Smart Cards for Access Control
Advantages and Technology Choices

Introduction

Security managers have never had more options for access control cards and other badging and credentialing applications. Magnetic stripe, Wiegand and proximity technology all remain popular and effective.

One new technology many security and IT managers are evaluating is contactless smart cards. Just as proximity technology brought advantages over Wiegand card technology 20 years ago, contactless smart card technology today is bringing new advantages over proximity for physical access control as well as other applications.

The objective of this white paper is to discuss smart card technology in an access control context, present its advantages, and discuss implementation considerations.

Benefits of Contactless Smart Cards for Access Control

Whether you are installing a new or expanding an existing system, or undertaking a major upgrade, there are several considerations for using contactless smart cards instead of proximity or other access control card technologies. Following are the most important benefits of contactless smart cards.

1. Contactless smart cards achieve a higher security level of the credential and the overall access control system.

Contactless smart card technology is optimized to provide highly-secure devices by using cryptography, encryption and the internal computing power of the smart chip. Since the ISO/IEC standards do not address security and authentication, this capability must be examined specific to each supplier.

For example, access control data in the card may be protected using 64-bit diversified security keys based on a unique card serial number. This security can be further customized by the end-user with a card programmer. The reader never transmits this unique card serial number to the control panel, because it is used exclusively for key diversification and to prevent data collisions when reading several cards at the same time.

RF data transmission between the cards and readers is encrypted using a secure algorithm so that with certain contactless technology, the transaction between the card and reader cannot be "sniffed" and replayed to a reader. In addition, the cards and readers authenticate each other using a symmetrical key-based algorithm. For even higher security, card data may also be protected with DES or triple-DES encryption.

By using diversified unique keys and industry standard encryption techniques, the risk of compromised data or duplicated cards is reduced. Even if an unauthorized person obtains a reader, without the keys the reader will not authenticate with the card and data will not be transmitted.

These security measures are not implemented in proximity cards, giving contactless smart cards a significant security advantage.

2. Contactless physical access control credentials can carry secure IT applications such as secure logon to networks, digital signature, and encryption.

Every day there is news of some new incident involving breaches of information systems security, and smart cards are rapidly becoming the de facto choice for securing IT infrastructures. While still in the early stages, this trend is being established by two influential groups who know this subject well, the computer industry and the

United States government. For example, Sun, HP and Microsoft all have initiatives to use smart cards for their own network security. The United States Departments of Defense, Interior and Treasury all have smart card initiatives for network access and electronic signatures.

Bill Gates, in a well-publicized internal executive email, recently underscored the importance of smart card technology in IT security, when he explained Microsoft is "working with a number of major customers to implement smart cards as a way of minimizing the weak link associated with passwords. Microsoft itself now requires smart cards for remote access by employees, and over time we expect that most businesses will go to smart card ID systems."[1]

3. ***Contactless smart cards provide more storage and the secure reading and writing of data.***
Contactless smart card memory capacity ranges from 64 to 64k Bytes while proximity card memory ranges from eight to 256 Bytes (2k bit).

4. ***The capability to add other applications to the card is one of the most important advantages of contactless smart cards over proximity technology.***
Depending on the amount of memory available and the number of memory areas, contactless smart cards can serve as multi-application credentials that are used for many purposes. Since the memory can securely store any kind of information, physical access control credentials based on contactless technology can be used for just about anything. These application examples may include:

Biometrics
Secure Authentication
Health Records
Transit Passes
Digital Cash
Information Access

Time and Attendance
Guard Tour Information
Equipment and Material Check-out
Loyalty and Membership Programs
Lighting and HVAC Control and Billing
Authorized Access to Office Equipment

5. ***Organizations considering biometrics for either physical access or IT security applications can use contactless smart cards as a secure carrier of the biometric template.***
Smart cards are an ideal complement to a biometrics implementation, and are particularly well-suited for installations spanning multiple sites. Storing the template on the card simplifies system start-up and enables the support of unlimited populations. It also eliminates the redundant wiring requirement for biometric template management, lowering implementation costs significantly.

6. ***Users can define and control their access keys.***
In many cases, organizations consider control of their own keys for physical access control and other applications an essential element to security. Contactless technology makes it possible to do this.

7. ***Future-proofing - the desire to embark on a path offering greater expandability in the years to come.***
Today your immediate need may only be access control, but are you planning for tomorrow? A contactless smart card access control system provides an immediate benefit of higher security, and also better positions the organization with options for adding new applications in the future.

8. ***Contactless smart card technology is affordable.***
The many advantages of contactless smart cards have generated a great deal of interest in recent years, but one important factor that held the market back is cost. Until now, proximity technology held an important cost advantage over smart cards; however that has changed. Anyone with a budget to put in a standard proximity-based access control system can afford to install a smart card system instead.

[1] "Security in a Connected World," Executive Email from Bill Gates to Microsoft employees, Jan. 23, 2003, www.microsoft.com.

Advantages Over Contact Smart Cards

Contact smart cards never gained acceptance for use in physical access control systems for the three main reasons presented here.

1. ***A contactless presentation of the card is much more user friendly and convenient for physical access control.***
   With contact smart cards, users must properly orient the card to put the contact in the correct position, find the opening in the reader, insert the card and leave it there until the end of the transaction before removing it.

