Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Convergence of Logical and Physical Security

Today's security initiatives involve guarding buildings and equipment as well as protecting networks, dealing with privacy issues, and managing risk. Given the interrelated aspects of these initiatives, the question is, "Does the consolidation of security make sense?" Until now, in most organizations, physical access systems and logical access system have operated as two independent structures, and have been run by completely separate departments. Logical access, which grants admission to the IT infrastructure such as ...

Copyright SANS Institute
Author Retains Full Rights

AD

Convergence of Logical and Physical Security

Yahya Mehdizadeh

GIAC GSEC Certification

October 14th, 2003

Mehdizadeh1@slb.com

Abstract: This paper addresses the benefits and value of the convergence of logical and physical security systems by using a common token such as a smart card. Issues from architecture to pricing to user case scenarios are addressed in this paper.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Executive Summary

Today's security initiatives involve guarding buildings and equipment as well as protecting networks, dealing with privacy issues, and managing risk. Given the interrelated aspects of these initiatives, the question is, "Does the consolidation of security make sense?"

Until now, in most organizations, physical access systems and logical access system have operated as two independent structures, and have been run by completely separate departments. Logical access, which grants admission to the IT infrastructure such as the intranet/internet, mail servers, web servers, and database applications was run by the IT department. The facilities department controlled physical access systems, which includes the employee badging process, door access to the buildings, and life support systems, e.g., HVAC, Fire and CCTV.

This paper will demonstrate that the convergence of logical and physical security brings significant benefits, specifically identifying areas where the two can interconnect to the greatest positive effect, and also recommends practical steps to take in this direction.

Background

IT Security – In a general sense, IT security concerns the ability of on-line actors to interact with information objects. It is difficult to talk about IT security without talking about the on-line identities of the actors. This brings us to the concept of identity management. Liberty Alliance defines identity management as the "set of processes, tools and social contracts governing the life cycle of a digital identity for people, systems and services to enable secure access to an expanding set of systems and applications." Identity management is a core component of IT security environments and refers to administering account information for login access to systems and applications. Based on this definition an Identity Management System consists of the following interdependent elements:

> **Data Storage** – the logical repository and data model structure, often implemented in the form of a directory, holding policy information and data access usage
>
> **Authenticator** – is responsible for performing the authentication (verifying the identity) of a user associated with a given identity. These include passwords, biometrics, or X.509 PKI certificates
>
> **Policy control** – defines who has access to what information and under what conditions
>
> **Auditing** – tracks and records the flow of information when data is created, used and changed.

Joseph Pato, a senior researcher at HP Labs, states that these components work together to provide:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Single-Sign on – allowing a user to perform primary authentication once to access the set of applications and systems that are part of the identity management environment
- Personalization – associating an application and information to an identity
- Access management – allowing applications to make authorization and other policy decisions based on privilege and policy information.

The identity management system forms a primary building block of an IT security system. The components interact with the services to grant access to corporate IT resources such as e-mail, database permissions, web access, and intranet/internet connectivity. Authentication becomes the mechanism to grant access to these resources relying on directories and access control policies to determine who has access to what resources. A key driving force for such a system is improving the user experience both from an administration and end-user perspective to improve efficiency and compliance.

According to IDC, forgotten passwords cost the typical IT department $200 per user per year. Meta group suggests 11 percent of users experience an access rights problem every month. In a survey of help desk professionals, the data indicates that 45 percent of calls to a typical help desk are for password reset assistance. These statistics suggest that having a common mechanism to manage credentials, via an identity management system, can go a long way to alleviate this problem. Keep this thought in mind; we will address the solution later in this paper.

Physical security systems control who has access to enterprise facilities, for what timeframe and under what conditions. A typical infrastructure consists of:

- Physical access control such as card readers, or biometric devices (i.e., iris scans, facial recognition, palm/thumb readers)

- Power systems, including Uninterrupted Power Supplies (UPS) generators, backup batteries, electric distribution systems etc.

- Physical blockade and locking mechanisms, e.g., electromagnetic locking devices

- Fire control and suppression systems such as sprinklers, smoke detectors, CO detectors

- Life support systems, this includes heating and cooling, ventilation, HVAC system, environmental monitors of moisture, condensation, flood, dew point, temperature, humidity, etc.

- Voice, Video and data for closed circuit TV's this includes the infrastructure such as the CSU/DSUs FDDI rings, ATM backbones.

These systems interact with each other using infrastructure services deployed by the IT department. This for example, allows the door reader to be tied to the fire protection system that in turn is connected to the CCTV system, which is monitored by the physical security system. Physical security focuses on the protection of assets, people and structure against perceived threats. Furthermore, monitoring and managing the flow of

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

individuals and assets throughout the premises is another important aspect of physical security. Managing access methods, perimeter intrusion, and tenancy are all issues that must be dealt with on a daily basis when monitoring physical access.

Why the convergence?

9/11 changed the security perception in our nation and initiated a great focus on security in general. From physical security to cyber security, the office of Homeland Security is driving the policies and conformance by corporate and civil enterprises. Add to this the liability to protect private customer information, the cost of corporate compliance, the potential costs of cyber threats and attack and identity theft; logical and physical security becomes a key focal point.

