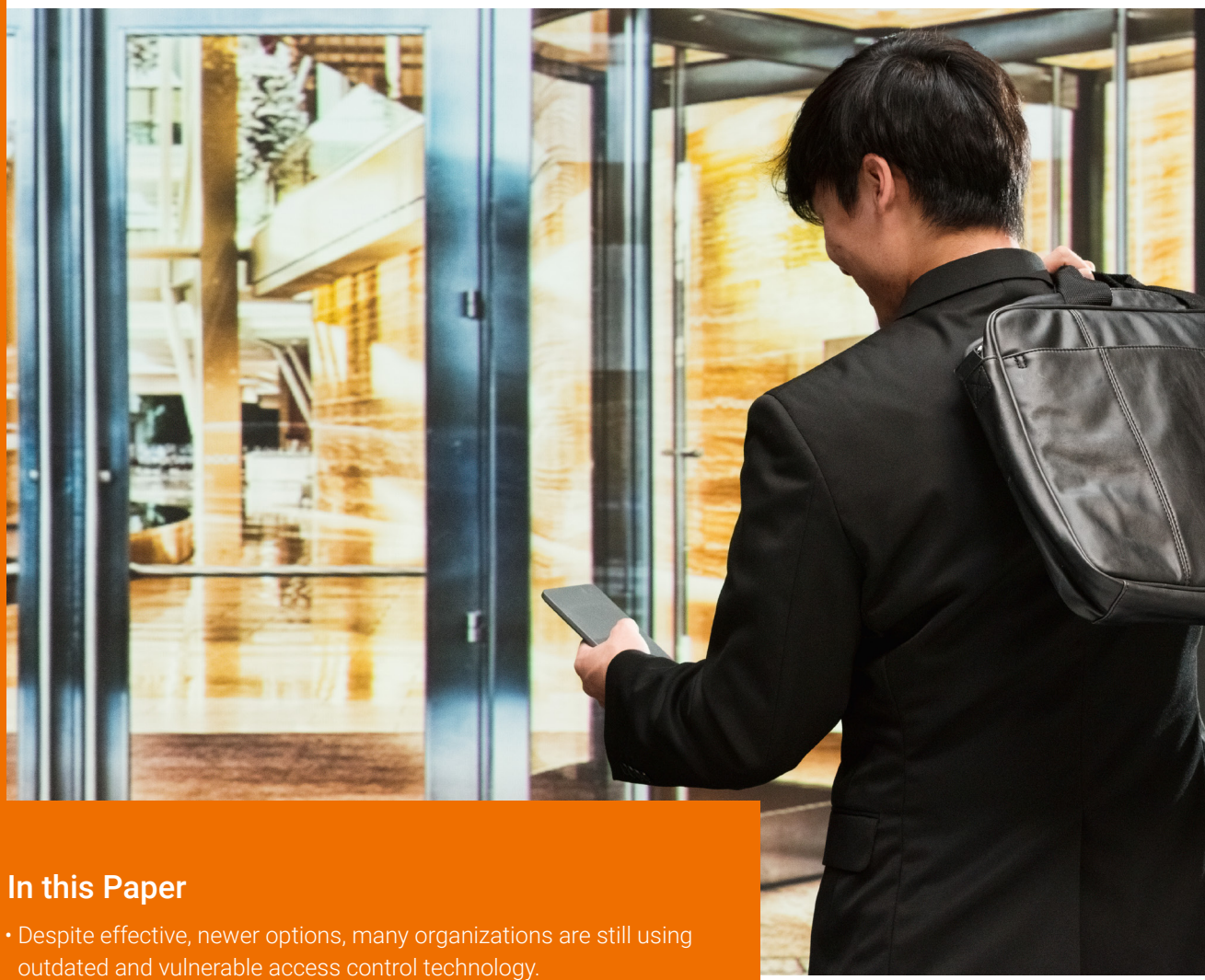
EXECUTIVE BRIEF

Sponsored by

HID

The Evolution of Cards and Credentials in Physical Access



In this Paper

- Despite effective, newer options, many organizations are still using outdated and vulnerable access control technology.
- Allowing building occupants to use their mobile device or wearable to enter controlled areas is the next generation of access control.
- Reaping the advantages of mobile and next-generation access control technologies requires a modern ecosystem.

Introduction

Physical access control has been a key component of many organizations' security strategies for several decades. Like any technology, access control has evolved over the years, and solutions now offer more security and convenience than ever before. From swipe technologies, such as the now antiquated magnetic stripe, to a variety of contactless technologies and mobile access credentials, businesses now have several choices when it comes to access control.

Despite the enhanced security and convenience that comes from newer options, many organizations are still using outdated and vulnerable access control technology. For these organizations, the time has come to analyze their security ecosystem and prioritize plans for a much-needed upgrade.

To better illustrate the importance of upgrading to the latest access control technology, let's explore the evolution of cards and credentials technologies. We will examine the technologies available today and the bright future of mobile access, as well as clarify why you should ensure that each component of the access control ecosystem is as secure as possible.

