



RFID WHITE PAPER US-3

RFID Credentials in Security Applications Critical Applications Parameters Choices & Capabilities Overview

April 5, 2007

©2007 Deister Electronics USA, Inc.

Author: Bill Nuffer, Deister Electronics USA, Inc.
Telephone: +1-209-772-0946
email: bnuffer@alum.mit.edu

BACKGROUND:

There exist a large number of technical and market options available with various forms of Smart Card technology and how those different options are presently playing out in the marketplace.

This white paper will outline, in brief, these critical differentiators. It will describe the general characteristics of each and summarize how the market is approaching these differentiators to date;. It will also describe existing and evolving industry capabilities in each arena. The areas that will be covered are:

- ✓ **Open versus Closed Smart Card Systems**
- ✓ **Encrypted versus Non-Encrypted and the role of Authentication**
- ✓ **Serial Number versus Sector Reading/Writing of Smart Cards**
- ✓ **The role of other technologies in the Smart Card Arena**
- ✓ **The role of expanded Smart Cards in Convergence**
- ✓ **The role of expanded Smart Cards in Government Security Programs**
- ✓ **Making Decisions in an Interrelated Option Matrix**

This is by no means an exhaustive treatment of the Smart Card topic; books have been written and the technology continues to evolve. However, it highlights some of the major criteria used by most markets in judging the appropriateness of a Smart Card technology and the decisions of how it is applied.

OPEN versus CLOSED:

This question has three dimensions:

1. The first dimension is the **level of proprietary** and it has three characteristics. They are:
 - a. **Open:** This is a published standard that is available to anyone. It is usually published under the auspices of ANSI and/or ISO procedures and is thus guaranteed to always be open even as it undergoes changes and additions. Good examples are ISO 15693 (Smart Tags) and ISO 14443 (Smart Cards).
 - b. **Available Proprietary:** These are standards developed by a specific company or consortium and comprise intellectual property owned by that entity. However, available proprietary technologies are always licensed to “qualified” other companies in the field. These standards and technologies thus become “effectively open” in that they are available to a sufficiently large (and expanding) group of manufacturers and developers, so that users of the technology have a choice of vendors and the technology continues to be spurred in its development. Good examples are Mifare® and the sector designs of Infineon and Philips ISO 15693 cards.
 - c. **Hyper Proprietary:** These are standards (or sometimes simple encrypted road blocks) put in place by a manufacturer or consortium with the specific purpose of protecting a product or market from competition. Historically, these have taken the form of patents but more recently have

taken the form of protected encryption keys within the rubric of available proprietary technology. These standards force users or systems providers to lock themselves in to a single provider of technology. The effect of this is to normally stifle innovation and preserve higher prices. Occasionally, a hyperproprietary option will come cloaked as Open—at first this may seem counter-intuitive. But opening up applications on otherwise closed systems is becoming common. The real measure of a hyperproprietary solution is whether or not the reader and/or the credential can be purchased from more than one source.

2. The second dimension is a simple one with two characteristic choices:
 - a. **Full Compliance:** This means that when a standard exists (whether Open or Proprietary—although the question is moot for Hyper-Proprietary), the standards is completely complied with. Most Open Standards vendors maintain compatibility with selected partial compliance applications (for backwards compatibility and retro-fit circumstances), But such vendors always engage full compliance with accepted standards in their own offerings to the extent that industry practices allow.
 - b. **Partial Compliance:** For reasons of expediency and/or cost, some technology vendors will only comply with a part of a standard. An example would be a technology which is specified as ISO 15693-2 compliant—meaning that Section 3 of ISO 15693 is not complied with.
3. The third dimension also has three characteristic boundaries. It is the dimension of the **Open/Closed Boundary** and is defined by the three principle characteristics:
 - a. **Totally Open:** This boundary keeps all levels of technology (e.g. sourcing) open down to the End User level, effectively giving the End User the ability to source alternative cards and/or readers for the selected technology. ISO 15693 Serial Number readers effectively are examples of this.
 - b. **Systems Provider Boundary:** This boundary maintains the open (or available proprietary) characteristic down to the system provider level but uses available encryption or other techniques to transition to hyper-proprietary at the level of the Integrator and/or End User. An example of this would be the Mifare Sector technology provided to selected OEMs—where the keys are owned by the OEM; thus protecting their specific card/reader application but the OEM is free to source other Mifare readers/cards.
 - c. **Technology Provider Boundary:** This boundary is set at the technology provider (at least for some portions of the technology—while some portions may remain open) level and locks the systems provider into the technology and provides a direct path from the technology provider to the end user and/or integrator.

