Verschlüsselnde Kartentechnologien für die Einbruchmeldetechnik und Zutrittssteuerung

Berührungslose Kartentechnologien haben sich sowohl in der Einbruchmeldetechnik als auch in der Zutrittssteuerung durchgesetzt. Einbruchmeldeanlagen werden über entsprechende RFID-Leseeinheiten scharf/unscharf geschaltet, an Türen wird über den gleichen Weg Zutritt gewährt und in beiden Fällen wird der Nutzer erkannt. Es handelt sich hierbei zwar um sicherheitstechnisch unterschiedlich zu bewertende Ansätze, aber in beiden Fällen wird die Sicherheit der Gesamtsysteme durch Kryptoverfahren für Ausweis und Leser erheblich erhöht.

Neue VdS-Anforderungen

Seit dem 01.01.2017 gelten für berührungslose Kartenleser in der Einbruchmeldetechnik und Zutrittssteuerung geänderte VdS-Anforderungen.

Künftig muss in Anlagen der VdS-Klassen B und C auf der Luftstrecke (also zwischen Karte und Leser) eine verschlüsselnde Technologie eingesetzt werden, die die Forderung des VdS nach einem „erhöhten Schutz gegen Fernkopieren und Abhören“ erfüllt. Mit Fernkopieren ist ein „Kopierschutz“ für Kartentransponder gemeint, um ein Duplizieren von Berechtigungen zu verhindern. Mit Abhören ist ein Mitlesen der zwischen Karte und Leser über die Luftstrecke ausgetauschten Daten gemeint.

Bislang zugelassene, nicht verschlüsselnde Kartenleser wurden aufgrund der geänderten Anforderungen auf VdS-Klasse A zurückgestuft oder haben ihre Zulassung verloren.

Unverschlüsselnde Leser VdS-Klasse A sowie bei DIN VDE 0833 und DIN EN 50131

Unverschlüsselnd arbeitende Leseeinheiten können nach einer Einzelfallprüfung auf Antrag des Herstellers noch bis zum 31.12.2020 die VdS-Klasse A erhalten. Dies umfasst die 125 kHz-Leseverfahren wie z. B. EM 4200, sowie in der unverschlüsselnden Betriebsart die 125 kHz-Verfahren wie z. B. Hitag 1, 2, S. Auch Leseeinheiten mit 13,56 MHz-Verfahren wie Mifare Classic und Mifare DESFire, Legic Advant und Legic Prime können für den unverschlüsselnden Betrieb die Klasse A erhalten bzw. in Anlagen nach DIN VDE 0833 sowie DIN EN 50131 verwendet werden. In diesen Fällen wird nur die Unikatsnummer (UID) der entsprechenden Transponder ausgewertet.

Verschlüsselung muss für die Klasse B und C auch aktiviert sein

Um in der Praxis wirklich ein Plus an Sicherheit zu erreichen, muss die Verschlüsselung am Leser auch aktiviert werden. In der oft eingestellten „Standardbetriebsart“ wird lediglich die Unikatsnummer (UID) der Karte unverschlüsselt ausgelesen und ist dann nicht sicherer als ein unverschlüsselnd arbeitender Leser. Die Verschlüsselung kann entweder am Leser oder aber über die angeschlossene Auswerteeinheit aktiviert werden. Dies hängt in der Regel von der Komplexität der Schnittstelle zwischen Leser und Auswerteeinheit ab. Ältere Leserdatenschnittstellen wie z. B. Wiegand oder Clock-Data arbeiten nur unidirektional. Sie können nur Daten vom Leser zur Auswerteeinheit übertragen und eignen sich daher nicht als Administrations-Schnittstelle zur Kartenkonfiguration. In diesen Fällen ist die Verschlüsselung zwischen Karte und Leser gekapselt und über die Kabelschnittstelle wird in der Regel eine nicht verschlüsselte Information zur Auswerteein-

heit gesendet. Andere, z. B. RS485-basierende Schnittstellen, können bidirektional arbeiten und erlauben somit auch ein Senden von Daten von der Auswerteeinheit zum Leser und somit eine Konfiguration des Lesers. Außerdem bieten diese höherwertigen Schnittstellen häufig die Option einer durchgängigen Verschlüsselung; also auch auf dem Kabelweg bis hin zur Auswerteeinheit. Der VdS fordert derzeit die Verschlüsselung zwischen Karte und Leseeinheit und eine Kabelführung im gesicherten Bereich.

