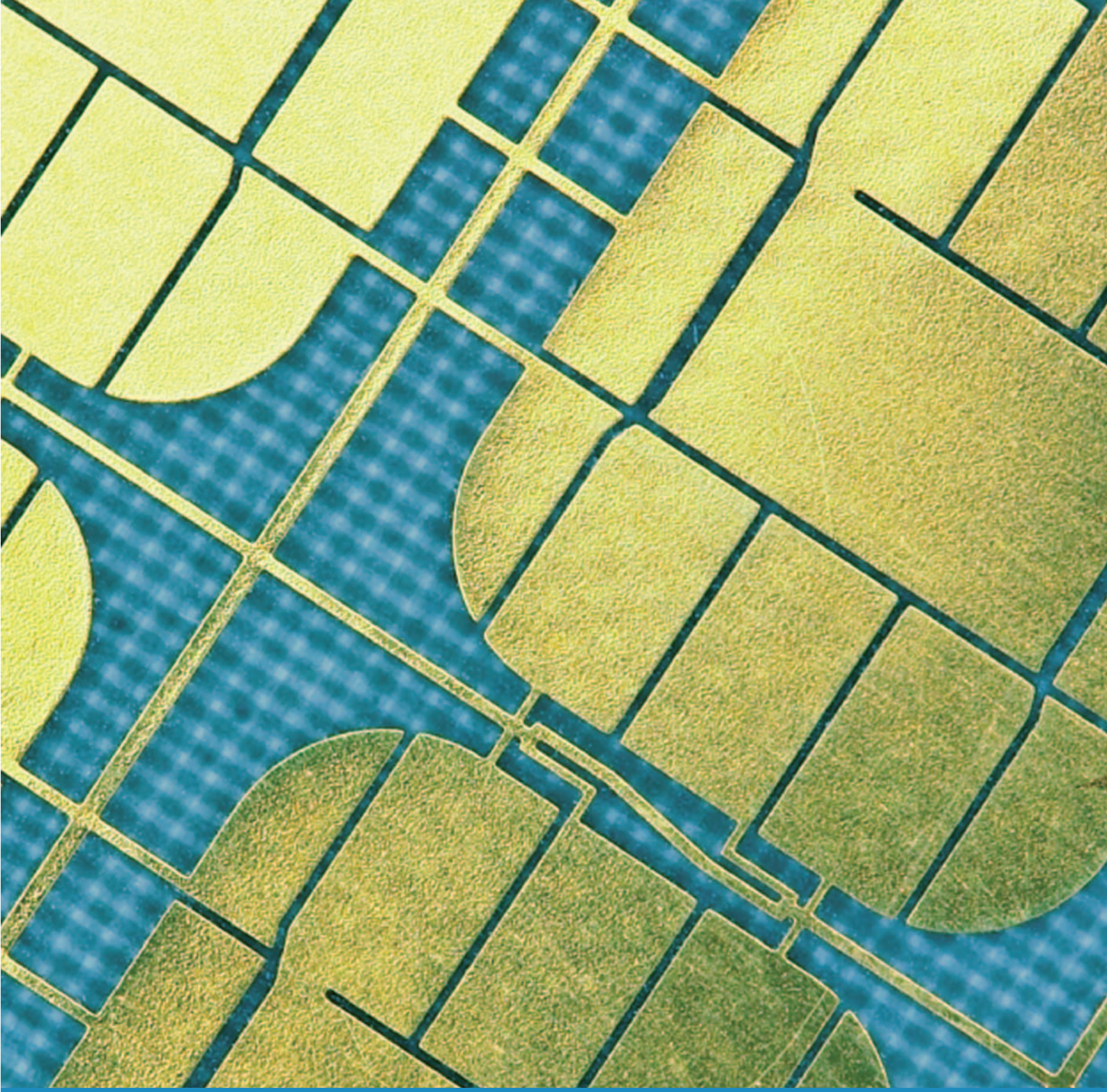
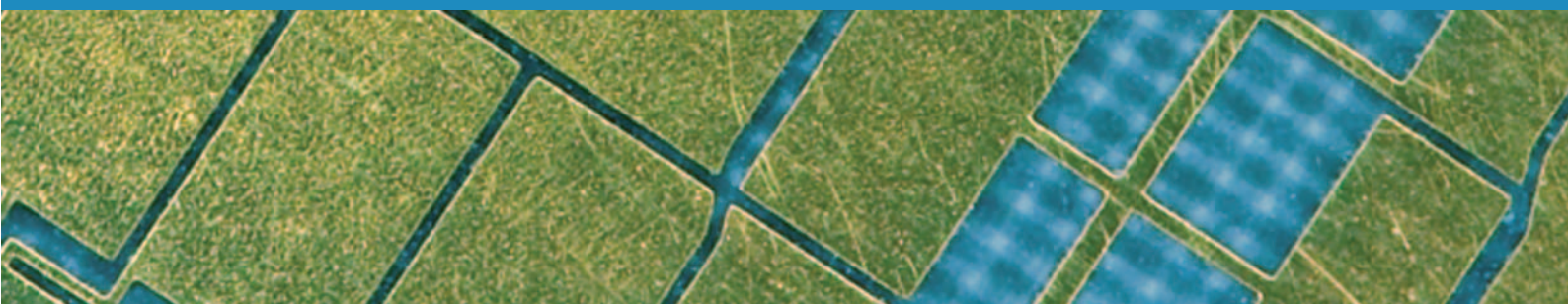


