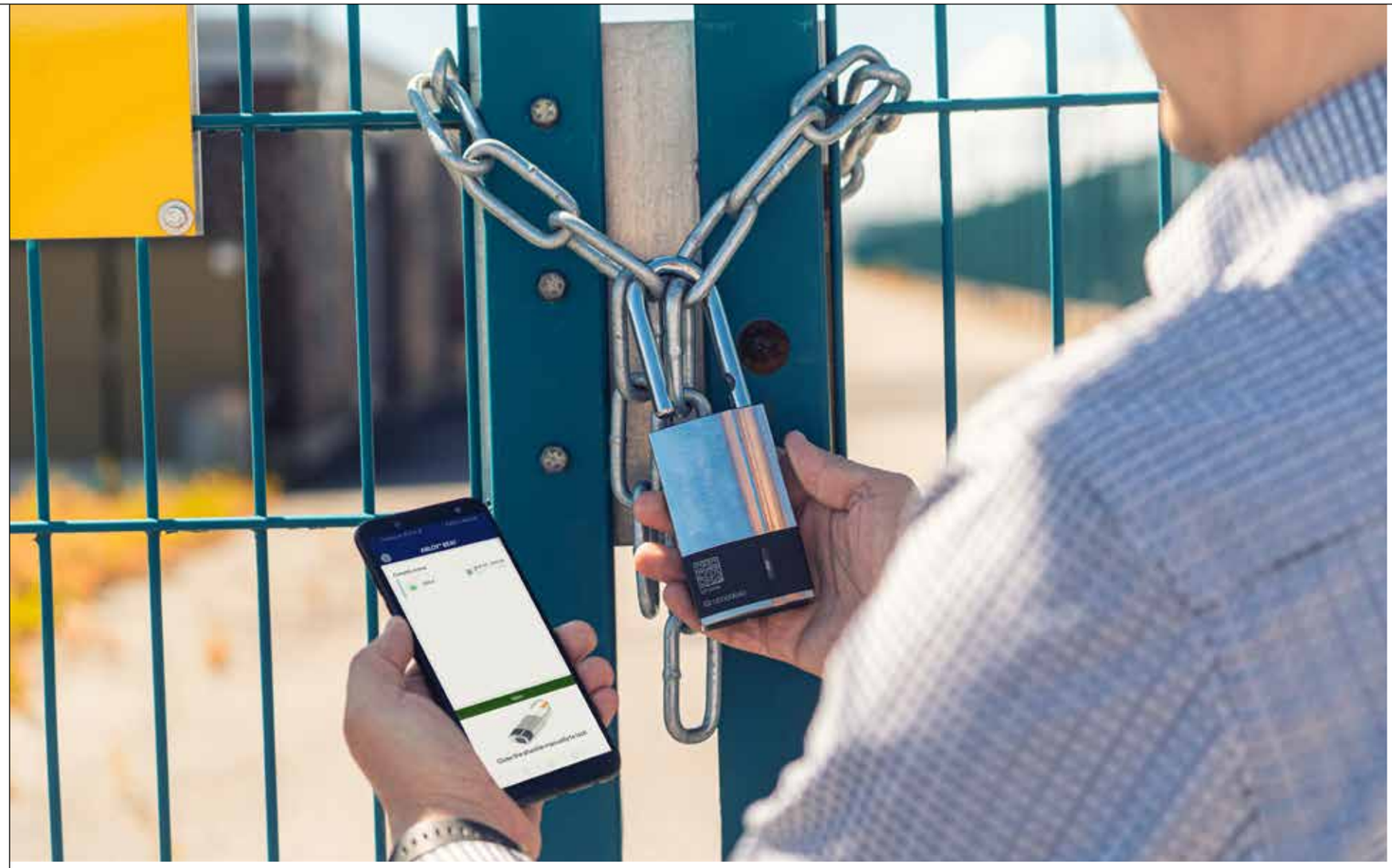

Picture credit: ABLOY

OPENING DOORS

Steve Wintle *reports on mobile credentials and how they are revolutionising access control for a digital world*

The world is adopting new technologies at an astounding rate, and as a society we are becoming more reliant on digital devices. When it comes to managing access control, mobile credentials are similarly gaining popularity across a wide range of industries and applications.