Facilities access makes compromising the security of IT systems easier. Individuals who have physical access can not only steal a PC or confidential data, but can also compromise network security. A combination of IT and physical security gives a more comprehensive view of potential intrusions across the physical and IT environments. The availability of IT sensors for SCADA systems and TCP/IP based web cam systems that monitor both the internal and external premises are just some of the ways where logical security is tied to the physical access systems.

The need to cut costs is another driving factor for this convergence. According to the Gartner Research firm, the integration of the budgets for physical and IT security can deliver substantial efficiency, particularly if provisioning is used. More on provisioning later.

Corporate mergers also contribute to this paradigm shift. One visible outcome from the union of multinational organizations is the need for a multi-purpose common identity in the form of the corporate badge. This “standard” badge is designed to provide what has become known in the industry as “global roaming” where a single card is used to access all the facilities worldwide depending on the authorizations granted. Combining multiple physical access systems results in significant cost savings. A good testament to this trend can be seen with the merger of Chevron & Texaco and the creation of their “Smart Badge” program.

Improving efficiencies is yet another factor driving this alliance. By managing the entire credential life cycle of the employee, the enterprise can control when the employee was badged, what buildings/facilities they have access to, what systems they can access and most important what happens when an employee is terminated, leaves or is transferred. The efficiencies become even more compelling when a common data repository is used for all identity related information. The data is entered into the system once and then replicated throughout the organization. This allows for common administration of users, privileges, and credentials—across the physical as well as IT realm—and means less effort and fewer possibilities for oversights or omissions whenever an employee is hired, leaves, or has a change in access permission.

Another reason for this convergence is the audit trail of such systems, which can be a tremendous help to forensic investigations. For example, during a security event, a comprehensive security log should show the PC used, the username and password, and who accessed the building. A centralized information repository is also useful for real time

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

monitoring systems. For example, when a malicious attacker enters a username and password to a secure mainframe, but the owner of that user name hasn't been logged as entering the building, then physical access alarms should go off.

Last but not least, most organizations have a physical badge issuance process in place. Typically the employee must present himself or herself to obtain a new badge. This is the ideal place to add logical identity enrollment, because it is a face-to-face meeting, which makes it easy to collect biometrics (such as photo, fingerprint, signature, or iris scan), to securely deliver the badge to the subject, and to instruct the subject in selection of the PIN and secrecy of credentials. Combining the enrollment processes results in only a slight cost increase over physical badge issuance alone. The synergy is strongest when logical credentials (e.g., PKI keys) are issued and stored on the badge at the same time, as was the case with the Department of Defense Common Access Card.

In order to make this convergence happen, security management must be integrated with existing business processes for managing facilities, personnel and IT systems. This requires clear organizational ownership and accountability across a number of critical management processes. These include:

- Enterprise security policy definition
- User provisioning and asset management
- Security monitoring and auditing
- Incident response
- Business continuity planning [1]

Source: Open Security Exchange, PHYSBITS

Technology becomes a key enabler of these processes, where it can reduce the threat of specific vulnerabilities. An integrated approach to event management with defined business processes, enables complex attacks on facilities and IT systems to be detected, correlated and prevented. The diagram above depicts how physical and IT security can interface with business security management processes.

How to bring about this convergence?

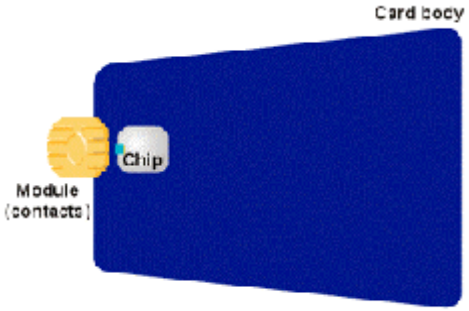
To bridge the gap between IT and Physical security, a common token is needed. A multi-purpose smart card, featuring embedded micro-controller silicon is the logical choice. The chip card hardware platform is both secure and mature. It is difficult to clone or tamper with and offers versatility needed for this association. The card has the capability to hold a picture ID and other printed identifiers, including the cardholder's signature, fingerprint or other biometric identifier, as well as a magnetic "swipe" strip and/or a bar code.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Smart cards can provide several security-level options ranging from simple access control to complex data encryption. For example, employees can enter controlled buildings by passing their smart-card badges in front of a reader and use the stored keys on their smart cards to log on to networks or send encrypted e-mail messages.

The card is embedded with two chips; first a programmable chip that is used with a card reader to authenticate the cardholder to computers and data. The second chip is the proximity chip, which is used for access to facilities and building.

When selecting smart card technology for IT purposes, two important selection criteria are memory space and operating system.



