 werden aktuelle Schwerpunktanwendungen und Entwicklungstendenzen erläutert. Es ist geplant, diese Kapitel häufiger zu aktualisieren als das Grunddokument.
In der vorliegenden Version werden beispielsweise die Verwendung von Biometrie im ePass beschrieben und ein Quellenhinweis zum Bundespersonalausweis gegeben, sowie Übersichtsinformationen zu den technischen Standards zur Biometrie.

Fragen, Kritik und weitere Anregungen sammelt Dr. G. Laßmann, T-Systems Enterprise Services GmbH, unter der Mail-Adresse:
gunter.lassmann(at)t-systems.com

Berlin, den 18.08. 2006

Dr. Gunter Laßmann

Inhalt

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. Selbst bei Nutzung von Ausweisen ist man nicht sicher vor der nichtauthorisierten Nutzung oder der freiwilligen Weitergabe des ID-Mittels. Der Einsatz eines biometrischen Verfahrens kann hier Abhilfe schaffen, um tatsächlich nur autorisierte Personen zuzulassen.

Dabei wird die Biometrie betrachtet als die Lehre von der (automatisierten) Messung eines individuellen statischen oder verhaltenstypischen Merkmals einer Person zum Zweck der Identifikation bzw. Verifikation.

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 daher eine neuartige Sicherheitsqualität erreicht werden.

1.2 Beispielhafte Anwendungsszenarien

In diesem Abschnitt sollen dem Anwender und/oder Betreiber anhand von Beispielen die praktische Anwendung biometrischer Erkennungsverfahren nahe gebracht 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 zurzeit auf dem Markt angebotenen biometrischen Systemen für PC-Login zum Einsatz.

1.2.2 Sicherung einer Tür (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 inzwischen Produkte auf dem Markt, die verschiedenste biometrische Merkmale (z.B. Fingerbild, Gesicht, Iris, Sprache, oder auch in kombinierten Verfahren) für die Authentifizierung einer Person nutzen.

1.2.3 Zugang zu geschützten Ressourcen, Freischalten einer elektronischen Signaturfunktion

Als weiterer Einsatzbereich eines biometrischen Verfahrens kommt die so genannte qualifizierte elektronische Signaturfunktion in Betracht. Zum Freischalten des Signaturmechanismus wird ein Besitzelement, herkömmlich eine Signaturkarte, benötigt, die in aller Regel in einem Kartenlesegerät mittels einer PIN frei geschaltet 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[1]: „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.

1.2.4 Personaldokumente

Bei Personaldokumenten trägt die Verwendung von Biometrie zusätzlich zu den bisher schon etablierten Sicherungsmechanismen dazu bei, das Dokument stärker an seinen berechtigten Inhaber zu binden und so das Risiko eines erfolgreichen Missbrauchs durch andere Personen zu minimieren. Personaldokumente mit Biometrie (siehe 8.2 für nähere Betrachtungen) sind in manchen Ländern schon im Einsatz. Bei Personaldokument-Anwendungen können die biometrischen Daten in der Regel auf dem Personaldokument gespeichert und das Prüfsystem als Verifikationssystem konfiguriert werden zur Entscheidung der Frage, ob es sich um den rechtmäßigen Besitzer des Dokuments handelt.

[1] 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)

1.3 Prinzipieller Ablauf einer biometrischen Erkennung

Ein System zur biometrischen Erkennung verarbeitet die 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 ist der grundsätzliche Aufbau eines biometrischen Systems dargestellt. Mit Hilfe eines Sensors werden die Eingabedaten aufgenommen. Sie werden vor oder während des Mustervergleichs vorverarbeitet. Zum Erkennungsprozess 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 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.

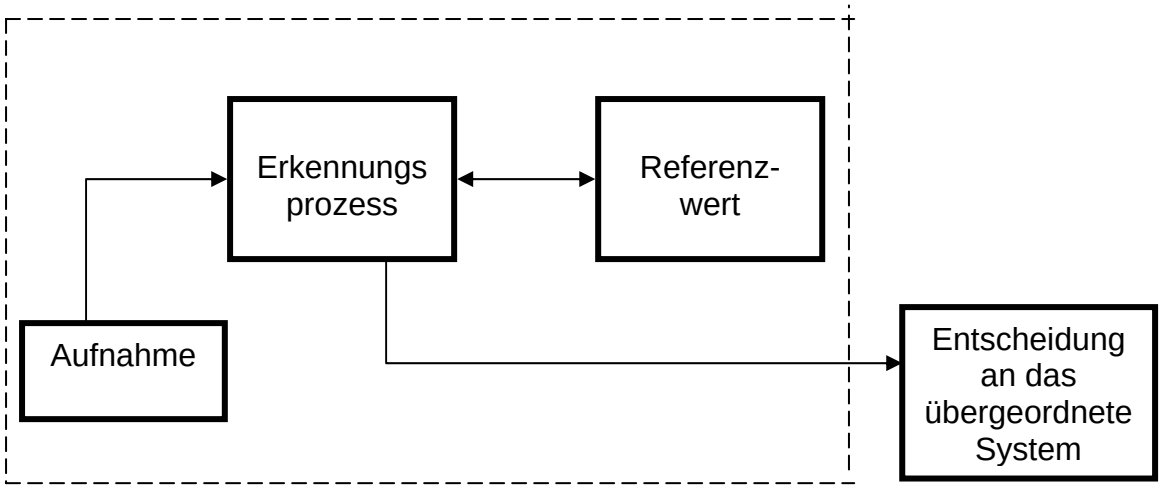

Bild 1-1 Ablauf eines biometrischen Verfahrens

1.4 Definitionen

Betreiber (Anwender)

Personen, Unternehmen oder Organisationen, die ein System mit bestimmten Anwendungen betreiben und dabei biometrische Verfahren verwenden wollen.

Hersteller

Ein Unternehmen, das komplette biometrische Produkte, die Integration von biometrischen Komponenten zu biometrischen Systemen oder biometrische Erkennungssoftware auf dem Markt anbietet.

Nutzer (Benutzer)

Personen, deren biometrische Merkmale geprüft werden sollen.

Verifikation (genauer: Verifikation einer Person durch ein biometrisches Verfahren)

Verifikation bedeutet „Bestätigung der Identität." Die Personenverifikation entscheidet die Frage, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt.

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.

Identifikation (genauer: Identifikation einer Person durch ein biometrisches Verfahren)

Identifikation bedeutet „Feststellung der Identität." Bei der Personenidentifikation wird festgelegt, um welche Person es sich handelt.

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.

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.

Hinweis

Beim Einsatz eines biometrischen Verfahrens ist zu unterscheiden, ob die Nutzer ein Interesse daran haben erkannt zu werden, also **kooperativ** sind, oder ob die Nutzer eher Interesse daran haben nicht erkannt zu werden, also **nichtkooperativ** sind.

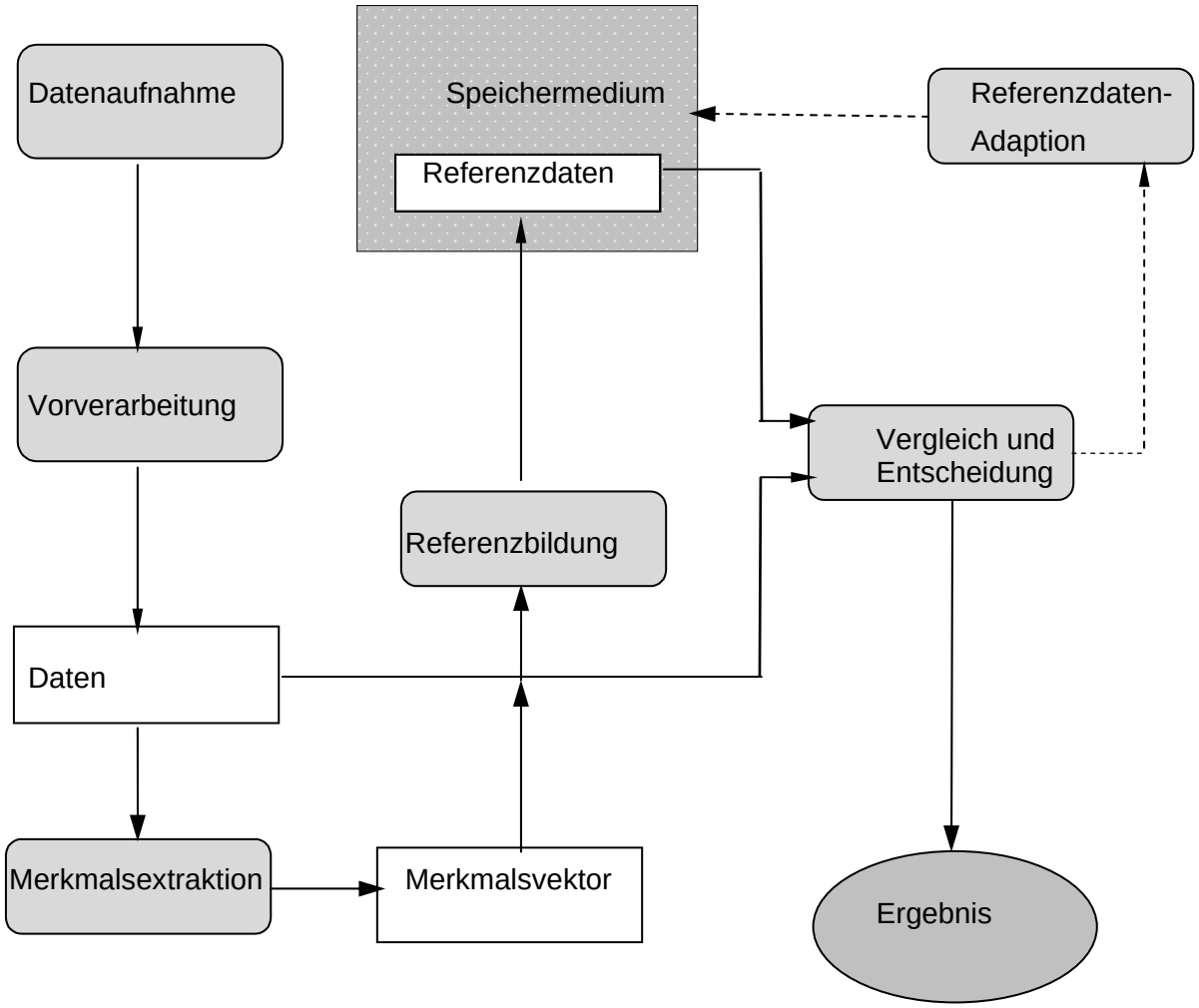

Bild 1-2: Ablauf einer biometrischen Erkennung

2 Eigenschaften des verwendeten biometrischen Merkmals

2.1 Verwendete Merkmalsart

Bei biometrischen Verfahren unterscheidet man zwischen physiologischen Merkmalen und verhaltensbasierten Merkmalen. Physiologische biometrische Merkmale sind Körpermerkmale einer Person, die sich nicht oder nur sehr geringfügig über einen längeren Zeitraum verändern. Verhaltensbasierte biometrische 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
- Retina
- Handgeometrie
- Ohr
- Iris
- Finger
- Venenmuster

Verhaltensbasiertes Merkmal (auch aktives Merkmal genannt)
Zum Beispiel:

- Unterschrift (dynamisch/statisch)
- Gang
- Tippverhalten an der Tastatur
- Gestik / Mimik beim Sprechen
- Stimme / Sprechverhalten

Merkmalskombination

Zum Beispiel:

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

2.2 Merkmalseigenschaften

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

2.2.1 Einzigartigkeit des Merkmals

Ein Merkmal sollte, um für ein biometrisches Verfahren geeignet zu sein, einzigartig in dem Sinne sein, dass es für unterschiedliche Menschen hinreichend verschieden ist, also eine Unterscheidung von Personen anhand des Merkmals ermöglicht.

2.2.2 Konstanz

Ein Merkmal sollte, um für ein biometrisches Verfahren geeignet zu sein, sich im Laufe der Zeit möglichst wenig ändern. Geringfügige Merkmalsänderungen können im Rahmen der definierten Toleranzbereiche akzeptiert bzw. durch adaptive biometrische Verfahren gemildert werden.
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 Möglichkeit, dass der erpresste Merkmalsträger einen stillen Alarm ohne Erkennbarkeit für den Erpresser abgeben kann, indem er z.B. den vorher entsprechend definierten Finger zur Erkennung verwendet.

2.2.4 Merkmalsverbreitung

Ein Merkmal sollte, um für biometrische Verfahren geeignet zu sein, möglichst bei allen 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. 3.2.8). 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

2.2.5 Merkmalsakzeptanz

Zusätzlich zu den in 2.2.1. bis 2.2.4. genannten Basisanforderungen sollte 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. 6.9 näher erläutert.

3 Fehlerraten und Qualität

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 praktischen Versuchen ermittelten oberen Schranken der Fehlerraten zu, die in der Regel um mehrere Größenordnungen 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 Übereinstimmungsgrad 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.

