Contactless Technology for Secure Physical Access: Technology and Standards Choices

A Smart Card Alliance White Paper

October 2002

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

Executive Summary

Contactless Cards Provide Advantages for Physical Access
Contactless cards are increasingly accepted as the credential of choice for controlling physical access. They are both robust and flexible, giving security professionals the ability to reduce maintenance costs, improve employee productivity and increase security.

Contactless smart cards offer advantages to both the organization issuing the card and the cardholder. The issuing organization can support multiple applications on a single card, consolidating an appropriate mix of technologies and supporting a variety of security policies for different situations. Applications such as logical access to computer networks, electronic payment, electronic ticketing and transit can be combined with physical access to offer a multi-application and multi-technology ID credential. The issuer can also record and update appropriate privileges from a single central location. The organization as a whole incurs lower maintenance costs over the system life, due to the elimination of mechanical components and reader resistance to vandalism and harsh environmental conditions. With hybrid and dual-interface cards, issuers can also implement systems that benefit from multiple card technologies.

Three Primary Contactless Technologies Support Physical Access Control Applications
There are three primary contactless technologies considered for physical access control applications: 125 kHz, ISO/IEC 14443, and ISO/IEC 15693 technologies.

125 kHz read-only technology is used by the majority of today's RFID access control systems and is based on de facto industry standards rather than international standards. 125 kHz technology allows for a secure, uniquely coded number to be transmitted and processed by a back-end system. The back-end system then determines the rights and privileges associated with that card.

Contactless smart card technology is based on ISO/IEC 14443 and ISO/IEC 15693 standards. Cards that comply with these standards are intelligent, read/write devices capable of storing different kinds of data and operating at different ranges. Standards-based contactless smart cards can authenticate a person's identity, determine the appropriate level of access, and admit the cardholder to a facility, all from data stored on the card. These cards can include additional authentication factors (such as biometric templates or PINs) and other card technologies, including a contact smart card chip, to satisfy the requirements of legacy applications or applications for which a different technology is more appropriate.

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.

Contactless Smart Cards Offer Application Flexibility
Standards-based contactless smart cards offer organizations the flexibility to select appropriate technologies driven by business requirements, rather than implementation constraints. This allows organizations to implement and enforce a wide range of security policies by deploying a system best suited to the appli-

cation. Smart card technology – both contact and contactless – provides a flexible platform that can address both current and future needs. Hybrid and dual-interface cards provide additional flexibility to help with migration from existing systems and incorporate multiple technologies appropriate for different applications. Additionally, implementation considerations, such as the impact on the organization, cost, and the effect on the user population, are more effectively addressed.

About This White Paper

This white paper was developed by the Smart Card Alliance to describe the advantages of using contactless smart cards for physical access. The paper focuses on providing a basic tutorial of physical access system operation and an overview of the three primary contactless technologies in use today for physical access control. The paper does not attempt to fully discuss contact smart card technology or applications other than physical access. The paper provides answers to commonly asked questions about contactless technology, such as

- Why consider contactless technology for physical access?
- What types of contactless technologies are available?
- How does a physical access control system work?
- What standards apply to contactless smart cards?
- What implementation considerations are critical to selecting the appropriate technology?

Why Contactless Technology

Smart cards are rapidly gaining acceptance as a means of addressing the requirement for systems that can accurately and securely verify a person's identity and rights. Smart cards include an embedded chip (either a microcontroller with internal memory or a memory-only chip), contain the tools necessary for security applications, and are available with both contact and contactless interfaces to readers. Properly implemented, a smart card-based identity verification system provides a robust barrier to unauthorized access.

Contactless smart card technologies offer security professionals features that can enhance systems designed to control physical or logical access (i.e., access to networks or other online resources). Contactless cards differ from traditional contact smart cards by not requiring physical connectivity to the card reader. The card is simply presented in close enough proximity to the reader and uses radio frequencies (RF) to exchange information.

The use of contactless technologies is particularly attractive for secure physical access, where the ID credential and reader must work in harsh operating conditions, with a high volume of use or with a high degree of user convenience. For example, consider the use of a contactless card to control access to public transportation. The card can be presented to the reader without having to be removed from a wallet or purse. The fare is automatically deducted from the card and access is granted. Adding funds through appropriate machines at transit centers or banks then refreshes the card. The process is simple, safe, and accurate.

Types of Contactless Cards

There are three types of contactless credentials (cards or tokens):

- Memory
- Wired logic
- Microcontroller (MCU)

Memory cards use a chip or other electronic device to store authentication information. In their most secure form, memory cards store a unique serial number and include the ability to permanently lock sections of memory or allow write access only through password-protected mechanisms. Other than these basic mechanisms, memory cards employ no additional security to protect their contents. System-level methods can be used to encrypt and decrypt the information stored on the card.

Wired logic cards have a special purpose electronic circuit designed on the chip and use a fixed method to authenticate themselves to readers, verify that readers are trusted, and encrypt communications. Wired logic cards lack the ability to be modified after manufacturing or programming.

MCU cards implement authentication/encryption methods in software or firmware. Contactless smart cards with an embedded MCU have more sophisticated security capabilities, such as the ability to perform their own on-card security functions (e.g., encryption, hardware and software-based tamper resistance features to protect card contents, biometric verification and digital signatures) and interact intelligently with the card reader. Contactless MCU cards also have greater memory capability and run card operating systems (for example, JavaCard or MULTOS).

Both hybrid and dual-interface contactless cards are becoming available. On a hybrid card, multiple independent technologies share the common plastic card body but do not communicate or interact with each other. For example, one card could carry a magnetic stripe, bar code, 125 kHz technology, picture ID, contact smart card module and either ISO/IEC 14443 or ISO/IEC 15693 contactless smart card technology. The advantage of a hybrid card is that existing installed systems can be supported, while new features and functionality can also be offered through smart card technologies.

A dual-interface card includes a single chip with both contact and contactless capabilities. Contact and contactless technologies can therefore be implemented on one card, each addressing the application requirements most suited to its capabilities and sharing the same data. Hybrid and dual-interface technologies are complementary and, with thoughtful implementation, transparent to the end user.

With current technologies, security system designers can implement an architecture that includes multiple ID credential technologies. This creates a significant opportunity for more efficient credential management, improved user convenience, and easier administration of multiple security policies and procedures. Imagine the value of using a single multi-technology credential to control building or parking access and time- or project-based access to specific areas, and to conduct financial transactions at a cafeteria, bookstore, or vending machine. Through the use of the appropriate card technology, cryptography, and digital signatures, logical access control can be incorporated into networks and databases. And because the credential is a plastic card, it also supports the use of pictures, logos, visual inspection information, holograms, digital watermarks, microprinting, and other security markings to deter counterfeiting and impersonation. A single card is also more efficient for the user, simplifying coordination for changes, reducing memorization for complicated passwords or personal identification numbers (PINs), and decreasing the time for authentication.

Benefits of Contactless Smart Card Technology for Physical Access Control

Contactless smart card technology is ideal for physical access control applications. Because ID credentials and readers are typically exposed to the elements and have high usage, sealed contactless technology prevents damage when cards and readers are exposed to dirt, water, cold, and other harsh environmental conditions. With no mechanical reader heads or moving parts, maintenance costs are minimized. Finally, with read ranges that can extend to many inches, contactless technology offers the user the convenience of “hands free” access.

The key benefits of using contactless smart card technology for physical access are summarized below.

- High speed of access and high throughput
- Useable in harsh or dirty environments
- User friendly
  - Less intrusive
  - Does not require insertion of the card into the reader
  - No issues with orientation of the card
  - May be kept in wallet or purse for personal security during use
- Same high level of security as contact smart cards (e.g., digital signatures)

- Protected storage of data on the card
- Flexibility to incorporate multiple applications with different modes
  - Contactless only card
  - Dual interface contact/contactless card
  - Hybrid card that includes 125 kHz technology, 13.56 MHz technology, magnetic stripe, barcode, hologram, photo, and other card security features.
  - Dual interface contact/contactless card that includes 13.56 MHz technology, magnetic stripe, barcode, hologram, photo, and other card security features
- Reduced maintenance costs for card readers (as compared to magnetic stripe and contact card readers)
- Reduced vandalism of readers
- More durable and reliable cards (no external parts that can wear out or be contaminated)
- Well-suited to accommodate local security staffing, training and implementation
- Established international standards (ISO/IEC)

History of Contactless Technology

Contactless technology was first developed by the British during World War II as a means of identifying aircraft returning from mainland Europe. This system, the IFF (Identify: Friend or Foe) system, was the first general use of radio frequency identification (RFID). In about 1977, contactless technology developed by the U.S. government was made available to the public sector by Los Alamos National Laboratory. Shortly thereafter, experimentation began on tracking cattle using implanted RFID tags.

