HAGER COMPANIES

DHI DS+S Magazine, October 2020

The Advantages of Mobile Applications and Credentials

by Nick Ealy

When Steve Jobs debuted the iPhone in January 2007, we couldn't have anticipated how much of an impact the smartphone would have on society. It has completely revolutionized the way we work and connect with others.

As the door and hardware industry continues to be at the forefront of security and proactively address COVID-19 concerns, the era of physical credentials is giving way to a secure and touch-free option: mobile credentials. Mobile credentials provide people with access to secured spaces that are convenient for the user and cost-effective for the building owners/ managers.

Two Platforms

Access control systems are either cloud-based or server-based.

Cloud-based services are usually online all the time and can allow openings to be controlled in two ways: remotely through a mobile app or locally with users unlocking doors using their smartphones as a credential.

In the remote scenario, the communication path starts with the administrator's phone equipped with an app. The command chain goes from the phone to the cellular/WiFi network, to the dedicated cloud space, to a local network, to a wireless hub and then to the locking device.

"The chain of communication may sound complex," explains James Stokes, Director of Corporate Training at Hager Companies. "But in reality, it happens in a matter of a few seconds."

Examples include admitting an outside service provider that arrives on-site when there is no staff available to admit them, or a new employee who does not yet have their permanent credential.

Additionally, the mobile app can give business administrators full control of users' access rights and can be managed from anywhere at any time. With cellular or WiFi service, openings can be remotely managed and monitored from anywhere in the world.

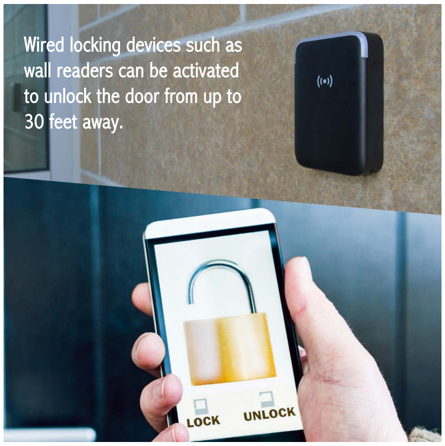
Cloud-based systems also provide the option of using smartphones as credentials. Instead of a card or fob, the phone is presented to the locking device or reader to gain access. In this setting, the phone app communicates with the locking device or reader, which transmits that data to the locally installed wireless hub that stores the access rights. If access is allowed, a signal is sent to the locking device to unlock. Similar to the remote scenario, this process is quick with minimal disruption to the user.

Once the transaction has been completed, the local wireless hub will communicate with the cloud to upload the audit record for future use while simultaneously downloading any access right changes.

Even in the case of communication failure between the hub and the cloud, the hub has users and access rights stored to ensure normal service is maintained. When communication is resumed, audits, activities and any other changes will be uploaded.

In the server-based world, building administrators can use mobile apps and credentials in a variety of ways without requiring all locking devices to be wired or wireless.

This can result in huge savings in capital infrastructure costs. Mobile credentials can be used with wired, wireless, and offline battery-operated locking devices – all managed under one software system.


Wired locking devices such as wall readers can be activated to unlock the door from up to 30 feet away.

Wired locking devices are typically readers on high-traffice entrances to buildings. Because they are not constrained by battery life, the readers' Bluetooth is constantly powered and a valid mobile credential can activate the door from up to 30 feet away.

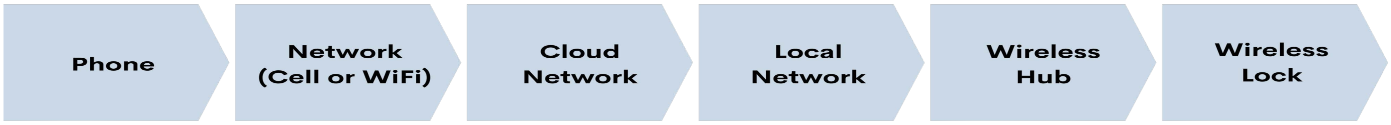
Wireless locking devices are generally battery operated. They require the mobile credential be held close to the reader to activate the Bluetooth lock to read access rights.

Offline locking devices are battery operated and also need a credential held close to the reader to activate.

Improved Security

There are several advantages to both the end-user and the distributor when adopting mobile credentials.

Mobile credentials give businesses greater flexibility to manage people, properties, and assets by enabling a more efficient and user-friendly experience across multiple sites without sacrificing security.


Phone → Network (Cell or WiFi) → Cloud Network → Local Network → Wireless Hub → Wireless Lock

While physical credentials, such as cards, can be lost, stolen or used by unauthorized people, a mobile credential provides additional layers of security. Most smartphone users set up authentication, such as a PIN, fingerprint or facial recognition to access their phones, which adds an extra level of security to the transaction. Many phones also have the ability to be tracked or erased remotely.

Added Convenience

From a user's perspective, mobile credentials are expedient because it is not necessary to carry a card, fob or other physical credentials.

