



PLASTIC KEYCARDS TO DIGITAL WALLET

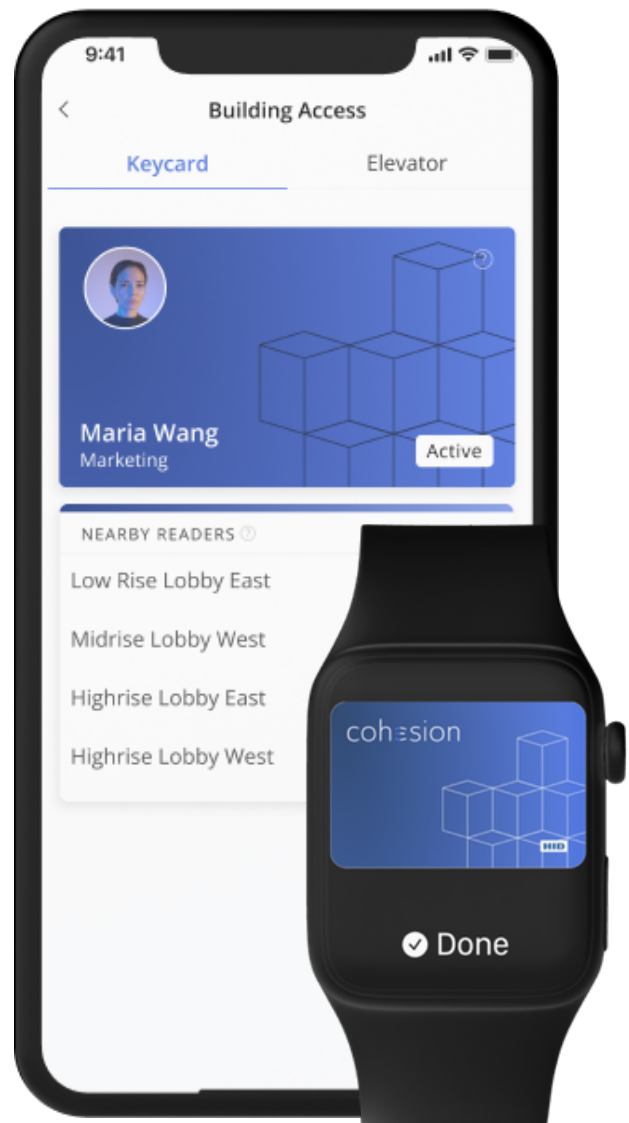
WHAT YOU MUST KNOW

cohesion

PLASTIC KEYCARDS TO DIGITAL WALLET: WHAT YOU MUST KNOW

IT'S TIME.

You can't put it off for much longer. Everyone expects fast, secure entry into buildings, offices, and spaces. The days of misplaced metal keys are long gone and everyone's had just about enough of plastic keycards.



WHY PLASTIC KEYCARDS ARE LITERALLY THE WORST

Let's do a quick takedown on exactly why plastic keycards are quickly becoming the worst possible way to control access to your properties and spaces.

Plastic Keycards are Inconvenient and Inefficient

For tenants and employees, plastic keycards can bring a lot of frustration. Digging through your purse or rifling through a wallet filled with lookalike cards in hopes of finding your plastic keycard slows down entry into a building or space. And then, if you use the wrong keycard, you're holding up the line, and everyone's going to start the day on the wrong foot. Not to mention, users can lose their cards just as easily as losing a paper receipt. Just think about how many lost keycards are floating around out there that no one knows about and the kind of access they could give a bad actor.

Plastic keycards are frustrating not only for the card bearer but also for security staff. Replacing and deactivating lost cards, changing access permissions, and constantly provisioning new employees and updating systems can be exhausting.

Terrible from the user side. Terrible from the staff side.





Plastic Keycards Are a Security Vulnerability

Back to the issue of the number of lost – or stolen – keycards out there that are roaming the streets unknowingly; this creates a huge security threat. A plastic keycard isn't that hard to copy or clone, and they are not supported with the latest advancements in cryptography to keep your data secure. This could allow open access to unauthorized individuals entering these properties who are up to no good. Think about how often keycards get lost compared to how often someone loses their smartphone.

