6. Ausweis- und Identifikationssysteme

6.1 Allgemeines

In der Zutrittssteuerung kommt der zuverlässigen, sicheren und schnellen Identifikation der Benutzer eine herausragende Bedeutung zu.

Im Rahmen von Zutrittssteuerungssystemen kann die Erkennung der Benutzer erfolgen über

- das Wissen der Person (bspw. PIN-Code, Passwort)
- den Besitz der Person (bspw. Ausweis, Transponder, codierter Schlüssel) und/oder
- die Eigenschaften der Person (bspw. biometrisches Merkmal).

In der Praxis wird häufig der „Besitz“, also ein Ausweis oder ein Transponder eingesetzt, weiter zunehmend gewinnt auch die Biometrie an Bedeutung. Das „Wissen“, i.d.R. die PIN, ist in Mitteleuropa nur noch selten alleiniges ID-Mittel zur Zutrittssteuerung, wird aber für die Mehrfaktorauthentifizierung nach wie vor eingesetzt.

Die Personenidentifikationsverfahren sind grundsätzlich umso sicherer, je mehr die Erkennungsparameter direkt vom Nutzer abhängig und personengebunden sind. Beispielsweise gewährleistet der bloße Besitz einer Karte noch keine zuverlässige Identifikation einer Person. Schließlich könnte die Karte defekt, gefunden oder gestohlen worden sein. Erst durch Ergänzung um weitere, möglichst schwer nachahmbare und personenbezogene/gebundene Merkmale, wie eine Unterschrift, ein PIN-Code oder körperliche Merkmale, ist eine sicherere Identifikation realisierbar. Bei erhöhten Sicherheitsanforderungen werden daher oft Kombinationen aus „Wissen“, „Besitz“ und/oder „Eigenschaften“ verwendet.

Die unterschiedlichen Erkennungsarten sind in den folgenden Kapiteln ausführlicher beschrieben.

6.2 Identifikation durch Wissen

Die Erkennung durch Wissen erfolgt bei der Zutrittssteuerung durch die Eingabe eines PIN- oder Tür-Codes. In der Anwendung werden hierzu in der Regel numerische Tastaturen als Schlossersatz verwendet.

Die Persönliche-Identifikations-Nummer (PIN) ist eine nur einer oder wenigen Personen bekannte Ziffernfolge, mit der diese sich an einer Zutrittsstelle gegenüber einem Zutrittsleser authentisieren können. Im engeren Sinne sind PINs numerische Passwörter. Beim PIN-Code wird die Person identifiziert, beim Türcode nicht.

Die „Identifikation durch Wissen“ kommt vorrangig bei einfachen Zutrittssystemen als alleiniges ID-Mittel oder als ergänzender Faktor in Mehrfaktor-Authentifizierungssystemen in Kombination mit eigenschafts- und/oder besitzbasierten Verfahren zum Einsatz.

Abb. 6.01: PIN-Eingabe

Bei der Zugangssteuerung zu IT-Systemen (Login) und Geräten oder der Zugriffskontrolle zu Daten erfolgt die wissensbasierte Berechtigungskontrolle mittels Passwort. Hierbei besteht jedoch die Gefahr der Weitergabe, des Erratens, des Vergessens oder Erpressens der für den Zutritt, Zugang oder Zugriff notwendigen Informationen. Keinesfalls sollte man wegen Einfachheit des Merkens die unsichere Zahl „4711“ wählen, was leider in der Praxis auch vorkommt. Bei einem höheren Sicherheitsbedürfnis werden daher meistens Kombinationen mit Ausweisen und/oder biometrischen Verfahren eingesetzt.

6.3 Ausweise und Codierverfahren

Für die angemessene Zutrittssteuerung reichen bedruckte Ausweise zur Sichtkontrolle nicht aus. Zu groß ist die Gefahr der Verwechslung oder der Täuschung durch Verwendung ähnlicher Ausweise. Wichtige Details, wie das Ablaufdatum, können außerdem leicht übersehen werden.