By the early to mid 1980's, companies started to reduce the size and cost of RF technology so that it could be embedded into employee cards for physical access. This technology grew in acceptance since it reduced operating costs (eliminating the $10-$20 cost per employee for re-keying locks and issuing new keys), improved productivity (providing easier, more convenient access for employees), and improved security (allowing access records to be kept).

By 1986, Atmel Corporation was producing RFID fish tags for tracking salmon. RFID tagging has grown into a major industry, used for animal tracking, baggage tagging, laundry identification, asset and inventory control, car immobilization and truck and cargo tracking, and access control. RFID products can operate over a wide range of frequencies. The most widely used frequency for access control today is 125 kHz.

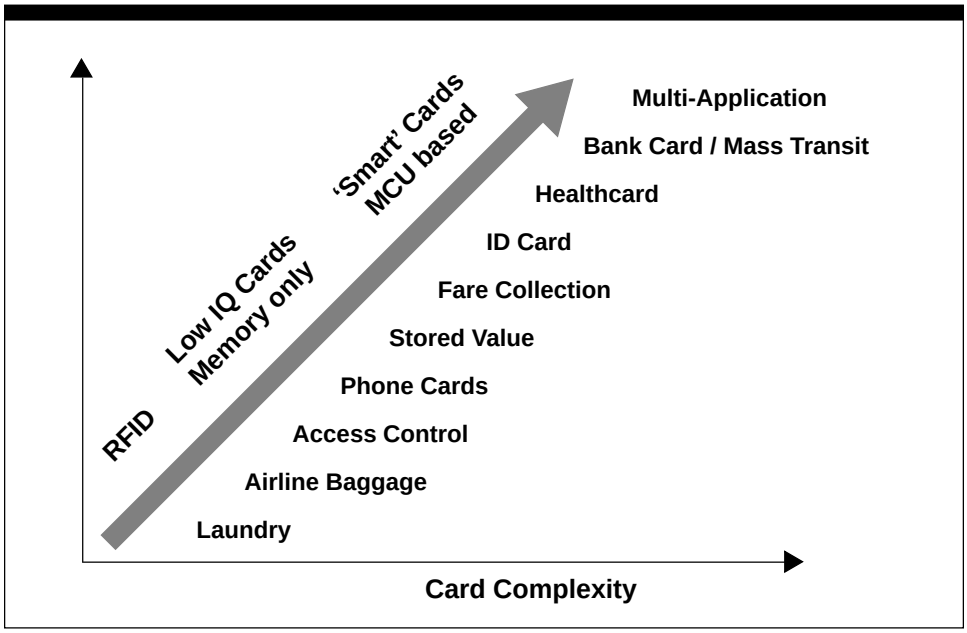
MCU-based smart card development also began in 1986, at GEC. The card initially was a two-chip solution with a custom radio frequency (RF) front end and a smart card microcontroller from Hitachi. This first contactless smart card operated at a much lower frequency (300 kHz) than current smart cards, which operate at 13.56 MHz. This card technology was the precursor to the ISO/IEC 10536 specification developed later for close-coupled cards. The card technology was introduced in a campus card for Loughborough University in the United Kingdom and issued by the Midland Bank in 1988 for a one-year trial. The trial was so successful that it was extended for an additional year. However, the initial card never became a mainstream product.

The first standards-based contactless smart card product to find market acceptance was the MIFARE® wired logic card invented by Mikron in 1994. Contactless cards using MIFARE technology are the mainstream products used for many card ticketing applications today.

The need for more secure and versatile products drove the evolution of contactless technology. The next generation card was a hybrid two-chip solution with a contactless memory chip and an MCU-based contact chip on a single card. The next step was a dual-interface chip that effectively offered a combined solution on a single chip. In early versions of the dual-interface card, access to memory in contact mode was via the MCU; access to memory in contactless mode was direct, via the RF interface. This initial approach allowed for simpler implementation of the design on a silicon chip. The MCU needed a direct supply of power to the contacts, whereas memory, which requires five- to ten-times less power, could receive enough power from the RF interface. However, because access to memory was not through the MCU, the contactless mode did not offer the same level of security as the contact mode.

Recent advances in silicon technology enable an RF interface to provide sufficient power to the MCU for all operations. The result is the availability of contactless products with a secure MCU that provides all of the features of a conventional contact smart card and options for contact, contactless, or dual interface. Figure 1 illustrates the evolution of technology that has resulted in today's multi-application MCU-based contactless smart cards. Multiple vendors now offer a range of products that support contactless applications, providing businesses with a wide variety of solutions that address their specific applications.

Figure 1: Contactless Technology Evolution
Source: FC Consulting



Physical Access Control Systems

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

- A card that is presented to a door reader,
- The reader, that responds with a signal indicating a valid card, and
- The door or gate, that is unlocked if entry is authorized.

Behind the scenes is a complex system of data, computers, and software that incorporates robust security functionality. This section describes the operation and components of a typical physical access control system to provide the context for understanding how contactless technology is used in an access control application.

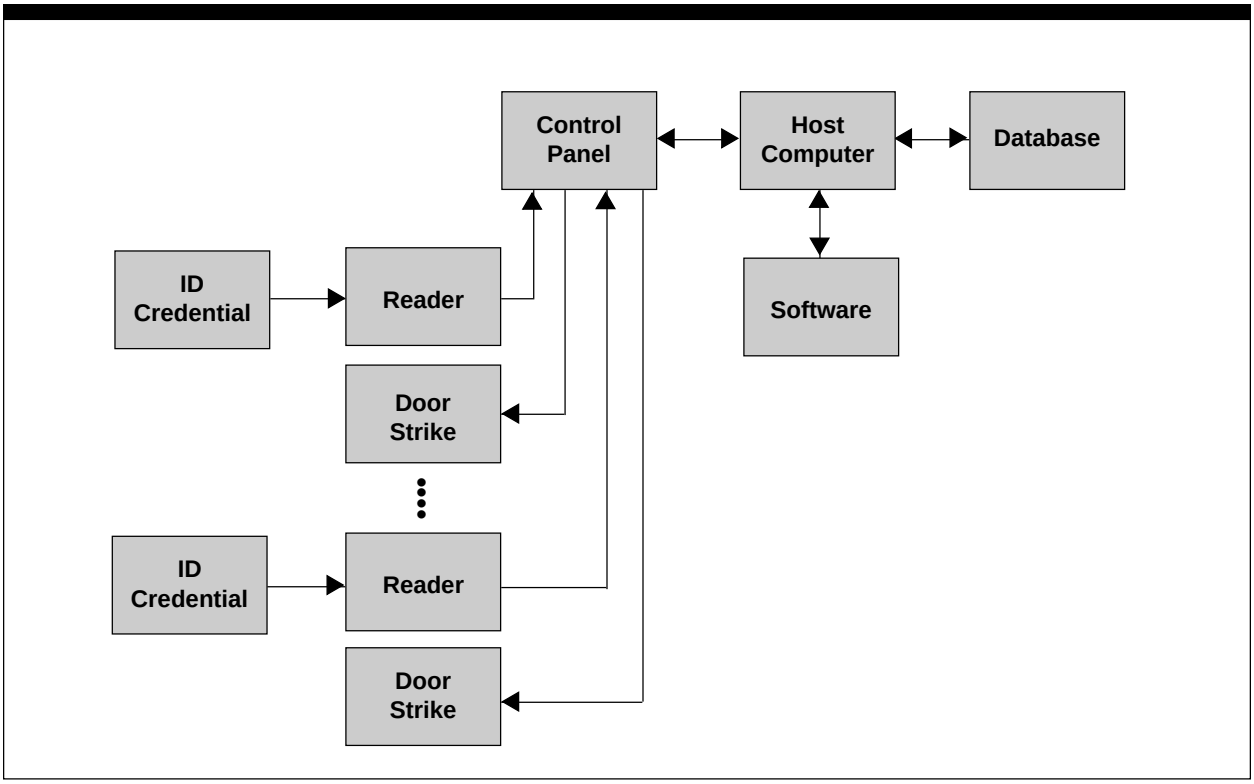
Access Control System Components

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

- ID credential
- Door reader
- Control panel
- Host computer
- Software
- Database
- Door strike

Figure 2 illustrates how these components interconnect.