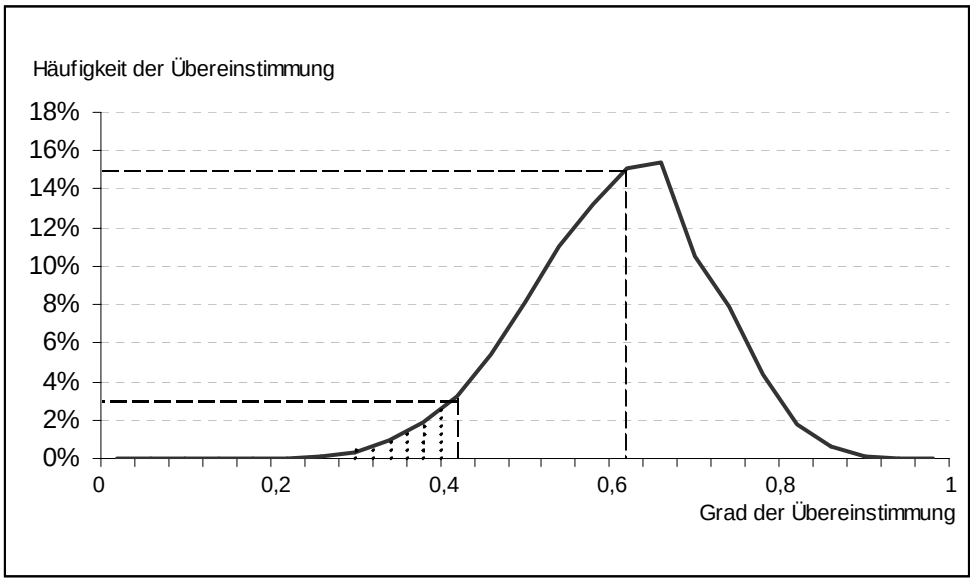

Bild 3-1: Verteilung der Anzahl der übereinstimmenden Merkmale

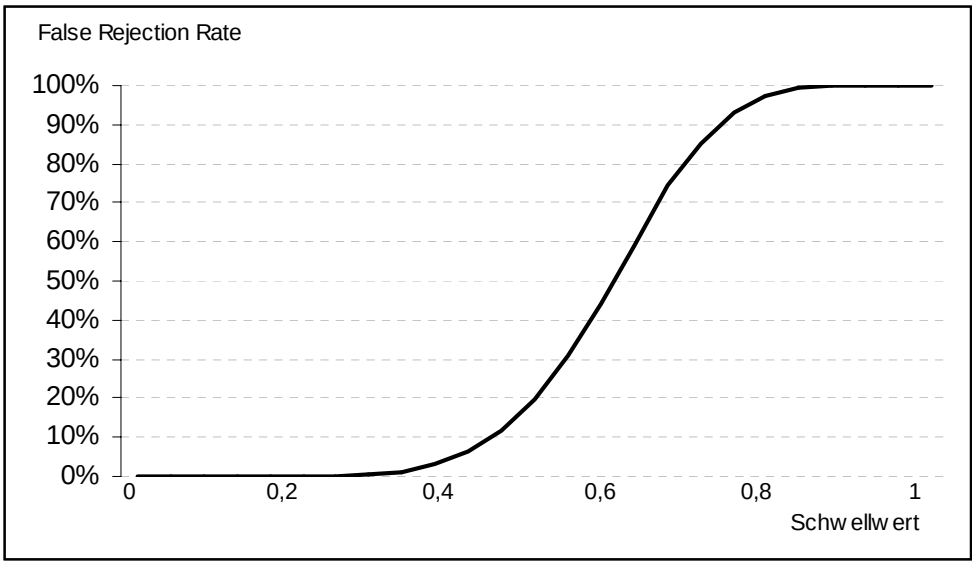

Bild 3-2: Verteilung des Anteils der zu Unrecht Abgewiesenen (FRR) in Abhängigkeit vom Schwellwert

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 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 0,42 oder

weniger erfasst wurde. Das sind im Beispiel 3,14 %. Der prozentuale Anteil fälschlich zurückgewiesener Berechtigter, die so genannte *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 unberechtigten und damit falschen Zurückweisungen.

3.2.3 Prüfung von Daten nicht erfasster Testperson

Wird das aus den vorangegangenen Abschnitten bekannte Beispiel weitergeführt, 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 sieht, kommt es bei diesem biometrischem Beispiel-System durchaus vor, dass bei nicht erfassten Personen keine Übereinstimmung der Merkmalskriterien auftritt. Das ist zwar erwünscht, jedoch ist auch damit zu rechnen, dass es Personen gibt, deren Merkmal eine hohe Übereinstimmung mit den Referenzdaten der erfassten Testpersonen besitzen kann.

3.2.4 Die False Accept 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 nicht erfasste Testperson zugelassen wird: Dies ist genau der Anteil der Fälle bei denen die nicht erfasste Testperson einen Übereinstimmungsgrad gleich oder größer 0,42 hatte. Der prozentuale Anteil fälschlich zugelassener Unberechtigter, die so genannte *false accept 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, desto größer wird die Zahl der Falsch-Akzeptanzen.

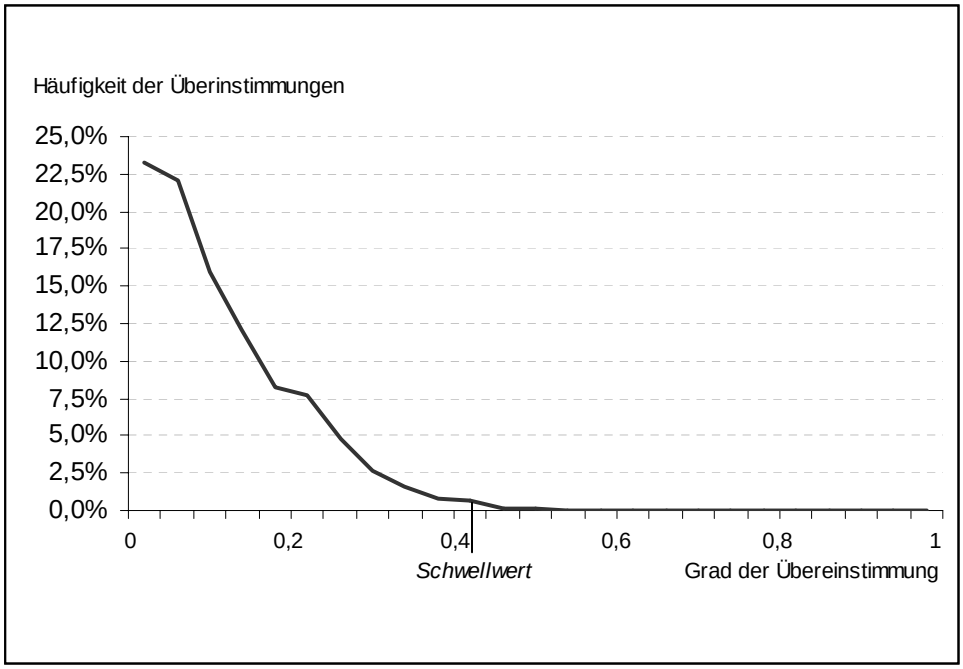

Bild 3-3: Verteilung der Anzahl der übereinstimmenden Merkmale

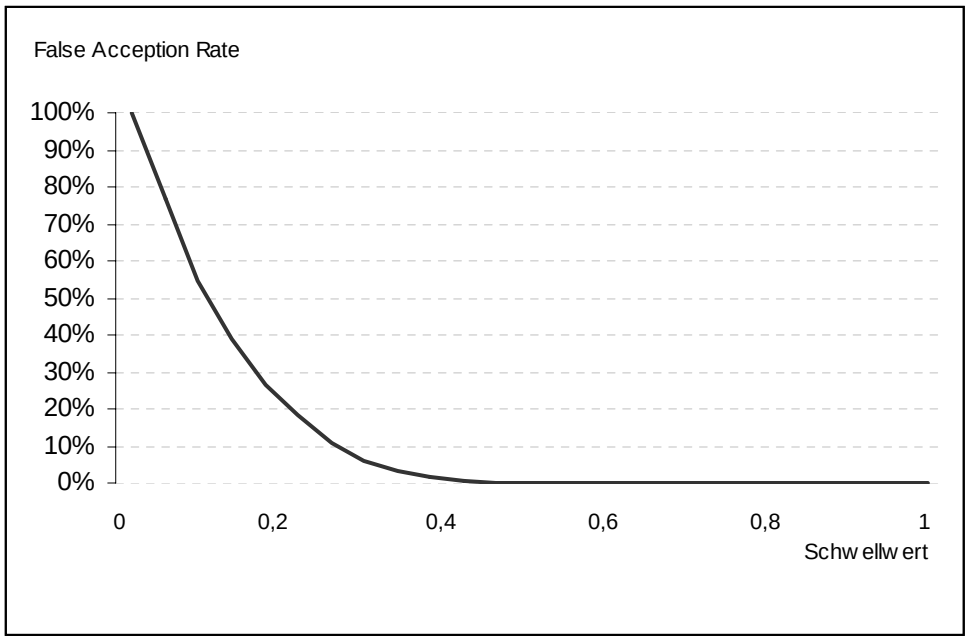

Bild 3-4: Verteilung des Anteils der zu Unrecht Zugelassenen (FAR) in Abhängigkeit vom Schwellwert

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*) gegeneinander abzuwägen. Maßgeblich sollten dabei die Anforderungen aus der konkreten Anwendung sein.

Einen Maßstab für die Möglichkeiten eines biometrischen Systems liefert die *EER*, die so genannte *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.

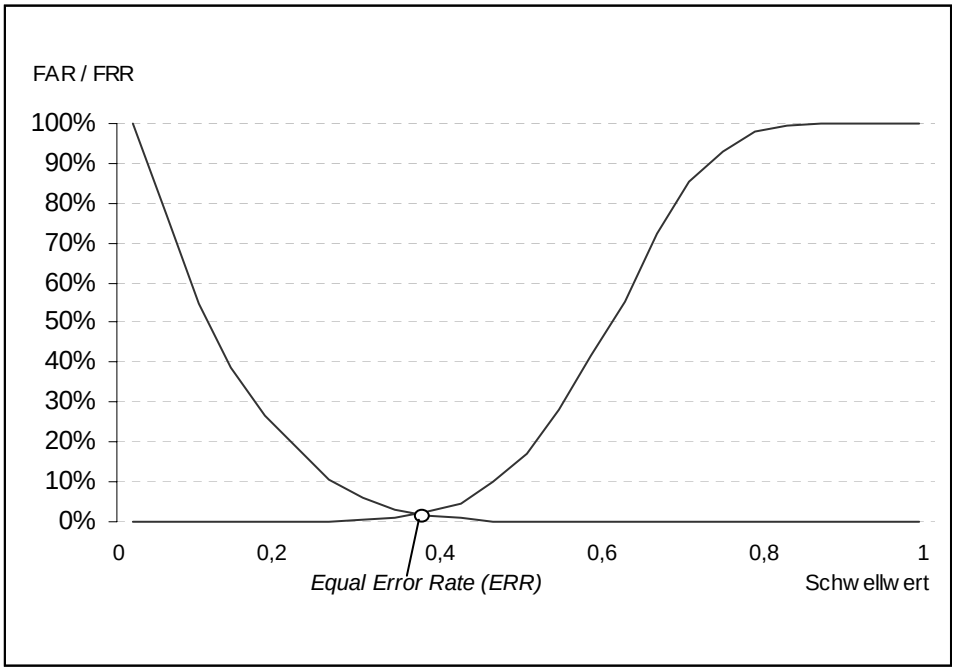

Bild 3-5: Verhältnis FRR und FAR

3.2.6 Berechnung der Fehlerraten in der Praxis

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

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

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 enrolee 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 umso mehr nichterfasste Nutzer akzeptiert.

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 Fehlerraten 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.

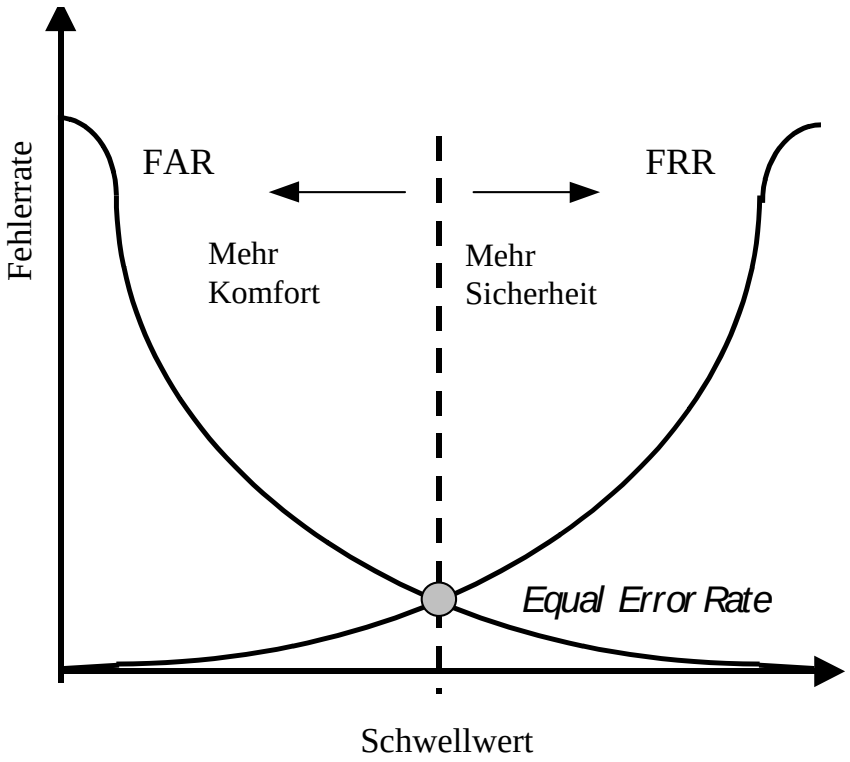

Bild 3-6:Typische Fehlerkurven bei biometrischen Verfahren

Konkrete Kenngrößen, die man aus der Kurve ableiten kann, sind beispielsweise die Breiten des Schwellwertbereiches, bei denen FAR und FRR gleichzeitig unterhalb einer gemeinsamen Schranke bleiben, d.h. bei denen zu einem vorgegebenen Wert ±delta die Bedingungen FAR < EER±delta und FRR < EER±delta gleichzeitig erfüllt sind.

3.2.7 Darstellung der Fehler in der DET-Kurve

Die Systemleistungsfähigkeit in unterschiedlichen Arbeitspunkten kann mit einer DET (Detection Error Tradeoff) Kurve (bzw. einer ROC-Kurve(Receiver Operating Characteristic) verdeutlicht werden. Diese Kurve trägt die Fehlerraten gegeneinander auf und eliminiert damit die Abhängigkeit der Darstellung von der Schwelle.
Die Fehlerraten werden meist logarithmisch dargestellt.
DET Kurven werden oft zur Beschreibung der Eigenschaften eines Detektierungs- oder Mustererkennungssystems gebraucht. Die nachfolgende Kurve stellt die oben beschriebene FAR/FRR Verteilung dar. DET Kurven ermöglichen die vergleichende Bewertung von biometrischen Systemen, ROC-Kurven stellen meist die Detektierungsrate (1 - FRR) dar, sind also gespiegelt.

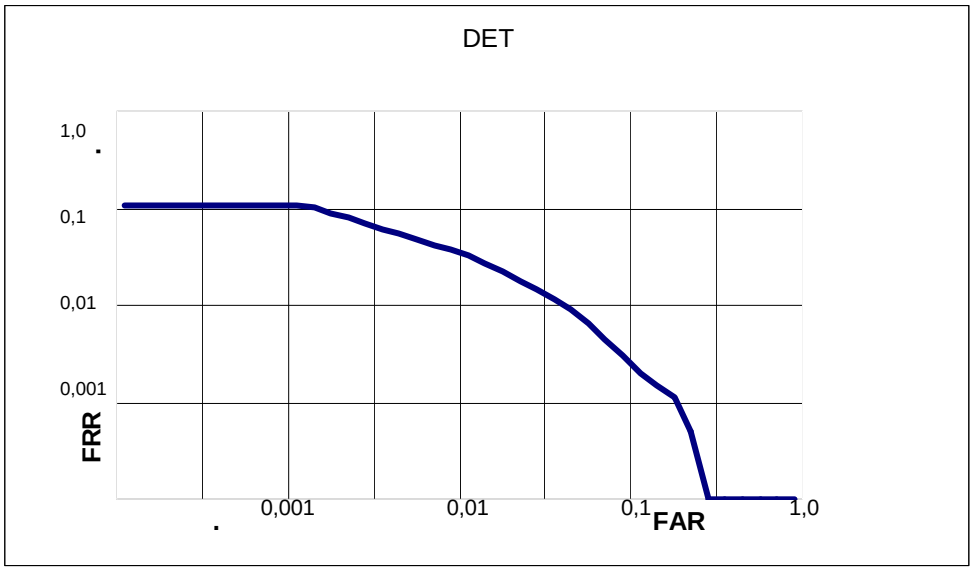

Bild 3-7: DET-Kurve mit obigen Messwerten.

