What to Know about Contactless Cards and Readers for Electronic Access Control Systems

By Scott Lindley, ***President, Farpointe Data***

More and more, companies that formally used only keys are now asking about keyless or electronic access control (EAC). Whether called badges, tokens or cards, they limit access to a facility to only those who possess one of these credentials. Countless companies take this a step further. In many cases, office workers can access their work areas but not areas such as food service while the exact opposite holds true for food service staff. Often, too, the security system is programmed to limit access only during specific time intervals, such as a few hours before and after a scheduled event. This is especially important for those venues that provide access credentials to vendors and/or delivery personnel.

A wide range of contactless cards and readers are available

Mullion style proximity reader with keypad

However, when you start exploring this world of keyless access, a whole new series of terms pop up - passive cards, active cards, proximity, smart cards, long range readers, Wiegand and so on. Let's demystify them.

Passive cards, the most popular, are powered by radio frequency (RF) signals from the reader. They do not have a battery of their own. Normally, they have a limited range of typically about four inches and must be held closely to the reader (hence, the term "proximity"). However, they can have a read range up to 20 inches. Typically, the larger the reader, the longer it will read. Also, readers which are mounted on walls are typically rectangular or square while other readers will fit on a mullion, that vertical element that forms a division between units of a window, door or screen.

The passive card and reader communicate with each other by an RF process called resonant energy coupling. Passive cards typically have three internal components - an antenna, a capacitor and an integrated circuit which holds the user's ID number or other data. The reader also has an antenna which constantly generates a short range RF field in a spherical orbit. When the card is placed within range of the reader, the card's antenna and capacitor absorb and store energy from the field and resonate. This powers the integrated circuit which sends the ID number to the card's antenna which transmits by RF signals back to the reader.

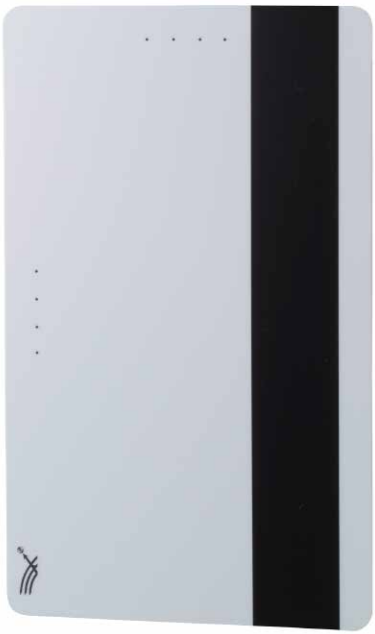
Active cards are powered by an internal lithium battery. As a result, they can produce a much longer read range measured in feet and yards, from 4 inches to 15 feet. Its integrated circuit contains a receiver and transmitter that uses the battery's power to amplify the signal so that the active card can be detected from farther away. The longer read ranges and that spherical orbit creates a problem that active cards can face. Several readers and cards could end up conversing with each other, creating a sort of communication mayhem.

What is the most important thing you need to know about all this? Pick the card that works best for the application and make sure you that you are using the right type of reader for the card.

What to Know about 125 KHz Proximity Cards and Readers

The 125 KHz proximity card and Wiegand standards currently constitute the majority of the card-based keyless access.

There are three main reasons why proximity cards and readers are still today's most widely used access control technology. First of all, there is no contact between cards and the reader. This eliminates the wear-and-tear factor. Secondly, proximity readers can be made very durable or even hidden into the wall to make them relatively vandal-resistant. Some are even bullet resistant. And, thirdly, for almost 20 years, they have provided the most cost efficient front-end for an access control system. Thus, there is a massive installed base.



PSM-25 - ISO standard size/multi-tech proximity card

Proximity card readers communicate to the rest of the access control systems in various protocols, such as the Wiegand protocol, a de facto wiring standard which arose from the popularity of Wiegand effect card readers in the 1980s. Another popular protocol is the ABA Track II interface, a holdover from magnetic stripe card technology. Again, you don't need to know what these protocols do or how they work. You just need to use the interface that the rest of the system uses.

