

## Zeit und Zutritt

Die technische Entwicklung bietet heute eine große Auswahl moderner Zutrittskontrollmöglichkeiten. Identifikationsmerkmale lassen sich auf Chipkarten oder Transponder speichern. Am sichersten ist jedoch die Identifikation unverwechselbarer Merkmale am Mitarbeiter selbst.



# Mit Chipkarte und Fingerprint Mitarbeiter identifizieren

In den letzten Jahren hat sich zur Identifizierung der Mitarbeiter bei vielen kartengesteuerten Anwendungen die Nutzung von kontaktlosen Chipkarten oder Transpondern durchgesetzt. Zur Erhöhung der Sicherheit, etwa für die Zutrittskontrolle in Hochsicherheitsbereichen, kann auch ein biometrisches Verfahren zur Personenidentifikation, wie der Fingerprint, eingesetzt werden.

### Zwei Varianten der Identifikation

Zur Überprüfung der Identität einer Person können unterschiedliche Merkmale verwendet werden, die entweder als direkte Information oder über einen Identträger zur Verfügung stehen. Ein Identifikationsmerkmal ist eine mit technischen Mitteln auswertbare Information. Dies können die persönliche Identifikationsnummer (PIN), die auf einer Chipkarte gespeicherte Ausweisnummer und personenspezifische Kennzeichen (biometrische Merkmale) sein, die gegebenenfalls auf einem Identträger codiert sind und eine eindeutige Personenidentifizierung erlauben.

Bei biometrischen Systemen kann die Identitätsüberprüfung einer Person in zwei Varianten erfolgen:

- **Identifikation:** Das System stellt fest, um welche Person es sich bei der Identitätsüberprüfung handelt, wobei die Erkennung beispielsweise anhand biometrischer Merkmale erfolgt.
- **Verifikation:** Das System prüft, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt, also, ob der zur Identifikation genutzte PIN oder Ausweis auch tatsächlich dem Karteninhaber gehört. Diese Angaben werden verifiziert, indem zusätzlich die aktuell erfassten biometrischen Daten einer Person mit dem entsprechenden gespeicherten Referenzmuster verglichen werden.

### Die Chipkarte als multifunktionaler Ausweis

Am weitesten standardisiert und verbreitet ist die mit Kontakten versehene Chipkarte. Bedingt durch die Art der Datenübertragung und den Aufbau des Lesesystems (Einstecköffnung, Kontaktierein-

heit) ist diese Technologie aber nicht für die Zutrittskontrolle oder den Einsatz in schmutziger oder feuchter Umgebung geeignet.

Günstiger ist die kontaktlose Chipkarte. Der Datenaustausch erfolgt kontaktlos, mittels eines elektromagnetischen Funkfeldes.

Neben der Karte werden auch sogenannte Transponder in diversen Formen und Größen, zum Beispiel als Schlüsselanhänger, angeboten. Unterschiede sind in der Art des Datenaustausches und in der verwendeten Speicher- oder Chip-Technologie zu finden. Abstandsleser identifizieren Mitarbeiter quasi im Vorbeigehen. Dabei ist lediglich die kontaktlose Chipkarte im Abstand von wenigen Zentimetern vor den Leser zu halten. Die Methode der kontaktlosen Identifikation bietet höchsten Benutzerkomfort und ein höheres Sicherheitsniveau als ein herkömmlicher Kartenleser, der durch Fremdkörper außer Funktion gesetzt werden kann. Abstandsleser vermögen den Ausweis selbst durch Glas oder Holz hindurch zu identifizieren.

### Kompakt

- Moderne Zutrittskontrollgeräte identifizieren Mitarbeiter entweder durch Erkennung ihrer biometrischen Merkmale über die auf einer Chipkarte gespeicherte PIN.
- Die kartengebundene Identifikation ist zuverlässig und geht meist sehr viel schneller vonstatten als die Erkennung personenspezifischer Merkmale.
- Biometrische Verfahren bieten eine wesentlich höhere Sicherheit.

