Using Smart Cards for Secure Physical Access

A Smart Card Alliance White Paper

July 2003

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

Table of Contents

Executive Summary

Smart Cards Make Sense for Securely Controlling Physical Access

Smart cards are increasingly accepted as the credential of choice for securely controlling physical access. Standards-based smart identification (ID) cards can be used to easily authenticate a person's identity, determine the appropriate level of access, and physically admit the cardholder to a facility. Through the appropriate use of contact or contactless smart card technology in the overall physical access system design, security professionals can implement the strongest possible security policies for any situation.

More than one access application can be carried on a single smart ID card, enabling users to access physical and logical resources without carrying multiple credentials. Security can change access rights dynamically, depending on perceived threat level, time of day, or other appropriate parameters. Information Technology (IT) can record and update privileges from one central location. Human Resources (HR) can process incoming and outgoing employees quickly, granting or withdrawing all access rights at once in a single transaction. The organization as a whole incurs lower maintenance costs.

Flexibility and Mature Standards Are Hallmarks of Smart Card Technology

Smart card support for multiple applications allows organizations to expand card use to provide a compelling business case for the enterprise. Smart cards not only secure access to physical or logical resources, they can store data about the cardholder, pay a fee or fare if required, certify transactions, and track ID holder activities for audit purposes. Because supporting system components can be networked, shared databases and inter-computer communication can allow separate functional areas in an organization to exchange and coordinate information automatically and instantly distribute accurate information over large geographic areas.

Smart card technology is based on mature standards (contact and contactless). Cards complying with these standards are developed commercially and have an established market presence. Multiple vendors are capable of supplying the standards-based components necessary to implement a contactless physical access system, providing buyers with interoperable equipment and technology at a competitive cost.

Implementation Should Be Driven by Application and Organizational Requirements

Organizations must consider many factors when implementing a new physical access control system, including: what user interface, performance and security requirements are needed; what level of integration is required with other enterprise applications; how to implement a system architecture that cost-effectively meets security requirements; which technology to use to meet organization requirements; how the life cycle of the ID credential is to be managed; and how the organization will migrate to the new technology while still leveraging legacy access control systems.

Smart cards are flexible, providing a migration path for which an organization's requirements, not card technology, is the driving force. Multi-technology smart cards can support legacy access control technologies, as well as include new contact or contactless chip technology. When migration

is planned carefully, organizations can implement new functionality, while accommodating legacy systems as may be required.

About This White Paper

This white paper was developed by the Smart Card Alliance to provide a primer on smart card-based physical access ID systems. This paper provides answers to commonly asked questions about the use of smart cards for physical access, such as:

- How does a physical access control system work?
- What role can smart cards play in a physical access control system?
- What are key issues that need to be considered when implementing a smart card-based physical access control system?
- What other applications can be combined with smart card-based physical access systems?
- What are migration options for organizations moving to smart card-based physical access systems?

Introduction

Managing access to resources is assuming increasing importance for organizations everywhere, from small entrepreneurial companies to large corporate enterprises and government bodies of all sizes. Even the most neutral organization now recognizes the danger of a security breach.

Administering access to resources means controlling both physical access and logical access, either as independent efforts or through an integrated approach. Physical access control protects both tangible and intellectual assets from theft or compromise. Logical access control enables enterprises and organizations to limit access to data, networks, and workstations to those authorized to have such access.

Background

Coordinating people and privileges has traditionally relied on the use of an identity card such as a driver's license, library card, credit card, membership card, or employee identification card. Such cards verify to a person (such as a guard) or a device (such as an electronic reader) that the holder has particular rights and privileges. In response to the need for increased security, industry developed technologies (such as magnetic stripe, bar codes and proximity chips) that can be included on a card. The card can then be passed through a magnetic stripe reader, scanned by a bar code reader, or presented to an electronic reader with an RF antenna for automatic access authorization. A personal identification number (PIN) can be entered via a keypad to add another authentication factor to help verify that the cardholder is indeed the owner of the card. However, while these technologies reduce cost and increase convenience, they do not guarantee that the user is in fact the authorized person.

Changes to the work force compound the problem of identifying and authenticating individuals. The days of a stable and recognizable workforce are essentially over. Currently, many corporations experience growing employee turnover or have difficulty filling specific assignments and frequently use outside contractors. This environment results in the presence of new or unrecognized personnel with access to corporate assets and information. While employee turnover generally is not as great an issue for government organizations, the rotation of personnel and the sheer size and complexity of such organizations creates a similar situation with potential for unauthorized people to obtain access to resources.

The stage is thus set for the introduction of access identification systems based on an identity card or other credential that includes integrated intelligence. Such a credential could support multiple secure applications for processing personal identification information, privileges, and access rights and include cryptographic protection of the information. The emergence of an intelligent credential was the genesis for an entirely new access control model that achieves fast processing, personal authentication, and risk mitigation. This model represents a blueprint for a secure identification system that solves the fundamental access control problem – how to accurately associate individuals with their rights and privileges at the location where the access decision must be made. Such a "smart" ID card can include a magnetic stripe, Wiegand strip, bar code, RF device, smart card chip and other security technologies.

Smart Card-Based Physical Access Control Systems

A physical access control system is a coordinated network of ID cards, electronic readers, specialized databases, software and computers designed to monitor and control traffic through access points.

Smart card-based physical access control systems are a powerful and efficient security tool for protecting enterprise assets. Each employee or contractor is issued a smart ID card displaying enterprise information and printed designs, both to thwart the possibility of counterfeiting and to identify the card as official. The card typically displays a picture of the cardholder. Each card stores protected information about the person and the person's privileges. When the person is initially enrolled and accepts the card, these privileges are accurately and securely populated throughout the system. (If such privileges change, the new information can immediately be updated securely throughout the network.) When the card is placed in or near an electronic reader, access is securely and accurately granted or denied to all appropriate spaces (for example, a campus, a parking garage, a particular building, or an office). When an employee leaves an organization, all physical access privileges are removed at once. Any future attempt by that person to re-enter the premises using an expired or revoked card could be denied and recorded automatically.

Both private enterprises and government agencies are increasingly implementing smart card-based access control systems. Brief profiles of the smart card implementations at Sun Microsystems™, Microsoft®, American Express and the U.S. Department of State are included in Appendix A. Also included in Appendix A are descriptions of planned smart card programs at the U.S. Department of Homeland Security, National Aeronautics and Space Administration (NASA) and Transportation Security Administration (TSA).

Additional Opportunities

Ideally, an access control system provides protection for both physical and logical access simultaneously. The credential used for physical access can also support computer network access and public key infrastructure (PKI) (including use for secure remote access, secure email, digital signature and secure virtual private network (VPN)). The goal of simultaneous protection can be achieved by commingling or sharing the secure databases dedicated to each type of application, enabling both centralized administrative control and analysis of unauthorized access attempts. By combining the monitoring information from both physical and logical systems, security policies can be universally enforced and investigated. Information collected can be invaluable in analyzing risk enterprise-wide.

Adoption of a smart card-based access control system can result in other advantages to an organization, including:

- Elimination or reduction of the need for multiple cards, PINs, and access codes.
- Leveraging of legacy systems, allowing for cost efficiencies including reuse of some physical access system components, while providing a significant increase in security.
- Elimination of the need to replace cards when rights or privileges change.

- Centralized administration, allowing the organization to maintain or increase security while saving time, achieving more comprehensive distribution of information, managing global changes for access privileges from a single point and reducing the complexities involved in synchronizing multiple systems.
- Flexibility for supporting multiple functions within an organization (for example, facilities security and IT) to manage and control separate applications on a single multi-application smart ID card.

This paper provides a primer for understanding physical access control systems that use a smart ID card for personal identification. Designed as an educational overview for decision makers and security planners, it describes physical access system architecture and components, provides guidance on key implementation considerations, describes smart card technologies used for physical and logical access, discusses migration considerations in moving from legacy physical access systems to smart card-based systems and showcases other applications that can be combined with a smart card-based secure physical access system.

Physical Access Control System Overview

To the user, an access control system is composed of three elements:

- A card or token (an identity credential) that is presented to a door reader
- A door reader, which indicates whether the card is valid and entry is authorized
- A door or gate, which is unlocked when entry is authorized

Behind the scenes is a complex network of data, computers, and software that incorporates robust security functionality. This section describes the operation and components of a typical smart card-based physical access control system. It provides a context for understanding how contact and contactless smart card technologies are used in an access control application.

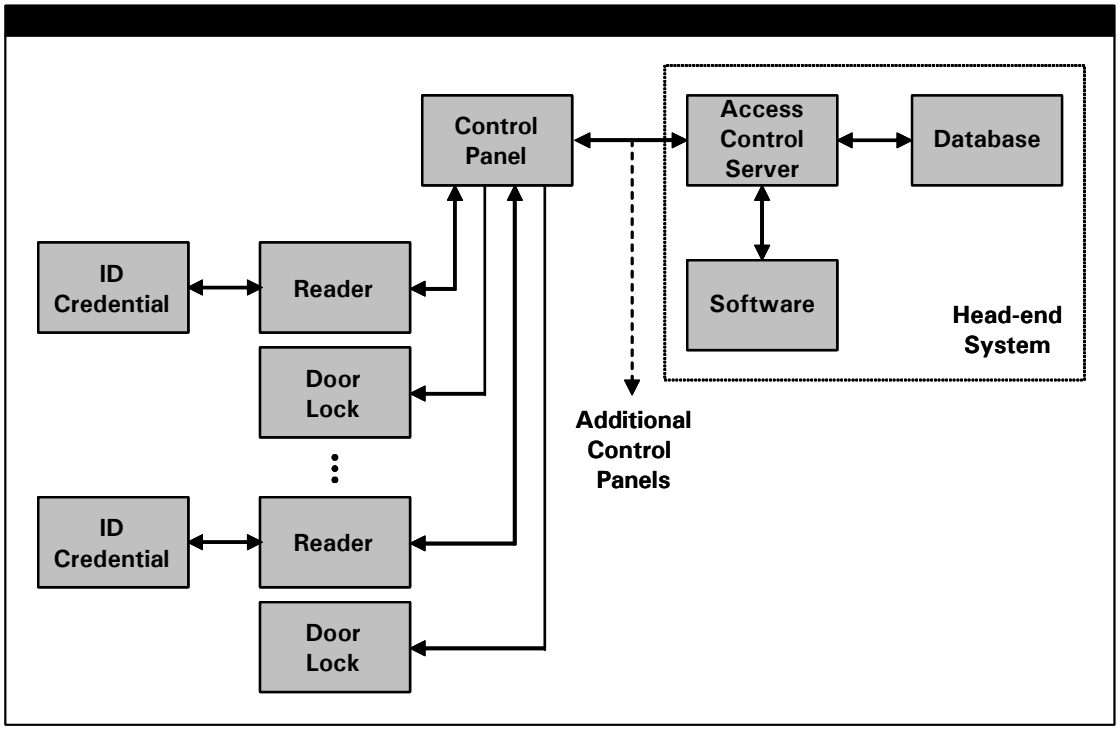
Access Control System Components

A typical access control system is made up of the following components:

- ID credential (smart card)
- Door reader (smart card reader[1])
- Door lock
- Control panel
- Access control server
- Software
- Database

Figure 1 illustrates how these basic components interconnect, with each component described in the following sections.

Figure 1: **Access Control System Schematic**



[1] Smart card "readers" can both read and write to a smart card.

Access Control Process

The access control process begins when a user presents the credential[2] (typically an employee's smart card badge or ID) to the reader, which is usually mounted next to a door or entrance portal. The reader extracts data from the card, processes it, and sends it to the control panel.

The control panel first validates the reader and then accepts the data transmitted by the reader. What happens next depends on whether the system is centralized or distributed.

In a centralized system, the control panel transmits the data to the access control server. The access control server compares the data received from the card with information about the user that is stored in a database. Access control software determines the user's access privileges and authorization, the time, date, and door entered, and any other information that a company may require to ensure security. When access is authorized, the access control server sends a signal to the control panel to unlock the door. The control panel then sends out two signals: one to the appropriate door lock, which unlocks the door, and one to the door reader, which emits an audible sound or otherwise signals the user to enter.