In der Praxis kommen daher codierte bzw. personalisierte Ausweise zum Einsatz, die als Speichermedium dienen. Zur Beurteilung der Ausweise und Codierverfahren können unterschiedliche Kriterien herangezogen werden, deren Bedeutung sich im Einzelfall unterscheiden kann. Häufig sind dies:

- Fälschungs- und Manipulationssicherheit
- berührungsloser Lesevorgang
- Lebensdauer
- (Produktions-) Kosten
- Lesefehlerrate
- Speicherkapazität
- Veränderbarkeit der Codierung

Ausweise bzw. ID-Mittel können hierbei (nur) 2 Arten von Informationen tragen:

- **die Identität**
  Daten, die den Ausweisinhaber in dieser Anwendung identifizieren
  (Ausweisnummer, Name, Abteilung usw.)
- **die Rechte**
  Daten, die die Rechte des Ausweisinhabers in dieser Anwendung nachweisen
  (Zutrittsrechte, Bedienrechte, Geldbeträge für Kasino/Automaten usw.)

Den verschiedenen Ansprüchen folgend, sind auf dem Markt unterschiedliche Ausweistypen (z.B. mit/ohne Passbild) und Kartencodierungen vorhanden. Grundlegend ist hierbei zwischen veränderlichen und statischen, nicht veränderbaren Codierungen zu unterscheiden.

Statische Codierungen, wie bei Hitag1 mit einer konstanten Seriennummer (UID Unique Identifier) und beim Barcode (z.B. auf Besucherausweisen) enthalten in der Regel verschlüsselte Informationen, die nicht veränderbar sind. Im Gegensatz dazu können die Karteninformationen veränderlicher Codierungen, wie Magnetstreifen oder Chipkarten, gelesen und geschrieben werden. Dies ermöglicht das nachträgliche Ändern, ohne einen neuen Ausweis ausstellen zu müssen.

An dieser Stelle ist vorauszuschicken, dass einfache, kontaktbehaftete Chipkarten, Barcode- oder Magnetstreifenausweise für die Zutrittssteuerung keine oder lediglich eine geringe Bedeutung haben. Daher wird nachfolgend stärker auf die moderneren RFID-Chips eingegangen und diesem Thema ein eigenes Kapitel gewidmet.

6.3.1 Magnetkarte

Magnetstreifenausweise sind aus vielen Anwendungen bekannt und besitzen ein breites Einsatzspektrum, z.B. als Zahlungsbeleg in Tiefgaragen oder auf EC-Karten. In der Regel ist der Magnetstreifen in drei Spuren aufgeteilt, wovon zwei nur für den Lesebetrieb vorgesehen sind und eine weitere auch beschrieben werden kann.

Der Vorteil dieser Ausweissysteme liegt in den geringen Kosten, da der schmale Magnetstreifen, der in der Längsrichtung verläuft, sehr leicht auf dem Ausweis angebracht werden kann. Schreib- und Leseeinheit sind vergleichsweise einfach und entsprechen dem Aufbau eines Magnetbandgerätes zur Tonaufzeichnung. Aus diesem Grund ist die Magnetkarte für alltägliche Zahlungsfunktionen noch weit verbreitet und standardisiert.

Der wesentliche Nachteil dieser Technik besteht darin, dass die Magnetstreifen bei starkem Magnetfeldeinfluss, beispielsweise durch einen Dauermagneten, sehr leicht ihre Informationen verlieren und diese dann neu programmiert werden müssen. Darüber hinaus lassen sich die gespeicherten Informationen in einfacher Weise auslesen, auf einen anderen Ausweis übertragen und manipulieren. Magnetkarten sind daher als Träger sensibler bzw. geheimer Informationen eher ungeeignet. Gegenüber Chipkarten verfügen sie zudem über eine nur sehr begrenzte Speicherkapazität. Durch den notwendigen Kontakt zum Lesegerät unterliegt der Magnetstreifen des Weiteren einem kontinuierlichen Abrieb und somit einer verkürzten Lebensdauer.

6.3.2 QR- und Barcode

Barcode-Ausweise

Ausweise mit Barcode sind einfach und kostengünstig herstellbar, beispielsweise mit einem einfachen Drucker, und unempfindlich gegen elektromagnetische Felder. Die bestimmte Abfolge schmaler oder breiter Striche/Streifen bildet, nach dem Binärprinzip, den Code. Genauso können Ausweise mit einem Barcode bedruckt oder beklebt werden, um bestimmte Informationen zu transportieren. Die Erfassung erfolgt durch ein Rotlicht oder eine Infrarot-Lichtquelle. Allerdings sind sie nur bei ausreichendem Kontrast zwischen den Balken und unter Einhaltung der Toleranzen fehlerfrei lesbar. Es können nur wenige Informationen codiert werden, da für Ausweise bisher nur eindimensionale Barcodes eingesetzt werden. Wie Magnetkarten unterliegen sie außerdem einer Abnutzung durch Umwelteinflüsse. Der Barcode sollte daher möglichst unter einer Schutzfolie angebracht werden.

