How to optimise mobile access control authentication with smart devices

Published on 1 Aug 2018

Considering how much the modern smartphone has become a common everyday tool and cultural icon, it’s hard to believe it has only been with us for a relatively short space of time. The first Apple iPhone was launched in 2007 and yet in a little over a decade the smartphone has become as essential as our keys or wallet.

From its conception as a multi-faceted communications device, it has morphed into something far more integrated in our daily lives. Services such as Apple Pay, Android Pay and PayPal have seen the smartphone become a credible replacement for cash and cash cards, but equally, it is possible
to replace access cards and keys as well.

"Smartphones can easily receive authentication credentials remotely and access can be confirmed or denied instantly"

The ability to accurately authenticate an individual and the applications this offers for security purposes, is something that the security industry needs to continue to embrace and further promote to our customers.

Considerable advantages

Most security professionals understand the potential benefits of using mobile device authentication, with flexibility being the key advantage. Smartphones can easily receive authentication credentials remotely and access can be confirmed or denied instantly. Equally, smartphones already contain many secure options to ensure they are only used by the authorised user – fingerprint and face recognition, as well as pattern authentication and PIN, being prime examples.

Unfortunately, there is still a lack of awareness amongst some security operators, customers and the public of these exciting benefits. Potentially there may also be some reluctance, in certain quarters, to trusting a mobile device with physical security. A lack of trust in seemingly ‘unproven’ technology is not unusual, but the security industry needs to demonstrate reliability along with the considerable security and convenience benefits of using it.

Trusted part of security network

"Many smart devices already securely bind the mobile device with the right person by using 2-factor authentication"

Mobile device security needs to earn its trust, in much the same way as any other new ground-breaking application. In fairness to the doubters, it’s not hard to imagine how much of a risk a badly protected mobile device could be to any secure network!
There are two key obstacles that smartphones need to clear before they can become a trusted part of the security network though. Firstly, that they are secure enough to be trusted as part of a security network, and secondly that they can reliably identify an authorised user in a real-world environment.

Many smart devices already securely bind the mobile device with the right person by using 2-factor authentication. For example, this could combine a PIN code with the fingerprint or face of the authorised individual.

In areas with particularly high security, you could also implement a wall-mounted biometric reader (fingerprint, facial recognition or iris scan) to add a further level of protection and ensure there is no wrongful use of the mobile device.

**Security by location**

With its many and varied functions, undoubtedly one of the most useful systems on any smartphone is its GPS location tracking. It’s also a perfect tool to assist with security systems interaction.

*“A benefit of using smart device authentication is the cost savings over operating traditional tokens”*

Consider any secure facility – it will feature different levels of access. This can vary from a humble canteen and break-out areas, right through to secured doors around potentially dangerous or highly sensitive areas - such as plant rooms, or even a nuclear facility!

Security tokens or access cards are typically rigid in their programming, only allowing access to certain areas. A smartphone, however, can be granted or denied access depending on the location of the request by the individual – GPS literally adds a level of extra intelligence to security.

**Personal items**
Using QR codes seem to be a simple but reliable identity and access control authentication option

Mobile devices tend to be guarded and protected with the same concern as your money or your keys. Many of us literally carry our mobile device everywhere with us, so they are relatively unlikely to be misplaced or lost – certainly in comparison to a key card for example.

Also, think about how often you use or hold your smartphone – some estimates suggest 2,600 times each day! With that level of interaction, you’ll be aware very quickly if it’s been misplaced, not least because of the inconvenience and cost to replace it. This level of personal connection makes it perfect for use with security systems.

Cost savings

Another obvious benefit of using smart device authentication is the cost savings over operating traditional tokens. No more plastic badges, access cards, lanyards, printers and consumables used to administer security. This is something the security industry really needs to shout about!

It will come as no surprise to hear that smartphones are exceptionally common too. Figures suggest that in 2015 there were nearly 41m in use in the UK and this is predicted to rise to 54m by 2022. With the UK population being just over 65m, that is a very high percentage of people already carrying this technology.