In a distributed system, the control panel allows or denies entry. The access control server periodically provides control panels with data that enable the control panel software to determine whether a user is authorized for access. The control panel then performs the access control server functions described above and makes the decision to allow or deny entry. Enabling control panels to perform the decision function has the advantage of requiring less communication between control panels and a central access control server, thus improving overall system performance and reliability.

If a biometric or PIN is incorporated into the system, the reader typically authenticates this data. Validity can be determined by the reader or within the smart ID card by comparing the data to a biometric template or PIN stored on the card. (In some cases, biometric data may be sent to the control panel for processing.) If the additional information is valid, the reader sends the credential's identification number to the control panel. If the information is invalid, then the card reader indicates that, and entry is denied.

The response to an invalid card is defined by the company's security policy and procedures. The access control server or control panel could ignore the data and not send an unlock code to the controller or door lock. It could send a signal to have the reader emit a different sound, signaling that access was denied. It could notify and activate other security systems (e.g., closed-circuit TV, alarms), indicating that an unauthorized card is being presented to the system.

Each access control system component in this process is described in more detail below.

[2] This white paper uses the term "credential" to refer to the general identification device (both the physical device and the data it holds). This is commonly referred to as the "ID token" in physical access control systems.

The ID Credential

A number of different ID technologies are currently in use for access control: magnetic stripe, Wiegand strips, barium ferrite, 125 kHz proximity technology[3], contact smart cards and contactless smart cards. These technologies can be packaged in a variety of form factors – everything from a key fob or an employee badge to even more exotic forms, such as a wristwatch or ring. However, all credentials operate in basically the same way: they hold data that authenticate the credential and/or user.

Some credential technologies are read-only. Information is permanently recorded on the credential, and when the credential is presented to a reader, the information is sent to the system. This type of credential only validates that the information itself is authentic. It does not confirm that the person presenting the credential is the person authorized to possess it, or that the credential itself is genuine.

Contact smart card technology defined by ISO/IEC 7816 and contactless smart card technology defined by ISO/IEC 14443 and ISO/IEC 15693 have both read/write and data storage capabilities. Credentials that use these technologies are intelligent devices. They can store privileges, authorizations, and attendance records. They can store PINs and biometric templates, offering two- or three-factor authentication capability. The credential is no longer just a unique number holder, but is a secure, portable data carrier as well.

The Door Reader

The door reader can have one or more interfaces, accommodating some combination of both contact and contactless smart cards and including a PIN pad and biometric reader. How the reader responds depends on the type of credential presented and the organization's security policy.

When the reader is used with a contactless smart card, it acts as a small, low-power radio transmitter and receiver, constantly transmitting an RF field or electromagnetic field called an excite field. When a contactless card is within range of the excite field, the internal antenna on the card converts the field energy into electricity that powers the chip on the card. The chip then uses the antenna to transmit data to the reader.

When the reader is used with a contact smart card, the reader includes an opening that contains a smart card contactor. The card and the connector in the reader must make physical contact.

Readers that include a PIN pad and a biometric reader (typically a fingerprint or hand geometry reader) generally support two- and three-factor authentication, if required. For example, a facility may require only the presentation of a contactless card when the security risk is low, but require biometric data as well when the threat level increases. When the security risk is high, it may be necessary to present a contact smart card and use the biometric reader and PIN pad. These multi-factor readers can be used when it is desirable to vary required inputs by time of day, day of week, or location. Requirements for additional authentication factors would be set by the organization's security policy.

[3] 125 kHz proximity technology is commonly referred to as "prox."

When the reader has received all required data, it typically processes the information in one of two ways. Either the information is immediately sent to the control panel, or the reader analyzes the data before sending it to the control panel. Both methods are widely deployed. Each has advantages and disadvantages.

The simplest readers send data directly to the control panel. These readers do nothing to evaluate the data or determine the legitimacy of the credential. These readers are typically one-factor readers and are generic, so that they can be stocked in inventory and easily added to or swapped out of an access control system.

Readers that analyze data must be integrated into the access control system. That is, they must interpret and manipulate the data sent by the card and then transmit the data in a form that is usable by the control panel. Such a system can offer an increased level of security. The reader can determine the legitimacy of the card (and the card can determine the legitimacy of the reader), compare the biometric data or PIN entry, and manipulate the credential data so that what the reader sends to the control panel is not the same as what was read from the card. The process of authenticating the card to the reader and the reader to the card is called mutual authentication. Mutual authentication is one of the advantages of a smart card-based system.

The Control Panel

The control panel (often referred to as the controller or simply the panel) is the central communications point for the access control system. It typically supplies power to and interfaces with multiple readers at different access points. The controller connects to the electro-mechanical door lock required to physically unlock a door or to the unlocking mechanism for an entrance portal (such as a turnstile, parking gate or elevator). It can be connected to different alarms (e.g., sirens, auto-dialers, lights). And finally, the control panel is usually connected to an access control server.

Depending on the system design, the control panel may process data from the card reader and the access control server and make the final authorization decision, or it may pass the data to the access control server to make this decision. Typically, the control panel makes the decision to unlock the door and passes the transaction data to the host computer and unlocking signal to the reader. It is important for the control panel (vs. the reader) to generate the unlocking signal, since the control panel is located inside the facility or in a secure room, while the card reader is located in an insecure or open area.

Finally, the control panel stores data format information. This information identifies what portion of the data stream received from a card is used to make access control decisions. Cards and readers implemented with different technologies can exchange data in different formats. However, the control panel needs to know how to interpret and process this data. For example, if a reader sends 35 bits of data and the control panel is designed to read only 26 bits, the panel must either reject the data or truncate 9 bits. The data format controls how the panel interprets received data.

The Access Control Server
The head-end system (also referred to as the back-end system or host system) includes the access control server, software, and a database. The database contains updated information on users' access rights.

In a centralized system, the access control server receives the card data from the control panel. The software correlates the card data with data in the database, determines the person's access privileges, and indicates whether the person can be admitted. For example, if a person is allowed in a building only between 8 AM and 5 PM and it is 7:45 AM, the person is not admitted. However, if it is 8:01 AM, then the computer should respond to the control panel, indicating that the door can be unlocked.

Most systems are decentralized. In a decentralized system, the access control server periodically sends updated access control information to the control panels and allows them to operate independently, making the authorization decision for the credential presented based on data stored in the panel.

The operational characteristics for centralized or decentralized systems are determined from the specific implementing organization's access control requirements.

Access Control System Data Formats

The access control system's data format is a critical design element. Data format refers to the bit pattern that the reader transmits to the control panel. The format specifies how many bits make up the data stream and what these bits represent. For example, the first few bits might represent the facility code, the next few a unique credential ID number, the next few parity, and so on.

Many access control system vendors have developed their own formats, making every vendor's coding unique. Like the pattern of teeth on a door key, the formats are kept secret to prevent an unauthorized person or company from duplicating a card. Existing installed access control system formats must be considered when defining the requirements for implementing new physical access control system technologies.

Operational Range

One important characteristic of access control system operation is the distance from the reader at which the credential is effective (called the *operational range*). This characteristic can affect the end user's perception of how convenient it is to use the system. For systems using contact smart cards, operational range is not an issue, as the card is inserted into the reader and physical contact is made.

Operational range is determined by many factors, including both the system's design specifications and the environment in which the reader is placed. Factors that affect operational range include the antenna's shape, the number of antenna turns, the antenna material, surrounding materials, the credential's orientation to the reader, the electrical parameters of the chip, anti-collision features and the field strength of the reader. Government organizations (for example, the FCC, UL, and CE) are involved in approving

or specifying frequency ranges or power transmission limits. Operational range can be increased by strengthening the antenna (for example, by increasing the number of antenna coils, the antenna size, or the power transmitted to the antenna).

The location of the reader can affect the operational range of a contactless reader. For example, the proximity of the reader to metal can distort the excite field or even shield it from the card. So a reader mounted on a solid metal plate, next to an all-metal door or encased in a metal cage (to protect it from vandals), may have a very short operational range

The ID credential operational range for any of the contactless technologies is a critical design decision for a physical access control system. The appropriate operational range will be determined as part of the organization's overall security policy, security architecture and requirements.

Security Considerations

To mitigate against risks of unauthorized access or deliberate attacks, the security of the entire access control system must be considered. This begins with the initial card issuance process and includes the actual components of the system (such as the network, databases, software, hardware, cameras, readers, cards), system processes (e.g., guard procedures), and the protection of data within system components and during transmission. The system's design will consider what security features need to be implemented given the environment of the system and the actual likelihood of an attack.

Card Security
Smart cards can help to deter counterfeiting, thwart tampering with an ID card and prevent usage of an unauthorized card. Smart cards include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks, including: voltage, frequency, light and temperature sensors; clock filters; scrambled memory; constant power sources; and chip designs to resist analysis by visual inspection, micro probing or chip manipulation. Where smart ID cards will be used for manual identity verification, security features can be added to a smart card body, such as unique fonts, ink color and multicolor arrangements, micro printing, high quality ultraviolet ink on the front and rear, ghost imaging (secondary photograph of the holder in an alternative location on the card), and multiple-layered holograms, including three-dimensional images.[4]

When properly designed and implemented, smart cards are almost impossible to duplicate or forge, and data in the chip cannot be modified without proper authorization (e.g., with passwords, biometric authentication, or cryptographic access keys). As long as system implementations have an effective security policy and incorporate the necessary security services provided by smart cards, organizations and ID holders can have a high degree of confidence in the integrity of the ID information and its secure, authorized use.

Data Protection
One of the most compelling arguments for the use of smart card-based systems for physical access control is the capability to use data scrambling

[4] State-wide Grand Jury Report: Identity Theft in Florida.

or cryptography to protect information both on the chip and during transmission. The security and reliability of information required to identify individuals and their rights and privileges is key to the success of a physical access control system.

Smart cards support symmetric cryptographic algorithms[5], which insure substantial protection and excellent processing times. Symmetric key cryptography is widely used for physical access control and uses the same key for encryption and decryption, making it extremely fast and reliable. When an access control system includes logical access and PKI privileges and when processing time isn't an issue, asymmetric cryptographic algorithms can be used.[6] Multiple keys can be stored on a single chip to address the security requirements for using multiple applications, thus providing better security for the growing complexity of today's systems.

Card and Data Authentication

A secure physical access system must have the unbiased assurance that both the ID card as presented to the reader and the data it contains are authentic. In some cases, it is important to verify that the reader is authentic as well (as determined by the card) to prevent counterfeit terminals being used to extract data.

Separate from the use of a PIN and/or biometric which unlocks the card or authenticates the person, smart cards have the unique capability to offer internal chip-based authentication features that use symmetric or asymmetric cryptographic mechanisms to offer highly reliable solutions to prove the card and data are genuine. For secure card authentication, smart cards are uniquely able to use active cryptographic techniques to respond to a challenge from the reader to prove that the card possesses a secret that can authenticate that the card is valid.

Card–Card Reader Communications

As with any process involving electronic signals, the data transmitted among components can be monitored. This possibility must be considered in the system security design in terms of the environment (for example, is the area under observation or could someone physically insert another device or place a monitoring device within signal range) and the actual likelihood of such an attack or effort.

Depending on the environment and risk profile, an organization may be concerned that the data sent from a contact or contactless ID card to a card reader can be monitored, allowing an illegal entrance to be effected if a rogue card or device can duplicate the data. Smart cards support industry-standard encryption and security techniques that both secure communication between the card and the reader and enable card and reader authentication methods.

[5] The most common symmetric key algorithms currently used are DES (Data Encryption Standard), Triple DES (either in two- or three-factor format), IDEA (International Data Encryption Standard), AES (Advanced Encryption Standard) and MIFARE™.

[6] The most common asymmetric cryptographic algorithms are RSA, ECC (Elliptic Curve Cryptography), and DSA (Digital Signature Algorithm).

The security keys used for both encryption and authentication are kept in secure tokens (smart card modules) on both the card and the reader and are highly resistant to attack.