## Varianten der Mitarbeiteridentifikation

Identträger	Speicher	Vorteile	Nachteile
<b>Kontaktbehafete Chipkarte</b>	Les- und beschreibbar Größe einige Bit bis mehrere kBytes	<ul style="list-style-type: none"> <li>• Verfügt über eine große Speicherkapazität (abhängig von der Chiptechnologie)</li> <li>• Hohe Daten- und Zugriffssicherheit, besonders bei Prozessorchipkarten</li> <li>• Über Prozessorchip können Anwenderdaten getrennt voneinander verwaltet werden</li> </ul>	<ul style="list-style-type: none"> <li>• Kontakte empfindlich gegenüber Verschmutzung und Verschleiß</li> <li>• Lage des Chips zur Kontaktiereinheit muss beim Lesen beachtet werden</li> <li>• Eingeschränkte optische Gestaltungsmöglichkeit</li> <li>• Prozessorchipkarte: relativ hoher Preis und Funktionalität, die für ZK/PZE allein nur selten genutzt werden kann</li> </ul>
<b>Kontaktlose Chipkarte oder Transponder</b>	Je nach Hersteller nur lesbar oder les- und beschreibbar, dann bis mehrere kBytes, je nach Hersteller	<ul style="list-style-type: none"> <li>• Unempfindlich gegen Feuchtigkeit, Staub, Schmutz, Fremdlicht</li> <li>• Freie optische Gestaltung</li> <li>• Verschiedene Datenträgertypen und Lesetechniken</li> <li>• Hohe Datenverschlüsselung und Sicherheitsniveau</li> <li>• Einfachste Handhabung: lesen lageunabhängig</li> </ul>	<ul style="list-style-type: none"> <li>• Herstellerspezifisches Identifikationsverfahren</li> <li>• Abhängig vom Verfahren: relativ hohe Karten- und Leserkosten</li> <li>• Bei häufiger Biegung oder starker Knickung der Karte, kann es zu einem Bruch der Antenne kommen und damit ist sie nicht mehr lesbar</li> </ul>
<b>Biometrische Verfahren</b>	Keine, da »Ident- oder Datenträger« die zu identifizierende Person ist	<ul style="list-style-type: none"> <li>• Sehr hohes Sicherheitsniveau</li> <li>• Identträger kann nicht verloren oder gestohlen werden</li> <li>• Kein Ausweis oder Transponder erforderlich</li> </ul>	<ul style="list-style-type: none"> <li>• Verfahren relativ aufwendig und kostenintensiv</li> <li>• Relativ lange Erkennungszeiten</li> <li>• Nicht für alle Umgebungsbedingungen geeignet</li> </ul>

Die Tabelle wurde entnommen aus: Müller/Störmer: Arbeitszeitmanagement & Zutrittskontrolle.

### Biometrische ID-Verfahren für Hochsicherheits-Zutrittskontrolle

Hohe Sicherheitsanforderungen verlangen ID-Merkmale, die unverwechselbar mit der Person verbunden sind und eindeutig als personenspezifisch erkannt werden. Die Verfahren zur biometrischen Erkennung sollen die Schwachstellen anderer Identifikationsmethoden ausgleichen: Beispielsweise können PINs vergessen oder aufgedeckt werden, Ausweise können abhanden kommen und vom Finder oder Dieb missbraucht werden.

Je nach Verfahren fallen große Referenzdatenmengen an. Werden diese Daten zentral abgelegt, dann wird bei einer hohen

Nutzerzahl nicht nur viel Speicherplatz benötigt, sondern die Suchzeiten für das Auffinden der jeweiligen Referenzdaten verlängern sich um mehrere Sekunden.

Durch die Kombination eines biometrischen Verfahrens mit einem Kartensystem lässt sich die Suchzeit verringern, weil nur noch gezielt auf den Datensatz auf der je-

nutzert nicht nur viel Speicherplatz benötigt, sondern die Suchzeiten für das Auffinden der jeweiligen Referenzdaten verlängern sich um mehrere Sekunden.

## Zeit und Zutritt



Abbildung 1: Wer einen Transponder bei sich trägt, kann im Vorübergehen identifiziert werden.



Abbildung 2: Verifikation über Ausweisidentifikation und Fingerprinterkennung.

weiligen Karte zugegriffen werden muss. Die bekanntesten biometrischen Verfahren sind:

- **Hand-/Fingergeometrie-Erkennung:** Abhängig vom Hersteller wird die Geometrie der Hand oder von Fingern zwei- oder dreidimensional erfasst und verglichen.
- **Gesichtserkennung:** Hier wird am Kontrollpunkt mittels Kamera automatisch ein Bild der zu identifizierenden Person aufgenommen und mit einem vorher abgespeicherten und ähnlich produzierten Bild verglichen.
- **Iriserkennung:** Durch Vergleich mit einem abgespeicherten Referenzmuster der Iris oder Regenbogenhaut, die durch ihre Äderchen, Pigmentierung und Streifen ähnlich individuell ist wie ein Fingerabdruck, erfolgt die Authentisierung von Personen.
- **Spracherkennungssystem:** Verschiedene Merkmale der Stimme des Betreibers werden abgespeichert. Im Überwachungsmodus wird gewährleistet, dass nur Personen einen Raumzutritt oder Rechnerzu-

gang erhalten, deren Sprache, nach Nennung ihres Passwortes, wiedererkannt werden. Zur Erhöhung der Erkennungssicherheit kann zusätzlich eine Analyse der Lippenbewegung bei der Spracheingabe erfolgen.

- **Gesicht, Sprache und Mimik, kombiniert:** Um die Sicherheit noch mehr zu erhöhen, können auch verschiedene biometrische Merkmale kombiniert überprüft werden. Solche Systeme können so programmiert werden, dass bei Ausfall einer Erkennungsart (etwa durch laute Geräusche oder grelles Licht) zwei eindeutig erkannte Merkmale ausreichen.

