Sorting Through Credential Technology Choices

Significant evolution of card/credential and RFID technology in recent years has generated many questions from end-users and suppliers. What are the technologies and what is the best choice for your organization? Answering these questions is the purpose of this white paper.

Most people have used *Magnetic Stripe, Bar Code,* and *Proximity* technology cards or credentials. However, there tends to be some confusion surrounding the capabilities and advantages of bar code, proximity and – most recently – smart card technology.

Card Types

First, it is important to note that although we refer mainly to *cards*, most card technologies related to proximity and contactless may appear in several forms including cards, keyfobs, and tickets.

- *Magnetic Stripe* cards have been the most common technology used in many applications in recent decades. Also referred to as mag-stripe or swipe cards, these cards contain a strip of coated magnetic recording tape affixed to the outside of a card that is read when swiped through a reader. Mag-stripe cards have been the standard in the payment systems industry for years as well as the technology used in swipe access control systems. There are three *tracks* on a magnetic stripe that differentiate simple information (similar to the transfer of "license plate" information). Although typically lower in cost, mag-stripe cards have very low security in regard to the protection of the information stored on the card.
- *Bar Code* credentials contain a series of lines that vary in width and distance from one another. Bar code readers use a laser beam (sensitive to the reflected light of the lines) to translate reflections into digital data that is transferred to a host computer for decision or storage. To date, bar code technology is the standard for retail check-out, inventory control and postal service. Next to magnetic stripe credentials, bar code credentials are the easiest and least expensive to produce. However, since bar codes are visible and easy to duplicate, the bar code card is the least secure of the access control credentials. (Recently, more secure bar code credentials have become available but represent an extremely limited percentage of access control credentials.)
- *Proximity* cards have become the standard for access control credentials. These credentials utilize radio-frequency identification (RFID) technology to communicate

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

- between a card and reader. The reader translates the information from a card into a digital format read by a host panel/computer that makes the decision to authorize a person's entry or acceptance. Proximity has become the standard in access control due to convenience (reading a credential presented within several inches of a door or reader) as well as greater transaction security when compared to magnetic stripe and bar code technologies.

- *Smart Card* credentials are typically credit card sized credentials containing an embedded processor chip with a memory capacity approximately 800 times that of a magnetic stripe card. Most smart card systems have the capacity to both read and write information to the card from the reader or panel, providing better data security while creating much greater flexibility for use in various applications. Smart Card credentials can be *Contact* or *Contactless*. *Contact* cards are similar in operation to mag-stripe cards in that they must be swiped or inserted into a reader to be read. They are recognizable by the gold chip visible on the outside of the card (which must make contact with the reader). *Contactless* cards utilize RFID technology, which may appear identical in operation to a proximity card to the average user. However, contactless smart cards have 100 times the information storage capacity, work on a different RF frequency and have far greater data security than a traditional proximity card.

A Smart Card Revolution in the U.S.?

A common question may be: We have heard of wide acceptance of smart card technology in Europe and of the impending smart card revolution in the United States for years, yet it has not appeared to happen. What would indicate that a revolution is more likely today than several years ago?

In the 1990s, acceptance of smart technology in the U.S. lagged behind Europe and Asia because the U.S. already possessed a highly advanced telecommunications and banking network. Lack of strong telecommunications infrastructures, increasing rates of identity fraud and the high cost of processing information drove Europe and Asia to quickly adopt technology that could address these acute challenges.

The absence of government and industry standards for smart cards in the 1990s also contributed to the slow acceptance of the technology in the U.S. Without standards to facilitate interoperability, the full potential of smart card technology could not be realized. In July, 2003, the U.S. government adopted industry standards (ISO 14443 and other requirements) that have since propelled acceptance of smart card technologies at an exponential rate.

Finally, most smart cards originally introduced in the U.S. were contact smart cards, whose limitations generated increased access control system maintenance (chip and reader damage, etc.). Since proximity technology was already the accepted

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

standard in the security industry in the U.S., there was also the perception of going backwards in technology – from proximity *back* to contact technology.

Brief Overview of RFID Technology (Proximity vs. Contactless)

Most experts project that RFID technology will gain acceptance explosively in the coming decades. However, there are many misconceptions regarding the capabilities of and privacy issues related to the technology. Pilot tests are being run in many industries but RFID technology has already been well proven and accepted in the security and public transportation industries.

The function of an RFID reader is very similar to that of a radio. Readers contain a receiver and transmitter used to send and receive radio waves (measured in *hertz* as a representation of *frequency).* Like a wave in the ocean, a radio wave goes up and down over time. The unit of measure representing one wave cycle per second is the *hertz* (Hz). The *frequency* of a wave is the number of wave cycles completed over a period of time, typically one second. Proximity technology operates in the low frequency band of 125 kHz (125,000 hertz/second). Contactless technology works in the higher frequency band of 13.56 MHz (13.56 million/second), roughly 100 times the speed of proximity technology. Higher frequency improves data transmission speed and security.

Simple 125 kHz proximity RFID technology has been the standard in access control for many years. Proximity is very similar to the technology used in applications such as animal identification and supply-chain inventory tracking. A basic RFID credential includes a simple chip of static memory and an antenna capable of transmitting the chip's ID to the reader. When a credential comes within range of the reader, it is powered by the electromagnetic field produced by the reader and proceeds to transmit its ID in much the same way a license plate identifies a vehicle. The communication is a simple, non-secure, one-way, read-only communication.

Contactless technology is typically a read/write, secure communication. Contactless smart cards are programmed with a unique identifier (UID) – similar to a vehicle VIN number – that enables interoperability and identification worldwide. Security information, such as the badge number used for access control, is contained within the application fields of the card (like pages of a book or rooms in a building) and is secured by special *keys*. Security of the information is further guarded by a process called *mutual authentication,* in which the reader and card verify that they belong to and are authorized to communicate with one another. The card and reader share a secret key that can only be verified through a process of *hashing* (mixing) random numbers with the secret key through an encryption method of algorithm processing. The secret key ensures secure communication because it is never communicated through the "air", and therefore cannot be intercepted (see application note #4 for more detail XceedID's website for more detail). In addition to superior security, contactless smart card technology also allows greater information storage and speed. One card can handle many applications like cashless

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

vending, cafeteria or payment systems, and biometrics. Contactless smart cards are particularly effective for biometric applications (the unique identification of a person's identity through physical characteristics such as fingerprint, iris recognition, hand geometry, etc.). Biometric templates containing large blocks of information can be stored securely on a smart card, ensuring the privacy of physical data (the card stays in the individual's possession) without the need for large data base storage.

What does the future hold? With standards in place, the market appears to be moving quickly towards contactless smart card technology. A far more powerful card, protected by superior data transmission security, clearly presents numerous advantages and potential applications to explore. VISA, Mastercard, and American Express have all begun pilot tests of contactless payment system programs with great success and an eye toward implementing the technology in the years ahead. Consumers prefer the simplicity of waving a card near a reader to the archaic swipe method of presentation. Vendors enjoy the benefits of that simplicity, as well as the lower maintenance inherently associated with contactless systems. The U.S. government has already introduced contactless visas and border control documents. The medical industry is in the process of evolving to contactless technology for rapid "check-in", patient medication and equipment tracking. The contactless revolution is clearly in full swing – be sure to incorporate this technology in your next credential decision-making process.

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