



Credentials Knowledge Guide

You can't make a decision about anything until you have a clear understanding of

everything



KEYS



CODES



CARDS



BIOMETRICS



MULTI

Choosing the right credentials for your facility is easier than you think.

WE'RE HERE TO HELP YOU BY:



The simple truth is, 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.

The variables are infinite.
Fortunately, so is our commitment to you.



We're here to help.

When you've been the leader in security for over 90 years, you learn a lot. We know what works – and what doesn't. Most importantly, we know how to help you analyze your needs to create a system that provides security for today and flexibility for tomorrow, and beyond.

»» What sets us apart?

OPEN ARCHITECTURE

Our credential solutions are designed to work with a wide array of competitive and complementary systems. That means you have the flexibility to integrate new credentials into your facility as time, budgets and needs allow.

CONSULTATIVE APPROACH

You'll make the right decision because we'll be there to help. Our security experts aren't simply sales people. They're trained to truly understand how the credentials in your facility work together to affect your overall efficiency. They can help you make the right decision for today, and for the future.

A WIDE RANGE OF CREDENTIAL OPTIONS

No one can offer you the spectrum of solutions that we can. And you don't have to settle for just one credential technology. You can choose from across our credential families to create your own personalized solution.

What exactly is a credential?

A credential is what you use to identify yourself to a system. Whether it's a key, a card, or a biometric, 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.

A woman with her hair in a ponytail, wearing a white lab coat and carrying a black bag, is shown in profile from the side. She is using a key to unlock a door in a brightly lit hallway. The hallway has white walls, a drop ceiling with recessed lights, and a door on the left. The background is slightly blurred, showing the continuation of the hallway.

» So, which credentials are right for you?

It depends.

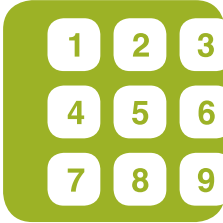
But this much is certain:

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



Keys

Mechanical key solutions can be used in a wide range of applications to provide basic or enhanced access control.
pages 2-3



Codes

Codes provide convenience and security, making it easy to protect assets and information.
pages 4-5



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.
pages 6-7



Biometrics

Biometric systems allow entry based on the unique characteristics of the human body while eliminating the possibility of lost or stolen keys and cards.
pages 8-9



Multi-Factor Authentication

Multi-factor authentication is the term used to describe applications where more than one credential technology is used for added security or convenience.
pages 10-11



KEYS



CODES



CARDS



BIOMETRICS



MULTI



Keys

A traditional solution to fit your needs.

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: First, the quality of the lock you choose; second, the type of key system you implement; and third, the effectiveness with which you manage your keys. Our consultants will work with you to analyze your needs, explain your options, and help you determine the best solution for enhancing the security of your facility.



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	Open keys are used in key systems that are non-patented. Non-patented systems have been on the market for many years and offer no protection from key duplication or aftermarket copies. Open keys can be duplicated almost anywhere including big box or hardware stores.
RESTRICTED 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	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.

Within each type of key system, there are several levels of security. To learn which is right for you, talk to your Schlage representative.



Are keys the right credential choice for your facility?

On some openings, keys are the only required credential. In higher security environments, keys are frequently used in combination with other credentials (such as smart cards or biometrics).

OPEN	<p><i>Ideal for:</i></p> <ul style="list-style-type: none"> • Applications where easy key duplication is necessary (keys may be cut without restriction at home improvement stores). 	<p><i>Not ideal for:</i></p> <ul style="list-style-type: none"> • Buildings with high turnover rates (apartments, schools and hospitals for example) where keys are likely to go missing. • Openings with high traffic rates. • Openings where a large number of people have keys.
PATENTED	<ul style="list-style-type: none"> • Where key control is required. • Areas that contain sensitive information or require higher security (hospitals, schools, or office buildings for example). • Use in conjunction with high security credential systems as a manual override (like smart cards and biometrics). 	<ul style="list-style-type: none"> • Applications where keys frequently need to be duplicated.



Upgrading Your Existing Key System

With Schlage, it's simple to upgrade your existing system. Our security professionals can give you more control over your keys – and your entire facility. If you're interested in upgrading your system, simply contact us today.



Codes

Increased functionality. Enhanced security. Schlage dependability.

