Biometrie - Was ist das?

- **Beurteilung der Einsatzmöglichkeiten und der Vor- und Nachteile aus Sicht des Anwenders**
- **Klarstellung zu hygienischen und/oder gesundheitlichen Bedenken**

0 Überblick

1 Einleitung 1
2 Personenerkennung bei der Zutrittssteuerung 1
3 Was ist Biometrie und wie funktioniert sie? 2
4 Welche zusätzlichen Informationen stecken hinter biometrischen Rohdaten? 2
5 Einzigartigkeit, Konstanz, Verbreitung 2
6 Welche Arten biometrischer Erkennungsverfahren gibt es überhaupt? 3
6.1 Fingerabdruck 3
6.2 Handgeometrie 3
6.3 Venenmustererkennung der Hand 3
6.4 Iris-Erkennung 3
6.5 Augenhintergrund-Erkennung (Retina-Scan) 4
6.6 Sprachmuster- und Sprechererkennung 4
6.7 Gesichtserkennung 4
7 Objektive Messkriterien: FAR und FRR 4
8 Nah am Ideal 5
9 Fakten zu hygienischen oder gesundheitlichen Bedenken 5
9.1 Fingerabdruck und Handgeometrie 5
9.2 Venenmustererkennung 6
9.3 Augenhintergrund- und Iris-Erkennung 6
9.4 Sprachmuster- und Sprechererkennung 6
9.5 Gesichtserkennung 6
10 Ist Biometrie gefährlich, z.B. wenn in meine Augen geleuchtet wird? 6
11 Ist Biometrie schnell genug für Zutrittssteuerung? 6
12 Wachsende Zahl von Anwendungen 6
13 Zwei wiederkehrende Begriffe: Identifikation versus Verifikation 7
14 Ist der Einsatz von Biometrie in Betrieben zustimmungspflichtig? 7
15 Was hat der Anwender, der Benutzer von Biometrie? 7
16 Fazit 7

1 Einleitung

Biometrie ist in aller Munde. Aber sie schmeckt nicht jedem. Die Biometrie-Entwicklung ist stetig voran geschritten. Meinungen zur Biometrie werden zum Teil noch mit älteren Systemen in Zusammenhang gebracht, die heute keine Bedeutung mehr haben. Aber auch ungenügende Information oder alte Vorbehalte sind anzutreffen. Diese Zusammenfassung stellt die Grundlagen der Biometrie dar, die Verfahren, die wichtigsten objektiven Messwerte sowie Fakten, die es gestatten, hygienische oder gesundheitliche Bedenken beurteilen und ausräumen zu können. Sie bietet eine allgemeine Beurteilung der Einsatzmöglichkeiten und der Vor- und Nachteile aus Sicht des Anwenders. Dazu sind hauptsächlich organisatorische und sicherheitstechnische Anwendungen in Unternehmen, sogenannte „geschlossene“ Anwendungen, betrachtet - nicht aber hoheitliche bzw. „offene“ Anwendungen.

2 Personenerkennung bei der Zutrittssteuerung

Die automatisierte Personenerkennung basiert ganz allgemein und insbesondere bei der Zutrittssteuerung/Zutrittskontrolle auf drei möglichen Konzepten: Der Prüfung des Wissens der Person

(PIN-Code), des Besitzes der Person (Ausweis) und der Eigenschaften der Person (Biometrie). Biometrische Erkennungsverfahren sind das einzige Mittel, um nicht nur einen Ausweis, sondern auch den zugehörigen Besitzer zu erkennen sowie den falschen Benutzer abzuweisen. Für flächendeckende oder landesweite Standardsituationen ist Biometrie heute in der Investitionshöhe und im erzielbaren Durchsatz (Begehungen pro Zeiteinheit) zu aufwändig. Der Markt ist jedoch auf Anbieter- und Anwenderseite in einem gravierenden technischen und psychologischen Umschwung begriffen. Vorbehalte sind weitgehend entkräftet, Kosten nachhaltig gesunken. Ein weiterer Kostenrückgang ist zu erwarten.