Another worry is the probability of keycards being damaged, demagnetized, or simply malfunctioning when they are most needed—at the point of access. These drawbacks can lead to security breaches, operational inefficiencies, and frustration for both users and security personnel. But guess what?

There's a better way. You already know what it is.

Plastic Keycards Have Limited Functionality

Better than a big carabiner of keys clanking on your belt or in your purse, keycards at least avoid the annoyance of metal keys. Let's also not forget that sometimes you need multiple keycards to get into your work building, enter your office, and access amenities. All of which could run on different turnstiles, hardware, and software. Even with all of this activity, you can bet all these different vendors have no idea of interoperability and were never made to communicate with each other. This leads to confusion and chaos.



4 REASONS TO SWITCH FROM PLASTIC KEYCARDS TO DIGITAL OPTIONS

Mobile credential technology offers a significant leap forward in access control compared to traditional plastic keycards.

Digital Options are More Secure

The move from actual metal keys to plastic keycards was a historic improvement in security. A magnetic stripe - and later a chip - was a fantastic evolution that increased security measures for everyone, everywhere. Mobile credentials stored on your smartphone bring enhanced security. With the security mechanics built into your smartphone hardware and OS, it is more difficult to forge or copy. Smartphones can also pair multi-factor authentication beyond just the phone swipe, including requiring a PIN or biometric verification like a face scan or fingerprint. Unlike plastic keycards, if a smartphone is lost or the credential is compromised, access can be immediately removed remotely.

Digital Options are More Convenient

One of the most influential aspects of digital wallets is that they are simply more accessible and convenient. No juggling keys or shuffling through stacks of cards or unneeded panic attacks when you lose or forget your keycard. They provide improved access and reliability all around. Having the entire experience in your smartphone's digital wallet is an ease that no key or keycard could ever match. It's easier to update or revoke permissions on the security staff side. In addition, new users can be quickly added to the system with minimal effort, access rights can be easily granted, modified, or revoked based on user roles and needs, and mobile credentials can be programmed for specific access points, timeframes, or areas within a facility.

Digital Options are More Cost Effective in the Long Run

Going digital means cost savings. There's no need for physical cards, printers, distribution, inventory management, or replacement costs. Plus, with access management being easier, there's less administrative burden on security personnel and staffing.

Digital Options Work Well With Others

Plastic keycards and access control hardware and software aren't built to be flexible or interface with other systems. Digital credentials can be easily connected to other online systems and software making access more secure. Mobile credentials like digital wallet-based credentials can be integrated with other security systems' single sign-on systems, even intrusion detection or video surveillance. They can also be integrated with contactless payments, building automation systems, or event access control.

MORE SECURE, MORE CONVENIENT

LETS GET STARTED

Planning and Assessment: Evaluating Your Needs

A successful transition from keycards to mobile credentials requires careful planning and a thorough understanding of your organization's needs.

This section delves deeper into the essentials of evaluating and implementing a mobile access control system.

- 1. Document Your Current State.....7
- 2. Understand Your Users.....8
- 3. Vendor Selection: Selecting the Right System9
- 4. Define Budget and Scope.....10
- 5. How to Have the Best Digital Wallet Roll-Out11
- 6. Industry Best Practices You Should Know12

DOCUMENT YOUR CURRENT STATE

First Things First

You'll need to document your current access control protocols and mechanics. Be sure to outline the system's intended use – but also talk to staff to understand how it is *actually* used so you can identify any potential hacks or workarounds.



Questions To Answer

Compatibility: Can your current access control system integrate with a mobile credential solution?

Hardware Compatibility: Can your current card readers be upgraded to support mobile credentials? BLE or NFC or both?

Software Compatibility: Can your current access control software be integrated with the chosen mobile credential platform?

