Trends in Access Control

As the security landscape continues to evolve in new and complex ways, organisations are viewing this as an opportunity for improvement and value rather than an interruption or distraction.

Open Architecture

Customers are increasingly moving towards more open and secure architectures. They want to ensure that the organisation's access control solution can adapt to future threats and take advantage of opportunities and applications beyond mere access control. The goal is to deploy a fully interoperable, multilayered security solution across company systems and facilities. By using solutions that are based on industry standards such as OSDP bidirectional communications, and incorporating dynamic rather than static technologies, security becomes independent of hardware and media and the infrastructure can more easily evolve beyond current abilities and also have the adaptability to combat continuously changing threats.

Security Integration

The momentum of security integration is unlikely to slow down in 2014. It will continue to be a key market driver. The benefits are unquestionable, with the drive for efficiency being the core proposition. It enhances security reaction times – for instance if a door is forced the combined system will sound an alarm, lock-down key areas and direct the security team to the location of the potential incursion. Integration makes installation and upgrades easier and more cost-effective and it makes full use of legacy and existing systems. There is a massive growth in the use of BACnet protocols as well, which are adding a new level of software integration which is helping to move away from the remaining proprietary software that was once commonplace in the security industry.

Integrated security systems allow authorised users to minimise the security details they have to memorise and this is a major advantage. The ability of integrated systems to intelligently provide access also means that workforce management is much easier using integrated security. From

managing working hours to activating buildings services only when they are needed (and thus saving energy and resources), **integration is providing intelligent solutions that will save money.**

Integrating Physical Access Control with IT Security

Historically, physical and logical access control functions were mutually exclusive within an organisation. These systems were also managed by different groups. The boundaries between these groups are beginning to blur. Organisations find the need to provide physical access control system (PACS) and IT identities on a single card that can be used to open doors and log on to computers. This will create a seamless user experience. Individuals will be able to create, use and manage identities across many different applications on both smart cards and smart-phones. Users will soon be able to carry many types of access control credentials as well as one-time password (OTP) tokens on a single microprocessor-based smart card or smart-phone. Such integration will improve efficiency through centralisation of credential management for multiple logical and physical access control identities across IT resources and facilities. **Organisations will be able to achieve true convergence through a single solution that can be used to access IT resources, while also enabling many other physical security applications.** There will be a single process for provisioning and enrolling both IT and PACS identities, and it will be possible to apply a unified set of workflows to a single set of managed identities for organisational convergence.

Smarter Smart Cards with Multi-layered security.

Card technology continues to evolve from proximity cards to magnetic stripe cards and on to smart cards. Today's gold standard for access control applications is contactless smart cards that are based on open standards, featuring a universal card edge, also known as a card command interface, which improves interoperability with a broad ecosystem of products within a trusted boundary.

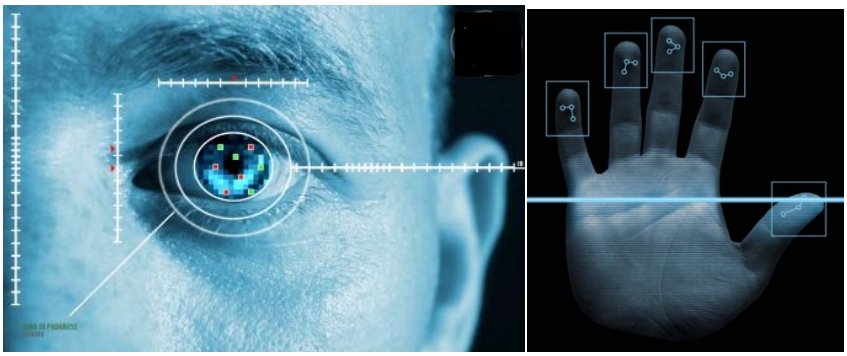
The latest cards improve security, privacy and portability to mobile credentials. **Users are increasingly enhancing their cards and badges with more and more layers of additional visual and digital security.** Visual elements include higher-resolution images, holographic card over-laminates and permanent and unalterable, laser-engraved personalization attributes.

Cards also increasingly incorporate expanded digital storage capacity so they can include biometric and other multi-factor authentication information to enhance identity validation. Printing technology also continues to advance in support of these trends, simplifying how cards are produced and distributed while making them more secure.

Migrating to smart cards offers stronger security. They also enable multiple applications on a single card. Both physical and logical access control can reside on NFC-enabled smart phones.
Although migration does involve change, the combination of multi-technology cards and readers plus field-programmable cards and systems minimizes disruption to the day-to-day workflow. Employees and the organization can benefit from a more secure and user-friendly environment that provides the scalable foundation for future capabilities and applications.

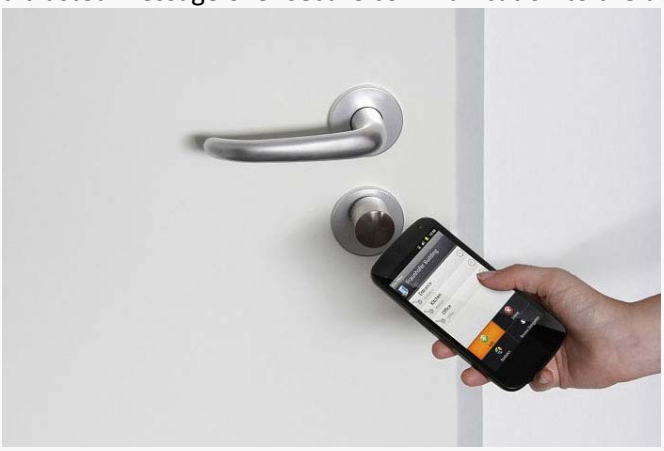
Biometrics

Biometrics will find even greater acceptance in 2014. The quality and accuracy of biometrics have rapidly improved in recent years. Fingerprint readers and facial recognition systems are now widely accepted. Advances in biometrics will result in the deployment of more complicated systems such as palm vein and heartbeat recognition readers.