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. Additionally, overall security can be enhanced by reducing the number of keys in circulation in your facility.



Are codes the right credential choice for your facility?

Ideal for:

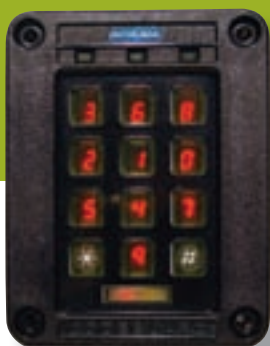
- Facilities with a small number of users and relatively simple access control needs.
- Openings that require audit trails.
- Use in conjunction with high security credential systems (like smart cards and biometrics).

Not ideal for:

- Independent use without being paired with another credential.
- Areas where unauthorized users may see codes being entered.



Schlage electronic locks (that feature keypads requiring PIN codes) are available in a number of styles and configurations. Depending on the specific model you choose, you can add up to 5000 separate user codes and create audit trails. You can also select models that allow you to manage user codes at the lock itself, or through your network.





Cards

*We're not just keeping up with technology.
We're leading the way.*

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, and 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-based credentials are a great deal more secure than others. Your trained Schlage representative will work with you to help you understand your options.

Magnetic Stripe Cards & Readers

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.

Proximity Cards/ KeyFobs & Readers

Proximity cards are the most basic form of "contactless cards." 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.

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.

Smart Cards/KeyFobs & Readers

Smart cards are the most advanced "contactless" cards on the market today. They function just like proximity cards but with one key difference: smart cards have the ability to store information. Because of this ability, smart cards can be used in diverse applications such as access control, cashless vending, meal programs, and transit. 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.

Form Factors



Are cards the right credential choice for your facility?

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 either high volume openings or in high user populations.

MAG STRIPE	<p><i>Ideal for:</i></p> <ul style="list-style-type: none"> • Low security applications. 	<p><i>Not ideal for:</i></p> <ul style="list-style-type: none"> • Dirty environments, due to the electromechanical nature of the acquisition device. • Applications requiring data storage. • Areas with strong magnetic fields (checkout counters for example).
PROX	<ul style="list-style-type: none"> • Wide array of environmental conditions. • Applications requiring a unique identification number. • High volume openings. • Large number of users. 	
SMART	<p><i>All of the applications for prox, plus:</i></p> <ul style="list-style-type: none"> • High security applications. • Situations requiring data storage. • Protection of high value areas or information. • Scenarios requiring multiple credential applications. 	



CARDS



Biometrics

Reliable solutions for the most secure applications.

Biometrics are automated methods of recognizing an individual based on unique physical characteristics. 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, you will find them used in universities, data centers, day care centers, airports, healthcare facilities and government buildings – any place where resources, lives, or sensitive information requires the highest level of security.

Hand Geometry

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.



Are biometrics the right credential choice for your facility?

Biometrics are ideal for use where the most valuable resources must be protected. These technologies verify people and ensure that the right person is at the right place at the right time.

HAND GEOMETRY

Ideal for:

- Harsh environments (dirty, greasy and wet conditions, for example).
- Applications with a high number of users due to relatively low error rates.
- Environments with privacy concerns (as no handprint is left behind).
- Areas where hygiene is a factor and antimicrobial surfaces are needed.

Not ideal for:

- Applications where aesthetics are a primary concern.
- Applications where size and form factor of the solution is an issue.





Multi-Factor Authentication

Sometimes the right credential is several credentials.

It's common sense, really. Two credentials can be more secure than one. That's the concept behind multi-factor authentication.



Keys

Codes

Cards

Biometrics



Facilities with unique or heightened security needs may wish to implement a multi-factor (or blended) credentials strategy. For example, a hospital may choose to require authorized personnel to present a key and a smart card and a 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. With Schlage technology, you're free 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.