The Evolution of Cards and Credentials in Physical Access

Electronic physical access control has played a key role in enterprise security for decades, evolving from swipe technologies in the 1980s to first-generation contactless smart cards in the 1990s and 2000s, and subsequently to second-generation contactless smart cards, which emerged at the start of this decade.

> "Despite the enhanced security and convenience that comes from newer options, many organizations are still using outdated and vulnerable access control technology."

To fully understand today's technology, it is important to understand the evolution and transformation of access control, detailed below.

1980s — Swipe Technologies: Initial swipe technologies were a major administrative improvement over manual locks and keys in terms of management, traceability, and forensics. Knowing who had access rights to certain areas and being able to efficiently control those rights removed the need to re-key as employees left or changed roles in the organization.

The fundamentals of swipe technology are simple with straightforward and universal usability: Contact technology requires a manual swipe to transfer the unencrypted credential's information to a reader. When the user needed access to a particular area, she would physically swipe a card — much like a credit/debit card in a retail store or gas station — through a card reader.

Primary PACS technologies were:

- Magnetic stripe cards
- Wiegand swipe cards
- Barium ferrite cards

Because the credential is unencrypted, swipe technologies are less secure than today's offerings, but they provided adequate

security for the time, partly because to read or clone data, hackers were required to physically obtain the card.

1990s – "Prox": In time, the limitations of swipe technologies began to be felt. The need for physical contact between readers and credentials could be cumbersome and inefficient for users, while broken cards and physical wear on readers became costly and time-consuming for administrators.

Thus, the emergence of contactless technologies was a game-changer in the access control industry. The predominant technology during this phase is known as "Prox", also known as "low frequency proximity". It featured low frequency, 125 kHZ technology whereby the data on the card is detected when presented a few inches from the reader. Prox also provided the additional option of leveraging fobs and tags as form factors, meaning users were no longer required to use a card.

Although Prox benefited the access control industry by ushering the proliferation of electronic physical access control thanks to lower maintenance costs, increased user convenience, and new options for form factors, the technology had limitations. To start, the credential is unencrypted, static, and can be read in the clear, making the cards easy to clone or forge. Prox cards also cannot be encoded with multiple IDs or other data attributes.

Late 1990s-2010s — First-Generation Contactless Smart Cards: Around 2000, contactless smart cards emerged that offered more sophisticated technology than Prox. These smart cards, including brands such as MIFARE® and iCLASS®, utilized high frequency technology (13.56MHz) and featured new credentials. They also addressed the two main limitations of Prox cards.

First, the reader and credential could mutually authenticate on every transaction, providing an increasingly important layer of data privacy and security. With mutual authentication, both the credential and reader contain a set of cryptographic keys (consider these keys like a password or shared secret handshake). When the credential is first presented to the reader, the two use a complex mathematic process to compare keys. If it is determined that the keys match, the credential shares the binary data with the reader and the reader accepts it as genuine. However, if the keys do not match, the credential will keep the binary data private and the transaction will be terminated with generally no reaction from the reader.

Second, these cards could store more information than just an ID number, such as a cashless vending debit value or a biometric template. The result was a substantial increase in both security and multi-application functionality.

Despite these benefits, most first-generation smart cards have vulnerabilities in the mutual authentication algorithms that have been exposed by researchers in published documents. Such vulnerabilities make it possible for a hacker to forge/clone/spoof a credential as if the mutual authentication was not present. Secondly, cryptographic keys must be unique to an organization and treated as highly confidential information. Further, all devices that contain the keys (credentials, readers, encoders) should store the keys and execute cryptographic operations on a secure hardware platform/chip such as a secure element.

Because of these vulnerabilities, a new, more secure wave of contactless smart cards entered the market.

> "Initial swipe technologies were a major administrative improvement over manual locks and keys."

2013-Present — Second-Generation Contactless Smart Cards: Earlier this decade, contactless smart cards evolved further to better meet the needs of today's businesses. Second-generation contactless smart cards differ from their predecessors in two key areas: security and applications.

1) *Security:* Gone are the proprietary protocols that were more vulnerable in first-generation smart cards. Among the many downsides of proprietary protocols are that they are developed by one company and thus subject to blind spots that accompany a single point of view. Such blind spots inevitably lead to greater vulnerability, as issues cannot be fixed until the vendor is alerted to the issue, marshals resources to develop a patch or new version of the software that addresses the bug, and then releases it.

   Today's credentials feature open, widely adopted standards that did not exist when first-generation smart cards were created. Developed and approved by a broad research and academic community (e.g., ISO and NIST), these open standards are consistently updated and adjusted, enabling them to be leveraged across multiple technologies. Incorporating these inspires confidence for better protection both within and outside the organization.

2) *More applications:* Second-generation smart cards (e.g., iCLASS® Seos® cards) aren't just more secure, they are architected to enable virtually unlimited applications. Today's organizations are seeking the ability to manage user identities independent of the underlying hardware form factor (and micro-processor chip). These organizations want to be able to create and manage 'secure identities', not just on cards but also on mobile phones, tablets, wearables and other credential form factors, connecting through NFC, Bluetooth and other communication protocols.