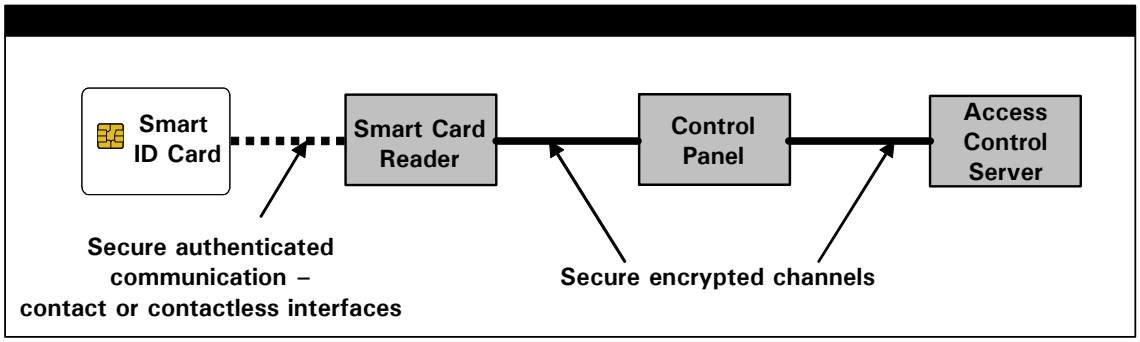
Card Reader–Control Panel Communications
In an access point location that is not observed or that doesn't have physically secure wiring, organizations may be concerned that an intruder could remove a card reader from its mounting and read the data stream sent to the control panel or place a personal computer or other device on these wires and mimic the insertion of a valid card to gain authorization. Most card readers currently transmit data to the control panel using one of two formats: Wiegand or magnetic stripe. Wiegand format uses two signal lines: D0, for transmitting "zero" data pulses; and D1, for transmitting "one" data pulses. The magnetic stripe format uses two signal lines – one for data and one for clock. These data strings are not considered secure.

Providing a secure channel from the card to the reader and from the reader to the control panel overcomes this potential security threat. Providing secure channels neutralizes the most serious threats because the reader and the card are the two elements that are exposed and physically available to an attacker.

The communication channel from the reader to the control panel can be secured in a way similar to that used to secure the channel between the card and the reader. The data exchanged between the two devices can be encrypted for maximum security and the reader and panel can be authenticated during the transaction.

Because the connection between the control panel and the access control system is internal to a building or located in a secure room, it is generally not as susceptible to attack. If desired, however, this connection can be secured using the techniques described in this section so that the entire system has an end-to-end secure data channel. Figure 2 illustrates an example of how smart card-based physical access control systems can provide end-to-end security.

Figure 2: Example of End-to-End Security in a Smart Card-Based Physical Access System

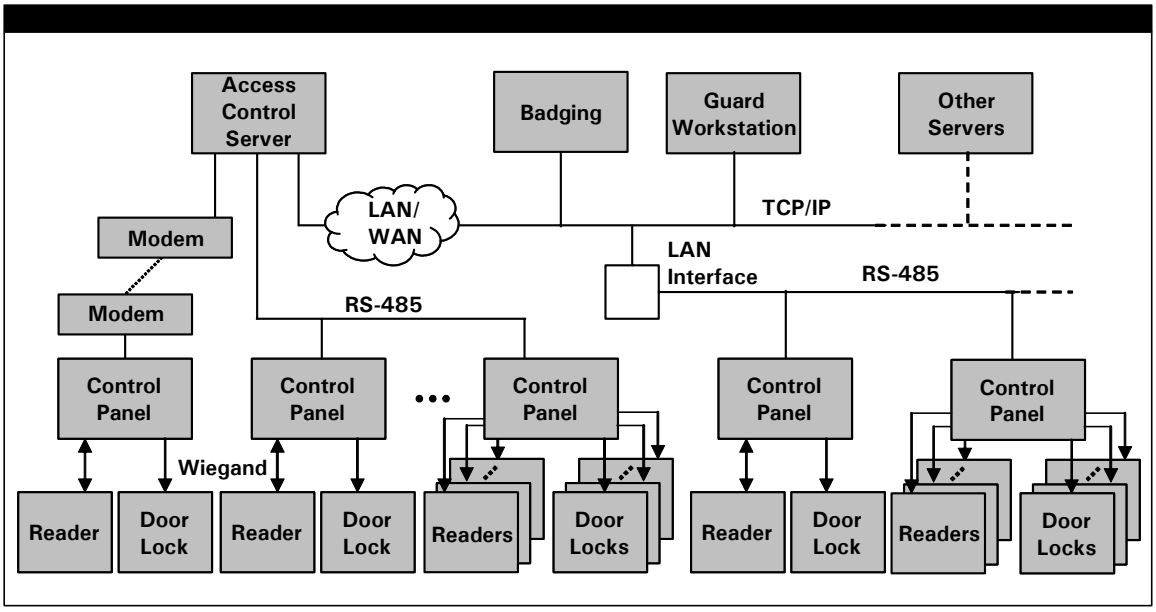


Implications of Recent Trends in System Architecture

Physical access control systems traditionally have been controlled by the corporate security department. However, with the advent of network-centric systems based on Internet technology and TCP/IP, access control systems have evolved into networked systems that combine many functions and involve multiple departments. Modern systems can include not only access control functions, but also corporate functions such as credential management and personnel databases. Nor have networked access control systems reached their functionality limits: it is easy to conceive of the card reader acting as a time clock, thus extending the system into the HR and payroll departments (Figure 3), or an ID card that includes a payment application for the local transit system.

This new multi-application, networked architecture requires the involvement and cooperation of the security, IT, HR, and other departments in the implementation of a corporate physical access control system.

Figure 3: Example of Networked Physical Access Control System



The Smart ID Card: The Role of Smart Cards in Secure Physical Access Systems

Originally, the employee badge was used as a visual identity credential. Access into buildings and doors was granted when a guard recognized the cardholder's badge. Technologies for automating access control (such as magnetic stripe, bar codes and proximity chips) were developed to decrease operating costs, improve security, and increase convenience.

While these technologies reduce operating costs and increase convenience, they do not guarantee that the badge holder is in fact the person authorized to have the badge. Older ID technologies provide minimal or no security for computer networks. The requirement for a single secure credential for logical and physical access and for protection of an individual's private information have led to the emergence of the smart ID card: an ID credential in which contact and/or contactless smart card technologies are integrated into the corporate ID to allow access systems to be implemented with additional levels of security – authentication, authorization, and non-repudiation.

The smart ID card grants a person (or device) secure, authenticated access to both physical and virtual resources. The badge can authorize access to buildings, computer networks, data files or the user's personal computer. In addition, these same cards can now include applications that allow access to mass transit systems, payment accounts, and other secured data. The one common requirement for all of these applications is authenticated user identification.

Many of the people involved in the purchase, implementation, and use of the smart ID card – from the chief executive officer (CEO) to (most importantly) the employee – are realizing the card's benefits. Almost every security magazine includes at least one article, if not a cover story, on the convergence of physical and logical access. Such articles describe security advantages, ROI, convenience, and implementation considerations.

Benefits of the Smart ID Card

The choice of an access credential must address the concerns of a variety of functional areas in an organization. Executive management needs to secure both physical and network access. With lower operating budgets, CEOs and chief financial officers (CFOs) are demanding a solid business case and the most cost-effective solutions. The chief security officer (CSO) and chief information officer (CIO) need to be notified of security breaches quickly, identify and locate the perpetrator, and gather forensic evidence that can hold up in court. HR wants new employees to hit the ground running, to increase efficiency and profitability. Government legislation demands that a person's privacy be respected. And last but not least, employees need an ID credential that is easy and convenient to use. Otherwise, either employees will find ways to circumvent security or the costs of employee credentialing will increase so significantly that the company will abandon the system.

Smart ID cards are a cost-effective and flexible solution that addresses requirements throughout the organization. A single smart ID card can incorporate multiple technologies, accommodating both new and legacy access control systems as part of an overall migration plan to the new access control technology. Badges for employees can support a range of

security profiles depending on the level of access required by the employee. For example, some badges may provide only limited facility and network access while other badges provide special access to restricted areas and use contactless or contact smart card chips to support: biometric templates that authenticate the user to the card; secure challenge-response algorithms that authenticate the card and reader to each other; and a key management/secure protocol that changes every time the badge is presented to a reader to prevent card duplication and protect information privacy.

New software and system integration specifications and products help to identify and analyze security breaches. Linking the physical access and IT databases provides the potential for suspicious activities to be identified immediately. For example, if a computer is accessed by an employee who has left the building, the IT department can be notified immediately and investigate the activity. Similarly, security can be notified if a computer in a restricted area is accessed by an employee who is not authorized to be in that area. Joint communication between the physical and logical access systems enables companies to protect confidential data and identify security issues.

Access control systems must address employer and employee needs and meet legal requirements. Smart ID cards are available that use the latest security protocols and anti-probing prevention techniques. An employee's information is consequently only available to parties to whom the employer has authorized access. An organization may want to use a single process to manage an employee's authorizations, accesses, and privileges. Linking the HR, IT, and physical access databases means that an employee can make one trip to one department to receive a badge containing all required information. The HR database may indicate what access privileges need to be assigned. The IT software can check the HR database and assign the required passwords and certificates. A biometric fingerprint and a digital photo can be taken. With this information, a blank card can then be inserted into the badge printer, all required information can be downloaded onto the card, and the card can be printed. The employee receives the badge within minutes and starts working immediately.

Smart ID cards are convenient and easy to use. Employees have only one badge to maintain, thus reducing the odds of a badge being lost, forgotten, or damaged. Employees need not fumble for the correct badge or feel that they are carrying around a deck of cards.

Conclusion

Governments, corporations and universities are finding that a smart ID card can meet their needs for both physical and logical access applications. A smart card-based system provides benefits throughout an organization, improving security and user convenience, while lowering overall management and administration costs. Smart card technology provides a flexible, cost-effective platform not only for physical access control, but also for new applications and processes that can benefit the entire organization.

Key Considerations for Secure Physical Access ID System Implementation

Implementation of a secure smart card-based physical access ID system requires consideration of certain key issues, starting with the careful consideration and analysis of the operational requirements.

Candidate Smart Card Technologies

When considering the implementation of a new secure physical access system, there are two solutions to the problem of how a physical security application reads a credential: contact and contactless. Whether to adopt contact or contactless smart card technology depends on an organization's requirements.

Contactless Smart Card Technology
Contactless smart card technology is best suited for physical access through high-traffic portals or doors and is the superior choice for use in areas where the physical environment is hostile or in areas that are exposed to weather. (Door access readers that must stand up to wind, dust, rain, snow, ice, and the occasional piece of gum, paper, and cigarette ashes must be protected.)

Two contactless smart card standards, ISO/IEC 14443 and ISO/IEC 15693, are good candidates for use in physical access control applications. New access control system implementations consider these contactless smart card standards to satisfy application requirements for higher security (e.g., biometric or other advanced authentication techniques), to accommodate multiple applications on a single card (e.g., physical access, logical access, payment transactions), and to protect the privacy of cardholder information.

ISO/IEC 14443 is a 13.56 MHz contactless technology with an operational range of up to about 4 inches (10 centimeters). ISO/IEC 14443 was originally designed for electronic ticketing and electronic cash applications. For these applications, short operational ranges and fast transaction speeds are critical. The same market requirements led ISO/IEC 14443 to be adopted for transit, off-line purchase, and vending transactions. Since applications using ISO/IEC 14443 often require a stored value on the card, new product development focused on security, with this technology now offering secure cores and sophisticated encryption schemes supported by various crypto co-processors.

ISO/IEC 14443 products are now starting to move into the physical access control market. Physical access credentials conforming to ISO/IEC 14443 offer solutions ranging from low-cost memory cards to highly secure microprocessor cards. Microprocessor cards offer levels of interoperability and security identical to the levels offered by contact smart card solutions. Because ISO/IEC 14443 cards can transfer large blocks of data very quickly, many of the biometrically enabled physical access locks available today are used with ISO/IEC 14443 cards. Several products now support data rates up to 848 kilobits/second, and an amendment to modify the standard has been submitted to the standards organizations to include these higher data rates.

ISO/IEC 15693 is a 13.56 MHz passive RF technology designed to operate at ranges of up to 3 feet (1 meter) while still meeting FCC power output limits

in the United States. The specification can be used for facility access control in buildings where read ranges may be set to 4 to 6 inches (10 to 15 centimeters) for building doors. ISO/IEC 15693 is also ideal for parking lots where cards and readers can be set to operate at higher ranges, making it unnecessary for a driver to extend an arm out of the car window.

