Evolution of the connected opening

Opening a door with anything other than a metal key was once unimaginable. Keys are still used in today’s applications, but more and more openings use an electronic “key.”

Security solutions have advanced with technology, offering increased security, privacy, monitoring and convenience more than ever before. As options evolve, so does the meaning of a connected facility.

Key
- Easily copied, stolen or shared
- Limits access only if you have control of all keys
- Patented key systems prevent duplication without authorization

PIN code for keypad
- First connected credential
- PIN easily changed if access needs to be restricted
- PINs easily shared or stolen, causing privacy concerns

Barcode
- First card to work with standalone readers
- Originally stored data by varying the width and spacing of parallel lines
- Easy to duplicate with a photo copier or printer

Wiegand cards
- Data stored on small pieces of specially processed wire
- Highly secure because it can’t be altered or copied
- More durable over time—but more costly
- Production discontinued in 2013

Magnetic stripe card
- Stores data on high- or low-coercive magnetic stripe
- More affordable option than Wiegand cards
- Wear-and-tear over time, leading to unreliability and higher replacement requirements

Proximity card
- First contactless card that can be “read” without inserting or creating contact with a reader
- Range of about four inches—allowing it to be left in wallet
- Holds more data than magnetic stripe

aptiQ  LCN  SCHLAGE  STEELCRAFT  VON DUPRIN
Smart card
- Greater security with an encrypted credential that must be decrypted by a reader
- More flexibility and functionality with storage capacity for different applications: access control, POS, computer access, etc.

Near Field Communication (NFC)
- Smartphone serves as credential
- Can’t be easily cloned or duplicated, unlike proximity and magnetic stripe cards
- Credential storage area in same memory location as other app passwords and sensitive information
- Able to share the same badge ID as physical badge, allowing users to have two forms of ID with the same number in the access control system

Biometrics
- Most advanced security solution on the market
- Measure one or more unique physiological human characteristics (shape of hand, fingerprint, iris, etc.)
- Can never be forgotten, lost or copied

Connected solutions from Allegion
AD-Series
The AD-Series is a flexible, adaptable and scalable solution for many facilities. Here’s why:
- Patent-pending modular design: This innovative design allows locks to be configured in multiple ways, depending on the need of each opening. It provides flexibility for various types of openings with different access protocols and uses.
- Easy credential migration: When your clients are ready to migrate to a different credential, they don’t have to discard the current locks and invest in brand-new door hardware. Migrating to smart card technology is as simple as changing the reader head on the lock—and far more convenient and cost-effective than changing an entire lock.
- Open architecture: The AD-Series can easily integrate with a variety of access control systems or other networked software solutions. It isn’t limited to one type of credential the way other locks often are.
- NFC-ready: The AD-Series is already equipped to work with any NFC platform—an important characteristic since NFC is becoming more popular.

Everest 29 patented key system
You can fortify your client’s mechanical lock choice with a key control system like Everest 29™ from Schlage®. A patented key system is the foundation for any secure access control system because it prohibits the duplication of a key without the manufacturer’s authorization. Only the system’s manufacturer, through its distribution network or contracted locksmith vendors, can acquire key blanks. Without patent protection, anyone can take a key to a locksmith and duplicate it. Just like that. When you specify a patented key system, you help property owners reduce risk, limit exposure and ensure the integrity of every opening.
Choice driven by application

Since many of these options are still available today, the question becomes, “Which one do I choose?”

There’s no one-size-fits-all solution, says Erik Larsen, Allegion National Account Manager – Electronic Integrators. It’s all about balance.

“Typically, security, technology and usability are the key priorities,” he explains. “The goal is to balance priorities for each organization. In a clean room environment, for example, usability may be the driving priority because handling keys, cards or keypads may not be conducive or convenient. In that scenario, the client likely needs a biometric solution.”

The goals in a university environment may be to reduce the cost of resident room keys and combine access control with other university transactions (POS, transportation, etc). In this case, the school likely needs smart cards or NFC.