Smart cards

the Devil, and the opportunity, is in the detail

By Dan Isaaman
Dot Origin Ltd.



The common implementation gaps

The use of smart cards for door access control has been common for many years, but ensuring that they provide the expected levels of protection, and deliver the efficiency benefits they are capable of, requires some in-depth understanding.

IDENTITY MANAGEMENT OR JUST DOOR CONTROL?

Unfortunately, the industry that has grown up around the supply of physical access systems has often made choices about using specific RFID technologies which are more about protecting their business models than protecting the people, buildings and assets of their customers. This has led to fragmentation, 'security by obscurity' and a lack of choice and flexibility when it comes to users benefiting from the 'smart' nature of their cards, as well as the systems behind the scenes managing and controlling their access.

This has never been more important, now that the cyber threats to organisations often include a physical dimension, while ever-mounting compliance requirements, such as PCI-DSS and GDPR, also require an integrated and layered approach to security, forcing the convergence of identity and access management across IT, HR and Facilities departments.

ARE YOUR CARDS AS SECURE AS YOU THINK?

Starting with the cards themselves, and ignoring the technology for a moment, what do we actually mean when we ask 'Are my cards secure?' If we think about other well-known uses for smart card technology – payments and mobile – what we usually mean is 'Can they be cloned or spoofed by a bad person?' Sadly, even today, many users are still buying old and compromised technology cards that can be easily and instantly copied, some by quietly scanning your pocket in an elevator! Many organisations also seemingly trust everyone in their supply chain to prevent replication of their access cards, even though this is actually very easy, and one of the industry's 'dirty secrets', even with the latest 'secure' technologies.

Only a very few users are managing their own encryption keys, encoding their own cards, and thus holding the keys to their own castle, just as most companies do when it comes to managing their IT infrastructure (after all, which IT Manager would give their firewall or domain admin password to anyone else?!)

At Dot Origin, we spend much of our time uncovering and explaining to end users how these card technologies actually work, where they are sourced, who owns the keys, and just how much information can be gleaned from a card dropped in the street or left in the gym.

This can lead to an informed decision about the level of security, integrity and flexibility of cards that they buy, which, after all, can have major long-term risk implications for the entire organisation.

The identity management opportunities

ONE CARD, MANY USES

What about the opportunities for improved workflows, productivity and security through convergence? This is where being smart about smart cards can lead to significant benefits - ie not just believing the sales pitch of a single vendor, but working out how to converge multiple needs, technologies and systems into a pragmatic, end-to-end solution. Again, the devil really is in the detail, and it often requires multiple departments and external suppliers to work together in (relative!) harmony.

Issuing a single smart card for multiple applications can deliver real value. Typical uses include photo-ID, physical access, follow-me printing, and secure two factor PC/laptop/network logon. The convergence of these functions onto a single card also mirrors the trend towards unifying the management of user identities across multiple systems, and leads to reduced overheads and increased security, almost by default. Such cards will be more valuable to staff, and thus less likely to be lost or damaged, and more likely to be carried universally. Horror scenarios of secure logon cards being cut down and taped permanently into laptops can be avoided by ensuring that the same card is used for buildings access and on-demand printing. Separate processes of issuing one card for access, another tag for printing and an OTP token for VPN access can be simplified into a single, streamlined workflow. And the benefits become even clearer when looking at the entire employee on-boarding and off-boarding risk profile, as well as managing access for contractors and visitors.

While the individual card may cost more, that cost can be divided across multiple budgets, and, in many cases, can significantly undercut the total cost of ownership of separate solutions. One Dot Origin customer initially implemented four critical applications using new cards, and achieved a payback in under 18 months, while they now have over eight separate uses and even encourage individual departments to suggest new ideas, which are then evaluated and implemented by the project team if the business case stacks up.