When selecting a proximity card and reader for your customers, there are several things to check. First of all, make sure they comply with one or both of the afore-mentioned two main interface protocols so that the cards and readers will interface with a wide range of electronic access control systems. Also, order readers that support several proximity card and tag technologies/brands. Check to see if the reader electronics are secured with tamper- and weather-resistant epoxy potting. This is important as, often, the readers are outdoors or in wet or dusty environments not suitable for electronics. Look for a lifetime warranty.

Some customers will want what is called multi-factor verification. That means that they want a system that adds more than just a card (what you have) to activate the door lock. The most popular is the card/keypad reader. This makes anyone

Wall mounted proximity reader

requesting entrance to show the system what they have, a card, and what they know, a PIN (personal identification number).

What to Know about 13.56 MHz Smart Cards and Readers

As proximity became the predominant credential technology over the last decades, contactless smart cards will augment proximity over the next three to five years. At often a cost comparable to proximity card systems, smart card systems may be more secure and can be used for applications beyond access control, such as tool checkouts, the company cafeteria and so on.

All the leading smart card providers conform to ISO standards. ISO 14443 cards operate from zero to four inches while ISO 15693 cards may provide longer ranges, something comfortable for the user and assuring a positive read. Be aware. There are proprietary, non-standard-based smart card technologies that could bind you to a single-supplier dependency and potentially restrictive pricing and delivery structures. Only in certain circumstances do you want to consider them.

The next term you must look for is "MIFARE DESFire EV1." We could go into a deep technological explanation but, suffice it to say, MIFARE DESFire EV1 has become the contactless digital RFID technology benchmark for smart cards. MIFARE is the gateway to a series of security levels. That's a whole new article but really not that complicated. Ask your manufacturer for a quick run-through so you pick the right level of security for your customer.

As with proximity cards, you will also want to assure that the readers comply with the Wiegand communication standard. Review what to look for in proximity cards again. Basically, it's the same list - potted, different sizes, card plus keypad, and so on.

What to Know about OSPD

The Open Supervised Device Protocol (OSDP) is a communication standard adopted by the Security Industry Association (SIA) that lets security equipment, such as card and biometric readers from one company interface easily with control panels and equipment from another manufacturer. In other words, OSPD fosters interoperability among security devices. It also adds sophistication and security benefits through features such as bi-directional communication and read/write capabilities. A two-way channel paves the way for forward-looking security applications such as the handling of advanced smartcard technology, PKI, and mobile device access. Not only does it provide a concise set of commonly used commands and responses, it eliminates guesswork, since encryption and authentication is predefined.

In other words, OSDP helps ensure that numerous manufacturers' products will work with each other. Interoperability can be achieved regardless of system architecture. For instance, the specification can handle smartcards by constantly monitoring wiring to protect against attack threats and serves as a solution for high-end encryption such as required in federal applications. The specification for handling LEDs, text, buzzers and other feedback mechanisms provides a rich, user-centric access control environment.

What to Know about 433 MHz Transmitters and Receivers

Note that the terms "transmitters and receivers" are used in place of "cards and readers." The receivers support either 2-button or 4-button transmitters from ranges up to 200 feet. Each button outputs transmitter data, the user's ID number or other data, over separate Wiegand outputs yet the receiver installs just like a standard proximity reader for easy integration with popular access control systems.

They are a terrific solution for long range access control applications such as gates and vehicle barriers, moving aircraft in and out of secure hangars, arming and disarming alarm systems as well as situations calling for emergency duress. Instead of using a card, which could activate more than one device or door at a time, the transmitter holder selects exactly the mechanism to be immediately triggered.

Available in either a two- or four-button configuration and equipped standard with a potted proximity or contactless smart card module, the transmitter can also be used as a traditional, presentation-style access credential. For example, a button may be pressed to activate a long range application, such as a gated parking barrier, and then be

Long Range receivers and transmitters

presented to a proximity reader to allow entry through a door and into the building.

What to Know about Contactless Cards and Fobs

The different technologies use somewhat different cards but they all tend to work in the same manner.

Most proximity manufacturers provide one of three types of cards: standard light, image technology and multi-tech card. The standard light proximity card is a clamshell design, meaning that there are two connected sides sealed together to hold the electronics. An image technology card is a slightly thicker card appropriate for dye sublimation printing. Lastly, the multi-tech card is a proximity card the same size as a credit card that can or not have a magnetic stripe on it. It is commonly referred to as an ISO standard size.