3 Was ist Biometrie und wie funktioniert sie?

Biometrische Erkennungsverfahren, häufig kurz mit "Biometrie" bezeichnet, sind Verfahren, die eine Person anhand physiologischer Charakteristika (z. B. Fingerabdruck, Gesicht, Muster der Iris) oder Verhaltensweisen (z. B. Stimme, Bewegung, Unterschrift) automatisiert erkennen. Dazu wird der Teilbereich des menschlichen Körpers „vermessen“, der für das angewandte biometrische Verfahren benötigt wird. Bei der erstmaligen Benutzung, dem sogenannten Enrollment, werden die Kennwerte jedes Teilnehmers gespeichert - vergleichbar mit der Ausstellung eines Ausweises. Dieser Datensatz, das „Template, enthält nur die für den Erkennungsalgorithmus benötigten Informationen, die aus den ursprünglich erfassten Rohdaten ermittelt wurden. Bei der weiteren Benutzung werden die aktuell aufgenommenen Messwerte mit diesem gespeicherten Datensatz verglichen, wie bei einer Passkontrolle.
Der gespeicherte Datensatz ist also meist keine Bild- oder Tondatei. Er enthält keine "Rohdaten" wie ein Passbild, ein kriminalistischer Fingerabdruck oder eine Sprachaufnahme, sondern nur die daraus extrahierten Merkmale, z.B. eine mathematische Beschreibung der Endungen und Verzweigungen der Fingerabdrucklinien beim Fingerprint oder des Iris-Musters bei der Iris-Erkennung.

4 Welche zusätzlichen Informationen stecken hinter biometrischen Rohdaten?

Aus den Rohdaten lassen sich einige Rückschlüsse ziehen, insbesondere aus einem Bild des Gesichts, z.B. auf das Geschlecht, das ungefähre Alter oder die Hautfarbe einer Person. Aber auch aus dem Bild des Augenhintergrundes, der Retina, sind grundsätzlich Rückschlüsse auf Krankheiten wie Diabetes oder Bluthochdruck möglich. Auch Fingerabdrücke erlauben eine ungefähre Schätzung des Alters. Welche Rückschlüsse noch möglich sind, ob sie automatisiert gezogen werden können und ob auch Templates diese "Zusatzinformationen" enthalten könnten, ist noch nicht hinreichend erforscht. Jedoch enthalten „Templates“ nach heutigem Wissensstand keine überschüssigen Daten. Solche Sekundär-Kriterien sind evtl. theoretisch denkbar, aber zweifellos nicht primäres Ziel bei der Zutrittskontrolle. Im Zweifelsfall ist die Nutzung der Sekundär-Kriterien im Rahmen einer Betriebsvereinbarung auszuschließen.

5 Einzigartigkeit, Konstanz, Verbreitung

Biometrische Erkennungsverfahren nutzen entweder statische, also physiologische Merkmale oder dynamische, also verhaltensbedingte Merkmale. Biologische Eigenschaften, die als biometrische Merkmale heranzuziehen sind, müssen die Attribute Einzigartigkeit, Konstanz und Verbreitung aufweisen. Die Einzigartigkeit ist bei einer hinreichend großen Varianz des Merkmals bei einzelnen Individuen gewährleistet. Die Konstanz legt eine möglichst geringe Änderung des Merkmals beim einzelnen Individuum im Laufe der Zeit zu Grunde. Die Verbreitung schließt vorhandene und messbare oder abnehmbare Merkmale bei möglichst allen Individuen ein. Für eine biometrische Erkennung müssen die drei genannten Attribute erfüllt sein. In der biometrischen Identifikation oder Verifikation werden einzigartige Merkmale einer Person über statische (physiologische) oder dynamische (verhaltensbedingte) Verfahren erfasst. Bei den statischen Verfahren sind heute Fingerabdruck, Handgeometrie, Iris und Gesicht zur Grundlage der Bemessung geworden, bei den dynamischen Verfahren werden Unterschrift und Sprachmuster oder das Sprachfrequenzspektrum herangezogen. Die Erfassung erfolgt über entsprechende Sensoren.

