



RFID und/oder Biometrie*

Personenerkennung für Zeit und Zutritt

Zur Überprüfung der Identität einer Person können unterschiedliche Erkennungsmerkmale verwendet werden. Ein Identifikationsmerkmal ist eine mit technischen Mitteln auswertbare Information, insbesondere die persönliche Identifikationsnummer (PIN), ein codierter Personal- oder Mitarbeiterausweis sowie biometrische Merkmale. Ausweise oder Transponder als Identträger nutzen zunehmend die RF-basierende Identifikation, wie z.B. der neue Reisepass. Soweit auf diesem Datenträger auch biometrische Merkmale abgespeichert sind, ist eine eindeutige Personenidentifizierung möglich.

Unterscheidung von Authentifikation, Verifikation und Identifikation

Die Überprüfung der Identität einer Person wird im allgemeinen Sprachgebrauch als „Identifikation“ bezeichnet. Im Verlauf der Identifizierung übermittelt eine Person ihre Identität an das überwachende/kontrollierende System, z.B. durch die Erfassung eines Passwortes/PIN oder Identträgers (Ausweis, Transponder oder biometrisches Merkmal). Im Rahmen der Authentisierung weist der Benutzer gegenüber dem System nach, dass die von ihm während der Identifizierungsphase bekannt gegebene Identität seiner Person tatsächlich zugeordnet ist.

Die Authentifizierung (auch Authentifikation, engl. authentication) bezeichnet also den Vorgang, die Identität oder Echtheit eines Objek-

tes, einer Person oder einer Sache, z.B. eines Programms, an Hand bestimmter Merkmale zu überprüfen. Nah verwandt mit der Authentifizierung ist die Authentisierung. Die Authentisierung ist das Nachweisen einer Identität, die Authentifizierung deren Überprüfung. Im Englischen wird zwischen den beiden Begriffen nicht unterschieden, das Wort authentication steht für beides.

Die Authentifizierung einer Person kann erfolgen durch:

- Wissen der Person (Beispiel: PIN-Code, Pa-
role, Passwort)

* **Bild oben: Beispiele für Identifikation (links) und Verifikation (rechts) mittels Fingerprint an einem kombinierten Terminal für Zutrittskontrolle und Zeiterfassung.**

- Besitz eines Identträgers (Beispiel: Ausweis, Transponder, etc.)
- Persönliche Merkmale (Beispiel: Finger-
print, Gesicht, Sprache etc.)
- Standort der Person (Beispiel: Adresse
des Arbeitsplatzrechners, Netzverbindun-
gen, etc.)
- Eigenschaften der Person (Beispiel: Mi-
mik, Gang, Unterschrift, etc.)

Wenn zwei dieser fünf Möglichkeiten kombi-
niert werden, spricht man von einer 2-Faktor-
Authentifizierung. Ein typisches Beispiel dafür
ist ein Geldautomat. Man besitzt einen Ident-
träger, die Bankkarte, zusätzlich muss man
aber noch etwas wissen, nämlich die PIN.

Bei biometrischen Identifikationsystemen
kann die Identitätsüberprüfung einer Person in
zwei Varianten erfolgen, wobei auch hier als
Oberbegriff die „Authentifikation“ definiert
wurde:

- Identifikation (v. lat.: idem = derselbe + fa-
cere = machen): Das System stellt anhand
eines oder mehrerer biometrischer Merk-
male fest, um welche Person es sich han-
delt.
- Als Verifizierung oder Verifikation (von lat.
veritas, Wahrheit) wird der Vorgang be-
zeichnet, einen vermuteten oder behaup-
teten Sachverhalt als wahr zu belegen. Bei
biometrischen Erkennungssystemen wird
geprüft, ob es sich bei einer Person um die-
jenige handelt, für die sie sich ausgibt
(zum Beispiel mittels Identträger oder PIN).
Diese Angaben werden verifiziert, indem
die aktuell erfassten biometrischen Daten
einer Person mit dem entsprechenden ge-
speicherten Referenzmuster verglichen
werden.