Figure 2: Access Control System Schematic



Access Control Process

The access control process starts when the user presents the credential (typically an employee badge or ID card) to the reader, which is usually mounted next to a door. The reader reads data from the card, processes it, and sends it to the control panel. The control panel validates the reader and accepts the data. Depending on the overall system design, the control panel may next send the data to the host computer or may have enough local intelligence to determine the user's rights and make the final access authorization.

If the control panel sends the data to the host computer, the host computer compares the data from the card to the user's information in a database. Software determines the user's access privileges and authorization, the time, date, door entered, and any other information that a company may require to ensure security. If access is authorized, the host computer sends a signal to the control panel to unlock the door. The control panel then sends out two signals: one to the appropriate door strike, which unlocks the door, and one to the door reader, which emits an audible sound or otherwise signals the user to enter.

In a typical distributed system design, the host computer will periodically provide the control panels with data that allows their software to determine if the user is authorized for access. The control panel then provides the host system functions described above. This system has the advantage of requiring less immediate communication between the control panels and central host computer, improving overall system performance and reliability.

The response to an invalid card is defined by the company's security policy and procedures. The host computer or control panel may ignore the data and never send an unlock code to the controller or door strike. They may send a signal to have the reader emit a different sound, signaling that access was denied. They may also notify and activate other security systems (e.g., CCTV, alarms), indicating that an unauthorized card is being presented to the system.

The role each access control system component has in this process is described below.

The ID Credential

A number of different credential technologies are currently in use for access control: magnetic stripe, Wiegand strips, barium ferrite, 125 kHz technology, 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 authenticates the credential and/or user.

Some credential technologies are read-only. The data is permanently set, and when the credential is presented to a reader, the data is sent to the system. This type of credential only validates that the credential itself is authentic. It does not confirm that the person presenting the credential is the person authorized to possess the credential.

The contactless smart card technologies defined by ISO/IEC 14443 and ISO/IEC 15693 have both read/write and data storage capabilities. Credentials that use these technologies are more intelligent devices. They can store privileges,

access authorizations, and attendance records. They can also store PINs and biometric templates, offering two- or three-factor authentication capabilities. The credential is no longer just a unique number holder but is a secure, portable data carrier.

The Door Reader

The contactless door reader acts as a small, low-power radio transmitter and receiver. It constantly transmits 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. The chip then uses the antenna to transmit data to the reader.

Once the reader has received the data, it typically processes the information in one of two ways. Either the data 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.

Readers that send data directly to the controller do nothing to evaluate the data or determine the legitimacy of the credential. These readers do not manipulate the data but act simply as conduits. They are generic readers and therefore can be stocked in inventory and easily added or swapped out of an access control system.

Readers that analyze data must be integrated into the access control system. That is, they must be able to interpret and manipulate the data sent by the card and then transmit it in a form that is usable by the control panel. Such a system can offer an increased level of security. The reader can first determine the legitimacy of the card and can manipulate the data so that what the card transmits is not the same as what the reader sends up to the control panel. Because these components are interdependent, each configuration may have to be stocked in inventory.

The Control Panel

The control panel (also called the controller or simply the panel) acts as 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 strike required to physically unlock the door. It can also be connected to different alarms (e.g., siren, auto-dialers, lights). Finally, the controller is usually connected to a host computer system. Depending on the system design, the control panel may process data from the card reader and the host computer and make the final authorization decision or may pass the data to the host computer for this decision.

The controller performs one additional function. Credentials and readers are able to transmit data in different size formats. However, just because the cards and readers can transmit data in these formats does not necessarily mean that the control panel can interpret and process the data. For example, if a control panel is designed to read 26 bits of data and the reader sends 35 bits, the controller either rejects the data or truncates 9 bits of the data. Complete data format information resides on the controller, not on the card or reader, and the controller determines what data will be used from the card to make the access control decision.

The Host System

The host system includes a computer, software, and database. The database contains the updated information on users' access rights. In a centralized host system design, the computer receives card data from the control panel. The software correlates the data with data in the database and determines the person's access privileges and whether the person should be admitted. For example, if a person is only allowed in a building between 8 AM and 5 PM and it is 7:45 AM, the person is not admitted. If it is 8:01 AM, however, the computer responds to the control panel, indicating that the door can be unlocked. The controller sends a signal to the door strike to unlock the door for a few seconds. At the same time, the controller sends a signal instructing the reader to indicate that the door is open.

In most system designs, the host system will periodically send updated access control information to the control panels and allow them to operate independently in making the decision of whether the user presenting the card is authorized for access. The operational characteristics are determined from the specific implementing organization's access control requirements.

Access Control System Formats

The access control system format is a critical design element in the overall system and refers to the mathematical algorithm that specifies how data transmitted by the system is to be interpreted. The format specifies how many bits make up the data stream and which bits represent different types of information. 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.

Access control system vendors developed their own formats, making every vendor's coding unique. These formats were developed to be unique for security reasons. Like the pattern of teeth on a door key, the formats are kept secure to prevent an unauthorized person or company from duplicating a card. Existing installed access control formats must be considered when defining the requirements for the implementation of any new contactless technology.

Read Range

To the end user, one of the most important features of access control is the read range (the distance between the reader and the credential); another is the time it takes for an access transaction. Users have come to expect read ranges of at least 4 to 6 inches (10 to 15 centimeters) and in some special cases, as much as 12 inches (about 30 centimeters), for hands-free access. Longer ranges are useful for applications such as entering a parking garage, allowing the user to avoid extending the credential too far out of the car window, especially in bad weather.

Read range is determined by many factors, including both the system's design specifications and the environment in which the reader is placed. Design factors that affect read range include the antenna shape, number of antenna turns, antenna material, surrounding materials, credential orientation to the reader, electrical parameters of the chip, and field strength of the reader. Read range can be increased by strengthening the antenna (by increasing the number of antenna coils, the antenna size, or the power transmitted to the antenna).

Government organizations (for example, FCC, UL, CE) are also involved in approving or specifying frequency ranges or power transmission limits.

The location of the reader can also affect the read range. 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 read range or even no read range at all.

The ID credential read range for any of the contactless technologies is a critical design decision in any physical access control system. The most important factor in selecting an appropriate read range is the application's requirements, which are determined by the implementation of the organization's overall security policy, security architecture and requirements.

Contactless Technologies for Physical Access

There are three contactless technologies in use today that are good candidates for physical access control applications. These technologies include 125 kHz, ISO/IEC 14443, and ISO/IEC 15693 technologies.

125 kHz Technology

125 kHz read-only technology is used by the majority of today's RFID (also called proximity, or prox) access control systems. The 125 kHz technology is a passive RF technology because the RF field emitted by the reader powers the card's chip.

This technology is not based on any ISO/IEC standard but rather on de facto industry standards. Manufacturers have therefore had greater latitude to develop different products and protocols. While the absence of an international standard has led to interoperability issues between what seem to be similar technologies, it has also made available products with a wide array of features and capabilities that businesses can tailor for a specific application.

The de facto industry standard for 125 kHz technology access control systems is called Wiegand, named after John Wiegand, the inventor of the technology. As a pioneer in access control systems, Mr. Wiegand invented an interface, signal, 26-bit format, and card technology, along with some general security concepts. Wiegand-compliance typically refers to the communication protocol and interface used between readers and the other non-card components of a physical access system.

This section summarizes the key features of 125 kHz technology.

The Card

The 125 kHz technology card contains a chip and an antenna. Typically, the antenna is an air-wound copper coil including over 100 turns and is thin enough to fit into an ISO/IEC 7810 card body without any deformities that might affect printing. The chip stores data that represents a facility code, a card number, and overhead data, such as start bits, stop bits, and parity bits.

An ISO/IEC 7810-compliant card body allows for the inclusion of graphics, bar codes, a magnetic stripe, and a smart card chip. It is therefore possible to include ISO/IEC 14443 or ISO/IEC 15693 contactless smart card chips on a 125 kHz card with little or no degradation of performance. These cards offer the user a hybrid, multi-technology, single-card credential that is compatible with installed systems while also making newer technologies available.