There are two main types of smart cards. The clamshell contactless smartcard is an ISO14443-compliant card with a 1K-byte memory. More memory may be added. The ISO contactless smartcard is an ISO14443-compliant card with a 1K-byte memory. It, too, can be ordered with more memory. Manufactured from glossy PVC, it is appropriate for dye sublimation imaging.

Keyfobs are also available in both proximity and smartcard technologies. They are often used in place of cards, being designed to be carried on a key ring. The most durable typically include a brass reinforcing eyelet.

What to Know about Preventing Hacking and Duping of Your Card System

The bad guys have figured out how to capture and use card-based information to fool the system and let the unauthorized in by using skimming, eavesdropping or relay attacks. Skimming occurs when the attacker uses his reader to access information on the victim's RFID token without consent. An eavesdropping attack occurs when an attacker can recover the data sent during a transaction between a legitimate reader and a token. A successful relay attack lets an attacker temporarily possess a 'clone' of a token, thereby allowing him to gain the associated benefits. Using any of these relatively inexpensive methods will let an unauthorized person in.

Adding to the problem is that Wiegand, the industry standard over-the-air protocol commonly used to communicate credential data from a card to an electronic access reader, is no longer inherently secure due to its original obscure and non-standard nature. Today, no one would accept usernames and passwords being sent in the clear nor should they accept such vulnerable credential data. ID harvesting has become one of the most lucrative hacking activities. In these attacks, a credential's identifier is cloned, or captured, and is then retransmitted via a small electronic device.

Leading card and card reader manufacturers offer security options. The first is to provide a

higher-security handshake, or code, between the card or tag and reader to help ensure that readers will only accept information from specially coded credentials. The integrator will never provide another organization with the same code. As a result, no other organization will have this reader/card combination. Only that single company's readers will be able to read their cards or tags and their readers will read no other organization's cards or tags.

The second major solution is Valid ID, an anti-tamper feature available with contactless smartcard readers, cards and tags. It adds an additional layer of authentication assurance to NXP's MIFARE DESFire EV1 smartcard platform, operating independently, in addition to, and above the significant standard level of security of DESFire EV1. Valid ID lets a smartcard reader help verify that the sensitive access control data programmed to the card or tag is not counterfeit.

At manufacture, readers, cards and tags are programmed with this fraudulent data detection solution. The Valid ID algorithm cryptographically assists in ensuring the integrity of the sensitive access control data stored on the card or tag.With Valid ID, readers scan through the credential's access control data searching for data discrepancies, which may occur during the counterfeiting, tampering or hacking of the credential. If tampering is detected, the reader reports it promptly to the access controller, identifying the credential in question.

What to Know about Vandal-Proofing the Card Reader

Vandal-resistant and bullet-resistant contactless card readers are ideal for installations where more durability is required than with a standard reader. They are becoming big hits at schools, universities, correctional institutions, housing authorities, factories, hospitals and other locales where RFID proximity and smart card readers can take a beating.

Keyfob

Smart card reader

In both types of hazard-resistant readers, protection is greatly enhanced because the electronics are sealed in weather-and tamper-resistant epoxy potting for both indoor and outdoor operations, providing an IP67 rating which assures the electronics are protected from water, steam, detergents, dust, sand, tools and other elements which could be used to impede data collection. In addition, the vandal-resistant readers are manufactured from thick polycarbonate material and feature tamperproof screws. An anti-tamper mode is also available, providing supervision of both the reader and its cabling.

Bullet-resistant proximity card readers can provide the highest level of vandal resistance by featuring a virtually indestructible exterior. These readers are milled from a solid block of stainless steel and reinforced with a bullet-resistant insert that is compliant with UL752 performance level standards of ballistic protection.

What to Know about Lowering Energy Costs

Some vendors provide as an option eco-friendly readers with a technology that cuts energy costs and is an easy addition to any company's green initiative. In emergency power situations, proximity readers using the low energy option can reduce average current draw by as much as 50 percent, providing significantly longer up-times with their back-up batteries. They can also expect long term energy savings.

The Bottom Line

Whatever you may need at the front end of your access control system, you should be able to find a solution that meets your needs.

For more information, please visit: www.farpointedata.com. SST