6 Welche Arten biometrischer Erkennungsverfahren gibt es überhaupt?

Aufgrund der Vielzahl verschiedener Arten biometrischer Merkmale sind unterschiedliche, teilweise sehr aufwändige Verfahren zur zuverlässigen Erkennung nötig. Häufig sind sie speicher- und rechenintensiv. Viele Verfahren hatten zunächst mit Akzeptanzproblemen zu kämpfen, da sie aus psychologischen (gedankliche Nähe zur Kriminalistik beim Fingerabdruck), hygienischen (Handgeometrie) oder gesundheitlichen Gründen (Retina/Iriserkennung) abgelehnt wurden. Ein Großteil dieser Bedenken konnte durch Untersuchungsergebnisse entkräftet werden. Heute sind besonders die Erkennung der Handgeometrie und des Gesichts beliebt. Ähnliche Akzeptanz ist in letzter Zeit für die Fingerprinterkennung zu beobachten, die durch den Einsatz auch im neuen deutschen Reisepass starken Auftrieb erhalten hat.

6.1 Fingerabdruck

Für die Fingerabdruckerkennung ist der Markt in starker Bewegung. So stellt unter anderem die Anwendung von CCD-Halbleitern und Glasfaseroptiken neue und preisgünstige Sensoren in Aussicht.
Bei den meisten biometrischen Fingerabdruck-Verfahren extrahiert der Fingerabdruck-Algorithmus die Minutien aus dem durch den Sensor gewonnenen Bild. Die Minutien, die Kennpunkte des Fingerabdrucks, bestehen aus Endungen und Verzweigungen der Papillarlinien. Zur Zeit arbeiten Unternehmen an Verfahren, die eine Komprimierung der Kenndaten auf rund 256 Bytes ermöglichen, da dann das Fingerabdruckprofil auch auf Ausweisen mit relativ kleiner Speicherkapazität mobil aufzubringen ist. Der Fingerprint macht momentan rund 40 Prozent biometrischer Anwendungen aus. Dieser hohe Anteil rührt vor allem daher, dass dieses Verfahren schon seit Jahrzehnten vor allem in der Kriminalistik zum Einsatz kommt.

6.2 Handgeometrie

Bei der Handgeometrie werden im Finger- und Handknöchelbereich über 90 Messpunkte erfasst und nach einem Hersteller-Algorithmus zueinander in Relation gesetzt. Die Kennwerte lassen sich bei ausreichend hoher Erkennungssicherheit auf weniger als 10 Bytes abspeichern. Die Vermessung der Handgeometrie wird vor allem in den USA und in Kanada auf Flughäfen, in Behörden und an Universitäten eingesetzt. Eine breitere Öffentlichkeit hat das Verfahren mit dem Einsatz bei den Olympischen Spielen 1996 in Atlanta erreicht. Ähnliche Anwendungsgebiete sind in Europa im Gespräch. Die Handgeometrie ist mit einem weltweiten Biometrie-Marktanteil von rund 20 % eine technisch ausgereifte und akzeptierte Lösung.

6.3 Venenmustererkennung der Hand

Das menschliche Handflächen-Venenmuster ist komplex, weist viele Gefäße auf und ist für jedes Individuum einzigartig. Das Verfahren von mehreren Anbietern basiert auf der IR-Absorption. Nah-IR-Leuchtdioden beleuchten die Handfläche - eine Kamera erstellt das Raw-Image des Handflächen-Venenmusters. Das Bild entsteht dadurch, dass zum Herz zurückfließendes sauerstoffreduziertes Blut einen Teil der IR-Strahlung absorbiert. Ähnlich dem Fingerprintverfahren wandelt die Template-Software das Raw-Image in ein Template um. Die Venenmustererkennung arbeitet schnell, ohne physischen Kontakt der Handfläche mit dem Sensor und ist bei jedem Menschen anwendbar, da die Gefäßpositionen zeitlebens unverändert bleiben. Eine wachsende Bedeutung dieses Verfahrens ist deshalb denkbar.

6.4 Iris-Erkennung

Die Iris, auch Regenbogenhaut, ist die durch Pigmente gefärbte Blende des Auges. Die Iris reguliert den Lichteinfall in das Auge (Adaptation). In der Iris bilden sich kurz vor der Geburt typische individuelle Muster. Sie sind nach heutigem Wissensstand nicht genetisch bedingt, behalten aber ihre Ausprägung lebenslang. Diese Muster, nicht aber die Farbe, werden zur Erkennung herangezogen. Das Verfahren scheint eine strenge Grenze zwischen Akzeptanz und Rückweisung zu besitzen. Für

die Ausleuchtung des Auges gilt das gleiche wie bei der Retinaerkennung, jedoch ist die Beleuchtungsstärke nochmals erheblich niedriger. Zur Zeit liegt der Anteil der Iris-Erkennung, bezogen auf alle biometrischen Verfahren, bei rund acht Prozent.