2. ***Contactless smart cards and readers are much more durable in harsh, dirty, or outdoor environments such as those typically found in access control applications.***

3. ***Contactless card transactions are designed to be faster than contact transactions.***
   Contact smart cards were not optimized for fast transactions, but for very high-security applications like financial services and debit card PIN protection. Since contactless card were targeting high-throughput applications like transit fare collection and ticketing, fast transactions were mandatory while still maintaining high levels of security. For that reason, as contactless technology developed it was optimized for fast reading and authentication, an advantage in access control systems as well.

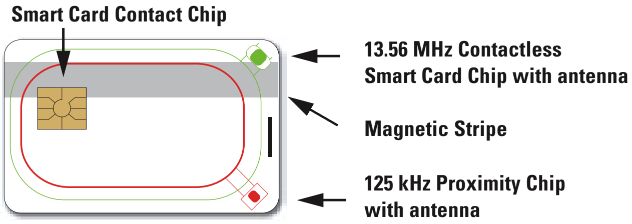
Multiple Technology Cards

Since contactless smart cards are generally delivered on ISO/IEC 7810 compliant card bodies, other features normally associated with plastic cards can be used in conjunction with contactless technology, including:

Magnetic Stripes
Bar Codes
Contact Chips
Holograms
Corporate Logos

Pre-printed Graphics
Photo Personalization via dye sublimation printing
Image Customization via dye sublimation printing
Signature panels
Punched slots for lanyards

In addition to these typical features, different technologies can be successfully combined on a single card, such as combining 15693 contactless with Wiegand, magnetic stripe or proximity technology as a way to transition to the new technology over time. Cards that carry more than one technology are often called hybrid cards, or simply multiple technology cards.


Smart Card Contact Chip
13.56 MHz Contactless Smart Card Chip with antenna
Magnetic Stripe
125 kHz Proximity Chip with antenna

Multiple technologies on a single credential can provide an excellent solution in many situations. One example is combining a high-performance crypto-processor contact card for secure network logon and contactless technology for physical access control on a single photo-ready identity credential. Another typical use is facilitating the migration from one access control technology to another over an extended period, across multiple facilities or for subsets of the entire cardholder base.

Another aspect important to physical access control is making the smart card technology available in other form factors, notably keys and tags. Tags are protected, self-adhering modules that can conveniently be added to an existing credential to simplify migration or as a quick way to add new capabilities to a part of the total card population. It is very important to confirm that your selected technology is available in these additional form factors common to the physical access control market.

iCLASS® Contactless Smart Card Technology for Physical Access Control

A good example of secure contactless memory cards that are optimized for physical access control applications and can be used for multiple applications are those based on the iCLASS technology from HID. This technology is ISO/IEC 15693 compliant, operates at 13.56 MHz, offers a high-speed communication feature, contains special features for digital cash applications and includes its own encryption/authentication protocol.

Two memory sizes are available with iCLASS contactless cards - 2k bit (256 Byte) and 16k bit (2k Byte). In the smaller card, this memory is divided into two separate areas. One is used for the physical access control data, and the other is available for another application.

In the larger card, the memory can be divided into either two or 16 separate areas, creating the possibility to have many applications on an iCLASS contactless smart card. Applications that require more storage, like fingerprint biometrics, can use more than one segment when required, making for a very efficient use of the available memory. Applications can be on the card when it is issued, or added at a later date if so desired. Each memory segment, and therefore each application, has its own unique security. Since they are memory cards, the iCLASS technology security features are implemented in wired logic.

The robust security features of the iCLASS technology encryption/authentication protocol, which include diversified keys, unique 64-bit card serial number, encrypted RF communications and mutual card and reader authentication, are covered in the section entitled, "Benefits of Contactless Smart Cards for Access Control."

iCLASS cards support both standard 15693 communications and the faster 14443 Type B. If you are implementing a physical access control based on iCLASS technology, you are able to have a longer read range complemented with faster data communications.

iCLASS 16K cards feature standard anti-counterfeiting including:

1. Ultra-violet (UV) fluorescent inks, invisible to the naked eye, can be used to verify the authenticity of a card when placed under a black ultra-violet light.
2. Holograms are the accepted security measure in the financial and banking world, are easily recognizable by security personnel, and allow for quick visual identification of counterfeit cards.
3. Custom holograms or UV fluorescent ink design incorporating corporate logos can be created to enhance corporate identity and brand recognition.

In addition to cards, HID offers iCLASS technology in key and tag form factors. The tags are round, self-adhering modules protected by a plastic cover. These can be added onto an existing credential, or used to secure assets like mobile phones, portable computers or other high-value or high-security assets.

Conclusion

Contactless smart card technology is well-suited for access control applications. It provides higher levels of security than traditional access control technologies and the platform from which additional applications can be implemented on the same credential. There are products available on the market today that provide an affordable migration path to smart card technology while protecting customer investments in existing infrastructures.

With the introduction of iCLASS technology, HID established a new and significantly lower cost for contactless smart cards. Traditionally, proximity cards have been more convenient to use, and HID's iCLASS contactless technology brings this same level of convenience to smart cards.

Whether a company is implementing an IT security solution today, or is looking downstream and planning for the future, it makes sense to put in a contactless smart card access control system like iCLASS, because it creates a technology base that can support IT security and physical access applications on the same credential.