ISO/IEC 15693 technology was developed to operate at longer read/write ranges. Initial applications using this technology included asset tracking and tagging, which require longer operational ranges and transmission of larger blocks of data. Because of this technology's capabilities, it became one of the preferred technologies for physical access. Longer operational ranges support capabilities users expect when they approach a door. The read/write storage of biometric templates, data and personal information is also leading to the migration from 125 kHz to contactless smart cards like ISO/IEC 15693.

ISO/IEC 14443 and ISO/IEC 15693 technologies have evolved with their own features and specifications. The key differentiators between the technologies are their operational ranges, speed (data transfer rates), and the extent and maturity of features and applications that use the technologies. Figure 4 summarizes the key specifications and features that are generally available for products supporting the two contactless smart card standards as of this white paper's publication.[7]

Figure 4: Key Contactless Smart Card Specifications and Features

Features	ISO/IEC 14443	ISO/IEC 15693
Standards	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 15693 ISO/IEC 7810
Frequency	13.56 MHz	13.56 MHz
Operational range (ISO)[8]	Up to 10 centimeters (~3-4 inches)	Up to 1 meter (~3.3 feet)
Chip types supported	Memory Wired logic Microcontroller	Memory Wired logic
Encryption and authentication functions[9]	MIFARE, DES/3DES, AES, RSA[10], ECC	Supplier specific, DES/3DES
Memory capacity range	64 to 64K bytes	256 and 2K bytes
Read/write ability	Read/write	Read/write
Data transfer rate (Kb/sec)	Up to 106 (ISO) Up to 848 (available)	Up to 26.6
Anti-collision	Yes	Yes
Card-to-reader authentication	Challenge/Response	Challenge/Response
Hybrid card capability	Yes	Yes
Contact interface support	Yes	No

[7] For additional information about contactless technologies, see "Contactless Technologies for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance white paper, October 2002.

[8] Distances specified by the ISO/IEC standards. The physical access implementation would set a specific operational range, typically up to 15 centimeters (6 inches).

[9] The ISO/IEC standards do not specify security functions.

[10] RSA-based encryption and authentication may not be available on all cards due to power consumption, execution time or key length constraints.

Contact Smart Card Technologies
Contact smart cards complying with the ISO/IEC 7816 standard are currently used for a wide variety of applications, including physical and logical access.

Contact smart cards are typically used for lower volume entry where speed of entry is not a primary concern, such as internal areas or high security areas where the use of multiple factors mitigates the advantage contactless cards offer for more rapid access. Contact smart cards are typically not used for physical access systems that involve a high volume of users and thousands of accesses per day, that require weather or vandal resistance, or that need highly convenient user access. However, contact smart card technology is more mature and does offer advanced processing capabilities that currently are not available with contactless technologies (for example, more advanced processors, higher memory capacity, advanced operating systems). Because of this, organizations that need these features may require a contact smart card approach.

The choice of which smart card technology is appropriate for a new secure physical access system should be driven by the organization's short-term and long-term needs. By defining both immediate and future requirements for the system, organizations can select the technologies that best meets overall implementation goals.

User Interface Requirements and Issues

Throughput and ease of use are key considerations in a physical security system. At a large facility, many thousands of employees may need to obtain access in a short time. Contactless technology has definite throughput advantages over contact technology or visual inspection of badges. However, certain trade-offs must be considered.

Ease of Use vs. Performance and Security
Any decision regarding an access control system and the choice of identification credential must balance cardholder ease of use with the performance and security of the system and the ID. Careful evaluation of these, and other, organizational requirements is the first step in the selection of a contact or contactless technology

The contactless environment has obvious advantages in terms of speed and ease of use. Issues arising from the requirement to align a card to a reader or insert a card into a reader are eliminated, so throughput increases (unless there is a requirement for multi-factor authentication such as the use of a PIN or biometric). However, in some cases a contact environment may be regarded as a more secure system if there are concerns about the RF signals from contactless cards being compromised (since the physical connection between the card and readers mitigates potential compromise of the wireless signals). Using challenge-response and other cryptographic techniques in a contactless smart card implementation helps to minimize this risk.

The operational range of the contactless technologies is a key consideration for ease of use. Longer operational ranges may be the preferred solution where access point throughput and convenience to the user are seen as major concerns, or where hands-free access is required. A shorter operational range may be preferred when other authentication factors are required.

Any implementation decision must take compatibility with overall physical security policies and procedures into account.

Impact of the Americans with Disabilities Act
Public facilities in the United States are currently required to comply with regulations imposed by the Americans with Disabilities Act. This requirement may influence the selection of an appropriate physical security technology, since organizations must consider issues of manual dexterity and other physical limitations. For users who may be confined to wheelchairs or otherwise need assistance to move around, the requirement to orient a card into a reader may be a concern. Moreover, there may be issues with presenting a card in close proximity to a reader. Readers may need to be installed lower to the ground for wheelchair access. A longer operational range provides advantages for users with disabilities.

System-Level Considerations

The choice of a system design and security architecture must be determined by looking at performance and user interface requirements as well as at requirements for integration with other security and non-security systems (such as HR and building controls). In addition, the functionality of the various systems components (credential, reader, panel, access control server, database) must be examined to ensure that the system is designed with the desired security, flexibility and scalability.

Centralized vs. Distributed Systems
One primary system design consideration is whether the system should be centralized or distributed. This decision determines where much of the functionality of the system lies. Decisions must be made such as where PINs or biometric templates are stored and what level of encryption is included on a credential. Central storage vs. on-card storage has different implications for the vulnerability of data to different types of threats and for the protection of private information.

Open vs. Proprietary Systems
Another factor in the development of a secure physical access system is the degree to which integration with other security systems is desirable. (The next section discusses interoperability in more detail.) These other systems can include intrusion detection devices, surveillance cameras, video storage, and building controls. When interoperable solutions are required, the system should be designed to incorporate an open architecture and open standard application programming interfaces (APIs) to the greatest degree possible.

Indeed, the best approach to defining the requirements for a secure physical access system is to take an enterprise-wide view of security. By making decisions on individual security solutions and technologies while fitting them into a holistic enterprise-wide security plan, one can make decisions that pay long-term dividends and eliminate “stop gap” measures that result from implementing stand-alone, closed systems.

The technology to be used must be chosen carefully. Choosing a system based on an open architecture using open APIs has certain advantages, such as easier integration with other systems, procurement flexibility, easier expansion, and scalability. In the final analysis, proprietary or closed

systems may have a cost or implementation timing advantage in the short term, but in the long term, sacrifice flexibility, scalability and integration.

Interoperability
Interoperability is a key element in the design and implementation of a physical access control solution. What "interoperability" means is often understood differently by various businesses and organizations. However, some important points to consider are the following:

- How do new technologies interoperate with legacy physical or logical access systems?
- How do available contactless products from multiple vendors interoperate with each other?
- How do physical and logical access systems affect an enterprise's infrastructure and other applications?

Interoperability must be considered in the context of the various technology choices available for physical access control solutions.

125 kHz proximity technology is widely used and will typically be the legacy system that is being upgraded or that must be integrated with a new system. One major issue with 125 kHz proximity systems is that they are not bound to any official standard, but are rather proprietary vendor solutions or, at best, subject to *de facto* standards. This issue is of particular importance when an organization is implementing or integrating a newer smart card technology. It may (for example) be necessary to plan for the implementation of multiple contactless technologies until the migration of the enterprise infrastructure to the newer contactless smart card technology is complete.

Smart card standards – ISO/IEC 7816, ISO/IEC 14443 and ISO/IEC 15693 – specify how components interact to a certain level, with different standards supporting interoperable functions at different levels. The standards do not include all of the commands or security features necessary to support a full system implementation. Smart cards that include microprocessors provide more flexibility for implementing interoperable protocols. Plus, the introduction of the "general purpose" card operating system creates a generic platform that can be used by several applications.

Card Solution vs. Reader Solution. Simply requiring that cards and readers conform to a single ISO/IEC standard is not enough to ensure interoperability between systems and devices from different manufacturers, application providers or integrators. Interoperability at some level can be accomplished by using an interoperable reader or an interoperable card. Each approach incurs different costs and has different advantages and disadvantages.

Many reader manufacturers are now offering readers that can read and write cards that meet both the ISO/IEC 14443 and ISO/IEC 15693 standards. Other products are available that can communicate with both ISO/IEC 14443- and ISO/IEC 15693-compliant cards using a single reader chip.

When selecting a contact or contactless smart card technology, system designers should review at what level interoperability is supported and how products accommodate non-standard functions.

To resolve the issue of the lack of interoperable security and application standards, user organizations may collaborate to develop industry-focused specifications for interoperability. For example:

- The **EMV specification** was developed by the financial industry for contact smart cards used with credit and debit payment applications.
- The **Government Smart Card Interoperability Specification** (GSC-IS) provides solutions to a number of interoperability issues associated with contact smart card technology implementation. It allows the application programmer to develop client applications without having an intimate knowledge of card edge interfaces. The specification was defined to provide the ability to develop secure identification smart cards that can operate across multiple government agencies or among federal, state and local governments. An upcoming GSC-IS revision (managed by the National Institute of Standards and Technology (NIST)) will include interoperability definitions for contactless smart card technologies, providing an industry resource that can be used for contactless smart card implementations.

Life-Cycle Management

One issue critical to the implementation of a physical access system is the need to track each access card and each application on the card. One function unique to a smart card is the capability to load or modify applications after the card has been issued (so-called post issuance personalization). Because information on a smart card can be changed dynamically, it is necessary to track the life cycle of applications on a card and the life cycle of the card. Life-cycle management[11] tracks and in some cases manages all changes to smart card data, regardless of whether information on the card is a new version of an application, a new chip technology, or updated information about the cardholder.

At the simplest level, life-cycle management can be thought of as a database linked to a specific access control application. The database records information about life-cycle state transitions and data such as the following:

- The card type, such as an employee, contractor, or guest card.
- Card request and authorization information.
- Card personalization information, including:
  - The operating system version and chip data.
  - Personalization data, including visible elements such as a photo, signature, or barcode.
  - Database links.
- Application management information, including:
  - The status of privileges (issued or updated).
  - Card expiration, replacement, and reissuance information.
  - Application activation, suspension and resumption (reversible block and unblock).
  - Post issuance of applications.

[11] The following documents from Global Platform and Open Security Exchange provide a more comprehensive review of card life-cycle management issues: "A Primer to the Implementation for Smart Card Management and Related Systems," available at www.globalplatform.org; "Physical Security Bridge to IT Security," available at www.opensecurityexchange.com

Access control card inventory should be tracked and audited to protect against unauthorized card issuance. Card inventory management includes counting all cards received and disbursed to issuance centers. The card life cycle therefore begins with a record of the chip serial number provided by the card supplier. Life-cycle management subsequently tracks all additions or changes to the data stored in each individual card, and simplifies the process of card reissuance assuring that the new card has the same set of applications and application parameter values included with the initial card.

Single Application Access Cards

Single application access control cards link one application to a card. For such cards, the application and the card are managed as one life cycle. For many access control systems, administrators can control changes to the application by requiring cardholders to bring their cards to a specific location to be updated, eliminating the need to replace cards when privileges or applications change. In this case, the application manages any changes to the card and the database is updated.

Administration of the card can be automated by linking the cardholder database to the access application and applying decision rules on access privileges. In this case, an application management system assures that information is consistent among databases, providing a complete audit trail that tracks issuance, updates and expiration, or revocation.

Organizations with multiple locations can use an automated application management system to assure the integrity of application data and improve system security, ensuring (for example) that a card issued at one location is valid at all locations, or that a change in application status at one facility is immediately implemented across all locations. The level of security for controlling updates to the card data or the database is in this case controlled by the application.

Multiple Application Cards

Smart card technology provides an opportunity to include multiple applications on one card. (For examples, see the later section, *New Applications Enabled by Smart Card Systems,* on page 35.) Each application may be managed by a different group within an organization or even by an external application provider (for example, a third-party electronic purse for cafeteria use). While requiring more complex organizational coordination, implementation of multiple applications can enhance the business case supporting the adoption of smart cards. Smart card technology enables the use of Web-based tools that allow individual users to securely add, modify, or delete applications without requiring an administrator to make such changes. In these cases, life-cycle management must control and track the status of each application loaded on each card.

