

Identifikation und Zutrittskontrolle – Teil I

Zur Prüfung der Zutrittsberechtigung einer Person ist deren schnelle und sichere Identifikation (ID) erforderlich. Dazu stehen mittlerweile eine Vielzahl von Identträgartypen und ID-Verfahren zur Verfügung, die sich von der klassischen Ausweiserfassung bis hin zu biometrischen Erkennungsverfahren erstrecken.

Zunehmend wird die Zutrittskontrolle auch mit anderen kartengesteuerten Anwendungen, wie Personalzeit-, Kantinen- und Betriebsdatenerfassung, kombiniert. Dann ist die Auswahl des richtigen, multifunktional nutzbaren, Identträgers von besonderer Bedeutung. Ist zusätzlich noch die Zutrittskontrolle für einen Hochsicherheitsbereich zu berücksichtigen, dann müssen auch biometrische ID-Verfahren einbezogen werden.

Überblick der verschiedenen Verfahren zur Personenerkennung

Die erste Aktion zur Absicherung eines Systems (Rechner/Netzwerk) oder zur Zutrittskontrolle ist die Identifikation und Authentisierung von zugriffs- bzw. zugriffsberechtigten Personen. Im Verlauf der Identifizierung übermittelt eine Person seine 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.

Bei niedrigen bis mittleren Sicherheitsanforderungen innerhalb der Zutrittskontrolle ist das gängigste Verfahren zur Personenerkennung die Ausweiserfassung. Solche codierten Karten werden aber nicht nur zur Personenidentifikation,



Beispiel für Identifikation mit kontaktloser Chipkarte zur Zutrittskontrolle und/oder Personalzeiterfassung

sondern auch als elektronischer Datenträger und als Zahlungsmittel eingesetzt. Deshalb sollte hier ein multifunktional nutzbares Medium, wie die kontaktlose Chipkarte, eingesetzt werden.

Für die Zutrittskontrolle von Hochsicherheitsbereichen muss die Identität einer Person eindeutig und unwiderlegbar festgestellt werden. Hierzu werden biometrische Authentisierungssysteme eingesetzt, die Personen anhand physiologischer und verhaltensbedingter Merkmale eindeutig erkennen. Diese biometrischen Merkmale sollen die Schwächen anderer Identifikationsarten, wie vergessener PIN oder verlorener bzw. beschädigter Ausweis, eliminieren.

Es können statische physiologische Attribute (z.B. Fingerabdrücke, Handgeometrie, 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 meist noch an der Akzeptanz. Einen Ausweg bietet hier die Verifikation, bei der das ID-System prüft, ob es sich bei einer Person um diejenige handelt, für die sie sich z.B. mittels Identriträger und/oder PIN ausgibt. Hierfür werden seine biometrischen Referenzdaten auf einer Chipkarte gespeichert. Diese Angaben werden verifiziert, indem die aktuell erfassten bio-metrischen Daten einer Person mit dem entsprechenden gespeicherten Referenzmuster verglichen werden.

Da solche – oft auch für andere Anwendungen genutzte – Karten 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.

Chipkarten als Ausweise

Am weitesten standardisiert und verbreitet ist die mit Kontakten versehene Chipkarte. Bedingt durch die Art der Datenübertragung und den Aufbau des Lesesystems (Einstecköffnung, Kontaktiereinheit) ist diese Technologie aber nicht für die Zutrittskontrolle oder den Einsatz in schmutziger oder feuchter Umgebung geeignet. Günstiger ist die kontaktlose Chipkarte, bei der der Datenaustausch kontaktlos, mittels eines elektromagnetischen Funk-Feldes, erfolgt. Neben der Karte werden auch so genannte Transponder in diversen Formen und Größen, zum Beispiel als Schlüsselanhänger, angeboten. Unterschiede sind in der Art des Datenaustausches und in der verwendeten Speicher- bzw. Chiptechnologie zu finden. Abstandsleser werden als integrierte Module für Karten-Terminals sowie als abgesetzte oder eigenständige Leser angeboten.

Neue Normen

Die Identifikation kann quasi im „Vorbeigehen“ erfolgen, dabei ist lediglich die kontaktlose Chipkarte im Abstand von wenigen Zentimetern vor den Leser zu halten (Abb.). Dabei hängt die Lesereichweite 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 herstellerspezifischen und genormten

Verfahren zu unterscheiden. Die zur Zeit am meisten genutzten Lesereichweiten für Remote-Coupling-Karten werden in den nachfolgend aufgeführten Normen beschrieben:

- ISO/IEC 14443
proximity coupling, PICC
für eine Reichweite bis ca. 10 cm
- ISO/IEC 15693
vicinity coupling, VICC
für eine Reichweite bis ca. 1 m


Hier wurden die physikalischen und datentechnischen Eigenschaften der Übertragungsstrecke zwischen einem Lesegerät und dem Datenträger 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 ZK-Terminal vor Vandalismus schützen. Bei der kontaktlosen Chipkarte ist eine Kombination mit anderen Verfahren, wie Magnetstreifen, kontaktbehafteter Chip oder Barcode, möglich (Kombikarte). Eine sehr interessante Weiterentwicklung ist die so genannte Dual-Interface-Card. Der Chip bietet zwei Schnittstellen, die wahlweise den kontaktlosen als auch den kontaktbehafteten Datenaustausch ermöglichen. Hier werden die Funktionen und Eigenschaften beider Technologien in einem Medium vereint.

Dadurch besteht 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 der kontaktbehaftete Datenaustausch.

In der nächsten Ausgabe lesen Sie über biometrische Verfahren wie Fingerprint, Gesichtserkennung und über Empfehlungen zur Systemauswahl.

Werner Störmer

PCS Systemtechnik GmbH • wstoermer@pcs.com
Adresse des Anbieters am Hefende in der Einkaufsrubrik  Kategorie Zeit + Zutritt.

PCS auf der CeBIT:
CeBIT, Halle 7, Stand A14