Access control goes mobile

There are more options with access control than any other security technology but are we about to experience a game-changing moment? There is an opinion that the pandemic of 2020 and security concerns will lead to smartphone credentials becoming the mainstream choice for access control in buildings

Access control is an entirely different beast than the other security technology staples of intruder and surveillance in that there are many different ways to achieve the same result. There may be lots of camera types, but they all function in pretty much the same way, whereas for access control there is a range of options. You could use a card, a fob, a key, biometrics, a QR code, Bluetooth and the list goes on. Depending on whether your customer wants to simply secure a door or restrict access to certain people and build an audit trail of visitors/times there are a number of ways you can choose to deliver access control.

But now that smartphone ownership is so widespread and after a year like 2020 could the tide be about to change? Things certainly don't look good for measures that involve human contact so it's no surprise that 2N is predicting that mobile credentials are set to become the mainstream choice for access control of residential and office buildings. Concerns around security and COVID-19 are forcing organisations and businesses to reconsider their approach to access control and use technology that offers a safe and secure living and working environment for residents and occupiers.

The outbreak of COVID-19 has brought new challenges for buildings with multiple occupiers and high frequency touch points. Smartphone credentials offer an effective and convenient contactless solution for access control which reduces safety risks for end users. Security and privacy concerns around facial recognition technology have also raised the profile of mobile credentials as the credible and secure

Concerns around security and COVID-19 are forcing organisations and businesses to reconsider their approach to access control

> *"Organisations and businesses need to ensure they have the right access control solutions in place to keep pace with changing consumer needs and concerns"*

(continued from previous page)

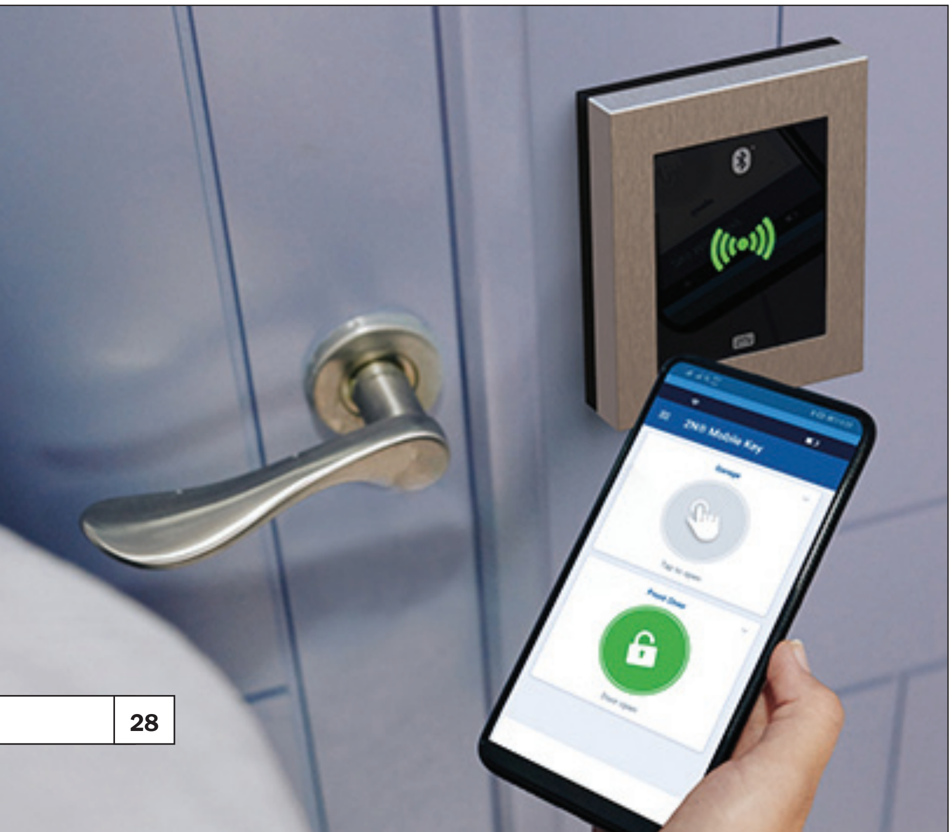
alternative to touchscreens and key cards.