Die DET-Kurve bietet die Möglichkeit unterschiedliche Arbeitspunkte zu bestimmen.

3.2.8 Failure to Enrol Rate

Wie in Kapitel 2.2.4 dargelegt, kann das ausgewählte Verfahren ein biometrisches Merkmal verwenden, dass 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 den das Enrolment nicht durchgeführt werden konnte (*number of not enroled person*),

- *NPU*: die Gesamtanzahl der potentiellen Nutzer innerhalb der Organisation des Betreibers (number of potential users).

3.2.9 Failure to Acquire Rate

Auch zum Zeitpunkt einer Identifikation oder Verifikation kann es jederzeit vorkommen, dass die Datenaufnahme fehlerhaft verläuft, so dass keine aktuellen Daten zum Abgleich mit den beim Enrolment aufgenommenen Referenzdaten zur Verfügung stehen. Der Prozentsatz von Benutzern, bei denen dieser Fehler eintritt, wird als *Failure to Acquire Rate (FTA)* bezeichnet. Folgende Aspekte sind als Ursachen zu berücksichtigen:

- Ein Benutzer, bei welchem das Enrolment noch erfolgreich war, hat zu einem späteren Zeitpunkt eine (vorübergehende oder dauerhafte) körperliche Beeinträchtigung erfahren.
- Das biometrische Merkmal eines Benutzers ist sehr schwach ausgeprägt, unterliegt statistischen Schwankungen und konnte zum Zeitpunkt des Enrolments nur "zufällig" mal einen brauchbaren Datensatz liefern.
- Es handelt sich um einen unberechtigten Benutzer, der nicht registriert ist und bei welchem das Enrolment auch nicht funktioniert hätte.

Die *FTA* errechnet sich wie folgt:

$$FTA = \frac{NNA}{NPU} \cdot 100\%$$

wobei *NNA* die Anzahl der Personen darstellt, bei denen die Aufnahme der aktuellen Daten schief gegangen ist.

Die *FTA* ist bei den Fehlerraten *FAR* und *FRR* mit zu berücksichtigen, d.h. die Anzahl *NNA* muss bei den berechtigten und unberechtigten Zutrittsversuchen (*NEA*, *NIA*) mitgezählt werden. Zur Berücksichtigung bei der statistischen Verteilung der Übereinstimmungsgrade sind die Fälle, in denen ein *Failure to Acquire* auftritt als Ergebnisse mit Übereinstimmungsgrad 0 zu werten.

3.2.10 False Match Rate, False Non-Match Rate

Geht man sowohl bei berechtigten als auch bei unberechtigten Zutrittsversuchen von der Situation aus, dass die Aufnahme eines aktuellen Datensatzes korrekt funktioniert hat (d.h. lässt man die o.g. *FTA* außer Acht), so spricht man gelegentlich auch von den folgenden Fehlerraten:

False Match Rate (FMR): Wahrscheinlichkeit, dass die von einem unberechtigten Benutzer aktuell aufgenommenen Daten fälschlicherweise eine korrekte Übereinstimmung mit den Referenzdaten eines berechtigten Benutzers ergeben.

False Non-Match Rate (FNMR): Wahrscheinlichkeit, dass die von einem berechtigten Benutzer aktuell aufgenommenen Daten fälschlicherweise keine korrekte Übereinstimmung mit den Referenzdaten ergeben.

Die beiden Fehlerraten *FMR* und *FNMR* können als charakteristische Größen zur Analyse mathematischer Vergleichsverfahren für biometrische Daten dienen. Zur Beurteilung der Praxistauglichkeit biometrischer Systeme sind sie jedoch weniger geeignet, da man hier (wie oben erwähnt) auch immer die Möglichkeit eines *Failure to Acquire* mitberücksichtigen muss.

Zu den für die Praxis relevanten Fehlerraten *FAR* und *FRR* besteht der folgende Zusammenhang:

$$FAR = (1 - FTA) \cdot FMR$$
$$FRR = FTA + (1 - FTA) \cdot FNMR$$

3.2.11 Mehrere Erkennungsversuche

Alle bekannten biometrischen Systeme räumen dem Nutzer mehrere Versuche ein, um sich gegenüber dem System zu authentifizieren.

Wie wir unten sehen werden, existiert aber ein erheblicher Unterschied zwischen zwei Verfahren, die zwar den gleichen Sensor und gleichen Erkennungsalgorithmus haben, aber verschiedene Anzahlen von Fehlversuchen zulassen.

Beispiel 1

Sei bei einem System die FAR = p = 0,01 und die FRR = q = 0,02.

Sind zwei Versuche zugelassen, so gilt

FAR_2 (lies: FAR bei zwei zugelassenen Versuchen)
= p + (1-p)p = 0,01 + 0,99*0,01 = 0,0199

Der Nichtberechtigte hat zwei Chancen: Beim ersten Mal kommt er mit Wahrscheinlichkeit p in das System, ist er beim ersten Mal abgewiesen worden (Wahrscheinlichkeit (1-p)), so schlüpft er beim zweiten Versuch wieder mit Wahrscheinlichkeit p durch die Kontrolle.

FRR_2 = q * q = 0,02 *0,02 = 0,0004.

Das System muss den Berechtigten zweimal hintereinander abweisen (Jeweils Wahrscheinlichkeit q), wenn dieser komplett abgewiesen werden soll.

Man sieht schon an diesem einfachen Beispiel, dass das Verfahren mit zwei Versuchen ganz andere Parameter hat.

Beispiel 2

Sei bei einem System die FAR = p = 0,01 und die FRR = q =0,02.

Sind drei Versuche zugelassen, so gilt

FAR_3 = p + (1-p)p + (1-p)*(1-p)*p = 0,01 + 0,99*0,01 + 0,99*0,99*0,01
= 0,029701

Sind n Versuche zugelassen, so gilt

$$FAR\_n = p + (1-p)p + (1-p)*(1-p)*p+.... = 1- (1-p)^n$$

Sind drei Versuche zugelassen, so gilt für die FRR:

FRR_3 = q * q * q = 0,02 * 0,02 * 0,02 = 0,000008
.

Sind n Versuche zugelassen, so gilt

$$FRR\_n = q^n.$$

Zusammenfassung
Sind bei einem biometrischen System mehrere Versuche zugelassen, so steigt mit jedem weiteren zugelassenen Versuch die FAR und fällt die FRR. Es fällt also die Sicherheit und es steigt der Komfort.
Die genauen Werte sind: $FAR\_n = 1- (1-p)^n$ und $FRR\_n = q^n$.

Für kleine n und kleines p gilt die Näherung $FAR\_n \approx np$.

Wie oben aufgezeigt, verändern sich die Fehler erheblich, wenn man mehr als einen Vergleich zulässt.
Man kann allgemein sagen, die FAR erhöht sich drastisch, es werden also mehr Unberechtigte zugelassen, während die FRR gegen Null geht.

3.2.12 Größerer Fehler bei Betriebsart Identifikation gegenüber Betriebsart Verifikation

Da die obige Berechnung nicht voraussetzt, dass die einzelnen Vergleiche immer gegen die gleiche Referenz durchgeführt werden müssen, kann sie auch für den Vergleich der Systeme in den Betriebsarten Identifikation und Verifikation angewendet werden. Voraussetzung ist, dass beim betrachteten System der 1:n -Vergleich durch n Durchführungen von 1:1 Vergleichen durchgeführt wird.

Soll biometrische Erkennung im Identifikationsmodus betrieben werden, muss das eingesetzte System einen sehr niedrigen FAR_1-Wert aufweisen, wenn die Sicherheit noch angemessen hoch sein soll. [D1]

3.2.13 Gleichzeitige Prüfungen mehrerer Merkmale

Systeme die eine gleichzeitige Prüfung mehrerer biometrischer Merkmale vorsehen, erfordern einen erhöhten Hard- und Softwareaufwand und sind deshalb nicht sehr verbreitet.
Bei diesen Systemen gibt es verschiedene Betriebsarten: So kann ein System, dass 3 Merkmale prüft, so betrieben werden, dass alle drei Prüfungen positiv ausgehen müssen oder auch so betrieben werden, dass zwei von drei Prüfungen erfolgreich sein müssen.

Wir bezeichnen das erste Verfahren mit „ 3 aus 3“, das zweite Verfahren mit „2 aus 3“. Allgemein: eine Gesamtprüfung, die k erfolgreiche Prüfungen aus m Teilprüfungen erfordern als „k aus m“.

Beispiel 3 „3 aus 3“

Sei bei dem Teilsystemen die jeweilige FAR p1 = 0,01, p2 = 0,02, p3 = 0,03
und die FRR q1 = 0,01, q2 = 0,02, q3 = 0,03.

FAR_3aus3 = p1 * p2 * p3 = 0,000006

FRR_3aus3 = q1 + (1-q1)*q2 + (1-q1)(1-q2)*q3
= q1 + q2 + q3 – q1*q2 – q1*q3 – q2*q3 + q1*q2*q3 = 0,058906

Werden bei einem biometrischen System die Teilprüfungen „m aus M“ ausgewertet, so fällt mit jeder weiteren (unabhängigen) Teilprüfung die FAR und steigt die FRR. Es steigt also die Sicherheit und es sinkt der Komfort.

Die genauen Werte sind: FAR_n = $\prod$ pi und FRR_n = $\sum \prod$ (1-qj)qi

Wie die hohe Abweisungsrate von Zugelassenen von fast 6 % zeigt, liegt hier das Problem. Durch die entstehende hohe Abweisungsrate können nicht sehr viele parallele Teilprüfungen durchgeführt werden.
Hier stößt also die erreichbare Sicherheit auf ihre Grenzen.

Beispiel 3 „2 aus 3“

Sei bei dem Teilsystemen wieder die jeweilige FAR p1 = 0,01, p2 = 0,02, p3 = 0,03
und die FRR q1 = 0,01, q2 = 0,02, q3 = 0,03.

FAR_2aus3 = p1 * p2 * p3 + p1 * p2 * (1-p3) + p1 * (1-p2) * p3 + (1-p1) * p2 * p3
= 0,001088

FRR_2aus3 = q1 * q2 * q3 + q1 * q2 * (1-q3) + q1 * (1-q2) * q3 + (1-q1) * q2 * q3
= 0,001088

Man beachte, dass die Parameter FAR und FRR nur dann wesentlich besser als die beste Teilprüfung sind, wenn die Verfahren ungefähr gleichwertig sind. Sonst ist die besten Einzelprüfung nicht viel schlechter als eine wesentliche aufwändigere Mehrfachprüfung im „2 aus 3“ Modus.

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 Anzahl der verwendeten Datensätze 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 sichergehen, dass die wirkliche Fehlerrate, z.B. die FAR, mit hoher Wahrscheinlichkeit unterhalb einer bestimmten oberen Grenze liegt. Es ist demnach folgende Frage zu beantworten:
Wie viele Datensätze werden benötigt, um mit einer bestimmten Sicherheit sagen zu können, dass die Fehlerrate eines gegebenen biometrischen Systems unterhalb der bestimmten oberen Grenze gemäß des gewählten Sicherheitsniveaus liegt?

Statistisch gesprochen entspricht das der Anzahl benötigter Beobachtungen n_τ zur Schätzung einer relativen Häufigkeit bei bekannter Varianz *h*, Irrtumswahrscheinlichkeit τ und Genauigkeit δ.

Das heißt für

- eine Sicherheit von 95% (τ = 0.05), d.h. Z_τ = 1,96 (siehe unten)
- eine *FAR* von 10% (*h* = 0,1) sowie für
- eine maximale Abweichung der realen von der geschätzten Fehlerwahrscheinlichkeit von 5% (δ = 0,05)

benötigt man nach der Formel

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

mindestens 138 Datensätze.

Dabei ist Z_τ das so genannte "τ-Quantil" der Standardnormalverteilung, d.h. eine Standardnormalverteilte Zufallsvariable nimmt größere Werte als Z_τ (nur) mit Wahrscheinlichkeit τ an.
Der interessierte Leser sei z.B. auf das Buch von *L. Sachs*[2] verwiesen. Weitere wichtige Schranken von Z_τ für den zweiseitigen Test sind Z_τ =2,58 (für τ = 0.01) und Z_τ =2,24 (für τ = 0.025).

In Bild 3-8 sind Mindestzahlen n_τ von Testpersonen angegeben mit Z_τ = 1,96, die für eine bestimmte Sicherheitsklasse und *FAR* notwendig sind. Die Messung der *FAR*

[2] Lothar Sachs, *Statistische Methoden: Planung und Auswertung*, Springer-Verlag Berlin Heidelberg New York, 7. Auflage, 1993.

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. Wie man schon an der Formel erkennen kann, ist die zulässige Abweichung δ ein kritischer Faktor, welcher – bei Forderung von kleineren Werten – zu einem überproportionalen Anstieg der Anzahl der benötigten Testpersonen führt. 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 derselben Sicherheitsanforderung zu genügen.
Dagegen ist die geforderte Sicherheit zur Unterschreitung der maximalen Abweichung ein weniger kritischer Faktor. Der Wert von Z_τ geht zwar ebenfalls als quadratischer Faktor ein, steigt aber mit kleiner werdendem τ nur noch langsam an.
Des Weiteren ist zu erkennen, dass die Anzahl der benötigten Personen mit dem Wert der typischen Fehlerrate (bei gleich bleibender zulässiger Maximalabweichung) deutlich zurückgeht, sofern sich die Fehlerraten im Bereich deutlich unter 50 % bewegen.

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.

obere Grenze (*FAR*+δ)	δ	*FAR*	n_τ
15,0%	5,0%	10,0%	138
10,0%	2,0%	8,0%	707
5,0%	1,0%	4,0%	1475
4,9%	0,9%	4,0%	1821
3,6%	0,6%	3,0%	3105
2,5%	0,5%	2,0%	3012
1,9%	0,4%	1,5%	3547
1,5%	0,5%	1,0%	1521
1,0%	0,3%	0,7%	2967
1,0%	0,2%	0,8%	7622
0,5%	0,1%	0,4%	15305
0,3%	0,1%	0,2%	30671

Bild 3-8: Anzahl benötigter Testpersonen zur Bestimmung der FAR

Zum Vergleich die Strength of Function (SOF) nach BEM (Biometric Evaluation Methodology): http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf

Table 11: SOF defined in Terms of FAR

Strength of Function Level	Maximum FAR
SOF-Basic	0.01 (1 in 100)
SOF-Medium	0.0001 (1 in 10,000)
SOF-High	0.000001 (1 in 1,000,000)

Zum Erreichen dieser Stärke sind, wie wir oben gesehen haben, eine große Anzahl von Tests nötig.