Überblick der verschiedenen Verfahren zur Personenerkennung

Bei niedrigen bis mittleren Sicherheitsanfor-
derungen innerhalb der Zutrittskontrolle ist
das gängigste Verfahren zur Personenerken-
nung die Ausweiserfassung. Solche codierten
Karten werden aber nicht nur zur Personen-
identifikation, sondern auch als elektronischer
Datenträger und als Zahlungsmittel einge-
setzt. Ein multifunktional nutzbares Medium
ist die RFID-basierende kontaktlose Chipkar-
te.

Für die Zutrittskontrolle von Hochsicherheits-
bereichen muss die Identität einer Person ein-
deutig festgestellt werden. Hierzu werden bio-
metrische Authentisierungs-Systeme
eingesetzt, die Personen anhand physiologi-
scher oder verhaltensbedingter Merkmale ein-
deutig erkennen. Diese biometrischen Merk-
male sollen die Schwächen anderer
Identifikationsarten, wie vergessener PIN
oder verlorener bzw. beschädigter Ausweis,
eliminieren.

Es können statische physiologische Attribute (z.B. Fingerabdrücke, Handgeometrie, Iris- oder Netzhautmuster) oder variable physiologische Attribute (z.B. Gesichtsmimik, Stimme) und verhaltensabhängige Attribute, wie der Schreibrhythmus auf einer Computertastatur oder eine Unterschriftserkennung, herangezogen werden.

Alle vorab aufgeführten Verfahren zur Identifikation und Authentifizierung von Personen weisen Schwächen und Nachteile auf. Ausweise können entwendet werden und bei den biometrischen Verfahren fehlt es leider noch an der grundsätzlichen Akzeptanz. Eine Alternative zur Identifikation über ein (persönliches) Merkmal bietet hier die Verifikation. Hierfür werden die biometrischen Referenzdaten auf einer Chipkarte gespeichert. Diese Angaben werden verifiziert, indem die aktuell erfassten biometrischen Daten einer Person mit dem entsprechenden gespeicherten Referenzmuster verglichen werden.

Da solche – oft auch für andere kartengesteuerte Anwendungen genutzte – Ausweise sich im Besitz der Mitarbeiter befinden, können die personenbezogenen Daten nicht von Dritten zu anderen Zwecken missbraucht werden. Durch die Kombination mehrerer Identifikationsverfahren wird nicht nur die Sicherheit, sondern auch die Akzeptanz des biometrischen ID-Verfahrens erhöht.

Je nach Verfahren fallen große Referenzdatensätze an. Werden diese Daten zentral abgelegt, wird bei einer hohen Nutzerzahl nicht nur viel Speicherplatz benötigt, sondern die Suchzeiten für das Auffinden der jeweiligen Referenzdaten verlängern sich. Durch die Kombination eines biometrischen Verfahrens mit einem Kartensystem lässt sich die Suchzeit verringern, weil nur noch gezielt auf den Datensatz auf der jeweiligen Karte zugegriffen

werden muss. Die meisten Anbieter z.B. von Zutrittskontrollsystemen bieten sowohl die Identifikation als auch die Verifikation an. Die verbreitetsten biometrischen Verfahren werden nachfolgend beschrieben:

Fingerprint

Hierbei werden – optisch oder über Sensoren – Grundmuster der Fingerkuppe (Minutien), deren Tiefe, Breite und Position als Parameter erfasst und mit einem Referenzmuster verglichen. Das Verfahren zeichnet sich durch die Integrationsfähigkeit des Sensormoduls in Zutrittskontrollgeräten, Tastaturen und PC-Maus sowie eine hohe Benutzerfreundlichkeit aus. Um eine Täuschung des Systems auszuschließen, können ggf. Sensoren zur Lebensderkennung, z.B. zur Bestimmung des Blutsauerstoffgehaltes oder der Pulsfrequenz

Gehackter Fingerabdruck

IBM erforscht Gefahren durch gekaperte biometrische Daten

IBM forscht derzeit an Lösungen im Umgang mit Angreifern, die beispielsweise einen digitalen Fingerabdruck erfolgreich hacken.