Discussion:

The best technology is a combination of True Open and Effectively Open. Modern responsible vendors provide an Open/Closed boundary at either the System Provider or End User Boundary Level depending on the requirements of the customer.

System Providers and Integrators have a decision to make as to what boundary level they wish to close off the open architecture the next level down. This decision has a fundamental trade-off, to wit:

- Lower the Open Boundary: This provides the systems provider and integrator with a powerful sales tool to speak to the open nature of their architecture and the advantages it confers upon their customers:
 - Second sourcing capability.
 - Continued technology development spurred by the competitive aspects of open architecture where development is spurred by competition and broad competence of many entities contributing to the growth of the capability.
- Raise the Open Boundary and effectively furnish a Closed product (at least from the perspective of the End User): This locks the systems provider and/or integrator into the customer once sold—the customer must buy cards and readers unless they make the hard choice of switching total systems. But it also serves as a negative sales feature that must be overcome.

NOTE: Interestingly, it is possible to create closed systems from Open technologies by using combinations of sectors, serial numbers and proprietary reader algorithms. Generally, these aren't ultimately effective but they are possible.

Whichever decision (above) is made, the choice to make it is not available to the Systems Provider and/or Integrator unless the technology is delivered in an open format to them from their vendor. Open Provider vendors have always made the technology available for systems providers to make that decision for themselves.

ENCRYPTED versus NON-ENCRYPTED:

ISO 14443 (A & B) and ISO 15693 technologies offer a choice of encryption versus non-encryption data read/write.

Within specific credentials, portions of a card may be encrypted and portions not encrypted. In addition, writing & reading can be separately encrypted with different keys and in many cases with one encrypted and the other unencrypted.

Levels and types of encryption commonly available in the market today are:

- Mifare®: The Serial Number is not encrypted but each of the sectors is encrypted (although encryption can be turned off for individual sectors). Uses proprietary (but licensable) 48 bit key encryption.
- Hyper-Proprietary Smart Cards: The Serial Number is not encrypted. The ID number is encrypted and the encryption is not openly available (this is the hyper-proprietary characteristic). Other sectors are encrypted or not, depending on application.

- Infineon 10P: Serial Number plus flexible sectors. All unencrypted.
- Infineon 10S: Serial Number unencrypted plus flexible sectors that can be highly encrypted (for security or for setting open boundaries). Uses 64 bit proprietary (but licensable) encryption.
- Philips I-Code®: Currently unencrypted but encryption chips are under development.
- DESFire®: Open standard uses standard DES and triple DES encryption algorithms. Early implementations of TWIC often use this card type.
- SmartMX®: This one of several card types (this is a growing area with new chip vendors entering the arena) that have embedded operating systems. Because it is a programmable platform almost any application (if space allows) including emulating simpler card types can be handled. This is the type of card used in the PIV-II world. (The basic concept behind the government's PIV-II requirements is to be compatible with a large variety of vendors for competitive reasons—a significant parameter for civilian organizations as well).

High end RFID vendors provide products in each of these arenas and work closely with the major chip manufacturers in updating the encryption/authentication algorithms and offerings. A good multi-technology reader will read all of these card types (to some extent) in the same reader so that organizations can easily and cheaply migrate from one technology to another.

SERIAL NUMBERS versus SECTORS:

(Nearly) all Smart Card technologies have both serial numbers (which are invariably open) and sectors (which can be a combination of Open, Proprietary &/or Hyper-Proprietary).

It is critical to be able to read/write and structure sectors within the various smart card technologies.