A mobile credential is a digital access key that sits on a smart device such as a mobile phone. This replaces a traditional credential such as a key, fob or card. A mobile credential allows you to authenticate with your smartphone and use it as your key to gain access to a building, room or location.

Forecaster IHS Markit predicts over 120-million mobile credentials will be downloaded in 2023 – an enormous increase in contrast to the 4.1-million downloads recorded back in 2018. Furthermore, research finds that over two-thirds of organisations will have adopted mobile access control to some extent within the last two years.

Here, we explore some of the reasons for this increased demand for mobile credentials, including the need for flexibility and convenience, an easy way to manage access rights with instant delivery and increased security and sustainability. We also consider some of the barriers to implementation of mobile credentials and recommend which type of applications are most likely to have the most success.

The global mobile workforce – a group of employees not bound by a central physical location but connected by various types of mobile technology – is expected to reach 1.87-billion workers by 2022, and this new way of working brings a requirement for adaptable and flexible access control.

Mobile credentials offer a way to enable access permission changes in real time for contractors travelling between remote sites

Mobile credentials offer convenience as there is no need for a separate RFID credential when you open secure doors and openings with a device you already carry. They are also flexible, as facility managers can amend, issue or cancel credentials from anywhere and building users always have their access rights up to date. Plus, as mobile credentials are updated wirelessly and remotely, it reduces face-to-face contact for both staff and visitors as they do not need to collect a card or fob. This improves efficiency too, as employees waste less time collecting or amending access credentials in person and visitors get instant temporary access as and when they require it.

Passwords are no longer enough in the cyber world as they can be shared, stolen and copied – just like some keys. The only way to overcome this issue is to verify the identity of each individual that is attempting to gain access.

Identity verification has become standard practise in society, for example in the realm of online shopping. Consumers are familiar with having to enter a verification code when using a shopping app to confirm their identity, and this offers peace of mind that their details are secure.

Mobile credentials utilise on-device passwords and biometrics such as fingerprint, voice and facial recognition, to keep unauthorised people from accessing the key stored on the smartphone. They are also seen as a more secure way to manage access because people are less likely to lose a mobile phone in comparison with a key card or fob. In fact, 17.3 percent of people lose at least one card or fob annually, compromising security and creating a cost for the organisation to replace.

If a key or fob goes missing, it can easily be used by anyone that discovers it. In direct contrast, if a smartphone is mislaid, the level of security on the device makes it incredibly difficult for anyone to access it, let alone get far enough to utilise the credential that's stored on it. Also, people are more likely to notice if they have lost a mobile than if they misplace a key or fob. This means the organisation can be promptly alerted to the missing smartphone, so they can revoke access instantly using the credential's management software.

When using traditional credentials such as a key, card or fob, there is a time and efficiency cost in distribution, whether that is via delivery or handing them out physically. By using mobile credentials, organisations can reduce these costs and increase operational efficiency, making them an attractive option from a sustainability perspective.

It's a more efficient system, and employees and contractors waste less time collecting or amending access credentials in person and visitors get instant temporary access when they need it. Eliminating the need for key cards and fobs – and the constant replacement of lost cards and fobs – additionally reduces plastic usage.

For organisations with contractors travelling between disparate and remote sites mobile credentials offer a way to enable access permission changes in real time. This not only reduces CO2 emissions from wasted trips and going back and forth to collect and return keys, but improves operational efficiencies, saving time and money while improving management and tracking of who accessed what and when.

With all these advantages, it's easy to forget there is still a management requirement for a mobile key. Mobile credentials can be convenient and flexible, and in some cases practical for external applications, but it's not the credential that's providing the actual security. The credential provides confirmation that the holder can access a site or open a lock – and that's where practicality issues come into question.

The credential is seen as the answer to no physical keys, which has been a challenge for most businesses to manage. The reality is, a mobile credential still needs to be managed and this seems to be a factor that's not clearly understood. Without question, integration of mobile technologies with Permit To Work ticketing and individuals' training and competencies management systems can make the management of controlling access easier and at the same time enforce compliance. Automation will allow the process to happen routinely, providing a seamless and efficient operation and enabling the exceptions to be scrutinised. But beyond the credential, little thought is often applied to what it could operate.