The Door Reader

The 125 kHz technology door reader emits a constant excite field operating at 125 kHz. Different companies use different return frequencies or modulations to communicate back to the reader. Therefore, one manufacturer's cards do not necessarily work with another manufacturer's readers.

Some reader and controller manufacturers have incorporated secure authentication features into their products. For example, some card/reader systems use a password transfer protocol that requires the card to authenticate itself to the reader before the card data can be transmitted.

Readers can also incorporate keypads, providing additional security that requires the cardholder to present their card and PIN for stronger two-factor authentication. Biometric readers are also available. These readers compare a stored biometric template to the actual biometric read at the access control point, providing strong authentication of the cardholder. Readers that incorporate both a keypad and a biometric reader can also be used to provide either two- or three-factor authentication.

Conclusion

125 kHz technology is a secure and proven technology for access control applications. Because the newer contactless technologies (described below) operate at 13.56 MHz, it is possible to include both contactless technologies on a single card. These hybrid cards can also include graphics, bar codes, holograms, magnetic stripes, and contact smart card chip, providing multiple technologies on a single card.

Key Features of 125 kHz Technology

- Operating frequency: 125 kHz
- Read/write range: Up to 3.3 feet (1 meter)
- Speed: 4 Kbps
- Storage memory available: 8 to 256 bytes
- Security: Supplier specific
- Vendors: Many

ISO/IEC 14443 and ISO/IEC 15693 Technologies

The International Organization for Standards (ISO) has created standards for three contactless technologies:

- ISO/IEC 10536 close coupling cards
- ISO/IEC 14443 proximity cards
- ISO/IEC 15693 vicinity cards

ISO/IEC 10536 has not been widely deployed. In addition, advances in the ISO/IEC 14443 and ISO/IEC 15693 technologies have made the ISO/IEC 10536 contactless standard increasingly less appealing.

This section describes the two most popular contactless smart card technologies, which are based on the ISO/IEC 14443 and ISO/IEC 15693 standards. New access control system implementations are considering these newer contactless smart card technologies to satisfy application requirements for higher security (e.g., with biometric or other advanced authentication techniques), to accommodate multiple applications on a single card (e.g., physical access, network access, payment transactions), and to protect the privacy of cardholder information.

ISO/IEC 14443 and ISO/IEC 15693 technologies have evolved with their own set of features and specifications. Both solve specific market requirements and each is now expanding into application areas originally addressed by the other technology. The key differentiators between the technologies are their read ranges, speed (data transfer rates) and extent and maturity of features and applications using the technologies.

ISO/IEC 14443 and ISO/IEC 15693 technologies share the following important features and benefits:

- 13.56 MHz frequency of operation. This frequency is able to be used

throughout the world for contactless applications.

- Read/write capability to the card. This allows user information to be stored and updated on the card (for example, a PIN or biometric template) and helps eliminate the need to access a host computer or database during use.
- Ability for manufacturers to implement security features. Although neither standard specifies security, features such as DES, Triple DES and AES, are commonly available.
- Support for card-to-reader authentication.
- Support for hybrid readers, allowing a single reader to work with multiple technologies. These hybrid readers allow users of installed card systems to access the unique card serial number or use their existing proximity defined formats. This approach offers businesses a migration path into contactless smart card technology that does not require them to abandon their currently installed access control solution.
- Ability for vendors to develop readers that incorporate additional security capabilities, such as keypads and biometric readers. For ease of installation, readers also offer different connector options, including a Wiegand connector (to be fully compatible with 125 kHz systems) or RS-232 interface (for full read/write capabilities) or both.
- Hybrid card capability, allowing incorporation of multiple technologies on a single card.

The following two sections describe ISO/IEC 14443 and ISO/IEC 15693. For more detailed descriptions of the standards, see Appendix A.

ISO/IEC 14443

ISO/IEC 14443 is a contactless technology with a read range of up to about 4 inches (10 centimeters). This 13.56 MHz technology was originally designed for electronic ticketing and electronic cash. For these applications, short read 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. ISO/IEC 14443 products are now starting to move into the physical access control market.

Initiated in 1994 to standardize contactless proximity cards, ISO/IEC 14443 was finalized in 2001. The standard includes two versions with different modulation approaches: Type A and Type B. During the standard definition period, the technology matured, resulting in large-scale implementations. Physical access cards conforming to ISO/IEC 14443 offer solutions ranging from low-cost memory cards to highly secure MCU-based cards. Contactless MCU-based cards offer levels of interoperability and security identical to the levels offered by contact card solutions.

State of the Market

Approximately 250 million contactless smart cards using ISO/IEC 14443 have been shipped to date.[1] The majority of these cards are used in transportation applications, for automatic fare collection. Most of the contactless cards in circulation (approximately 200 million) are based on ISO/IEC 14443 Type A with

[1] Source: "Contactless Smart Card Technology for Physical Access Control," Avisian Inc., April 1, 2002.

wired logic encryption. A common encryption/authentication protocol used with ISO/IEC 14443 Type A is MIFARE, whose strongest appeal is an independent certification institute that offers compliance testing to the MIFARE specification, ensuring that multiple vendors' certified products will work together.[2] The MIFARE technology is an extension of ISO/IEC 14443 Type A; the standard itself does not define a specification for encryption on the card. ISO/IEC 14443 cards are supplied by the largest base of card manufacturers today.

Because of its capability to very quickly transfer large blocks of data, ISO/IEC 14443 technology is migrating into physical access applications. If stored photos or fingerprints are used in contactless physical access applications, fast block transfers are very important. Most of the biometrically enabled physical access locks available today are used with ISO/IEC 14443 cards. ISO/IEC 14443 products offer up to 2 Kbit blocks in devices with wired logic conditional access, and many times this capacity in MCU-based cards.

Contactless MCU cards that comply with ISO/IEC 14443 offer an excellent combination of interoperability and security. New dual-interface or contactless MCU cards already fully comply with ISO/IEC 14443 (up through part 4 of the standard). The importance of full compliance cannot be overstated. Full compliance gives contactless and dual-interface smart cards the same level of interoperability as contact card solutions. Like the contact card interface standard, ISO/IEC 7816, ISO/IEC 14443 fully defines the contactless communications protocol. This protocol requires manufacturers supplying cards and readers that meet the standard to provide compliant drivers and routines for the transfer of information to and from the cards for use in applications. This is analogous to USB-compliant devices being supplied with the drivers required for the devices to communicate with the PC. The required use of compliant drivers in both the card and reader pushes interoperability into the software layers above the hardware communications interface.

For example, dual interface cards made available by Visa execute the same financial applets in either ISO/IEC 7816 contact or ISO/IEC 14443 contactless mode. As this example illustrates, it is possible to integrate both contact and contactless applications using a single dual-interface chip. Standard MCU-based smart card security features, such as memory firewalls, also provide a secure means for separating contact applications from the contactless applications.

Current semiconductor fabrication technology has reduced the cost of MCU-based contactless ISO/IEC 14443 products. These products are now closer in price to some of the larger (2 Kbyte – 4 Kbyte) wired logic chips. As a result, these new, lower cost contactless chips can be used in cost-sensitive physical access applications, achieving the high security levels available in contact smart cards.

Reader Technology

The growth of the contactless market using ISO/IEC 14443 technology has resulted in a variety of readers. Most products are built with passive components, but semiconductor manufacturers also offer highly integrated solutions supporting the full ISO/IEC 14443 standard.

[2] See reference documents from Avisian and SEIWG for additional details on MIFARE's relationship to the ISO/IEC 14443 standard.

Because the number of readers for a card application is small relative to the number of cards, many applications require that the reader, rather than the card, support multiple protocols. More card sources are available when terminals/readers are fully ISO/IEC 14443 compliant. Hybrid readers and reader chips are available that can support both ISO/IEC 14443 and ISO/IEC 15693.