Data Integration: As you interview vendors, consider how user data (e.g., employee IDs, access levels) will be transferred to the new system. Also, how many steps (and how many people) will it take to add, update, or remove users in the system?

UNDERSTAND YOUR USERS

Once you've profiled the technology side of things, you need to look at the current user base.

Questions To Answer

User Demographics: Analyze the smartphone penetration rate among your employees so you know what percentage can move from a plastic keycard to a digital solution. You'll also need to know the distribution of operating systems. How many users are on Google Android devices versus Apple iPhones?

Technical Literacy: Consider the comfort level of your user base with technology. What devices and apps do they already use every day at work or at home?

Access Requirements: Identify the different access levels and security needs for various user groups (e.g., tenants, staff, employees, contractors, visitors).

Access Point Audit: Determine and map the number and variety of access points (doors, gates, elevators) to be integrated with a new mobile credential system.



VENDOR SELECTION: SELECTING THE RIGHT SYSTEM

As you start the vendor selection process, many questions must be asked and answered.

Here's a broad overview of what you should ensure goes into it:

WHICH CREDENTIAL TECHNOLOGIES DOES THIS VENDOR SUPPORT?

The two leading mobile credential technologies are BLE and NFC.

BLE

BLE is short for Bluetooth Low Energy. Users will use their smartphone's embedded Bluetooth to connect to the access control card reader. This provides a contactless digital experience without a keycard but has a few hitches: The user must open the digital credential app on their smartphone and ensure that both Bluetooth and location services are turned on.

NFC

NFC is short for Near Field Communication. Your phone manufacturer calls this a digital wallet. This is the same digital wallet technology that enables you to tap to pay for things with your smartphone. Digital wallet technology provides several advantages. There's no need to open an app, worry about Bluetooth being on, or have location services activated. It can also store more than one credential. For example, if there's one access control reader for the building but the user has another system to enter their floor or office, they can both be stored in a digital wallet.

DEFINE BUDGET AND SCOPE

If you're trying to make the case for switching from plastic to digital, it is essential to evaluate and present the economic value in a way that benefits the user and the business.

SHOULD YOU WORRY ABOUT THE CLOUD?

Older access control systems might store their data onsite—the server is down the hall or that old computer in the basement. This presents risks in the event the hardware is damaged or compromised. Nearly all modern access control vendors now use cloud-based user management. So, instead of user profile and access data being stored on a machine down the hall, it's stored in a cloud server with additional layers of security, redundancy, and disaster recovery.

Cost Analysis: Present the numbers that account for the upfront costs of implementing a mobile access control system and the long-term cost savings from eliminating keycards. Be sure to include the ongoing operating costs and costs associated with potential breaches. Plus, the annoyance users feel when they have to pay a fee to have a plastic keycard replaced.

Desired Features: Detail and prioritize the functionalities you require in this new mobile credential system (multi-factor authentication, access level management, audit trails).

Scalability: Consider your organization's future growth and choose a system that can accommodate additional users, access points, and even different properties in different regions.

Security Protocols: Ensure that the proposed mobile credential system aligns with your existing security policies and any regulatory or compliance requirements due to industry, customer base, or region.

User Preferences: Gather feedback from your user base about their preferences for mobile credential technology.

* By comprehensively evaluating these factors, you can decide on the most suitable mobile credential solution for your organization's needs and budget.

HOW DO YOU DECIDE?

Will keycards still work?

Some organizations go cold turkey. “Go digital or go home!” Others will take a gentler approach that allows for plastic keycards to remain usable as user adoption of the mobile credential increases.

How well does this vendor integrate with our existing infrastructure and security stack?