Tomas Vystavel, Chief Product Officer at the IP access control systems company 2N, said: "Although intercom systems with touch screens or key cards are still commonplace solutions for access control into multi-occupier buildings, the world is changing fast. Organisations and businesses need to ensure they have the right access control solutions in place to keep pace with changing consumer needs and concerns. We expect to see mobile credentials become the mainstream choice for many organisations and businesses looking to improve access control."

PSI spoke with Gareth Robinson, Access Control Product Manager at 2N to find out more about the use of smartphones for access control and to discuss the security of the technology:

Why do you think smartphone credentials will replace established forms of ID?

We already see them gaining traction after a sluggish beginning. The number of mobile credential unit shipments set to grow by almost tenfold by 2024. Driving that are some clear advantages of a mobile based access control system. A single mobile device is capable of holding an almost unlimited set of credentials. We already see how plastic store loyalty cards are being replaced by apps – nobody wants to carry around so many cards; people expect they can be handled digitally. It is the same for access credentials, especially for those who may have to use credentials in a range of different locations; the apartment block, a variety of work locations, the gym. Phone base credentials offer added convenience in other ways, too. They enable us to control our physical contact with the access control system and create a frictionless access experience. Added to the convenience is the security factor; mobile based access solutions can offer strong encryption, not just of the credential but of the communication channel, preventing them being compromised, as is such a huge problem with prox cards. The security features of the phone itself, like screen lock, can be further leveraged to ensure a lost phone cannot be used to get unauthorised access. Our behaviour, too, adds to the security. How many times have you left your RFID card on your desk at work over the weekend? It's really not likely to happen with your mobile! In the short to mid-term though, it's about complementing established ID forms; offering the convenience of mobile credentials alongside the established forms to give flexibility as the migration to mobile credentials continues.



Are there any IT or physical security risks in using mobile credentials?

As a technology; mobile based access systems offer many great security advantages. If the solution is implemented properly; it should carry no additional risks. For example, there have been some attacks demonstrated on Bluetooth communication generally, but our own mobile access solution doesn't use standard Bluetooth communication. Instead, we merely establish a connection via Bluetooth; our app then creates an encrypted tunnel through which communication takes place using our proprietary technology. Similarly, in a high security environment, security managers can enforce our ‚tap in app' mode of door opening, and enforce a screen lock on corporate smartphones to ensure lost phones can't be used for access abuse. Such digital credentials may also be remotely revoked from a mobile device. Perhaps one of the bigger challenges comes with totally contactless ‚proximity' modes, where the door opens as the user approaches. We purposely chose not to support this mode as we were not comfortable with the security trade-off – how to ensure the phone doesn't cause unwanted door opening as a user walks by. Having said that, the work we have undertaken in our Reliable Bluetooth project takes the technology a drastic leap forward, so we expect to be able to eliminate the risk of unwanted door opening.

Will the change in ID technology require new system installations?

Not necessarily. For example, our modular IP Verso intercom offers a range of totally interchangeable reader modules. An RFID reader module can be switched for a Bluetooth capable one in a matter of minutes, without needing to replace the intercom itself. Additionally, our reader range includes options which support multi technology credential types. By choosing a reader which supports both RFID and Bluetooth, or PIN codes and Bluetooth, people can migrate to the more convenient mobile based credentials over time, without there needing to be an overnight change for all people who use the reader. As for the platform itself, support of mobile credentials is increasingly becoming a core feature. Our own Access Commander software supports enrolment and management of Bluetooth credentials and has done for some time, so all that is required is to ensure the software is up to date. Choosing a system which offers flexibility is the key in transitioning to new technology, like mobile credentials, as they emerge.

Why do you think there is resistance to biometric technology?

There are several risks with biometric technology. Firstly, there is a perception that biometric credentials represent some invasion of privacy – they are tied to immutable and personal physical characteristics and people feel uncomfortable knowing that data is out there, beyond their own control. There's also the problem that, once compromised, biometric credentials cannot be simply ‚changed' and limiting the damage potential of a breach can be difficult. Biometric credentials also tend to make people feel a little exposed, especially in the case of facial recognition, where the cameras that are ubiquitous in our modern age can track us wherever we go, they can't be disabled by simply turning off your phone! Furthermore, there's a risk from the legislative uncertainty surrounding biometric credentials. The introduction of GDPR caused a big headache in the handling of such personal data and the local laws governing use of biometric data is a very dynamic landscape, subject to sudden changes. This uncertainty translates into a risk in the financial investment required to fit a biometric access control system.