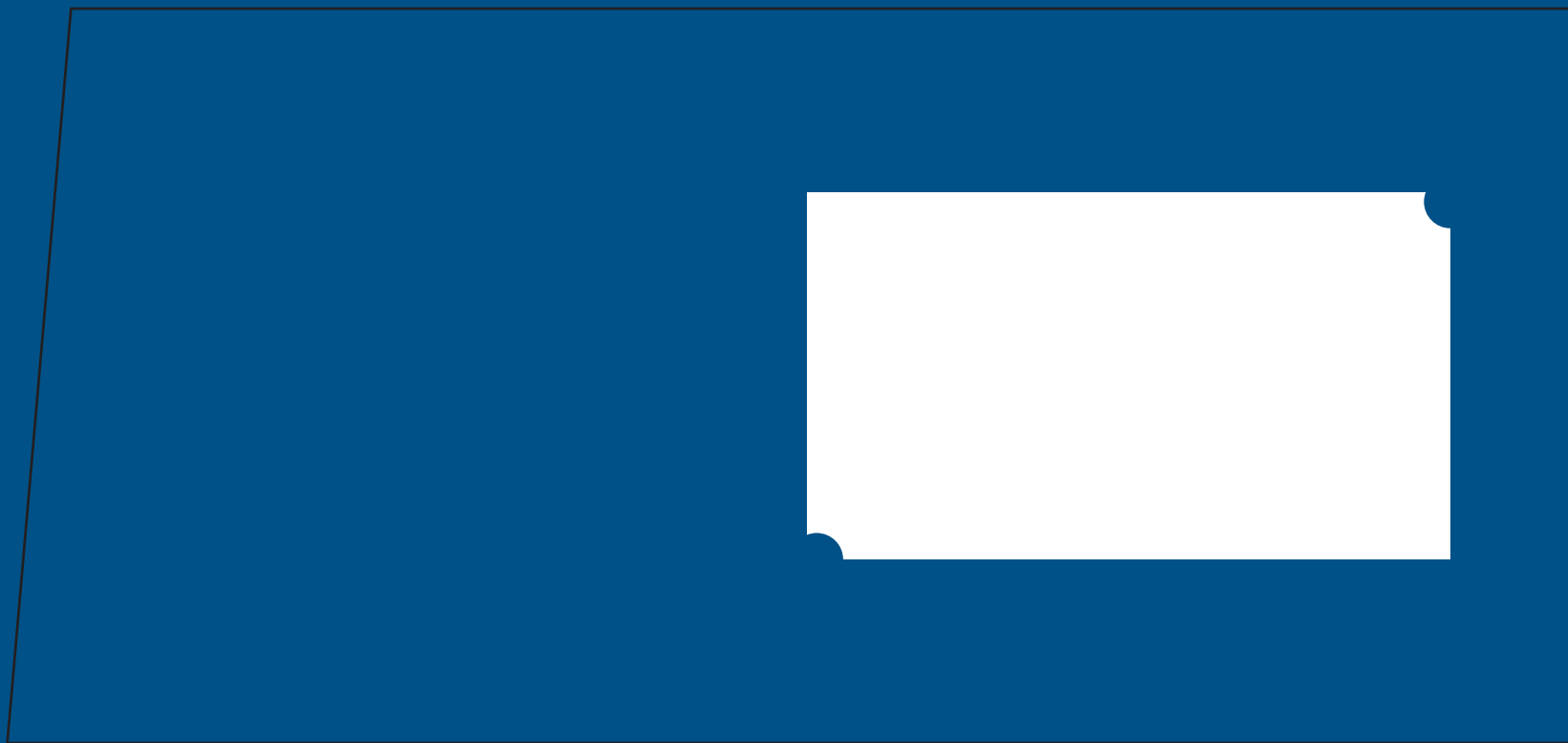
Of course, there are a wide range of variables when it comes to multi-factor authentication. A Schlage security expert will be happy to discuss all of your options with you.

THE ONLY THING MORE COMPREHENSIVE THAN OUR LINE OF SOLUTIONS IS OUR EXPERTISE.

If you have a question, just ask. We'll give you everything you need to make informed, confident decisions.

Visit us on the web at [schlage.com](https://www.schlage.com) or call us at **877-671-7011** and choose Option 3 to talk to your local sales office.







Ingersoll Rand's Security Technologies sector is a leading global provider of products and services that make environments safe, secure and productive. The sector's market-leading products include electronic and biometric access-control systems; time-and-attendance and personnel scheduling systems; mechanical locks; portable security; door closers, exit devices, architectural hardware, and steel doors and frames; and other technologies and services for global security markets.

877-671-7011

www.schlage.com www.ingersollrand.com