ONE SYSTEM, ALL LOCATIONS

Businesses often grow through acquisition and mergers, and this leads to significant opportunities to increase security and productivity through centralised management of both access control cards and systems. Very often, the requirement to unify disparate access systems, card technologies and suppliers' interests is just too difficult, and so a proper migration path needs to be worked out, which might involve a staged approach, for example by first issuing multi-technology cards, then replacing door access readers on a site-by-site basis, and then later unifying the databases and access rights management onto a common, wide area network.

While this process can be somewhat painful and complex, the end goal, of a unified smartcard and access management system, is a prize worth aiming for, and it is really not that difficult to achieve when using modern, open technology and careful project planning.

Stronger data security

TRUE INTEGRATION WITH CYBER-DEFENSES

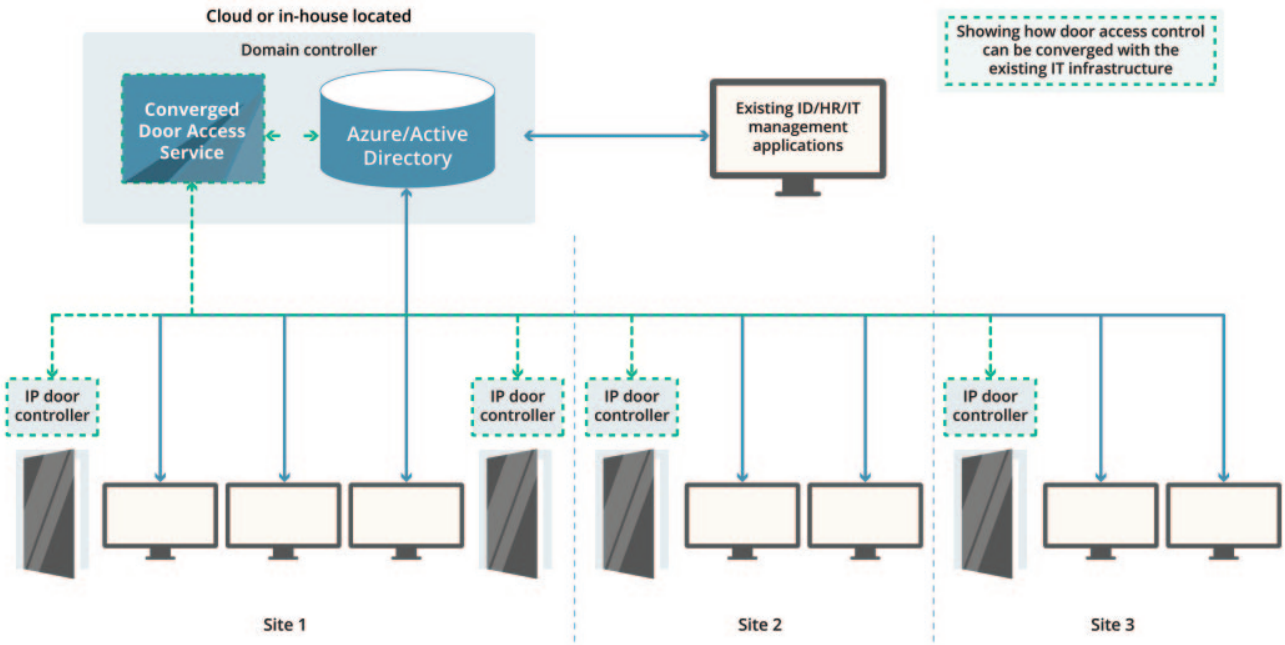
The latest door access control systems are now truly integrated into the IT infrastructure, for example using Active Directory to manage both physical and logical access rights within a single role-based user database that is automatically replicated across multiple sites and servers. By turning a door access request into something that is carried over the IP network and processed centrally in real time, there is an immediate opportunity to use this information as part of a wider cyber security and compliance strategy:

→ Can this user access the secure Wi-Fi network? No, because they haven't actually entered the building yet;

→ Can this user shut down that critical server? No, because they didn't first enter the server room and then open the appropriate rack;

→ Can this user access the credit card processing application? No, because they're not in the approved PCI-DSS call centre enclave;

→ Can this user freely roam the building? No, because they have just been suspended and their PC logon has been disabled...!