Source: Gemplus - All About Smart Cards

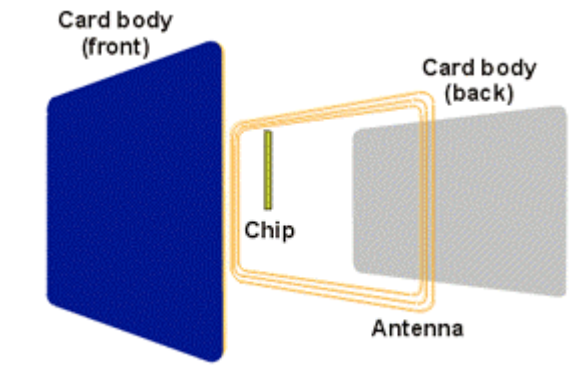
The existing space for the electrically erasable programmable, read-only memory (EEPROM) smart cards is 8, 16, 32 and most recently released, 64K (kilobytes). To determine the memory size needed for an organization, it is imperative to identify the applications needed for logical access. The common types of application include: windows logon, e-mail and file encryption, password management, application (web) authentication and electronic purse for vending machines and cafeteria. For example, authentication applications require only 8K of memory, while each private key takes an additional 3K of memory space. Add to this a loyalty program (5K) or password management applet (8K) and you can determine the memory size needed.

On the OS side the choices are MULTOS from MAOSCO and JavaCard from Sun Microsystems. In recent years, JavaCard has gained significant market share due to its ability to store and update multiple applications. According to Gartner, 15% of the smart cards shipped in 2000 were JavaCard compliant.

The security heritage of smart cards allows them to provide confidentiality, authentication, and non-repudiation for practical IT uses. Furthermore, smart cards use a unique serial number and a Personal Identification Number (PIN) to identify a user, prove identity and grant network access. In addition, by combining smart cards with Public Key Infrastructure (PKI), the cards can store the algorithms, keys, and certificates required to encrypt confidential information. Once this information is encoded (encrypted), the information is extremely difficult to decode without the keys, which never leave the card, which prevent them from being intercepted by a third party.

On the Physical side, the choices are contact and contactless cards.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.



Source: Gemplus - All About Smart Cards

Contact smart cards use an eight-pin contact, micromodule to physically connect to the card reader. Although some of the older facilities still have this technology deployed, it is being replace with contactless cards. This is due to poor reliability of the contact smart cards and the wear and tear on the card as a result of inserting into the reader.

Contactless smart cards use an antenna with approximately a 10-centimeter (cm) range to communicate with the reader. These cards derive their power from a radio frequency (RF) generated by the electromagnetic field produced by the card reader antenna. The RF field also transfers information to and from the card and card reader. Employee identification badges issued by large companies for building access are typically contactless smart cards.

The fundamental benefit of using a smart card for both physical and IT security is enhanced security due to the use of multiple factors in authentication: i.e., you need both the card and a personal identification number (PIN) to gain access. A related benefit is the ability to enforce this stronger security while eliminating the need for multiple passwords that tend to increase demand for technical support as well as impact productivity. Smart cards can improve return on investment, through the elimination of multiple passwords and increased transparency that eliminates abuses, such as credential sharing. This is a good solution to the problem of high password management costs noted by IDC and Gartner, as stated earlier.

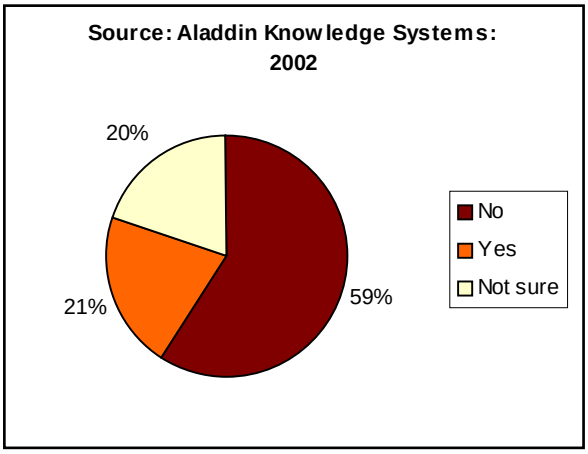
Are enterprises deploying this technology?

Tim Gower, an analyst from London based research firm Datamonitor, predicts substantial growth in the number of smart cards issued by large enterprises to their employees for the purpose of identification. According to Gower, it is expected that this category will grow from 14 million cards in 2002 to 36 million cards in 2006, a compound annual growth rate of 27%.

IBM, Microsoft, NEC, Nissan, Shell, Sun Microsystems and Schlumberger are examples of corporations that have issued tens of thousands of smart cards to their employees. Procter & Gamble, Boeing, and Pfizer are companies that have a embarked on a pilot program to replace corporate badge with smart cards.

Finally government agencies have helped boost smart card ID's, such as the US department of defense rollout of 4 million chip based Common Access Cards to its civilian and military personnel.
Finally government agencies have helped boost smart card ID's, such as the US department of defense rollout of 4 million chip based Common Access Cards to its civilian and military personnel.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.



Are you currently merging, or planning to merge, network security and physical security?

In November of 1999, the Deputy Secretary of Defense directed the Military Services to implement smart cards in the form of a Common Access Card (CAC). The CAC has numerous functions – literally combining several cards into one. In addition to replacing the existing DoD identification card, the CAC enables physical access to buildings and controlled areas, access to computer network and systems as well as serving as the primary platform for the Public Key Infrastructure (PKI) token.