   This has allowed for additional use cases for smart cards and logical access — controls intended to identify, authenticate and authorize access to networks and information — and enabled convergence between physical and logical access. Secure printing and cashless vending are additional examples of easier and more flexible applications that second-generation smart cards can facilitate.

As Internet usage and mobile devices further transform user expectations in every aspect of life, including access control, organizations are now shifting from storing credentials on a physical card to a mobile device.

The Next Generation of Credentials — Mobile Devices: Much of the next generation of credentials is already here. Mobile devices are well entrenched in nearly all aspects of everyday life. Allowing building occupants to use their smartphone, tablet or wearable to enter controlled areas to supplement or replace cards will likely be well accepted by all involved parties.

The benefits to both business and employee are clear. First, there is the convenience factor for employees in having to carry fewer items. Also, because very few people go anywhere without their mobile device, lost or forgotten cards will be less of an issue. Mobile credentials also allow users to authenticate from a distance, meaning they are not required, for example, to roll down their car window in cold weather to open a parking gate.

Secondly, mobile credentials make the administration of access control easier. Digital processes make it simple to streamline operations with integration to access control or visitor systems. Organizations can provide remote workers and visitors with credentials over-the-air and replace physical credential management with a digital experience. Beyond saving time and resources, the result is a more sustainable process with reduced waste and a smaller carbon footprint.

Mobile credentials offer security benefits as well, providing higher levels of authentication in physical access control. Because credentials are granted and revoked over-the-air, it is easy to deactivate users and deprovision unauthorized devices. For companies with numerous short-term employees or long-term vendors frequently on premises, this streamlines credentials management.

In addition, mobile credentials are advantageous due to their dependence on the device itself. Unlike cards, mobile devices are

rarely forgotten, lost, or stolen. Should they go missing, the loss is reported almost immediately. Furthermore, applications can be protected with biometrics or passcodes, and vulnerabilities can be addressed quickly through remote updates.

With mobile authentication, only one device is needed to provide secure access to cloud applications, data and the physical door. Policies can be established that leverage this convergence (e.g., network access is allowed only after authentication at the door, or a VPN connection is permitted only after a GPS has been verified that it is in sync with travel plans).

With proper implementation, this convergence will reduce costs, enhance user experience, simplify management and improve security. But to achieve this, organizations must have the right equipment to create a secure access control ecosystem, including both strong readers and credentials.

The Danger of One Weak Link: Using "Me-Too" Cards with Newer Readers

After making an investment in modern readers, some organizations may look to cut costs by purchasing cheaper cards and credentials. This is a mistake. The reader is only as secure as the weakest credential it supports. Ensuring the security of the entire ecosystem, including cards, is not something that should be driven by cost.

One common example is when an organization purchases less expensive cards from a third-party reseller. Colloquially known as "me-too" cards, these cards and credentials are marketed with the promise that they will work with state-of-the-art readers. However, these cheaper credentials often use technology that is easier to hack or duplicate and do not offer the same security.

> "However, these cheaper credentials often use technology that is easier to hack or duplicate and do not offer the same security."

While the temptation to save money is strong for many companies, enterprises should be extremely cautious when it comes to security. It takes only one misstep to create a massive vulnerability that can impact the entire ecosystem. This is why it is so important for each organization to perform their own risk analysis to determine the right choice for their needs.

Skimping on security to save money can often result in a more expensive proposition in the long run. The cost of a security breach, an increased possibility due to the vulnerabilities that less sophisticated cards introduce, can be much higher than the cost of buying more sophisticated cards and credentials.

Beyond financial costs, as recent news indicates, a breach can have a significant impact on company reputation. For large businesses, any type of data or security breach can turn into a high-profile incident. For smaller and mid-sized businesses, less sophisticated cards and credentials can result in a failed security audit that requires a larger, more costly upgrade.

In addition, vendor selection matters. Cards from reputable providers most often come with a lifetime warranty, something that cheaper "me too" cards simply don't offer. Working with a reputable provider also means that you have go-to customer service, as well as important capabilities like card printing, a choice of multiple form factors, personalization options for re-badging, and customized card printing options.

Conclusion

Cards and credential technologies have come a long way since they first hit the market over 30 years ago. The transition from

Magstripe to Prox in the mid-1990s introduced early contactless technology capable of storing unencrypted credentials inside the card.

Today's contactless smart cards follow industry protocols, making them much more secure than prior generations. As access control technology finds a role in more than just physical access, mobile devices have been found to be a synergistic fit, as they offer not only more security and convenience in a cost-effective form factor, but also increased functionality in the form of applications.

Reaping these advantages requires a modern access control ecosystem, however. Only a modern ecosystem will be able to keep pace with the transformative trends today's organizations are facing.

Fortunately, upgrading your physical access control system is not as difficult as you may think, as it often only requires installing new readers and issuing new credentials.

To learn more about how a modern access control ecosystem can benefit your business, go to https://www.hidglobal.com/access-control.