In der Untersuchung BioP II [3] wird nach Erkennungsleistungen für verschiedene Sicherheitsniveaus differenziert, die aber leichter durch Tests erreichbar sind:

- FAR=0,001%
- FAR=0,01%
- FAR=0,1%
- FAR=1%

Dabei wird in BioP II eine FAR von 0,1% als akzeptables Sicherheitsniveau für ein realistisches Einsatzszenario angesehen.

3.4 Praktische Bewertung der Fehlerraten

Im Gegensatz zur Kryptographie fließen nicht nur die Geräteeigenschaften des biometrischen Systems in die Fehlerrate ein. Die maßgeblichen Einflussgrößen für Gesamtfehler bei biometrischen Systemen sind:

a) **(Labor)-Qualität des biometrischen Systems**
   Die idealisierte Fehlerrate des Systems, d.h. in der Regel die unter optimalen Laborbedingungen und mit geeigneten Testpersonen erzielte Fehlerrate.
b) **Qualität des Enrolments**
   Werden die biometrischen Daten in der Enrolmentphase nicht sorgfältig eingelernt, so kann auch ein gutes System überwunden werden. Das kann bei der Betriebsart „Identifikation“ dazu führen, dass durch die Hinzunahme einer einzigen weiteren Person, bei der nicht auf eine hohe Qualität beim Enrolment geachtet wird, das gesamte System unsicher wird.
c) **Qualität der aktuellen Messung des biometrischen Merkmals**
   Durch wechselnde Einsatzumgebungen der Biometrie kann der Einsatz problematisch werden. Jedes biometrische Erkennungssystem ist aufgrund der unterschiedlichen Technologien der Sensoren (Kameras, Scanner, Mikrofone, ...) typischen Umgebungsstörfaktoren ausgesetzt. Licht hat z. B. keinen Einfluss auf die Sprechererkennung, wohl aber auf die Gesichtserkennung. Abhängig von den Umgebungsstörfaktoren ist die Eignung der einzelnen biometrischen Verfahren zu bestimmen.

[3] www.bsi.bund.de/Biometrie

3.5 Ermittlung der Qualitätskennzahlen

3.5.1 Fehlerrate

Wie wurde vorgegangen um die Fehlerraten zu bestimmen ?

a) Wurde die Fehlerrate mit wirklichen Messwerten 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) Folgende Biometrien sollten auch mit Vorinformationen getestet werden, um die Stärke der eigentlichen Biometrie beurteilen zu können:
   - Schriftdynamik, Schrifterkennung:
     Informationen über das zu schreibende Wort, Bild einer Unterschrift
   - (Statische) Sprechererkennung:
     Informationen über das zu sprechende Wort
   - Tippverhalten ohne Vorgaben:
     Informationen über den zu tippenden Text

3.5.2 Versuchsanordnung

a) Art des durchgeführten Versuches (Feldtest oder Labortest)

b) Erfahrungsbericht

c) Anzahl der Probanden

d) Anzahl der durchgeführten Vergleiche

e) Zusammensetzung der Testgruppe im Bezug auf das untersuchte Merkmal

f) Gesamtdauer des Tests (Tage / Wochen / Monate)

g) Motivation der Probanden

Berücksichtigung von Interoperabilitätskriterien, z.B. Durchführung von Enrolment und Erkennung mit unterschiedlichen Systemen (siehe Kap. 7)

3.5.3 Natürliche Variabilität der Referenzdaten

Biometrische Verfahren werden in verhaltensbasierte und physiologische Verfahren unterschieden. Verhaltensbasierte Verfahren, die auf dem Verhalten des Menschen beruhen, wie Unterschriftserkennung, Tippdynamik oder Sprechererkennung unterliegen immer natürlichen Schwankungen, die, unabhängig von Schwankungen in der Datenaufnahme, zu unterschiedlichen Beispielcharakteristiken führen. Physiologische Eigenschaften des Menschen hingegen, wie Irismuster oder Fingerabdruck, verändern sich 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.

3.5.4 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.

3.5.5 Art der Erhebung der Falschakzeptanzrate

Um die Falschakzeptanzrate zu bestimmen, müssen die biometrischen Daten möglichst vieler verschiedener 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 Personen gewonnen wurden. Dabei werden zwei Arten unterschieden:

- **Zufällige biometrische Daten**: 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.
- **Einfache Fälschungen**: Hier ist den Testpersonen die erfasste biometrische Kennung bekannt und sie versuchen diese Originale so gut wie möglich nachzuahmen. Dies kann durch Üben bei aktiven Merkmalen (Schrift, Stimme) oder durch einfache Manipulationen (Gesicht: Schminken usw.) geschehen. Mit einfachen Fälschungen erzeugte Fehlerraten werden im Normalfall wesentlich schlechter als solche mit zufälligen biometrischen Daten nicht erfasster Personen sein. Solche einfachen Fälschungen sollten auch in die Fehlerrate eingerechnet werden, da ein seriöser Test eine pessimistische Abschätzung für den realen Einsatz liefern muss und solche einfachen Angriffe vorkommen.

3.6 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 dargestellt werden. Dazu zählt beispielsweise der Fingerabdruck, den eine Person an vielen Orten unbeabsichtigt hinterlässt (Beispiel Trinkglas). 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 Nebenstehender 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.

3.7 Schutz des Systems vor Angriffen

3.7.1 Aufwand eines Angriffs

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

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

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.

3.7.2 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 so genannten *Replay-Angriffe*, bei denen Daten 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 Erkennungsdaten in das biometrische System einspielt.

Besonders zu beachten sind auch:

a) Vandalismus

b) Diebstahl

c) Manipulation / Attrappe

d) Insiderattacken

e) Denial-of-Service Angriffe

3.7.3 Beispiele für biometriespezifische Angriffsszenarien

Im Folgenden werden beispielhaft denkbare Angriffsmodelle mit verschiedenem Aufwand auf biometrische Systeme zu unterschiedlichen biometrischen Merkmalen vorgestellt.

<u>Fingerabdruck</u>

- 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).

<u>Stimme</u>

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

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.

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.

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

Augen

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

- geringer Aufwand der Angreifer: Farbige Kontaktlinsen verfälschen Messung. 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 Augenmodelle.

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.

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 Merkmalserfassung im System

a) Erfassung

- Enrolment: Die Aufnahme der ersten biometrischen Datensätze, die später bei der Identifikation oder Verifikation des Nutzers als Grundlage der Referenzdaten herangezogen wird, 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 Template 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 für 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 ist nur in eng geregelten rechtlichen Grenzen zulässig. (siehe Kap.5.2.4).

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

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

4.2 Anforderungen aufgrund möglicher Einsatzorte

Je nach Einsatzort des biometrischen Systems können die Anforderungen zur sicheren und störungsfreien Funktion des biometrischen Systems sehr unterschiedlich sein. Die möglichen Einsatzorte nach Norm DIN EN 50133 (1998) und CC-BSI Version 2.1 (1999) sind: Wohn-/Büroumgebung, Innenraum allgemein, geschützt im Freien und 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 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. In 4.6 sind einige hinsichtlich der Sicherheitsanforderungen sehr unterschiedliche Anwendungsfälle aufgeführt.

4.4 Toleranz des biometrischen Systems

a) Verändertes Benutzerverhalten

Es kann durchaus vorkommen, dass vor allem 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 anderseits auch bei verändertem Benutzerverhalten die Erkennung noch funktioniert und die Falschrückweisungsrate in vertretbaren Grenzen gehalten wird.

b) Veränderung des Merkmals

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) 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, das für alle denkbaren Bereiche einsetzbar sein soll, auch in diesem Fall bestimmte Veränderungen zulassen können muss.

4.5 Mobilität

a) Stationäre Einsatzmöglichkeit
   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 der Vergleich erfolgt.

4.6 Einsatzfelder

Biometrische Verfahren können in den verschiedensten Anwendungen zum Einsatz kommen und dabei für die Erhöhung der Sicherheit sorgen. Im Nachfolgenden werden die wesentlichsten biometrischen Verfahren mit ihren Möglichkeiten in verschiedenen Anwendungsszenarien beschrieben.

IT-Zugang (Login)
In den meisten Unternehmen besitzen die Mitarbeiter verschiedene Passwörter, um sich an ihrem PC und für bestimmte Softwareanwendungen anzumelden. Durch die Menge dieser Passwörter und durch den häufig erforderlichen Wechsel sind Passwörter ein lästiges Übel geworden. Login ist zurzeit die mit Abstand häufigste Anwendung von Biometrie. Die Analyse des Fingerabdrucks mittels Sensoren an Maus oder Tastatur regelt den IT-Zugang einfach und meist zuverlässig. Daneben ist in sensiblen Bereichen der Einsatz zum Freischalten eines Bildschirmschoners sinnvoll. Ein weiteres noch recht junges Anwendungsgebiet ist die Passwort-Reset-Funktion mit Hilfe der Stimmerkennung über das Telefon. Die Anwendung sieht vor, dass bei Vergessen des Passworts nicht der übliche Help Desk kontaktiert wird, sondern ein Programm, das mittels der Stimmauthentifizierung Berechtigten ein neues Passwort ausgibt.

Zutrittskontrolle
Die physische Zutrittskontrolle wird klassischerweise mit Schlüsseln, PINs oder Ausweisen, die entweder Personal oder ein Kartenlesegerät kontrolliert, geregelt. Der Einsatz biometrischer Verfahren senkt hier die Gefahr, dass unberechtigte Personen Zutritt erlangen und Schaden verursachen. Für die biometrische Zutrittskontrolle wird ein Erfassungssystem vor einer Tür installiert und mit dem Schließmechanismus verbunden. Werden solche Zutrittskontrollen für alle Mitarbeiter eingeführt, dann lassen sich die erhobenen Daten beispielsweise auch für die **Zeiterfassung** nutzen. Bei den für die Zutrittskontrolle in Frage kommenden Verfahren kommt es auf Schnelligkeit und komfortable Bedienung an. Da die meisten biometrischen Verfahren auf wechselnde Umweltbedingungen sehr empfindlich reagieren, müssen die Verfahren entsprechend robust ausgewählt werden.

Freigabe von elektronischen Schlüsseln
Als Unterthema des IT-Zugangs ist die Freigabe von elektronischen Schlüsseln zum Verschlüsseln und Signieren zusehen. Mit der Vernetzung von Datenbeständen und dem immer häufigeren Versenden elektronischer Daten steigt der Bedarf, diese Daten zu schützen. Um aber einen Datenbestand z.B. mittels Public und Private Keys verschlüsseln zu können, muss der Anwender die Schlüssel erst aktivieren. Diese Aktivierung erfolgt zurzeit mit einem Passwort oder einem PIN, wird hier Biometrie eingesetzt, ist weitgehend sichergestellt, dass die verschlüsselte Nachricht nur von der Zielperson gelesen werden kann, bzw. die elektronische Signatur nur von einer bestimmten Person stammt.
Hierbei ist aber zu beachten, dass zurzeit **kein** biometrisches Verfahren eine Zulassung als PIN-Ersatz nach dem Signaturgesetz hat (Mechanismenstärke hoch). Die größten Chancen bald zumindest ergänzend zur PIN zugelassen zu werden haben Fingerabdruck und Iris (mittel).

Bezahlen mit Biometrie
Mittels biometrischer Merkmale lassen sich, unter Verwendung einer Chipkarte, auch die übliche PIN oder die Unterschrift bei Bezahlungs- oder Abhebungsvorgängen ersetzen.
Hierbei ist aber zu beachten, dass zurzeit **kein** biometrisches Verfahren eine Zulassung als PIN-Ersatz durch die Gremien der Geldwirtschaft hat. Die größten Chancen zugelassen zu werden haben Fingerabdruck und Iris.
Bezahlen nur mit Biometrie, ohne Chipkarte oder Codenummer, also in der Betriebsart Identifikation, wird es auf absehbare Zeit wohl nicht geben.

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 Produktausprägung

Die Untersuchungen der T-Systems zeigten, dass nicht eine einzige reine Hardwarelösung existiert. Für den Vergleichsprozess 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

4.9 Das Trägersystem

4.9.1 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

4.9.2 Software

Betriebssystem

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

Einbindung des biometrischen Systems

Des Weiteren ist von Interesse, ob und wie das biometrische System in ein übergeordnetes 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.

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 Datenschutz

5.1 Einleitung

Biometrische Verfahren arbeiten mit spezifischen körperlichen Merkmalen, die bestimmten natürlichen Personen eigen sind. Biometrische Informationen sind daher personenbezogene Daten, die dem Schutz des informationellen Selbstbestimmungsrechts unterliegen, wie es in den Datenschutzgesetzen des Bundes und der Länder festgeschrieben ist.

Die Datenschutzgesetze in Bund und Ländern lassen Datenverarbeitungen nur zu, wenn und soweit sie erforderlich sind. Dieser Erforderlichkeitsgrundsatz ist in § 3a BDSG wie auch in Landesdatenschutzgesetzen durch das Gebot der Datenvermeidung und Datensparsamkeit konkretisiert. Das bedeutet, dass vor dem Einsatz eines biometrischen Systems geprüft werden muss, ob alternative Methoden zur Verfügung stehen, denn es muss die datenschutzfreundlichste Lösung gewählt werden. Dies kann im Einzelfall auch die Wahl eines nicht-biometrischen Systems bedeuten.

Vor Einführung eines biometrischen Verfahrens muss geprüft werden, ob der beabsichtigte Personenkreis für die Anwendung auch solche Personen erfasst, deren Merkmalsausprägungen für eine biometrische Erkennung nicht ausreichend sind und die deshalb an der Anwendung nicht teilnehmen können. Ist dies der Fall, ist eine Alternativlösung für diesen Personenkreis zu realisieren.

Der Einsatz von biometrischen Verfahren setzt die Erhebung biometrischer Merkmalsdaten, also personenbezogener Daten voraus. Diese ist nur zulässig

- für den öffentlichen Bereich,
  wenn eine Rechtsvorschrift das erlaubt und soweit die Daten zur Erfüllung der Aufgabe der verantwortlichen Stelle erforderlich sind (§§ 4 Abs. 1 und 13 Abs. 1 BDSG) oder wenn der Betroffene eingewilligt hat;
- für den nicht öffentlichen Bereich,
  wenn es der Zweckbestimmung der "Geschäftsbeziehung" mit dem Betroffenen dient oder zur Wahrung der berechtigten Interessen der verantwortlichen Stelle erforderlich ist und schutzwürdige Belange des Betroffenen nicht entgegenstehen oder wenn der Betroffene eingewilligt hat (§ 28 BDSG).