Could smartphone credentials eventually be adopted in domestic applications?

Mobile based access technology is already popular in domestic environments such as single villas or multi-family homes. And we are currently working on a new solution which will offer a flexible, intuitive platform for facility managers to manage their resident's access credentials and rights, whilst delivering an application to tenants which will enrich their living experience at the property; handle video door calls remotely, enable mobile based access, and grant access to guests and visitors. We certainly plan to further develop that platform to provide even more convenience to residents by answering a broader range of their domestic needs within a single interface.

Do you think CCTV will one day carry out all security and fire functions for premises including access control?

From an access control perspective; no, I don't believe this will become the norm. An important consideration of credentials is how they are enrolled and paired with a person. Mobile credentials offer the great advantage that they can be provided to users remotely. To enrol a face into a system, the user must attend some enrolment station – they must physically travel to that location, where they must interact with an admin or an automated system to capture their face for use by CCTV based access control. This fails totally to accommodate visitors and guests, who may need credentials attributed to them before they arrive on site, in order to gain access. It also poses a massive barrier in terms of convenience to the user, as well as meaning additional cost for the facility managers, since enrolment facilities are rarely totally automated. There's also the problems we already covered with the resistance to the biometric credentials required for CCTV access control, coupled with the accuracy problems of a camera based access system, especially if the camera doesn't face the approaching user. So if there needs to be a camera at or near every door, why not simply use a more cost-effective mobile credential reader?

> *"By choosing a reader which supports both RFID and Bluetooth, or PIN codes and Bluetooth, people can migrate to the more convenient mobile based credentials over time"*

Ringing the changes?

A study by Which? magazine and reported widely online has reportedly found security flaws in some video doorbells, such as weak password policies or a lack of data encryption. Do we need more government legislation to protect consumers?

The consumer group tested eleven devices being sold online and found that the kits could easily be hacked or switched off by criminals. As a result Amazon has apparently removed at least seven product listings.

Brands tested included Qihoo, Ctronics and Victure and common flaws were listed as weak password policies, and a lack of data encryption.

Kate Bevan, Which? Computing editor, was quoted at the time of the report release saying that better regulation was needed: "Government legislation to tackle unsecure products should be introduced without delay and must be backed by an enforcement body with teeth that is able to crack down on these devices."

But do we really need more legislation to tackle this issue? We put this question to the PSI Panel:

Richard Cunliffe – CSL

In recent years, cybersecurity has moved up the agenda to become a focus for the government and the professional security industry. The BSIA, BSI and other industry bodies have long been working in partnership with government on this and levels of working now exist. However, the challenge remains from those systems that sit outside of the professional sector, which we would categorise as 'lower-end' or DIY. DIY solutions have always existed, and they have their place, but not when it comes to network-based systems that require encryption and high levels of resilience. The professional security industry is best placed to deal with these vulnerabilities, and we hope people look to us for advice on how to overcome these challenges. One of the required measures is password management and two-factor authentication. Often, this is not seen in DIY solutions and therefore increases their vulnerability. Unsecured IP-enabled devices, such as cameras and access control panels, are potential gateways for hackers to exploit. The threat is to the security industry as a whole if the trust is lost because of poorly implemented DIY solutions.

In the future, the government can assist us to ensure that the leading benefits are exclusively for professionally installed systems, such as police response and the use of evidence. We may also be presented with opportunities when DIY systems ultimately fall short – although this could be after a vulnerability has been exposed! The challenge remains, however, how do we make sure these high standards apply to anything being considered as 'security'. Everything coming into our sector, professional or DIY, should be subject to the same restrictions. We expect the same in sectors like food and beverage, don't we? We must embrace these new products and features, but raise them to our standards and show people why they should always choose a professional installer!

Mark Massie – Fortus UK

With the rise in popularity of smart home technology, it was inevitable that there would be an increase in fraud from systems being compromised. Unfortunately, many people don't realise that if a smart doorbell is connected to their home wi-fi network, once the security is breached, it gives access to personal information (eg, bank details).

Although it's easy to pass some of the responsibility onto Government to better legislate, ultimately they can only educate of the risks and it's the homeowner's responsibility to ensure their system is password protected; as a minimum this means changing the factory code setting to a 'strong' passcode.

