ARE YOUR CREDENTIALS STUCK IN THE 70S?

KeShia Thomas, Brand & Solutions Marketing Manager at Allegion reveals why and how to upgrade your access control credential technology effectively

ID cards and credentials play a vital role in an organization's day-to-day activities, from controlling access to cashless payments, visitor management and more. The global physical security market was valued at $127 billion in 2022 and is estimated to continue to grow at 6.8% annually until 2030 (Grandview Research). Post pandemic, security remains top of mind for companies, no matter the size.

With so much riding on the credential, why are so many people still relying on technology that has been around since the 1970s? According to the 2022 OMDIA market report, nearly 50% of the credential units sold in 2021 featured outdated and unencrypted proximity technology.

There are many reasons why businesses might consider upgrading their credentials to newer smart cards and mobile credentials for access control. However, some are not sure where to start or they don't know what they need to make the transition. Understanding the benefits of upgrading and outlining a clear, strategic migration path from your current state to your ideal future state can help make it a smooth transition.

> "SMART CARDS AND MOBILE CREDENTIALS OFFER ENCRYPTED SECURITY, WHICH CAN PROTECT AGAINST UNWANTED DUPLICATION."

The benefits of upgrading your credential

More security for a safer tomorrow

Encryption is like a technologically advanced handshake. It protects the data being relayed between the reader and credential by essentially taking the information in the chip of the credential, scrambling it, sending it to the reader and putting it back together. It does this by using a microprocessor and encryption algorithm to protect the data when it is transmitted over the air.

Proximity and magnetic stripe cards are unencrypted, leaving organizations vulnerable to duplication, threats and unauthorized access. There are devices, hacker tutorials and cloning kiosks that make duplication easier and more accessible than ever.

Smart cards and mobile credentials offer encrypted security, which can protect against unwanted duplication. These credentials offer the highest in physical security and deliver the perfect balance of security, speed and performance. Mobile credentials can use the same level of encryption as smart cards and in some cases these technologies use more advanced encryption. It's based on the design of the mobile credential, so it's important to inquire about the encryption upfront.

More convenience for seamless visitor and employee experiences

When considering an upgrade, the overall user experience is an important factor to focus on when making a decision. Can your employees access printers or other items with the same credential that allows them to effortlessly move around a facility? The goal for most organizations is to simplify the credentialing process as much as possible. Carrying multiple cards and brass keys isn't ideal anymore.

Smart credentials can be used in multiple applications beyond access control, such as transit, cashless vending and cafeteria point-of-sale. They also come with more computing power than proximity or mag stripe options, which allows users a single credential. It's also much more convenient for users.

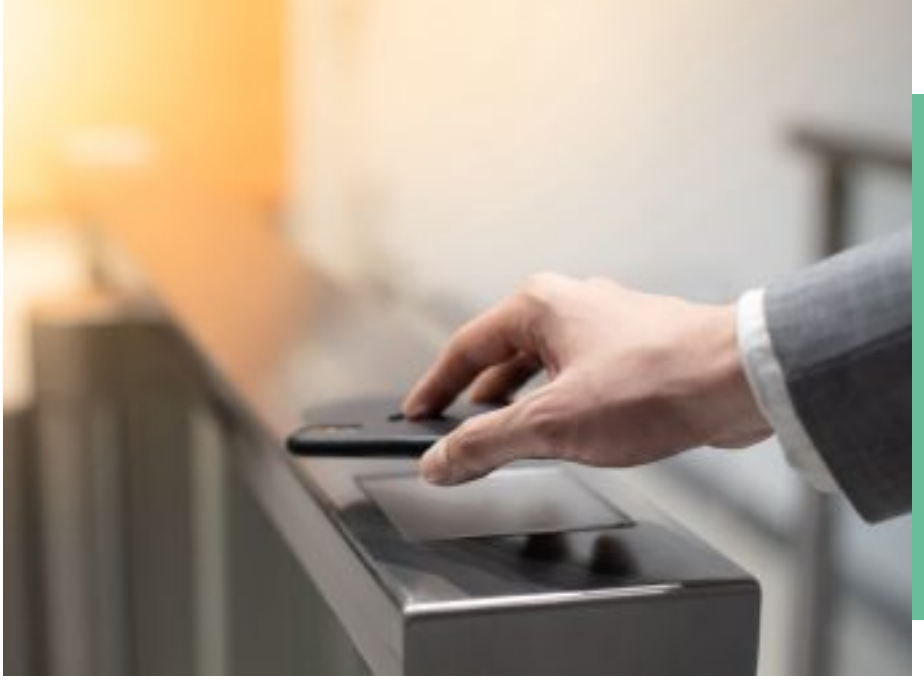
Mobile IDs make access and transactions throughout any organization seamless and gives users the option of just carrying their mobile device if their employer does not require them to carry an ID card.

