Basic Overview of Smart Card Technology

What is a Smart Card?

Smart cards are typically credit card sized, plastic credentials containing a microprocessor chip that serves the dual functions of communication and extensive data storage. Although it is packaged in the form of a card, a smart card operates much like a personal computer in that it can store data, manipulate data, and perform functions like mathematical equations. Smart cards normally contain application fields/sectors secured by special, application-specific security keys (much like keys that unlock various rooms in a building). These sectors can contain information for various applications – such as access control, cashless vending, mass transit, and payment systems – securely separated from one other by security keys. Smart cards can come in two forms: contact and contactless. Contact smart cards operate much like magnetic stripe cards (credit cards, etc.), requiring insertion into or direct contact with a reader. Contactless cards are read when presented near or in "proximity" to a reader.

Contact Smart Cards

Most cards originally introduced in the market were contact smart cards. This technology contains approximately 800 times the storage capacity of its predecessor, the magnetic stripe card. Although most new applications of smart cards appear to be heading toward contactless technology, contact smart cards are still the standard for logical (computer) access and some other applications, such as payment systems in Europe.

Contactless Smart Cards

Contactless cards should not be confused with their predecessor – the proximity card. Although both technologies transmit data via radio frequency (and the visible operation of each appears the same to a user), a contactless card provides much greater security and contains approximately 100 times the data storage of a traditional proximity card. Most new applications of smart cards, such as payments systems, are currently running pilots in anticipation of transitioning to contactless technology.

ISO Standards Governing Smart Cards

The International Standards Organization (ISO) is a network of 148 countries' institutes of standards that provides consensus for decisions governing standards for various products worldwide. Members include one representative per nation, including both government and private sector individuals. Decisions made by the ISO affect both business and government standards.

ISO 7816 is the ISO standard governing contact smart cards. The standard covers physical characteristics, dimensions and contact locations, transmission protocols, commands for interchange, application identifier systems and data elements.

ISO 14443 is a four-part contactless standard consisting of physical card characteristics, radio frequency power and signal interference, initialization and anti-collision and transmission protocols. The operating frequency defined in this standard is 13.56 MHz, providing a read range up to 4 inches (10 cm). There are two "flavors" of ISO 14443: Type A and Type B. Although originally meant to serve different functions, both Type A and Type B are now microprocessor standards similar in function. However, ISO 14443A is the more commonly used technology, while Type B is used primarily in banking applications. Due to faster data speeds, 14443 technology is recommended for applications in which extensive amounts of data, such as large biometric templates, need to be transmitted. Anticipating an increase in data-intensive applications requiring high data rates, the U.S. government recently selected ISO 14443 as its official standard.

ISO 15693 is a 13.56 MHz technology referred to as *vicinity* because it provides greater operational read ranges, making it the preferred choice for many high-traffic locations like access control.

Proximity can refer to ISO14443 or to the older 125 kHz technology traditionally used in access control. 125 kHz proximity is not "smart" technology and is not governed by ISO standards. 125 kHz proximity is typically proprietary, requiring that cards

and readers be purchased from the same vendor.

Unique Identifier (UID): All ISO-compliant smart cards are provided with a UID number (akin to a VIN number on a vehicle). For interoperability purposes, a card's UID is *open* and available to be read by all compliant readers. Since this unique number is not secured by keys, reading the UID of a smart card is comparable to reading a proximity card, mag stripe card or other technology that utilizes open, unsecured numbers.

Advantages of Contactless Smart Cards

There are a number of advantages to consider when comparing contactless technology to contact smart cards and 125 kHz proximity cards:

1. *Convenience:* Given the choice, users will virtually always choose contactless over contact technology. Contactless smart card users do not have to worry about where to insert the card, how to insert the card, or how fast to slide the card.

2. *Less Maintenance/Warranty:* Contactless smart cards require very little wear and tear maintenance because they contain no moving parts and require no points of contact. As a result, most contactless smart cards come with lifetime warranties covering defects and workmanship.

3. *Higher Security*: Contactless products are uniquely capable of

XceedID Corporation * 112 N. Rubey Dr., Suite 100 * Golden, CO 80403
Phone: (303) 273-9930 * Fax: (303) 273-9937 * www.XceedID.com

providing optimal transmission security with optional encryption and mutual authentication features. Mutual authentication is a three-way communication process between a card and reader using hashed, encrypted messages to authenticate each other without broadcasting a shared secret key.