The primary benefit of CAC deployment is the automation of many paper-based processes. What had been taking days to do, is now taking just hours. Military personnel are using the card to enter their installation, log onto computers, verify medical benefits eligibility and gain dining facility privileges. All of this added to PKI adds up to increased protection for both personal and national security.

Today, the DoD CAC program is the largest deployment of cryptographic Smart Cards for information security. The Department of Defense (DoD) embraced this technology due to the security, flexibility, cost/unit, ease-of-use, and durability the cards provided. It is anticipated that the initial CAC issuance to DoD personnel will be completed by end of October 2003.

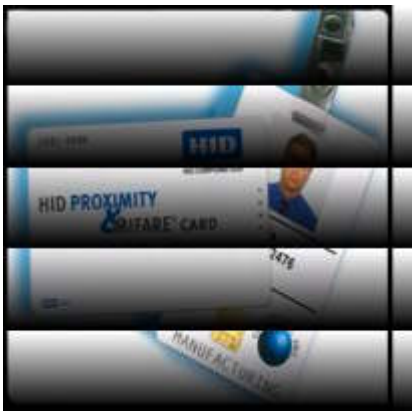
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Technology architecture

As the value of the convergence of physical and logical security becomes more apparent, the question becomes, how best to do this? The first step is to examine each system's requirements independently and then incorporate the collective requirements during the design phase.

Physical Access systems must be reviewed both from a technology and process standpoint. From a technology perspective, physical access standards need to be reviewed and agreed upon. A quick review of fortune 500 companies, indicate that proximity (contactless) cards are the more prevalent physical access card in corporate environment. Two of the leading building-access card vendors are HID and Casi-Rusco. Both companies have partnered with smart card vendors and IT security system integrators to allow their customers to integrate facilities and network security. More information about the two vendors can be found at http://www.hidcorp.com/ and http://www.casi-rusco.com



Once the physical access type has been specified it's important to define card specifications. It is recommended that the card comply with ISO specifications 7810, 7811 and 7816 for size, thickness, smart chip contact locations, and magnetic stripe locations. See Appendix A for more information on the ISO specs. Contactless smart cards should conform to ISO 14443 (Type A, B or C). This spec is specifically for contactless proximity cards operating at 13.56 MHz in up to 5 inches distance. See Appendix B for more information on the ISO specs for contactless cards. When selecting contactless badge stock for physical access, combination cards that have multiple contactless modules such as an HID + MIFARE combo card can be helpful in a multi environment physical access system. This also becomes useful when migrating from one technology to the other.

To ensure logical access technology can reside on the same card, evaluate multiple badge vendors. As an example, HID's Smart ISOProx II and Smart DuoProx II multi-technology cards are proximity cards that can be embedded with the contact smart modules. There are many smart card vendors to choose from. According to Gartner, GemPlus, Orga, Schlumberger, Oberthur and Giesecke & Devrient control 89% of the worldwide chip card production. As long as a card vendor complies with the stated standards, any vendor can be chosen based on availability, pricing, features and delivery.

Once the card technology has been defined, next comes the door reader. In selecting door reader technology, the existing system should be reviewed with an understanding of future directions. Technology selection should consider migration path as well as upward and downward compatibility. For example, the HID MultiProx reader makes it possible to replace an existing Schlage/Westinghouse card access control system with any Wiegand protocol system, without replacing the existing Schlage/Westinghouse cards or the installed wiring.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The logical access system is more complicated. The key components are the directory, the public key infrastructure (PKI), and the integration with the existing computing infrastructure to allow for credential based interaction with mail servers, web server, and other corporate applications. For a PKI infrastructure, there are many technology providers such Entrust, Baltimore, Microsoft, RSA, and VeriSign to choose from with each having their own implementation issues. More information on PKI implementation can be found at: http://www.pki-page.org/ and http://csrc.nist.gov/pki/. Other components needed for logical access are the PC smart card reader (USB, PCMCIA, Keyboard reader), and the client PC middleware that allows the smart card to be read by the PC reader.

Once the technology has been selected for logical and physical access systems, the next step is the process definition. The badge issuing process needs to be reviewed and documented. This is where considerable amount of time is spent defining processes such as new badge creation, badge deployment, lost badge replacement, temporary badge issuance, visitor/contractor badge issuance and more. To tie the logical and physical access system, a single identifier is needed with attributes defined in a common record in the data repository. For example, Entrust embeds the DN into name of the cert issued. This identifier is then used by both the logical and physical access system in the data repository.

As a part of the IT infrastructure, deploying a provisioning system can be complementary when upgrading or deploying a badging system. In addition to managing the provisioning of various IT resources, such as creating email accounts and granting intranet access, provisioning systems improve enterprise security by providing visibility into and control over user access privileges. For instance the provisioning system can be designed to react to potential risks such as inactive badges, or can have the ability to enforce consistent corporate security policies while providing a central point from which user accounts and facilities access can be instantly revoked. Another benefit of a provisioning system is the reduced user administrator cost and improved assurance of administrative actions. Business Layers and WaveSet are strong players in the provisioning space who have solutions that address managing both physical and logical credential life cycles.

