Access Control Technologies for the Common Access Card

A Study by the Security Equipment Integration Working Group

April 2002

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

1.2 Organization

1.3 Applicability and Scope

2 LEGACY ACCESS CONTROL TECHNOLOGIES

2.1 Magnetic Stripe

2.2 Bar Coding

2.3 Proximity Cards

2.4 Smart Cards and Tokens

3 ACCESS CONTROL SYSTEMS AND THE CAC

3.1 Typical Access Control System Architecture

3.2 Candidate Numbering Schemes

3.2.1 The SEIWG 012 Numbering Specification

3.2.2 The EDIPI Numbering Specification

4 CONTACTLESS ACCESS CONTROL TECHNOLOGIES

4.1 ISO Standards for Contactless Access Control

4.1.1 ISO/IEC 10536 Close Coupling Cards

4.1.2 ISO/IEC 14443 Proximity Cards

4.1.2.1 ISO 14443 Type-A Interface History

4.1.2.2 ISO 14443 Interface Comparison

4.1.3 ISO/IEC 15693 Vicinity Cards

4.1.4 Nonstandard Contactless Technologies

4.2 Comparison of ISO 14443 and ISO 15693

4.2.1 Performance of Compliant Equipment

4.2.1.1 Transaction Speed

4.2.1.2 Read Range

4.2.1.3 Anticollision Techniques

4.2.2 Cost and Availability of Compliant Equipment

4.2.3 Security Techniques and Concepts

4.2.3.1 Data Integrity

4.2.3.2 Dynamic Authentication
4.2.3.3 Key Diversification
4.2.3.4 Nonrepudiation
4.2.3.5 Physical Security
4.2.3.6 Data Security

5 MIGRATION CONSIDERATIONS

5.1 Technical Considerations
5.1.1 Issuance Obstacles
5.1.2 Integration Issues
5.1.3 Field Viability
5.1.4 Security
5.1.5 Biometrics
5.1.6 Numbering Schemes
5.2 Operational Considerations
5.2.1 Guidance Evaluation
5.2.2 Training
5.3 Economic Considerations

6 RECOMMENDATIONS

APPENDIX A: MIGRATION PATH

1 INTRODUCTION

In fiscal year 2001, the Smart Card Senior Coordinating Group (SCSCG) tasked the Physical Security Equipment Action Group (PSEAG) and the Security Equipment Integration Working Group (SEIWG) to research physical access credential technologies and make recommendations for future configurations of the new military identification card, called the Common Access Card (CAC).

The purpose of this investigation was to develop recommendations for access control technologies with reciprocal capabilities between the branches of the armed services. While this goal is broad, the application of the technologies within a specific branch can then be governed by the desires of the branch decision-makers. In other words, the recommended technologies will be the key to the front door. Once inside the door, security tokens and processes will be controlled by each individual branch.

1.1 Background

Currently, the CAC contains multiple data storage technologies. These technologies allow cardholders to access computer networks, sign documents electronically, encrypt email messages, and enter controlled facilities.

A magnetic stripe and contact smart chip can be used on the CAC to store information for physical access control purposes. Unfortunately, these technologies require that contact be made with a card reader to gather cardholder information prior to completing an access control transaction. This contact reduces the life span of the CAC, however, incorporating a contactless technology would reduce wear. As part of this study, an independent team of smart card consultants evaluated all contactless smart card technologies. A technology migration plan was then developed using those results.

1.2 Organization

This section provides a brief introduction to the study. Section 2 summarizes current and future access credential technologies. Section 3 describes a generic Department of Defense (DoD) access control architecture and process and also discusses standardized credential numbering schemes. Section 4 describes contactless smart card technologies. The section identifies the security techniques and concepts used by those technologies to help the reader understand the issues important to selecting a contactless technology. Section 5 details the technical, operational, and economic issues involved in using the CAC as a physical access credential, including issuance, integration, field viability, security, policy requirements, cost, and availability. Section 6 summarizes the recommendations. Appendix A outlines a 5-year migration path highlighting key dates in the process for using the CAC as a physical access credential.

1.3 Applicability and Scope

Critical evaluation criteria were identified at the outset of this study. Prioritization of the criteria helped establish goals, objectives, and an estimated timeline. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence concurred with the study goals and objectives prior to study commencement.

The impact study was divided into six functional areas:

- Technical evaluation of physical access credential technologies
- Assessment of market direction and availability of access control equipment
- Evaluation of backward and forward compatibility with access control security systems
- Determination of the cost impact of potential credential configurations
- Investigation of standard numbering schemes
- Evaluation of DoD security regulations and policies

2 LEGACY ACCESS CONTROL TECHNOLOGIES

Card-based identification systems rely on the reading of a token, which may be a card, key, or tag. These items are encoded with information by special manufacturing equipment. They must have an acceptable level of resistance to copying or transfer of this information onto other cards. Resistance to copying and the physical resilience of the card itself vary between technologies. Different technologies also offer different levels of security and durability.