Verschlüsselnde Leser VdS-Klasse B und C

Leser mit aktivierter Verschlüsselung auf der Luftstrecke können die VdS-Klasse B und C erhalten. Als besonders sicher werden Verfahren eingestuft, die mit einer 128-bit AES Verschlüsselung arbeiten. Dieses Verfahren kommt z.B. bei Mifare DESFire und Legic Advant serienmäßig zum Einsatz.

Auf ausreichenden Leseabstand der Karten/Transponder achten

Generell ist zu beachten, dass sich in der verschlüsselnden Betriebsart der Leseabstand zwischen Karte/Transponder und Leser beträchtlich verringern kann. Aus diesem Grund ist es besonders wichtig, die eingesetzten (verschlüsselnden) Karten/Transponder an den Lesern auf ihre Bedienbarkeit zu prüfen. Grund für einen unzureichenden Leseabstand können sein: Montage des Lesers in metallischer Umgebung oder ungeeignete Karten/Transponder mit einem zu geringen Leseabstand. Daher ist der Einsatz der vom Leserhersteller qualifizierten Karten/Transponder vorzuziehen.

Migration

Eine Migration eines bestehenden Lesersystems, z. B. von einem nicht verschlüsselnden Leseverfahren zu einem verschlüsselnden, unter weiterer Verwendung der bestehenden Auswerteeinheiten, kann möglich sein. Hier ist zu beachten, dass die neuen Leseeinheiten die im Einsatz befindliche Leserdatenschnittstelle und das passende Protokoll der Auswerteeinheit unterstützt. Gerade in der Einbruchmeldetechnik werden in Deutschland selten Standardschnittstellen wie z. B. Wiegand, oder das RS485-basierende OSDP-Protokoll verwendet, sondern herstellerspezifische Lösungen. Selbst innerhalb der zuvor genannten Standardschnittstellen gibt es auf Protokollebene häufig individuelle Besonderheiten, die einen Einsatz eines Lesers mit „Standardschnittstelle“ an einem System mit der gleichen Schnittstelle unmöglich machen. Hier sollte dringend mit den jeweiligen Herstellern Rücksprache gehalten werden. In der Regel arbeiten die Auswerteeinheiten der Hersteller mit der unveränderten Leserdatenschnittstelle. Es ist also sicherzustellen, dass die neuen, verschlüsselnden Leser das identische Schnittstellenprotokoll wie die zuvor eingesetzte Technik unterstützen. Werden diese Punkte berücksichtigt, kann durch ein Tauschen der Leseeinheiten und Karten die Anlage auf den aktuellen Stand gebracht und damit die VdS-Anforderungen zur Verschlüsselung auf der Luftstrecke erfüllt werden.

Bidirektionale Schnittstellen sind zu bevorzugen

Ein großer Nachteil von unidirektionalen Schnittstellen wie z. B. Clock-Data/Wiegand ist, dass nur Daten vom Leser zur Auswerteeinheit unverschlüsselt gesendet bzw. abgeholt werden können. Bei einem auf der Luftstrecke verschlüsselnden Leser mit unidirektionaler Schnittstelle zur Auswerteeinheit wird die Verschlüsselung im Leser gekapselt administriert und durchgeführt. Danach wird über die Datenschnittstelle eine einfache Unikatsnummer an die Auswerteeinheit übertragen. Damit z. B. Datensätze zum Leser gesendet und somit etwa die Verschlüsselung von der Auswerteeinheit und damit dem Bedienprogramm des Systems administriert werden können, sind bidirektionale Schnittstellen notwendig, in deren Protokollen diese Funktionalitäten unterstützt werden. Mit dieser Technologie kann dann ggf. auch die Kommunikation auf der Datenleitung verschlüsselt werden.

BHE Bundesverband Sicherheitstechnik e.V., Feldstraße 28, 66904 Brücken, Tel.: 06386 9214-0, Fax: 06386 9214-99, info@bhe.de, www.bhe.de