Das Ablesen dieser Codierung erfolgt optisch, durch die unterschiedliche Reflektion eines Rot-/Infrarot-Lichtstrahls. Das entsprechende Medium wird durch den Führungsschlitz des Durchzugs-/Einstecklesers an der Leseoptik vorbei gesteckt, gezogen oder geschoben. Neben der Verschmutzungsempfindlichkeit der Leseoptik ergibt sich der Nachteil einer sensiblen Durchzugsöffnung, in die Fremdkörper gelangen können. Dieses Verfahren wird als Identträger dort zum Einsatz kommen, wo z.B. kontaktlose Chipkarten aufgrund spezieller Umgebungsbedingungen, z.B. starke Magnetfelder, nicht eingesetzt werden können oder aus Kostengründen, z.B. bei Gäste- oder Besucherausweisen.

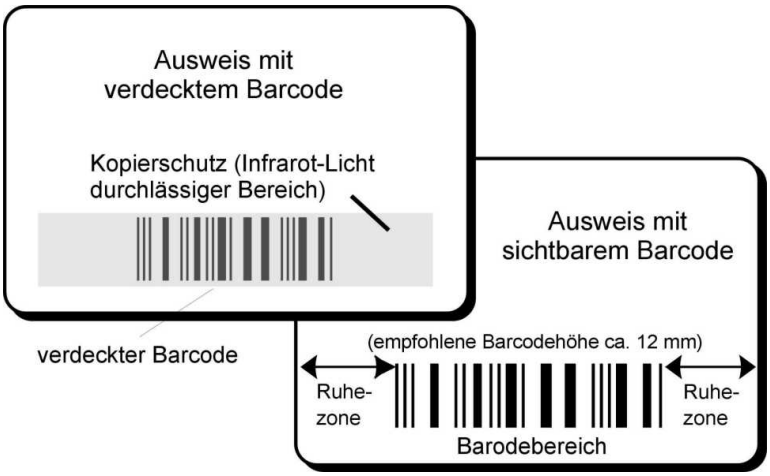

Abb. 6.02: *Ausweise mit sichtbaren und verdeckten Barcode*

Um die Ausweis-Codierung gegen Umgebungseinflüsse und Vervielfältigung (z.B. durch Fotokopieren) zu schützen, wird der Barcode mit einer infrarotdurchlässigen und abwaschbaren Folie abgedeckt. Zur Vereinfachung der Handhabung kann der Barcode auch beidseitig auf der Karte aufgebracht werden. Dabei sind allerdings die Kosten und die Einschränkungen bei der grafischen Gestaltung des Ausweises zu beachten.

QR-Code

Ein QR-Code (englisch Quick Response, „schnelle Antwort“, als Markenbegriff „QR-Code“) ist ein zweidimensionaler Barcode, in dem Informationen durch schwarze und weiße Punkte (sog. Datenpixel oder auch „QR-Code-Module“) dargestellt werden. Aufgrund einer automatischen Fehlerkorrektur ist dieses Verfahren sehr robust. Während beim eindimensionalen Barcode bis zu 128 Zeichen darstellbar sind, liegt die Informationsdichte beim QR-Code bei über 4.000 alphanumerischen Zeichen. Darum findet er in der Zutrittssteuerung insbesondere bei der Besucherverwaltung eine hohe Verbreitung. Beispielsweise kann dem Besucher per E-Mail ein Ausweisdokument mit QR-Code mit Sicherheitshinweisen und Lageplan-Optionen zum Ausdrucken zugesendet werden. In einer solchen Bestätigungsmail kann ein QR-Code generiert werden, mit dem alle wichtigen Daten

über den Besucher schnell erfasst werden. Für wiederholten Besuch werden die Eingaben gespeichert. Alternativ kann der QR-Code auch auf dem Smartphone-Monitor angezeigt werden und ähnlich der Ticket-Erfassung an Flughäfen, auch für die Zufahrts- und Zutrittssteuerung von Gästen genutzt werden.

6.3.3 Chipkarten

Ausweise mit integriertem Mikrochip, sogenannte Chipkarten, finden eine weite Verbreitung und sind in der Anwendung sehr beliebt. Sie besitzen Eigenschaften, die sie anderen Codierungen überlegen machen.