Many access credential technologies are in use today. The technologies that could be used on the CAC are presented in this section. Because the primary purpose of this study is to evaluate contactless smart card technologies, these receive considerable attention in Section 4.

2.1 Magnetic Stripe

The magnetic stripe card is the most widely used card technology. Magnetic stripe cards are inexpensive, easily manufactured and encoded, and able to carry alphanumeric data. They consist of a magnetically sensitive oxide strip fused onto the surface of a PVC material. The card is encoded by means of bars of magnetized and non-magnetized material on the strip. The magnetized and non-magnetized areas represent the numbers 1 and 0, forming the binary code that is deciphered by the reader on presentation.

The magnetic stripe card has several disadvantages. The card can be physically damaged by misuse. The encoded data can be affected by proximity to magnetic fields. A high volume of equipment is available for the reading and copying cards, so unauthorized duplication and copying is possible.

Currently, the magnetic stripe on the CAC is not encoded. Flash badges with magnetic stripes are utilized in a number of DoD sites for access control. In these locations, the SEIWG 012 number is encoded on the stripe and the reader performs a stripping process to generate a unique credential of the required character length.

2.2 Bar Coding

Barcodes are widely used as an identification technology on ID cards, although they are more common on labels, products, and tags. Traditionally, barcodes were one-dimensional, with meaningful data encoded only in the horizontal dimension of the bars. In other words, any horizontal slice of the barcode contained the same information as any other slice. The information contained by the symbols is limited to the physical width of the printable area. Common one-dimensional symbologies include the Uniform Product Code (UPC), Codabar, and Interlaced 3 of 9. These barcodes could contain alphabetic or numeric data but typically are used for data strings of less than 20 characters.

Two-dimensional barcodes have overcome the limited storage capacity of traditional barcodes by taking advantage of both the horizontal and vertical space. In a two-dimensional barcode, each vertical slice holds unique data. A two-dimensional barcode is like a number of thin one-dimensional barcodes stacked on top of one another. The most common two-dimensional symbology is PDF 417.

Throughout the U.S. Marine Corps, both Interlaced 3 of 9 and PDF 417 barcodes are used for access control purposes. Other branches of service have also used barcodes for access control.

2.3 Proximity Cards

Proximity cards, or prox cards, are read-only devices that are encoded once and then used to transmit a fixed numeric value to a reader. The underlying mechanism is a radio frequency identification (RFID) token, which is embedded in an ID card. The cards contain a chip and an antenna which, when brought within the geographic vicinity of a reader's radio field, enables the card to draw power from the reader to communicate. Though the term can describe other variances of card technology, the typical prox card uses the 125 kHz frequency band. Prox cards are reasonably resistant to counterfeiting, but they do little to protect the data held by the card.

The majority of prox cards are manufactured by HID Corporation, which commands an estimated 80% of the total proximity card market. In 2001, HID reported sales of more than 27 million units (*AVISIAN Inc. Contactless Smart Card Technology for Physical Access Control. April 2002*). Other manufacturers include Indala (formerly owned by Motorola, recently purchased by HID's parent corporation Assa Abbloy), Casi Rusco, and a variety of small volume producers. There is a significant base of deployed HID cards at DoD locations.

2.4 Smart Cards and Tokens

A smart card is a standard-sized plastic card with an embedded integrated circuit (IC) chip. The chip includes components for storing, transmitting, and processing data. Data transfer can be conducted by using contacts on the card surface (contact chips) or electromagnetic energy/radio frequencies (contactless chips).

Smart cards offer significant advantages over conventional magnetic stripe cards. The storage capacity of a smart card is many times greater than that of a magnetic stripe card. Additionally, smart cards can use security techniques to protect their stored data against unauthorized access and tampering.

In addition to reducing the card's lifespan, utilizing a contact chip for access control has traditionally proven cumbersome. The time required to fulfill security requirements (such as encrypted handshaking) between a contact chip and a reader, coupled with the time required for physical insertion of the card into the reader, tends to result in excessively long transaction times. In addition, only one card can be processed at a time. The use of contact chips to control access therefore produces a greater likelihood of long lines and disgruntled customers than the use of contactless technologies.

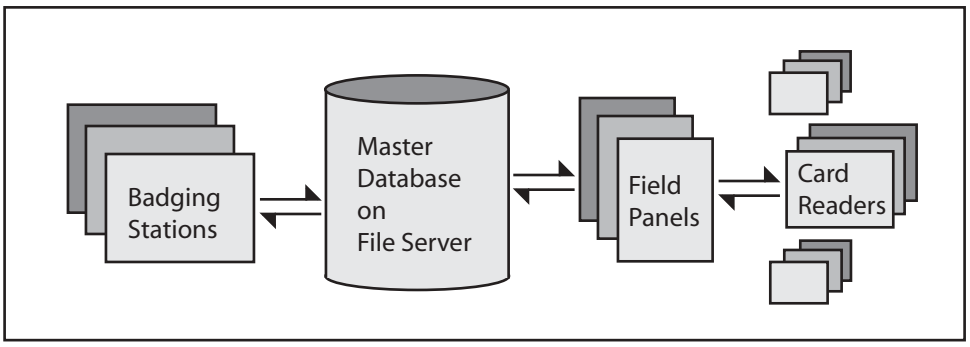
3 ACCESS CONTROL SYSTEMS AND THE CAC

To clearly understand the role of any new access control card, it is important to understand the current status of both the access control market and the DoD's utilization of numbering schemes. In this section, the physical card component is placed into perspective within the framework of typical access control architectures. Additionally, numbering schemes used within the DoD are investigated in reference to their use with an access control credential.

