ALLEGION™

Article

Back to basics: Readers and credentials

Access control readers and credentials are the standard in new facilities today. From high-rise offices to hospitals and just about everything in between, building owners seek the security, convenience and efficiency these solutions offer.

It's beneficial to understand the options available so you can help your customers plan for access control in their facilities. Whenever possible, it's best for end users to plan for access control early. Neglecting it can lead to a costly burden for the building owner down the road, especially if there is a need to run wiring at an opening.

First, it's important to understand the basics.

Mechanical vs. electronic: How to choose

While electronic solutions have grown in popularity, there are many applications that still require mechanical hardware. So how do you choose between electronic and mechanical solutions? The goal is to create a cohesive user experience that strikes the right balance of security, convenience and efficiency at every opening.

There isn't a one-size-fits-all answer. Successful properties blend the two for a holistic experience. To achieve this, it comes down to understanding the intended function of each opening, and then selecting the appropriate solution.

"The key is to provide convenience while maintaining security for the end user" says Brian Marris, product manager for readers and credentials at Allegion. "It is essential to help the building owner analyze his or her security needs and expected traffic for each opening. For example, a janitor closet is probably only used by one person throughout the day. But the back door to the parking lot sees high traffic and probably requires increased security. Using a reader and credential in that application adds convenience and efficiency by providing a tap-and-go experience—while still providing a safe and secure door."

Use Marris' advice to figure out the needs of each door, starting at the perimeter and working your way inside, tailoring the experience by opening. Here are additional questions to address:

- What is the general level of security required for the facility?
- Do specific openings require more security than others?
- How often do access privileges change?
- What is the frequency of use?
- Which openings could benefit from ease of access?
- Is there high abuse?
- Is there a preferred method of electric locking (i.e. electric locksets, electric strikes, magnetic locks, etc.)?
- Are audit trails important at specific openings?
- What is the budget?
- Does the facility need lockdown capabilities?
- How many keys will exist to each opening? Consider the cost and time to rekey those openings if one of those keys was lost or stolen compared to removing a credential from a database.

Selecting the reader

"Reader usage began with a focus solely on perimeter access control, commonly found on the exterior of a commercial or multi-family building," Marris explains. "Then the advantages were found in new construction scenarios to electrify the interior openings with wireless locks. The ability to electrify both the exterior and interior of the building, in a cost-effective and efficient manner, has dramatically increased the use of electronic access control systems."

ALLEGION™

Today, readers are used in a variety of applications, including higher education, healthcare and commercial offices. And there are many benefits for your customers. Readers offer greater security by requiring personalized credentials to enter an area and providing audit trails to show who accessed specific openings and when. Using credentials is cost effective compared to manual keys because your building owners won't need to replace keys or rekey locks over time.

There are a number of options to choose from. Readers can be contact-based, which requires the credential to be swiped or touched by the reader. Or they can be contactless, which only requires a certain proximity or range to communicate. Some readers are self-contained units on a door frame or wall, while others are part of a wireless electronic lock. Biometric readers are also an option. These use unique human characteristics as the credential, such as the size or shape of the hand. The most secure reader options on the market, biometrics are more common in high-security applications, such as data centers, airports, banks and government buildings.

Multi-technology readers, like those offered by Schlage®, are designed to simplify access control. Your customers can transition from magnetic stripe cards to smart cards without changing the entire reader.

Regardless of the type, readers communicate with an access control system to grant or deny access to an opening when a credential is presented. While there are some proprietary reader options that only accept a specific type of credential, it is recommended to choose a technology that can be programmed by multiple companies to provide future flexibility to your clients.

Types of credentials

Mag (magnetic) stripe

- Card credential must be swiped through a reader
- Limited encryption, which is more susceptible to duplication
- One-way communication only, making duplication possible

Proximity

- Contactless card that doesn't require physical contact with the reader
- May be read from within a few inches of the reader depending on the reader and card
- Storage limited to card number alone
- Limited security, duplication possible

Smart technology

- Most secure option
- Advanced data encryption makes duplication nearly impossible
- Two-way communication between the card and reader provides mutual authentication
- Multiple sectors on the card allow for storage beyond access control, including data storage and cashless vending

Mobile credentials

- Based on encrypted smart card technology, using phones as credentials
- "Green" option eliminates the need to replace cards or issue new ones
- Increased use of smartphones and apps makes them more common

Early planning is essential

Customers expect the conveniences readers and credentials offer, so it's important to recognize when and where they should be used to complement mechanical solutions, and which ones to choose. It's best to start planning for access control early. It is critical that the various details for the electronic access control system are detailed and communicated so the correct product and credential programming can be ordered for quick installation and ease of use. Include all of the key stakeholders, such as the hardware consultant, security consultant, integrator, electrical engineer and building owner.

Keep in mind that access control solutions directly impact door specifications. Bring in an expert who is familiar with the mechanics of a door, including fire and life safety building codes. Allegion hardware consultants are available to help choose the best access control solutions for your project.

Allegion has a team of more than 150 specification writers located around the world who would be happy to assist on your next project. Contact an Allegion specification writer, or check out the iDig Hardware blog for information and updates on door hardware codes.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

011895, Rev. 01/19
www.allegion.com/us