Arbeitszeiterfassung mit Fingerabdruck

Was ist Biometrie?

Unter Biometrie, im Zusammenhang mit einer Personenidentifikation, versteht man die Erkennung von Personen anhand von einzigartigen und unverwechselbaren biometrischen Merkmalen. Diese Merkmale sind unmittelbar an den Körper der Person gebunden und müssen nicht erst zusätzlich zugeordnet werden. Zu den biometrischen Verfahren, die mit passiven physiologischen Merkmalen arbeiten und zur Personenidentifikation eingesetzt werden, gehören:

- Fingerabdruckerkennung
- Gesichtserkennung
- Iriserkennung
- Venenerkennung
- Handgeometrie

Warum Biometrie?

Biometrische Merkmale sind bezogen auf den Benutzer einzigartig und eindeutig. An ein biometrisches Merkmal muss sich der Benutzer nicht erinnern, er kann es weder vergessen, noch verlieren, sondern trägt es ständig bei sich. Körperliche Merkmale können nicht wie ein Passwort oder Karte einfach weitergegeben und missbräuchlich verwendet werden.

Deshalb bietet sich die Biometrie als Alternative oder Ergänzung zu herkömmlichen Methoden, wie Karte oder PIN/Passwort zum Einsatz in Zeiterfassungssystemen und Zutrittskontrollsystemen an.

Warum Fingerabdruckerkennung?

Von allen biometrischen Verfahren hat in den letzten Jahren weltweit die Erkennung anhand des Fingerabdruckes die weitaus größte Verbreitung erfahren. Die Fingerabdruckerkennung hat einen Anteil von 40% an den verwendeten biometrischen Verfahren. Deshalb existieren mit der Fingerabdruckerkennung auch die umfangreichsten praktischen Erfahrungen.

In einer 2005 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführten umfangreichen Studie zur Leistungsfähigkeit verschiedener biometrischer Systeme, erzielten Fingerabdrucksysteme mit optischen Sensoren die besten Ergebnisse (noch vor Iriserkennung und Gesichtserkennung). Es wurde bescheinigt, dass die Fingerabdruckerkennung auch für sehr hohe Sicherheitsanforderungen geeignet ist.

Fingerabdrucksysteme weisen bezüglich der Anschaffungskosten gegenüber allen anderen Systemen deutliche Vorteile auf.

Grundlagen der Fingerabdruckerkennung

Die Einzigartigkeit des Fingerabdruckes (Es existieren keine zwei Menschen mit gleichem Fingerabdruck, selbst eineiige Zwillinge mit genetisch identischer DNA weisen unterschiedliche Fingerabdrücke auf) lassen ihn als ideal geeignet erscheinen zur Verwendung in automatisierten Erkennungssystemen. Für die automatisierte Erkennung werden die Fingerabdruck-Feinmerkmale, die so genannten Minuzien verwendet. Diese ergeben sich aus dem Vorhandensein von Verzweigungen und Endungen in der Fingerlinienstruktur. Die Anordnung dieser punktförmig definierten Merkmale ergibt ein ganz spezifisches Bild, das ebenfalls einmalig ist und sich maschinell auswerten lässt. Die Anordnung dieser Minuzien, ihre relative Lage zueinander und ihre Richtung, ist hauptsächlich zufällig und nicht vererbbar.

Der Ablauf der biometrischen Identifizierung ist bei allen biometrischen Systemen unabhängig vom verwendeten Verfahren prinzipiell gleich:

- Registrierung des Nutzers im System (Enrollment) durch Erfassung der biometrisch relevanten Eigenschaften dieser Person und Erstellung und Speicherung eines Datensatzes(Template)
- Erfassung der biometrisch relevanten Eigenschaften einer Person, Erstellung eines Datensatzes (Templates) und Vergleich der aktuell präsentierten mit den zuvorabgespeicherten Daten (Matching).

Zur Erfassung einer Person in einem biometrischen System wird beim Enrollment vom Fingerabdruck zunächst ein Bild erzeugt. Mittels eines speziellen Algorithmus, der bei jedem Hersteller unterschiedlich ist, wird dieses in einen Datensatz, das Template, umgewandelt und gespeichert. Es ist nicht möglich aus diesem extrahierten Datensatz auf dem umgekehrten Wege wieder einen Fingerabdruck zu generieren!

Beim Matching wird ein Vergleich zwischen dem gespeicherten Template und dem Datensatz, der bei einer erneuten Präsentation gewonnen wurde, durchgeführt. Wird eine hinreichende Übereinstimmung festgestellt, erkennt das System den Benutzer.

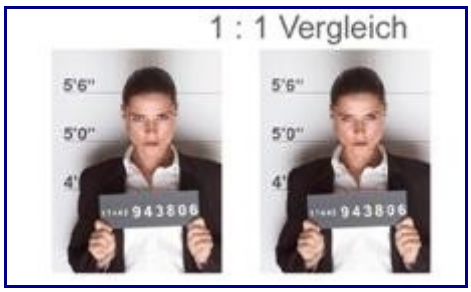
Identifikation und Verifikation

Bei der Verwendung biometrischer Systeme zur Authentifizierung von Personen stößt man immer wieder auf die Begriffe **Identifikation** und **Verifikation**. Ziel einer biometrischen Erkennung ist stets, die Identität einer Person zu ermitteln (Identifikation) oder eine behauptete Identität zu bestätigen bzw. zu widerlegen (Verifikation).