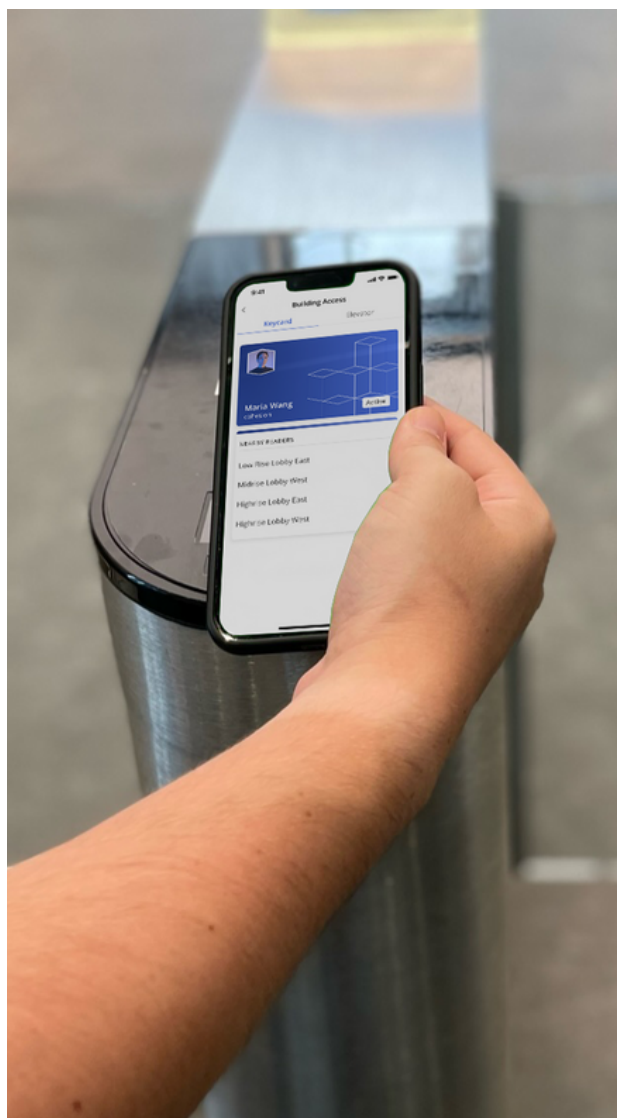
Your vendor should be able to document how they can work with your existing access control infrastructure and security stack, noting systems or methods that may need to be upgraded, replaced, or removed.

What additional security features do we need?

While BLE and digital wallet technologies are very secure, some organizations may want additional security. The same multi-factor technologies you see for logging in to software systems can also be used here.

What support does the vendor give you before, during, and after the roll-out?

Some vendors throw things over the wall and yell, “Good luck with all of that!” Be sure the vendor you choose supports you with user adoption consulting, security staff admin and training, expansion into new properties, and support coverage for the occasional hiccup.



HOW TO HAVE THE BEST DIGITAL WALLET ROLL-OUT

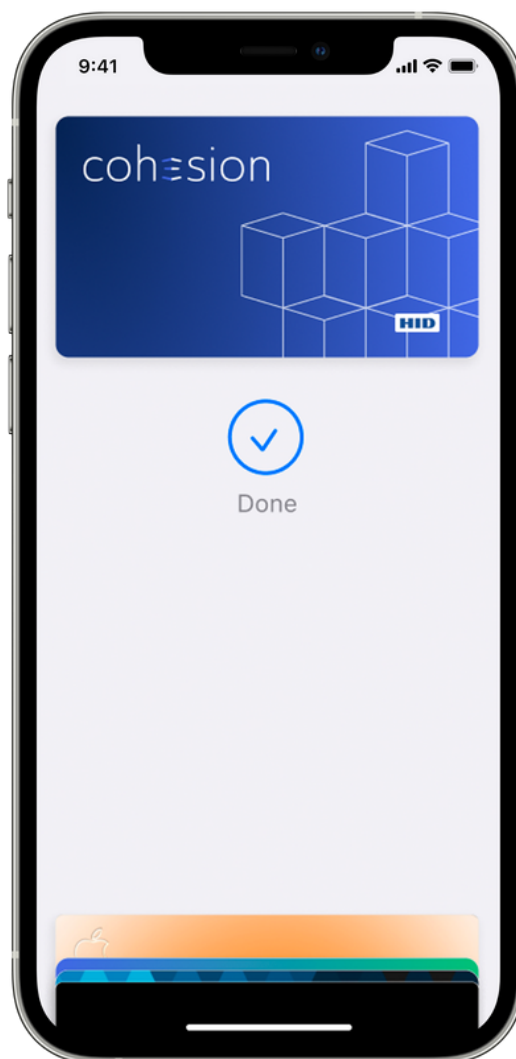
After your vendor selection committee has gathered requirements, talked to vendors, seen demos, and received proposals, it's time to get going and select a vendor.

