A Brief History of Access Control Credentials

HOW TECHNOLOGY HAS EVOLVED TO REDUCE VULNERABILITIES

Contents

Introduction	**3**
The Danger of One Weak Link	**4**
Credential Technology Through the Years	**5**
The Next Generation of Credentials	**10**
The HID Mobile Access® Solution	**11**
Conclusion	**12**

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, like the now antiquated magnetic stripe, to contactless technologies and mobile access credentials, businesses now have several choices when it comes to access control.

Despite the enhanced security and convenience offered by newer options, many organizations are still using outdated and vulnerable access control technology. For these organizations, the time has come to take action and prioritize plans for a much-needed upgrade.

To better illustrate the importance of upgrading to the latest access control technology, we take a step back in time to explore the evolution of cards and credentials technologies between the 1980s and the present-day. We examine the technologies available today and the bright future of access control, as well as clarify why using out of date access control technology can leave your organization at risk.

[1] Access Control Systems Trends Survey, HID Global and Security Management Magazine, 2019.

Access control components are aging and most organizations report that any upgrades will take place years into the future, if they're planned at all[1]

Software

48% / 32% / 19%

Credentials

58% / 29% / 13%

Controllers

61% / 28% / 10%

Readers

63% / 27% / 10%

Timescale for Upgrades

3-6 years **1-2 years** **< 1 year**

The Danger of One Weak Link

Using Legacy Card Technology with Newer Access Control 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 has been enabled to support. 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. Such 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, therefore compromising the security level of the entire system**.

While the temptation to save money is strong for many companies, 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.

To better illustrate the importance of upgrading to the latest access control technology, let's explore the evolution of cards and credentials technologies.

Credential Technology Through the Years

1980s

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

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, they would physically swipe a card — much like a credit or debit card in a retail store.

The Dangers

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.

1980 1990 2000 2010 2020

1990s

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.

The Dangers

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.

1980 1990 2000 2010 2020

Late 1990s-2010s

At the turn of the century, 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 (13.56 MHz) and featured new credentials. They also addressed the two main limitations of Prox cards.

First, mutual authentication, both the credential and reader contain a set of cryptographic keys (consider these keys like a password). When the credential is first presented to the reader, the two use a complex mathematic process to compare keys. If 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.

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.

The Dangers

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.

1980 1990 2000 2010 2020

2010s-2020

As the security landscape continued to evolve, so did access control credentials. Second-generation contactless smart cards (e.g: Seos® and MIFARE DESFire EV3) were introduced to meet the needs of dynamic businesses. Second-generation contactless smart cards differ from their predecessors in two key areas: security and applications.

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 resource to develop a patch or new version of the software that addresses the bug, before subsequently releasing.

Second-generation credentials also offer enhanced privacy protection and feature open, widely adopted standards 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.

1980 1990 2000 2010 2020

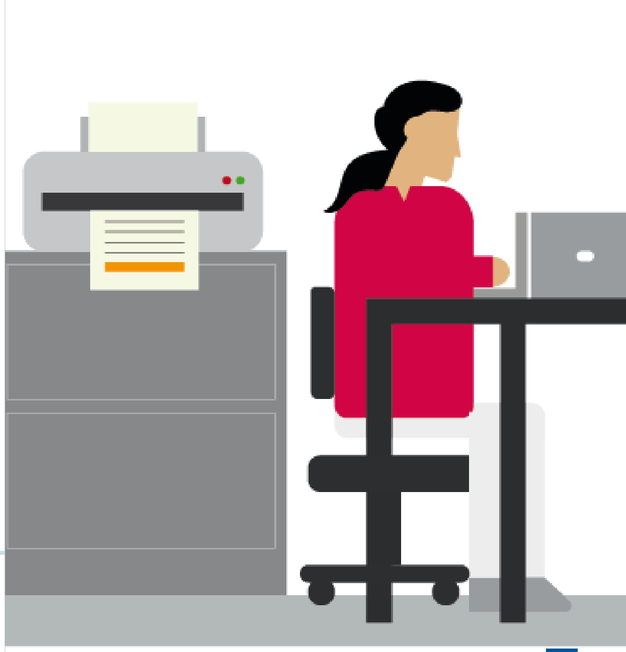
More Applications

Second-generation smart cards are architected to enable virtually unlimited applications with enhanced data and privacy protection. 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 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.

During this time, mobile devices transformed user expectations in every aspect of life, including access control.

These trends would quickly impact how organizations address security and improve the user experience when managing access control, including the shift from storing credentials on a physical card to a mobile device.



1980 1990 2000 2010 2020

The Next Generation of Credentials

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 contactless entry to doors and authentication from a distance, meaning users 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. In the event of a security issue, a user's credential can also be deprovisioned quickly and efficiently. Beyond saving time and resources, the result is a more sustainable process with reduced waste and fewer physical touchpoints.

A Brief History of Access Control Credentials

With mobile authentication, only one device is needed to provide secure access to cloud applications, data and the physical door. Following proper implementation, this will:

Reduce costs

Enhance user experience

Simplify management

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 HID Mobile Access® Solution

HID Mobile Access® introduces a new era of convenience and functionality to access control. Breakthrough technologies meet the growing demands of a smarter, mobile-first world - while instilling confidence that identity data is secure and privacy is protected.

More Choice

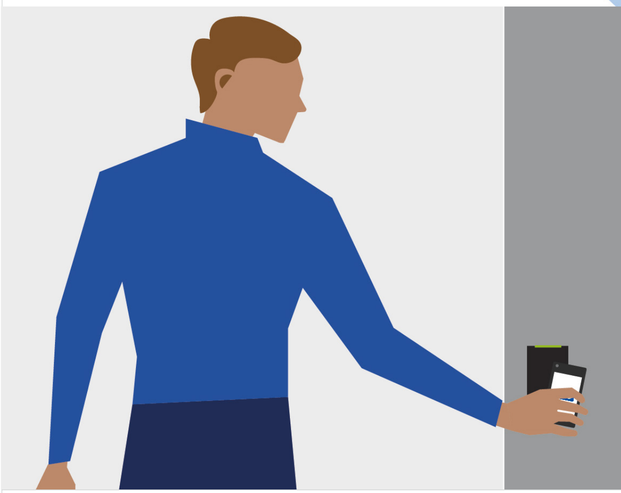
Mobile technology is being leveraged at a rapid pace. The freedom to move access control to phones, tablets, wristbands, watches and other wearables is a matter of end-user preference. HID Mobile Access® is a platform-neutral solution and supports the widest variety of mobile devices in the industry today, or it can be used in addition to traditional card access.

More Applications

Managing identity in the organization is changing; IT departments, Security and Facility Management are working toward the development of consolidated access programs. HID Mobile Access® enables more than one secure identity to reside in a smart device - creating a single device solution for physical and logical access control.

More Confidence

HID Mobile Access®, powered by Seos technology, is based on ISO standards used by the U.S. government and other organizations globally to encrypt classified or sensitive data, providing unprecedented security and privacy protection of identity data.



Conclusion

Cards and credential technologies have come a long way since they were first introduced over 40 years ago.

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.

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.

Learn more about how a modern access control ecosystem can benefit your business.

CONTACT US

North America: +1 512 776 9000 • Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 • Latin America: +52 55 9171 1108

© 2020 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design and HID, the HID logo, iCLASS SE, Seos, iCLASS and HID Mobile Access are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.
2020-09-08-hid-card-evolution-eb-en PLT-03288

An ASSA ABLOY Group brand

ASSA ABLOY