Managing the life cycle of an application is fundamentally different from managing the life cycle of a card. The functional area issuing the card (for example, the facilities department) can be entirely separate from the functional area managing an application (for example, IT or HR). Centralized card life-cycle management requires the issuing entity to be responsible for initial card production and for providing an interface to the other application providers for loading, personalizing, and updating applications.

Once cards are issued, making changes to data or an application can be done centrally or remotely, using secure communications. A hybrid

environment provides the greatest flexibility, combining the best elements of both central and distributed management. When the Internet is used for post-issuance personalization, adequate controls are required to verify the cardholder and assure data integrity and encryption. This requires a secure application loader that is under the control of the application provider.

When multiple applications are considered for an access card, a card life-cycle management system based on a set of business rules can manage several card types and applications. This system can provide the following functions:

- Centralized administration of card issuance, with an interface for each application for application loading and personalization.
- Centralized administration of cards and applications, applying decision or authorization rules for adding, modifying, blocking or locking and unblocking or unlocking applications, and administering roles.
- Implementation of event-based changes to an application, such as blocking privileges for a lost card or locking an application if card usage is suspicious.
- A process for addressing user-based requests to add applications and add or modify privileges and for personalizing cards securely after they are issued.
- A central audit trail of application life-cycle state transitions.
- User support and access to life-cycle state data.

Other Considerations

Key generation and key management are critical functions. The generation of key pairs and associated digital certificates must be controlled during the issuance and update processes. Security schemes must protect key sessions, beginning with the use of the card manufacturer's transport keys, during all life-cycle changes to the card. The initial data preparation process (preparing the unique data sets, scripts, and keys) remains a function of the application provider. The issuer then provides the infrastructure that enables smart ID cards to be "future-proofed," assuring that applications and new functionality can be securely implemented after the card is issued.

Costs and Benefits

It is challenging to accurately quantify the potential benefits of a security system. Security initiatives are part of an overall risk mitigation strategy and the mitigation costs must be weighed against the risks. Where possible, the system should be designed to benefit both security and operations. For example, a secure credential may increase security and throughput. In addition, if the credential is used for multiple purposes, administration costs may be reduced.

A major consideration in designing and implementing any business solution is determining who pays for the system. A physical security system can be seen as the responsibility of the security department. However, if the system is regarded as another IT system, it can alternatively be considered part of the IT network. Further, since security is an organization-wide function, there can be many system owners, including security, building management, HR, or executive management.

The ability for smart cards to support multiple applications can help to build the business case for implementing a new system. Multiple organizations or departments can implement applications and share the cost of the new smart ID card and infrastructure. Once the smart card-based access control

system infrastructure is in place, the incremental cost of adding new applications or functions is lower.

Sharing the burden of planning, designing, and paying for a physical security system allows decisions to be made that result in a flexible, scalable solution for physical security. The process must include evaluating the requirement for open architecture with the goal of achieving an integrated system that handles multiple applications.

Market Trends

Both government and industry are currently involved in implementing applications based on smart card technology. Many of these applications use the smart card for access to buildings and facilities. Applications in other vertical markets, such as financial institutions and retail, have the potential to link with a physical access card in the future. To facilitate multi-application scenarios, technology developers are introducing cards with a variety of types of contactless and contact interfaces.

Government
In the United States, the Federal government is backing the use of smart card technology for millions of Federal employee identification cards.

- The General Services Administration (GSA) has developed a specification for multi-application smart cards (GSC-IS), and several agencies are planning to use cards complying with this specification for physical access.
- The Department of State (DoS) is implementing an access control system for their facilities in Washington, D.C. DoS employees and contractors will be issued contact smart cards for physical and logical access.
- The Department of Defense (DoD) is issuing smart card credentials to millions of military personnel, civilian employees, and contractors as part of the Common Access Card (CAC) program. These cards currently provide one common platform for PKI, logical access, and identification meeting Geneva Convention requirements, and will provide physical access in the future.
- The Transportation Security Administration (TSA) is testing different technologies for physical and logical access under the Transportation Worker Identification Credential (TWIC) program. This program may result in deployment to public- and private-sector transportation workers nationwide.

Many public transit agencies that have already introduced contactless smart card technology for payment of fares are now exploring the use of the same technology for access to facilities and equipment. The Washington Metropolitan Area Transit Authority (WMATA) is using the SmarTrip™ fare card technology for employee access to WMATA offices. In addition, WMATA and the U.S. Department of Education (DoE) have demonstrated a contactless smart card for DoE employee IDs that is used both for facility access and transit fare payment. The Chicago Transit Authority has introduced contactless smart card technology for fare payment and has used proximity cards for access to facilities and equipment such as cash boxes on buses.

A revision of the GSA smart card specification that includes contactless smart card technology will be issued in the summer of 2003. Demonstrations

of contactless technology for physical access are planned by the Departments of Interior and Treasury. Contactless technology cards may be evaluated for use at ports and other transportation facilities where rapid throughput is essential.

Commercial

Commercial industries are deploying applications of smart card technologies. A number of commercial enterprises, including Sun Microsystems, Microsoft, Schlumberger, Shell, Boeing and Proctor & Gamble[12] have implemented or are planning to implement smart ID cards for logical and/or physical access.

Smart cards are being used for payment throughout the world, with American Express, JCB, MasterCard and Visa International initiatives in place to test or extend the use of smart cards for contactless payment. For example, in Orlando, Florida, MasterCard and several banks have issued thousands of contactless smart cards in the MasterCard® PayPass™ pilot. In this pilot, contactless smart cards are being used at retail stores and fast food outlets, where transaction speed and customer convenience are regarded as major benefits.

As contactless technology emerges in various industries, the potential grows for multi-application cards that could be used for identification, physical access, payment, and other purposes. Currently, several foreign governments are issuing this type of multi-application card. In some locations, such as Hong Kong, use of contactless technology for public transit fare payment is being expanded to support additional types of payment and other functions. The technology already exists that can support these programs. The challenges are to link government and private sector programs, and to resolve issues of program administration, cost sharing and privacy.

Emerging Technologies

New products are being introduced that will facilitate the use of contactless smart card technologies for physical access control. Physical access control systems are being deployed that accept ISO/IEC 14443-compliant cards that are simply tapped on a reader, ISO/IEC 15693-compliant cards with an expanded operational range or contact smart cards that are inserted into a reader.

Organizations have a number of choices for smart ID card technology, including multiple technology cards, hybrid cards and dual interface cards. To allow access to facilities by persons from different organizations, access control systems are being developed with cards and card readers that can support multiple ID technologies. For example, a contactless or contact smart card can include legacy technologies such as magnetic stripe or bar code. Multiple technology cards are available that can combine either of the ISO/IEC standard contactless technologies with 125 kHz proximity technology, enabling cards to operate in both legacy physical access systems and new ISO/IEC-compliant systems.

Dual interface cards are being introduced to incorporate both contact and contactless interfaces on a single card with one chip. Hybrid smart cards are available that include two chips – one contact and one contactless. These products allow organizations to combine contactless physical access

[12] "Building Blocks of the U.S. Smart Card Market," *Card Technology*, May 2003

applications with applications requiring a contact interface, such as logical access to computers and networks. This integration of physical and logical access can provide powerful security benefits. Organizations can link physical and logical access privileges to increase security. (For example, the requirement to use the card to leave a facility can reduce unauthorized access into employee computers and improve emergency management response in the event of a facility catastrophe.) This type of programmatic integration can reduce card issuance and administration costs and provide users with the convenience of a single access ID credential.

To provide additional authentication factors, smart cards can include multiple biometrics. The biometric templates can be stored on the card or in other components of the access control system.

New smart card-based physical access control systems can provide organizations with greater flexibility. Such systems include programmable components, allowing access privileges to be modified “on the fly” to meet changing requirements and threat conditions. In addition, TCP/IP-based components are network-ready, allowing for centralized monitoring of facilities at different locations.

Migration to a Smart Card-Based Physical Access ID System

An organization can move to a smart card-based physical access ID system for a variety of reasons – for example, to improve security, implement more efficient identification processes, reduce the number of ID cards carried, provide access to new locations or add new applications. Regardless of the reasons, implementing such a system requires consideration of whether the new system will replace older systems or whether it needs to be integrated and compatible with legacy systems. While the ideal solution may be to replace all older systems immediately, moving to a new smart card-based system may need to be accomplished incrementally – requiring a plan for making the move with the least amount of disruption and cost. Such a plan, called a *migration* plan, must consider all of the components of the physical access control system and develop a strategy that meets new requirements, while leveraging existing investment and managing the ID holder experience during the migration process.

Some key questions that should be considered in planning migration include:

- What is the desired timing to replace legacy systems? How many legacy systems are in place? Are different legacy systems in place at different locations? Are there new locations that must be considered?
- What access points require new readers? Do some or all access points require new functionality (e.g., biometrics or PIN pads) or is new functionality only required at selected sites? What ID technologies are required to meet security requirements at access points?
- Which employees require new ID card functionality? Is it desirable to replace all ID cards to improve security and add functionality throughout the organization or are new ID cards only required for a subset of employees?
- Will the ID system numbering scheme or data format change? How will legacy systems be modified to accommodate these changes?
- Are there new security requirements that will require replacement or upgrades of the physical access system architecture or components?

Key Migration Considerations

Some of the key migration decisions concern what new card and reader technologies are chosen and how the system handles legacy data formats.

Multi-Technology Cards

ID cards may be composed of many different elements, each specific to a particular circumstance, such as:

- Printed cardholder photo
- Printed cardholder name
- Barcode(s)
- Magnetic stripe
- Debit stripe
- Multiple contactless technologies (125 kHz, 13.56 MHz)
- Contact smart card technology
- Optical stripe
- Embossing
- Security markings[13]

[13] Security markings can be used to deter tampering and counterfeiting. Technologies such as ornamental borders, microtext, ultraviolet text, holograms,

- Signature panel
- Issuing authority logo and address

The use of *multi-technology cards* can be part of a migration strategy or the solution itself. In considering a multi-technology smart ID card, it is important to remember that combining a small number of compatible ID technologies may be a practical solution, while other combinations may be impossible or impractical to implement.

Multi-technology cards provide a potential solution as long as the legacy and new technologies can cohabitate. For example, a legacy 125 kHz proximity chip can cohabitate with a new 13.56 MHz contactless smart card chip and the technologies will not interfere with each other. Multiple technology cards supporting both 125 kHz technology and a single 13.56 MHz technology are currently available. Similarly, contact smart card technology can cohabitate with 125 kHz and 13.56 MHz contactless technologies.

Contactless technologies (125 kHz and 13.56 MHz) and contact smart card technology can cohabitate with other ID technologies such as magnetic stripes, bar codes and optical stripes. Such a multi-technology card can offer the user a single ID card credential that is compatible with installed systems, while making newer technologies available.

While it is technically possible to mix various technologies on one card, care must be taken to consider the overall impact. Multi-technology card constraints include:

- **Inclusion of multiple contactless technologies that operate at the same frequency.** In general, cards cannot include multiple contactless technologies (125 kHz or 13.56 MHz) that operate at the same frequency since they will interfere with each other.
- **Card thickness**. The ISO/IEC 7810 standard defines the maximum allowable thickness for a card. Multi-technology cards must comply with this maximum thickness specification. Otherwise, contact readers that require cards to be of a certain maximum thickness may not be able to read the card.
- **Embossing location**. If embossing is required, the chip location, antenna coil, Wiegand wire or optical data location must be taken into account so that these areas are not damaged by the embossing process. ISO/IEC standards provide solutions for these potential problems.
- **Card cost**. In theory, companies can design cards to support any combination of contactless and other ID technologies. In practice, however, the cost and complexity of such a card may limit marketplace acceptance. Complex multi-technology cards invariably cost more than the sum of their parts.
- **Card manufacturability and availability**. Non-standard multi-technology cards may be able to be produced, but there may be long lead times to engineer the card body and qualify the manufacturing processes in conformance with ISO processes. If multiple manufacturers are involved to supply the different technologies, warranty issues may be a concern.
- **Card failure rate**. Each technology has the potential to introduce possible defects (cosmetic or functional) during card manufacture,

kinegrams, multiple laser images and laser engraving are some examples. Although adding to printing costs, security markings may be required if tampering or counterfeiting is a real or perceived threat.

increasing the risk of having to scrap a card. Furthermore, the greater the number of embedded technologies on a card, the more potential the card is to have a higher failure rate after issuance. Shorter life spans impact the total cost, which includes not only the replacement cost of a card, but also the operational costs of reissuance.