Konkret bedeutet das für biometrische Anwendungen:

Wird die flächendeckende Einführung eines biometrischen Systems im hoheitlichen Bereich geplant (z. B. zur Einführung eines biometriegestützten Passes wie dem „ePass“, siehe im Einzelnen Kapitel 8.2.1), so ist dies nur aufgrund einer Rechtsvorschrift möglich. So wurden Pass- und Personalausweisgesetz in Deutschland entsprechend angepasst, um die Aufnahme weiterer biometrischer Merkmale sowohl im Reisepass als auch im Personalausweis zuzulassen. Etwas anderes gilt allerdings, wenn Systeme lediglich für die Abwicklung des internen Betriebs bei staatlichen Stellen eingeführt werden, wie z. B. Zugangssysteme. Nicht nur bei der Erhebung biometrischer Daten, sondern insbesondere beim Einsatz biometrischer Verfahren sind die entsprechenden Regelungen des BDSG bzw. des

jeweils geltenden Landesdatenschutzgesetzes zu beachten.

Der Grundsatz, dass keine Daten erhoben werden dürfen, die für den konkreten Zweck nicht erforderlich sind, sowie die Gebote der Datenvermeidung und Datensparsamkeit sind bei der Auswahl von Datenverarbeitungssystemen und bei der Ausgestaltung der einzelnen Verarbeitungsschritte zu beachten. Beim Einsatz eines biometrischen Systems 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 können. So kann insbesondere im Bereich der Datensicherheit – je nach Einbindung ins Gesamtsystem - 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 Anforderungen eingehalten und gleichzeitig Datenschutz und Datensicherheit gefördert werden können; in diesem Fall spricht man von so genannten *datenschutzfördernden Techniken* (*privacy enhancing technologies-PET*).

5.2 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.

5.2.1 Erforderlichkeit, Datenvermeidung und -sparsamkeit

Das BDSG schreibt vor, bei der Datenerfassung, -speicherung und Weiterverarbeitung deren Erforderlichkeit genau zu beachten (d.h., sich sparsam zu verhalten).[3] Das bedeutet, dass nur die Daten erhoben und gespeichert werden dürfen, die für die eigentliche Erkennung auch tatsächlich notwendig sind. So ist zum bloßen Feststellen der Identität bzw. Berechtigung in den meisten Anwendungsumgebungen überhaupt nicht erforderlich, die für den Erkennungsvorgang aktuell erhobenen biometrischen Daten über den Erkennungsvorgang hinaus zu speichern.
Eine eventuell erforderliche Protokollierung muss sich auf den erforderlichen Umfang beschränken. Zudem müssen 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 und etwa durch das Vier-Augen-Prinzip zusätzlich beschränkt werden können.

5.2.2 Zweckbindung

Die Daten dürfen grundsätzlich nur für den Zweck verwendet werden, für den sie erhoben wurden (§ 14 BDSG). Es sind deshalb Vorkehrungen zu treffen, die eine zweckwidrige Verwendung ausschließen.

[3] Stichwort „Datensparsamkeit“, § 3a BDSG

5.2.3 Ort der Speicherung der biometrischen Referenzdaten

Aus der Sicht des Datenschutzes sollten die biometrischen Referenzdaten dezentral unter der Kontrolle und Verfügungsgewalt des Nutzers z.B. auf einer Chipkarte, einem Token oder einer anderen mobilen Speichereinheit gespeichert werden. Ein zentraler Datenbestand birgt größere Gefahren für das informationelle Selbstbestimmungsrecht, nicht zuletzt wegen des höheren Missbrauchspotentials, der weitgehenden Anwendungsmöglichkeiten im Privatbereich und der umfassenden Datenerhebungsbefugnisse der Strafverfolgungsbehörden. Je mehr Daten zentral abgelegt sind, umso größer sind die Begehrlichkeiten, die bei Behörden und privaten Stellen zur Nutzung dieser Daten entstehen können.

Ein weiteres Problem besteht darin, dass zentrale Datenbestände ohne Wissen (und Zutun) der Betroffenen ausgewertet werden können, weil die Auswertung keine Mitwirkung der Betroffenen erfordert. Der Einsatz identischer biometrischer Verfahren in unterschiedlichen Anwendungen führt für den Nutzer zu erhöhten Risiken, da sein biometrisches Merkmal potentiell als ein (im Gegensatz zu Namen und Adresse) unveränderbares Personenkennzeichen verwendet werden kann und damit z.B. sein jeweiliges Nutzungsverhalten oder z.B. seine Zugriffsrechte zu einem umfassenden Profil zusammengeführt bzw. anderweitig missbraucht werden 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 unzweckmäßig ist), so müssen insbesondere der Zweck der Datenverarbeitung (Zweckbindung) und die Zugriffsbefugnisse restriktiv und besonders sorgfältig definiert werden. Eine etwaige Übermittlung an Dritte bedarf der Einwilligung des Betroffenen, sofern hierfür keine andere Rechtsgrundlage besteht.

5.2.4 Keine unbemerkte Erhebung der biometrischen Daten

Der Nutzer muss bei der Referenzdatenerfassung des biometrischen Merkmals willentlich mitwirken, denn die Erhebung personenbezogener Daten, also auch der biometrischen Daten, hat grundsätzlich beim Betroffenen zu erfolgen (§ 4 Abs. 2 BDSG). Ihm muss aber auch die spätere Überprüfung, also die durch den konkreten Einsatz des biometrischen Verfahrens bewirkte Datenverarbeitung im Einzelfall erkennbar sein (Transparenzgebot, insbesondere auch beim Einsatz mobiler Speichermedien, siehe § 6c Abs. 3 BDSG). Eine aktive Mitwirkung des Nutzers baut zudem mögliche unberechtigte Ängste ab und trägt somit positiv zur Akzeptanz des Systems bei.

5.2.5 Informationsgehalt der biometrischen Daten

Zur Wahrung des informationellen Selbstbestimmungsrechts der Betroffenen sollten solche biometrische Verfahren eingesetzt werden, bei denen sich aus den Merkmalsdaten möglichst keine sog. Überschussinformationen ergeben. Dies sind solche, die für den eigentlichen Zweck der Authentifizierung nicht notwendig sind. So dürfen Rückschlüsse auf den gesundheitlichen Zustand des Merkmalsträgers von vornherein nicht möglich sein, oder aber nicht ausgewertet werden können. Da üblicherweise aus den biometrischen Rohdaten solche Rückschlüsse leichter als aus den Templates gezogen werden können, sollte auf die Speicherung von Rohdaten ganz verzichtet werden. Biometrische Daten mit solchen zusätzlichen Informationen unterliegen als besondere Arten personenbezogener Daten weiteren

Beschränkungen in der Verarbeitung[4].

Hierbei ist auch zu beachten, dass biometrische Verfahren noch nicht abschließend wissenschaftlich erforscht sind und daher auch erst in der Zukunft nutzbare Zusatzinformationen berücksichtigt werden müssen.

5.2.6 Rückschluss auf die hinter den biometrischen Daten stehende natürliche Person

Die Möglichkeit, aus den reinen Erkennungsdaten 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 möglichst nicht gespeichert 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. Zudem sollte ausgeschlossen werden, dass aus mehreren biometrischen Verfahren bzw. Anwendungen, sozusagen akkumulierend, auf die natürliche Person und ihre Daten rückgeschlossen werden kann, etwa indem mit Hilfe des Merkmals mehrere Datenbestände verknüpft werden.

5.2.7 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 allermeisten Fällen auf natürliche Weise gegeben ist und dauerhaft anhält. Dadurch ergibt sich eine noch über lange Zeit hinweg wirkende Missbrauchsgefahr der Daten.

5.3 Konkrete datenschutzrechtliche Empfehlungen für den Einsatz biometrischer Verfahren

5.3.1 Allgemeine Anforderungen

Biometrische Daten sind personenbezogene Daten. Verfahren, die biometrische Daten nutzen, müssen deshalb die Grundsätze der Datenschutzgesetze erfüllen. Für die Datenverarbeitung muss es eine *Rechtsgrundlage* geben (s. Ziff. 5.1 und 5.3.2), der Einsatz des Verfahrens und der Umfang der personenbezogenen Daten muss *erforderlich* sein, die Grundsätze der *Datensparsamkeit* und *Datenvermeidung* sind bei der Ausgestaltung zu beachten. 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. Die entsprechenden

[4] nach § 3 Absatz 9 BDSG

Regelungen für technische und organisatorische Maßnahmen zu Datenschutz und Datensicherheit finden sich in den Datenschutzgesetzen Die behördlichen bzw. betrieblichen Datenschutzbeauftragten sind bei Einführung und Betrieb der Verfahren einzubeziehen.

Besonderes Augenmerk ist auf die Einhaltung des Grundsatzes der *Zweckbindung* zu legen, 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 Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert wurden, nicht für andere Zwecke verwendet werden[5].

5.3.2 Zulässigkeit der Datenerhebung, -verarbeitung und –nutzung

Die Erhebung sowie auch die Verarbeitung und Nutzung biometrischer Daten und damit der Einsatz eines biometrischen Verfahrens ist nur zulässig, wenn es dafür eine Rechtsgrundlage gibt. Als Rechtsgrundlage kommt in Betracht:

- die Personen, um deren Daten es sich handelt, haben eingewilligt (§ 4 Abs. 1 BDSG) oder
- im öffentlichen Bereich erlaubt eine Rechtsvorschrift den Einsatz und die Daten sind zur Erfüllung der Aufgabe der verantwortlichen Stelle erforderlich (§§ 4 Abs. 1 und 13 Abs. 1 BDSG) oder
- im nicht öffentlichen Bereich sind die Voraussetzungen des § 28 BDSG erfüllt.

5.3.2.1 Einwilligung der Betroffenen

Eine datenschutzrechtlich wirksame Einwilligung[6] muss *freiwillig, informiert* und *bestimmt* sein. Dies bedeutet im Einzelnen: diese Einwilligung 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 die Tragweite seiner Entscheidung absehen kann. Daneben gibt es gewisse formale Anforderungen, 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 Ablauf der Datenverarbeitung, der Ort der Speicherung etc. verständlich, d.h. unkompliziert und ohne verwirrende technische Details, vermittelt wird. Da eine umfassende Aufklärung üblicherweise zudem hilft, Ängste abzubauen, wird eine ausreichende Transparenz vermutlich auch die Akzeptanz bei der Nutzung des Verfahrens steigern. Hinzu kommt, dass die Bedienung erfahrungsgemäß gerade bei aktiv zu bedienenden 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 allenfalls marginal, nicht aber in wesentlichen Punkten geändert werden darf. Insbesondere

[5] , s. § 14 Abs. 4 und § 31 BDSG
[6] gemäß § 4 a BDSG

darf ohne Einwilligung keine Datenübermittlung an Dritte erfolgen, sofern nicht gesetzlich zugelassene Gründe vorliegen. Vor einer solchen Datenübermittlung ist zu prüfen, inwieweit schutzwürdige Belange des Betroffenen überwiegen. Ist dies der Fall, ist eine solche Übermittlung 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 (s. Kap 6.7)

5.3.2.2 Rechtsvorschriften als Zulässigkeitstatbestand im nicht-öffentlichen Bereich

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. Diese 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[7] (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[8], 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. Es sind immer die schutzwürdigen Interessen der Arbeitnehmer zu den berechtigten Interessen des Arbeitgebers abzuwägen (Verhältnismäßigkeitsgrundsatz). Zusätzlich sind die Mitbestimmungsrechte der Arbeitnehmer zu beachten, siehe dazu Kap. 6.7).

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 nachträgliche Zweckänderung ist nur in Ausnahmefällen möglich. Dies bedeutet für den Arbeitgeber beispielsweise, dass bei der Einführung eines biometrischen Systems als Zutrittskontrolle eine zusätzliche Verwendung der Daten zur Zeiterfassung im Vorfeld geregelt sowie dem Arbeitnehmer mitgeteilt werden muss.

Als weitere Rechtsvorschrift kommt insbesondere beim Einsatz biometrischer Verfahren am Arbeitsplatz neben einem Tarifvertrag auch eine Betriebsvereinbarung in Betracht, die dann sowohl die Berücksichtigung der Arbeitnehmerrechte regelt

[7] § 28 Abs.1 Nr. 1 BDSG
[8] § 28 Abs.1 Nr. 2 BDSG

(siehe dazu im Einzelnen Kap. 6.7) als auch die Rechtsgrundlage für die Datenverarbeitung darstellt. Um eine Datenverarbeitung im Sinne von § 4 Abs. 1 BDSG legitimieren zu können, werden 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 der Datenverarbeitung 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 BDSG 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 einer Vereinbarung, die für alle Nutzer gültig ist, mehr Klarheit.

6 Weitere nicht-technische Aspekte

6.1 Rechtliche Aspekte

Die rechtliche Einordnung eines biometrischen Verfahrens generell sowie eines bestimmten Systems und insbesondere die rechtlichen Anforderungen an einen rechtmäßigen Einsatz hängen von grundsätzlichen Prinzipien der einschlägigen nationalen Rechtsordnung ab[9]. Die folgenden Überlegungen beziehen sich auf vornehmlich deutsche Regelungen. Neben grundsätzlichen Rahmenbedingungen sind auch bereichsspezifische Bedingungen zu beachten, bei denen es auf die konkrete Anwendung und das einschlägige Fachverfahren 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. Wenn jemand dazu verpflichtet wird, seinen Körper zu Zwecken der Informationsauswertung (für ein biometrisches Verfahren) zur Verfügung zu stellen, kann dieser Aspekt daher relevant werden. Eine umfassende Katalogisierung der Persönlichkeit durch eine einheitliche Personenkennziffer kann ebenso einen Würdeverstoß darstellen, wie das BVerfG in dem bekannten Volkszählungsurteil festgestellt hat. Verhältnismäßigkeit ist darüber hinaus überall dort gefordert, wo widerstreitende Interessen auftreten können. Beim Einsatz von Biometrie sind das in der Regel die (berechtigten) Interessen des Betreibers an dem Einsatz des biometrischen Systems einerseits und die (schutzwürdigen) Belange des Nutzers etwa in Bezug auf dessen Persönlichkeitsrechte andererseits.

Im staatlichen Bereich können neben verfassungsrechtlichen Grundsätzen strafrechtliche und -prozessuale Regelungen beim Einsatz durch Strafverfolgungsbehörden, Pass- und Personalausweiswesen, Asylverfahrens-regelungen, Grenzkontrollvorschriften (Bundesgrenzschutzgesetz) und etwa Aspekte des Sozial(versicherungs)rechts eine Rolle spielen. In datenschutzrechtlicher Hinsicht ist bei einem verpflichtenden hoheitlichen Einsatz von Biometrie grundsätzlich eine gesetzliche Grundlage erforderlich.