6.5 Augenhintergrund-Erkennung (Retina-Scan)

Für die Augenhintergrunderkennung gibt es mehrere Systeme am Markt. Die psychologische Hemmschwelle der Nutzer in Bezug auf Akzeptanz scheint noch nicht ausgeräumt zu sein. Bei Nutzern besteht die Befürchtung, dass zur Ausleuchtung des Auges ein Laserstrahl verwendet wird. Dies verbinden die meisten mit einer potenziellen Verletzungsgefahr des Augenlichts. Nach Herstellerangaben trifft dieses jedoch definitiv nicht zu. Die Augenhintergrund-Erkennung hat in der EU kaum Bedeutung.

6.6 Sprachmuster- und Sprechererkennung

Bei der Sprachmustererkennung gibt es widersprüchliche Aussagen über die praktischen Erfahrungen. Bei einigen Systemen wirken sich die Umgebungsgeräusche störend aus. Nötige Wiederholungen des Erkennungswortes stören wiederum den Benutzer. Bei umfassenden Neuentwicklungen ist die Spracherkennung im Verbund mit anderen biometrischen Erkennungsverfahren kombiniert. Diese Form der Biometrie ist vor allem beim Online-Banking weit verbreitet, bei Zutrittskontroll-Anlagen weniger gebräuchlich.

6.7 Gesichtserkennung

Diese Art der Erkennung ist mittlerweile mit vertretbarem maschinellem Aufwand möglich. Das Verfahren zeigt gute Ergebnisse und ist am wenigsten aufdringlich. Der Nutzer stellt sich gut sichtbar vor das Terminal, ohne die gewohnten Bewegungsabläufe verändern zu müssen. Zwischen Benutzer und Gerät ist kein Kontakt nötig – ein nicht zu unterschätzender Vorzug. Die Gesichtserkennung hält rund zwölf Prozent am Gesamtmarkt biometrischer Erkennung. Die Tendenz ist stark steigend.

Innerhalb der Gesichtserkennung ist zwischen der Muster- und der Geometrieerkennung zu unterscheiden. Im Falle des Geometrie-Verfahrens bilden beispielsweise die Abstände von Augen, Nase und Mund die Basis des Vergleichs. Zudem dienen mehrere unterschiedliche Algorithmen zur Gewinnung der individuellen Merkmale und zur Berechnung der Templates. Die neuesten kombinierten Verfahren suchen aus Videobildern die Gesichtsgeometrie aus. Anschließend vergleicht das System die Aufnahme mit hinterlegten Referenzbildern und wertet über Mustererkennung die Vergleiche aus. Damit soll vor allem auf schlecht zu überblickenden öffentlichen Plätzen mehr Sicherheit erreicht und Täter umgehend erkannt werden. Neue Verfahren erlauben eine 3-dimensionale Erkennung des Gesichts, die mehr Toleranz bei der Aufnahme und höhere Erkennungssicherheit bieten.