The combination of a small number of compatible ID technologies into a single card is easier and can be more cost-effective than combining many technologies. While multi-technology cards may provide solutions for accommodating legacy access control systems, organizations must carefully consider the added complexity of implementing and maintaining multiple technologies.

Multi-Application Cards

Organizations may prefer to use a single technology smart card that can support both legacy and applications. A *multi-application smart card* can allow each different legacy application technology data to be stored in its own area with its own security keys. For example, a contactless smart ID card chip can communicate with a reader using 13.56 KHz but use the formats and data required by a legacy 125 kHz access control system. A single contact or contactless smart card may be highly desirable because of reduced cost and increased convenience.

Multi-Technology Readers

The use of a *multi-technology reader* is another approach to migration. Multi-technology readers can read more than one technology at the same time. The reader can be simple or complex, depending on whether the technologies can cohabitate. The physical interface and protocol from the reader to the panel is typically the same for both technologies, but the data content is not. A multi-technology reader can therefore be as simple as two separate readers in one box, each with its own output data stream; or it can be a more sophisticated reader that can read more than one technology and transmit the card data using a single interface and wires.

Physical access control systems that use multiple RF technologies operating at the same frequency can be combined cost-effectively in a single reader. For example, multiple technology readers and reader chips are currently available that support both ISO/IEC 14443 and ISO/IEC 15693.

Generally, multi-technology readers that combine technologies using different RF frequencies are not ideal solutions because of the cost of the readers and their limited availability. Additionally, since a new reader must be installed anyway, it is generally simpler to install the new technology reader and either issue new cards or use multi-technology cards that can interface with both readers. However, depending on the number of cards and readers involved, there are migration scenarios in which readers supporting a variety of technologies are practical.

Access Control System Cabling

A migration cost component that is frequently overlooked is the replacement of cabling or the requirement for new cabling. Many current access control systems use a read-only technology that requires only a few wires between the reader and panel. If new access control functions require a two-way communications protocol (e.g., RS-232, RS-485 or TCP/IP) between the reader and panel, a different type of cabling may be needed (e.g., category-5 or similar cabling). Pulling new wires throughout a building can be costly

and, in some cases, impossible without major modifications to the building itself.

Access Control Data Formats
Moving data from the old technology physical access ID card into the new chip-based card can be a key consideration, depending on how many cards are involved and whether cardholders are geographically scattered. One approach to moving data is to duplicate the data from a 125 kHz card onto a smart card. This solution is particularly attractive because smart card readers are available with the same output interface as 125 kHz readers, so that access system control panels would not need to be replaced.

New physical access systems may have new data or new data formats that are incompatible with the older legacy systems. This will require a migration strategy that issues new cards and incorporates new readers, panels, and access control server functionality that can understand the new format, but that also considers how legacy formats can be supported during migration.

Conclusion

It is critical for an organization to define the long-term objectives for a new physical access ID system and develop a careful migration strategy and plan that implements the system in a logical, convenient, timely and cost-effective way. Migrating to a newer access control technology can be economical and relatively straightforward if the move is well planned.

New Applications Enabled by Smart Card Systems

Using smart cards enables an access control system to include applications that do more than authorize physical access. By taking advantage of the smart card chip's capabilities, organizations can enhance the business case for implementing a new secure physical access control system and increase the ability of that system to handle future needs.

This section describes three applications that are often implemented along with physical access control on multi-application smart cards:

- Logical access control applications (e.g., for computer or network authentication)
- Payment applications
- Secure data storage applications

Logical Access Control Applications[14]

As the need for physical security has increased, there has been a simultaneous rise in the requirement for greater cybersecurity (i.e., secure access to IT network resources). The news is replete with examples of network security breaches, particularly on the Internet, where fraudulent transactions have been conducted and identities stolen by hackers who access databases containing personal information. A clear threat exists to the security of both corporate and government networks.

To minimize the risk of hacker attacks and security breaches, there has been an increase in the implementation of technology designed to provide secure access to network resources. Such technology is intended to help network operators control access, making it available only to those individuals to whom the network operator wishes to provide access. Network access is controlled by two processes: authentication and authorization.

Authentication is the process by which an individual proves that he or she is the person to whom a credential was originally issued by some trusted third-party organization, which originally confirmed the individual's identity. For example, if a picture ID card is issued to John Doe, then John Doe authenticates himself by demonstrating that his face matches the face in the picture. Authentication proves that a person is the individual identified by a credential.

Authorization is the process by which an authenticated individual is granted access to resources. Access rights can be granted according to an individual's status within an organization, or rights can be granted by the network operator.

Smart card technology enables a variety of mechanisms to support authentication.

PIN/Password Protection

One common scheme to achieve authentication involves storing a PIN or password on a smart card. When a user wishes to gain access to a network resource (a local PC, server, Web-based application, or an intranet/extranet

[14] Case studies illustrating the use of smart cards for logical access can be found on the Smart Card Alliance web site, www.smartcardalliance.org.

application), the user enters the PIN. The PIN entered is compared to the PIN stored on the smart card. If they match, the user is authenticated and can access the desired resource. The PIN access control service uses two-factor authentication to provide a relatively simple means of making sure that the correct person is accessing a resource.

To support the PIN access control service, software packages are available that allow a user to manage the PIN stored on the card. For example, this software (sometimes called middleware) can allow the PIN to be changed over time, disable the PIN if it is entered incorrectly a certain number of times, and unblock the PIN if it is inadvertently disabled.

PKI Support
Another methodology for enabling user authentication is to use the digital certificates that are issued as part of a PKI to provide a unique digital identifier ("digital passport") for each individual user.

These certificates and the keys from which they are derived (which are stored in the memory of the smart card chip) can then be used to perform a digital signature operation (after a registration process designed to prove the exact identity of the person being issued the certificate). The operation cryptographically binds the person who holds the smart card to the certificate. Generally, a smart card ID holder would use a PIN or biometric to "unlock" the card to perform the requested digital signature operation.

More and more certificates are being used to support authentication to computer networks where a PKI has been implemented. For example, Windows® 2000 and Windows® NT provide native support for secure logon via certificates (as issued by the Microsoft Certificate Authority). The current deployment of the DoD CAC uses separate certificates to support network logon and digital signatures for non-repudiation of transactions.

A smart card chip can store private keys securely. Private keys are one-half of the public-private key pairs that are created to provide the cryptographic functionality that enables PKI applications like digital signatures and email encryption. Moreover, some chips are designed to generate the public-private key pairs on the smart card itself. Generating the key pair on the card adds a level of security to the private key, since it never has to be imported to the card from another source. The public key is sent to the certificate authority, where the certificate is created for distribution and sent back to the smart card for secure storage.

Symmetric Key Support (One-Time Passwords)
Some organizations may not be able to justify investment in a full-scale PKI system but may still require a robust authentication process for access to network resources. Robust authentication can be accomplished by using symmetric key schemes and dynamic or static password management. In this scenario, a PIN is combined cryptographically with a shared secret key (and potentially other data such as the time or a date) to create a digital code. The code is then compared to a code generated by the network service provider in a similar fashion. If the two codes match, the user is considered to be authenticated.

A smart card is capable of securely storing a secret key that can be used to authenticate a user when the key is compared to a secret key held by the network operator. This simple one-to-one match provides a certain level of

assurance, since the user's card can only hold the secret key when it is issued by the network operator. The weakness of this scheme is that if the secret key is compromised, the user can easily be impersonated. The effectiveness of using static keys or passwords relies on the tamper-resistant nature of the smart card chip to protect the key or password from hackers. Some organizations use "key rotation" or "key versioning" schemes to make it more difficult to compromise the system.

An ancillary scheme is to generate a key or password dynamically. In this scheme, every transaction has a different key, which can then be used by both sides of the transaction to ensure security. Smart cards can support this process, using the computational power of the chip to create the dynamic key or password.

Biometric Support

Another increasingly important use of the smart card is to support biometric-based authentication.[15] The smart card stores biometric information for an individual against which the individual is authenticated in real time. Smart card chips, depending on memory size, can store virtually any type of biometric information, either as a compressed digital template (e.g., fingerprint minutiae), or as a complete digital representation of the biometric feature (a digital image).

Biometric authentication requires that the individual provide the particular unique biometric characteristic to a reading or scanning device. The device captures the biometric and compares it to the biometric stored on the smart card. If they match, the individual is considered to be authenticated.

The addition of smart card-based biometric authentication can raise security to very high levels. The smart card supports three-factor authentication, taking advantage of something the user has (the smart card credential), something the user knows (a PIN or password) and something the user is (one or more biometrics). In some cases, a biometric may be used instead of a PIN for a two-factor authentication process that provides more secure access to data on the card.

The latest physical access systems use "match on card" techniques, where the reader captures the biometric and sends it to the card. The card then compares the acquired biometric with the one that is stored in the card and tells the reader whether the biometric matched. This further improves the security of a system since the original biometric is never exposed and, as a result, cannot be captured.

Logical Access Summary

A physical access smart card can deliver robust user and ID card authentication (by using digital signatures, biometric data, and password/PIN technologies), allow for non-repudiation of transactions, and encrypt email. If these benefits are sought by an enterprise as part of its overall network security plan, they can be quantified and incorporated into the overall business case for adoption of smart card technology to support both physical and logical access.

[15] For more information about the use of biometrics with smart cards, see the Smart Card Alliance white paper, "Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems," published in May 2002.

A growing number of enterprises in both the public and private sectors is adopting smart cards to support both physical and logical access in one card. For example, Microsoft is issuing an employee badge that not only opens doors using a contactless interface, but also supports secure network logon using an application that resides on the contact chip embedded in the card.

Currently, a major obstacle to the development of the market for ID cards supporting both physical and logical access is the historical separation of physical security and network security. These two functions are generally handled by two distinctly different parts of an organization, each with a separate mission, budget and technical infrastructure. However, as the technology has become more widely available in a variety of forms (e.g., contact, contactless, USB), more enterprises are developing business cases that require the integration of these two security functions to achieve cost savings and improve enterprise-wide security.

Payment Support

A smart card that enables physical access control can support payment transactions, through either a contact or a contactless interface. One example is the SmarTrip card, a contactless smart card used by the WMATA transit system. Passengers load a fare amount onto a card, then use the card to access the subway through the entry turnstiles, which simultaneously deduct the fare amount from the amount stored on the card.

While this application of smart card technology has been pioneered in the transit environment where the combination of secure payment and fast physical access control are paramount requirements, contactless card-supported payments are beginning to appear in the general retail sector in the U.S. The MasterCard PayPass and American Express ExpressPay pilot programs both use contactless technology to effect secure credit card payment transactions.

Payments can be supported by a contact chip embedded in the same card body as the contactless chip used for physical access. Currently, contact chips can support a wide variety of payment applications, ranging from electronic purses in which monetary value can be stored to conventional credit/debit transactions. A global specification called EMV has been created so that smart cards can support chip-based credit and debit transactions just as magnetic stripe cards do today.

A smart card application that was initially designed to only support physical access control could include an additional application to support a wide variety of payment functions as well. The combination of these functions could result in a more compelling business case for the adoption of smart card technology. For example, an enterprise's bank could provide a corporate smart card to employees that would include the bank's payment application, as well as a contactless chip used for physical access to enterprise facilities. In this case, the enterprise could potentially reap financial benefits from not having to run two separate card programs, and the bank could potentially underwrite some of the cost of managing the physical access program.