A CREDENTIAL CARRIED OR SENT TO A MOBILE PHONE IS IDEAL FOR SHARED SITE ACCESS

Mobile credentials require a lock that has an inbuilt reader, a power source and something to operate it – turn the lock – a function traditionally performed by a key. At present, a large thumb turn is usually provided on the outside, acting as the reader and a means of operating the lock.

This design leaves the lock vulnerable for a vandal or organised criminal to attack and disable, causing disruption and potential easy access for the perpetrator. This in turn also causes an issue for the authorised engineer or contractor that needs to gain access.

If it's a high security door, how do you protect the thumb turn with a high security shroud against hammer or drilling attacks simulated by the LPS standards? In this instance, a key is actually a far more practical means of securing and controlling access to critical assets.

Among other concerns raised by integrators around the implementation of mobile credentials for access control, phone battery life is listed as a potential issue. A phone with no power left means no access can be granted by the user, which can impact a business in terms of lost working hours. Plus, in areas where there is no internet signal, the credentials on the smartphone can not be updated if access needs granting on arrival. This is where unpowered fobs or cards, or a physical key are seen as a more reliable source of credential.

Keyless solutions aren't perfect for every application, and keys are still a very practical solution especially for legacy estates with traditional

locking mechanisms. The practicality of keyless solutions working in dirty harsh remote conditions is completely different from warm dry office applications. In addition, there will be certain environments where mobile phone usage is simply not permitted – nuclear sites, for example – making mobile credentials an unsuitable solution.

Although there can be barriers to success with mobile credentials, there are instances where the technology can thrive and come into its own. A credential carried or sent to a mobile phone is ideal for shared site access, for example.

IF A KEY GOES MISSING, IT CAN EASILY BE USED BY WHOEVER FINDS IT – A LOCKED PHONE CAN'T

This is ideal for the ad hoc visitor needing to access once, rather than on a regular basis. Abloy Beat is a prime example of this, offering the ability to use a phone to open and lock a padlock. The padlock is physically secure, and access is managed via an app controlled by the same piece of mapping software as Protec2 Cliq.

With this in mind, CIPE Manager from Abloy UK brings together a keyless solution, an electromechanical key solution and a mechanical key solution that can secure all applications with easy management – with all three elements working together. It is tailored to give a comprehensive situational overview and increase operational efficiency in critical infrastructure access management. The solution allows organisations to manage all their keys, locks and access rights from any location, with a user-friendly, cloud-based management system.

CIPE Manager connects with every locking solution in Abloy's digital portfolio, including the Beat keyless Bluetooth padlock, the electromechanical Protec2 Cliq system, as well as Abloy's high-security mechanical master key systems. Beat combines three main components: a digital key, a mobile application and a heavy-duty Bluetooth padlock, all managed with the visual CIPE Manager user interface.

Alternatively, ASSA Abloy's Incedo Business Mobile Keys are a new type of credential that offers secure mobile access, simplified management and user convenience and efficiency.

Incedo Business provides a user-friendly interface for managing your access control platform. You have a choice of system management options – Lite or Cloud – to administer Incedo-enabled hardware in a way that best suits your business' needs.

It's clear to see why mobile credentials are gaining in popularity and while there is certainly a place for this kind of technology, there still remains a requirement for alternative solutions in certain environments. Ultimately, the key is still a very practical credential and shouldn't be written off as a less robust access solution just yet.

By choosing a solution such as CIPE Manager, organisations can get the best of both worlds and adapt their credentials for different applications in relation to their requirements. This offers the ability to have a mix of physical keys, cylinders and padlocks, as well as digital technology using mobile credentials where it is most appropriate, all integrated into one platform for convenient, controlled and secure access management ●

Steve Wintle is Head of Critical Infrastructure at Abloy UK

Mobile credentials use on-device passwords and biometrics such as fingerprint, voice and facial recognition to keep unauthorised people from accessing the key stored on the smartphone

Picture credit: ABLOY