Architecture Diagram

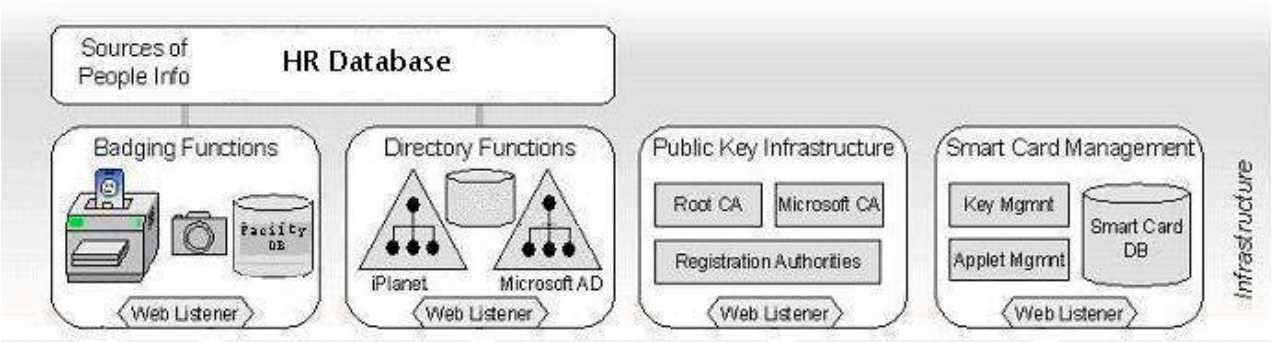
In the next section we will discuss a proposed architecture of a physical and logical access system to examine and illustrate how they interact with each other. A combined physical access and logical security system can be broken down in the following sub systems:

The **Infrastructure Sub-System** consists of the components that are used by the facilities and IT departments. This includes the badging station for digital and facilities access, the directory containing employee information that is linked to the HR database. In addition, there is the Public Key Infrastructure (PKI) for certificate-based resources and the Smart Card Management System, which is used to manage smart card badge throughout its life cycle. It is recommended that the primary mechanism for communication across these

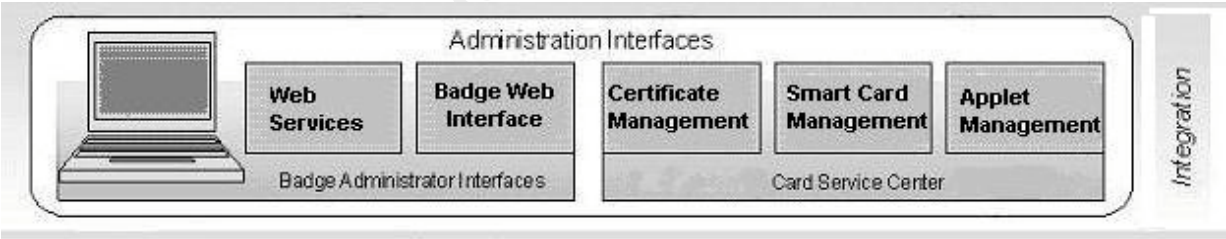
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

systems be via web interface and therefore that the primary communications protocol among the sub-systems and their internal components should be HTTP.

From a design standpoint, the Smart Card database is separate from the directory functions. This gives it the ability to operate independently for card services and can be commissioned and decommissioned by choice. This also makes separation of duties and responsibilities within an organization more attainable.



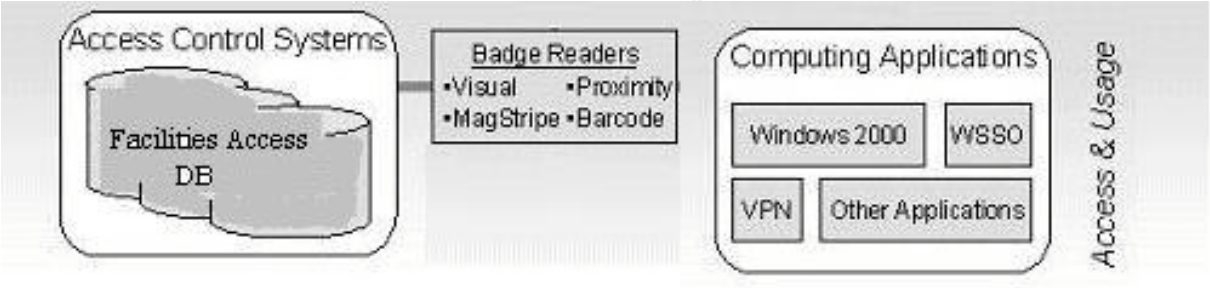
The **Integration Sub-Systems** are mainly used to manage the smart card both for logical and physical access. The Badge Administrators Interface manages the access authorization to the facilities, while the Card Service Center controls all user-initiated card management tasks including applet management. Some of the more popular applets deployed in corporate enterprises are: single-sign-on (SSO), password manager and e-purse applet for cafeteria access. Although the two systems are independent, they do interact where necessary to support intrusion detection and other security services.



The **Distribution Sub-System** includes the devices, software, and hardware that employees interact with enabling them to use their smart card in their PCs. This includes, the smart card, the smart card reader (USB or PCMCIA), and the client middleware that resides on the PC.

