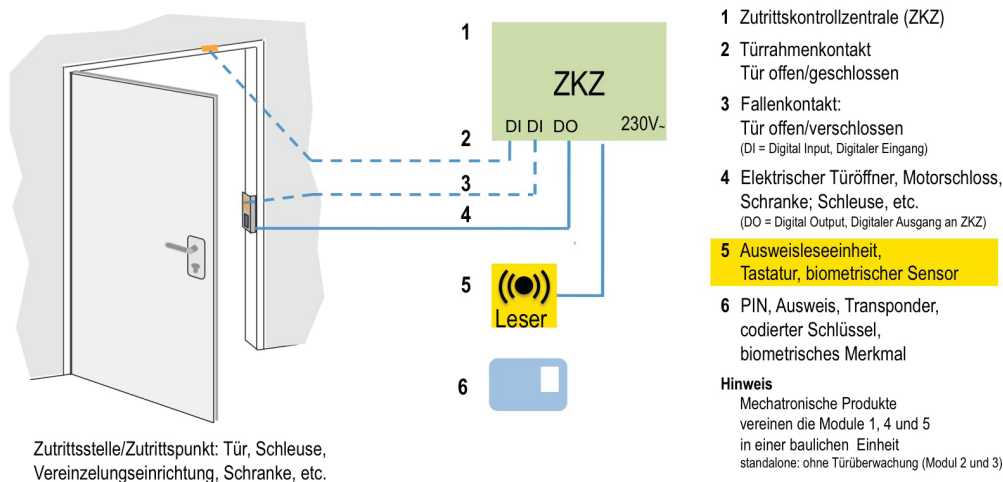


Erkennen der Benutzer einer Zutrittssteuerungsanlage

Die grundlegende Aufgabe einer Zutrittssteuerungsanlage besteht darin, zu entscheiden, wer wo und wann in einen gesicherten Bereich eintreten darf. Während das **Wo** und **Wann** auf der Einteilung in Raum- und Zeitzonen und damit auf organisatorischen Festlegungen beruht, steht hinter dem **Wer** die Identifikation, d.h. die Erkennung des Benutzers.

Der Sicherheit und Ergonomie der Identifikation (ID) kommt eine herausragende Bedeutung zu. Diese Aspekte sind deshalb in der Norm IEC 60839-11-1 „Elektronische Zutrittskontrollanlagen - Anforderungen an Systeme und Geräte“ wichtige Kriterien für Sicherheitsanwendungen.

Einfaches Zutrittssteuerungssystem



In der Zutrittssteuerung kommt der zuverlässigen, sicheren und schnellen Identifikation der Benutzer eine herausragende Bedeutung zu. Die Erkennung der Benutzer kann erfolgen über:

- den Besitz der Person (Ausweis, Transponder, Smartphone)
- das Wissen der Person (PIN-Code)
- die Eigenschaften der Person (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“, also die PIN, wird als alleiniges ID-Mittel in Mitteleuropa in der Zutrittssteuerung nur selten eingesetzt. Bei erhöhten Sicherheitsanforderungen erfolgt eine Zwei-Faktor-Authentifizierung, eine Kombination aus „Wissen“, „Besitz“ und/oder „Eigenschaften der Person“. So ist eine verlorene und noch nicht gesperrte Karte bei der Kombination mit „Wissen“ oder „biometrischem Merkmal“ vom Kartenfinder nicht verwendbar.

Ein biometrisches Erkennungsverfahren, z.B. Fingerabdruck, Gesichts-, Venen- oder Iriserkennung, ist das einzige Mittel, den zu einem Ausweis gehörenden Besitzer auf Grund des hinterlegten biometrischen Merkmals zu „erkennen“. Wird ausschließlich ein biometrisches Merkmal verwendet, so handelt es sich um Identifikation.

Wird zusätzlich zur biometrischen Erkennung ein ID-Mittel eingelesen oder ein Wissensmerkmal (PIN) eingegeben, handelt es sich um Verifikation (von lat. veritas „Wahrheit“: Prüfung, ob eine Person diejenige ist, die sie vorgibt).