3.1 Typical Access Control System Architecture

A typical access control system architecture has two parts: (1) a card issuance and badging system, and (2) an authorization and privilege control system. A server running specialized software and housing a database of user demographics and assigned rights connects these two distinct functional components.

Figure 1: Typical Access Control System Architecture



The card issuance and badging system creates the physical credential, using data accessed from the database. It also enables the real time addition or updating of data to the database. At the badging station, photos are captured, demographics collected, and access privileges/rights assigned. The physical credential is then printed and encoded.

The authorization and privilege control system consists of a number of field panels sitting between the server and the network of dispersed card readers. When a card is presented to a reader, the reader typically makes the first-level decision based on particular parameters (e.g. the initial agency code, system code). If these parameters are not satisfied, the card is rejected.

If the card passes this first-level decision, the credential number is passed to the field panel using Weigand communication or an RS-232 connection. The field panel checks the credential number against a local list of recently seen credentials maintained in flash memory or an EPROM. The capacity of the field panel is defined by the amount of onboard memory. If the number is found, the credential is approved at the field panel level. If the number is not found, the panel passes the number on to the server. The server checks the database of credentials and the credential is accepted or rejected.

As suggested by this description, the card or token is merely a container for the numeric credential. If a new type of reader (e.g. smart card reader) placed in the field can interpret data from the card or token and communicate with the field panel, then the access control system will operate exactly as it did when magnetic stripe or barcode readers were installed.

3.2 Candidate Numbering Schemes

Regardless of the technology used, the numeric credential must be:

- *Meaningful*. The data must be tied to the individual in a database.
- *Formatted and presented consistently*. The data must have the same length and structure and be located in the same place on all access cards or tokens.
- *Unique*. The data must be tied to a single individual only.

That a numbering scheme must provide meaningful data is obvious and requires no further explanation. The remaining characteristics pose real issues in the DoD environment.

Consistent presentation of data is necessary to ensure that the card reader, field panel, and software can automatically know how to handle the received data. Automatic handling is essential to gathering a valid numeric credential. The credential data should be in the same place on every card and contain the same number of characters encoded in a consistent format. The numeric credential stored in the database does not have to be identical to the numeric credential stored on the card. A long numeric string can be shortened via stripping, truncation, mathematical calculation, or some combination of these techniques. The shorter, "adjusted" number can be used by the access control system. This process can occur at various points in the access control architecture, but most often is accomplished by software at the reader level.

Uniqueness is essential to the use of numeric credentials for individual access control. Each credential can represent only a single individual. Therefore, the credential must have enough characters that a unique credential can be created for every individual in the database. The database must include records both for people with current authorization and, in most cases, records for people with past authorization. In addition, there must be some reasonable allocation for reissued authorizations.

The process for issuing numbers is also of major importance. Software-controlled number assignment is preferable to human-controlled assignment, because it reduces the potential for keystroke or other types of errors. If the assignment responsibility is dispersed across multiple locations, controls must be in place to ensure that two systems do not issue the same number.

3.2.1 The SEIWG 012 Numbering Specification

Currently, DoD utilizes the SEIWG 012 specification. This Prime Item Product Function Specification, developed by the Security Equipment Integration Working Group, went into effect on 28 February 1994. SEIWG 012 specifies a 40-digit credential, to be encoded on all magnetic stripe cards used for access control within any service branch.

The 40-digit credential includes the following elements:

- A 4-digit agency code identifying the government agency issuing the credential.
- A 4-digit system code identifying the system in which the card is enrolled.
- A 6-digit credential number, assigned by the issuing agency. The number is unique within the set of numbers issued by that agency.
- A single-digit ICI indicating the number of replacement cards issued to the individual (due to card loss or damage).
- The individual's 9-digit social security number. This element currently contains zeros due to privacy concerns.
- A 7-digit element reserved for future use.
- The remaining characters serve as data separators.

The SEIWG 012 numbering scheme was designed to create a sufficiently long credential to ensure non-replication and provide key data on the background of the credential and the credential's holder. Because access control systems frequently strip, truncate, or otherwise reduce credentials, SEIWG 012 should continue to function appropriately as the numeric credential. SEIWG 012 does not need to change to accommodate the system modification, but the approach to how the system uses the SEIWG 012 data must be defined.

3.2.2 The EDIPI Numbering Specification

The Electronic Data Interchange Person Identifier (EDIPI) is a unique, 10-digit index number assigned to every person enrolled in the Defense Enrollment Eligibility Reporting System (DEERS) database. Data entry errors and the non-uniqueness of the social security number led to the development of the EDIPI in 1999. The number is created by an Oracle database to ensure its uniqueness.