Use of Smart Cards falls into the following taxonomy:

1. **Serial Number Only:** This is, by far, the most common reader/smart card application. It is not terribly sophisticated and is quite open. It does have the advantage of being easy to understand and does not require any card programming by either the system provider or the integrator. The initial ISO 15693 access control readers and many ISO 14443 readers fall into this category.
2. **Sector for ID Purposes Only:** This the most common use of sectors in security applications. In this case, a programmable credential ID (with a selection of site codes, user codes and other fields) is programmed into a field by the technology provider, the system provider or the integrator. This may be encrypted or non-encrypted depending on the market choices of the end user and others in the market chain. Using a sector product requires a decision about sector structure. Some manufacturers make this decision easy by providing frame structures which allows for a variety of card technologies to be used with a single reader/writer and to contain the cord ID information within this frame technology—further

- increasing the open/closed choices available to the System Provider, Security Director and/or Security Systems Integrator.
3. **Full Sector Programming:** This provides selected points on the market chain the opportunity to create application sectors targeted towards specific uses. These sectors are differentiated technically by:
 - Size**
 - Write Encryption**
 - Read Encryption**
 - Automated or Manual Entry**

Examples of applications include:

- Biometric Templates**
- HR Records**
- Medical Records**
- On Chip Tracking & Time Tagging**

Some manufacturers can a full range of serial number and sector based devices (within Mifare, ISO 14443B, Legic®, and with several ISO 15693 technologies) and, more important, is familiar with the process of key management—a process that requires both management and technological skills to implement and control in a productive fashion.

The choice of serial number and/or sector and/or encryption and/or sector structure and/or point of key management are all areas driven by RFID options and are areas where Systems Providers and Security Directors must make appropriate decisions relative to their market.

SMART CARDS GET SMARTER RFID CREDENTIALS AS CONVERGENCE DRIVERS:

In the last few years, government initiatives, starting with CAC and following by HSPD-12, FIPS 201 and TWIC (with more to follow) have been emerged and now dominate not only the government market security market but impact government contractors and port vendors. The size of this market are creating huge technology and cost impacts on the credential/reader decision making and embedding the IT Director increasingly into the physical security decision making process.

1. FIPS 201 was created principally by the IT side of the government (the various governing documents are, for the most part, government IT documents) in response to HSPD-12.
2. This standard (and many other developing standards) reflect a differentiation between the technology used for Physical Security and that used for IT Security, yet based on a similar platform.
3. The PIV-II card is probably the most advanced of these technologies:
 - a. It used ISO 14443A or B for the contactless Physical Security Interface; and,

- b. A contact card interface for IT purposes. This allows PKI processing to be implemented between the card and the reader/system. NOTE: contactless interface data rates are generally not fast enough (400 KBit/Sec being typically the fastest within the ISO 14443 standard and 106 KBit/Sec being more common.
4. For organizations not requiring the level of IT security specified by the Federal Government, it may make more sense to consider other alternatives:
 - a. Use existing cards but with a glue-on disk/label for a secure contactless ID interface providing IT access. A number of card manufacturers provide “Smart” glue-ons for older proximity cards. These are a quick and modestly priced alternative but do create a somewhat bulky and easily damaged identification solution for converged organizations.
 - b. Upgrade to a basic Smart technology (not all the way to PIV-II or equivalent systems—as these tend to be fairly expensive). This can be a gradual shift (only individual requiring key IT access need be issued these cards to start. Low cost multi-technology readers can allow old and new cards to co-exist to minimize transition costs. This ultimately is the lowest cost solution and allows for an organization to set its own transition rate.

OTHER TECHNOLOGIES IN A COMPLETE SMART CARD RFID FAMILY:

Those of us in the security industry have a somewhat limited view of RFID. We consider it the realm of “Prox” and until recently “Prox” has meant simply, unencrypted 125 KHz applications.

Now the Security Industry has entered into the realm of using Smart Cards for physical security applications. Key to this decision has been the recent ability to purchase Smart Cards and Readers at prices equal to or less than traditional 125 KHz Prox and a trend likely to continue.

But even within Smart Cards, there are other considerations. For example: Legic® has a major market presence in much of Europe and Asia and is now appearing from time to time in North America.

