Choosing the Right Credentials Is Easier than You Think

Jennifer Toscano, Ingersoll Rand Security Technologies, Portfolio Marketing Manager, Credentials, Readers, Software, and Controls

Security is complicated. In any given facility, there are multiple openings to secure and multiple people who need access. Varied layers of clearance, employee turnover rates, and a long list of other factors play a role in dictating exactly which credential solutions make the most sense.

That credential is what you use to identify yourself to a system. Whether it's a key, a code, a card, a biometric or multi-factor authentication, your credential can provide access to spaces or services within your facility. Higher security credentials, like smart cards and biometrics, are often required for restricted areas or rooms containing sensitive information or materials. Keys or PIN codes may be sufficient for supply closets and other less sensitive areas that still require security but where convenience takes precedence. Many times, several types of credentials are used in unison.

Once you understand all of the choices and how they work, you can address your needs with confidence.

The Good Ol' Key

Mechanical locks have been a staple of commercial security for years – and with good reason. They're dependable, affordable and secure. Today, mechanical locks play a vital role in the broader security system of many hospitals, schools and universities, offices and other commercial buildings.

The effectiveness of mechanical security systems depends on three factors:

1. The quality of the lock you choose.
2. The type of key system you implement.
3. The effectiveness with which you manage your keys.

Keys are the credential used for mechanical locks and key systems. Determining if keys are the right credential for you depends on the type of key system you deem appropriate for your facility. There are three types of keys.

Open keys are used in key systems that are non-patented. They have been on the market for many years and offer no protection from key duplication or aftermarket copies. On some openings, keys are the only required credential. Open keys are ideal for applications where easy key duplication is necessary. They can be duplicated almost anywhere, including at big box and hardware stores. However, they are not the right choice for buildings with high turnover rates, such as apartments, schools and hospitals for example where keys are likely to go missing. They can create problems in applications where openings have high traffic rates or where a large number of people have keys.

Restricted keys are sold and distributed in a controlled manner by the manufacturer. However, since these types of keys aren't always patent protected, there is always a risk of key proliferation and loss of control.

Patented keys are protected by legally enforceable patent protection from "look alike" key blanks. This is the most reliable and effective way to prevent people from making unauthorized key copies. Patented keys work best where key control is required and in areas that contain sensitive information or require higher security, such as at hospitals, schools, or office buildings. They can create problems in applications where keys frequently need to be duplicated.

In California's Napa Valley School District, exterior doors and the outside of classroom doors are equipped with patented keys, Schlage Classic Primus cylinders, while the inside classroom locks use Schlage conventional cylinders, open keys. These can be keyed so the Primus keys will open them as well, which reduces the number of keys issued.

The school district's locksmith Jon Darnell notes, "One reason we are using the Primus is to stop unauthorized key copying." The restricted keyway prevents unauthorized duplication because key blanks are available only from the manufacture through the distributor.

What's Your Code?

Personalized codes, rather than keys alone, enhance convenience while still providing secure access. PIN codes offer a greater level of control and flexibility than traditional keys. A PIN (or "Personal Identification Number") is a numerical code assigned to authorized users. When a recognized PIN code is entered, during an authorized time period at an authorized opening, the user is granted access.

There are several advantages to using PIN codes. Users can be granted access to a number of different openings without carrying a pocket full of keys. Codes are ideal for facilities with a small number of users and relatively simple access control needs and openings that require audit trails. They make a good choice when used in conjunction with high security credential systems like smart cards and biometrics.

They are not the answer for areas where unauthorized users may see the codes being entered.

Some Credentials Are in the Cards

Card-based credentials are available in a variety of technologies, including magnetic stripe, proximity and smart cards. They're also available in a number of form factors to suit your needs. For system managers, card-based credentials offer a solution that is easier to manage than keys and harder to duplicate than PIN codes. Access privileges can be easily assigned and revoked plus access privileges of a single user can be altered without impacting the entire user population. With card-based access, the threat of unauthorized keys or shared PIN codes is eliminated.

In facilities that require permission to multiple systems, card-based credentials offer the potential to consolidate technologies across multiple systems, enabling users to carry one credential to achieve multiple activities. But remember, not all card technologies are the same. In fact, some card credentials are a great deal more secure than others.

With magnetic stripe cards, users physically swipe their card through a reader (much like a credit card). Magnetic stripe technology has been around for decades and provides an affordable option for low security environments and convenience based applications. They don't work well in dirty environments, due to the electromechanical nature of the acquisition device. They also aren't right for applications requiring data storage or areas with strong magnetic fields, such as at checkout counters.

Proximity cards are the most basic form of "contactless cards." Proximity cards are encoded with a unique number that cannot be updated or changed. This ensures that the data on the card remains intact and unaltered. They are applicable for a wide array of environmental conditions and especially in applications requiring a unique identification number. They will not work well in applications that require data storage though.