6.2 Elektronische Signaturen

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 vor Gericht anerkannter Beweis besonders wichtig ist (Beweisfunktion). Neben dieser elektronischen Form wird der qualifizierten elektronischen Signatur auch in prozessualer Hinsicht ein „Vertrauensvorschuss“

[9] Vgl. aber auch den Technical Report der Working Group 6 von SC 37, der länderübergreifende Empfehlungen zu den rechtlichen sowie weiteren Aspeken des sozialen, ethischen und kulturellen Bereichs der Biometrie beinhaltet; vgl. http://www.jtc1.org/sc37

gewährt. Wird diese verwendet, wird per Gesetz nunmehr zunächst vermutet, dass diese auch tatsächlich vom berechtigten Signaturinhaber verwendet wurde (§ 371a 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. Rechtlich gesehen handelt es sich bei einer „missbrauchten" Signatur zunächst um eine vollständig wirksame elektronische Signatur des Signaturinhabers, mit allen damit verbundenen Rechten und Pflichten der Beteiligten im Rechtsverkehr.

Die bloße Nutzung einer PIN kann, wie in anderen Anwendungen auch, also den Aspekt der Autorisierung der betreffenden Signatur nicht abbilden. Während die Zuordnung einer elektronischen Signatur zu einer natürlichen Person über ein Zertifikat als „Ausweis" erfolgt, kann die Zurechnung einer konkret geleisteten Signatur und damit letztlich die Authentizität wegen der stets möglichen fehlerhaften Autorisierung nicht gewährleistet werden. Dem könnte durch den Einsatz geeigneter biometrischer Systeme begegnet werden. 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[10]. 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. 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[11].

Nach den geltenden Vorschriften sollte ein biometrisches Verfahren, das im Rahmen der qualifizierten Signatur ergänzend zur PIN eingesetzt wird, zumindest Mechanismenstärke „mittel" erreichen. Soll die PIN durch die Biometrie ersetzt werden, ist Mechanismenstärke „hoch" erforderlich. Bisher wurde kein biometrisches System mit „hoch" zertifiziert.

6.3 Personaldokumente

Im Bereich von Personaldokumenten können biometrische Merkmale die bisher auf Personalausweis oder Führerschein schon vorhandenen persönlichen Merkmale ergänzen. Im Gegensatz zu den bisher auf den Dokumenten befindlichen Passbildern und Angaben zu Augenfarbe und Körpergröße können biometrische Merkmale automatisiert ausgewertet werden 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

[10] §§ 17 Abs. 1 Satz 1 SigG in Verbindung mit § 15 Abs. 1 SigV
[11] § 15 Abs. 1 Satz 1 SigV

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. Seit Ende 2005 trägt der neue deutsche Reisepass dementsprechend ein digitales Passbild, dass auf einem RFID-Chip im Pass gespeichert wird[12].

6.4 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 (positiv) zu ermitteln und (negativ) auszuschließen.

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 konnten. Auch in diesem Zusammenhang ist die Sicherheit des biometrischen 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.[13] 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 zu beachten, 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[14], das seit 1992 beim BKA eingesetzt wird, werden aus den so gewonnen Rohdaten der Fingerabdrücke Templates erstellt und diese

[12] weiterführende Hinweise auch zur technischen Umsetzung unter http:// www.bsi.bund.de/epass
[13] vgl.§ 81g I StPO und DNA-Identitätsfeststellungsgesetz vom 07.09.1998, BGBl. I S.2646
[14] Automatisches Fingerabdruck Identifizierungs System

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[15].

6.5 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.

6.6 Allgemeine Geschäftsbedingungen beim Einsatz biometrischer Merkmale

Die kundenfreundliche Ausgestaltung der Allgemeinen Geschäftsbedingungen, insbesondere zur Verteilung von Verantwortlichkeiten und damit auch der Haftungsfragen, ist bei der Verwendung biometrischer Systeme 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 End-Kunden das verbleibende Restrisiko mittels kundenfreundlicher Geschäftsbedingungen abnehmen.

Gemäß der rechtlichen Grundsätze zur Regelung der Allgemeinen Geschäftsbedingungen[16] und der allgemeinen Mitverschuldensregelung im Zivilrecht[17] ist von folgenden Grundsätzen auszugehen:

[15] dies folgt u.a. aus §§ 22, 23 Kunsturhebergesetz
[16] vgl. §§ 305 ff. BGB
[17] § 254 BGB

- 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.

- Hinsichtlich einer Regelung zur Beweislastverteilung sollte je nach konkretem Anwendungszweck versucht werden, diese möglichst gleichberechtigt und fair sowie den unterschiedlichen Risikospähren bei Betreiber auf der einen Seite und Nutzer auf der anderen Seite angemessen zu gestalten. Aus Nutzersicht würde eine kundenfreundliche Regelung der Beweislastverteilung (und damit des Risikos des Prozessverlustes) 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. Aus Sicht des Betreibers, der ein biometrisches System möglicherweise vor allem deshalb einführt, um dem Kunden besser als mit z.B. einer PIN bestimmte Transaktionen verbindlich zurechnen zu können, muss abgewogen werden, inwieweit das eingesetzte biometrische System tatsächlich den hier erforderlichen Sicherheitsbedürfnissen entspricht.

6.7 Betrieblicher Einsatz

Bei Einführung eines biometrischen Systems in den Betrieb beispielsweise als Zutritts-, Anwesenheits- und Verweildauerkontrolle oder Zugangs- und Zugriffssicherung etwa zum PC ist grundsätzlich davon auszugehen, dass eine im

Betrieb vorhandene Arbeitnehmervertretung an dem Entscheidungsprozess nach den einschlägigen Rechtsvorschriften beteiligt werden muss. Die Erarbeitung und Realisierung einer entsprechenden Betriebsvereinbarung hat dabei bestimmten, in den betriebsverfassungs- bzw. personalvertretungsrechtlichen Regelungen festgelegten Grundsätzen zu folgen. Ausführliche rechtliche und praktische Hinweise zum Erstellen einer solchen Betriebsvereinbarung finden sich in einer Orientierungshilfe, die von Mitarbeitern der AG 6 unter fachanwaltlicher externer Beratung erstellt wurde und kostenlos von der TeleTrusT-Webseite herunter geladen werden kann [TTT OH Betriebsvereinbarung].

6.8 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. 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. deren 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 manche Anbieter 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 bestimmten 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. 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.

6.9 Benutzerakzeptanz

6.9.1 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.

6.9.2 Allgemeine Haltung und Nutzungstypen

Ein weit reichendes 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 Personen, die dem Erkennungssystem gegenüber positiv eingestellt sind, die durch die Anwendung eines biometrischen Systems einen Vorteil verspüren.

- Nicht-Kooperativer-Nutzer

Es handelt sich bei diesen Nutzern eher um Personen, die dem Erkennungssystem gegenüber negativ eingestellt sind, 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, sich dem Verfahren anpassen und es korrekt benutzen wollen.

6.9.3 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 den 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.

6.9.4 Enrolment und Benutzerführung

Die Aufnahme der ersten biometrischen Datensätze, die 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 Erkennung 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 Template zu überprüfen und ggf. eine neue Erfassung vorzunehmen.

Wegen der 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.

6.9.5 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.

6.9.5.1 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 Zutrittssicherung 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.

6.9.5.2 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.

6.9.5.3 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.

6.9.5.4 Kosten für den 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. 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.

6.9.6 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.

6.9.6.1 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.

6.9.6.2 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.).

6.9.6.3 Ergonomie der Anwendergeräte

Die ergonomische Ausgestaltung des Endgeräts sollte häufig vorkommende körperliche Einschränkungen (s. auch unter Ausgrenzung) berücksichtigen. Die behindertengerechte Gestaltung gehört z.B. dazu durch die Möglichkeit, auch mit einem Rollstuhl nah genug an z.B. 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.

6.9.6.4 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.

6.9.7 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.

6.9.7.1 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.

6.9.7.2 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

6.9.7.3 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.

6.9.7.4 Nutzung für Zwecke der Strafverfolgung

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

6.9.7.5 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.

6.9.8 Verlässlichkeit des Systems

Das verlässliche Funktionieren 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.

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 Entwicklungstand 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 Pilotinstallationen bzw. Referenzinstallationen gefragt werden, die benannten Stellen auch wirklich kontaktiert werden 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 Reflektionen, 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, Grafiktabletts, 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 andere 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 neuer Benutzer in der Datenbank

b) Löschung alter Benutzer in der Datenbank

c) Erzeugung neuer Referenzmuster

d) 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

c) Können unterschiedliche Sicherheitsanforderungen abgedeckt werden?

d) 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

a) 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

b) 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.

c) 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 Bereich (eigene Haustür, Garagentor, Kfz).

7.9 Interoperabilitätskriterien

Beim Betrieb "offener Systeme" (mit Systemkomponenten unterschiedlicher Hersteller) oder bei Verwendung unterschiedlicher Systeme für Enrolment und Verifikation bzw. Identifikation kann es leicht zu Problemen kommen, die beim Betrieb geschlossener Systeme (alle Systemkomponenten vom selben Hersteller) oder bei Verwendung desselben Systems für Enrolment und Verifikation bzw. Identifikation nicht auftreten. Es gibt jedoch zahlreiche Anwendungen, bei denen die Verifikation bzw. Identifikation von Benutzern an verschiedenen Orten notwendig ist. Des Weiteren sind auch häufig einzelne Systemkomponenten – z.B. Sensoren oder Software-Module für Merkmalsextraktion bzw. Merkmalsvergleich – als OEM-Produkte verfügbar. Für einen effizienten Einsatz biometrischer Systeme ist hier die Einhaltung bestimmter Interoperabilitätskriterien von großer Wichtigkeit.

7.9.1 Austausch von Systemkomponenten

a) Technische Interoperabilität: Können unterschiedliche Systemkomponenten unterschiedlicher Hersteller "sinnvoll zusammenarbeiten", d.h. in ihrem Zusammenspiel eine Verifikation bzw. Identifikation sinnvoll durchführen? (z.B. korrekte Interpretation von Datensätzen)

b) Performance-basierte Interoperabilität: Können bei Austausch von Systemkomponenten gleichermaßen gute Fehlerraten (FAR/FRR) erzielt werden?

7.9.2 Unterschiedliche Systeme für Enrolment, Verifikation bzw. Identifikation

a) Technische Interoperabilität: Ist ein System vom Hersteller X in der Lage, die Verifikation bzw. Identifikation eines Benutzers sinnvoll durchzuführen, wenn das Enrolment mit dem System eines anderen Herstellers Y durchgeführt wurde?

b) Performance-basierte Interoperabilität: Können die bei den Systemen zweier Hersteller X und Y erzielten Fehlerraten (FAR/FRR) weiterhin erzielt werden, wenn das eine System für Enrolment und das andere für Verifikation bzw. Identifikation verwendet wird? Kann eine registrierte Person sicher sein, auch an anderen Orten mit anderen im Einsatz befindlichen Systemen gleichermaßen gut wiedererkannt zu werden?

8 Untersuchungsberichte, Schwerpunktanwendungen und Entwicklungstendenzen

8.1 Untersuchungsberichte

Im Folgenden werden einige der zwischen 2002 und 2006 durchgeführten Untersuchungen zu biometrischen Verfahren exemplarisch dargestellt.

8.1.1 Nationale Projekte

8.1.1.1 BioFinger: Evaluierung biometrischer Fingerabdrucktechnologien[18]

Das Projekt BioFinger I wurde vom BSI initiiert und finanziert. Das Fraunhofer Institut für Graphische Datenverarbeitung (IGD) führte das Projekt in der Zeit von Dezember 2002 bis Mai 2004 nach Maßgaben durch, die das BSI in Kooperation mit dem Bundeskriminalamt (BKA) erstellte.

Hintergrund für dieses Projekt war die mögliche Integration von Fingerabdrücken in deutsche Personaldokumente mit dem Ziel, die Verifikation der Ausweisinhaber zu verbessern. Demzufolge war das Verifikationsszenario Grundlage des Projektes, d.h. die Überprüfung der vorgegebenen Identität der Person (1:1 Vergleich). Dazu wurden mit 11 Scannern verschiedenster Technologien Fingerabdrücke aufgenommen und mit 7 Algorithmen verschiedener Hersteller ausgewertet. Zusätzliche Fingerabdrücke aus den Beständen des BKA ermöglichten die Untersuchungen bzgl. Fingerabdrücken, die nicht zeitnah aufgenommen wurden. Die Evaluierung liefert Antworten u.a. auf die folgenden Fragen.

- Welche Erkennungsleistung ist mittels Fingerabdruckerkennung mit heute verfügbaren Scannern und Algorithmen zu erzielen?
- Welchen Einfluss auf die Erkennungsleistung haben die Scanner, welchen die Algorithmen?
- Wie wirkt es sich aus, wenn die Aufnahme des Referenz-Fingerabdrucks ein Alter von 10 Jahre erreicht?

8.1.1.2 BioFace: Untersuchung der Erkennungsleistung von Gesichts-erkennungssystemen[18]

In den Teilprojekten BioFace I und BioFace II wurde eine vergleichende Untersuchung der Erkennungsleistung von Gesichtserkennungssystemen durchgeführt. Die Untersuchungen liefen dabei einmal auf der Ebene reiner Algorithmentests (Labortests) im Bereich der Verifikation (1:1-Vergleich) und der Identifikation (1:n-Vergleich) und zum anderen auf der Ebene eines Tests unter realistischen Einsatzbedingungen im Bereich der Identifikation (Praxistest/Systemtest) ab. Die vorrangige Zielsetzung dabei war, die Leistungsfähigkeit der Systeme bei großen Datenbeständen und den Einfluss von Störfaktoren zu analysieren. Der hier vorliegende Bericht dokumentiert die Rahmenbedingungen, das verwendete Datenmaterial sowie Vorgehensweise und Ergebnisse der Untersuchungen selbst.

[18] www.bsi.bund.de/Biometrie

8.1.1.3 BioPI + II: Untersuchung der Leistungsfähigkeit von Gesichts-erkennungs- und weiteren biometrischen Verfahren in Bezug auf Ausweisdokumente[18]

Neben zahlreichen Labortests wurde mit der Projektreihe "BioP I und II" ein umfangreiches Feldtestprogramm zu Finger-, Gesichts- und Iriserkennung realisiert.

„BioP I“: Untersuchung der Leistungsfähigkeit verfügbarer Gesichtserkennungs-systeme für eine Verwendung in Personaldokumenten

Das Projekt BioP I wurde unter der Gesamtprojektleitung des BSI gemeinsam mit dem Bundeskriminalamt (BKA) durchgeführt und durch die Firma secunet Security Networks AG als Auftragnehmer des BSI im Zeitraum von Januar bis August 2003 in Wiesbaden mit Mitarbeitern des BKA als Testteilnehmer realisiert.

