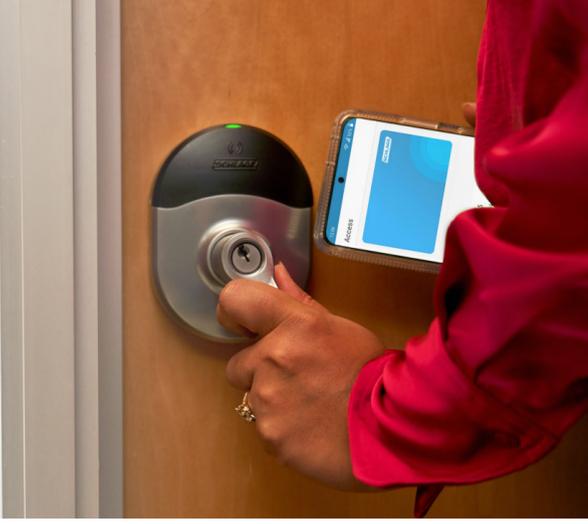




Four things to consider when choosing your credentials



In the access control world, the word credential can often mean different things to different people. An access control system allows system administrators to customize and control who can gain access to certain areas in a building by utilizing credentials to confirm a person's identity.

Typically, stakeholders look at a credential from a security perspective and choose one based on the security details. However, a user's perspective can be much different as most people want a convenient, easy way to enjoy seamless access throughout their office, school or any type of facility with a physical access control system in place.

“ The ideal situation is having the right balance between both security and convenience, knowing the investment will pay off long term in many different ways. ”

Selecting the most effective credentials for your organization can be challenging as many considerations should be reviewed to help make the right decision. Key factors include:



User experience

There are many different types of form factors when it comes to physical credentials. From fobs to ID badges, wristbands and mobile phones - each has its own unique set of advantages and disadvantages for users.



Keyfobs, ID cards and wristband

- Physical credentials carried by users
- Grant access with a tap, swipe or wave
- Upsides: broad hardware support, low cost, ease of use
- Downsides: plastic waste, varying degrees of security and the time and difficulty associated with administration and replacement of lost and stolen credentials
- When choosing this option, look for high-security encrypted credentials that minimize the ability to be replicated and offer multiple storage options to support applications beyond access control



Keypads and PIN

- Used when doors have keypads
- Grant access when users enter the appropriate PIN
- Upsides: convenience factor, as it does not require individuals to physically carry something with them
- Downsides: forgotten passwords and PINs, potential security risk if the PIN is used as the sole credential (can be shared easily); to solve for this, the PIN can be used in combination with an ID card, fob or wristband for greater security



Mobile

- Credentials protected and stored on mobile device
- Grants access with users smartphones
- Upsides: combined convenience and ease of use, improved security technology like multi-factor authentication
- Administrators find value in easily managing user permissions remotely and utilizing contactless distribution



Credential technologies

The days of using a mechanical key as the sole credential type are slowly dwindling, as most businesses have recognized the value of upgrading to electronic credentials. Today, more organizations are using advanced forms of credentials that include both physical ID cards and mobile credentials. Understanding how credential technologies have evolved over the years can help when evaluating your credential platform.



Mobile

Two mobile credential solutions are available in the market: Near Field Communication (NFC) and Bluetooth® Low Energy (BLE). Both solutions leverage best practices for security and encryption; however, they each provide different user experiences.

- NFC mobile credentials are similar to physical cards or fobs when they are added to the Apple Wallet or Google Pay and can also be used for vending, dining and other services, in addition to access control
- BLE credentials generally require the user to open a mobile app on a smartphone and show intent by making a motion or tapping on the door



Smart technology

Like proximity technology, smart credentials use RFID technology. However, they also use a microprocessor and encryption algorithm to protect the data when it is transmitted over the air. Different levels of security are available, including MIFARE® DESFire® technology with AES 128-bit encryption.



Proximity technology

Proximity credentials use RFID technology, almost like an AM/FM transmitter and receiver. When in range and tuned to the correct frequency, the hardware can pick up the signal to read the information on the credential. This legacy technology is not encrypted, leaving it exposed to the possibility of duplication.



Use of credentials

Security and IT professionals are faced with a myriad of choices when it comes to credentials as functionality can go well beyond access control. In many cases, a single credential can be used for secure printing, point of sale, cashless vending, public transportation and more. How an organization wishes to use its credentials is directly related to the type of credential technology that should be considered.



Secure printing



Point of sale



Cashless vending



Public transportation

In addition, understanding proprietary solutions vs interoperable solutions and custom encryption keys are also important. It's suggested to meet with an experienced security consultant or service provider who can assess your requirements and evaluate cross-platform compatibility in further detail.



Investment

Typically, implementing a credential solution requires a significant investment that will pay back in the long term in different ways, including lessened operating costs, improved efficiency and reduced security risks.

Organizations should not only look at their short-term needs, but build a long-term strategy when reviewing their options. Most credential solutions are designed to be scaled over time, and it is common to take a phased approach.

The process of selecting the right credential takes time as there are many different factors for organizations to consider. **It's important for key stakeholders to analyze how their credential platform can deliver the most value for their organization,** now and in the future. Reaching out to an experienced security consultant or service provider can also be beneficial to help find the right solution.

As we move forward and credential technologies continue to evolve, we will see a significant shift from legacy card technology (like proximity and magnetic stripe) to secure smart card and mobile technology. From small, to medium, to enterprise-level organizations – each has their own unique set of needs when it comes to credentials; **but one need that stays constant is providing a more secure environment for all.**

LEARN MORE ABOUT THE CREDENTIAL OPTIONS AVAILABLE

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in seamless access. We keep people and their assets safe, wherever they are, bringing together simple solutions, convenient access and advanced technology.



For more, visit www.allegion.com

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

© 2022 Allegion
015580 Rev.10/22
www.allegion.com/us