Heutzutage erkennt ein Zutrittssteuerungssystem in den meisten Fällen das „Wer“ aus dem Lesen einer Ausweis-Codierung. Das am weitesten verbreitete Verfahren ist die RF-Identifikation (RFID).

Leseverfahren

Die folgende Darstellung gibt einen Überblick über gängige Leseverfahren, deren Hauptkriterien, Vor- und Nachteile sowie Kombinationen mehrerer Verfahren.

RFID (Radio Frequency Identification) mit passiven Transpondern	
Leseverfahren:	Karte oder Transponder/Tag (jeweils ein Chip und eine Antenne in einem ID-Träger) wird durch ein hochfrequentes elektromagnetisches Feld mit Energie versorgt und überträgt Daten, auch bidirektional Weitere Bezeichnungen: berührungslos/Proximity (für Distanzen bis ca. 10 cm), Midrange (für Distanzen > 10 - 30 cm) und Handsfree (Vicinity) (für Distanzen > 30 cm) Aktuelle und normgerechte Technologie-Varianten sind: Mifare DESFire EV1/EV2/EV3, Legic advant® und im außereuropäischen Raum noch i-Class). Drei Generationen von RFID-Chips unterscheiden sich nach Frequenzbereich, Speicherkapazität und insbesondere Sicherheitsmaßnahmen, nämlich • RFID der ersten Generation - meist 125 kHz-Systeme (z.B. Miro/EM4102 und Hitag), die über eine werkseitige einmalige Chip-Seriennummer und teilweise über zusätzliche Daten identifiziert werden. Sie besitzen keine Authentifizierung und keine Verschlüsselung auf der Luftstrecke sowie keinen Zugriffsschutz auf den Speicher und weisen relativ kleine Datenmengen auf (ca.100-300 bit). • RFID der zweiten Generation (z. B. Legic prime, Mifare classic; i-Class,Hitag (125 kHz)) - meist 13,56 MHz Systeme, die über geheime Verschlüsselungsverfahren und Zufallszahlen authentifizieren (challenge/response Verfahren) und Zugriffsschlüssel mit speziellen Zugriffsverfahren besitzen. Die Kommunikation auf der Luftstrecke ist verschlüsselt. Die Datenmengen bewegen sich im Kilobit- bzw. unteren Kilobyte-Bereich. • RFID der dritten und jetzt aktuellen Generation (z. B. Legic advant, Mifare DESFire EV1/EV2/EV3) - meist 13,56 MHz-Systeme neuester Technik. Sie besitzen im Gegensatz zur zweiten Generation anerkannte Kryptoalgorithmen (z.B. AES oder 3DES) und mindestens 128 bit Schlüssellängen und sind somit nach heutigen Erkenntnissen sicher. Die Ablage der Schlüssel in den Lesestationen ist in sogenannten „secure elements“ (SAM) möglich und gilt ebenfalls als sicher. Die Datenmengen können bis zu mehrere Kilobyte betragen.
Lesedistanz:	Abhängig von der Baugröße des Identträgers (Ausweis/Transponder) und der Antenne in Empfänger/Sender i.d.R. 5 - 10 cm, einige Systeme bis über 50 cm, mit Verstärkern/Boostern auch i.d.R. 50 - 150 cm
Lesegeschwindigkeit:	Abhängig vom Verfahren und der Speicherkapazität
Frequenzen:	In Altprojekten 125 kHz und gemäß ISO/IEC 14443 und 15693 13,56 MHz

