AU/ACSC/083/2001-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

IMPLEMENTING SMART CARDS

INTO THE

AIR FORCE RESERVE

by

Keith D. McClannan, Major, USAFR

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major Ronald Olienyk

Maxwell Air Force Base, Alabama

April 2001

Distribution A: Approved for public release; distribution is unlimited.

IBM v. Digital Doors,
IPR2023-00972, 7,958,268
DigitalDoors EX2012

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	4/1/2001	Research Paper 4/1/2001

4. TITLE AND SUBTITLE
Implementing Smart Cards Into the Air Force Reserve
(AU/ACSC/083/2001-04)

5. FUNDING NUMBERS

6. AUTHOR(S)
McClannan, Maj Keith D.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Command and Staff
College, Air University
Maxwell Air Force Base,
Alabama

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

Smart card technology is essentially about a credit card with a brain.Smart cards have an embedded microchip that allows the card to hold digital data up to the available memory installed on the card.Smart cards first became popular in the financial industry in Europe, however,they have quickly gained favor in the United States.1
The Department of Defense (DoD)also saw the utility in using smart card technology.The DoD began tests with smart cards that sought to take advantage of the many capabilities present
in this technology.Not merely content to use the card as just an identification (ID)card,the
military wanted to exploit the smart card ‘s ability to store large amounts of encrypted data In

14. SUBJECT TERMS
IATAC Collection, smart cards

15. NUMBER OF PAGES
29

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

IBM v. Digital Doors,
IPR2023-00972, 7,958,268
DigitalDoors EX2012

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

Smart card technology is essentially about a credit card with a brain. Smart cards have an embedded microchip that allows the card to hold digital data up to the available memory installed on the card. Smart cards first became popular in the financial industry in Europe, however, they have quickly gained favor in the United States.[1]

The Department of Defense (DoD) also saw the utility in using smart card technology. The DoD began tests with smart cards that sought to take advantage of the many capabilities present in this technology. Not merely content to use the card as just an identification (ID) card, the military wanted to exploit the smart card's ability to store large amounts of encrypted data. In particular, DoD is intending to use smart cards to replace current ID cards for all active and Reserve members, plus use them to allow access to computer networks, maintain personnel and medical records; and with such capabilities, attempt to ease the burden to the military member during deployment processing.[2]

The intent of this research paper is to explore the smart card story, with a particular emphasis on how implementation is effecting DoD, the Air Force, and the RC.

Notes

[1] www.scia.org
[2] Deputy Secretary of Defense memorandum dated 10 Nov 99

Contents

Page

DISCLAIMER ii

ACKNOWLEDGEMENTS iv

ABSTRACT v

SMART CARDS – THE TECHNOLOGY BEHIND THE CARD 1

IMPLEMENTING SMART CARDS IN THE DOD 7

SMART CARD INITIATIVES AND TESTS IN THE DOD 12

CONCLUSION AND SUMMARY 20

GLOSSARY 23

BIBLIOGRAPHY 24

Acknowledgements

This research paper started with an idea from Major Ellen Fiebig, USAFA. She and I spoke during an Air Command and Staff College (ACSC) orientation at Washington, D.C., and she indicated she was looking for a student to research issues surrounding smart cards. As I had some familiarity with this technology from having seen smart cards being implemented through a program at the United States Central Command (USCENTCOM), I told her I would be willing to conduct research into how the Reserve Component (RC) was implementing smart cards.

I would especially like to thank Major Ron Olienyk from the ACSC faculty for his continuing guidance throughout the life of this project. From conception to conclusion, he always made himself available for questions, and for that, I remain indebted to him. Similarly, I wish to thank Ms. Pam Hollabaugh for her expert assistance in navigating my way through the ACSC research template. Ever cognizant of the fact that I was one of probably 135 research students who continued to vie for her time, she maintained her pleasant demeanor every time I spoke to her. Her technical expertise made even the most difficult computer software problem disappear.

Finally, I wish to acknowledge the continuing support of my wife, Kathy, and daughter, Kristen. Even though we are separated by 500 miles, they have rallied behind me and kept my spirits high. I could not have completed this paper, or the rigorous ACSC curriculum, without their unfailing support.

IBM v. Digital Doors,
IPR2023-00972, 7,958,268
DigitalDoors EX2012

Chapter 1

Smart Cards – the Technology behind the Card

Smart cards have been a part of the global economy ever since the banking and financial industries learned of their capabilities. Rather than customers using traditional currency, European companies' in particular leveraged key aspects of smart cards in order to encourage their use. Using the security inherent in these new digital wonders called smart cards, consumers no longer had to ensure they carried various denominations of currency to get them through the day. The financial industry particularly liked one aspect of the smart card - the ability to track a consumer's spending habits, and that in most cases, transactions conducted with smart cards were secure and therefore absent from fraud. But the real question for smart cards was to determine how far this technology could be pushed. For the DoD, the answer lay in years of development and testing, to where finally, the military felt that smart cards could be **the** single card to replace the military ID card for active duty and RC personnel, with potential follow-on applications in later years. But is this wholesale replacement of ID cards for RC personnel the panacea envisioned, or are there more questions to be answered? The answer lies in knowing the capabilities offered by smart cards, and in particular, what key questions need to be asked about our RC personnel to ensure their specific concerns are addressed in any implementation plan. What follows next in this chapter is a review of the history of smart cards since their inception,

and a look at the particular technology that has enabled smart cards to become such a pervasive force in this new century.[1]