The EDIPI is used by all CAC technologies except the magnetic stripe. Those technologies include the contact chip, the PDF 417 bar code, and the Interlaced 3 of 9 bar code. It may serve as the common personnel systems identifier in the future. The number is not classified because it is simply an index to an individual's information in the DEERS database.

4 CONTACTLESS ACCESS CONTROL TECHNOLOGIES

Contactless cards consist of a coupling element and an electronic microchip (smart chip). The cards use radio frequencies to transfer data between the data carrying device (smart chip) on the card and the reader.

There are two kinds of contactless chips: passively powered and actively powered. Passively powered chips do not include a power supply and must use the electromagnetic energy (inductive coupling) transmitted by the reader. Actively powered chips include their own power supplies. This study reviews only passively powered chips because actively powered chips have proven unacceptable for use in individual access control situations involving ID cards.

Much of this section is based on the information found in the report "Contactless Smart Card Technology for Physical Access Control," produced by AVISIAN Inc. and issued on April 1, 2002.

4.1 ISO Standards for Contactless Access Control

Three contactless technologies have received standard classification from the International Organization for Standards (ISO). This section describes the three standards and also summarizes the major nonstandard contactless technologies.

The three standard contactless technologies are:

1. ISO/IEC 10536 close coupling cards
2. ISO/IEC 14443 proximity cards
3. ISO/IEC 15693 vicinity cards

4.1.1 ISO/IEC 10536 Close Coupling Cards

The ISO/IEC 10536 close coupling card technology standard (ISO 10536) was the first contactless standard to be developed. ISO 10536 cards must either be inserted into a slot or placed on the surface of the reader. This scenario illustrates the drawbacks that have discouraged the use of contact cards in access control environments: the requirement for short reading distances and extremely accurate placement of the card.

The ISO 10536 standard has not been accepted by industry and, at this date, only a small project in Asia is still using the technology (*Christian, Francis. Chairman of B10.5 Group and Head of U.S. Delegation to WG8. Personal interviews. Feb. 2002*). Cards meeting the ISO 10536 standard should not be considered for new applications such as the CAC for the following reasons:

- No chip manufacturer currently produces the electronic circuit required for the cards.
- The technology is not being used in the open market to any significant extent.
- The card and reader require precise alignment in order to function, making ISO 10536 less user-friendly than other contactless technologies.

4.1.2 ISO/IEC 14443 Proximity Cards

The ISO/IEC 14443 proximity card technology (ISO 14443) has been used for the overwhelming majority of contactless card deployments. The targeted range of operations for this standard is from 0 to 10 cm, although this range varies, depending on power requirements, memory size, CPU, and co-processor. ISO 14443-2 allows for two types of interfaces, referred to as Type A and Type B.

4.1.2.1 ISO 14443 Type A Interface History

ISO 14443 Type A cards are commonly called MIFARE® cards. In 1994, when the standard was first being discussed, an Austrian company called Mikron worked alongside the standards body. Mikron's intellectual property (IP) contributed to the development of the standard, and the company benefited from having its patented IP (the MIFARE® technology) incorporated into the standard.

This situation is not uncommon in the development of standards. The guiding rule is that the company owning the IP must agree to make the technology available to the market at a fair and equitable price. Mikron's Mifare® technology therefore became available for licensing following the publication of the ISO 14443 standard.

The overwhelming majority of Type A cards issued to date are MIFARE® cards. MIFARE® is Type A compliant, but it uses a distinct command set and encryption technique, elements not specified by the ISO 14443 standard. It is possible to produce Type A cards that are not MIFARE® cards, however, the name MIFARE® has become synonymous with Type A due to its market dominance.

In 1995, Philips Semiconductors acquired Mikron and as a result is positioned to receive royalties from the deployment of the MIFARE® technology. It is important to note that Philips has not charged or collected any license fees for MIFARE® to date *(AVISIAN Inc. Contactless Smart Card Technology for Physical Access Control. April 2002)*. If Philips begins to assess a license fee in the future, the fee will be paid to Philips by the chip manufacturer, not borne directly by the end user, issuer, or card manufacturer. The license fee will be extremely modest, reportedly less than $0.01 for each integrated circuit (IC) and will not significantly impact total cost of ownership. By ISO specification the license must be negotiated "under reasonable and non discriminatory terms and conditions" *(ISO/IEC 14443-2)*.

4.1.2.2 ISO 14443 Interface Comparison

The ISO 14443 Type A and Type B interfaces originated as complementary technologies. Type A began with memory cards only. Type B was originally developed as the microprocessor alternative to Type A.

In recent years, both microprocessor and cryptographic cards have been developed for Type A. Philips and Infineon produce the majority of Type A chips.

Type B development began in 1995. Just as additional card varieties have been added to Type A, Type B has expanded from its beginnings as a microprocessor-only card to

include both a memory and cryptographic option. The majority of chips for Type B cards are provided by STM, Infineon, Samsung, and Atmel.