Most organizations will start the vendor working on one property or set of buildings first, converting one property in their portfolio from plastic to digital or adding digital while continuing to allow plastic keycards. A phased rollout will help test the systems' functionality and how well the users understand the technology and how this rollout may scale to the rest of your organization.

Be sure your first set of users is diverse enough to match the variation in the overall population of users.

Finally, define your success metrics for this first phase of your roll-out:

- What adoption rate are you wanting to achieve in the first 3 months?
- How will you measure user satisfaction?
- How easy is it for staff to manage and administer the system?



THE MAIN STAGES OF A PLASTIC TO DIGITAL MIGRATION PILOT ARE:

1 Configuring Access Control Point

- Upgrade existing readers or install new mobile credential readers at designated access points.
- Program the readers to recognize the chosen mobile credential technology (e.g., NFC, BLE).
- Define access rules for each reader, specifying authorized users and access levels.
- Conduct thorough testing to ensure all readers function correctly with mobile credentials.

2 Integrate HR and Directory Services

If applicable, integrate the mobile access control system with your HR or directory services platform. This will streamline user provisioning by automatically adding new employees and updating access rights. Ensure data security during the integration process and follow data privacy regulations.

3 Establish a Communication Plan and Schedule

Develop a clear and comprehensive communication plan to inform users about the transition from keycards to mobile credentials. Your vendor should be able to help with this with existing templates and collateral you can customize.

- Explain the benefits of the new system.
- Address any security concerns and emphasize the enhanced security features.
- Utilize multiple communication channels (e.g., email, signage in lobbies, town halls, video tutorials) to reach all user groups.

4

User Training

Along with the communications above, be sure to develop and provide user training on downloading and using the mobile credential app or adding the credential to your mobile wallet.

- Offer training sessions or create user guides with clear instructions and step-by-step walkthroughs.
- Consider offering different training formats (e.g., in-person sessions, and online modules) to accommodate diverse learning styles.
- Train IT support staff and onsite security staff to assist users with troubleshooting and answer common questions.

5

Confirm Deployment Timeline

Clear Timeline: Establish a clear timeline for phasing out keycards and transitioning to mobile credentials.

- Communicate the timeline to all users well in advance, including key milestones and deadlines.
- Allow for sufficient overlap between the old and new systems to give users an adjustment period. Expect some users to backslide to the old system and find ways to encourage them to get into the fold.

Ongoing Team Communications: Maintain open communication channels with users throughout the rollout process.

- Provide regular updates on the progress and address any concerns or questions promptly.
- Gather feedback from users to identify areas for improvement and ensure a positive user experience.

* By following these steps, you can ensure the smooth and successful implementation of your mobile credential system, minimize disruption, and maximize user adoption.

INDUSTRY BEST PRACTICES YOU SHOULD KNOW

Transitioning to mobile credentials offers significant security benefits, but maintaining a robust security posture requires ongoing vigilance. This section explores critical security considerations and best practices for managing your mobile access control system.

Security Best Practices

User Education on Phishing Scams

- Train users to identify phishing attempts that trick them into revealing their PINs or login credentials.
- Educate them on how to distinguish legitimate app notifications from fraudulent ones.
- Emphasize the importance of only downloading the mobile credential app from official app stores.