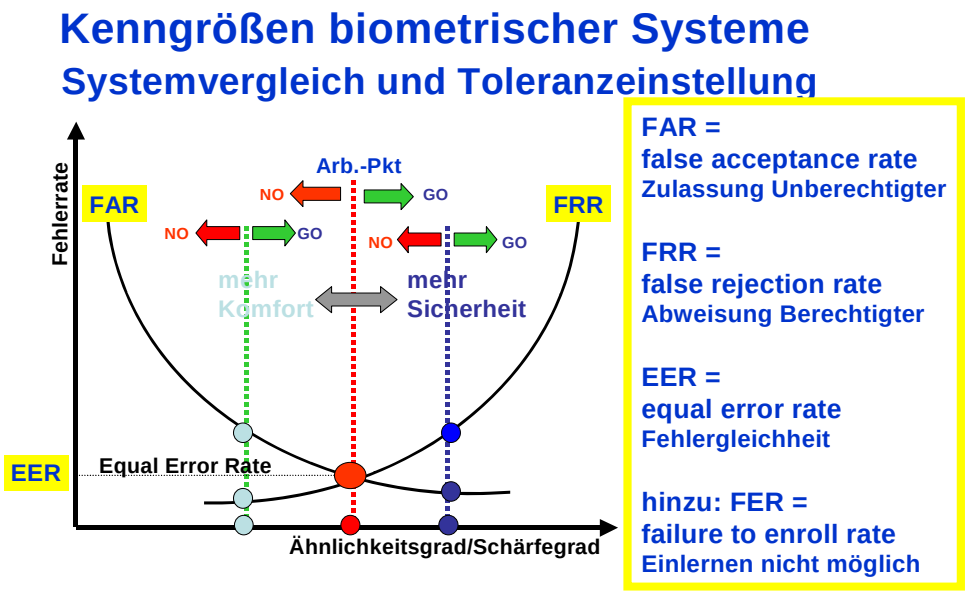
7 Objektive Messkriterien: FAR und FRR

Bei den biometrischen Verfahren wird die Sicherheit nach drei Kriterien beurteilt:

- nach der Rate der Zulassung Unberechtigter (FAR – false acceptance ratio)
- nach der Rate der Abweisung Berechtigter (FRR – false rejection ratio)
- nach der Rate der nicht einlernbaren Personen (FER – failure to enroll)

Im Fall des Kriteriums Abweisung Berechtigter ist der Komfort bei der Benutzung des Systems beeinträchtigt, es entsteht jedoch kein Sicherheitsrisiko. Beim Kriterium Zulassung Unberechtigter, lassen sich Voraussetzungen schaffen, die durchaus die Sicherheit beeinflussen. In Hochsicherheitsbereichen ist deshalb die FAR zu Ungunsten der FRR so niedrig wie möglich eingestellt. In anderen Anwendungen, bei denen es primär auf eine hohe Durchlassrate oder schnellen Eintritt ankommt, ist die FRR möglichst niedrig gehalten. Dabei wird gerne eine etwas erhöhte FAR in Kauf genommen. Die Genauigkeit dieser Abtastung ist entscheidend abhängig von der Wiederholgenauigkeit der Positionierung bei der Messwerterfassung. Bei biometrischen Verfahren soll sie nach Norm EN 50133-1 Pkt. 5.2.6 mit FAR kleiner/gleich 0.01% und FRR kleiner/gleich 1% besonders niedrig sein. Die FER

gibt an, mit welchem Prozentsatz nicht einlernbarer Personen man bei diesem biometrischen Erkennungssystem rechnen muss. Liegt die Rate relativ hoch, ist nicht nur eine geeignete fallback-Massnahme vorzusehen, man muss vielmehr im späteren Echtzeitbetrieb auch mit einer erhöhten FRR rechnen.



8 Nah am Ideal

Systemgebunden oder durch die vom Entwickler gewählten Algorithmen und Bewertungskoeffizienten ist bei einem spezifischen Biometriesystem der Wert EER (equal error rate - Gleichheit der Fehlerraten) definiert. Dieser Wert entspricht dem Schnittpunkt der beiden Kurven FAR und FRR. Je niedriger der Wert EER ist, umso besser unterscheidet das System zwischen Berechtigten und Nichtberechtigten. Mit der Einstellung des Arbeitspunktes, der entweder als Schärfegrad oder Toleranz des Systems (das bedeutet eine umgekehrte Darstellung von FAR und FRR) systemweit und meist zusätzlich auch noch individuell eingestellt werden kann, wird das System auf höhere Sicherheit oder auf höheren Komfort eingestellt. Das nur theoretisch erreichbare Idealsystem hätte einen EER = 0 und damit auch FAR = FRR = 0.

9 Fakten zu hygienischen oder gesundheitlichen Bedenken

Manche Menschen halten biometrische Systeme für nicht hygienisch. Für die hauptsächlich eingesetzten Systeme gilt aus technisch-hygienischer Sicht:

9.1 Fingerabdruck und Handgeometrie

Bei beiden Verfahren erfolgt für alle Teilnehmer eine direkte Berührung eines Gegenstandes. Im Falle des Fingerabdruckes ist ein Kunststoff- oder Glasträger mit dem Finger zu berühren. Bei der Handgeometrie ist die Hand auf eine Platte zwischen Bezugspunkte zu legen. Diese Platte wird vom Hersteller neuerdings aseptisch produziert. Bei beiden Verfahren findet ein Kontakt mit i.d.R. einem einzigen Finger bzw. einer Handfläche statt, der weniger intensiv ist als die Berührung eines Türgriffs, Türknaufs oder einer Türstange und der im Allgemeinen als zumutbar empfunden wird.

