sesamsec

# Readers for RFID-based access control

## Current technology increases security and user acceptance

**Systems for access control and intrusion detection based on RFID (Radio Frequency Identification) are used in numerous public or commercial buildings. RFID readers are a central component of these systems. Reader technology makes a decisive contribution to how secure, user-friendly and flexible the system is. In order to make a sustainable investment decision, a number of aspects must therefore be taken into account when selecting the devices.**

Contactless applications based on RFID have established themselves in both intrusion detection technology and access applications to protect assets and people. Intrusion detection systems are armed and disarmed via RFID readers using transponders, for example, in the form of an employee ID card. At doors, access is enabled in the same way, and the user is authenticated in both cases. To ensure that the systems perform their function reliably over the long term and gain user acceptance, the readers selected should combine security with convenience and offer a high degree of flexibility. This applies to new installations as well as to the migration of an existing reader system. A smooth migration may be achieved by replacing the devices with new, high-performance readers to meet current and future requirements. The wiring and other components of the system can usually be retained. Solution providers in the field of access control and intrusion detection technology can support building operators during the migration and show them options for the changeover.

The following criteria should be considered when choosing readers: the ability to work encrypted with cards as well as with the connected controller and the ability process a wide range of transponder technologies as well as mobile credentials.

**Security through encrypting readers**

Whether burglar alarm system or access control solution: encrypting readers offer the option of using crypto processes for both the transponder and the connected controller. This significantly increases the security of the overall system. To achieve this in practice, however, encryption must actually be activated for cryptographic readers. In the "standard operating mode" that is often set, the unique identifier number (UID) of the card is simply read out without encryption. In this case, however, the reader is no more secure than an outdated 125 kHz reader.

Encryption can be activated either on the reader or via the connected controller. This usually depends on the complexity of the interface between the device and the controller. Older data interfaces like Wiegand only work unidirectionally. This means that they can only transmit data from the device to the controller and are therefore not suitable for configuring the transponders and thus raising them to a higher security level. For this reason, bidirectional interfaces are preferable. They allow data to be sent from the controller to the reader and thus also allow the latter to be configured. In addition, these higher-quality interfaces often offer the option of end-to-end encryption—i.e., also on the cable route up to the controller.

If the devices are operated in encrypted mode, it should be noted that the reading distance between the transponder and reader may be considerably reduced. This means that in these cases, the transponder may have to be held directly against the reader, which is less user-friendly. Possible reasons for a short read distance can be the installation of the reader in a metallic covering or the use of unsuitable transponders. For an ideal read distance with encrypting readers, the transponder recommendation of the manufacturer must be observed.

**Future-oriented: Access with smartphone and card**

While RFID cards have been the proven standard for access control for decades, there is now a strong trend toward mobile credentials. Instead of carrying a physical ID card with them, many people today prefer to have digital credentials, so-called mobile credentials, on their cell phone or smartwatch, which is always at hand anyway.

A distinction is made between two transmission standards for mobile access control. For the BLE (Bluetooth® Low Energy) standard, users usually need an app on their cell phone to enable access—for example, a hotel app replaces the room key. BLE can also be used wherever a higher reader range is required, for example, when opening parking lot barriers.

Unlike BLE, NFC does not always require a manufacturer-specific app. Instead, the access authorization can also be stored as a mobile pass directly in the smartphone wallet. Here, a Mifare DESFire card is emulated in the encrypting variant. This results in a reading distance of a few centimeters, as is standard for cards. Such a solution is, therefore, ideal wherever classic access applications are used. The NFC-based, quick-to-install wallet passes are also particularly suitable for temporary access authorizations such as visitor passes.

Digital credentials have advantages for users and also for operators of access control systems. For one thing, there is no need to hand out keys or cards. On the other hand, the badge is loaded directly onto the user's smartphone and can be easily blocked in the event of loss or theft and reactivated on the replacement device.

RFID cards and smartphones can be conveniently combined as identification media in access control. Hybrid systems work with both cards and mobile technologies. This means that both physical and digital credentials can be used without any problems, depending on requirements.

**Flexible: Support for different transponder technologies**

In addition to mobile technologies, powerful readers should also be able to process a wide variety of transponder technologies. After all, not all RFID cards are the same. Companies or organizations with multiple, possibly even transnational, branches often use different transponder technologies from location to location to regulate access to the building—this is often the case when systems have grown over a longer period of time. In order to nevertheless enable uncomplicated access for not only employees but also temporary visitors, a flexible solution is required. Multifrequency readers are available on the market that are compatible with up to 60 common transponder technologies and certified for use in up to 110 countries worldwide. Such a broad spectrum ensures that compatibility with the readers is also guaranteed when adding or changing to other transponder technologies.

**Conclusion**

Powerful readers can make a significant contribution to making access control and intrusion detection applications more secure and convenient. Operators thus have the chance to install a new system or modernize an existing one so that it meets their requirements and those of the users today and in the future.

Author: Carsten Hoersch, Managing Director, sesamsec GmbH

In cooperation with:

building&automation

digital | elektrisch | qualifiziert