As the name implies, contactless cards don't need to physically touch a reader. Instead, users simply wave them in front of a reader – reducing wear on the reader and card and extending the life of the system. This makes them an ideal choice for facilities with a high volume of traffic on specific openings or a large number of users.

Smart cards are the most advanced contactless cards on the market today. As far as users are concerned, they function just like proximity cards. But there's a key difference. Smart cards have the ability to store information. This makes them significantly more useful than magnetic stripe or proximity cards.

Smart cards can be used in diverse applications such as access control, cashless vending, meal programs and transit applications because of their ability to read data from and write data to the card. Smart cards also employ advanced security features that make them an ideal candidate for both high security applications and those in which important data or financial information will be transmitted.

They cover all of the applications in which proximity works plus high security applications, situations requiring data storage, where protection of high value areas or information is needed and in scenarios requiring multiple credential applications.

In general, cards are ideal for applications where the ability to generate audit trails is desired and where the ease of adding or revoking privileges is important. Cards are also useful in applications where secure access is required such as in high volume openings or in high user populations.

Even when the only application is access control, smart credentials make sense for the security behind a proximity card is minimal. Compared to being easily copied, as proximity cards can be, MIFARE DESFire™ EV1 smart cards by Schlage offer several different layers of security, including:

1. **Mutual authentication** ensures that the reader and the card are allowed to talk with each other before any information is exchanged.
2. **AES 128-bit encryption** is a key encryption technique that helps protect sensitive information.
3. **Diversified keys** virtually ensure no one can read or access the holder's credentials information without authorization.
4. **Message authentication code (MAC)** further protects each transaction between the credential and the reader. This security features ensures complete and unmodified transfer of information, helping to protect data integrity and prevent outside attacks.

Verifying that You Are You

Biometrics provide an automated method of recognizing an individual based on his/her unique physical characteristics and eliminate a person gaining entry by using another's key, code or card. Biometric technologies, like hand geometry, enable a facility manager to ensure that only verified users have access to a facility at authorized times. Biometrics provide the highest level of assurance that the actual authorized individual, rather than just the authorized key, card or code, has access to a secure facility.

Because of the versatility of biometric technologies, they are used in universities, day care centers, airports, healthcare facilities and government buildings – any place where resources, lives or sensitive information require the highest levels of security. For instance, large data center installations use biometric hand readers at the entrance, on the security corridor and on the individual customer areas of their data centers. However, many find it surprising that their biggest deployments are where they are chosen for convenience.

That's because they can eliminate the need for keys or cards. While keys themselves don't cost much and dramatic price reductions have lowered the capital cost of the cards in recent years, the true benefit of eliminating them is realized through reduced administrative efforts. For instance, a lost card or key must be replaced and reissued by someone. Just as there is a price associated with the time spent to complete this seemingly simple task, when added together, the overall administration of a key or card system is costly. Hands are not lost, stolen or forgotten. They also don't wear out or need to be replaced.

Hand geometry measures the size and shape of a user's hand, including length, width, thickness and surface area to verify the person's identity. In conjunction with a PIN code or a card, the individual can gain access to a facility. Hand geometry technology is well accepted by users, as there are no palm prints taken and the user does not leave behind any trace of their biometric data. In addition, hand geometry can be utilized in both diverse indoor and outdoor applications.

Hand geometry is typically the chosen biometric in harsh environments, such as dirty, greasy and wet conditions. Because of its relatively low error rates, it is selected for applications with a high number of users. Users prefer hand geometry for environments with privacy concerns since no handprint is left behind and in areas where hygiene is a factor and antimicrobial surfaces are needed.

Sometimes the Right Credential is Several Credentials

Multi-factor authentication describes applications where more than one credential technology is used for added security or convenience. It's common sense, really. Two credentials can be more secure than one. That's the concept behind multi-factor authentication. Facilities with unique or heightened security needs may wish to implement a multi-factor (or blended) credentials strategy.

As University of Virginia, Facilities & Systems Engineer, Office of Business Operations in Charlottesville, Va. Gary Conley, states, “We wanted a Grade 1 ANSI spec locking system with dual credentials – something the student had, their magnetic stripe ID card, plus something the student knew, a PIN – to get into (residence) halls and their rooms.

In another example, a hospital may choose to require authorized personnel to present a key and a smart card and code to enter pharmaceutical storage areas. In doing so, they have additional protection against the use of lost or unauthorized credentials.

There are other benefits to a blended credentials strategy as well. They provide the freedom to use a single credential on multiple kinds of readers. For example, imagine a college that currently uses magnetic stripe, proximity and smart readers in different buildings across its campus. Without the cost of migrating to a campus-wide smart card system, they could issue each student a single card that works with each system – and doubles as a library card, meal card, and more.

Of course, there are a wide range of variables when it comes to multi-factor authentication. Your security consultant should be able to advise you.

Don’t Be Confused

To determine the credentials you need to use, describe what type of protection you want at each ingress/egress point. What is the environment in which this credential will work? With that quick overview, you can determine which credential will work best.

When in doubt, your security consultant or integrator can help.

-30-