Identifikation (1:n Vergleich)

Bei einer Identifikation wird ein biometrisches Merkmal mit allen im System gespeicherten Referenzmerkmalen verglichen (1:n Vergleich). Gibt es eine Übereinstimmung, ist die Identifikation erfolgreich und die zum betreffenden Referenzmerkmal gehörende User-ID lässt sich weiterverarbeiten.

Verifikation (1:1 Vergleich)



Bei einer Verifikation gibt der Nutzer dem System seine Identität vorab bekannt (z. B. über eine PIN oder Karte), das System muss das biometrische Merkmal dann nur noch mit einem zur User-ID passenden Referenzmerkmal (1:1 Vergleich) vergleichen. Im Übereinstimmungsfall ist die Verifikation erfolgreich.

Wie effektiv sind biometrische Systeme?

Die Erfassung und Auswertung biometrischer Merkmale ist naturgemäß mit Messfehlern behaftet, da sich die verwendeten Merkmale sowohl im Laufe der Zeit als auch temporär durch äußere Einflüsse ändern und auch die Präsentation gegenüber dem System niemals gleich erfolgt. Die zu unterschiedlichen Zeitpunkten erzeugten digitalen Abbilder des gleichen biometrischen Merkmals können also nicht zu 100% identisch sein. Es erfolgt also beim Matching deshalb keine Überprüfung auf Gleichheit sondern auf hinreichende Ähnlichkeit.

Für die Effektivität und Sicherheit biometrischer Systeme existieren zwei allgemein anerkannte Messgrößen:

- die Falsch-Zurückweisungsrate (FRR)
- die Falschakzeptanzrate (FAR)

Falsch-Zurückweisungsrate (FRR)

Die FRR ist die Häufigkeit (ausgedrückt als prozentualer Anteil), mit der berechtigte Personen unberechtigterweise zurückgewiesen werden. Die FRR ist in der Regel ein Komfortmerkmal, da falsche Abweisungen vor allem lästig sind, aber die Sicherheit nicht beeinträchtigen. Der typische Wert für unsere Systeme liegt bei weniger als 1%.

Falschakzeptanzrate (FAR)

Die FAR ist die Häufigkeit (ausgedrückt als prozentualer Anteil), mit der nicht berechtigte Personen als berechtigt akzeptiert werden. Da eine falsche Akzeptanz in der Regel zu Schäden führt, ist die FAR ein sicherheitsrelevantes Maß. Die FAR wird allgemein als wichtigstes Kriterium für die Qualität einer Biometrielösung angesehen. Der typische Wert für unsere Systeme liegt bei 0,0001%.

Beide Werte können oftmals durch Änderung der Toleranzschwellen innerhalb des Systems beeinflusst werden, stehen jedoch immer in direkter Abhängigkeit zueinander: eine Verringerung der FAR führt unmittelbar zu einer Erhöhung der FRR und umgekehrt.

Hinweise zur Verwendung biometrischer Verfahren im Unternehmen

Folgende Beispiele können in die Diskussion einbezogen werden:

- Eine Person (Pförtner) ist beauftragt, die Mitarbeiter beim Betreten des Firmengeländes anhand von elektronisch gespeicherten Lichtbildern zu identifizieren.
- Unterschriften der Mitarbeiter werden auf Arbeitsverträgen, Arbeitsanweisungen etc. archiviert und damit „gespeichert“.
- Fingerabdrucksensoren in Autos zum Zweck des Diebstahlschutzes gewinnen an Interesse privater Verbraucher.
- Fingerabdrucksensoren an Notebooks werden immer populärer zum Schutz persönlicher Daten und zum Schutz von Kindern und Jugendlichen vor jugendgefährdenden Inhalten.

Entscheidend ist die **Zweck gebundene Verwendung** der biometrischen Daten, nämlich zur Erfassung der Arbeitsstunden und zur Sicherung eines reibungslosen, für den Arbeitnehmer und Arbeitgeber sicheren Ablauf dieser Erfassung. Stundenzettel, die eigenhändig von den Mitarbeitern unterschrieben werden, kommen dieser Art der Erfassung gleich. Der Mitarbeiter leistet bei jeder Identifikation seine Unterschrift, dass er die Arbeit beginnt oder beendet. Die Vorteile der elektronischen Erfassung für Arbeitnehmer und Arbeitgeber sollen hierbei nicht weiter erläutert werden.

Grundsätzlich raten wir Ihnen zu folgenden Maßnahmen:

Schaffen Sie Vertrauen. Geben Sie Ihren Mitarbeitern **so viele Informationen wie nur möglich**. Sorgen Sie für Transparenz, wie mit den persönlichen Daten im Unternehmen verfahren wird. Verfassen Sie z.B. eine Datenschutzerklärung, unterzeichnet von der Geschäftsführung, worin die Speicherung sämtlicher persönlichen Daten geregelt ist. Das betrifft u.a. auch die Speicherung von Adressdaten, Geburtsdaten, Lichtbildern, Unterschriften und eben biometrischer Merkmale.

Als Arbeitgeber sind Sie verpflichtet, für den Datenschutz persönlicher Daten Sorge zu tragen. Dieser Forderung kommen Sie bei der Verwendung von Zeiterfassungsterminals der Serie NTB 960 und 980 nach, da die Art der Speicherung keine Reproduzierbarkeit des Fingerabdrucks ermöglicht. Wir verweisen hierbei auf die oben beschriebenen technischen Spezifikationen der Speicherung des Fingerabdrucks in diesen Zeiterfassungsterminals.