Anders als ein Passwort kann der Mensch seinen Fingerabdruck oder seine Iris nicht einfach austauschen. Gelingt es einem Fremden, die Sicherheitsschranke einmal zu durchbrechen, bleibt demnach entweder eine lebenslange Sperre des gehackten Kennzeichens oder die stete Gefahr weiteren Missbrauchs. Die Forschung soll nun dahingehend vorangetrieben werden, dass die bei einer Kontrolle abgefragten Daten zwar aus dem biometrischen Kennzeichen generiert werden, ohne jedoch die gesamte Information des Originals zu enthalten.

(SAP info)

sowie zur Temperatur- oder Hautwiderstandsmessung, eingesetzt werden, worauf aufgrund der Kosten und des technischen Aufwandes, meist verzichtet wird (siehe Bild links).

Der Einsatz von Fingerprint zur Zutrittskontrolle erfordert unbedingt Leistung vor Ort, um Geschwindigkeit zu erhalten. Bei der Maus für den Single-user-PC (1:1-Verifikation) ist dies unkritisch, da man beim Einschalten auf den Programmstart wartet. Aber für Zeiterfassung/Zutrittskontrolle in einem Betrieb ist das nicht akzeptabel.

Gesichtserkennung

Zur Gesichtserkennung wird mittels Kamera automatisch ein Bild der zu identifizierenden Person aufgenommen und mit einem vorher abgespeicherten und ähnlich produzierten Bild verglichen. Nachdem die Kamera das Gesicht mit Augen, Nase und Mund aufgenommen hat, wertet das Erkennungssystem die geometrischen Proportionen, die diese Merkmale zueinander aufweisen, aus. Alternativ kann mit Hilfe einer Videokamera die Wärmeabstrahlung der Blutgefäße unter der Gesichtshaut erfasst werden.

Innovative Bildverarbeitungsalgorithmen berechnen aus den digitalisierten Daten der Kameraaufnahme einen Merkmalsdatensatz, der mit dem auf dem Rechner abgelegten und einem einer Person eindeutig zugeordneten Datensatz auf Übereinstimmung geprüft wird. Auch bei unterschiedlicher Mimik oder Position des Gesichts vermag das System aus der Bildverarbeitung die Person sicher zu identifizieren.

Iriserkennung

durch Vergleich der Iris oder Regenbogenhaut, die durch ihre Struktur und Pigmentierung ähnlich individuell ist wie ein Fingerab-



Beispiel für Zutrittskontrolle an einem RFID-basierten Leser mit hinterlagerter Vereinzelungseinrichtung

druck. Das Verfahren zeichnet sich durch hohe Sicherheit aus.

Bei allen biometrischen Systemen, hier beispielsweise der Fingerprint, ist zu beachten:

1. Der Einlernvorgang, denn hier werden die Weichen für den Erfolg oder Misserfolg gestellt, deshalb:
 - sorgfältiges Einlernen
 - Mitarbeiter erst trainieren lassen
 - Alle Finger im „Training“ einlernen, die „tauglichsten“ 2 oder 3 Finger abspeichern!
2. Aufklärung der Mitarbeiter, damit das System akzeptiert wird:
 - Was wird abgespeichert: nur Merkmale, keine Möglichkeit daraus das Bild zurück zu gewinnen
 - Im Gegensatz zum Reisepass, hier wird das Bild als Datei abgespeichert

RFID mit kontaktlosen Chipkarten

RFID ist die Abkürzung für Radiofrequenz-Identifikation, eine mittlerweile gängige Technologie zur berührungslosen Erkennung von Waren und Objekten sowie zur kontaktlosen Erfassung von Informationen auf Ident- bzw. Datenträgern mithilfe von Radiowellen. Ein RFID-System besteht aus einem Transponder (Funketikett/Smart-Label, Ausweis, Schlüsselanhänger, etc.) mit integrierten Mikrochip und Antenne sowie einem mobilen oder stationären Lesegerät. Sendet ein RFID-Lesegerät ein Funksignal aus, antworten in der Nähe befindliche Transponder, indem sie die auf ihnen gespeicherten Daten, z.B. den Zugangs-/Zutritts- oder Berechtigungscode an die Lesestation übermitteln. Der mögliche

Leseabstand von RFID-Systemen beträgt wenige Zentimeter bis einige Meter (siehe Bild oben links).