Key Features of ISO/IEC 14443

- Operating frequency: 13.56 MHz
- Read/write range: Up to 4 inches (10 cm)
- Speed: The ISO/IEC standard specifies a speed of 106 Kbps. ISO/IEC 14443 technology (A or B) is now capable of 212 Kbps, 424 Kbps, and 848 Kbps, with higher speeds under discussion by the ISO/IEC committee.
- Storage memory available: 64 bytes - 64 Kbytes.
- Security:
  - Wired logic cards: Authentication mechanisms are available. The only solution for conditional access that is interoperable from multiple sources is the MIFARE encryption unit.
  - MCU cards: Security mechanisms available in contact smart cards are also available for both ISO/IEC 14443 Type A and Type B (e.g., hardware memory firewalls, sensors, tamper resistance features).
  - Crypto coprocessors, such as 3DES, AES, ECC and RSA, can be used.
  - The close proximity of the card to the reader helps limit unintended communication.
- Interoperability: Supported through full definition of communication commands in ISO/IEC 14443, part 4.
- Vendors: Many

ISO/IEC 15693

ISO/IEC 15693 is a 13.56 MHz passive vicinity 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 is well suited for facility access control in buildings where read ranges are 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 higher ranges, making it unnecessary for drivers to extend an arm out of the car window.

For ISO/IEC 15693 to achieve its read/write distance, data is transmitted at 26.6 Kbps (as opposed to 106 Kbps for ISO/IEC 14443). Physical access system designers can use a number of implementation techniques to compensate for the slower data rate and decrease read times. For example, ISO/IEC 15693 allows applications to set memory sectors of either less than 1 Kbit or greater than 1 Kbit per application, reducing the number of unused bits or increasing an application's sector size for a single read cycle and resulting in fewer read/write cycles. The speed of a transaction between a card and reader is also dependent on the volume of data that is transferred. Since access control applications typically require only a unique identifier to be passed between the card and reader, the actual transaction time for ISO/IEC 15693-based cards most likely will not be an issue for the system designer.

Since ISO/IEC 15693, like ISO/IEC 14443, does not define any security protocols or requirements, vendors have implemented a number of security features, including card-to-reader mutual authentication based on random generated keys, DES and Triple DES encryption of stored data, and a 64-bit authentication key for

each memory sector. These features prevent unauthorized reading of card data, brute force attacks, and sniffing and resending of transmitted data. A portion of the information can be encrypted, allowing access to some information while other details are protected.

State of the Market

ISO/IEC 15693 technology was developed for tracking and access control applications. These applications require longer read ranges and transmission of large blocks of data. Longer read ranges support the hands-free capabilities users expect when they approach a door. Large blocks of data are required for user verification, time and attendance, and access privilege authorization. For these reasons, many of the physical access control companies are adopting ISO/IEC 15693 as the migration path from 125 kHz technology. As users demand a single credential, ISO/IEC 15693 is also migrating into the electronic ticketing and electronic payment markets.

Reader Technology

Manufacturers of ISO/IEC 15693 readers are beginning to integrate the capability to read and write both ISO/IEC 14443 and ISO/IEC 15693. Semiconductor manufacturers have supported this effort by offering products that communicate using both ISO/IEC 14443 and ISO/IEC 15693 within a single reader chip.

Key Features of ISO/IEC 15693

- Operating frequency: 13.56 MHz
- Read range: Up to 3.3 feet (1 meter)
- Speed: 26 Kbps
- Storage memory available: 1Kbit (128 bytes), 2 Kbit (256 bytes) and 16 Kbit (2 Kbytes)
- Security:
  - Wired logic/memory only credentials: Authentication/encryption mechanisms are available but are supplier-specific.
  - Mutual authentication between card and reader.
  - DES and 3DES data encryption.
  - Sector key length: 64 bit
  - Card serial number: 64 bit
- Interoperability: Supported through full definition of communication commands in ISO/IEC 15693, part 3.
- Vendors: Multiple

Figure 3 summarizes the key features of the technologies discussed in this section.

Figure 3: Comparison of Contactless Technology Technical Features

Features	14443	15693	125 kHz
Standards	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 15693 ISO/IEC 7810	None[3] (de facto)
Frequency	13.56 MHz	13.56 MHz	125 kHz
Read range	Up to 10 centimeters (~3-4 inches)	Up to 1 meter (~3.3 feet)	Up to 1 meter (~3.3 feet)
Chip types supported	Memory Wired logic Microcontroller	Memory Wired logic	Memory Wired logic
Encryption and authentication functions[4]	MIFARE, DES/3DES, AES, RSA[5], ECC	Supplier specific, DES/ 3DES	Supplier specific
Memory capacity range	64 to 64K bytes	256 and 2K bytes	8 to 256 bytes
Read/write ability	Read/write	Read/write	Read only[6]
Data transfer rate (Kb/sec)	Up to 106 (ISO/IEC) Up to 848 (available)	Up to 26.6	Up to 4
Anti-collision	Yes	Yes	Optional
Card-to-reader authentication	Challenge/Response	Challenge/Response	Password
Hybrid card capability	Yes	Yes	Yes
Contact interface support	Yes	No	No

[3] The Security Industry Association (SIA) has published the industry specification, SIA AC-01 (1996.10): Access Control: Wiegand Card Reader Interface Standard. This industry specification covers electrical specifications for the transfer of data between Wiegand card readers and security, access control, and other related control panels. The specification also defines power requirements and limits, as well as electrical control of devices contained in the reader.

[4] The ISO/IEC standard does not specify security functions.

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

[6] While the majority of the installed 125 kHz technology is read only, cards are commercially available that support read/write.

Key Implementation Considerations

The selection of the appropriate technology for an access control application should be based on business and application requirements. Additional factors, such as installed base, costs, and other user-specific requirements, also affect the choice of a technology.

Application Type

Access applications can be generally categorized as physical access applications (entering a building or place) or logical access applications (accessing a network or system).

Physical Access Application Solutions
Contactless devices were developed and the technology standardized to provide a fast, reliable interchange of data for physical access applications. Physical access applications typically require a user to present a valid credential at an entrance guarded by a checkpoint. If the credential is authentic, the user is permitted to access the area.

For physical access applications, contactless technology offers reliable and quick throughput. If another authentication factor is introduced, such as fingerprint recognition, the throughput advantages offered by contactless technology are decreased, but the strength of security and authentication is increased.

Where hostile environmental conditions exist, such as when the reader is subjected to heavy rain or contaminants are present, contactless technology offers a significant advantage over any contact technology. Contactless readers are also more resistant to tampering and vandalism, and the lack of moving mechanical parts (e.g., landing pins or read heads) significantly reduces maintenance.

Logical Access Application Solutions
Currently, contact technology provides a convenient and cost-effective way to transfer significant amounts of data between a card and a reader/host system quickly and perform complex cryptographic operations for authentication applications. For these reasons, contact smart cards are a prominent solution for network security implementations.

To accommodate the user's desire for a single ID credential, using a contactless card for both physical and logical access could be attractive. Depending on system requirements, a contactless smart card can now be used to provide the required level of security for logical access, while providing a reliable and easy to use solution. Contactless technology has the advantage of not suffering from physical contact contamination or requiring precise insertion and release.

Hybrid and Dual-Interface Solutions
Hybrid cards offer backward interoperability with installed systems, plus the ability to migrate to new functionalities. These cards offer an affordable way to add capabilities such as biometrics or strong cryptographic authentication to existing systems, without having to discard the existing access control investment. Hybrid cards are best suited to environments that have multiple existing systems and that require the user to carry a single credential.

Just now coming to market are ISO/IEC 14443 dual-interface cards, which include a single chip that provides both contact and contactless capabilities. These cards offer the ability to perform a complete strong cryptographic authentication, including biometric verification, in a contactless environment. Dual-interface devices can be used in situations where the environment favors one or the other.

Application Requirements

Proper application requirements definition is critical to selecting the appropriate contactless technology. Once defined, the requirements can help determine the appropriate technology. It is important to select a technology that:

- Delivers required functionality.
- Provides sufficient security for the application.
- Provides a cost-effective solution.
- Offers convenience to the user.

Card Management

The need to manage the issued card base is a primary consideration. Card management systems and new or modified back-end systems may be required to ensure that only valid cards are usable and to block compromised, lost, stolen or revoked cards.

Security Policy

The security policy for an application defines the required level of security and authentication. It should balance the convenience of the user with the right level of security. In other words, the level of security for what is being protected must be commensurate with the authentication requirement for persons trying to access what is being protected.

Each situation must be analyzed carefully to assess the security requirements. The only thing that is certain is that different security requirements will have to be implemented using different technologies. To write a meaningful security policy it is necessary to have a clear understanding of a specific application with respect to the following:

- Level of security required.
- Speed of transaction (time the card is in the reader field).
- Distance of the card from the reader.