Use of Smart phones as access cards

Smart-phones will function similarly to how a card transacts today, depending on technology and business ecosystems already in place. In future the phone's onboard computing power and multimedia capabilities will be leveraged to overcome limitations and provide a more functional and rich user transaction and experience. Looking forward further, the connectivity of smart-phones will be used to perform most tasks that today are jointly executed by card readers and servers or panels in traditional access control systems. This will include verifying identity with rules such as whether the access request is within a permitted time and, using the phone's GPS capability, whether the person is actually in the vicinity of the door. The user can then be validated using a cloud application and granted access via a trusted message over secure communication to the door.



With this, mobile devices (rather than an access control system) make the access decisions and doors (rather than cards) present their identity. This role reversal, sometimes called duality, changes how access control solutions are offered. Organisations will be less dependent on the expensive

infrastructure required for connecting servers, panels and readers - just electronic locks that respond to a mobile device's encrypted 'open' command. **This simplified and more economical model will enable the industry to secure more assets: interior doors, filing cabinets, storage units and other areas that have been prohibitively expensive or complex to secure in the past.**
However mobile devices, by their highly portable nature, also pose a potential risk of unauthorised misuse. Accordingly though, mobile device manufacturers have beefed up handset security and this has offset many of the potential concerns – in some ways echoing developments in the security industry itself. Fingerprint readers are now available on iPhones.

NFC authentication

Near field communications (NFC) RFID tags will increasingly be attached to many items in public places, to establish their unique identity so that authenticity can later be conveniently verified using contactless readers or any NFC-enabled smart-phone or tablet. This authentication model will enable a variety of new transactions and services, ranging from authenticating items and documents and securely managing chain-of-custody, warranty and other transaction data, proof of presence (electronic visitor verification - EVV) and authorising a phone to operate in an organisation's virtual telecom system.

Security levels of NFC tags will increase by a combination of NFC tags containing cryptographically signed data elements that cannot be copied or modified without detection, plus secure cloud-based authentication services that are backed by a proven server infrastructure. With this ecosystem in place, it will be possible to develop applications that allow an NFC-enabled smart-phone or reader to communicate tag information to a secure, cloud-based server, which validates whether the tag is authentic and asks for a proof of presence, then transmits this information back to the smart-phone or reader.

Visitor management technology being integrated with access control systems.

Visitor management will increasingly be integrated with access control systems to provide complete security solutions that protect employees and temporary visitors from intruders and unwanted guests.
Integration of visitor management with access control systems enables lobby attendants to easily and safely provide temporary proximity credentials to guests through the visitor management system, rather than the access control system. The information entered into the visitor management system during check-in is seamlessly passed to the access control system so that a proximity card for the visitor can be activated.

When the visitor leaves and is checked out by the visitor lobby system, the card is automatically deactivated, and the expiration date and time are automatically passed to the access system, ensuring that a lost or stolen card can no longer be used. Integrating visitor management with access control also eliminates the problems of having a supply of live cards at the reception desk for those who have forgotten their employee badges. **The visitor system also has a record of all visitors who have been provided an access card, so there is a complete audit trail, including information about the dates and times when cards were active.**

Cloud-based Security

The adoption of cloud-based security is another area that has gained enormous ground in recent years and looks set to continue. Security concerns over using cloud based services have been largely quashed by a wider acceptance of online use of services such as banking or retail, which have demonstrated that using IP needn't compromise vital security. As well as ease of use and installation, cloud-based services also rapidly roll out updates. Besides this eliminates the need for large servers onsite - freeing space and resources. (Refer pages 66-68 of the January issue)

Strong user authentication

Security professionals understand the importance of **multifactor authentication**, also known as strong authentication, especially for IT security. **The industry is quickly moving beyond simple passwords (something the users knows) to additional authentication factors including something the user has (such as a mobile or web token) and something the user is (ascertained through a biometric or behaviour-metric solution).** Advances in technology have made it possible for multi-application credentials that use a data model which can represent any type of identity information to be carried on smart cards or smart-phones. Users will simply take the same card (or phone) they use for building access and tap it to a personal tablet or laptop for authenticating to a VPN, wireless network, corporate intranet, cloud and web-based applications, single-sign-on (SSO) clients and other IT resources. There will be no need for a separate card reader or additional devices to issue and manage, nor will they need to enter a password on touch-screen devices.

Security Legislation

As well as the technology, legislation is moving forward to meet the demands of the security industry. IEC 60839, entitled, "Alarm and electronic security systems- Electronic access control systems - System and components requirements" aims to update the standard to take into account the latest integrated systems. It is being published at the IEC level (World standard) and also published by BSI as aN EN (European) standard. **IEC 60839 will have a profound impact on the security industry in 2014.**