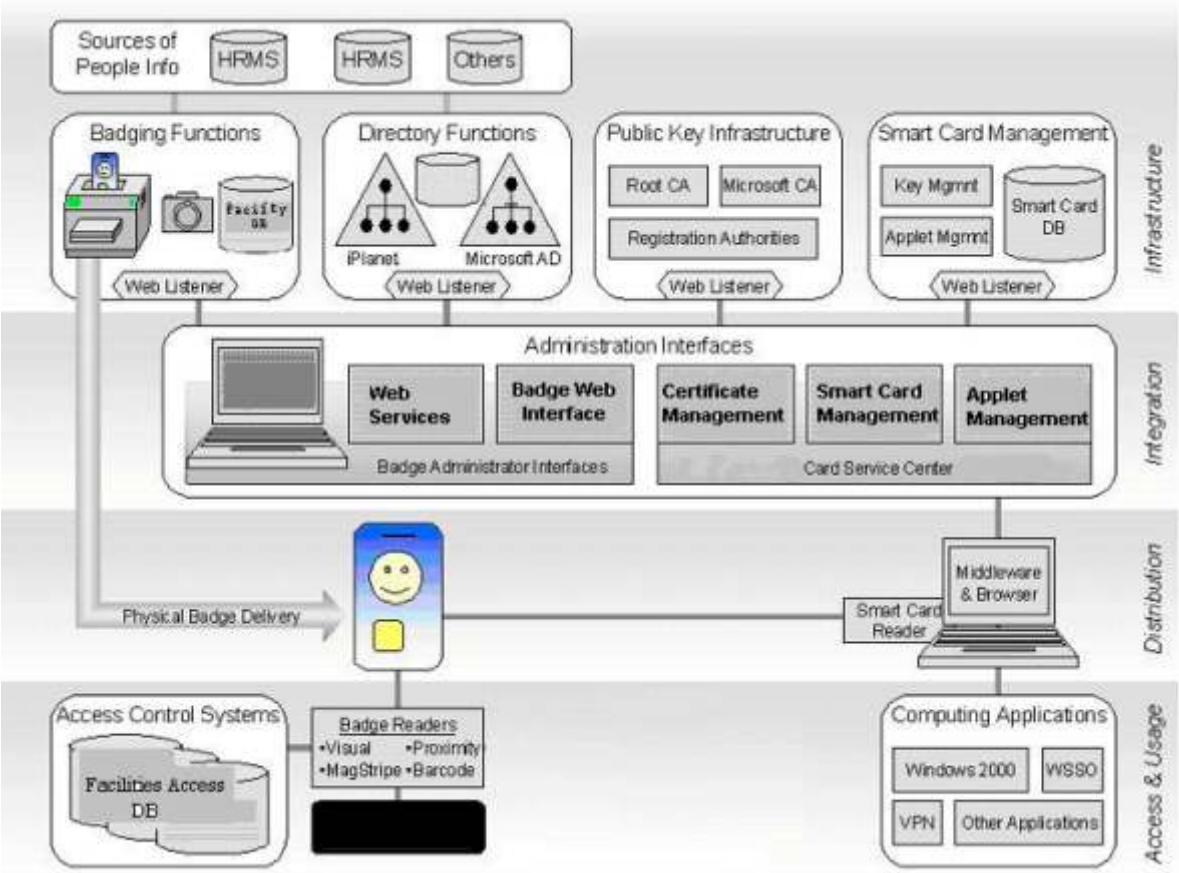
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The **Access and Usage Sub-System** includes the access control systems, and computing applications that use the smart card. Computing applications are applications that have been modified or deployed to use the credentials (public/private keys) on the smart card. For example, a primary use of the smart cards in a corporate enterprise can be to authenticate users to their domain (W2K/XP), provide single-sign-on (SSO), and grant access to remote users connecting via a VPN connection. Once again the preferred method for authenticating users is utilizing X.509 user certificates. This is also the layer that interacts with the facilities database to authorize physical access to the facilities.



These four sub-systems interact to enable the full badge management life cycle. Once the card issuance station issues the smart card, the smart card management system is used to personalize the card. Employee data from the directory must be correlated and associated with the facilities database and with the card management system database. Applications need to be modified to allow credentials to be used for authentication.

Yahya Mehdizadeh
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.



User Case Scenarios

Now that we have the system defined, let's examine a number of user case scenarios that makes the convergence of logical and physical access functional. We've previously presented the value of improved correlation of security events seen from the logical and physical systems. In addition to the traditional network logon, application authentication and building access, a combined logical and physical system can be beneficial in the following areas:

- Logical login required at the front desk to authorize contactless entry for each shift. This prevents the use of lost or stolen cards for building entry beyond one shift or accessing the database when the shift is over.

- For improved security, user can be required to use their card not only to enter the facilities, but also when leaving the building.

- Requiring a card to authenticate people at large events such as annual meetings or other company specific events.

- The card can be architected to produce "follow-me" behavior. Thus a user can walk from building to building, insert their card, and their desktop reappears so the user can log-in to any PC for email, intranet access or other common applications.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The SunRay from Sun Microsystems, Microsoft Terminal Server or a thin client Citrix solution are good examples of this.

