Bilder: Sesamsec

Lesegeräte für die RFID-basierte Zutrittskontrolle

Systeme für die Zutrittskontrolle und Einbruchmeldetechnik auf der Basis von RFID (Radio Frequency-Identification) kommen in zahlreichen öffentlich oder gewerblich genutzten Gebäuden zum Einsatz. Eine zentrale Komponente solcher Lösungen sind die eingesetzten Lesegeräte. Ihre Technologie trägt entscheidend dazu bei, wie sicher, nutzerfreundlich und flexibel das System ist. Um eine nachhaltige Investitionsentscheidung zu treffen, ist bei der Auswahl der Geräte daher eine Reihe von Aspekten zu beachten.

Carsten Hoersch

Berührungslose Anwendungen auf der Basis von RFID haben sich sowohl in der Einbruchmeldetechnik als auch in Zutrittsanwendungen etabliert, um Assets und Menschen zu schützen. Einbruchmeldeanlagen werden über RFID-Leser mittels Transponder, zum Beispiel in Form eines Mitarbeiterausweises, scharf und unscharf geschaltet. An Türen wird auf dieselbe Weise der Zutritt freigeschaltet und in beiden Fällen der Nutzer authentifiziert. Damit die Systeme ihre Funktion dauerhaft zuverlässig erfüllen und die Akzeptanz der Nutzer erhalten, sollten die verwendeten Lesegeräte Sicherheit mit Komfort verbinden und ein hohes Maß an Flexibilität bieten. Dies gilt für Neuinstallationen ebenso wie für die Migration eines bestehenden Lesersystems. Denn dieses lässt sich durch den Austausch der Geräte durch neue, leistungsfähige Leser ausbauen, um aktuellen und kommenden Anforderungen gerecht zu werden. Die Verdrahtung sowie die weiteren Komponenten des Systems können dabei in der

Autor:
Carsten Hoersch ist Managing Director bei der Sesamsec GmbH in Merching.

Regel beibehalten werden. Lösungsanbieter im Bereich Zutrittskontrolle und Einbruchmeldetechnik können Gebäudebetreiber bei der Migration unterstützen und Optionen für den Umstieg aufzeigen.

Folgende Kriterien sollten bei der Wahl der Leser berücksichtigt werden: Die Möglichkeit, Leser zu verschlüsseln sowie die Option, mobile Berechtigungsnachweise einzusetzen und ein breites Spektrum an Transpondertechnologien zu verarbeiten.

Sicherheit durch verschlüsselnde Lesegeräte

Ob Einbruchmeldeanlage oder Zutrittskontrolllösung: Verschlüsselnde Leser bieten die Option, sowohl für den Transponder als auch das Lesegerät Kryptoverfahren einzusetzen. Damit erhöht sich die Sicherheit des Gesamtsystems erheblich. Um dies in der Praxis zu erreichen, muss bei kryptografischen Lesern die Verschlüsselung allerdings auch tatsächlich aktiviert werden. In der oft eingestellten „Standardbetriebsart" wird lediglich die Unikatsnummer (UID) der Karte unverschlüsselt ausgelesen. Der Leser ist in diesem Fall jedoch nicht sicherer als ein unverschlüsselnd arbeitendes Gerät.

Die Verschlüsselung kann entweder am Lesegerät oder aber über die angeschlossene Auswerteeinheit aktiviert werden. Dies hängt in der Regel von der Komplexität der Schnittstelle zwischen Gerät und Auswerteeinheit ab. Ältere Datenschnittstellen arbeiten nur unidirektional. Das heißt, sie können nur Daten vom Gerät zur Auswerteeinheit übertragen und eignen sich daher nicht, um die Transponder zu konfigurieren und damit auf ein höheres Sicherheitsniveau zu heben. Aus diesem Grund sind bidirektional arbeitende Schnittstellen vorzuziehen. Sie

Viele Menschen bevorzugen heute digitale Berechtigungsnachweise auf dem ohnehin ständig griffbereiten Handy

erlauben das Senden von Daten von der Auswerteeinheit zum Leser und somit auch eine Konfiguration desselben. Außerdem bieten diese höherwertigen Schnittstellen häufig die Option einer durchgängigen Verschlüsselung – also auch auf dem Kabelweg bis hin zur Auswerteeinheit.

Werden die Geräte verschlüsselnd betrieben, ist zu beachten, dass sich der Leseabstand zwischen Transponder und Leser beträchtlich verringern kann. Das bedeutet, der Transponder muss in diesen Fällen unter Umständen direkt an den Leser gehalten werden, wodurch der Nutzerkomfort beeinträchtigt wird. Gründe für einen geringen Abstand können die Montage des Lesers in metallischer Umgebung oder der Einsatz ungeeigneter Transponder sein. Für einen idealen Leseabstand bei verschlüsselnden Lesern ist auf die Transponderempfehlung des Herstellers zu achten.