Bei Einsatz der RFID-Technologie kann die Identifikation quasi im „Vorbeigehen“ erfolgen, dabei ist lediglich die kontaktlose Chipkarte im Abstand von wenigen Zentimetern vor den Leser zu halten (Bild 1). Die Lesereichweite hängt von der Art und Größe der Antenne im Lesegerät und im Transponder ab. Mittlerweile gibt es eine Vielzahl an kontaktlosen Chipkartentypen, wobei sich die Systeme mit einer Übertragungsfrequenz von 125 kHz/13,56 MHz durchgesetzt haben. Dabei ist zwischen herstellereinspezifischen und genormten Verfahren zu unterscheiden. Die zur Zeit am meisten genutzten Lesereichweiten für Remote-Coupling-Karten werden in den nachfolgend aufgeführten Normen beschrieben:

DIN/ISO/IEC 14443
proximity coupling, PICC
für eine Reichweite bis ca. 10 cm

DIN/ISO/IEC 15693
vicinity coupling, VICC
für eine Reichweite bis ca. 1 m

Hier wurden die physikalischen und datentechnischen Eigenschaften der Übertragungstrecke zwischen einem Lesegerät und dem Datenträger als Norm spezifiziert.

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; dadurch lässt sich das Zutrittskontrollterminal vor Vandalismus schützen. Bei der kontaktlosen Chipkarte ist eine Kombination mit anderen Verfahren, wie Magnetstreifen, kontaktbehaftetem Chip oder Barcode, möglich (Kombikarte).

Erreicht wird dadurch eine völlige Unabhängigkeit zwischen dem Chipkarteninterface (Kontakte, kontaktlos, Infrarot, etc.) und der Chipkartenlogik bzw. Chipkartenanwendung. Die berührungslose Technologie ist weitgehend sabotagesicher und bietet einfachste Handhabung zur Identifizierung. Für sicherheitsrelevante Lese-/Schreibvorgänge mit relativ vielen Daten, wie bei Zahlungsfunktionen, erfolgt jedoch zunächst weiterhin der kontaktbehaftete Datenaustausch.

Empfehlungen zur Systemauswahl

Die Auswahl des ID-Systems kann nach einer Kosten-/Nutzen-Analyse erfolgen und sich nach den Anwenderbedürfnissen richten: Bedienerfreundlichkeit, Benutzerakzeptanz, Zuverlässigkeit, Sicherheit und Tauglichkeit unter Berücksichtigung der Umgebungsbedin-



Zutrittskontrolle im Außenbereich an einem RFID-basierten kontaktlosen Lesesystem

gungen (z.B. bei Außeninstallationen, schmutziger Umgebung, usw.). Abhängig von der Frequenzierung je Zutrittsstelle sind insbesondere die Erkennungszeiten zu beachten, hierzu gehört die richtige Positionierung und Handhabung des Identträgers (Ausweis, Transponder oder biometrisches Merkmal) am Identifikationssystem und die Zeit/Performance für den Vergleich und die Prüfung der Daten.

Bei der Einführung von Mitarbeiterausweisen ist die uneingeschränkte Nutzungsmöglichkeit zu beachten, damit die Mitarbeiter nicht mit mehreren monofunktionalen Ausweisen, z.B. Zutritts- und Kantinenkarte, hantieren müssen. Nur der les- und beschreibbare Ausweis mit Chip, unter Umständen auch mit Magnetstreifen, kann multifunktional eingesetzt werden. Die kartengebundene Identifikation ist relativ zuverlässig, sehr preisgünstig und geht meist viel schneller als die Erkennung der meisten biometrischen Merkmale. Nachteil ist, dass Ausweise verloren oder beschädigt werden können und der Nutzer nicht immer der Besitzer bzw. Berechtigte sein muss (siehe Bild oben rechts).

Dagegen bieten die biometrischen Verfahren eine wesentlich höhere Sicherheit und oft einen größeren Benutzerkomfort, sind jedoch nicht für alle Einsatzarten geeignet. Die Auswahl muss also entsprechend der jeweiligen Anforderungen und den Umgebungsbedingungen sorgfältig erwogen werden. Bei den biometrischen Verfahren fallen sehr große Referenzdatenmengen an, die bei einer hohen Nutzerzahl großen Speicherplatz und relativ lange Suchzeiten benötigen. Auch mit intelligenten Verfahren und schnellen Computern kann der Suchvorgang für die Referenzdaten

einige Sekunden dauern. Durch die Kombination mit der Ausweisidentifizierung lässt sich die Suchzeit reduzieren und die persönlichen Referenzdaten bleiben im Eigentum des Besitzers.