Speichergröße:	Bis mehrere kByte; hersteller- und verfahrensabhängig Neben flexiblen Schreib-Lese-Systemen sind am Markt auch Nur-Lese-Systeme verfügbar.
Dateninhalt und Speicherorganisation:	Herstellerspezifisch in Bereiche eingeteilt; einige Verfahren sind multiapplikationsfähig (z.B.: Mifare DESfire EV1/EV2 und Legic advant), bei anderen (z.B. Miro und Hitag) wird nur die Unikats- bzw. Seriennummer verwendet
Vorteile:	Lesung erfolgt berührungslos und praktisch verschleißfrei; hoher Bedienkomfort, hohe Lese-Sicherheit; Lesen ist weitgehend lageunabhängig; ID-Mittel sind in verschiedensten Bauformen verfügbar; unempfindlich gegen Feuchtigkeit, Staub, Schmutz, Fremdlicht; bei einigen Verfahren hohe Datenverschlüsselung möglich
Nachteile:	Funktioniert nicht hinter Metall und im Bereich starker Magnetfelder
Kombination mit	kontaktbehafteten Chipkarten, Barcode, Magnetstreifen, Infrarot, Induktiv, ...

RFID mit aktiven Transpondern

Leseverfahren:	Transponder-Karte oder Tag wird durch eine integrierte oder angeschlossene Spannungsquelle mit Energie versorgt und sendet Daten an die Leseinheit, wenn die Karte/Tag in deren elektromagnetisches Nahfeld kommt. Diese Systeme werden meist als Nur-Lese-Systeme angeboten. Andere Transponder-Bauformen werden vom Benutzer per Taste aktiviert.
Lesedistanz:	I.d.R. einige Meter (Longrange)
Frequenzen:	< 150 kHz, 433 MHz, 868 MHz, 2,45 GHz
Speichergröße:	10 - 20 kByte
Dateninhalt:	Anbieterspezifisch
Vorteile:	Große Reichweite durch aktiven Sender
Nachteile:	Begrenzte Batterielebensdauer; größere Kartenstärke von einigen Millimetern
Kombination mit	passiven RFID-Chips möglich

Biometrie*

Leseverfahren:	Unterschiedliche Verfahren: Fingerabdruck, Gesichtserkennung, Handvenenmuster, Iris, ...
Speichergröße:	Keine „Datenträger“ ist das persönliche Merkmal (z.B. Template des Fingers, Gesicht, Iris, etc.) der zu identifizierende Person. Wird dies auf dem Mitarbeiterausweis gespeichert (empfehlenswert!), ist die jeweilige Speichergröße des Templates zu beachten.
Dateninhalt:	Meist höherer Speicherbedarf im Zutrittssteuerungssystem oder auf der Chipkarte, wenn diese als persönlicher Datenträger verwendet wird, jedoch abhängig vom Speicherbedarf des persönlichen Merkmals (Template)
Vorteile:	Höheres Sicherheitsniveau; bei einigen Verfahren kein Ausweis erforderlich; Biometrie wird aber meist als Verifikation betrieben in Verbindung mit Identkarte oder PIN-Code

Nachteile:	Meist höherer Preis; längere Erkennungs-Zeiten möglich; 100 % Identifikations- und Verifikationsrate ist systembedingt (wie bei allen Erkennungsverfahren) nicht gegeben
Kombination mit	nahezu allen Leseverfahren möglich Abhängig von der Bauform der Antenne können auch RFID-Verfahren, z.B. Hitag mit Mifare, kombiniert werden.

* Siehe hierzu ergänzend das BHE-Papier „Biometrie - Was ist das?“

Verfahren mit geringer Bedeutung für die Zutrittssteuerung:

Barcode (als Strich- oder QR-Code)	
Leseverfahren:	Optisch mittels Scanner (Strichcode auch mit Stift oder Durchzugsleser)
Speichergröße:	In praktischer Anwendung bis zu 15 Zeichen; read only
Dateninhalt:	Numerisch/alphanumerisch
Vorteile:	Sehr einfach mit Drucker zu erstellen; Ausweis oder Belege sehr preisgünstig; unempfindlich gegen elektromagnetische Felder; Kopierschutz durch Infrarotfolie
Nachteile:	Code nur lesbar, kann kopiert werden, nur für Besucherausweise nutzbar
Kombination mit	Magnetstreifen, Induktiv, Infrarot, Berührungslos, Chipkarten

Sonstige Verfahren wie Magnetstreifen oder kontaktbehaftete Chipkarten haben für die Zutrittssteuerung keine Bedeutung!