Mit leistungsfähigen Lesegeräten lässt sich die Zutrittskontrolle und Einbruchmeldetechnik sicherer und komfortabel gestalten

Vorteile: Zum einen müssen keine Schlüssel oder Karten ausgehändigt werden. Zum anderen wird der Ausweis direkt auf das Smartphone des Nutzers geladen und kann bei Verlust oder Diebstahl unproblematisch gesperrt und in einem nächsten Schritt ersetzt werden.

RFID-Karte und Smartphone lassen sich in der Zutrittskontrolle als Identifikationsmedien ausgezeichnet kombinieren: Hybride Systeme arbeiten sowohl mit Karten als auch mit mobilen Technologien. So können je nach Bedarf problemlos sowohl physische als auch digitale Berechtigungsnachweise eingesetzt werden.

Zukunftsorientiert: Zutritt mit Smartphone und Karte

Nachdem RFID-Karten jahrzehntelang bewährter Standard bei der Zutrittskontrolle waren, zeichnet sich heute ein starker Trend zu mobilen Berechtigungsnachweisen ab. Denn statt eine physische Ausweiskarte mit sich zu führen, bevorzugen viele Menschen heute digitale Berechtigungsnachweise, sogenannte mobile Credentials, auf dem ohnehin ständig griffbereiten Handy, der Smart Watch oder als Wearable in Form eines Armbands.

Bei der mobilen Zutrittskontrolle wird zwischen zwei Übertragungsstandards unterschieden: Für den Standard BLE (Bluetooth Low Energy) benötigen Nutzer in der Regel eine App auf dem Handy, die ihnen den Zutritt ermöglicht – so ersetzt beispielsweise eine Hotel-App den Zimmerschlüssel. BLE kann auch überall dort verwendet werden, wo eine höhere Leserreichweite erforderlich ist, beispielsweise beim Öffnen von Parkplatzschranken.

Im Unterschied zu BLE ist bei NFC nicht immer eine herstellerspezifische App erforderlich. Stattdessen kann die Zutrittsberechtigung auch als mobiler Pass direkt im Smartphone-Wallet hinterlegt werden. Hier wird in der verschlüsselnden Variante eine „Mifare-DESFire"-Karte emuliert. Dadurch ergibt sich, wie von Karten bekannt, ein Leseabstand von wenigen Zentimetern. Eine solche Lösung ist daher überall dort ideal, wo klassische Zutrittsanwendungen eingesetzt werden. Die NFC-basierenden, schnell zu installierenden Wallet-Pässe eignen sich zudem besonders für temporäre Zugangsberechtigungen, wie Besucherausweise.

Digitale Berechtigungsausweise haben für die Nutzer und auch für die Betreiber von Zutrittskontrollsystemen

Flexibel: Unterstützung unterschiedlicher Transpondertechnologien

Neben mobilen Technologien sollten leistungsfähige Lesegeräte auch in der Lage sein, unterschiedlichste Transpondertechnologien zu verarbeiten. Denn RFID-Karte ist nicht gleich RFID-Karte. Unternehmen oder Organisationen mit mehreren, möglicherweise sogar länderübergreifenden Niederlassungen nutzen häufig von Standort zu Standort unterschiedliche Transpondertechnologien, um den Zutritt zum Gebäude zu regeln – das ist insbesondere dann häufig der Fall, wenn Systeme über einen längeren Zeitraum gewachsen sind. Um trotzdem unkomplizierte Zugänge für Nutzer wie Mitarbeiter, aber auch temporäre Besucher zu ermöglichen, ist eine flexible Lösung gefragt. Am Markt sind Multifrequenz-Leser verfügbar, die mit bis zu 60 gängigen Transpondertechnologien kompatibel und für den Einsatz in bis zu 110 Ländern weltweit zertifiziert sind. Ein solch breites Spektrum sorgt dafür, dass auch beim Hinzufügen oder beim Wechsel auf andere Transpondertechnologien die Kompatibilität mit den Lesern gegeben ist.

Fazit

Leistungsfähige Leser können einen wesentlichen Beitrag dazu leisten, Anwendungen in der Zutrittskontrolle und Einbruchmeldetechnik sicherer und komfortabler zu gestalten. Betreiber haben so die Chance, ein System neu zu installieren oder ein Bestehendes so zu modernisieren, dass es ihre Anforderungen und die der Nutzer heute und in Zukunft erfüllt.

www.sesamsec.com/de