Converging Access of IT and Building Resources:

The Meaningful Coming Together of IT and Physical Security
Understanding the Drivers for Convergence

By Julian Lovelock, VP of Product Marketing, HID Global, Identity Assurance

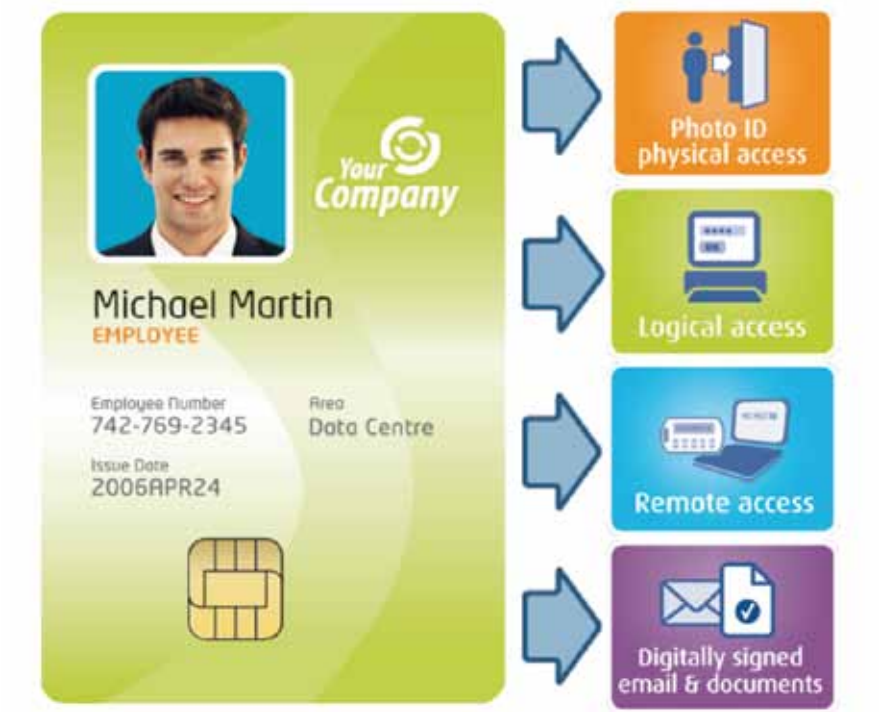
Speed and Simplicity – we all want it. When it comes to access, we want to use a single credential to quickly and easily get the resources we need, when we need them, whether they're in a building or the cloud. The problem is this level of access has traditionally been anything but simple to provide.

Organizations often struggle because the domains of physical and online security have traditionally been separate worlds. However, just as the lines of a distinct, defensible perimeter are fading, as the user population of any given organization is increasingly distributed, mobile and varied, so are the lines between physical and online security starting to blur.

Facilities and IT must support all the different needs of all their different users - including employees, partners, consultants, contractors, vendors and customers - and they must enable them to access the resources they want, from wherever they are, using whatever means necessary. They must also provide this access without compromising security, which is a big challenge given the ongoing escalation in frequency and sophistication of attacks making up today's threat landscape. And they must contain costs, minimizing the capital investments and operational expenses associated with deploying and managing access systems.

All these requirements and pressures are forcing organizations to become better coordinated in their approach to managing user identities and access. As a result, the physical and virtual security roles that were once separate are now coming together. Out of necessity, we are seeing more and more convergence between the two worlds to enable access solutions that deliver simplicity to the user, with better security at a reduced cost.

CONVERGED ACCESS CARD



A converged credential is a single card, which could be an ID badge, that enables the user to get into the building, log onto the network and gain secure access to the applications and other systems that he or she needs. The card may also be used to gain remote access to secure networks, replacing the need for a one time password (OTP) token or key fob.

A converged credential is more convenient for users, eliminating the need to carry multiple devices or re-key one-time passwords. It also greatly improves security by enabling strong authentication throughout the IT infrastructure on key systems and applications, rather than just at the perimeter.

Convergence Reality – It's Happening

A holistic, coordinated approach makes sense, yet it's not as easy to accomplish as one might hope. As mentioned, physical and virtual security have traditionally taken place in two different domains, with very little visibility into what the other is doing. This is changing, however, as the economics of a simple, effective access solution combined with the capabilities of today's technology are accelerating the convergence between physical and virtual security.

The reality is that over the last few years, these two domains have been forced to come together to share resources and solve real problems for the organization. For example, physical access systems already rely heavily on the IT department, and by implication, IT security, so the more tightly linked they are the more efficient and effective they can be. In addition, physical access systems, particularly video, generate large amounts of data that flows across the network and is stored in the data center. Understanding the role this information plays in the overall security and compli-

ance of the organization can ensure it is treated appropriately.