In addition, a security policy must consider budget requirements in determining what cryptographic algorithms and security protocols to use to address both the level of security and user convenience.

Legacy System Considerations

Another consideration is whether any legacy contactless deployment exists or whether this is a new implementation. For existing deployments, it is necessary to consider both the current investment and the impact of change on ongoing operations. In environments where physical access security has already been introduced using magnetic stripe or an early contactless technology (such as 125 kHz), there may be a need to transition users to a new technology over time. How to do this will be specific to each implementation. Hybrid cards are designed to ease the migration by offering multiple technologies on a single card.

Multiple Technology and Application Support

Hybrid cards are a physical medium on which several technologies coexist. Such cards can support different external systems and applications. Hybrid cards may be composed of many different elements, each potentially specific to a particular circumstance, such as:

- Printed cardholder photo
- Printed cardholder name
- Barcode(s)
- Magnetic stripe
- Multiple contactless technologies (125 kHz, 13.56 MHz)
- Contact smart card technology
- Embossing
- Holograms
- Signature panels
- Issuing authority logo

The definition of the hybrid card components must be carefully considered to ensure that a single card can support the features desired. For example, if embossing is required, antenna coil location must be taken into account so that the contactless technology is not damaged during the embossing process.

To aid the transition to contactless technology or to cope with two different physical access system implementations, it may be appropriate to consider one card that combines multiple technologies. Combining magnetic stripe and one contactless (RF-based) technology is relatively straightforward. Combining two contactless devices into one card is more complex. However, providing that the radio frequencies used by the contactless technologies do not interfere with each other and that the readers can operate correctly in the presence of both technologies, one card can support both implementations. There are clearly advantages in issuing a single card to users and in users having to deal with a single card.

Other factors need to be weighed when considering a hybrid card. If a hybrid contact and contactless card is required, it is important to specify that the card comply with ISO/IEC 7810. Along with other card physical characteristics, ISO/IEC 7810 specifies the card thickness, which can be a critical design factor if the card is to be printed at issuance or if it is to be used with a contact smart card reader.

Hybrid cards that include multiple contactless technologies or both contact and contactless technologies are in the early stages of market deployment. As such, it is also important to consider whether there may be any mass deployment issues and define the appropriate specifications and tests to ensure that the new technologies will meet the overall business and application requirements.

Interoperability

Interoperability is a complex consideration, which is understood differently by different business and organizational communities. It is a critical consideration for any physical or logical access system design. Important points to consider are:

- How new technologies interoperate with (i.e., are backward compatible with) installed physical or logical access systems.
- How available contactless products from multiple vendors interoperate with each other.
- How physical and logical access affects other enterprise infrastructure and applications.

- How the interaction of applications is affected by the system components.
- How the applications may interact with each other.

When implementing contactless smart card technologies, it is important to consider that much of the current installed base of 125 kHz physical access systems uses a variety of protocols and vendor-specific access control formats. When implementing or integrating the newer contactless smart card technology, the system design must take these into account to provide an easier integration with the installed system. It may even be necessary to plan for the implementation of multiple contactless technologies until the migration of the enterprise infrastructure to newer contactless smart card technology is complete.

As with other smart card standards, contactless standards only specify how components interact to a certain level and do not include all of the commands or security features necessary to support a full system implementation. When selecting a contactless smart card technology, system designers should review at what level interoperability is supported and how products accommodate non-standard functions. In some cases, it may be necessary for users to collaborate to develop industry-focused specifications for interoperability. For example:

- The EMV specification was developed for 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. It is expected that future enhancements of GCS-IS will include interoperability definitions for contactless smart card technologies, providing an industry resource that can be used for contactless smart card implementations.

A wide range of effective, secure physical and logical access systems can be implemented using contactless smart cards based on current standards. Currently available contactless smart card technologies can provide much greater system flexibility, interoperability of the system components and overall security of the system.

Reader Requirements

In general, contact smart card readers currently cost significantly less than contactless smart card readers. In part, this is because it is relatively straightforward to electrically connect a contact smart card to a reader. Also, the need to issue a low-cost contact reader to each computer user to provide logical access has created market demand that has helped drive the supply. On the other hand, contactless readers have traditionally been designed for use in situations where multiple people use a single reader for physical access. Lower maintenance costs may reduce the total cost of ownership compared to magnetic stripe or contact smart card readers in high volume implementations. As demand for contactless readers increases, it is anticipated that market forces will drive the availability of low-cost contactless readers.

An organization must also review the capabilities of the existing access control system when implementing new reader technology. The majority of installed physical access control readers (barium ferrite, magnetic stripe, Wiegand, and

125 kHz) use the Wiegand protocol. Control panels and facility wiring (e.g., the number and types of wires) are designed to support this protocol. If an organization wants to replace their existing access control system with a newer technology, the new readers' ability to output the Wiegand protocol must be considered. While the Wiegand protocol is widely deployed, it has the limitation that it is a one-way communication protocol. The new contactless smart card technologies (ISO/IEC 14443 and ISO/IEC 15693) offer the advantage of read and write capability. New readers with RS-232, RS-484, LAN or other two-way connections allow the access control system to take advantage of the full capabilities of the contactless smart card, but also will require upgrades to control panels and cabling.

Two-Factor Authentication Requirements

When an application requires a higher degree of authentication of an individual beyond the physical presence or possession of a card, additional factors can be combined to further tie the physical card to an individual.

The use of a PIN in conjunction with contactless technology may be sufficient to ensure the card/user relationship. However, the delays added to the authentication process by the time required for the user to enter a PIN may be detrimental to traffic throughput or may expose the PIN to discovery by an observer.

A combined contactless smart card and biometric ID system provides a powerful method to ensure that the cardholder is the valid owner of the card. Through the combination of the biometric information and on-card security functions, cardholder identity can be verified more accurately and securely. While the combination of biometric and smart card technologies is only now starting to be implemented in secure ID programs, smart cards today provide the optimal implementation platform for a biometrics-based ID system. Smart cards can store the biometric templates, perform a local comparison and ensure that any network and reader communication is encrypted and authenticated. As with a PIN, however, using biometrics with a contactless card will reduce traffic throughput.

Organizational Issues

The use of multi-technology credentials, implemented as hybrid or dual-interface cards, often requires the close collaboration and virtual, if not functional, integration of the information technology (IT) and physical security departments and, potentially, other departments in an organization. This integration can create an entirely new model and sophistication in the security architecture design. Cross-organizational planning and team involvement in the definition of system requirements and design are critical to promoting agreement and cooperation on the new system implementation.

Implementation is also significantly easier if an organization can leverage appropriate legacy systems while adding more advanced technologies to address new requirements. By promoting symmetric administration, an organization can maintain, or even increase, security, while saving both time and effort.

Centralized administration allows security managers to eliminate the management of multiple card systems, PINs, and access codes. Planners and implementers can achieve greater technological benefits while expending fewer resources on migration and implementation. And finally, the level of security can

be adjusted to meet organizational security requirements and policy as slowly or quickly as desired.

Implementation Cost

When considering the cost of implementation, a number of factors need to be considered, including:

- Will the new technology reduce operating costs, increase productivity and/or improve security?
- What is the cost of replacing legacy system cards, readers, and potentially door locks with a newer technology?
- What is the total cost of implementation, including cards, readers, printers, support staff, card management, and back-end systems?
- What types of card technologies are appropriate and cost-effective for the application?
- Are hybrid cards appropriate and cost-effective for the application?
- Would two cards be practical or sufficient in the application environment?
- Is single-factor authentication sufficient when combined with a photo?
- Is two-factor authentication required for a different class of cardholders or for some access checkpoints?
- Must the physical access system be integrated with the logical access system in some way?
- How will a compromised card be revoked throughout the system and how quickly does the change need to be propagated?

The implementation of a secure physical access system should include a stage of fully defining the system requirements, taking into consideration all of the issues discussed above. By carefully defining usage, security, cost, and integration with other legacy and new applications and systems, organizations can select the card technology best suited for their needs.

Conclusion

Organizations are increasingly concerned with the problem of how to verify a person's identity and privileges before granting that person physical access (to a building or place) or logical access (to information or other online resources). Organizations are also increasingly interested in providing users with a single identification credential that can provide an appropriate level of access to multiple resources.