With the addition of other card types, what started out as complementary technologies—Type A as a lower cost memory card and Type B as a higher security microprocessor card—became rivals in the marketplace. Type A tokens have captured the majority of the worldwide market for contactless identification technologies, accounting for 80%, or an estimated 200 million units *(Philips Electronics. Corporate Web Site. http://www.semiconductors.philips.com/news/content/file_798.html.February 2002)*. The remaining 20% of the market is shared mainly between Type B cards and two proprietary cards: Cubic's GO-Card and Sony's FeliCa card.

4.1.3 ISO/IEC 15693 Vicinity Cards

The ISO/IEC 15693 vicinity card technology (ISO 15693) was developed in response to the industry's desire for a contactless card technology with an operational range greater than 10 cm. The vicinity card has three modes of operation: read mode, authenticate mode, and write mode. The maximum stated ranges are 70 cm for read mode, 50 cm for authenticate mode, and 35 cm for write mode.

ISO 15693 allows cards to operate at longer distances than ISO 14443 cards. The ISO 15693 standard was originally envisioned as a fare collection tool for longer ranges and/or an inventory control tag. For fare collection, users would actively present the card as they entered a bus or train and be reidentified as they passed though a large read field on an exit door. Users would not need to re-present the card, as it could be read from a pocket, wallet, or purse. However, it is still uncertain what, if any, security problems are introduced by the longer communication distances.

4.1.4 Nonstandard Contactless Technologies

A number of proprietary contactless interfaces are used in the industry in addition to the standardized contactless techniques described above. Two common technologies are Cubic Corporation's GO-Card, used primarily in the United States and England, and Sony's FeliCa card, used in Hong Kong and several Asian countries.

In general, these proprietary technologies are variations on ISO 14443 that use nonstandard bit rates and/or bit encoding methods and lack a subcarrier. Recent attempts by Cubic and Sony to receive standards classification for these products under ISO 14443 were unsuccessful.

4.2 Comparison of ISO 14443 and ISO 15693

This section compares the candidate technologies identified in Section 4.1 (ISO 14443 Type A, ISO 14443 Type B, and ISO 15693). The metrics used are:

- Performance of compliant equipment
- Cost and availability of compliant equipment
- Security techniques

4.2.1 Performance of Compliant Equipment

This section analyzes the performance of equipment compliant with the three contactless technology candidates (ISO 14443 Type A, ISO 14443 Type B, and ISO 15693) on the basis of transaction speed, read range, and anticollision techniques.

4.2.1.1 Transaction Speed

In general, a data exchange transaction can be broken down into four events: input/output (I/O), memory access, encryption, and processing. Each of these events takes approximately one-quarter of the total transaction time.

A significant factor in determining transaction speed is bit rate–the rate at which data is transferred between the card and the reader. Both ISO 14443 variations have the identical bit rate: 106 kb/s. The ISO 15693 standard specifies a significantly lower bit rate, not exceeding 26.69 kb/s. Thus, ISO 14443 transactions are significantly faster than ISO 15693 transactions.

However, transaction speed in the field is also determined by the volume of data involved in a transaction. Highly secured financial transactions using an e-purse transfer a great deal of data between reader and card. Access control transactions typically transfer much less data. Once communication has been established and approved, only an encrypted unique identifier must pass from the card to the reader; reader-to-card communication may involve only a status code.

Thus, while ISO 14443 calls for significantly faster transaction speeds, noticeable differences in the field will depend largely on how much data is involved in the transaction.

4.2.1.2 Read Range

The read range for a contactless card is the maximum distance between the card and the reader within which a transaction can be successful. The read range specified in ISO 14443 (both Type A and Type B interfaces) is up to 10 cm. For ISO 15693 cards, the read range varies: 70 cm in read mode, 50 cm in authenticate mode, and 35 cm in write mode.

However, the ranges listed in the standards documents are targets, not guarantees. The actual read range experienced in the field depends on a number of factors. One is the energy required to power the card, which depends on the chip type and manufacturer and can even be different for cards in the same lot. The greater the amount of power required, the shorter the read range.

Another factor affecting read range is whether the card is a microprocessor card or a memory card. Microprocessor cards have a shorter practical read range than memory cards, because additional power is required to process data on the card. Though it would be unlikely for a user to notice the difference in the field, an ISO 14443 microprocessor card would actually need to be held closer to the card reader than an ISO 14443 memory card.

The ISO 15693 standard was originally envisioned as a solution for applications requiring longer read ranges, such as inventory tracking. However, a longer read range without deliberate card presentation could prove problematic. Such a scenario may not provide an acceptable level of security, allowing users to simply pass through security points without the active presentation of their card/credentials or to have their card read without their knowledge.

In the past, read range was of greater importance due to the process used to present a contactless card to a reader. It was long assumed that waving the card through the invisible field surrounding the reader was the proper means to present a card. When a card is waved, however, its actual time within the field can be just milliseconds. Today, most projects are training cardholders to tap the card on the face of the reader. This "tap-and-go" process results in the card remaining in the reader field for a longer period of time.