Smart card technology began its life overseas when various inventors in Germany, Japan and France filed the original patents. Due to constraints imposed primarily by the lack of experience in the semiconductor industry, smart cards did not really come into favor until the mid 1980's. Once the initial technological hurdles had been cleared, the French financial and telecom industries began to flood the market with these new cards. The public was quick to accept this new technological innovation, especially as it offered a realistic option to carrying large amounts of cash. The net result was that the smart card industry has blossomed, allowing more than one billion cards per year to be shipped since 1998.[2]

There are basically two types of smart cards that are being used today. They are known as contact and contactless cards. The contact card requires that the card be inserted into a reader, which allows a direct connection to the embedded computer chip. Through this physical contact, the card can have data transferred to it or read from it. The other option, the contactless card, only requires close proximity to a reader to do its job. In this case, both the reader and the card have antenna that allows the transfer of data to take place. Most of the contactless cards obtain their power for the embedded microchip through the proximity of the electromagnetic signal. The ideal range for this to happen is about two to three inches, making this type of card the card of choice for use in point of sale type situations.[3]

There are also two additional categories of cards in use today. They are the Hybrid and Combi cards. The Hybrid card has two chips, each having a respective contact and contactless interface. While the two chips are not connected, they serve their separate purposes for the industry. The newer Combi card has a single embedded chip, but in this case has both a contact

and contactless interface. The advantage to having the Combi card is it allows access to either chip interface, contact or contactless, with a very high level of security (inherent in its design architecture). In particular, these features alone make the Combi card attractive to the banking industry and to the military that have a need for such security.[4]

The embedded chip found in smart cards typically falls into one of two categories. These are memory chips and microprocessor chips. Memory chips can be thought of as being similar to a floppy disk (due to their data holding size), but it should be noted they have optional security components. Using current technology, the memory card can hold from 103 bits to 32,000 bits of data. As technology improves, we can expect that the data storage capability for these cards will increase from 32K to 64K to 128K, and so on. The memory cards are less expensive to manufacture than the microprocessor cards, with the resulting trade-off being a decrease in data management security. The memory card depends on the inherent security found in the card reader, and would be best suited to applications requiring only low to medium security.[5]

The microprocessor chip has the advantage of being able to add, delete and alter the data being stored in its memory. This type of card can be viewed as a miniature computer with an input/output port, an operating system, and a small hard disk drive, but minus the usual keyboard and monitor. The microprocessor chips are available in 8, 16, and 32 bit architectures, with data storage range currently up to 32K bytes of data. Again as with the memory card, advances in semiconductor technology should see the amount of data storage increase.[6]

The basic standards that all smart cards adhere to is ISO 7816, part 1-10. These standards describe in detail all aspects of each card such as the physical size, electrical components and requirements, mechanical interfaces, and the particular software applications to be used. The smart card envisioned for use by the DoD will have an integrated circuit chip containing 32K of

data storage and memory, a linear (Code 39) barcode, a two-dimensional (PDF 417) barcode, a magnetic stripe, and a color digital photograph. Color-coding of DoD smart cards will indicate the status of that individual. **White** will be used for U.S. citizen civilian employees, U.S. citizen military personnel, non-U.S. citizens serving in the U.S. Armed Forces who have been lawfully admitted to the United States for permanent residence, and U.S. citizen employees and foreign national employees of DoD contractors who have been identified and approved as emergency personnel for the purpose of deploying with U.S. forces overseas and who would be subject to capture. **Red** will be used to identify foreign national personnel, including DoD contractor employees (other than those issued a white card as outlined above). **Green** will be issued to U.S. personnel of DoD contractors (other than those issued a white card as outlined above). Multiple technologies exist on the card to allow the use of a myriad of software applications in the near future.[7]

Crucial to many potential users, and in particular the DoD, is the ability of the smart card to use the Public Key Infrastructure (PKI). Basically, the processes, all the hardware and software, the people associated with the registration, generation, distribution of various security certificates are all lumped under the umbrella of PKI. In simple terms, PKI will allow smart cards to verify a user to a computer network, or to another user who might access smart card data. There are also various levels of this assurance that can be embedded within the card, driven entirely by the need for a particular level of security.[8]