Some of the better-known automation products on the market have a higher level of authentication as they use Google credentials. Additional security could come in the Secure by Design accreditation being extended from professional CCTV systems to cover smart home solutions. Also, in the future technological advances could mean systems automatically ask for a passcode reset or two-factor authentication within a 24-hour period upon installation.

Unfortunately, any security measures can be exploited if your reputable security company →

"DIY solutions have always existed, and they have their place, but not when it comes to network-based systems that require encryption and high levels of resilience"

(from previous page)

has unknowingly employed less that trustworthy contract staff.

David Davies – DVS

I don't believe the government needs to take control over the issue of device security. Many of these devices are fitted domestically and therefore they would not have the resource to even police this, but I do believe there should be a minimum standard that manufacturers globally should meet, which in turn can help drive down unwanted activity from devices with no password or default ones. But this logic would need to be applied for any device that could connect to a network including phones, laptops etc as they have just if not more potential for harm to a connected network.

We should always work with manufacturing to help drive the increase in security functions and as I said there are many reputable vendors that meet and exceed what I would call minimum standard; at the very least upon activation of any network based device it should allow you to set a password that we would deem more complex, and give the option to allow notifications of failed attempts to access the device.

The issue I see is not always the product that connects to the network but the actual network itself, there are so many networks out there that are not protected in any way with access to other devices and data is just far too simple. There are many steps that could be taken to setup a more secure network and this in simple terms is just not being done. We should look to improve this more than the device itself as I see this as the bigger win and getting device manufacturers to comply with security functions should not be that difficult as they to do not want to end up as a target in the press.

> *"Many of these devices are fitted domestically and therefore they would not have the resource to even police this, but I do believe there should be a minimum standard that manufacturers globally should meet"*

Michal Kratochvíl – 2N

The importance of robust safeguards and high security standards to protect smart buildings and critical data from potential hacking attacks should not be underestimated, but we think that government intervention through regulation would be too strong a policy response at this stage.

Instead, there are steps that both consumers and manufacturers can – and should – take which would help limit the problem and avoid regulation becoming necessary.

First, consumers. IP technology has many benefits. These devices are easy to install and

can be administered remotely or connected to third-party systems. IP-based systems are therefore ideal for access control and door communication. But making use of these internet-enabled features doesn't come risk-free. Consumers must do their research before choosing a video intercom device and should look for excellent security standards, not just a good user experience. There are various simple rules that they can follow to avoid problems.

Second, manufacturers. Cybersecurity starts with an acknowledgement that today's world is connected. It's not only about a product, it's about the whole chain of products that are integrated into one system. A weakness of a single product can put the whole system in danger. That's why it's crucial to focus on the security of each product and application.

Jamie Evans – Oprema

With the IOT/Smart home industry growing exponentially each year, by no means does the topic of insecure network security devices surprise us. It does, however, remain a looming concern when discussing privacy and comfortability for consumers. As we connect more devices within our homes to stay close with friends and family, we only become more aware of the vulnerability and exposure of our data. So, how can we ensure our safety – does the government need to get involved?

As always, security falls into two categories – Physical and Digital. On production, manufacturers ensure all their products are safe and secure for the end user. However, the line becomes blurred when defining what manufacturers deem as safe and secure. Leaving the question: what measures can consumers put in place at home to deter security risks?

Physically, measures such as security fixings and the ability to lock a device to an account, will deter what would be thieves, from stealing these devices for a quick sale.

Digitally, this continually poses a challenge. Exploits such as Heartbleed, Shellshock and Spectre are constantly being found, even in the most common libraries with which the world relies on for secure communication. There's still no excuse for making critical mistakes, such as transmitting or storing sensitive data in plain text – it's nothing more than lazy development.

Strong security development should not be overshadowed. Devices and software should be designed with security being the forefront of the developer's mind – not shoehorned in as an afterthought. Brands towering over the safety aspect have fallen foul to security breaches previously, making it harder for consumers to understand their best option through the jargon presented.

The possibility of government involvement to help improve the posed risks facing us today is an open debate. The market for these consumer devices is so spread globally, it would be difficult to govern. However, an initiative such as the "Secure by Default" scheme – displaying a standard for when configuring software, is a step in the right direction for peace of mind.

> *"With the IOT/Smart home industry growing exponentially each year, by no means does the topic of insecure network security devices surprise us. It does, however, remain a looming concern when discussing privacy and comfortability for consumers"*