“Many people try to select credentials by leading with the technology,” Larsen says. “Instead, they should be finding out about the user, the applications and the culture. The right technology will follow once those things are understood.”

In order to specify the best level of security and the right type of credential, it’s important to understand the following factors:

- Level of security needed
- Existing credential system in place
- Different zones in the facility that may require varying levels of security
- Current culture of users with respect to security and normal safe work environment
- High-security locations or areas that need multi-factor authentication (e.g. card + pin / card + biometric / card + pin + biometric)

aptiQ Multi-technology Readers

aptiQ™ Multi-technology Readers are designed to simplify your access control solutions now and for the future. Facilities can transition a system from magnetic stripe or proximity to smart card technology at a pace that works for them—and all without changing out readers down the road.

- **Specs:** One sleek reader handles applicable ISO standards (14443A, 14443B, 15693), is FIPS 201-1 compliant and is versatile enough to read 125 kHz proximity and 13.56 MHz contactless smart cards in a single unit.

- **Flexible:** aptiQ readers recognize magnetic stripe credentials, most proximity credentials and aptiQ smart credentials (MIFARE® Classic and MIFARE DESFire™ EV1).

- **Easy installation:** With quick-connect cable and simple mounting brackets, aptiQ readers are easy to install.

- **Easy credential migration:** The MT11 and MT15 readers allow a customer to start with proximity cards and migrate to smart cards without having to replace the readers. Like the AD-Series, they are NFC-ready. Likewise, the MTMS15 reader allows the customer to transition from magnetic stripe to proximity or smart cards. It’s simple: When they are done with magnetic stripe, the magnetic stripe read head can easily be removed and the remaining parts of the reader can still be utilized.

Since many of these options are still available today, the question becomes, “Which one do I choose?”

There’s no one-size-fits-all solution, says Erik Larsen, Allegion National Account Manager – Electronic Integrators. It’s all about balance.

“Typically, security, technology and usability are the key priorities,” he explains. “The goal is to balance priorities for each organization. In a clean room environment, for example, usability may be the driving priority because handling keys, cards or keypads may not be conducive or convenient. In that scenario, the client likely needs a biometric solution.”

The goals in a university environment may be to reduce the cost of resident room keys and combine access control with other university transactions (POS, transportation, etc). In this case, the school likely needs smart cards or NFC.

“Many people try to select credentials by leading with the technology,” Larsen says. “Instead, they should be finding out about the user, the applications and the culture. The right technology will follow once those things are understood.”

In order to specify the best level of security and the right type of credential, it’s important to understand the following factors:

- Level of security needed
- Existing credential system in place
- Different zones in the facility that may require varying levels of security
- Current culture of users with respect to security and normal safe work environment
- High-security locations or areas that need multi-factor authentication (e.g. card + pin / card + biometric / card + pin + biometric)
Combining credentials for the best security

It’s not uncommon for a facility to employ different types of credentials associated with distinct security zones. In fact, most still use a combination of both mechanical and electronic solutions.

“While one will be chosen as the base credential,” Larsen says, “there will likely be areas that need something more—or perhaps even less.”

He uses a hospital to illustrate this point:

A magnetic stripe or proximity card may be the main credential to access most openings throughout a hospital. But some areas may need a secondary, or multi-factor, authorization. A pharmacy, for example, may be outfitted with a reader for the mag or prox card, plus a biometric solution. Similarly, premium-priced readers may be used at external perimeters or highly secure areas, while lower-priced mechanical locks may be the most cost-effective option for maintenance rooms that require less security.

“Studies have shown that most facilities use the 80/20 rule,” he says. “Premium electronic solutions are used on about 20 percent of the openings—main lobby, office doors and areas of high value. These are Tier 1 security points that need real-time access and monitoring.”

The rest—general offices, restrooms, maintenance closets, etc.—are typically outfitted with offline or non-audited solutions, such as mechanical locks.

Contact an Allegion spec writer today for assistance selecting the right credentials for your facility.