IDESCO

Take control of your overall security.

Secure access control system

How can I strengthen my overall system security?

RFID security systems have historically relied on cards and tags, readers communicating with them, the card data those readers shared with their hosting system, and of course, systems' users.

When tags or any other kind of credential data are left unprotected, it clearly puts a system's security at risk. For example, a few years ago, cloners and hackers began targeting cards' unprotected unique serial number (UID) data. Their attacks began multiplying once hackers realized UIDs could be easily cloned to a new card, providing anyone unauthorized entry.

Today, not surprisingly, all those older UID technologies were defeated years ago. Additionally, the equally old cable data transmission protocol, Wiegand, never had protection. Today, systems still employing either run substantial risks since neither is encrypted.

By contrast, modern card technologies protect card and system data behind powerful encryption methods, even up to 128-bit AES. That cipher remains functionally unbreakable today. For data transmitted from a reader to its host, the Security Industry Association (SIA) standardized protocol, OSDP, has been shown to provide a thoroughly secure solution against Wiegand exposure risks.

More secure cards and tags

Two types of technology securely encrypt cards and tags today: proprietary and open technology. Proprietary technologies are manufacturer-specific – they cannot be sourced from other manufacturers. By contrast, open technologies rely on common standards that any manufacturer may choose to support. If you choose proprietary technology, it will also force you to purchase all future readers and tags from that same supplier – regardless of whether their supply is constrained.

By contrast, open technology never forces you to rely on a sole supplier. You remain free to source products from any supplier participating in and supporting the standard you select – a wise sourcing and supply choice. Open technology is also a wise choice from a security perspective because multiple companies participate in developing it, securing its future. It is why we recommend MIFARE DESFire open technology. Under constant development, DESFire is continuously strengthening itself with new security features.

More secure data transmission

We believe the most secure solution for securing data transmitted between readers and systems is Security Industry Association's open-source data protection protocol (OSDPv2). OSDPv2 doesn't just robustly secure internal data transmission. It also supports convenient, feature-rich two-way communication in your system. For

Idesco Oy

Elektroniikkatie 4
90590 Oulu
Finland

Tel. +358 (0)20 743 4175
Email info@idesco.fi
idesco.fi

example, it lets you perform remote firmware updating or even reconfiguring of readers, centrally, from your system. Its securely encrypted two-way data flow can also support personalized responses when users transact.

Mobile access security

An increasingly popular new capability is letting users identify themselves with their mobile phones. This requires a door reader to not only transact conventionally, with tags or cards, but also recognize digital credentials embedded in users' phones, over Bluetooth or NFC. When the user approaches the door with their phone, the phone's mobile ID will be detected and read in a transaction that's as securely encrypted as a contactless payment.

Security Key Management

Today, all encrypted technologies encode readers, cards, tags and phones with security keys. These keys are what authenticate every transaction between readers and credentials. As a result, your responsibility, when choosing a technology, is to determine how your preferred technology supplier will classify ownership of your site's keys. Some suppliers, despite selling you open technology devices and transponders, still require retaining ownership of security keys for themselves. Their practice is explicitly intended to prevent you from buying additional devices or cards from another supplier – despite your open technology choice.

That is why we encourage end-customers and sites to retain security key ownership for themselves. Our management of customers' security keys is confined to device and transponder coding, archiving and storage according to the strictest information security practices. Yet whenever our customers choose to, they remain free to recover their security keys for their own management and use.

Pin Codes

The easiest way to prevent the use of cloned or stolen access cards is requiring that users authenticate to your system with a pin code as well. A pin code essentially functions as a basic second authentication factor. This second factor significantly enhances any system's security because it is independent of the card. The user's pin code gets verified in the system alongside their card credential, and their correspondence authenticates their legitimacy to the system.

Summary aspect of overall security

Overall security unavoidably demands careful consideration of all aspects. It never depends wholly on technology, but rather the entirety of its components, from data transfer protocols and encryption to human factors.

It means a system is only as secure as its weakest links. Encryption won't protect you when someone, inconvenienced by a locked door, inserts a brick to keep it open. By contrast, deploying convenient, easy-to-use readers, the practices of constantly updating and informing about security policy, together with monitoring user compliance, are how a responsible security manager can successfully strengthen their overall security.

We can help you to choose access control readers for your system! Please contact: sales@idesco.fi.

Idesco Oy

Elektroniikkatie 4
90590 Oulu
Finland

Tel. +358 (0)20 743 4175
Email info@idesco.fi
idesco.fi