Gegenüberstellung der gängigsten Identifikationsverfahren

Der zuverlässigen, sicheren und schnellen Identifikation der Benutzer einer Zutrittssteuerung kommt eine herausragende Bedeutung zu. Besonders auf eine ergonomisch gute Bedienung des Systems ist zu achten, um bereits mit der Systemeinführung die Akzeptanz der Anwender zu gewinnen.

Relevante Kriterien bei dem ausgewählten Lese-/Identifikationsverfahren sind u.a. die Einsatzbereiche/Anwendungen, Flexibilität, Verschleiß/Haltbarkeit, Sicherheit, einfache Handhabung und der Gesamtaufwand zur Erstellung und logistischen Betreuung der Ausweise über einen i.d.R. längeren Zeitraum.

1. Identifikation mittels PIN, Ausweis oder Transponder:

- Wie bereits erwähnt, wird ein PIN-Code als alleiniges Identifikationsmittel (ID-Mittel) in Deutschland kaum eingesetzt.

Ein PIN-Code als geistiges Merkmal in Verbindung mit einer Karte kommt dagegen häufiger zur Verifikation zum Einsatz.



- Das gebräuchlichste ID-Mittel im Bereich der professionellen Zutrittssteuerung ist der RFID-Ausweis. Zunehmend werden Transponder (z.B. als Schlüsselanhänger) in unterschiedlichen Bauformen genutzt, die sich durch ihre Robustheit auszeichnen. Allerdings ist dabei die reduzierte Lesedistanz (< 5 cm) und geringe äußere Beschriftungsmöglichkeit zu beachten.

Die Karte wird, besonders als berührungsloser RFID-Ausweis bzw. als -Smartcard, auch in Zukunft eine führende Rolle spielen. Die meisten anderen Verfahren werden nur dort eingesetzt, wo besondere Umweltbedingungen oder Projekt-Kriterien vorliegen.

- Zunehmend werden für die Zutrittssteuerung Smartphones genutzt, die quasi als virtueller Ausweis dienen. Dafür werden die Berechtigungen als verschlüsselte, strukturierte Datei, z.B. in einer App, auf das Smartphone geladen.

Der Datenaustausch kann abhängig vom Anbieter, dem Lesertyp und der Smartphone-Parametrierung per Bluetooth oder mittels NFC erfolgen.



- Durch die Kombination mehrerer Codierungen auf einer Karte werden die Eigenschaften, Funktionen und Einsatzmöglichkeiten dieser verschiedenen Technologien vereint. So können die unterschiedlichsten kartengesteuerten Anwendungen, z.B. Zutrittssteuerung, Zeit- und Kantinendatenerfassung, auf einem Mitarbeiterausweis vereint werden, um dem Bediener mehrere ID-Träger in seinem Betrieb zu ersparen. Solche Kombinationsmöglichkeiten sind unbedingt mit dem Geräte- und Kartenhersteller zu klären.

2. Biometrie

Für die Zutrittssteuerung zu Hochsicherheitsbereichen wie einem Rechenzentrum muss die Identität einer Person eindeutig und unwiderlegbar festgestellt werden. Hierzu werden biometrische Systeme eingesetzt, die die Schwächen anderer Identifikationsarten, wie vergessener PIN oder verlorener bzw. beschädigter Ausweis, eliminieren. Bei solchen erhöhten Sicherheitsanforderungen werden meist Kombinationen aus „Wissen“, „Besitz“ und/oder „Eigenschaften“ zur Bestätigung der Identität (Verifikation) verwendet.



Bei der Auswahl des biometrischen Erkennungsverfahrens (z.B. Finger- print, Gesichts- oder Venenerkennung) sind die Einsatzbedingungen (z.B. Umgebung, Verfügbarkeit des Merkmals, Nutzer, etc.) zu beachten, da sie für die Verfahren, die Merkmalsdarstellung und auch für die Akzeptanz, die Datensicherheit und den Datenschutz erhebliche Unterschiede mit sich bringen.