- Using the card for information access control, where the authorization level determines facilities access and data access such as for employees that need access to a personnel file stored in secure data room.

- Controlling the sharing or printing of proprietary or private data. For example, the user prints a document and walks to the printer, but the document doesn't print until the card is inserted into the printer.

- Using the card for VPN access, either at home or on the road. When the user travels to another location, they not only need their smart card to access the facilities, but also need their card to get access into the corporate network.

How much does it cost?

The pricing of corporate ID cards depends on the complexity of the environments they are deployed in. Card technology magazine states that $100 per user is a reasonable estimate for introducing smart cards for network security. This includes the cost of cards, readers and software (middleware) for the client PC.

The 32K smart cards cost around $10 each depending on volume. Depending on the physical access chip, add another $3-5 to the card price, resulting ~ $15 per card. The middleware ranges from $10-$35 per seat depending on features and volume discount. The PC card reader pricing depends on whether USB (~ $22) or PCMCIA (~$50) interface is used. Add to all this the integration, deployment and testing, the price tag could easily go beyond $100 per user.

In addition to the network access infrastructure, door readers also need to be deployed or upgraded. The cost of such deployment range from $2500 - $5000 per door, depending on location, wiring and construction required. When upgrading the door readers, it is important to comply with all OSHA safety requirements and ensure that all appropriate permits from the city and fire department have been obtained.

Last but not least there is the technical consulting associated with software customizations, project management, deployment, transition and training. With an average rate of $175 an hour, a project could run between 8000 – 10000 hours for a 50,000 user deployment putting its price tag in the $1+ million dollar range.

Practical Steps

Combining logical and physical security is a complex project, but the cost savings and enhanced security can provide significant bottom line benefit. In embarking on such a venture, the following practical steps are recommended:

Yahya Mehdizadeh
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Proper due diligence in consolidating logical and physical security is extremely important. During this exercise, the degree of fusion between departments must be gauged to determine what works best within the organization taking into account culture, structure and geographic distribution.

Policies and procedures of both physical and IT security must be reviewed jointly to define a common framework. For example, a strict security policy might require that workstation login should not be permitted unless the cardholder is registered as having entered the premises. Security managers must be able to override network access controls and open doors, if necessary, typically through mechanical means.

Assigning the right people who are well versed in both IT and physical security is another step that will contribute to the success of this endeavor. Personnel with Certified Protection Professional (CPP), combined with a Certified Information Systems Security Professional (CISSP) are the best profile for such a project.

In general, networks that transmit control information for physical access systems should be separate from general enterprise data networks, however secure they may be.

Look at the various technology options. Matching organizational requirements with available technologies may be difficult but well worth the effort in the long run. It is important to keep actual deployment timelines in mind. For example, you may conduct your pilot with a 32K smart card, but when you are ready to deploy, the 64K card may be available and more cost effective long term.

Learn from a pilot deployment. No matter how clear a project plan, it is imperative to setup live pilots throughout the organization to identify technical issues, validate architecture and gauge end-user acceptance.

A deployment time frame of 12 to 24 months is reasonable depending on complexity.

And most important, obtain upper management support while communicating with key stakeholders during the various phases of the project.

Conclusion

Security concerns, cost control objectives, corporate efficiencies, and advances in security technology have all been significant factors in the integration of logical and physical access systems. While the synergies and benefits of creating such a union are great, the deployment of such a project requires substantial resources: time, money, people, technology and processes.

Clearly, smart cards are the right choice to bring about the convergence for access to buildings, networks and PCs. They provide the versatility and security needed for large enterprises. Successful deployment requires extensive planning combined with senior corporate sponsorship and buy-in from executive management.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

Andrew Phillips. "Enterprise Smart Cards: Securing Buildings, PC and Corporate Networks" Gartner Dataquest (January 2002) http://www4.gartner.com/Init

Donald Davis. "The New Look in Corporate ID Cards." Card Technology Volume 8 Number 8 (July 2003): Page 30 – 39

Bring IT and Physical Security Together, InfoTech Research Group (June 2003) http://www.infotech.com/

[1]Open Security Exchange, PHYSBITS, April 2003, Page 39 – 41 http://www.opensecurityexchange.com/

"Physical And IT Security: Converging With The Traditional Roles Of The Facility Manager," Today's Facility Manager, March 2003 http://www.facilitycity.com/tfm/tfm_03_03_special.asp

Linda McCarthy, IT Security – Risking the Corporation, New Jersey, Prentice Hall PTR, 2003

Joseph Pato, Jason Rouault, "Identity Management: the drive to federation" http://devresource.hp.com/drc/technical_white_papers/IdentityMgmt_Federation.pdf

http://www.fbi.gov/congress/congress00/cyber021600.htm

http://www.gemplus.com/basics/index.html

http://www.hidcorp.com/

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix A

ISO 7810, 7811 & 7816

ISO Magnetic Stripe Card Standards

The majority of magnetic cards used in the UK, Europe and USA confirm to the following ISO standards for magnetic cards.