Lost or Stolen Phone Protocols

- Develop clear procedures for users to report lost or stolen phones.
- Implement a system for immediate remote revocation of stolen mobile credentials, restricting access.
- Encourage users to enable "Find My Device" or similar functionalities to locate lost phones and potentially wipe data remotely.

Strong PINs and Multi-Factor Authentication (MFA)

- Enforce strong PIN policies that require complex combinations of letters, numbers, and symbols.
- Implement multi-factor authentication as a mandatory layer of security. This could involve a fingerprint scan, facial recognition, or a one-time passcode sent via SMS.
- Educate users on the importance of not sharing their PINs or authentication credentials with anyone.



INDUSTRY BEST PRACTICES YOU SHOULD KNOW

System Monitoring and Maintenance

Regular System Audits

- Conduct regular security audits of your mobile access control system to identify and address potential vulnerabilities.
- Stay updated on the latest security threats and patch any software vulnerabilities promptly.
- Partner with your mobile access control provider for security recommendations and updates.

Credential Updates

- Encourage users to regularly update their mobile device operating systems and the mobile credential app.
- Implement a system for automatic or prompted updates to ensure users have the latest security patches.

User Access Management

- Establish transparent processes for granting, modifying, or revoking user access privileges based on their roles and responsibilities.
- Regularly review user access rights and ensure they are aligned with current job functions.
- Deactivate access credentials promptly when employees leave the organization or change roles



* By prioritizing these security best practices and maintaining a proactive approach to system monitoring and access management, you can ensure your mobile credential system remains secure and protects your organization's physical assets.

CONCLUSION

A SECURE AND CONVENIENT FUTURE WITH MOBILE CREDENTIALS

Transitioning from traditional plastic keycards to a mobile credential system offers many benefits for VPs of Physical Security and their teams.

Here's a Recap of the Key Advantages:

Enhanced Security: Mobile credentials leverage secure elements within smartphones, multi-factor authentication, and remote revocation capabilities, significantly reducing the risks associated with lost or stolen keycards.

Improved Convenience: Users are less likely to lose or forget their phones, eliminating access disruptions and streamlining the access control process.

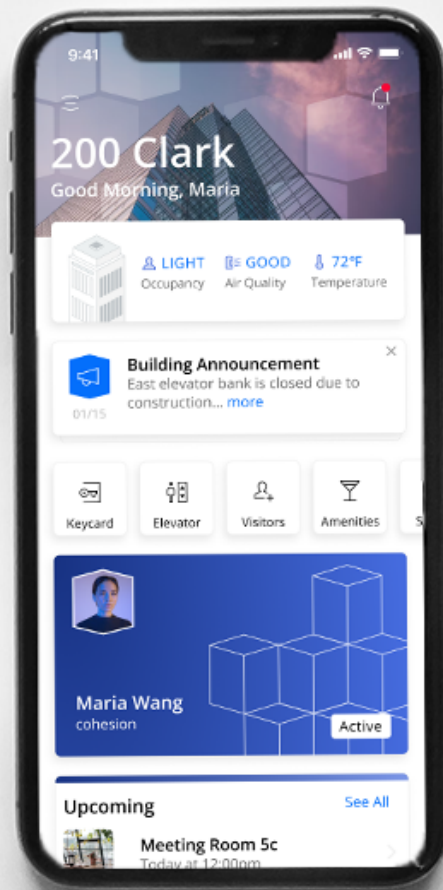
Increased Cost-Effectiveness: Mobile credentials eliminate the need for physical cards, reducing printing, distribution, and replacement costs. Additionally, streamlined access management lowers administrative burdens.

Greater Scalability and Flexibility: New users can be easily added to the system, and access rights can be granted or revoked efficiently. Mobile credentials can be programmed for specific access points and timeframes.

Enhanced Functionality: Mobile credentials can integrate with other security systems and building automation technologies, offering a more comprehensive security and access control approach.



LET'S GET TO IT.



Ready to get started?

Talk to one of our migration experts today about making the move to digital wallet. We have a complete transition and upgrade plan ready and waiting.

Go to cohesionib.com

cohesion