We have already started to see some of the benefits of greater awareness in security incident resolution, as physical and IT security work together more and more to address threats. For example, physical security professionals may ask for the expertise of their IT counterparts to help figure out what a user, who piggybacked their way into the building, did on the network. Conversely, when IT identifies a breach, the log records that tell when a user entered and left the building, combined with video footage from the physical security team, can be extremely helpful to validate the identity of the attacker.

Both groups oftwen rely on the same master user repository (Active Directory), not only for key attributes like name and title, but also for role and group information, to directly drive access rights. Understanding how each uses the identity database can ensure a more consistent and secure user experience. They often must use the same log analytics tools to provide compliance officers with consolidated audit records that account for both physical security and IT systems access logs; better coordination on the front end can make the back end reporting easier and more comprehensive.

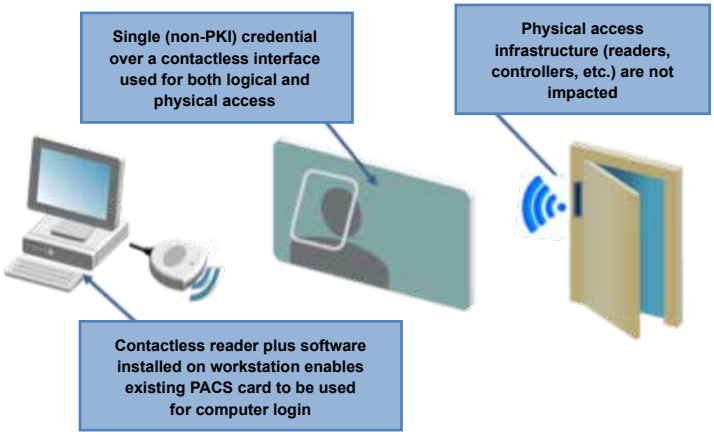
These situations have brought to light the need for these groups to work together; the more they do, the better they understand the role each plays and the better the overall access experience and security. Ultimately, the goal is to deliver a single access solution with strong authentication that is convenient for end users and cost effective to deploy and manage.

The Value of a Converged Access Card

Truly converged access consists of one security policy, one credential and one audit log. In some organizations, user management is already fully converged, with a single corporate policy that defines what's acceptable and what's not, a single master user repository, and a single logging tool for simplified reporting and auditing. This makes a converged credential the logical next step.

It's cheaper from a capital expenditure perspective because the organization doesn't have to invest in multiple security devices for physical access and remote network access. And it delivers substantial OPEX savings, reducing the management costs associated with deploying and maintaining multiple solutions, not to mention the benefits associated with having a single set of administration and helpdesk processes around issuance, replacement, revocation.

LEGACY CONTACTLESS



This approach doesn't use a public key infrastructure (PKI), which binds public keys with user identities through a certificate authority (CA). While this eliminates many of the key management challenges faced by organizations that deploy PKI, this model supports a limited number of use cases and doesn't deliver the same security strength as PKI-based solutions.

How Does It Work?

The technology to deliver a converged access card is available today and adoption is growing rapidly as organizations realize the benefits of a converged solution. The following are the three most common models for converged architecture:

Legacy Contactless enables existing contactless cards (e.g. Proximity, iClass, MIFARE) already deployed for physical access to also be used for desktop and application login. Software is deployed on the end user workstation, and a contactless reader is connected to or embedded in the workstation. The card can be "read" without needing to be physically inserted into a reader device. This offers great convenience for users, who can usually keep their cards in their wallets or purses; a tap on the reader with the wallet or purse provides access to the computer.

The contactless, non-PKI model is being deployed in hospitals, schools and other environments where multiple users need access to the same workstation in quick succession. It is also being used as a bridging solution, where mandates such as CJIS require workstations and applications to be protected by strong authentication.

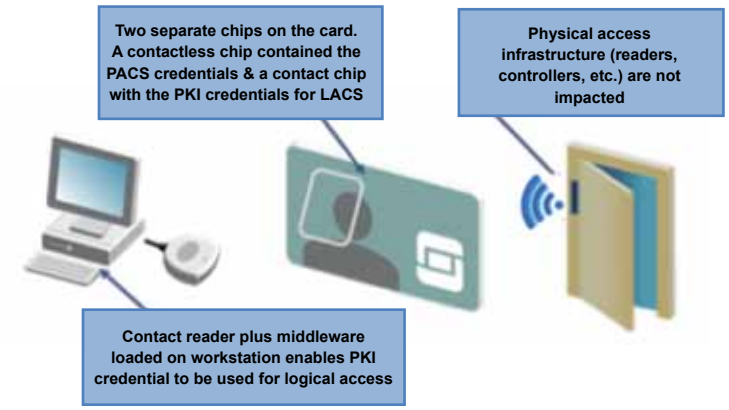
Dual Chip Cards have both a contactless chip for physical access and a contact chip for IT security use cases. While both are embedded on the same card, the chips are completely separate. Credentials such as PKI certificates and OTP keys are managed on the contact chip using a card management system (CMS).