4. *Large Memory*: Contactless cards have a data storage capacity approximately 100 times greater than that of a proximity card. Contactless smart cards can also process information, calculate mathematical formulas and perform other computing functions.

5. *Enhanced Privacy*: Even large biometric templates can be stored and verified using a single contactless smart card, allowing private information to stay in the possession of the card holder instead of being stored in a data base.

6. *Versatile Form Factors*: Unlike its contact counterparts, contactless smart communication can utilize a variety of credential technologies. Keychain fobs, watches and even stickers can be used as contactless credentials.

7. *Multiple Applications*: Carrying a contactless smart card is like carrying many cards in one. A single contactless smart card can manage multiple applications such as access control, payment systems, cashless vending, paring, mass transit, etc. Additional features and applications can be added to a contactless smart card as user needs evolve.

8. *Future Protection*: Contactless smart technology will no doubt soon replace mag strip and proximity technologies. Choosing contactless products now will avoid the use of obsolete and outdated systems while providing the best avenue for system expandability.

Card Technology Overview

MIFARE® is a 13.56 MHz contactless technology family of microprocessors developed by Philips. MIFARE is the most common contactless chipset on the market and is used in most applications around the globe. It is an ISO 14443 product that ensures compatibility with future products. Cards can be purchased that contain memory up to 32k bits, a capacity robust enough to process the largest biometric templates while still incorporating other applications.

DESFire® is a high-end chipset in the MIFARE family that is the first chip compliant with the Government Smart Card Interoperability Specification (GSC-IS). The GSC-IS standard was created to ensure the interoperability of contactless and contact smart cards throughout the federal government.

DES Encryption is a strong cryptographic algorithm protecting classified information. It is a public algorithm determined by the National Institute of Standards and Technology (NIST) to be open, inexpensive, widely available and – most of all – very secure.

XceedID Corporation * 112 N. Rubey Dr., Suite 100 * Golden, CO 80403
Phone: (303) 273-9930 * Fax: (303) 273-9937 * www.XceedID.com

Triple DES is slower than regular DES but its longer key length and triple encryption process is billions of times more secure. Its advantage over other security algorithms is that it is based on the DES algorithm, making it easy to modify existing software to incorporate triple DES. Triple DES is also public with proven reliability.

my-d® is a 13.56 MHz contactless technology family of microprocessors developed by Infineon Technologies, one of the world's leading semiconductor companies. Its advanced security algorithms also make it a worldwide leader in ISO 15693 contactless technology.

iCLASS® is a proprietary, ISO 15693 compliant, 13.56 MHz contactless product line developed by HID Corporation (an industry-leading card and reader manufacturer).

ISO-X ™ is a line of multi-technology readers developed by XceedID Corporation. These products were the first to incorporate 13.56 MHz contactless and 125 kHz proximity technology in the same reader as well as secure ISO 14443 and ISO 15693 communication.

Security

The XceedID smart card system offers a high level of security and data integrity through the use of high-level cryptographic techniques. The memory of the ISO-X credential is divided into several sectors (also called applications). Each sector is secured by an *Authentication Key*. A reader can only access a secure sector after a successful mutual authentication is performed. A successful mutual authentication requires that the reader and the card share a common secret - the mutual authentication key. The size of the mutual authentication key employed by the ISO-X smart card system is 128 bits – the largest in the industry. After a successful authentication has taken place between the reader and the credential, communication is authorized and the reader gains access to the authenticated sector or application using *Message Authentication Codes* (MACs). Each message going back and forth between the reader and the credential is digitally signed, ensuring that the communication remains authentic at all times and that an unauthorized device cannot interfere with the communication between the credential and the reader. The ISO-X smart card system is the only ISO15693 access control system offering Message Authentication Coding. The ISO-X smart card system also offers encryption of the data stored on the credential. The encryption algorithms employed by the ISO-X system are the popular DES and 3DES, which are strong, proven algorithms.*

*For more information regarding ISO-X security, key management and application fields, see *Application Note #4* found on XceedID's website – www.xceedid.com.