A more likely scenario (and one that has already been implemented in a number of colleges and companies) is the so called "campus card." The

campus card is a multi-application smart card that can be used as an ID card (including a picture) and can be used to pay for food and vending machines, open dormitory doors, check out books from the library, and pay for telephone calls. Generally, these cards employ a variety of technologies such as magnetic stripe, bar code, and smart card chip to support a wide range of functional applications. Most implementations support physical access control in combination with payment applications and a variety of other applications, all of which add value to the card.

Secure Data Storage

When the ability of smart card technology to provide secure and portable data storage is added to the computational capability of the chip, the end result is a portable, distributed computing device that can support a wide variety of applications securely. The only technical constraints are the physical size of the chip and the amount of available memory.

For this reason, smart cards are being used in a number of innovative ways, supporting functions that involve the secure, portable storage of sensitive and not-so-sensitive information. For example, medical records can be stored on a smart card in such a manner that only the cardholder or the cardholder's doctor can access the records. Record access is typically protected by some kind of access control logic, such as a PIN.

Similarly, the DoD CAC being issued to military personnel includes several secure storage applications that store personal information about each cardholder. The CAC can potentially store information related to medical history or other data relevant to the person's mission.

Contactless cards used for physical access systems can securely store information that tracks card usage. For example, a contactless card can be used to record when the cardholder enters a particular building (i.e., door location, time, date) for retrieval and auditing. This function can be managed by the card or at a central server, depending on the enterprise's requirements and infrastructure.

Summary

The business case in support of adopting smart cards for physical access control can be enhanced dramatically by identifying additional features and functions supported by a smart card platform. The additional functionality can use the contactless interface that supports physical access, an additional contactless chip and interface dedicated to a different application, or an additional contact chip included in the smart card body.

Any development of a smart card program should therefore include an analysis of other functions that can leverage the smart card investment. Through this process, an enterprise may uncover additional benefits of migrating to a smart card technology that could result in overall savings to the enterprise while enhancing user convenience and simplifying business processes.

Conclusion

Significant activities are underway in both government and industry to implement new access control systems that verify a person's identity and privileges before granting the person physical access (to a building or place) or logical access (to information or other online resources). Key requirements for these systems include more secure access control, improved user convenience, simpler identity verification processes, and lower overall management and administration costs.

Many Federal government agencies are implementing smart card-based physical and logical access control systems, with efforts aimed at the implementation of standards-based technology. As part of this effort, cross-agency government initiatives managed by the GSA and NIST have driven the definition of specifications for interoperability among government implementations. Commercial enterprises, such as Sun and Microsoft, are now implementing smart card-based access control systems to manage global employee access to corporate resources.

Designing a secure physical access system includes considerations beyond the choice of credential and reader. Appropriate system design requires a full definition of system requirements, including required functionality and security policy, and must take into account factors such as cost, requirements to integrate with and migrate from legacy systems, and the effect of implementation on the users and the organization.

Both contactless and contact smart card technologies are being used in access control systems. Smart card technology delivers many benefits to an access control system, including:

- High speed of access and reduced maintenance costs for contactless physical access control.
- Robust security, supporting multi-factor authentication and a variety of authentication and encryption techniques.
- Flexibility to incorporate multiple applications and to support multiple technology cards and readers.
- Established standards-based solutions, providing a selection of interoperable components and availability of cards and readers from multiple vendors.

The convergence of government and commercial needs and the availability of secure, standards-based smart card solutions are driving the implementation of smart card-based access control systems. Smart card technology enables access control systems to implement more secure identity verification for both physical and logical access and provides a technology platform for adding new applications that further enhance user convenience and simplify business processes.

For more information about smart cards and the role that they play in secure identification and other applications, please visit the Smart Card Alliance web site at www.smartcardalliance.org or contact the Smart Card Alliance directly at 1-800-556-6828.

References and Resources

"Access Control Technologies for the Common Access Card," a study by the Security Equipment Integration Working Group (SEIWG), April 2002

"Amex Opts for Biometric RFID Card," *RFID Journal*, February 17, 2003

"Building Blocks of the U.S. Smart Card Market," *Card Technology*, May 2003

"California Independent System Operators (CalISO) secures access to electric power grid control with smart cards and PKI," Smart Card Alliance case study

"Contactless Smart Card Technology for Physical Access Control," Avisian, Inc. report, April 1, 2002

"Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance white paper, October, 2002

"Department of Defense to issue 13 million Common Access Cards," Smart Card Alliance case study

"Dutch bank deploys 33,000 smart cards to authenticate internal users and secure online transactions," Smart Card Alliance case study

"Federal Deposit Insurance Corporation deploys smart cards and PKI to internal staff and field agents," Smart Card Alliance case study

"Microsoft employees to use smart card access controls," Paul Roberts, *IDG News Service/Boston Bureau*, www.idg.net, September 23, 2002

"Navy's DENCAS system centralizes dental records and secures access with smart cards and PKI," Smart Card Alliance case study

"A Primer to the Implementation for Smart Card Management and Related Systems," Global Platform, www.globalplatform.org

"Physical Security Bridge to IT Security," Open Security Exchange, www.opensecurityexchange.com

"Schlumberger/SEMA deploys 89,000 smart cards and PKI to protect corporate and customer data," Smart Card Alliance case study

"Shell Group's info security centers around 85,000 smart cards with PKI and single sign-on for smart card-enabled PKI," Smart Card Alliance case study

"Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems," Smart Card Alliance white paper, May, 2002

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, healthcare, retail and entertainment industries, as well as a number of government agencies and universities. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. For more information, visit **www.smartcardalliance.org**.

Publication Acknowledgements

This position paper was developed by the Smart Card Alliance to provide a primer on secure physical access ID systems and to discuss how these systems are migrating to smart card technology. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their comments and contributions. Participants from 28 organizations, both public and private, were involved in the development of this white paper including: ACI Worldwide, ActivCard, ASSA ABLOY ITG, Bell ID, Datacard Group, *e*ID Security, EDS, Gemplus, Hitachi America Ltd., Honeywell Access Systems (OmniTek), IBM, ISR Solutions, LaserCard Systems, MasterCard International, MGM Security Consulting, NASA, Northrop Grumman Information Technology, SC Solutions, Schlumberger, SCM Microsystems, Smart Commerce Inc., Transportation Security Administration, Unisys, U.S. Dept. of Defense, U.S. Dept. of Homeland Security, U.S. Dept. of State, U.S. Dept. of Transportation/Volpe Center, XTec Incorporated.

Special thanks go to the individuals who wrote, reviewed and/or edited this white paper.

Tim Baldridge, NASA
Dovell Bonnett, ASSA ABLOY ITG
Kirk Brafford, ActivCard
Joe Broghamer, U.S. Dept. of Homeland Security
Mike Davis, Honeywell Access Systems (OmniTek)
Mike Dinning, U.S. Dept. of Transportation/Volpe Center
Kevin Kozlowski, XTec Incorporated
Lolie Kull, U.S. Dept. of State
Philip Lee, SC Solutions
Mark McGovern, MGM Security Consulting
John McKeon, IBM
Cathy Medich, Consultant and Task Force Chair
Bob Merkert, SCM Microsystems
Dwayne Pfeiffer, Northrop Grumman Information Technology
Tate Preston, *e*ID Security
J. C. Raynon, SCM Microsystems
James Russell, MasterCard International
James Sharp, Transportation Security Administration
Randy Vanderhoof, Smart Card Alliance
Mike Vermillion, EDS
Tim Weisenberger, U.S. Dept. of Transportation/Volpe Center
Chuck Wilson, Hitachi America Ltd.
.

Copyright Notice

Trademark Notices

Appendix A: Profiles of Smart Card-Based Secure Physical Access System Implementations

This appendix summarizes the following implementations of smart card-based secure physical access systems:

- Sun Microsystems JavaBadge
- U.S. Department of State Access Control Smart Card Implementation Project
- Department of Homeland Security Identification and Credentialing Card
- Transportation Security Administration Transportation Workers Identification Card (TWIC)
- NASA Smart Card Project
- American Express New York Headquarters Physical Access Control
- Microsoft

Sun Microsystems JavaBadge

”At Sun Microsystems we created a new smart card solution for network security and physical access control called Java™ Badge," said Chris Saleh, marketing manager and program manager for JavaBadge. "We've rebadged every Sun employee in the United States and we're on track to finish all 35,000 employees worldwide in 128 countries by July 2003. We are using JavaCards manufactured by Schlumberger and readers from SCM Microsystems as well as our own embedded ones. The cards have a magnetic stripe for access control today, and MIFARE contactless chip we plan to use for access in the future. We chose a Java card because it offers the important advantage of being able to dynamically add applications in the field in real time."

One application of the card is building access, but the main reason Sun adopted smart cards was to implement logical access to the company's network using Sun Ray™ appliances, the thin clients deployed at Sun. "We have flexible offices for 25,000 employees, meaning you do not always work at the same office," said Saleh. "Sun Ray delivers IT services in a very cost effective manner, because all sessions reside on servers. The smart card is the key to the system, because it lets people bring up their own sessions and user environment."

"For example, say you want to leave for the gym. You pull out your JavaBadge from the Sun Ray appliance, which powers down to save energy. When you return from the gym you go to another office and use your card to get your session back up again. Once you insert the JavaBadge into the appliance it powers up, gets your personal session from the Sun Ray appliance and takes you right back to your personal session where you left off. Sun calls it 'Session Mobility,' which is being able to carry your user environment from one area to another," explained Saleh.

"We're entering a new phase with JavaCard to issue certificates on smart cards," said Saleh. "We'll have three applications secured by PKI: authentication/single sign on, signature, and encryption for secure email transmissions. For the highest levels of security we want dual-factor authentication – what you have and what you know. The card is what you have and the PIN is what you know in order to log in to services. Down the

road, maybe we'll use three-factor authentication with addition of biometrics."

In addition to Sun Ray appliances, there were many reasons for Sun to go to smart cards. "It's technically safer to store PIN and key information on smart card hardware tokens than on a computer hard drive in some server room. It eliminates the inefficient use and inherently weak security of passwords. We were motivated to go to smart cards for legal reasons too. To move commerce to the Internet we needed a robust system that offers non-repudiation, and Europe dictates smart cards and PKI to achieve this. Finally the smart cards enabled us to consolidate four or five credentials into one card," stated Saleh.

"The user reaction is extremely positive. The consolidation of cards, not having to remember passwords, mobility and increased sense of security are huge pluses and convenience for them. We are a big proponent of smart cards," he concluded.

Sun, Sun Microsystems and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

U.S. Department of State Access Control Smart Card Implementation Project

The U.S. Department of State is in the process of implementing smart ID cards to function as an individual's identification card throughout the government enterprise. All U.S. Department of State employees, contractors, and affiliates who work within the Department will be issued smart ID cards by the Bureau of Diplomatic Security to be used for physical access. The Bureau of Information Resource Management (IRM), which oversees logical access, will use the smart ID card as a token for PKI. The Department of State is one of the first federal agencies to use a smart card for both physical access as well as logical access and PKI.

Employees and contractors will be required to insert their smart ID card into a physical access card reader, installed at external and internal entrances, allowing authorized users access to the facilities. The access control readers are secure, programmable readers provided by XTec™ Incorporated. One beneficial feature of the intelligent readers is the ability for a security manager to securely inject authentication keys into the reader. This is currently done at the reader, but will be done from a central management point in the near future. Plus, the smart ID cards and physical access readers adhere to GSC-IS smart card interoperability specifications.

Another value of the programmable readers is the ability to communicate with the different legacy access control systems currently deployed at State Department. State Department has a three-year migration path to update or replace the current legacy access control system. The programmable reader allows the legacy MDI OS/2 system to operate with the smart cards in addition to the newly installed Software House C*Cure system. From a user perspective, it makes the conversion invisible. It gives State Department the ability to replace the old Wiegand card technology in a shorter time period.

Approximately 35,000 users will use the new card for facility access to State Department buildings. Because it is one of the first agencies to fully adopt the GSC-IS, the State Department is able to issue a variety of smart cards to

meet specific needs. There are two cards used strictly for access control: the XTec Secure Mediametric™ memory card, and Oberthur CosmopolIC™ Java card. In addition, the Datakey 330G file card is being used not only for access control, but for logical applications such as secure email, network authentication, and logon.