As a solution to these challenges, contactless technologies offer significant advantages. Contactless cards can carry multiple technologies, including contact-based technologies and the more traditional authentication mechanisms, such as bar codes and photographs. Contactless cards can therefore implement the level of security that is appropriate to each situation in which a cardholder requires authentication. Organizations can leverage contactless cards to consolidate and strengthen their overall security. Users can present one card in multiple situations, and organizations can administer a single card for each user.

In addition, cards based on contactless technologies support faster access with higher throughput rates, which is important in handling high volumes of people for mass transit, airport access or physical access to buildings. Because they do not have to be inserted into a reader, they are easy to use and protect. Unlike contact-based systems, contactless systems are better suited to operate in harsh or dirty environments. The lack of mechanical contacts makes both the cards and the readers more durable and less expensive to maintain.

Standards-based contactless smart card technologies are receiving increasing acceptance when the requirement is to augment or replace current physical access systems. Products based on ISO/IEC 14443 and ISO/IEC 15693 are commercially available. Key differentiators between products based on the different standards are read range and data transfer rate. Other considerations in choosing a product include the maturity of the specification on which the product is based and the variety of available supporting components. As is true for any new technology, the marketplace is constantly changing, as standards are enhanced and vendors create new products. While this may make an organization's decision process more complicated, it is also indicative of a healthy and competitive market.

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 legacy systems and the effect of implementation on the users and the organization. Additional considerations apply to multi-application systems, which cut across organizational lines.

Careful definition of the physical access application permits an organization to identify critical system requirements. Implementation using a standards-based technology helps ensure that the system chosen provides appropriate core functionality, that the components are interoperable, and that the system can be acquired from multiple vendors.

For more information about both contact and contactless smart cards and the role that they play in secure identification systems, 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

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

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

"TB6 WP1 Interoperability," eEurope Smart Cards Document, Draft, 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. 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. 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 United States. For more information, visit www.smartcardalliance.org.

Publication Acknowledgements

This position paper was developed by the Smart Card Alliance to discuss the implementation and technology issues associated with the use of contactless technology for secure physical access systems. 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. Members from 16 organizations, both public and private, were involved in the development of this white paper, including: Assa Abloy ITG, Atmel, Bank of America, DMA Marketing, EDS, Gemplus, GSA, IBM, Infineon Technologies, LaserCard Systems, MasterCard International, NTRU Cryptosystems, Inc., Philips Semiconductors, SchlumbergerSema, SCM Microsystems, Turtle Mountain Communications Inc., Visa U.S.A. Special thanks go to the Task Force members who wrote, reviewed and edited this white paper.

Dovell Bonnett, Assa Abloy ITG
Jean-Paul Caruana, Gemplus
Henk Dannenberg, Philips Semiconductors
Ian Duthie, Atmel
Diana Knox, Visa
Philip Lee, SC Solutions
Gilles Lisimaque, Gemplus
Don Malloy, DMA Marketing
Mark McGovern, Turtle Mountain Communications Inc.
John McKeon, IBM
Cathy Medich, Task Force Co-Chair
Bob Merkert, SCM Microsystems
John Moore, GSA
Neville Pattinson, SchlumbergerSema
Joe Pilozzi, Philips Semiconductors
Herve Roche, Atmel
James Russell, MasterCard International
Randy Vanderhoof, Smart Card Alliance
Michael Vermillion, EDS
Jeremy Wyant, NTRU Cryptosystems, Inc.

Copyright Notice

Trademark Notice

Appendix A: Contactless Standards

This appendix summarizes the current contactless technology standards.

Current contactless smart card standards cover the following:
- Card physical characteristics
- Test methods for compliance
- RF interface and modulation scheme (OSI physical layer)
- Initialization and anti-collision (OSI transportation and data-link layer) transmission protocols, commands and data structures

Other standards would apply when other technologies are used in combination on the contactless smart card (e.g., contact, magnetic stripe, embossing).

It is important to note that there is no standard for printing requirements on plastic cards. Depending on the manufacturing process used and the plastic characteristics, some printing equipment (mainly for de-localized issuance) may or may not be able to print on a given contactless card.

Basic Standards for All ID Cards

Two basic international standards cover all ID cards.

ISO/IEC 7810 - Identification Cards – Physical Characteristics
This standard was published in 1985 and describes major characteristics for different sizes (ID-1, ID-2, ID-3) of cards. ID-1 is the standard size for contact as well as contactless smart cards. Standard card dimensions are: 54 mm x 85.6 mm x 0.76 mm (2.125 in x 3.370 in x 0.03 in).

ISO/IEC 10373 – Identification Cards – Test Methods
Part 1: General characteristic tests
Part 2: Cards with magnetic stripes
Part 3: Integrated circuit(s) cards with contacts and related interface devices
Part 4: Close coupled cards
Part 5: Optical memory cards
Part 6: Proximity cards
Part 7: Vicinity cards

Contactless Standards

There are three major groups of contactless card standards, which differ in the range of operating distance between the card and the reader antenna.
- ISO/IEC 10536 – Close coupling contactless cards (operating distance less than 2 millimeters)
- ISO/IEC 14443 – Proximity contactless cards (operating distance up to 10 centimeters)
- ISO/IEC 15693 – Vicinity contactless cards (operating distance up to 1 meter)

ISO/IEC 10536 – Identification cards – Contactless Integrated Circuit(s) Cards – Close Coupled Cards
Part 1: Physical characteristics (published in April 2000)
Part 2: Dimension and location of coupling areas (revised in October 2001)
Part 3: Electronic signals and reset procedures (published December 1996)

A survey done by ISO in 1995 recorded that five countries were using this standard (United Kingdom, Australia, Korea, Germany, and Italy). The advances in proximity and vicinity technologies make this contactless standard increasingly less appealing. It allowed use of capacitive or inductive coupling between the card and the reader but had issues with vibration or radio interference. No large deployment of this technology has been announced in the past 5 years.

ISO/IEC 14443 – Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards
Part 1 – Physical characteristics
Part 2 – Radio frequency power and signal interface
Part 3 – Initialization and anticollision
Part 4 – Transmission protocol

ISO/IEC 14443-1 - Physical characteristics

ISO/IEC 14443-1 was published as an international standard on April 15, 2000. The standard defines the following:

- Card dimensions (referring to ISO/IEC 7810 for ID-1 cards)
- Surface quality for printing
- Mechanical resistance
- UV and X-ray resistance
- Sensitivity to surrounding magnetic fields

The standard also introduces the following specific terms:

- PICC: Proximity integrated circuit(s) card
- PCD: Proximity coupling device (the card reader or terminal)

ISO/IEC 14443-2 Radio frequency power and signal interface

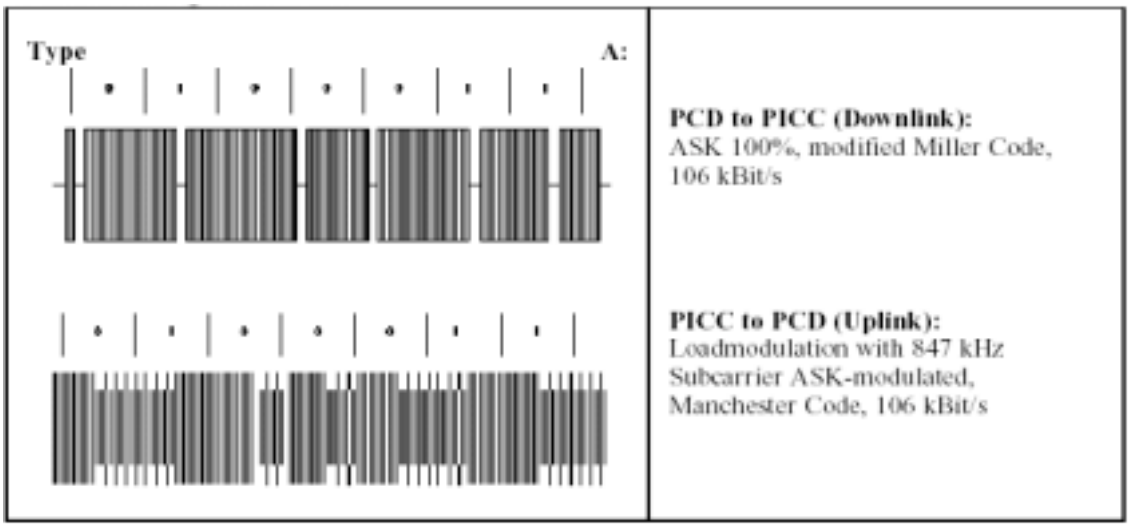
ISO/IEC 14443-2 was published on July 1, 2001. This standard describes the characteristics of power transfer (based on inductive coupling) and communication between the PICC and PCD. Power is transferred to the card using a frequency-modulated field at 13.56 MHz +/- 7 kHz.