Bei den Beschaffungskosten muss zwischen einmaligen Ausgaben beim Kauf des ID-Systems und den laufenden Kosten unterschieden werden. Auch der Aufwand für die Systeminstallation, der Platzbedarf des jeweiligen Systems und die notwendige Wartung, spielt eine wichtige Rolle. Beispielsweise sind Ausweisleser für kontaktlose Chipkarten oder Fingerprintsysteme relativ preiswert, einfach zu installieren und haben den geringsten Platzbedarf. Dagegen arbeitet die Gesichtserkennung meist mit in Standsäulen integrierten Kameras, oft kombiniert mit Spiegel als Positionierungshilfe. Solche Systemeinheiten sind relativ groß, um sie architektonisch einfach und optisch ansprechend integrieren zu können.

Alle aufgeführten Verfahren haben ihre Vor- und Nachteile. Bei der Vielfalt der unterschiedlichen Sicherheitsanforderungen, Einsatzbedingungen und Unternehmenstypen hat der Anwender somit eine große Auswahlmöglichkeit. Ausführliche Informationen zur Planung, Auswahl und Einführung von Identifikations- und Zutrittskontrollsystemen mit Checklisten zu den einzelnen Themenberei-

chen enthält das Fachbuch „Arbeitszeitmanagement und Zutrittskontrolle mit System“, das im Luchterhand Verlag, Neuwied (ISBN 3-472-03680-X) erschienen ist.

Kombinationsbeispiel: RFID und Biometrie – Der neue Reisepass

Deutschland hat als einer der ersten EU-Staaten den neuen biometriegestützten Reisepass eingeführt. Dieser enthält einen zertifizierten RFID-Sicherheitschip mit kryptographischem Coprozessor, auf dem neben den bisher üblichen Passdaten auch biometrische Merkmale gespeichert werden können. Zunächst soll ein digitales Foto des Passinhabers gespeichert werden. Ab März 2007 werden in neuen Pässen zusätzlich zwei Fingerabdrücke gespeichert. Der elektronische Pass – kurz ePass genannt – erlaubt eine elektronische Überprüfung, ob der Nutzer des Dokuments tatsächlich der Passinhaber ist.

Die Integrität und die Authentizität der in dem RFID-Chip gespeicherten Daten soll über eine digitale Signatur gesichert werden. Der Chip soll durch einen Zugriffsschutz nicht unbemerkt ausgelesen werden können. Mit dem neuen Reisepass setzt Deutschland eine internationale Vereinbarung um, die die Sicherheit des internationalen Reiseverkehrs durch Einführung biometrischer Merkmale in Pässen erhöhen soll.

Ausblick

RF-basierende und biometrische Identifikationssysteme haben weltweit eine stark zunehmende Verbreitung und zeichnen sich durch ein hohes Anwendungsspektrum aus. Wie erwähnt, ermöglicht der Einsatz von RFID-Chips den Datenaustausch von wenigen Zentimetern bis zu mehreren Metern. Sie bergen ein großes Innovationspotenzial und werden heute zunehmend in der Industrieautomation, dem Warenmanagement, der Tier- und Personenidentifikation, bei Zugangs- und Zutrittsystemen oder elektronischen Wegfahrsperrungen eingesetzt. Die berührungslose Lokalisierung von Produkten oder Identifizierung von Personen führt zu enormen Zeitersparnissen und einem geringeren Arbeits-, Personal- und Verwaltungsaufwand. Denkbare weitere Anwendungsfelder sind das Gesundheitswesen und Zahlungsfunktionen.

Viele biometrische Identifikationssysteme haben sich im Einsatz bewährt und weitere sind in der Planung. Weil sie die höchste Erkennungsgenauigkeit bieten, einfach zu bedienen sind und langfristig Wachpersonal sparen, könnten sie schon bald zur unverzichtbaren Technologie für alle sicherheitsrelevanten Anwendungen werden.

Autor: Werner Störmer, Erkrath