Using a resource that people already have, and which is highly secure, makes unquestionable financial as well as practical sense.
GPS location tracking is a perfect tool to assist with security systems interaction

Integrated technology

Agreeing on common and shared open protocols has unfortunately been one of the stumbling blocks for the security industry in adapting to a predominantly smartphone authentication approach. NFC (Near Field Communications) technology in mobile phones and smart devices has failed to be the universal success it promised.

"Not everyone has an iPhone, but it is such an important segment of the market for customers"

Mobile technology trends have dictated to the systems that use it. Apple’s earlier (Pre iOS 11) decision to restrict the use of NFC to Apple Pay on its devices has had a profound effect on the implementation of NFC in other applications too. Not everyone has an iPhone, but it is such an important segment of the market that other manufacturers are wary of how customers will be able to use any new technology.
We have seen a much bigger focus on using Bluetooth Low Energy technology on mobile devices instead. With providers such as HID Global, STid in France and Nedap in the Netherlands now concentrating on developing Bluetooth Low Energy readers and mobile credential applications, this seems like a highly credible alternative.

Along with NFC and Bluetooth Low Energy options, there also seems to be a lot of interest in using QR codes as simple but reliable identity and access control authentication. These can easily be displayed on a screen or printed if necessary, giving great flexibility over the type of technology that is used in the future.

**Upgrading existing security systems**

There are strong arguments for many businesses to continue using MIFARE+ systems if they suit operations well

We are steadily seeing the signs of smartphone authentication replacing the cards and tokens we have been familiar with. However, many consumers still want options rather than to just be railroaded down one path.

A business that has invested in cards or tokens will want to use that technology investment fully. The changes will come when readers are updated – this is when security specifiers and installers need to promote the advantages of dual-technology readers, which offer options to include smartphone authentication into the mix.

There is still considerable diversity amongst smart devices, the operating systems they use, and the security technology employed by each. Android, Apple iOS and Blackberry devices all vary with regards to the biometric authentication available, so security administrators may need to be flexible on the types of authentication they accept.

Interestingly, card technology has also progressed at an astonishing speed too – with MIFARE+ proving to be a highly cost-effective, practical and secure system that can easily be integrated.
There are strong arguments for many businesses to continue using these systems if they suit operations well.

NFC (Near Field Communications) technology in mobile phones and smart devices has failed to be the universal success it promised

**Hybrid systems**

A hybrid approach may be the best answer for many security operators. This means those who choose to enjoy the benefits in terms of flexibility and convenience of smartphone authentication can do so, whilst those who are more hesitant can continue to use more traditional methods.

“A hybrid approach may be the best answer for many security operators

Larger organisations may find that the swap over is a slower and more gradual process, whilst smaller start-up businesses may prefer to jump to a smartphone-based approach straight away. If security systems are well integrated but modular in their approach, then it becomes much simpler to
evolve as time goes on.

**Embracing the benefits**

Using their app-based systems architecture, smartphones are ideally placed to evolve with security systems in the future. There are many benefits for the security industry and our customers, but we need to remember that this move will involve a culture change for many security operators and users.

The security industry needs to be mindful and respectful of any anxiety, but also be positive and promote the considerable benefits mobile authentication offers.

**Author Profile**

John Davies
John joined TDSi in 2003 when it was owned by Norbain SD Limited and led the management buyout in February 2005. TDSi manufactures electronic access control and integrated security systems. Export sales have grown from 25% of the business to 40+%. 
You may also be interested in...

Cloud systems, cybersecurity and mobile credentials to drive security...

Overall, it’s been quite a year for the industry and Vanderbilt. Last year, we predicted that the security industry would see a rise i...

Are mobile credentials more secure than smart cards?

For the past several years, there has been a focus by integrators and customers to assure that their card-based access control systems are s...

Applying biometric authentication to physical access control systems

Over the past few years, biometrics has rapidly expanded into consumer applications, like the financial market for customer authentication,...