### Fingerprint bei mittleren Sicherheitsanforderungen

Bei mittleren Sicherheitsanforderungen ist die Fingerprint-Methode am vielversprechendsten. Sie zeichnet sich durch einen vergleichsweise niedrigen Speicherplatzbedarf sowie den geringen Material- und Installationsaufwand aus. Hierbei werden – optisch oder über Sensoren – Grund-

#### Mehr zum Thema

Ausführliche Informationen zur Planung, Auswahl und Einführung von Zeiterfassungs-, Identifikations- und Zutrittskontrollsystemen mit Checklisten zu den einzelnen Themenbereichen enthält das Buch:

**Mülder/Störmer:** Arbeitszeitmanagement & Zutrittskontrolle mit System Anforderungen – Einführungsstrategien – Beispiele Luchterhand, 3. vollständig überarbeitete Auflage, 2002, 404 Seiten, gebunden, 48 Euro, ISBN 3-472-03680-X



muster der Fingerkuppe (Minutien), deren Tiefe, Breite, Position und Merkmale als Parameter erfasst und mit einem Referenzmuster verglichen. Die neuartigen Module zur Fingererkennung sind so entwickelt, dass diese anstelle von schmutzanfälligen optischen Scannern, mit Silizium-Chips oder CCD-Sensormodulen arbeiten. Das Verfahren zeichnet sich durch die Integrationsfähigkeit des Sensormoduls in Zutrittsgeräten, Tastaturen und PC-Maus sowie eine hohe Benutzerfreundlichkeit aus. Um eine Täuschung des Systems auszuschließen, können Sensoren zur Lebenderkennung, etwa zur Bestimmung des Blutsauerstoffgehaltes oder der Pulsfrequenz sowie zur Temperatur- oder Hautwiderstandsmessung, eingesetzt werden. Zur Erhöhung der Sicherheit ist auch eine Kombination aus Fingererkennung und herkömmlicher Identifikation per Karte möglich. Die Daten des Fingerabdrucks werden im System so codiert, dass sie auf einer Chipkarte gespeichert werden können. Dies erspart den Zugriff auf eine Rechner-Datenbank und ermöglicht kurze Erkennungs- und Prüfzeiten. Das neue Sicherheitsbewusstsein und die mittlerweile attraktiven Preise für den Fingerprint führen verstärkt zum kombinierten Einsatz von Ausweis- mit biometrischen Systemen. Hier wird Sicherheit mit Nutzen in Einklang gebracht. Um ein erfolgreiches Zusammenspiel sicher zu stellen, müssen folgende Grundvoraussetzungen erfüllt sein:

- Das biometrische Template wird anstatt in einer Datenbank im relativ sicheren Speicher einer kontaktlosen Chipkarte hinterlegt. Die persönlichen biometrischen Daten bleiben in der Verantwortung des Eigentümers.
- Dann findet der Abgleich zwischen dem auf der Karte gespeicherten und am Identifikationssystem erfassten Template statt. Bei Übereinstimmung und geprüfter Berechtigung wird beispielsweise der Zutritt an einer Tür freigegeben.

Zur Zeit ist Biometrie hauptsächlich in ausgesprochenen Sicherheitsbereichen anzutreffen, sei es als Zutritts- oder Zugangskontroll-Lösung. Je größer jedoch die Nut-

zergruppe wird, desto höher werden die Fehlerraten und oft sind die Erkennungs-, Zugriffs- und Verarbeitungszeiten nicht akzeptabel.

### Auswahl des Identifikationssystems

Bei der Einführung von Mitarbeiterausweisen, ist die uneingeschränkte Nutzungsmöglichkeit zu beachten, damit die Mitarbeiter nicht mit mehreren monofunktionalen Ausweisen, etwa Zutritts- und Kantinenkarte, hantieren müssen. Nur der les- und beschreibbare Ausweis mit Chip, unter Umständen auch mit Magnetstreifen, kann multifunktional eingesetzt werden. Bei der Entscheidung für ein bestimmtes Identifikationssystem sind vorrangig die Akzeptanz bei der Belegschaft und die Frequentierung (etwa pro Erfassungs- oder Zutrittsstelle) zu beachten.

Die kartengebundene Identifikation ist zuverlässig und geht meist sehr viel schneller vonstatten als die Erkennung personenspezifischer Merkmale. Dagegen bieten die biometrischen Verfahren eine wesentlich höhere Sicherheit.

Die Auswahl des ID-Systems muss nach einer Kosten-/Nutzen-Analyse erfolgen und sich nach den Anwenderbedürfnissen richten: Bedienerfreundlichkeit, Benutzerakzeptanz, Zuverlässigkeit, Sicherheit, und Tauglichkeit unter Berücksichtigung der Umgebungsbedingungen (etwa bei Außeninstallationen oder schmutziger Umgebung). Bei den Beschaffungskosten muss zwischen einmaligen Ausgaben beim Kauf des ID-Systems und den laufenden Kosten unterschieden werden. Auch der Aufwand für die Systeminstallation, für seine Integration in vorhandene Anlagen und die notwendige Wartung, spielt eine wichtige Rolle.



**Autor**

**Werner Störmer,**  
Prokurist, PCS System-  
technik GmbH,  
wstoermer@pcs.com