9.2 Venenmustererkennung

Dieses Verfahren arbeitet optisch und ohne Berührung des Sensors, da die Hand in einigem Abstand vor den IR-Sensor gehalten wird.

9.3 Augenhintergrund- und Iris-Erkennung

Beide Verfahren arbeiten optisch und berührungsfrei.

9.4 Sprachmuster- und Sprechererkennung

Auch diese Verfahren arbeiten berührungsfrei, indem ein Mikrofon/Schallaufnehmer besprochen wird.

9.5 Gesichtserkennung

Bei der Gesichtserkennung wird eine Kamera verwendet – ein berührungsfreies Verfahren.

10 Ist Biometrie gefährlich, z.B. wenn in meine Augen geleuchtet wird?

Bis auf die kaum eingesetzten Retina-Erkennungssysteme, bei denen der Augenhintergrund mit einer Lampe geringer Intensität beleuchtet wird, werden bei biometrischen Systemen mit Kameras höchstens allgemeine Beleuchtungsquellen wie Lampen oder LEDs eingesetzt, die die Iris oder das Gesicht erhellen. Theoretisch kann es - wie bei jedem Gerät - zu Fehlfunktionen kommen; eine spezifische Gefahr gibt es nicht. Laser werden nach heutigem Wissensstand nicht zur Ausleuchtung biometrischer Merkmale eingesetzt. Die auf einigen Geräten genannte Einstufung in eine „Laserklasse“ wird für alle Geräte mit optischer Ausleuchtung gefordert.

11 Ist Biometrie schnell genug für Zutrittssteuerung?

Bei biometrischen Systemen spielt die Erkennungszeit eine entscheidende Rolle. Da sie meist höher ist als die Buchungszeit, die mit einem herkömmlichen Ausweis erreicht wird, ist generell der verringerte Durchsatz pro Zutrittspunkt zu beachten. In jedem Fall darf die Erkennungszeit die Geduld der Buchenden nicht überstrapazieren, denn die Akzeptanz eines Systems ist wesentlich von seinem Bedienungs- und Benutzungskomfort abhängig. Moderne biometrische Systeme bieten Erkennungszeiten von wenigen Sekunden, was als zumutbar akzeptiert wird.

12 Wachsende Zahl von Anwendungen

Aufgrund dieser Entwicklung erobern biometrische Erkennungsverfahren neue Märkte – vor allem dort, wo sich Verbesserungen durch die Anwendung biometrischer Verfahren abzeichnen. Biometrie stellt je nach Einsatzbereich eine sinnvolle Ergänzung zu den auf Wissen und Besitz basierenden Verfahren dar. Die sichere Identifikation über ausschließliche biometrische Verfahren ist beim heutigen Stand der Technik nur mit kleinen Teilnehmerzahlen möglich, mit Ausnahme der Iriserkennung und teilweise der 3D-Gesichtserkennung. Dadurch eignet sich die Identifikation nur eingeschränkt oder in Kombination mit Zutrittssteuerungskomponenten zur Sicherung der Außenhaut eines Gebäudekomplexes. Bei größeren Teilnehmerzahlen und bei höherem Sicherheitsbedarf werden biometrische Erkennungsverfahren zur Verifikation oder Authentifikation genutzt. Eine vorgeschaltete Identifikation erfolgt dabei über PIN-Code oder die Überprüfung einer Ausweiskarte durch ein Zutrittsterminal. Mit den zu erwartenden technischen Verbesserungen und vor allen Dingen den nachfolgenden Kostensenkungen sind biometrische Lösungen künftig auch für Anwendungen in alltäglichen Sicherungsbereichen möglich. Auch innerhalb von administrativen Applikationen wie der Zeiterfassung ist eine steigende Bedeutung der Biometrie zu erwarten.