Description of Standard	ISO Number
Physical Characterisitics of Credit Card Size Document	7810
Embossing	7811-1
Magnetic Stripe - Low Coercivity	7811-2
Location of Embossed Characters	7811-3
Location of Tracks 1 and 2	7811-4
Location of Track 3	7811-5
Magnetic Stripe - High Coercivity	7811-6

Full copies of these standards can be pruchased from www.iso.org and www.ansi.org. The information below is abstracted from these standards.

Physical Dimensions of Cards:

Physical Plastic Card
2.175", 55.245mm
3.375", 85.725mm
0.030", 0.762mm thick

© SANS Institute 2004, Author retains full rights.

Characteristics of Tracks:

Position

Track Number
Recording Density
(bits per inch)

Character Configuration
(including parity bit)

Information Content
(including control characters)

0.223" (5.664mm) from card edge

0.110" (2.794mm)

Track 1
210BPI
7 bits per character
79 Alphanumeric characters

0.110" (2.794mm)

Track 2
75BPI
5 bits per character
40 Numeric characters

0.110" (2.794mm)

Track 3
210BPI
5 bits per character
107 Numeric characters

ISO 7816 is the main international standard for smartcards. It is split into various sections that defines the physical and electronic properties of the cards including the position of the contacts and the communications protocols that are used. ISO 7816 standard are separated in 3 different parts:

- ISO7816-1 which define the physical characteristics of the card.
- ISO7816-2 which define dimension and contact position of the card.
- ISO7816-3 which define the electrical signals and transmission protocols.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix B

ISO/IEC 14443 is one of a series of International Standards describing the parameters for identification cards as defined in ISO 7810 and the use of such cards for international interchange.

This part of ISO/IEC 14443 describes the physical characteristics of proximity cards. This International Standard does not preclude the incorporation of other standard technologies on the card, such as those referenced in the informative annexes.

Contactless Card Standards cover a variety of types as embodied in ISO/IEC 10536 (Close coupled cards), ISO/IEC 14443 (Proximity cards), ISO/IEC 15693 (Vicinity cards). These are intended for operation when very near, nearby and at a longer distance from associated coupling devices respectively.

Identification cards - Contactless integrated circuit(s) cards - Proximity cards
Physical characteristics

1 Scope

This part of ISO/IEC 14443 specifies the physical characteristics of proximity cards, (PICC). It applies to identification cards of the ID-1 card type operating in proximity of a coupling device.
This part of ISO/IEC 14443 shall be used in conjunction with later parts of ISO/IEC 14443 which are in development.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 14443. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 14443 are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.
ISO/IEC 7810:1995, Identification cards - Physical characteristics.
ISO/IEC 10373, Identification cards - Test methods.

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of this part of ISO/IEC 14443, the following definitions apply:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3.1.1 Integrated circuit(s) (IC):

3.1.2 Contactless:

Pertaining to the achievement of signal exchange with and supplying power to the card without the use of galvanic elements (i.e., the absence of a direct path from the external interfacing equipment to the integrated circuit(s) contained within the card).

3.1.3 Contactless integrated circuit(s) card: An ID-1 card type (as specified in ISO/IEC 781

3.1.5 Proximity coupling device (PCD):

The reader/writer device that uses inductive coupling to provide power to the PICC and also to control the data exchange with the PICC.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

4 Physical characteristics

4.1 General

The PICC shall have physical characteristics according to the requirements specified for ID-1 cards in ISO/IEC 7810.

4.2 Dimensions

The nominal dimensions of the PICC shall be as specified in ISO/IEC 7810 for the ID-1 type cards.

4.3 Additional characteristics

4.3.1 Ultra-violet light

4.3.2 X-rays

shall continue to function normally exposure of either face to medium-energy X-radiation, with energy 100 keV, of a cumulative dose of 0.1 Gy per year.

NOTE 1. This corresponds to approximately double the maximum acceptable dose to which humans may be exposed annually.

4.3.3 Dynamic bending stress

shall continue to function normally

4.3.4 Dynamic torsional stress

shall continue to function normally

4.3.5 Alternating magnetic fields

a) The PICC shall continue to function normally after exposure to a magnetic field of average level given in the table below:

Frequency Range (MHz)	Average Magnetic Field Strength (A/m)	Averaging Time (minutes)
0.3 - 3.0	1.63	6
3.0 - 30	4.98/f	6
30 - 300	0.163	6

f - frequency in MHz

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The peak level of the magnetic field is limited to 30 times the average level.

b) The PICC shall continue to function normally after exposure to a magnetic field of 12 A/m at 13,56 MHz.

4.3.6 Alternating electric field

The PICC shall continue to function normally after exposure to a electric field of average level given in the table below:

Frequency Range (MHz)	Average Electric Field Strength (V/m)	Averaging Time (minutes)
0.3 - 3.0	0.614	6
3.0 - 30	1842/f	6
30 - 300	61.4	6

f - frequency in MHz

The peak level of the electric field is limited to 30 times the average level.

4.3.7 Static electricity

shall continue to function normally

4.3.8 Static magnetic field

shall continue to function normally

.

WARNING: The data content of a magnetic stripe might be erased by such a field.

4.3.9 Operating temperature

The PICC shall function normally over an ambient temperature range of 0 °C to 50 °C.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**