Die Untersuchung biometrischer Gesichterkennungsverfahren im Rahmen dieses Projekts diente dazu, Aussagen zur Leistungsfähigkeit der zum gegenwärtigen Zeitpunkt auf dem Markt verfügbaren Gesichtserkennungssysteme bezüglich verschiedener Aspekte zu treffen und daraus Erkenntnisse für eine Verwendung von Gesichtserkennung im Zusammenhang mit Personaldokumenten zu gewinnen.

„BioP II“: Untersuchung verschiedener biometrischer Verfahren mit Bezug auf Ausweisdokumente

Die zweite Projektphase BioP II hat sich unmittelbar an BioP I angeschlossen. Hier wurde der Testsieger aus BioP I einem vergleichenden Systemtest mit den beiden biometrischen Verfahren der Fingerabdruck- und Iriserkennung unterzogen. Neben dem Gesichtserkennungssystem kamen ein Iriserkennungssystem und zwei unterschiedliche Fingerabdruckssysteme zum Einsatz. Für die Durchführung von BioP II konnten die beiden Unternehmen Fraport AG und Deutsche Lufthansa AG gewonnen werden. Der Test wurde nach den notwendigen Abstimmungen und gemeinsamer Festlegung insbesondere der Rahmenbedingungen vor Ort am Frankfurter Flughafen an vier unterschiedlichen Aufstellorten im Zeitraum von November 2003 bis November 2004 realisiert. Die Konstellation der Projektpartner war bis auf die Einbindung der beiden genannten Unternehmen dieselbe wie bei BioP I. Fraport AG und Deutsche Lufthansa AG stellten insbesondere die notwendige Infrastruktur für die Testumgebungen zur Verfügung und betreuten die Testteilnehmer.

Die hier interessierenden Fragestellungen beinhalteten die Leistungsfähigkeit der getesteten Systeme und deren Sicherheit sowie eine Studie zu Akzeptanz und Benutzbarkeit. Die zentralen Fragen betrafen insgesamt die Praxistauglichkeit der untersuchten Verfahren bei einer großen Nutzergruppe sowie mögliche Empfehlungen für einen späteren Einsatz in Ausweisdokumenten. Dabei ging es um grundsätzliche Aussagen zu den verschiedenen biometrischen Verfahren und nicht um die Auswahl des in Zukunft tatsächlich einzusetzenden Systems.

8.1.2 Internationale Projekte

8.1.2.1 FRVT2002

FRVT(Face Recognition Vendor Test) 2002, ist der bislang umfangreichste und anspruchvollste Leistungstest für biometrische Gesichtserkennung in den USA und wurde von den US-Behörden DARPA (Defense Advanced Research Projects

Agency), NIST (National Institute of Standards and Technology), DoD Counterdrug Technology Development Program Office, und NAVSEA (Naval Sea Systems Command) durchgeführt.
In der Beschreibung des Zieles der Untersuchung heißt es:
Der Face Recognition Vendor Test (FRVT) 2002 ist eine durch unabhängige Stellen durchgeführte Technologieuntersuchung von ausgereiften Gesichtserkennungssystemen. FRVT 2002 bietet Ergebnisse von Leistungsmessungen, die die Eignung von Gesichtserkennungssystemen für Massenanwendungen in der Praxis bewerten. Die Teilnahme an FRVT 2002 war offen für kommerzielle Systeme und ausgereifte Prototypen von Universitäten, Forschungsinstituten und Unternehmen. Zehn Unternehmen stellten entweder kommerzielle oder Prototyp-Systeme zur Verfügung. Die Systeme hatten Testszenarios zu durchlaufen, in denen die Erkennungsgenauigkeit bei Verwendung großer Gesichtsdatenbanken untersucht wurde ("large-scale verification", "identification" und "watch list performance"). In allen Tests ergab sich ein deutlicher Abstand zwischen einer Spitzengruppe von drei Herstellern (Cognitec, Identix, Eyematic) und den restlichen Systemen.
Weitere Informationen unter: www.frvt.org

8.1.2.2 FpVTE2003

Fingerprint Vendor Technology Evaluation (FpVTE) 2003, die Studie, die von der Justice Management Division des US-Justizministeriums in Auftrag gegeben wurde, dient der Bewertung der Genauigkeit von Systemen zur Überprüfung, Identifizierung und Verifizierung von Fingerabdrücken. Durchgeführt wurden die Tests vom National Institute of Standards and Technology (NIST). Ziel der Testreihe war es, das präziseste System zur Überprüfung von Fingerabdrücken zu finden und den Einfluss einer Reihe von Variablen auf die Treffergenauigkeit zu testen.
Insgesamt nahmen 18 Unternehmen an der FpVTE 2003 teil. Getestet wurden 34 Systeme. Die besten Systeme stellten die Firmen NEC, Cogent und SAGEM.
Weitere Informationen unter: http://fpvte.nist.gov/FpVTEMain.html

8.1.2.3 FVC2004

Unter der Bezeichnung FVC(Fingerprint Verification Competition)2004 veröffentlicht die Universität Bologna einen gemeinsam mit der Michigan State University und der San Jose State University organisierten Testwettbewerb zu Fingerprint Verifikationsalgorithmen, an dem sich eine Vielzahl von akademischen Einrichtungen, Industrieunternehmen und unabhängige Entwickler beteiligt haben. Ein wesentliches Ziel dieses Wettbewerbes war es, den Teilnehmern aufzuzeigen, wo sie im Vergleich zu anderen stehen und Wege zur Verbesserung Ihrer Algorithmen aufzuzeigen.
Weitere Informationen unter: http://bias.csr.unibo.it/fvc2004/default.asp

8.2 Biometrie im Alltag

8.2.1 ePass - Der neue Reisepass mit biometrischen Merkmalen

Biometrie im elektronischen Reisepass (ePass)
Mit der Einführung des elektronischen Reisepasses setzt Deutschland eine entsprechende EG-Verordnung um. Deutschland gehört zu den ersten europäischen Ländern, die den ePass einführen.

Die Integration von biometrischen Daten in elektronischen Identitätsdokumenten ist mit der Bereitstellung von Normen und Standardisierungsdokumenten von ISO und ICAO seit 2005 möglich geworden. Biometrische Daten bieten insbesondere ein weiteres Merkmal zur Erhöhung der Sicherheit von ID-Dokumenten gegen Fälschung und Verfälschung. Darüber hinaus tragen sie zur Erleichterung von Grenzüberschreitungen vor allem bei internationalen Reisen bei.

Die Erfassung der biometrischen Merkmale

Der grundsätzliche Erfassungsprozess der biometrischen Daten gliedert sich in der Europäischen Union zeitlich in zwei Phasen. In Phase eins wird nur die Aufnahme des Gesichts als biometrisches Merkmal von den Behörden erfasst. In Phase zwei werden dann zusätzlich zum Lichtbild die Bilder zweier Fingerabdrücke aufgenommen und auf dem Chip gespeichert. Im Rahmen des Erfassungsprozesses für die Phase der Aufnahme des Lichtbildes als biometrisches Merkmal ändert sich für den Bürger vorerst nicht viel. Anstelle der bisherigen Fotos mit leichtem Halbprofil sind jetzt Fotos mit Frontalaufnahme notwendig. Die Qualität der Fotos muss den Kriterien der ICAO genügen, damit die biometrischen Merkmale auch für den späteren Kontrollprozess beim Grenzübergang geeignet sind. Um den Prozess der Datenerfassung zu unterstützen und zu objektivieren werden IT-gestützte Systeme eingesetzt, die in die bestehende DV-Infrastruktur integriert werden. Anhand von konfigurierbaren Parametern werden z.B. Augenabstand, Kopfneigung und Kopfgröße analysiert und eine Empfehlung für die Eignung und Annahme eines Lichtbildes gegeben. Grundlage für die Gestaltung solcher Systeme sind die umfangreichen Studien und Tests der ICAO, des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Bundeskriminalamtes (BKA) und der Bundesdruckerei.

Diese Systeme sind jedoch keine Garantie für eine erfolgreiche biometrische Verifikation beim Grenzübergang. Das beruht darauf, dass für eine biometrische Kontrolle an den Grenzen auch die entsprechenden Umfeldbedingungen (geeignete Erfassungsgeräte, Lichtverhältnisse, Aufnahmegeometrien) geschaffen werden müssen.

Die Kontrolle von elektronischen Pässen

Für die Kontrolle von ePässen kommen innerhalb der EU hauptsächlich die EU-Außengrenzen in Frage. Diese Grenzübergangsstellen werden nach und nach mit dem geeigneten Equipment ausgestattet. Bereits jetzt wird deutlich, dass die neuen Techniken die kontrollierenden Beamten nur unterstützen, jedoch nicht ersetzen können. Innerhalb Deutschlands obliegt der Bundespolizei und der Polizei die Kontrolle der Echtheit der Reise- und Ausweisdokumente. Die Kontrolle erfolgt dabei zu ca. 90% an Flughäfen.

Unterstützt werden die Grenzbeamten dabei durch Lesegeräte. Diese stellen die maschinenlesbaren Zone dar und gleichen die Daten mit so genannten Negativdatenbanken ab, in denen die Daten gesuchter Personen oder die Seriennummern gestohlener Dokumente zentral gespeichert sind.

Ergänzend stehen Geräte zur Verfügung, die eine maschinelle Echtheitsprüfung durchführen und elektronische Reisepässe auslesen können. Auf der Kontrollebene werden zukünftig die im Dokument gespeicherten Daten mit den bei der Kontrolle erfassten Daten des Reisenden verglichen. Wie das jeweilige System ausgestattet ist hängt vom genutzten biometrischen Verfahren und dem Einsatzort ab. Die stationären Systeme können den jeweiligen Bedingungen vor Ort (Beleuchtung, Erfassung unterschiedlich großer Personen) angepasst werden. Dadurch kann eine

qualitativ hochwertige Datenerfassung der biometrischen Daten gewährleistet und die Erkennungsleistung dieser Systeme gesteigert werden.

Personalisierungsszenarien
Bei der Herstellung und Personalisierung der ePässe sind zwei Aspekte von entscheidender Bedeutung:

1. Die Sicherheit des kontaktlos betriebenen Chips und der darauf gespeicherten personenbezogenen und biometrischen Daten.

2. Der sichere Umgang mit personenbezogenen Daten während der Personalisierung.

Der erste Aspekt wird mit der Evaluierung und Zertifizierung des Chips als Gesamtsystem aus Hardware und Software sowie der damit verbundenen Auditierung der kompletten Logistikkette der Chipherstellung sichergestellt. Die Evaluierung geschieht nach dem international anerkannten Standard „Common Criteria“ auf Evaluierungsstufe EAL 4+ gemäß den Vorgaben des Schutzprofils [PPMRTD]. Damit ist auch der Schutz der im Chip gespeicherten Daten während der Passnutzung im Feld garantiert, so dass nur Befugte Zugriff auf die sensitiven Daten erhalten.
Der zweite Punkt betrifft stärker den Personalisierungsprozess. Hier müssen zwei Aspekte unter einen Hut gebracht werden: zum einen muss beim Umgang mit personenbezogenen Daten der Datenschutz sichergestellt sein, zum anderen müssen die auf dem Chip gespeicherten Daten auch integer und authentisch sein. Letzteres wird durch von der ICAO vorgegebene kryptographische Methoden ermöglicht und muss beim Passhersteller in geeigneter Weise umgesetzt werden.

Einsatz des ePasses im Feld: Interoperabilitäts- und Sicherheitsaspekte[19]
Die wesentliche Aufgabe der ePässe im Feld ist es, eine maschinengestützte Verifikation der auf dem Chip gespeicherten Daten zu ermöglichen. Dies heißt insbesondere, dass jedes Prüf-Terminal mindestens das primäre Identifikationsmerkmal (Gesichtsbild) aus jedem ePass der Welt auslesen können muss. Dies ist reibungslos nur dann möglich, wenn sowohl ePass als auch Prüf-Terminal international akzeptierte und abgestimmte technische Spezifikationen erfüllen. Diese Spezifikation ist durch die ICAO in den Dokumenten [ICAO-LDS] und [ICAO-PKI] verbindlich vorgegeben. Die Praktikabilität dieser Spezifikationen wurde in mehreren Feld- und Interoperabilitätstests mit internationaler Beteiligung unter Beweis gestellt.
Neben den Anforderungen an die Interoperabilität sind auch Sicherheitsaspekte für den Betrieb des ePasses zu beachten. Unterschiedliche Länder haben unterschiedlich hohe Sicherheitsansprüche an Mechanismen, mit denen die im ePass gespeicherten biometrischen Merkmale vor unberechtigtem Auslesen geschützt werden.
Prinzipiell ist es möglich, die Daten auf dem Chip so abzulegen, dass der Zugriff auf die Daten über die kontaktlose Schnittstelle immer möglich ist. Die Tatsache, dass das Auslesen kontaktlos erfolgt, impliziert allerdings, dass der Auslesevorgang erfolgreich durchgeführt werden kann, ohne dass der Passinhaber aktiv an diesen Vorgang beteiligt sein muss. Entsprechend den politischen Gegebenheiten des

[19] ausführliche Informationen unter www.bsi.bund.de/biometrie/epass

jeweiligen Staates kann dies als Sicherheitsrisiko gewertet werden. Deshalb hat die ICAO mit Basic Access Control (BAC) ein Verfahren spezifiziert, in dem der Passinhaber einen aktiven Part übernehmen muss: Erst indem er sein Dokument an den Grenzbeamten übergibt, erlaubt er das Auslesen der gespeicherten Daten.
Das Basic Access Control-Verfahren setzt die Kenntnis von kryptograischen Schlüsseln voraus, die nur aus den auf der Datenseite des ePasse optisch lesbaren Daten gewonnen werden können. Damit wird sichergestellt, dass einem Terminal ein ePass zur Überprüfung bewusst zur Verfügung gestellt werden muss. Erst das Auslesen der maschinenlesbaren Zeilen ermöglicht dann das Auslesen der auf dem Chip gespeicherten biometrischen Daten.
Ist das Auslesen der biometrischen Daten gelungen, so muss im nächsten Schritt geprüft werden, ob die Daten authentisch und integer sind. Nur so ist zu gewährleisten, dass die Daten von einer autorisierten Stelle personalisiert wurden und dass sie in unveränderter Form vorliegen. Auf dem ePass wird hierzu ein so genanntes Security Object File angelegt, dass zum einen Hash-Werte, also digitale Prüfsummen, der einzelnen Datengruppen enthält, und das darüber hinaus über eine digitale Signatur verfügt. Um zu prüfen, ob die Datengruppen integer sind, werden die Hash-Werte der vom Terminal aus dem ePassausgelesenen Daten erneut berechnet und mit den im ePass abgelegten Hash-Werten verglichen. Die Authentizität der Daten wird durch die Verifikation der digitalen Signatur geprüft. Dabei ist entscheidend, dass nicht nur mit dem öffentlichen Schlüssel der Signierinstanz (PKSIG) geprüft werden muss, ob die Signatur gültig ist. Auch die Authentizität des PKSIG selber muss unbedingt überprüft werden. Das passiert durch die Verifikation des Zertifikats des öffentlichen Schlüssels der Signierinstanz Cert(PKSIG) mit dem öffentlichen Schlüssel der Signierinstanz des jeweiligen Staates PKCSCA. Für das Terminal heißt dies, dass für die Verifikation von ePässen aus unterschiedlichen Ländern der Zugriff auf den jeweiligen PKCSCA nötig ist. Dies macht eine Anbindung des Terminals an eine PKI erforderlich.
Schließlich kommen neben dem Schutz der personenbezogenen Daten auch Aspekte des Datenschutzes ins Spiel. Das kontaktlose Protokoll nach ISO14443, dessen sich die Schnittstelle des ePasses bedient, macht es erforderlich, dass sich der ePass über eine Kennung gegenüber einem Leseterminal identifiziert. Falls ein ePass eine konstante Kennung aussenden würde, wäre es möglich, den ePass und somit seinen Besitzer rückverfolgen zu können. Deswegen wird eine zufällige Kennung verwendet, wie sie für den deutschen ePass umgesetzt wurde und wie sie im Rahmen von formalen Sicherheitszertifizierungen auch gefordert wird.