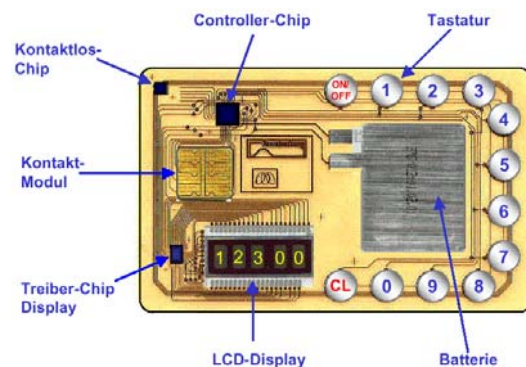


Figure 1: Ultimate Smart Card (Proof of Principle Prototype)

Cards with Operating Systems and both contact and contactless technologies, as a result of government initiatives, are increasingly appearing as well.

Smart Cards and the older Prox technologies all fall within a single rubric: Inductively coupled contactless technologies.

For now these technologies are still adequate to the world of security and in its overlap with IT.

However, there is a new world of RFID as well. The biggest growth area and the fastest development of technology is occurring in the world of "back scatter" (UHF and Microwave):

- The new ePC endeavors may replace barcodes using UHF and very inexpensive (5 to 40¢) tags. The range of this technology (2 meters passive; 8+ meters active) holds promise for security applications as well.
- ISO 18000-6 is a competing alternative in the UHF frequency in both vehicle tracking and supply chain. New technology (patent pending) for weaving UHF antennas into clothing tags to significantly reduce the cost and improve the convenience of using this technology. When used as name sewn name tags, this technology can offer a hands free alternative to traditional credentials.
- Parking and toll collection have opened a big vehicle tracking/ID market in both the UHF and Microwave ranges.

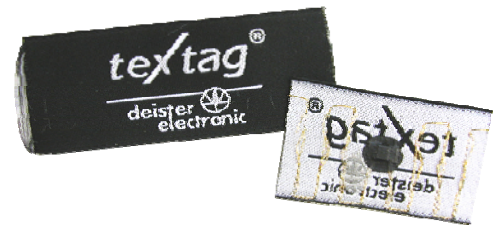


Figure 2: Woven Credential in the UHF RFID Space

Industries, most outside of security, are driving all the above new technologies with more choices, better performance and lower cost.

STRATEGIC DECISIONS FOR THE SECURITY AND IT DIRECTORS:

The overall strategic considerations of System Vendors, System Integrators & Security/IT Directors are not easy to address universally nor in their entirety. The authors recommend that the following be part of the broad strategic considerations of any Stakeholder.

As you plan your broad long-term RFID strategy, make sure it takes into account:

1. Your Open/Closed strategy.
2. Your Sector Utilization & Flexibility Strategy
 - a. Encryption
 - b. Key Management
 - c. Sector Structure and Priority
3. Your Multi-Vendor Strategy
 - a. Which Chip Vendors
 - b. Which Technologies with Which Vendors
 - c. Card Vendors
 - d. Card Families
4. Your Future Technology Road Map
 - a. Which Inductive Coupling Strategies
 - i. 125 KHz & ISO 14443/15693 Combo Readers

- ii. Which ISO technologies
 - iii. What about ISO 14443B?
 - iv. Template Biometric Storage Options
 - b. Back Scatter Technologies
 - i. Vehicle ID Technologies
 - ii. ePC and ISO 18000-6 Integration
- 5. Your Convergence Strategy
 - a. Credentials
 - i. Mutli-Technology
 - 1. One card; or,
 - 2. Add on disk/label.
 - 3. Contact Option
 - 4. Government Mandates
 - a. FIPS 201
 - b. TWIC
 - ii. Migration
 - 1. Cost of Reader Replacement (May be necessary anyway); versus,
 - 2. Cost of Instantaneous Card Replacement; verus,
 - 3. Cost of Card Add-Ons
 - iii. Single-Technology with Multi-Technology Transition enabled by Readers
 - b. Government Compliance
 - Is your organization/customer subject to FIPS 201 and/or TWIC Requirements
 - c. Minimum IT security requirements.
- 6. Final Cost Analysis of likely alternatives.

CONCLUSION:

We have attempted to address these many issues. No one source can provide options so broad that it incorporates every possible permutation of the options available in the Smart Card and RFID world. Rather it is necessary to pick, early on, strategic inflection points that will provide you the greatest long term leverage. This White Paper has been a brief overview of the major considerations.