Two different types of communication signal interfaces (bit coding) are specified: Type A and Type B. The bit protocol timings are defined and the standard (default) data transmission rate is defined at 106 kBaud.

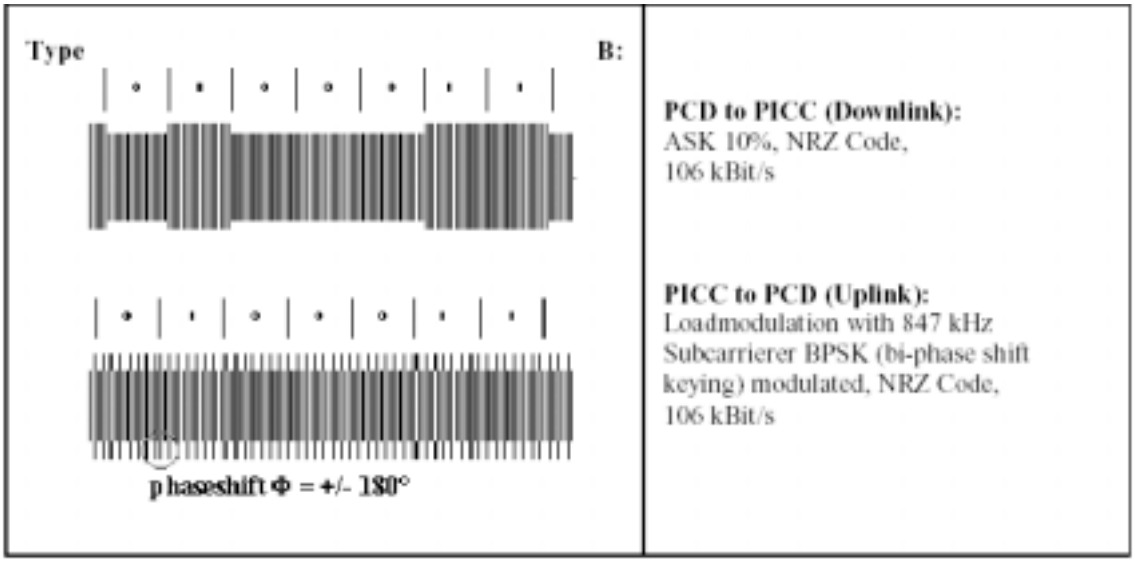
Some abbreviations used in this standard are:

- ASK Amplitude shift keying
- BPSK Binary phase shift keying
- NRZ Non-return to zero

Type A communication interface signal
Source: eEurope Smart Cards document: TB6 WP1 Interoperability Draft May 2002



Type B communication interface signal
Source: eEurope Smart Cards document: TB6 WP1 Interoperability Draft May 2002



The protocol as defined in the standard (Type A or Type B) does not imply the nature of the chip in the card. Since many current MCUs are able to generate their clock internally, even when the external modulation is 100% (Type A), MCU-based smart cards can be fully compatible with 14443 Type A protocol.

ISO/IEC 14443 Part 3 Initialization and anticollision

ISO/IEC 14443-3 was published as an international standard on February 1, 2001. This part of ISO/IEC 14443 describes:

- Polling for PICCs entering the field of a PCD (i.e., the terminal talks first).
- Byte format, command frames and timing.
- Request (REQ) and Answer To Request (ATQ) commands
- Anticollision methods to detect and communicate with one particular card when several cards are presented to the same reader. Anticollision methods rely on a unique ID per card; however, depending on the communication type (A or B), the anticollision method is different.
  - Type A: Binary search method referring to the unique identifier (UID) of the card.
  - Type B: Slotted Aloha method.

A complete state diagram explaining the sequence and status of the elements of the system is available in the eEurope Smart Cards TB6 WP1 Interoperability Draft (see references).

ISO/IEC 14443 Part 4 Transmission protocol

ISO/IEC 14443-4 was published as an international standard on February 1, 2001. This standard specifies a half-duplex block transmission protocol (T = CL). Several protocol scenarios are included in Appendix B of this standard, showing how this common transmission protocol can be used. The standard also defines the transparent exchange of data, independent of the lower layers. This set of commands are all mandatory, providing interoperability with fully compliant products.

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

Part 1 - Physical characteristics
Part 2 – Air interface and initialization
Part 3 – Anticollision and transmission protocol

ISO/IEC 15693-1 Physical characteristics

ISO/IEC 15693-1 was published as an international standard on July 15, 2000. It refers to ISO/IEC 7810 for dimensions and introduces specific terms:

- VICC: Vicinity integrated circuit(s) card
- VCD: Vicinity coupling device

This standard also includes definitions for the behavior of the card when exposed to mechanical stress, static and alternating electric fields, and magnetic fields.

ISO/IEC 15693-2 Air interface and initialization

ISO/IEC 15693-2 was published as an international standard on May 1, 2000. This part of ISO/IEC 15693 describes the characteristics of power transfer (based on inductive coupling) and communication between the VICC (card) and VCD (reader device). The power is transferred to the card using a frequency-modulated field at 13.56 MHz +/- 7 kHz. The standard requires that several different modes be supported by the VICC.

Abbreviations used in this standard:

- ASK Amplitude shift keying
- PPM Pulse positioning modulation

The standard defines the following two modes:

1 - Reader device (VCD) to card (VICC) : (Downlink)

Modulation: 10% ASK or 100% ASK
Coding: Pulse positioning modulation
"1 out of 256" (long distance mode)
"1 out of 4" (fast mode)
Baud rate: 1.65 Kbps (long distance mode)
26.48 Kbps (fast mode)

2 - Card (VICC) to reader device (VCD): (Uplink)

Modulation: Load modulation with one or two subcarriers
One sub-carrier: 432.75 kHz or
Two sub-carriers: 432.75 kHz and 484.28 kHz
Coding: Manchester coding
Baud rate: Depending on the number of sub-carriers, the Low Data Rate is either 6.62 Kbps or 6.67 Kbps and the High Data Rate is between 26.48 Kbps and 26.69 Kbps.

ISO/IEC 15693-3 Anticollision and transmission protocol

ISO/IEC 15693-3 was published as an international standard on April 1, 2001. This part of ISO/IEC 15693 describes:

- Protocols and commands.
- Other parameters required to initialize communication between a VICC and a VCD.
- Methods to detect and communicate with one card among several cards presented (anticollision).
- Data elements – for example, UID and Application Family Identifier (AFI).
- Memory organization.
- Behavior of VICCs described in state machine diagrams.
- Set of commands (mandatory, optional, custom and proprietary).

Appendix B: Glossary of Terms & Acronyms

Access control system format
The access control system format is the mathematical algorithm that specifies how data transmitted by the system is to be interpreted. The format specifies how many bits make up the data stream and which bits represent different types of information. 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
Contactless technology that uses barium ferrite in the composition of the credential to store data and make it available to the reading device.

CCTV
Closed Circuit Television.

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

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.

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

DES
Data Encryption Standard.

Door reader
The device on each door that communicates with a contactless card or credential and sends data from the card to the controller for decision on access rights.

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

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.

FCC
Federal Communications Commission.

FIPS
Federal Information Processing Standard.

GSA
General Services Administration.

IEC
International Electrotechnical Commission.

Integrated circuit
See chip.

ISO
International Organization for Standardization.

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 general purpose computer, a microcontroller is designed to operate in a restricted environment.

PC
Personal Computer.

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

PIN
Personal Identification Number.

PKI
Public Key Infrastructure.

Read range
The distance between the contactless card reader and the contactless card or credential.

RF
Radio frequency.

RFID
Radio Frequency Identification.
RSA
Refers to public/private key encryption technology invented 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.

3DES
Triple DES.

UL
Underwriters Laboratories.

USB
Universal Serial Bus.

Wiegand strip
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.