13 Zwei wiederkehrende Begriffe: Identifikation versus Verifikation

Die Identifikation prüft in einem so genannten „one-to-many-Vergleich“ die Identität der betreffenden Person. Damit beantwortet sie die sicherheitsrelevante Frage „Wer bin ich?“ Ein zusätzlicher Ausweis oder eine PIN sind nicht erforderlich.
Innerhalb der Verifikation (Authentifikation) bestätigt das System über einen one-to-one-Vergleich die Identität des Benutzers. Die Frage: „Bin ich tatsächlich der Besitzer dieser Identität?“ lässt sich auf diese Weise beantworten. Die zu prüfende Identität ist auf einem Ausweis oder durch eine PIN abgebildet, dessen Zugehörigkeit zu dem Ausweisinhaber ermittelt wird. Die in Europa bisher fast nur in Hochsicherheitsanlagen installierten biometrischen Erkennungsverfahren werden vor allem zur Verifikation eingesetzt. Selbst bei der in Nordamerika verbreiteten Sprechererkennung am Telefon in Homebanking-Anwendungen findet eine Verifikation statt, da die (Vor)identifikation über die Nennung der Kontonummer erfolgt.
Nach heutigem Stand der Technik ist es sinnvoll, die biometrische Erkennung zur Verifikation und nicht ausschließlich als Identifikation zu nutzen. Innerhalb der Zutrittssteuerung lässt sich so nicht nur die Unterscheidung der Berechtigten untereinander, sondern auch die sichere Abweisung der riesigen Zahl der Nichtberechtigten sicherstellen. Zu beachten ist, dass es bei der Identifikation ab einer Teilnehmergröße von ca. 500 Personen aufgrund der Anzahl der Vergleiche zu verlängerten Reaktionszeiten kommen kann. Die Identifikation ist somit zeitintensiver und birgt zudem eine Fehler-Multiplikation in sich, da die Fehlerraten pro Vergleich angegeben sind.

14 Ist der Einsatz von Biometrie in Betrieben zustimmungspflichtig?

Zustimmungspflichtig sind Anlagen und Verfahren, die es erlauben, automatisch bzw. maschinell Rückschlüsse auf die Leistung oder auf das Verhalten der Arbeitnehmer zu ziehen.
Biometrie als solche lässt sicher keine Rückschlüsse zu, aber sie wird zur Erkennung der Teilnehmer z.B. einer Zutrittsanlage eingesetzt. Daher ist ihr Einsatz im Rahmen der Zustimmungspflicht zur Zutrittskontrolle ebenfalls zustimmungspflichtig. Hierzu ist bei einer bereits vorhandenen Zutrittsanlage ein Zusatz zum Zustimmungsvertrag der ZK zu erstellen, in der die Erweiterung auf biometrische Erkennungsverfahren vereinbart wird. Diese Zustimmung wird mit der Arbeitnehmervertretung und nicht mit jedem einzelnen Arbeitnehmer herbeigeführt.

15 Was hat der Anwender, der Benutzer von Biometrie?

Eine gut und zügig funktionierende biometrische Zutrittssteuerung wird nach Anwenderuntersuchungen als modern und angenehm empfunden. Hauptargument ist, dass auf den Mitarbeiterausweis, je nach der angewandten Sicherheits-Philosophie, verzichtet werden kann. Somit benötigt der Mitarbeiter während seiner Tätigkeit im Betrieb keinen Ausweis - ein Vorteil nicht nur bei tätigkeitsbedingtem Kleiderwechsel. Biometrische Verfahren erkennen ja den Mitarbeiter persönlich - und nicht nur seinen Ausweis. Diese maschinelle Erkennung entbehrt nicht einer gewissen positiven Magie, der man sich auch nach längerer Benutzung nicht ganz entziehen kann. Biometrie erhöht die Sicherheit, da Manipulation z.B. durch die unerlaubte Weitergabe eines Firmenausweises an eine nicht berechtigte Person oder die unrechtmäßige Benutzung durch den Finder einer verloren gegangenen Karte entfällt.

16 Fazit

Biometrie hat angesichts der bisher gewonnenen Erkenntnisse Zukunft. Biometrie erhöht nicht nur deutlich die Sicherheit in einem Betrieb und die Sicherheit des Einzelnen, sondern bietet dem Nutzer auch eine Erhöhung des Komforts im Vergleich zu bisherigen Identifikationssystemen. Für die objektive Aufklärung und Information über solche Systeme können Hersteller und Anwender nie genug tun.