Auch spielt die Erkennungszeit eine entscheidende Rolle. Da sie meist höher ist als die Buchungszeit, die mit einem herkömmlichen Ausweis erreicht wird, ist generell der verringerte Durchsatz pro Zutrittspunkt zu beachten.

In jedem Fall darf die Erkennungszeit die Geduld der Buchenden nicht überstrapazieren, denn die Akzeptanz eines Systems ist wesentlich von seinem Bedienungs- und Benutzungskomfort abhängig.

Die besondere Bedeutung der RFID-Technologie



Bild: Zutrittssteuerung im Außenbereich mit Identifikation an einem RFID-Leser

Wegen der einfachen Handhabung, des verschleißfreien, zuverlässigen Einsatzes und der großen Flexibilität bevorzugen Anwender zur Zutrittssteuerung schon seit Jahrzehnten RFID-Ausweise/Transponder. Mittlerweile wird alternativ oder ergänzend das Smartphone (mittels NFC oder Bluetooth) zur Personenidentifikation genutzt.

Die verschiedenen Verfahren werden von unterschiedlichen Herstellern angeboten. Alle anerkannten Verfahren funktionieren in der Praxis zuverlässig. Wenn mehr als die Serien-/Unikatsnummer UID eines Ausweises gelesen werden soll, sind einige wichtige Parameter zu beachten:

Verfahren:

Ist abhängig von der Anzahl und Art der Anwendungen sowie den individuellen Sicherheitsanforderungen. Die

erzielbare Sicherheit lässt sich im Rahmen der technischen Optionen des gewählten RFID-Verfahrens noch variieren durch Datenaufzeichnung, Datenübertragung, Zugriffsschutz über Schlüssel und ähnliche Mechanismen bis hin zu RFID-Prozessorkarten und eigenen Verschlüsselungs- und Sicherungstechniken.

Aufgrund der Bedeutung hat der BHE ein separates Info-Papier „Verschlüsselnde Kartentechnologie“ herausgegeben, das [hier](#) abrufbar ist.



Billige Karten und Tags bieten sehr **begrenzte Sicherheit**

- Miro: Kopieren der Seriennummer „im Vorübergehen“
- Mit Hitag2 kann Miro emuliert werden
- Hitag: Schreiben auf Karte
- Mifare classic / Legic prime: Verschlüsselung, Kopierschutz?

Mifare DESFire EV1/EV2/EV3

- AES-128 Verschlüsselung
- EV2 mit erweiterten Funktionen
- wie Schutz vor Relay-Attacken über Zeitstempel
- Im Vergleich zum MIFARE DESFire EV2 verfügt der MIFARE DESFire EV3 über eine größere Lesereichweite und höhere Transaktionsgeschwindigkeit. Er bietet zusätzliche Funktionen.

Legic advant

- DES/3DES Verschlüsselung
- Master/Token Prinzip

Sicherheit bei RFID-Ausweisen und Transpondern

System (Lesen und Schreiben):

Nur Lesen: ausreichend bei Nutzung nur in einer Anwendung, z.B. für Zutrittssteuerung mit geringen (Sicherheits-) Anforderungen und Zeiterfassung.

Lesen/Schreiben: für Bezahl-Dienste, Produktverfolgung, komplexe Online- und Offline-Zutrittssteuerung mit dynamischen/ temporären Zutrittsrechten für die offline-Terminals auf dem Ausweis oder biometrischen Daten bzw. Templates auf der Karte.



Antikollisions-Verfahren:

Bedeutung: mehrere Karten befinden sich gleichzeitig im elektromagnetischen Empfangsfeld. Sie werden automatisch sequenziell gelesen.



RFID-Normen

- ISO 14443 (Proximity Card, < 10cm): beschreibt die physikalischen Charakteristika (Abmessung [nur referenziert, da sie in anderen Normen festgelegt ist], Frequenz, Initialisierung, Antikollision, Übertragungsprotokoll) sowie den Einsatz von Shortrange-Ident-Karten
- ISO 15693, (Vicinity Card, < 1,5m), entsprechend für Vicinity Cards
- ISO 18000, Referenz-Architektur für alle Frequenzen (135 kHz - 5,8 GHz) speziell für den Einsatz von RFID in der Logistik

Personenidentifikation und Datenschutz

Das Bundesdatenschutzgesetz (BDSG) regelt den Umgang mit personenbezogenen Daten. Gemäß § 3 Abs. 1 des BDSG sind dies Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Zu den Daten bei denen ein Personenbezug anzunehmen ist, gehören bspw. gespeicherte Angaben zur Person, Ausweisdaten, das Passbild sowie biometrische Merkmale des Betroffenen.