8.2.2 Biometrie im Bundespersonalausweis

In der aktuellen Diskussion befinden sich Überlegungen die Regelungen für den ePass auch für den Bundespersonalausweis zu adaptieren.
Weitere aktuelle Informationen des Gesetzgebers sind unter nachfolgendem Link zu erhalten:

http://www.bmi.bund.de

9 Standards zur Biometrie

9.1 BioAPI-Consortium

BioAPI – ist ein Industriestandard zur biometrische Authentifizierung an dessen Entwicklung mehr als 90 Firmen in dem Internationalen Gremium BioAPI-Consortium mitwirkten. Bei BioAPI handelt es sich um eine Schnittstellenspezifikation für Biometrie-Anwendungen auf Rechnern mit Erkennungshardware. Das Hauptziel ist die einfache Austauschbarkeit von Biometrien durch Festlegung einer biometrischen Schnittstelle, die in PC-Anwendungen integriert werden sollte, die biometrische Verfahren nutzen wollen. Diese Spezifikation liegt in der Version 1.1 vor und wurde auf Initiative amerikanischer Institutionen als ein Basisdokument in die internationale Standardisierung der Biometrie in den Ausschuss ISO/SC37 eingebracht und wird dort weiter behandelt.

Es wurden beispielsweise Protokolle zu folgenden Operationen spezifiziert:
- BioAPI_Capture: liefert Sensordaten
- BioAPI_CreateTemplate: erzeugt Template aus Sensordaten
- BioAPI_Enroll: erfasst Sensordaten und erzeugt Template
- BioAPI_Verify: erfasst Sensordaten und verifiziert Benutzer durch Vergleich mit gespeicherten bzw. von einer SmartCard importierten Daten; auch eine SmartCard kann als - Vergleichseinheit eingesetzt werden
- BioAPI_Identify: erfasst Sensordaten und identifiziert die betreffende Person durch Vergleich mit einer Datenbank, falls dort schon die biometrischen Daten erfasst waren

9.2 ISO/IEC JTC 1/SC37, DIN-NI37

Zu den Arbeitsschwerpunkten von SC37 gehört die Standardisierung verschiedener Aspekte der Biometrie, so z. B. auch von CBEFF, dem Common Biometric Exchange Formats Framework, und BioAPI, dem Biometric Application Programming Interface, die von den USA in die internationale Normung eingebracht worden sind und für die sich derzeit als Final Draft International Standards in der Abstimmung befinden.
NI-37 spiegelt auf nationaler Ebene das internationale Gremium ISO/IEC JTC 1/SC 37 "Biometrics" (http://www.JTC 1.org/, dann zu Subcommittee 37).
Das internationale Gremium wurde im Dezember 2002 gegründet. Der NI-37 wurde im März 2003 gegründet. Der NI-37 betrachtet die Einbringung der deutschen Interessen in die Internationale Normung als seine Hauptaufgabe. Er richtet deshalb seine Aktivitäten an denen des internationalen Normungsgremiums und seiner Working Groups aus:
WG 1: Harmonised Biometric Vocabulary and Definitions,
WG 2: Biometric Technical Interfaces,
WG 3: Biometric Data Interchange Formats,
WG 4: Profiles for Biometric Applications,
WG 5: Biometric Testing and Reporting,
WG 6: Cross-Jurisdictional and Societal Aspects.

Für die Working Groups von SC 37 gibt es keine nationalen Spiegelgremien. Ihre Tätigkeit wird durch NI-37 abgedeckt, wo informelle Bearbeitergruppen sich speziell den Working Groups widmen, an denen sie besonderes Interesse haben.

9.3 Zertifizierung und Prüfzeichen

Wie alle Systeme der IT-Sicherheit sollten auch biometrische Systeme geprüft werden. Es gibt informelle, semiformale und formale Prüfungen.
Formale Evaluierung 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 Zertifikationsschemas 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 Vertrauenswürdigkeitstufe 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 Tabelle 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 Vertrauenswürdigkeits-komponenten bilden die EAL, von EAL 1 – "funktionell getestet", bis EAL 7 – "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.

Exemplarische "Protection Profiles" zu den CC wurden bisher in Großbritannien bei der Biometrics Working Group unter Mitarbeit von AG6-Mitgliedern erarbeitet.

10 Referenzen / Literatur

10.1 Referenzen

[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 siehe http://www.iid.de/iukdg/gesetz/index.html

[D1] John Daugman (2000), Biometric Decision Landscapes, Technical Report No. TR482, University of Cambridge Computer Laboratory

[ICAO-LDS] ICAO: Technical Report: Development of a logical data structure –LDS, Revision 1.7

[ICAO-PKI] ICAO: PKI for Machine Readable Travel Documents offering ICC Read-Onl Access, Version 1.1

[SigV] Verordnung zur elektronischen Signatur (Signaturverordnung) vom 16. November 2001 (BGBl. 2001 Teil I, Nr. 59)
http://bundesrecht.juris.de/sigv_2001/

[SigG] Signaturgesetz, Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, vom 16. Mai 2001, (BGBl. 2001 Teil I Nr. 22)
http://bundesrecht.juris.de/bundesrecht/

[TAB] TAB-Arbeitsberichte Nr. 76 „Biometrische Identifikationssysteme" und Nr. 93 „Biometrie und Ausweisdokumente“
TAB Büro für Technikfolgenabschätzung beim Deutschen Bundestag,2002 und 2003
http://www.tab.fzk.de/de/arbeitsberichte.htm

[TTT OH Betriebsvereinbarung]
Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme, erarbeitet und hrsg. von der TeleTrusT AG 6

"Biometrische Identifikationsverfahren", Version 1.2. vom 21.09.2005, http://www.teletrust.de

[BWG] Biometric Working Group (Mansfield, T./Wayman, J.): „Best Practices in Testing and Reporting Performance of Biometric Devices", Version 2.01,August 2002, http://www.cesg.gov.uk/technology/biometrics/media/Best%20Practice.pdf (Stand: 17.03.2003)

10.2 Weiterführende Literatur

Weiterführende Literatur ist u.a. auf der Webseite der AG6 des TeleTrust e.V. unter http://www.teletrust.de zu finden.

10.3 Abkürzungsverzeichnis / Glossar

Adaption	(automatische) Anpassung/Aktualisierung der gespeicherten Referenzdaten bei der Benutzung des Systems
Authentifizierung/ Authentifikation	Authentifizierung/Authentifikation bedeutet „Bezeugung 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
BGB	Bürgerliches Gesetzbuch
Biometrischer Sensor	Hardwarekomponente eines biometrischen Systems, die aus der Erfassung eines körperlichen Merkmals biometrische Messdaten liefert (z. B. Fingerabdruck-Sensoren).
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	Eine 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
Chipkarte	Durch ISO-7816 standardisierter Datenträger des Typs ID-1 (Kreditkarten-Format) mit integriertem elektronischen Chip. Die Schnittstelle zum Chip kann mit Kontakten oder kontaktlos gestaltet sein. Chipkarten mit einem Prozessorchip können komplexe Funktionen (z.B. elektronische Signatur, Comparison-On-Card) ausführen; sie werden daher auch Smart Card genannt.
Comparison-On-Card Verfahren	Verfahren, bei dem der Vergleich aktuell erhobener bearbeiteter biometrischer Messwerte mit einer Referenzinformation auf einer Chipkarte stattfindet. Bei Comparison-On-Card braucht die Referenzinformation die Chipkarte nicht zu verlassen. Der Begriff „Comparison-On-Card“ ersetzt nach Vorschlag der ISO den bekannten Begriff „Match-On-Card“
DET	Die Leistungsfähigkeit eines biometrischen Systems in unterschiedlichen Arbeitspunkten kann mit einer DET-Kurve (Detection Error Tradeoff) verdeutlicht werden. Diese Kurve trägt die Fehlerraten FAR und FRR gegeneinander auf und eliminiert damit die Abhängigkeit der Darstellung vom Schwellwert. Die Fehlerraten werden meist logarithmisch skaliert.
EER	Maß für die allgemeine Trennfähigkeit zwischen Originalen und Fälschungen (*equal error rate)*, d.h. die Fehlerrate, bei der *FRR* und *FAR* gleich sind.
Enrolment, Enrollment	Umfasst das erstmalige Erfassen und (Ver-)Messen des biometrischen Merkmals der zukünftigen Nutzer, die Umwandlung und erstmalige Speicherung der so entstandenen Referenzdaten.
FAR	Falschakzeptanzrate (*false acceptance rate*), der (meist prozentuale) Anteil fälschlich zugelassener Unberechtigter
FRR	Falschrückweisungsrate (*false rejection rate*), der (meist prozentuale) Anteil fälschlich zurückgewiesener Berechtigter
Identifikation	Identifikation bedeutet „Feststellung der Identität.“ Bei der Personenidentifikation wird festgestellt, 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 Erkennung auf dem Markt anbietet.
Lebenderkennung	Auch „live check“ oder „liveness test“ genannt. Hierbei handelt es sich um eine Methode, um sicherzustellen, dass tatsächlich auch eine wirkliche, “lebende“ Person geprüft wird. Soll u.a. Angriffe mit Attrappen verhindern.
Match-On-Card-Verfahren	Durch die ISO wird der genauere Begriff "Comparison-On-Card" vorgeschlagen, der die Tatsache besser abbildet, dass nicht jeder Vergleich erfolgreich sein („matchen“) muss.
Messung von biometrischen Daten	Bei der Messung von biometrischen Daten werden die Merkmale des Nutzers entweder durch eine spezielle Hardwarekomponente (z. B. Fingerabdruck-Sensor) oder durch allgemeine IT-Sensoren (z. B. Tastaturen, Kamera) erfasst. Wie alle physikalischen Messungen haben die Messung biometrischer Daten immer einen Messfehler; Da sich biologische Daten in der Regel auch noch ändern, ist nie der gleiche Messwert zu erwarten.
Minutien	die charakteristischen Punkte eines Fingerabdrucks und deren Eigenschaften
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 enrole 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.
ROC	Die Systemleistungsfähigkeit eines biometrischen Systems in unterschiedlichen Arbeitspunkten kann mit einer ROC-Kurve (Receiver Operating Charactristic) verdeutlicht werden. Diese Kurve trägt die Fehlerraten FAR und FRR gegeneinander auf und eliminiert damit die Abhängigkeit der Darstellung vom Schwellwert. Die ROC (Receiver Operating Characteristics) Kurve ist die gespiegelte DET-Kurve, bei welcher anstelle der Fehlerrate FRR die positive Erkennungsrate 1-FRR aufgetragen wird.
Referenzdaten	Von einem Nutzer erfasster und für die Verifikation oder Identifikation gespeicherter Datensatz
Schwellwert	Der Schwellwert eine biometrischen Systems gibt den Mindestgrad an Übereinstimmung zwischen einer biometrischer Messung und den Referenzdaten an, ab dem die gemessene Person als „erkannt“ gilt.
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBl. 2001 Teil I Nr. 22), zuletzt geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 4. Januar 2005 (BGBl. 2005 Teil I Nr. 1).
SigV	Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16. November 2001 (BGBl. 2001 Teil I Nr. 59)
System-On-Card-Verfahren	Verfahren, bei dem die komplette biometrische Erkennung auf einer Chipkarte stattfindet. Beim System-On-Card-Verfahren braucht weder die Referenzinformation die Chipkarte zu verlassen, noch ist die Karte auf Vorberechnungen außerhalb angewiesen.
Template-On-Card-Verfahren	Verfahren, bei dem die Referenzinformation auf einer Chipkarte gespeichert wird. Der Vergleich aktuell erhobener bearbeiteter biometrischer Messwerte mit der Referenzinformation findet außerhalb der Chipkarte statt. Beim Template-On-Card-Verfahren muss also die Referenzinformation die Chipkarte verlassen.
Template	Datensatz, der aus biometrischen Rohdaten extrahiert wird.
Verifikation	Verifikation bedeutet „Bestätigung der Identität.“ Die Personenverifikation entscheidet die Frage, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt.

Spielen Sie mit dem Gedanken erstmals ein biometrisches Verfahren einzusetzen, oder wollen Sie sich über alle Aspekte der biometrischen Verfahren informieren?

Dann ist für Sie dieser "Kriterienkatalog" die richtige Lektüre!

Der "Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren" ist von der TeleTrusT-Arbeitsgruppe 6 "Biometrische Identifikationsverfahren" als Hilfsmittel für die Arbeitsebene potentieller Anwender oder Betreiber von biometrischen Verfahren erstellt worden.
Zuerst werden in dieser Broschüre exemplarisch einige Begriffe und Möglichkeiten der Biometrie erläutert. Dann werden dem potentiellen Anwender/Betreiber Kriterien an die Hand gegeben, die es ihm ermöglichen, biometrische Verfahren zu vergleichen und ein für seine Applikation geeignetes Verfahren auszuwählen.
Desweiteren werden wichtige Anmerkungen zum Datenschutz erläutert sowie auch juristische Aspekte betrachtet.

Diese Bewertungskriterien beschreiben also technische, juristische und anwendungsbezogene Aspekte des Einsatzes biometrischer Verfahren und Systeme.