In many cases, the CMS can be integrated directly into the physical access card security PACS management system (often referred to as the PACS head-end) to enable a single set of workflows to be managed through a single administrator console.

Dual Interface Chip Cards have a single PKI capable chip with both a contact and a contactless interface. The card can be used with a contact card reader for logical access use cases such as logging in to a computer or signing an email. The card can also be used where PKI authentication for physical access is required.

By default, PKI over a contactless interface is uncomfortably slow for physical access usage. Protocols such as OPACITY substantially improve performance over a contactless interface to enable an acceptable end user experience.

DUAL CHIP CARDS



The dual chip card model is popular with medium to large enterprises with sensitive IP or customer data on their networks, such as financial services, high-tech, and pharmaceutical organizations, because it delivers strong security and the ability to continue to leverage existing IT security infrastructure investments.

What About Mobile?

Users are increasingly mobile, bringing their own devices (BYOD) into the organization's environment, using smartphones, laptops and tablets to access the resources they need. According to ABI, there will be 7 billion new wireless devices on the network by 2015, which is close to one mobile device per person on the planet.

Organizations are trying to support all this mobile access, while looking at ways to leverage the mobile devices of their users to help maintain their security stance. There are already pilots, one at Arizona State University, for example, to prove the concept of a mobile phone as a physical access credential.

This requires rethinking the way physical access credentials are managed. Traditionally, the card and the credential have been inseparable. However, to accommodate the mobility of that credential, it must be decoupled from the container. In other words, it must be possible to manage the credential independently of the physical device on which it is stored.

This is because the phone or mobile device is often not the property of the organization; for example, when a student graduates from the University he/she doesn't hand their phone back the way an employee would hand their card back when they stop working for the company. As a result, organizations needed to be able to manage their users' access, and quickly add and remove users from the system, without having to physically control or touch the device.

Mobility is driving ongoing convergence as it forces the physical and IT security teams to work together to come up with a solution. The result can be a solution that can easily manage PACS credentials and IT access credentials on phones in a cost-effective way, while delivering the same level of security they were used to with cards.

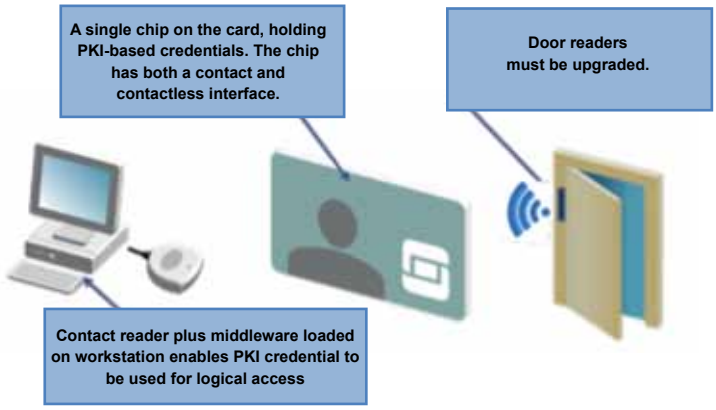
Summing Up the Value of Converged Access

The ability to manage identities and make decisions on access to both physical and online assets based on a common set of information makes a lot of sense. However, it requires a lot of collaboration between physical and IT security teams, which can be challenging due to the traditionally separate roles they have played in most organizations. With the increasing distribution, mobility and expanse of users in today's environment, there is increasing recognition within organizations that the physical and IT worlds need to come together. When they do, organizations can achieve truly converged access to deliver:

- Convenience – simple and fast access to resources for users, when they need it, from wherever they are located.
- Investment Savings – eliminating capital investments in multiple cards and approaches, while reducing ongoing management expenses.
- Strong Security: the ability to trust the identities accessing an organization's resources, both physical and cyber, to strengthen the security throughout the infrastructure, not just at the perimeter.

There is no question, we are going to be seeing more and more convergence to enable access solutions that deliver simplicity to the user, with better security at a reduced cost.

DUAL INTERFACE CARDS



User credentials are managed on the chip by a single card management system. It should be noted the physical access infrastructure needs to be upgraded to support PKI at the door. The dual interface card model is applicable primarily in US Federal government organizations, where mandate OMB-11-11 requires personal identification verification (PIV) credentials, specified by FIPS 201, be used for physical access.