Datenschutz bedeutet ein grundsätzliches Verbot der Erhebung, Verarbeitung und Nutzung personenbezogener Daten mit zwei Ausnahmen:

1. Der Betroffene gibt seine ausdrückliche Zustimmung oder
2. Es existiert eine Vorschrift (Gesetz, Tarifvertrag, Betriebsvereinbarung), die die Verarbeitung regelt.

Werden biometrische Daten erhoben, gelten die verschärften Anforderungen aus Art. 9 DS-GVO (Datenschutz-Grundverordnung), wobei insbesondere folgendes zu beachten ist:

- Die Rohdaten auf Referenzdaten (Templates) müssen reduziert werden, um weitere Rückschlüsse auf persönliche Merkmale und Eigenschaften zu vermeiden.
- Eine zentrale Speicherung dieser Daten sollte vermieden werden.



Die Verifikation am Kontrollpunkt durch den Vergleich gespeicherter Templates auf dem Mitarbeiterausweis ist einer Identifikation durch Abgleich mit im System hinterlegten Identitätsdaten vorzuziehen.

- Durch Verschlüsselung und ein Berechtigungsmanagement sollte ein unautorisierter Zugriff auf diese Daten vermieden werden.
- Prüfung der Erforderlichkeit: Biometrische Zutrittssteuerung kommt zum Einsatz, wenn alternative bzw. klassische Zutrittssysteme nicht die erforderliche Sicherheit hinsichtlich der Verhinderung eines unberechtigten Zutritts bieten können. Beispiel: Zutritt zu einem Hochsicherheitsbereich wie einem Rechenzentrum.

Zutrittssteuerung im BHE

Der *BHE-Fachausschuss Zutritt* bearbeitet aktuelle Themen der Zutrittssteuerung und entwickelt zahlreiche praxisnahe Papiere. Eine Übersicht finden Interessenten *hier*. Die Papiere stehen zum freien Download bereit oder können in gedruckter Version in der BHE-Geschäftsstelle angefordert werden.

Im Rahmen der *Weiterbildungsinitiative* des BHE werden regelmäßig Fachseminare im Bereich der Zutrittssteuerung angeboten.

Ausführliche Erklärungen zum Thema „Personenerkennung“ bietet z.B. das BHE-Seminar „Zutrittssteuerung und Identifikationsmanagement“.



BHE-Praxisratgeber Zutrittssteuerung

Der Praxis-Ratgeber Zutrittssteuerung erläutert das komplexe Thema der Zutrittssteuerung in einfacher und verständlicher Weise.

Der Ratgeber soll Errichter, Planer und Anwender bei ihrer täglichen Arbeit unterstützen und ihnen einen echten Mehrwert bieten. Neu- und Quereinsteigern der Zutrittssteuerung kann er als fundierte Einführung in das Thema dienen, Fortgeschrittenen als nützliches Nachschlagewerk.

Hierbei wurde sehr viel Wert auf das Feedback der Leser gelegt und darauf aufbauend neben zahlreichen Erweiterungen, Aktualisierungen und Verbesserungen auch das neue Kapitel „Projekte und Anwendungsbeispiele“ aufgenommen.

Weitere Infos

Der Inhalt wurde mit größter Sorgfalt zusammengestellt und beruht auf Informationen, die als verlässlich gelten. Eine Haftung für die Richtigkeit kann jedoch nicht übernommen werden.

BHE e.V.

Feldstr. 28
66904 Brücken

Telefon: 06386 9214-0
Telefax: 06386 9214-99

Internet: www.bhe.de
E-Mail: info@bhe.de