Presenting and withdrawing the card perpendicular to the reader makes it difficult to remove the card from the field in much less than one full second. This provides ample time for a successful card read and renders the practical concerns over read range somewhat moot. Though the read range for ISO 15693 cards is undeniably larger, the ISO 14443 read range is more than adequate for access control situations involving active card presentation by the individual.

4.2.1.3 Anticollision Techniques

Anticollision techniques are used when two or more cards respond to a reader's request for data transfer at the same time. Obviously, the longer the read range, the more likely a scenario in which collisions can occur. Similarly, longer transaction times increase the likelihood of collisions. Even with contactless technologies that employ relatively short read ranges and short read times, anticollision techniques are essential to ensure successful transactions when multiple cards enter the reader's field concurrently.

In contactless systems, the reader initiates the communication, asking cards in its field to identify themselves. When only one card is present, the communication returned to the reader is understandable, assuming the card type is familiar to the reader. When more than one card is present, all cards respond to the reader's request, making it difficult for the reader to interpret the responses. The reader, recognizing this as a potential collision situation, initiates an anticollision scheme.

ISO 14443 Types A and B both employ an anticollision scheme called the Bit Collision method. The reader ignores the jumbled responses and sends out a new request. Rather than requesting all cards to respond, the new request asks for any cards within a specific numeric sequence to respond. If this request returns a clear response, then one of the cards has been identified. The reader then asks for any cards within another numeric sequence to respond. This process continues until all cards have been inventoried. At that point, the reader knows how to manage the completion of all transactions.

The entire process is extremely rapid. In general, the inventory process takes only 5 milliseconds plus 1 or 2 additional milliseconds per card present in the field. In practice, the time required to conduct this anticollision process is not noticeable to the cardholder.

It should be noted that ISO 14443 allows for an alternative anticollision method, called the Time Slot method. Using the Time Slot method, the reader requests cards to respond at slightly different times after a collision has occurred. The reader can then read one card before transferring data from any other cards present in the field. However, nearly every implementation of ISO 14443 uses the Bit Collision method rather than the Time Slot method.

ISO 15693 utilizes the Slot Marker method for anticollision when multiple cards are present within its read/write field. This technique calls for the reader to inventory the cards. The reader then commands each card to send a response in a specified slot, a process that is repeated until each card is identified independently.

In general, any of these anticollision techniques are more than adequate to meet the speed and integrity requirements of a secure access control situation. The important point is not which anticollision technique is employed, but rather that the technology selected makes use of an anticollision technique. All three technologies being considered in this evaluation—ISO 14443 Type A, ISO 14443 Type B, and ISO 15693—handle anticollision needs adequately for physical access control applications.

4.2.2 Cost and Availability of Compliant Equipment

This section summarizes the cost and availability of equipment compliant with the three candidate standards.

In order of cost from least to most expensive, the options include:

- Low cost: ISO 15693 cards; ISO 14443 Type A and Type B memory cards
- Mid cost: ISO 14443 Type A and Type B microprocessor cards
- High cost: ISO 14443 Type A and Type B dual interface cards

Production volume is often the key to availability of components. Of the three candidate technologies, the ISO 14443 Type A product dominates, with an overwhelming 80% market share (see Section 4.1.2*)*. Several large card manufacturers offer the finished cards, a number of reader manufacturers build compatible access control readers, and other readers are available for additional uses such as point-of-sale acceptance and network security.

Certain non-eligible CAC personnel also require access to DoD facilities. Therefore they must be escorted or issued a “CAC-like” credential to gain access. “CAC-like” cards must be acquired to satisfy this requirement. A large supply of low cost ISO 14443 cards is available for purchase because of the technology’s popularity in both the access control and transit industries.

4.2.3 Security Techniques and Concepts

This section evaluates the security techniques used by the candidate technologies to safeguard identification, authentication, and data transmission. Security is described in the following terms:

- Data integrity
- Dynamic authentication
- Key diversification
- Nonrepudiation
- Physical security
- Data security

4.2.3.1 Data Integrity

Data integrity verifies that data has not been modified or assures that data has arrived intact, with no tampering or corruption. To achieve data integrity electronically, data is encrypted using a cryptographic algorithm. There are two categories of cryptography, private key and public key.

Private-key or symmetric-key cryptography is a scheme in which the same key is used for both encryption and decryption. This category includes the Data Encryption Standard (DES), triple DES, and the Advanced Encryption Standard (AES) that will replace DES when the standard is adopted on May 26, 2002 *(National Institute of Standards and Technology. Federal Information Processing Standard [FIPS] publication number 197. Nov. 2001)*. Triple DES is expected to remain an approved algorithm for U.S. Federal Government use for the foreseeable future *(National Institute of Standards and Technology. Web Site. http://csrc.nist.gov/encryption/aes/aesfact.html, March 2000*).