"Whether you are leaving your desk, your office, or your home, everyone makes sure to carry their smartphone," Stokes notes. "It's a lifestyle, so electronic access via the phone is incredibly convenient." Because the mobile app allows for updating access rights remotely without using a wired, online update point, it also creates a better user experience.

Limited Contact

COVID-19 has changed the way we move around in our lives. Now more than ever, businesses look at their buildings through the lens of COVID-19 to find ways to limit touch points. According to the Centers for Disease Control and Prevention (CDC), people may get sick by touching a surface that has the virus on it and then touching their mouth, nose or eyes. Mobile credentials can greatly reduce the number of necessary touches for a user to gain access to secured spaces.

Recurring Revenue Generator

Mobile credentials can be a recurring revenue generator for owners of buildings such as multi-family complexes. Many people are attracted to ease of use and convenience, so buildings that offer mobile credentials for access are quite desirable. Facilities can use this to their advantage in two ways:

- Charge a premium service fee for the convenience of mobile credentials.
- Offer one mobile credential as part of the rental package and charge an extra fee for additional mobile credentials, like roommates, on the same lease.

End-User Cost

The cost structure for mobile credentials can vary between manufacturers, software companies or even product lines. Occasionally, an access control system, using a paid cloud service, will not charge a fee since mobile credentials are just a feature of the service. Often, though, mobile credentials will have an extra fee.

Some access control systems require buying credentials in lots of 1,000. Each time you issue a credential, that credential is permanently used and cannot be changed, even if it is for the same person. So if a person's access rights change or they get a new phone, a new credential must be issued.

While there are drawbacks to this, the benefit is the credential often does not expire – which is ideal for companies with low turnover and where staff access rights do not change. However, if a property's access rights change frequently, users get new phones often or new users are added regularly, the credential allotment could be depleted quickly.

Many access control systems have a recurring annual fee for credentials. While this is an additional yearly fee, the mobile credentials can be reused. This means that when four people move out of a building and those credentials are canceled, they can be reissued to four new people with no additional fees to the system owner.

"Being aware and asking the right questions regarding credential costs will ensure you get the right access control system for the building with no future surprises," advises Stokes.

Mobile Credentials in Verticals

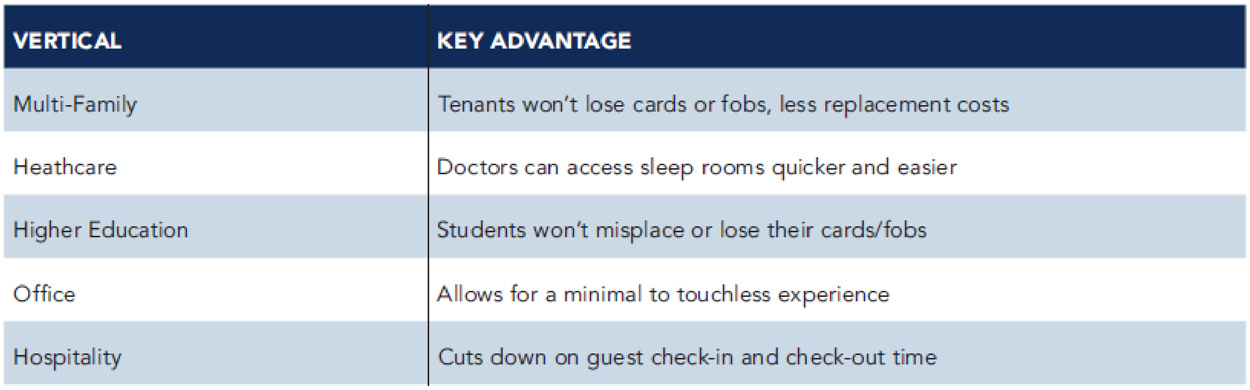
Mobile credentials have a place in multiple vertical markets, but this growing trend has affected five vertical markets in particular (see table below).

Long-Term Benefits

To know if mobile credential make sense for a client, they need to be asked, before hardware is specified, if they intend to use mobile credentials now or at any point in the future. If the answer is probably or yes, it is more cost-effective to invest in locks that accept mobile credentials at the outset then face replacement costs down the road.

"The beauty of both cloud-based and server-based platforms is that even if the end user isn't ready to switch over to mobile credentials entirely, both provide the option of using a card/fob or the smartphone app," Stokes points out. "It's simply a matter of having the foresight to put the components in place now, so it's ready to go when they're ready to upgrade." +

Nick Ealy
Technical Sales Specialist - Access Control
Hager Companies
Email: nealy@hagerco.com



VERTICAL	KEY ADVANTAGE
Multi-Family	Tenants won't lose cards or fobs, less replacement costs
Heathcare	Doctors can access sleep rooms quicker and easier
Higher Education	Students won't misplace or lose their cards/fobs
Office	Allows for a minimal to touchless experience
Hospitality	Cuts down on guest check-in and check-out time