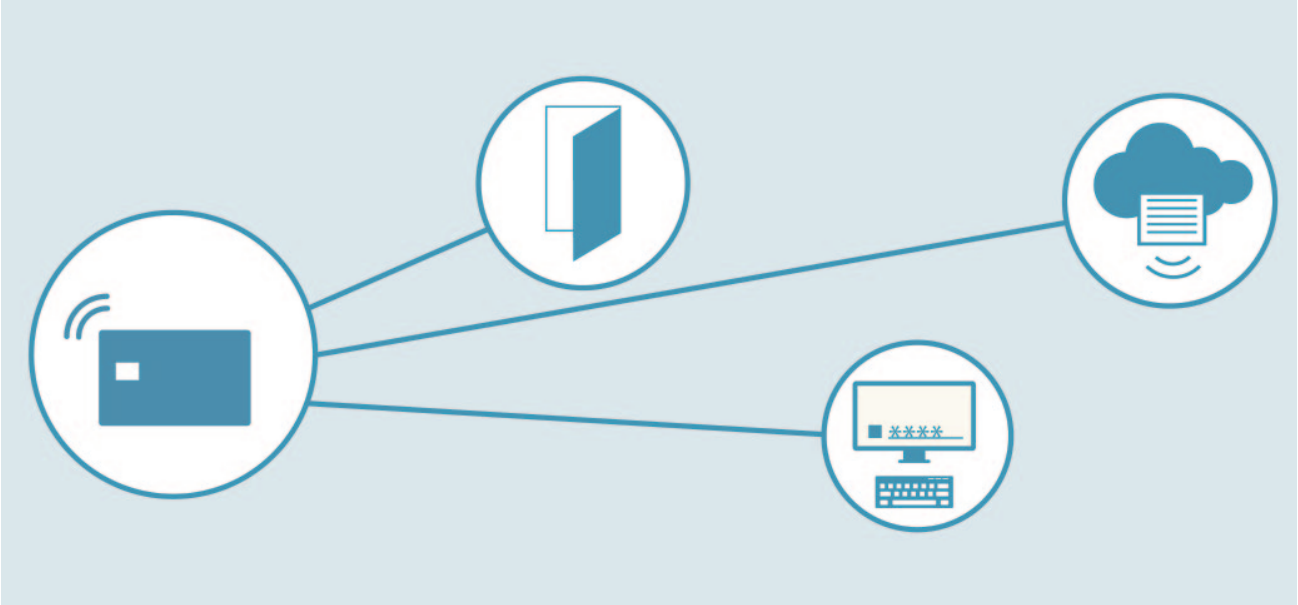
Smart card or mobile phone?

MOBILES CAN CONFIRM IDENTITY, BUT NEED TO BE SECURED

What about the mobile revolution? Is this an opportunity, a threat, or both? Looking at what has already happened in this space over the past few years, we would err on the side of caution. It's relatively safe to treat mobile devices as a new way of accessing corporate data and systems, but not yet to turn them into security devices themselves. Mobile devices should be treated much the same as PCs and laptops - firstly in desperate need of centralised management and control, and secondly requiring appropriate levels of user authentication to deliver security when accessing sensitive data.

This has been difficult to achieve until recently partly due to the lack of native smart card support in most mobile operating systems, unlike on the desktop, but advances in the use of NFC and Bluetooth technology have now started to reach the market, along with matching secure app environments and SDKs. Compatible smart cards can now be tapped to authorise access to applications, and personal smart card-like Bluetooth devices and wearables will start to enable better security across the board.

It is true that selected smart card functions can be replicated on mobile devices, which is particularly good for convenience, as long as this is adequately managed and the risks understood. So just as in payments, where your contactless card can now be stored in your phone, so your door access credentials can be stored and sent to the door via NFC or Bluetooth when you walk up to a building. But this technology is new, relatively expensive, and not yet open for use in multiple applications, so the benefits are not always clear.



Summary

SECURE YOUR DATA AND PHYSICAL ASSETS WITH ONE-CARD EFFICIENCY

As the UK Government's own information security survey found in 2015, people are just as likely to cause a breach as viruses and other types of malicious software, while another 2014 study found that 36% of desk-based workers in the UK and US are aware of having continued access to a former employer's systems or data.

Used and managed properly, a single physical device such as a smart card is a great tool for controlling access to both buildings and data, and can also reduce costs and increase compliance across multiple departments, as long as the technology being used is well understood, and implemented with care.

Dot Origin is a supplier and developer of products and solutions that use smart card technology, ranging from RFID door access control to strong PKI-based network security and encryption, and specialises in delivering converged solutions that deliver maximum benefits and return on investment.

EdgeConnector is the physical access control solution created by Dot Origin, that delivers real-time, location-aware, converged physical and logical access decision-making.

DOT ORIGIN

www.dotorigin.com

info@dotorigin.com

EDGECONNECTOR

www.edgeconnector.com

info@edgeconnector.com

Europe & Asia

+44 (0)1428 685 861

Northern & Latin America

Toll Free: (888) 262-9642 Direct: (562) 262-9642

Dot Origin Ltd.

Coopers Place

Combe Lane

Godalming

Surrey

GU8 5SZ

United Kingdom