Public-key or asymmetric-key cryptography is a scheme in which each user has a public key and a private key. The public key is distributed to others while the private key remains secret. One key is used for encryption; decryption utilizes the other key. Examples include RSA, Elliptical Curve Cryptography (ECC), Diffie-Hellman key management protocol, and the Digital Signature Algorithm (DSA, used for signatures only, not encryption). ECC has become a popular method and is supported by a number of IC providers, with dedicated cryptographic engines resident on the chip.

4.2.3.2 Dynamic Authentication

Dynamic authentication means that the challenge and response between the card and reader change with each transaction. This is possible with the use of a random number generator to produce the session key for each transaction.

Card cloning is a concern in the use of a smart card and is one reason why dynamic authentication is important. Dynamic authentication also helps prevent a transaction session from being recorded and used as the basis for a real transaction.

4.2.3.3 Key Diversification

A random number generator must be used for dynamic security as it generates unique keys for each session.

4.2.3.4 Nonrepudiation

Nonrepudiation is achieved through cryptographic methods that prevent an individual or entity from denying previous participation in a particular transaction. The fact that a third party can verify your authentication (e.g. your signature) on a transaction means that you cannot deny participation in the transaction.

4.2.3.5 Physical Security

Physical security of the IC chip prevents unauthorized access to read or modify stored data. Physical security is implemented by using various sensors, including voltage, frequency, light, and temperature. In addition, the layout of the chip is modified, so that the data paths are hidden, and the IC is interlaced with random false function, to hide the actual operation.

4.2.3.6 Data Security

Authentication and encryption are performed with a key-based cryptographic function. The keys are generated by a random number generator that is designed as part of the IC. The key or number is then incorporated into an algorithm residing on the IC. The algorithm function is computationally intensive and should be supported by a dedicated hardware co-processor. The circuitry involved is specially designed to perform the complex computation and makes using the supported cryptography viable without affecting transaction time and power consumption.

5 MIGRATION CONSIDERATIONS

Many issues arise when considering initial implementation of a contactless access control technology. Still others emerge in situations requiring transition from another (or multiple other) identification technologies to a contactless technology. While the full array of potential issues cannot be known until a project is undertaken, this section summarizes a number of key considerations.

5.1 Technical Considerations

5.1.1 Issuance Obstacles

The major question that must be addressed regarding issuance is timeliness—how long it will take to personalize the contactless portion of the CAC. The answer will be influenced by the nature of the data encoded on the contactless chip (e.g. SEIWG 012, EDIPI, biometrics), whether the contactless portion must be part of the CAC issuance, and the performance abilities of the equipment used. The Defense Manpower Data Center (DMDC) is very motivated to maintain or improve upon the current card issuance time of approximately 10 minutes per card (*Dixon, Mary. Director, Access Card Office, U.S. Department Of Defense. Presentation At Smart Card Alliance Conference. February 2002*). Care must be taken to ensure that the integration of the contactless process into the existing Realtime Automated Personnel Identification System (RAPIDS) production environment does not have an unacceptable impact on throughput.

5.1.2 Integration Issues

Legacy systems pose significant issues for the conversion of access control technologies. Specific integration considerations include:

- Logistical process for replacement of a widely deployed and diverse reader infrastructure.
- Communication protocol changes and the impact on existing infrastructure.
- Timelines and technical realities for supporting multiple tokens/credentials during a transition period.

5.1.3 Field Viability

The unique properties of the CAC and its operating environment will make it necessary to independently evaluate the field viability of the contactless module, the plastic that contains it, and the CAC chip. In other words, the work already done to ensure field viability of the CAC has presumably not reflected the impact of adding a contactless chip and antenna to the card. Other factors to be evaluated include durability and resistance to wear, delamination, antenna breakage, and contact chip displacement.

Extensive testing must also be performed to ensure proper operation of the contactless reader in the various DoD environments, particularly those not currently supporting contactless access control applications. For example, if ISO 14443 A or B is chosen,

past operation benchmarks for 125 kHz readers and cards will not be applicable. Further, performance benchmarks for existing deployments of ISO 14443 devices may not be applicable to the electro-mechanical environments found in other DoD installations around the world.

5.1.4 Security

The data security issues that are germane to the protection of information in general are equally critical to the protection of data involved in a contactless smart card transaction. These issues include confidentiality, integrity, authentication, non-repudiation, and reliability. See Section 4.2.3 for details.

5.1.5 Biometrics

Biometrics are methods used to recognize someone based on a physiological or behavioral characteristic. Common physiological biometrics include fingerprints, hand geometry, iris recognition, facial characteristics, and retina scanning. Behavioral biometrics include signature, keystroke pattern, and voice recognition. Issues to be considered include the size of the biometric template, its location either on or off the card, and the source of encryption (either on or off the card).

5.1.6 Numbering Schemes

The selection of a numbering scheme is a key decision, with both operational and technical implications. An overview of this topic is presented in Section 3.

5.2 Operational Considerations

5.2.1 Guidance Evaluation

A comprehensive investigation of governmental regulations, policies and directives was conducted to identify any guidance that may prohibit use of contactless smart card technology. The guidance includes all security-related guidelines from the DoD, its services, and the General Services Administration.

