RFID, UHF, QR-Code, Biometrie und virtueller Ausweis

Identifikationsmedien für den Zutritt im Vergleich

Komplizierte Schlüsselverwaltung ade – eine elektronische Zutrittskontrolle löst die Aufgabe viel eleganter. Die Frage ist jedoch: Welches Identifikationsmedium eignet sich für welche Art von Zutrittskontrolle. Die verschiedenen Technologien unterscheiden sich in ihren Funktionen und im Sicherheitsniveau. Im Folgenden stellen wir fünf verschiedene Identifikationstechnologien vor, die sich für Zutrittskontrolle nutzen lassen.

1. Mitarbeiterausweise mit RFID

RFID hat sich als Standardmedium für die Zutrittskontrolle etabliert und ist in zahlreichen Unternehmen schon seit vielen Jahren im Einsatz. Um hier auf der sicheren Seite zu sein, ist es notwendig, die eingesetzte Technologie regelmäßig auf Aktualität zu prüfen. Einige RFID-Verfahren wurden bereits gehackt und sollten daher nicht mehr in Zutrittssystemen genutzt werden. Gerade bei Zutrittskontrolle ist diese Nachlässigkeit fatal, da dadurch die Sicherheit des Systems gefährdet wird. Aber nach dem Motto „Never change a running system" scheuen viele Betriebe vor einer Modernisierung zurück. Im Sinne eines proaktiven Risikomanagements lohnt es sich unbedingt, einen Umstieg auf eine neuere RFID-Technologie wie Mifare DESFire EV2/3 oder Legic Advant anzugehen. Dies gilt nicht nur für die Ausweise, sondern auch die installierte Zutrittshardware. Auch hier bieten aktuelle Modelle Vorteile, wie z.B.:

- Kombinationsmöglichkeiten von vernetzter Zutrittskontrolle mit abgesetzten mechanischen Schließsystemen, z.B. auf Basis von OSS.
- Schnellere Reaktionszeiten am Lesegerät für das Buchen und Schreiben mit Identifikationsmedien.
- Neue Multifunktionsleser erlauben die parallele Nutzung von zwei Leseverfahren, so dass eine Migration auf aktuelle Technologie im laufenden Betrieb umzusetzen ist.
- Nicht zuletzt bieten moderne Hardware-Systeme die Möglichkeit, die Geräte in einer Cloud-Umgebung zu betreiben. Dies ermöglicht eine flexiblere und effizientere Verwaltung der Zeit- und Zutrittssysteme.

2. UHF-Transponder

Soll der Lesevorgang eines Ausweismediums über eine größere Distanz funktionieren, reicht RFID nicht aus. Hier bewähren sich UHF-Leser, z.B., um Lagertore zu öffnen oder die Zufahrt zu Parkgaragen zu ermöglichen. Sie arbeiten in der Regel auf der Frequenz von 865,6 bis 867,6MHz und werden mit passiven UHF-Transponder-Medien bedient. Sie sind z.B. als Klebe-Transponder verfügbar, die direkt ins Fahrzeug geklebt werden können. Wie Autobahn-Vignetten sind sie mit einer Einmal-Beschichtung ausgestattet, so dass sie nicht abgelöst und weitergegeben werden können. Diese UHF-Aufkleber kommunizieren in einer Distanz von bis zu 8m. Für Fahrzeuge in der Logistik, wie Gabelstapler oder Ameisen, eignen sich Transponder-Tags im Kunststoff-Gehäuse (HD-Tags). Durch ein zusätzliches Montageblech lassen sie sich an geeigneter Stelle anbringen. Die Metallplatte bringt den zusätzlichen Vorteil, dass sie die Reichweite des Transponders verstärkt – so wird eine Distanz von bis zu 15m erreichbar. Für sicherheitskritische Anwendungen sind UHF-Transponder mit verschlüsselter Datenübertragung erhältlich.

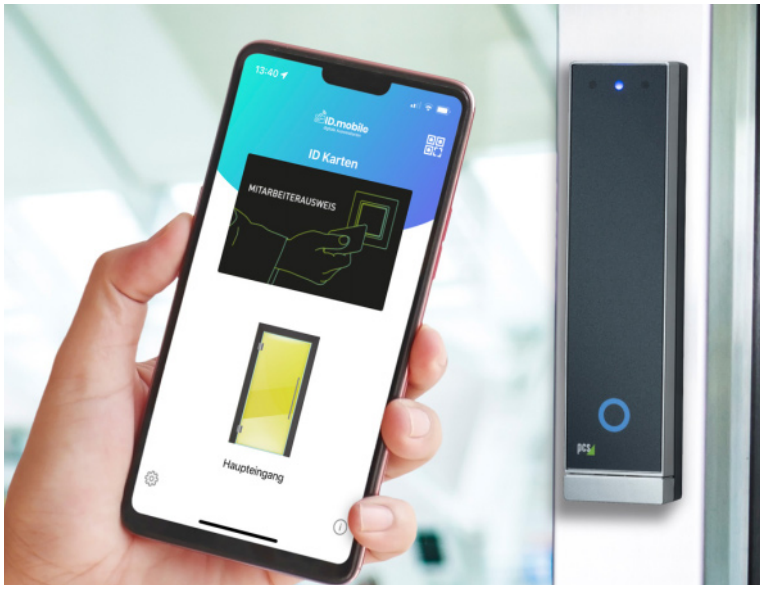
Bilder der Doppelseite:

3. QR-Code-Tickets

Eine schnelle Lösung für nur temporär genutzte Ausweise stellt die Nutzung eines QR-Codes dar. Dieses unkomplizierte Identifikationsmittel ist besonders kostengünstig. Es beinhaltet eine Zutrittsprofilnummer in grafischer Form und kann nach Bedarf auf Papier ausgedruckt oder auf einem Smartphone dargestellt werden. Damit lassen sich bequem einmalige Zutritts- oder Zufahrtsgenehmigungen regeln, denn eine persönliche Übergabe ist nicht notwendig. Der temporäre Ausweis erhält eine begrenzte Gültigkeit im System, so dass die Gültigkeit automatisch erlischt. Aus Sicherheitsgründen ist das Identifikationsmedium nur für temporäre Zutrittsrechte mit geringem Schutzbedarf zu empfehlen. Um sie in einem Zutrittssystem zu verwenden, können externe QR-Code-Leser über eine USB-Schnittstelle an herkömmliche Zutrittsleser angebunden werden.

4. Biometrische Identifikation

Zur Absicherung von besonders schützenswerten Zonen reicht ein Standard-Zutrittsmedium nicht aus, denn Karten können weitergegeben oder verloren werden. Besser ist es, auf ein Identifikationsmerkmal zu vertrauen, dass direkt mit der Person verknüpft ist. Hier ist Biometrie das Mittel der Wahl, denn die individuellen körperlichen Merkmale einer Person sind einmalig und können nicht verändert oder manipuliert werden. So ist im Hochsicherheitsbereich nach VdS-Richtlinie 2358 (ZKA Klasse C) eine 2-Faktor-Authentifizierung vorgeschrieben, um einen Kartenbesitzer eindeutig zu identifizieren. Dies kann sehr gut mit Handvenenerkennung erfolgen. Eine Person meldet sich über die Karte an und identifiziert sich am biometrischen Leser zusätzlich durch das Vorhalten der Handinnenseite. Der Abgleich des Handvenenmusters am Venenscanner erfolgt schnell und berührungslos gegen das auf der Karte gespeicherte Muster. Der Einsatz der Handvenenerkennung hat sich für hochsichere Zutrittskontrolle bewährt, z.B. auf Flughäfen, in Rechenzentren oder KRITIS-Einrichtungen. Allerdings muss der Einsatz biometrischer Zutrittssteuerungssysteme in Deutschland aufgrund der Datenschutz-Grundverordnung (DSGVO) mit einem berechtigten Interesse begründet werden. Dies stellt sicher, dass die Privatsphäre der Personen gewahrt wird und die Daten in Übereinstimmung mit den gesetzlichen Vorschriften verarbeitet werden.



5. Virtueller Smartphone-Ausweis

Immer öfter wünschen sich Kunden, das Smartphone zur Zutrittskontrolle zu nutzen. Um hier ein hohes Sicherheitsniveau zu erreichen, muss ein sogenannter virtueller Ausweis erstellt werden und in einem geschützten Container bereitgestellt werden. Dies ist z.B. über ein verschlüsseltes Neon-File möglich. Dieser virtuelle Ausweis kann mittels Bluetooth Low Energy (BLE) von kompatiblen Zutrittslesern ausgelesen werden. Das Sicherheitslevel ist dabei vergleichbar mit aktuellen RFID-Technologien. Der verschlüsselte Container speichert die Ausweisdaten und schützt sie vor externem Zugriff – auch wenn das Smartphone verloren geht. Wird das Smartphone gestohlen oder gehackt, können die Ausweisdaten nicht ausgelesen werden. Dieses Verfahren hat Vorteile, wenn Türen freigegeben werden sollen, ohne dass ein Ausweis physisch übergeben werden kann. Virtuelle Ausweise für das Smartphone können per E-Mail verschickt werden. Dies spart Zeit und Geld, gerade bei verteilten Infrastrukturen und einer zentral organisierten Ausweisverwaltung.

Zusätzlicher Tipp

Um das Zutrittskontrollsystem weiter sicher zu betreiben, sind ein regelmäßiges Risikomanagement und eine fachmännische Überprüfung der aktuellen Installation empfohlen. Denn nicht nur die eingesetzten Identifikationsmedien müssen aktuell sein, auch die installierte Hardware muss regelmäßig mit Software-Sicherheitsupdates aktualisiert werden. ■

Susanne Plank
PR und Content Marketing
PCS Systemtechnik GmbH
www.pcs.com