So erlauben sie in der Regel die Speicherung größerer Datenmengen als beispielsweise auf Magnetkarten und eine Aufteilung des Speicherplatzes in voneinander getrennte Bereiche für verschiedene Anwendungen (z.B. ID-Daten, Geld-Guthaben, Zutrittsrechte). Gleichzeitig bieten sie viele Möglichkeiten der Codierung und eine gute Absicherung gegen unberechtigten Zugriff (lesen), unberechtigtes Ändern der Daten (verfälschen), duplizieren und kopieren.

Grundsätzlich lässt sich zwischen kontaktbehafteten und kontaktlosen Chipkarten unterscheiden. **Kontaktbehaftete Chipkarten** sind mit außen liegenden Kontakten versehen, die beispielsweise von EC-Karten als goldfarbene Auflagefläche bekannt sind. Diese Ausweise müssen in einer bestimmten Lage so in einen Einsteckleser eingeführt werden, dass über die Fühler der Kontaktiereinheit eine Verbindung zu dem darunterliegenden Chip entsteht. Die Kontaktflächen sind daher vor Verschmutzung und Elektrizität zu schützen. Kontaktbehaftete Chipkarten können als sogenannte „Smart Cards“ mit einem Mikroprozessor ausgestattet sein oder als „Memory Card“ nur mit einem Speicher.

Im Gegensatz dazu besitzen **kontaktlose Chipkarten** keine sichtbaren, elektrischen Anschlüsse. Die Übertragung von Information von und zur Leseeinheit erfolgt hier über ein Hochfrequenzfeld, das von der Leseeinheit aufgespannt wird. Passive berührungslose Chipkarten erhalten ihre Energie aus diesem Feld und kommunizieren über eine Sendeantenne mit dem Leser. Im Gegensatz dazu erhalten aktive kontaktlose Chipkarten ihre Energie aus einer eingebauten Batterie oder externen Stromversorgung. Hierdurch sind höhere Reichweiten möglich.

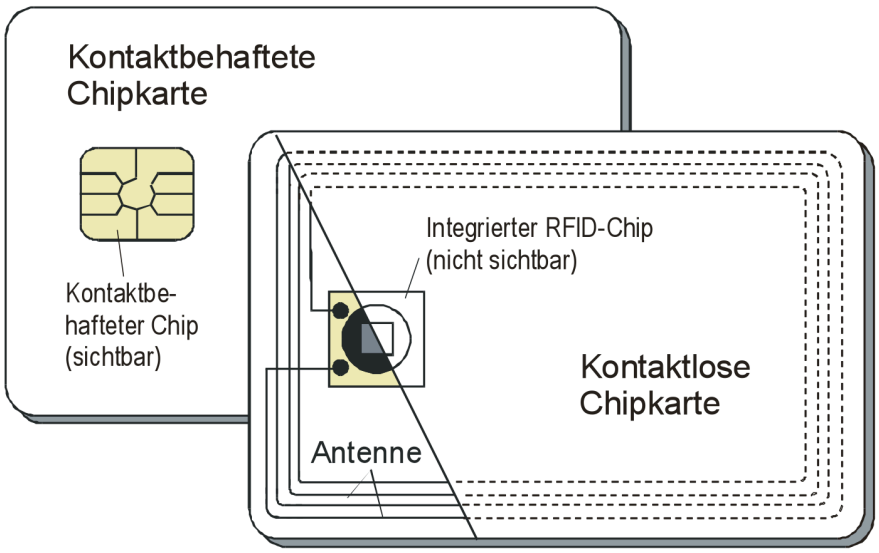

Abb. 6.03: *Prinzip von kontaktlosen und kontaktbehafteten Chipkarten*

Besondere Bedeutung im Umfeld der berührungslosen Chips hat die RFID-Technologie gewonnen, die immer häufiger zum Einsatz kommt. Auch die darauf basierende „Near-Field-Communication“ (NFC) wird in der praktischen Anwendung zunehmend eingesetzt. Beide Techniken werden daher in den nachfolgenden Kapiteln ausführlicher behandelt.

6.4 RFID - Radio Frequency Identification

6.4.1 Allgemeines

Der Schwerpunkt von RFID-Ausweisen oder allgemein RFID-Mitteln (RFID = **R**adio **F**requency **ID**entification; übersetzt: Radio-Frequenz-Identifikation) liegt in der Zutrittssteuerung auf dem Einsatz sogenannter passiver Systeme, bei denen der RFID-Chip keine eigene Energieversorgung hat, sondern seine Energie aus dem Feld der Schreib-/Leseeinheit bezieht.
Die RFID-Technologie, die es bereits ab den 80er-Jahren des letzten Jahrhunderts gab, kann als ausgereift und voll einsatzfähig bezeichnet werden. Anlagen für Zutritt und Zeiterfassung sind heutzutage in Mitteleuropa zu ca. 98% mit RFID-Technologie verwirklicht, ein weiterer Hinweis für die Attraktivität dieser Technik.