Most security regulations were written before smart card technology was a viable solution for access control, so they do not specifically refer to contactless smart card technology. However, contactless smart cards offer a higher level of transmission and data storage security than existing access control technologies. Therefore, we believe that future regulations will approve the use of contactless smart card technologies for physical access control.

Numerous existing policies and directives provide guidance to DoD services concerning the issuance and use of the CAC. However, there are no statements in the guidance we reviewed that prohibit the use of a smart card technology for physical access control.

5.2.2 Training

Training will need to include field support, system administration support, and user training for use of a contactless access card. Contactless technology is relatively easy to use, but its adoption will still require user education regarding issues such as card placement, proximity to the reader, and transaction time.

5.3 Economic Considerations

Contactless standards were investigated with regard to their economic implications to the DoD efforts. Estimates for the cost of the evaluated technologies in addition to the cost of the contact chip card component of the CAC are presented in the following table. Every attempt was made to obtain relevant and reliable cost estimates. Because some vendors were hesitant to provide figures, however, meaningful comparisons were often difficult to obtain. Additionally, the number of vendors whose products are approved by the GSA and FIPS certification process is limited. In all cases, the figures presented were provided in writing by a vendor representative. All can be described as good estimates, although any further claim to accuracy would be suspect.

Figure 2. Per card price increases for contactless technologies

	Per Card Price Above CAC	
14443 A Memory	**$2.51**	(1)
14443 B Memory	**$2.51**	(2)
125 kHz Proximity	**$4.22**	(3)
125 kHz + 14443 A Memory	**$8.50**	(4)

Notes:

(1) A price estimate within 10% of this figure was provided by both Schlumberger and Gemplus. The price delta was calculated by subtracting the previous CAC price estimate ($6.80 per card) from the finished card price that was inclusive of contact chip, card body, and 14443 A Memory insert.

(2) This price estimate was provided by Schlumberger and calculated in the manner described in (1).

(3) This price was calculated by adding the estimated price of a 125 kHz proximity card (one million quantity) provided by HID Corp. and a $0.50 fee for embedding the contact chip (the fee for this additional labor is estimated from information provided by industry sources).

(4) This price was calculated by adding the estimated price of a combined 125 kHz prox and 14443 A Memory card (one million quantity) provided by HID Corp. and a $0.50 fee for embedding the contact chip (the fee for this additional labor is estimated from information provided by industry sources).

6 RECOMMENDATIONS

This document is the result of a major effort by the SEIWG to investigate available access control technologies, identifying the most appropriate option for DoD needs and the CAC platform. The following eight recommendations are based on the findings of this project.

Recommendation 1:
Utilize ISO 14443 contactless technology

The ISO 14443 contactless standard should be used as an access control technology on the CAC. Either a Type A or Type B interface will adequately address identified access control needs.

Recommendation 2:
Require open command sets to ensure compatibility between card buys

The vendor awarded the contract should be required to make available (at no cost and for any purpose) the specific command set used, along with any other information that differentiates the cards via items not specified in the ISO 14443 standard.

Recommendation 3:
Specify multitechnology card readers

Multitechnology card readers accepting, at a minimum, ISO 14443 Type A and ISO 14443 Type B, should be required. A thorough consideration of readers that will accept one or more additional technologies should occur prior to specifying the readers for procurement.

Recommendation 4:
Support legacy access control technologies through FY-05

Legacy access control technologies should be supported during a transition period but phased out by the close of Fiscal Year 2005.

Recommendation 5:
Establish a certification process for CAC contactless elements

The Department of Defense should assign responsibility for certifying that all cards and readers purchased for the CAC program operate with those purchased previously. This responsibility should be assigned to an existing certification organization such as the Joint Interoperability Test Command.

Recommendation 6:
Task SEIWG to recommend the most appropriate numbering scheme

The SEIWG should undertake the development of a standard numbering scheme to be used for all future access control and card issuance needs.

Recommendation 7:
Approve the addition of 125 kHz proximity technology

Support for the addition of 125 kHz proximity technology to the CAC is contingent upon a determination of economic feasibility.

Recommendation 8:
Create contactless technology review process
Establish a process for the periodic reevaluation of contactless technologies to ensure that matured technologies are fielded as they become available.

APPENDIX A

The schedule for the inclusion of the contactless component into the CAC is agressive. As suggested in the timeline below, it is crucial to meet the dates mandated by the second CAC buy if access control needs are to be met with contactless technology before FY 2005. This is the case because the pending buy will establish capabilities for cards distributed in much of 2003, all of 2004, and the majority of 2005 as well.

It seems unlikely that the required evaluation and specification process for a biometric indicator to be included on the CAC would be completed prior to Q3 of FY 2004. This would leave just one year until the new cards–those specified in the third buy–would begin to be issued. Thus it is logical to avoid an attempt to speculate on the needs of the future biometric indicator in this second card buy. To do so would increase the cost per card of this buy significantly.

Figure 3. High level CAC timeline