The majority of Department of State users (80-90%) will use their smart ID cards to secure their PKI applications, including desktop security and encryption using Entrust Entelligence™, secure email, and VPN access. Future plans include integrating biometric readers for logical access and possibly physical access into sensitive areas. The State Department plans to store other data on the smart card, including emergency medical information, HR data, and travel orders.

According to Lolie Kull, smart card implementation manager for the Department of State, "The smart card brings it all down to one simple, safe and secure denominator. One single token will simplify how we practice security as we get in the door or access our computers. At the same time, it heightens security by 100%. The solution to our security challenges is this one smart card that does it all."

Department of Homeland Security Identification and Credentialing Card

The Department of Homeland Security (DHS) is establishing a common trust model across the enterprise, formally composed of 22 separate entities. This solution addresses both physical and logical identification with a single, multi-purpose smart card-based credential. The system supports various stakeholders' access control systems by providing strong, centralized managed authentication, while retaining decentralized control of data and facilities. This initiative will facilitate physical access to DHS facilities, logical access to computer networks, and remote access communications as well as enabling electronic commerce.

This comprehensive identification and credentialing effort will be implemented using a hybrid cryptographic smart card using a Public Key Infrastructure (PKI) for logical access and a contactless chip for physical access. Authentication of the individual to the card will employ biometrics, with a PIN as a backup. DHS has rejected proprietary security infrastructures and will take advantage of the organic security features available from open standards-based applications and operating systems.

These cards will be totally interoperable within DHS as well as with the DoD smart card program and the NIST/GSA smart card specifications. The cryptographic chip will be compliant with Java 2.1 and Global Platform 2. The contactless chip will adhere to ISO/IEC 14443 Type A specifications.

Joe Broghamer, lead for Identification and Credentialing within DHS states: "DHS is leveraging policies and technologies from DoD, GSA, NIST and within DHS in order to drive standards and interoperability. The adherence to open standards will greatly reduce the interoperability problems that have plagued previous smart card/PKI efforts. DHS is in a position to positively influence industry and to become a leader in critical areas of identification and credentialing."

Joe Broghamer summarized this effort as: "Once implemented, this card will not only provide increased security for DHS systems, but equally as

important, provide an eloquent, easy to use solution for enabling e-commerce and facility access."

Transportation Security Administration Transportation Workers Identification Credential (TWIC)

The Transportation Security Administration (TSA) is mandated by federal legislation to develop an identification system for individuals requiring access to secure areas of the nation's transportation system. The Transportation Worker Identification Credential (TWIC) is intended for each worker requiring unescorted physical or logical access to secure areas of the nation's transportation modes (maritime, aviation, transit, rail, and other surface modes).

The TWIC will allow implementation of a nationwide standard for secure identification of transportation workers and access control for transportation facilities. Current estimates are that 12 to 15 million workers will require the TWIC to gain access to secure transportation sites. Each individual enrolled in the TWIC system will be positively matched to his or her credential via a reference biometric (or multiple biometrics) and will have undergone a standard background check.

The program infrastructure carefully balances security, commerce, and privacy requirements. The TWIC is to be universally recognized so that workers will not require redundant credentials or background investigations to enter multiple secured work sites and will allow facilities to better manage site access. Additionally, the credential will have the capability to be used within a facility to meet multiple levels of secure access requirements.

The TWIC system will contain sufficient technologies to be compatible with Government Smart Card Interoperability Specification while maintaining access to and within local facilities. This will enable the TWIC to leverage existing access control system investments, rather than require replacement of these systems at considerable expense. Additionally, the TWIC system will serve as the standard platform for future technology purchases at transportation facilities.

The TWIC program has received authorization to conduct two regional multi-modal pilot projects. The Los Angeles/Long Beach and Philadelphia/ Delaware River areas have been selected as the TWIC regional pilot sites based on the broad range of facility types (e.g. mode, size, infrastructure), organization structures, transportation mode inter-relationships, and policy issues in each region.

TWIC program personnel are currently conducting a five-month technology evaluation phase. The intent of this phase is to evaluate a range of potential access technologies at various facilities in each area. The test will include four to six different access technologies incorporating features such as integrated circuit chips, optical (laser) media stripes, magnetic stripes, and bar codes. At the conclusion of this phase, a seven-month prototype phase will evaluate one or two selected technologies within the full range of business processes, policies, and requirements.

NASA Smart Card Project

The National Aeronautics and Space Administration (NASA) is planning to implement a multi-application, multi-technology smart card program with a user base spread across the agency. The NASA smart card deployment will provide users with a single identification credential to use for visual identification, physical access control, and logical access control.

The first phase of the NASA smart card program includes adopting the emerging GSC-IS V2.1, which includes a specification for contactless smart cards to be used in physical access applications. The NASA smart card will include both contact and contactless proximity technologies. In the initial phase, the principal development activities will include engineering integrated solutions for current physical access control systems and integrating logical access control for multiple platforms including Windows®, Macintosh®, UNIX®, and Linux.

A distributed-issuance, centralized card management system modeled after the DoD CAC RAPIDS stations and issuance portals will be deployed in the initial phase. New identification badges that include both contact and contactless smart card technologies are planned.

NASA's primary areas of endeavor are space science, earth science, biological and physical research, human exploitation and development of space, and aerospace technology. Its core structure consists of a headquarters in Washington, DC; 10 field centers located in Maryland, Virginia, West Virginia, Florida, Ohio, Alabama, Mississippi, Texas, and California; and various facilities across the nation. The agency has a workforce of approximately 18,000 full-time civil service employees, supplemented by academic and commercial contractors.

American Express Physical Access Control for New York Headquarters[16]

With its headquarters location directly across the street from where the World Trade Center once stood and physical security taking on new importance and momentum, American Express has installed a new access-control system that relies on fingerprint templates stored on contactless smart cards for employees.

The employee's fingerprint is stored on a contactless smart card with Philips Semiconductors' MIFARE chip. When evaluating the card for access, the reader compares the actual biometric to the encrypted template stored on the card and sends a unique ID to the central security system if there is a match.

The benefits of storing the template on the card are: improved privacy since it removes the risk of having the biometric stolen from a central server[17]; easier system administration; improved ID card portability.

American Express has been working for more than a year on the project.

[16] "Amex Opts for Biometric RFID Card," *RFID Journal*, Feb. 17, 2003.
[17] New York state laws prohibit companies from storing biometrics information.

Microsoft

Microsoft has deployed a smart card employee identity system at its Redmond, Washington campus.[18] The smart card system uses ActivCard and Indala technology and manages both physical access and remote access to company networks. As of September 2002, over 25,000 cards had been issued to employees as part of the initial deployment.

Microsoft has reported that the card replaces older access card technology and will be used for physical access to buildings on the Redmond campus and for authenticating employees who are remotely accessing Microsoft networks.

[18] "Microsoft employees to use smart card access controls," Paul Roberts, *IDG News Service/Boston Bureau*, www.idg.net, September 23, 2002

Appendix B: Definition of Terms & Acronyms

Access control system format
The access control system format refers to the bit pattern that the reader transmits to the control panel. The format specifies how many bits make up the data stream and what these bits represent. For example, the first few bits might transmit the facility code, the next few the unique ID number, the next few parity, and so on.

AES
Advanced Encryption Standard.

Barium ferrite
Magnetic technology that uses barium ferrite in the composition of the ID credential to store data and make the data available to the reading device.

Biometric
Biometric technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics.

CCTV
Closed Circuit Television.

Chip
Electronic component that performs logic, processing and/or memory functions.

Cohabitation
The ability for multiple technologies to reside on the same card and not interfere with each other (i.e., a multi-technology card).

Contact smart card
A smart card that connects to the reading device through direct physical contact between the smart card chip and the smart card reader. (See ISO/IEC 7816.)

Contactless smart card
A smart card whose chip communicates with the reader using RF and does not require physical contact with the card reader.

Control panel
The access control system component that connects to all door readers, door locks and the access control server. The control panel validates the reader and accepts data. Depending on the overall system design, the control panel may next send the data to the access control server or may have enough local intelligence to determine the user's rights and make the final access authorization. The control panel can be called the controller or panel.

Credential
The general identification device (both the physical device and the data it holds). This is commonly referred to as the "ID token" in physical access control systems.

DES
Data Encryption Standard.

Door reader
The device on each door that communicates with an ID card or credential and sends data from the card to the control panel for decision on access rights.

Door strike
The electronic lock on each door that is connected to the control panel.

DSA
Digital Signature Algorithm.

Dual interface card
An ID card that has a single smart card chip with two interfaces – a contact and a contactless interface – using shared memory and chip resources.

Excite field
The RF field or electromagnetic field constantly transmitted by the contactless door reader. When a contactless card is within range of the excite field, the internal antenna on the card converts the field energy into electricity that powers the chip. The chip then uses the antenna to transmit data to the reader.

ECC
Elliptic Curve Cryptography.

EMV
Europay MasterCard Visa. Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

FCC
Federal Communications Commission.

FIPS
Federal Information Processing Standard.

GSA
General Services Administration.

GSC-IS
Government Smart Card Interoperability Specification. The GSC-IS was defined to provide the ability to develop secure identification smart cards that can operate across multiple government agencies or among federal, state and local governments and provides solutions to a number of interoperability issues associated with contact smart card technology implementation. An upcoming GSC-IS revision (managed by NIST) will include interoperability definitions for contactless smart card technologies.

Head-end system
The access control server, software and database(s) used in a physical access control system.

Hybrid card
An ID card that contains two smart card chips – both contact and contactless chips – that are not interconnected.

IDEA
International Data Encryption Standard.

IEC
International Electrotechnical Commission.

Integrated circuit
See chip.

ISO
International Organization for Standardization.

ISO/IEC 14443
ISO/IEC standard "Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards."

ISO/IEC 15693
ISO/IEC standard "Identification Cards - Contactless Integrated Circuit(s) Cards - Vicinity Cards."

ISO/IEC 7816
ISO/IEC standard for integrated circuit cards with contacts.

Logical access
Access to online resources (e.g., networks, files, computers, databases).

MCU
See microcontroller.

Microcontroller (MCU)
A highly integrated computer chip that contains all the components comprising a controller. Typically this includes a CPU, RAM, some form of ROM, I/O ports, and timers. Unlike a general purpose computer, a microcontroller is designed to operate in a restricted environment.

Migration
The planned, incremental move from an existing physical access control system to a smart card-based system.

Multi-application card
A smart card ID that runs multiple applications – for example, physical access, logical access, data storage and electronic purse – using a single card.

Multi-factor reader
A smart card reader that includes a PIN pad, biometric reader, or both to allow multi-factor authentication.

Multi-technology card
An ID card that has two or more ID technologies that are independent and that don't interact or interfere with one another. An example is a card that contains a smart card chip and a magnetic stripe.

Multi-technology reader
A card reader/writer that can accommodate more than one card technology in the same reader (e.g., both ISO/IEC 14443 and ISO/IEC 15693 contactless smart card technologies or both 13.56 MHz and 125 kHz contactless technologies).

NIST
National Institute of Standards and Technology.

Non-repudiation
The ability to ensure and have evidence that a specific action occurred in an electronic transaction (e.g., that a message originator cannot deny sending a message or that a party in a transaction cannot deny the authenticity of their signature).

Operational range
The distance from the reader at which the contactless ID credential is effective.

PC
Personal computer.

Physical access
Access to physical facilities (e.g., buildings, rooms, airports, warehouses).

PIN
Personal Identification Number. A numeric code that is associated with an ID card and that adds a second factor of authentication to the identity verification process.

PKI
Public Key Infrastructure.

RF
Radio frequency.

RFID
Radio Frequency Identification.

RSA
Refers to public/private key encryption technology that uses an algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman and that is owned and licensed by RSA Security.

Smart card
A smart card includes an embedded chip that can be either a microcontroller with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.

Smart ID card
An identification card that is a smart card.

3DES
Triple DES.

UL
Underwriters Laboratories.

USB
Universal Serial Bus.

Wiegand technology
Wiegand technology is widely used for physical access applications and includes an interface, a signal, a 26-bit format, an electromagnetic effect, and a card technology. A Wiegand strip is the implementation of Wiegand technology on an ID credential.

Wired logic
A contactless card that has an electronic circuit that is designed for a specific function (e.g., security, authentication) without an embedded MCU.