Neben dem Einsatz in der Zutrittssteuerung und den damit oft verbundenen organisatorischen Applikationen nimmt seit Ende 2010 die hoheitliche Anwendung in Pässen, ID-Karten, Führerscheinen usw. einen breiten, auch öffentlich stark beachteten Raum ein.

Abb. 6.04: *Zutritt mit kontaktloser Chipkarte (mit RFID-*

6.4.2 Historie der RFID-Systeme

Vorläufer der aktiven RFID-Systeme war ein Gerät zur Freund-Feind-Erkennung, mit dem die USA ihre Kampfflugzeuge im 2. Weltkrieg ausstatteten. Den 1948 von Stockman veröffentlichten Aufsatz „Communications by Means of Reflected Power“ kann man als eigentliche Geburtsstunde der RFID bezeichnen, auch wenn mangels integrierter Schaltungen noch keine größeren Anwendungen möglich waren. Die Erfindung des integrierten Schaltkreises 1958 von Jack Kilby ermöglichte ab ca. 1960 die Herstellung von kleinen Transpondern.

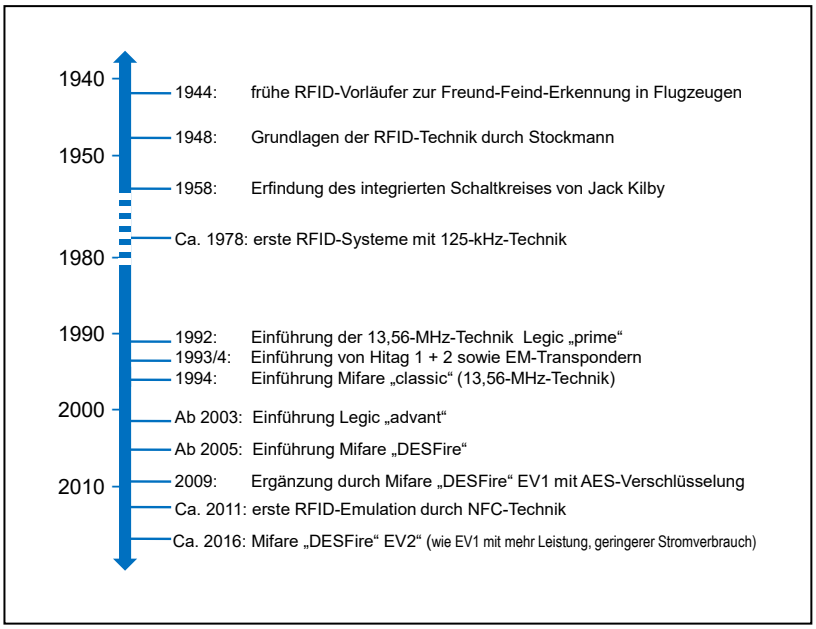

Abb. 6.05: *Historie der RFID-Entwicklung*

In den 60er Jahren des letzten Jahrhunderts kamen die 1-bit-Systeme, z.B. zur elektronischen Warensicherung gegen Ladendiebstahl auf. In den 70er und Anfang der 80er Jahren folgten weitere, wenn auch publizistisch wenig bekannte Anwendungen. Bedingt durch die geringe Verbreitung und die damit verbundenen hohen Chip-Preise sowie eine noch nicht ausgereifte Technologie, wurde diese Technik nur in Spezialanwendungen genutzt. In den 1970er Jahren wurden RFID-Systeme in der Landwirtschaft zur Kennzeichnung von Haus-/Nutztieren eingesetzt. Kurz danach kamen weitere Anwendungen hinzu, wie die Nutzung in der Containerlogistik oder bei der automatischen Fertigung.

Eine der ersten publizistisch bekannten Aktionen war ab 1988 eine Impfaktion bei sardischen Hunden und deren Kennzeichnung mit RFID in Form von glasgekapselten Transpondern. Ansonsten wurde in den 80er Jahren die Entwicklung der RFID-Systeme in den Vereinigten Staaten und einigen