Evolution of credential technology

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, efficiency and convenience more than ever before. As options evolve, so does the meaning of a connected facility.

**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 up to four inches—allowing it to be left in wallet
- Holds more data than mag stripe

**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

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.”

Larsen recommends considering the following questions to identify priorities:
- What level of security do you want?
- Are there different zones in the facility that require varying levels of security?
- What do you like/dislike about your existing credential system? (e.g. having to rekey locks or replace cards due to wear-and-tear)
- What is the current culture for the users with respect to security and normal safe work environment?
- In what locations will the security solution be used?
- Are there high-security locations? (e.g. pharmacies, bank vaults, data centers, etc.)
- Are there areas that need multi-factor authentication? (e.g. card + pin / card + biometric / card + pin + biometric)
- How important is it to future-proof security with what’s expected three, five or even 10 years from now?
- What are your maintenance requirements?
- Do you have installation concerns or constraints? (e.g. marble entrance way in a main lobby or dust concerns in a clean or sterile environment)
- How will a more “connected” option impact your staff and building occupants?
- What are your budget constraints?
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. Multi-Technology readers are available on the AD-Series, allowing the use of both proximity and smart cards within the same system. And AD-Series reader modules can be easily swapped out to enable transition from keypad or magnetic stripe to smart technology without having to replace the entire lock.

- **Open architecture:** The AD-Series is easily integrated with a variety of access control systems or other networked software solutions.

- **NFC-ready:** The AD-Series is NFC-ready.

**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. 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.
Combining credentials for the best security

The answers to these questions will guide the choice of a credential—or credentials. It’s not uncommon for a facility to employ different types of credentials associated with distinct security zones.

“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 a magnetic stripe or proximity 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. “Electronic solutions are used on about 20 percent of the openings—main lobby, office doors and areas of high value. These are security points that need real-time access and monitoring. However, technology advancements are driving the broader interest and adoption of electronic credentials for use beyond the typical perimeter access points.

Contact an Allegion integrator sales consultant for assistance in selecting the right credentials for your facility, or call 888-758-9823 to find a consultant in your area.