More efficiency for your organization through virtual experiences

Being on the forefront of new technology can open doors for organizations around the globe to help them work smarter. The pandemic highlighted the need for smarter solutions for people who are working remotely or in a hybrid environment that supports a safe and seamless experience for employees and visitors.

There are other advantages to having a physical smart card. Organizations often require employees, contractors and visitors to wear an ID badge in conjunction with a credential reader to gain access to their facility. Additionally, combining what might have been ▸

> "MOBILE IDS MAKE ACCESS AND TRANSACTIONS THROUGHOUT ANY ORGANIZATION SEAMLESS."



two or more cards helps from a management perspective.

With mobile credentials, digital IDs can be issued virtually, eliminating the need for most employees to have to come to the office to pick up a physical card. It also saves costs associated with ordering and printing.

More flexibility for today and in the future

Another common reason organizations want to upgrade their credential technology is to stay current by pioneering and adopting the latest technology. When it comes to your ID cards, preparing for the future relies heavily on the openness of your platform. Interoperability enables various systems from different manufacturers to communicate, exchange and interpret information.

One way to accomplish this is through custom encryption keys. With ID card systems, interoperability permits the credential to work with a range of software, hardware and applications, including door access and more. This means you get the freedom and control to choose best-in-class solutions and vendors that will meet your organization's specific needs.

How to effectively migrate your credential technology

Each organization has different security needs and different pain points that need to be addressed. For example, a larger business with tens of thousands of people moving throughout multiple buildings is going to have vastly different security needs compared to a smaller business with only a few employees. That said, a mobile or smart solution that's interoperable is a suitable choice for most companies.

When an organization chooses an interoperable mobile or smart card solution featuring custom encryption keys, they are shifting in the direction of a solution that offers a higher level of security, flexibility and convenience. This creates a safer environment for all and gives peace of mind to organizations of all sizes.

Each business should evaluate their needs, such as security, convenience and budget, to determine their ideal future state.

> **"BEING ON THE FOREFRONT OF NEW TECHNOLOGY CAN OPEN DOORS FOR ORGANIZATIONS AROUND THE GLOBE TO HELP THEM WORK SMARTER."**

How to get there will depend on your current hardware and technologies that you have in place. Many organizations have found it helpful to conduct a hardware audit upfront to determine what is needed in the future and how to make it happen.

Understanding what you have today and where you want to go tomorrow will help you plan a successful migration path – a strategy to upgrade your credentials to a smarter version. Do you have hardware in place that will support any credential upgrades you make in the future including mobile? Do you need mobile or smart card readers? Does your access control system support mobile IDs? All of this should be considered as you strategize your transition and shift to a more secure credential plan.

Here are some possible recommendations to consider when developing a migration path:

- Remember that this will look different for each organization. It should be a personalized approach that fits your company's individual needs
- Document your current state and ideal future state, knowing it might not be a direct jump from one to the other
- Involve all the stakeholders upfront. Communication and collaboration are crucial to success

Review the pros and cons of upgrading, challenges, possible scenarios and more with your team

- The interoperability of credential technology is important to your future choices in hardware and software. Regardless of the technology you choose, it's important to pick an open, secure platform that offers flexibility ▪