(New Blog Post) How to identify if you have Prox Cards vs. Secure Smart Cards

Is your organization currently utilizing a physical access control system? The key components for any access control solution are the control panels (with access control software), the readers and the credentials. HID Prox, iClass and Seos Contactless Smart Cards are the most recognizable types of credentials issued to employees, contractors and other personnel who interface with physical access control systems on a daily basis.

Below we'll evaluate the pros and cons of each type of credential technology, so you can distinguish between the levels of security, as well as which fits your business needs the most:

125 kHz Low-Frequency Legacy RFID, Prox II, Proximity, ISO Prox & Clamshell Prox :

For a brief summary, prox technology was first introduced over 20 years ago and was not built with any form of encryption to keep RFID data secure. Keep in mind, this was prior to the introduction of smartphones and well before the concept of cloud-based data storage. The concern for securing data on proximity credentials was not the focus when RFID & Proximity technology first came out and it was secure while offering superior automation and security

compared to existing technologies like barcodes and mag stripes. However, these days industries have massively transitioned to cloud-based businesses operations, SaaS applications, and storing proprietary resources and data on the cloud. Unfortunately given this shift, we've seen a parallel increase of cybercrime. While many organizations still rely on low frequency technology for its long life, durability, and low cost, many IT & security teams are reevaluating the liabilities in these legacy systems.

Here's a quick look at why low frequency 125Khz prox cards are one of the most popular type of credentials along with some concerns to consider:

Pros:

- Convenient To Use – Low-frequency proximity and RFID cards, tags, and disks can fit into a wallet or purse or secured with a strap and clip as a photo ID badge. This technology offers an extremely consistent read range. Unaffected by body shielding or variable environmental conditions, even when close to keys and coins.
- Long Life – Passive RFID, no-battery design allows for an infinite number of reads. Active RFID, battery life that can last for up to 10 years!
- Durability – Keys and credentials are strong, flexible, and resistant to cracking and breaking.
- Low Cost – RFID technology is the most economic option for those who are looking to save on adding secure access control features.
- Read Range – There are options to extend the read range for both active and passive RFID credentials. More powerful readers can remain at a distance without interfering with broadcast signals. Boosters can strengthen the signal of a passive RFID credential so that it can be read from a distance.

Cons:

- Outdated Technology – Offers low security because proximity cards can be easily copied as original patents ran out years ago. Copies can be gained with easy to use online websites for duplication of credentials in addition to increased public access to low cost RFID kiosks in retail store locations.
- Security – No encryption on these legacy RFID chips which means the identifying information is constantly exposed to being read.
- Limited Upgrade Capability – Many of these readers and cards have been discontinued so you can't just add more to your system if growth or expansion is needed. Also, many of these are not compatible with newer and more secure solutions where integration is needed between multiple applications.
- Limitations for Administrators – Credentials can only be issued and written onsite whereas newer credentials can be rewritten or re-encoded with new data using secure technologies.

For any access control installation where security is a critical factor, not just efficiency or ease of use through automation, it is essential to use encrypted technology for RFID which is built into most newer applications. This high frequency, smart chip credentials are often referenced by the following names in different organizations:

13.56 MHz High-Frequency RFID with HID iClass & Seos Contactless Smart Cards and MIFARE DESFire:

Pros:

- Security – Cryptography offers unrivaled data and privacy protection with multiple layers of encryption on a smart chip. This ensures data cannot be swiped by random users without verification and authentication from the access control system.
    - Card Operating System – An actual operating system resides on the chip to process transactions for reading and writing data, not just emitting a signal with an ID number.
    - Structure – Use of strong encryption that creates a secure framework to protect access to key data on smart card credentials.
- Convenience and Adaptability – More advanced credentials can be leveraged for use on smart devices to access doors, gates, networks, and more. New form factors allow for flexibility including use on mobile devices, multi-tech cards, and adhesive tags. Each company can choose from a variety of credentials to support higher-level executives or doctors to differentiate team leaders from the rest of the workforce.
- Industry Specific Applications – With greater security built into smart card technology, newer applications have been developed beyond physical access control, including uses tailored for health care, education, government, hospitality, and other enterprise environments. To maintain compliance with federal standards, implementing secure identification is not a choice for many organizations, and the fines for not keeping systems secure far outweigh the cost of upgrading.
- Memory Options – Expanded memory to store applications on different sized smart card chips, typically 8KB or 16KB. For Java card-based platforms, some credentials

can be loaded in the secure memory area with available memory up to 144KB to support custom application development.

- Customizable Credential Solutions – Security teams can issue a mix of smart cards and mobile devices to meet employee preferences including Mobile ID, where a smartphone app acts just like a physical credential. When a physical card is needed, the latest credentials are built with durable composite construction to withstand extreme temperatures without affecting cardholder personalization details.
- Selectable Protocol – Core elements of contactless smart chips provide flexibility in select communication protocols and present a consistent interface to the access control reader, regardless of the communication method.
- Deployable Remotely – Many encrypted RFID technologies run on newer solutions that have the ability to receive software patches to be deployed by email, web downloads, or over the air, as opposed to having to fully reissue chip-based credentials. The remote deployment also enables IT, teams, to issue credentials for multi-factor authentication and mobile credentials to employees that never even step foot on campus. These options allow a hybrid workforce to stay secure in accessing proprietary data in a frictionless environment.
- Cost Savings – In many cases, the new security technologies don't even cost more than the comparable legacy technology. However, the cost of a security breach far exceeds the actual cost of upgrading to any secure technology that you plan ahead to put in place. Manufacturers offer regular promotions to help customers transition into newer secure technologies so they can move away from unsecured systems that put organizations at risk.

Cons:

- Cost to Upgrade – It can seem expensive to swap out legacy readers and credentials that are functional. And it can be tempting to delay implementation of new technology vs leaving things "as is". The long-term benefits of increased data

security, encryption, storage memory, key diversification, and authentication provide peace of mind knowing your business is secure.

Prepare your organization's security systems for the future by incorporating one of these contactless smart card technologies. If you have multiple locations or a complex setup, consider a multi-tech card to support the transition so that you start the process and buvild the infrastructure needed for a secure future.

Many organizations are surprised to find out that upgrading your legacy proximity badges to encrypted RFID doesn't even cost more on a per card basis. One of the most popular secure technologies requested by users of HID prox cards is iClass SEOS which actually costs less than the comparable version of composite ISO Prox II cards. Plus with SEOS, you have the option of extending your credentials to Mobile ID which means the same ID number from a physical card to your smartphone. This is even more important in today's hybrid environment where employers are looking for ways to support remote workers and the onsite workforce with universal tools.

Not sure if you are ready to make the switch? No worries, we are happy to help outline the process! Simply click here to speak with an ID Solutions Expert today to build a roadmap or request a quote for the upgrades you should consider for readers, scanners, or credential keys based on your organization's unique security needs.

Shop All RFID credential technology on IDSuperShop, here!