Applications for smart cards appear to only be limited by their current technology. Because of their ability to hold encrypted data, the cards have found favor with both the financial industries and the military. There are also over 300,000,000 mobile telephones that use the smart card technology to enhance security and store subscriber information. The individual telephone

is personalized whenever the user inserts his smart card into the unit, immediately identifying the telephone to the network. It will also allow for precise, personalized billing information, and will store data useful to the consumer such as frequently called numbers and minutes used. Similarly, almost every satellite "mini-dish" receiver uses smart card technology. Using the security features built into each card, companies such as DirecTV and EchoStar have leveraged a key advantage in reducing fraud. Currently, there are over four million of these cards in use in the United States, and millions more to be found in Europe and Asia. The biggest commercial success, though, for smart cards has to be their use in the worldwide financial industry. In France, every Visa debit card has an embedded chip (over 25,000,000 cards). Germany also has about 40,000,000 cards being used in the banking industry. Using the "electronic purse" capability inherent with smart cards, the Proton company through its banking partners has issued over 25,000,000 electronic purse cards in several countries. Finally, there are over 100 countries in the world that have either reduced or completely eliminated coins from their pay telephone systems by instead issuing customers smart cards. Similar programs are also being implemented in Germany, France, United Kingdom, Brazil, Mexico and China. To say that smart cards have become a pervasive force in the financial industry would thus be an unqualified understatement.[9]

These same technologies can be used to a large degree in various military applications. As discussed in the following chapters, the DoD sought to use smart cards as debit cards, for identification purposes, and also to allow access to secure computer networks.[10]

Notes

[1] www.scia.org
[2] IBID
[3] IBID
[4] IBID
[5] IBID
[6] IBID

Notes

[7] IBID, DoD Common Access Card Fact Sheet
[8] www.knowledgenet.mil/knet/Feb00/PKI/pki.html
[9] DoD Common Access Card Fact Sheet
[10] Deputy Secretary of Defense memorandum dated 10 Nov 99

Chapter 2

Implementing Smart Cards in the DoD

There were many reasons for the DoD to get involved in the technology known as smart cards. Having seen the resounding success that the civilian banking and finance industries had enjoyed with smart cards (especially overseas), the DoD's interest in the technology was peaked. While the DoD saw limitless possibilities for this technology, the senior leadership within DoD was intent on ensuring there was competitiveness between smart card contractors to enable the government to garner the best possible price when purchasing the cards in bulk. Additionally, they were compelled to ensure the widest possible use of this technology, not only throughout the DoD, but other federal government agencies as well. This chapter provides the details of the DoD effort, and outlines in particular the mechanisms used to implement this huge undertaking.[1]

The DoD smart card effort officially began life on 10 Nov 1999, when then Deputy Secretary of Defense Hamry signed a memo titled "Smart Card Adoption and Implementation." Key provisions of his memorandum (sent to all service secretaries, Chairman of the Joint Chiefs of Staff, Under Secretaries of Defense, Director Research and Engineering, Assistant Secretaries of Defense, General Counsel of DoD, Inspector General of DoD, Director, Operational Test and Evaluation, Assistants to the Secretary of Defense, Director, Administration and Management, Directors of the Defense Agencies and Directors of DoD Field Activities) set the tone for how smart cards would be implemented throughout the DoD:

- "The Department's Chief Information Officer (CIO) is assigned the overall responsibility for the development of the Department's smart card policy and oversight. All DoD components are to take actions to implement the use of a standard DoD smart card."[2]
- "The initial implementation of the smart card shall be effected as a common access card (CAC). The CAC shall be the standard ID card for active duty military personnel (to include the Selected Reserve), DoD civilian employees and eligible contractor personnel. It will also be the principal card used to enable physical access to buildings and controlled spaces and will be used to gain access to the Department's computer networks and systems. This card would accommodate an integrated circuit chip and also contain such other relevant media as a magnetic stripe and bar codes."[3]
- "Secretary Hamre also mandated a DoD-wide movement to PKI. Since smart cards are already being used as authentication tokens for certificates and as private keys for digital signature and access authorization, the adoption of this technology within the Department—and placement on the CAC—will enable this card to serve as DoD's primary platform for the authentication token. Secretary Hamre authorized the CIO, therefore, to accommodate and incorporate the use of PKI with the CAC. The CIO was to ensure an initial implementation of the smart card based CAC at multiple locations no later than 30 Dec 2000. Furthermore, as a result of the recent Joint Requirements Oversight Council meeting, Secretary Hamre appointed the Department of the Navy as the lead service in preparing the Operational Requirements Document (ORD)."[4]
- "Secretary Hamre established a key guiding body that would provide oversight over all DoD smart card issues. Known as the Smart Card Configuration Management Control

Board (SCCMCB), this group includes representatives from Principal Staff Assistants (PSA's) within the Office of the Secretary of Defense and the DoD components. This group would oversee the operation of a Smart Card Senior Coordinating Group (SCSCG), chaired by the Navy. The SCSCG was charged with developing and implementing Department-wide interoperability standards for use of smart card technology, and a plan to exploit smart card technology as a means for enhancing readiness and improving business processes."[5]

The development of the SCSCG included management controls that delineated aspects of the smart card program that would ensure controls over key program aspects yet allowed flexibility in implementation. For example, centralized control of the program included program governance of the following: what applications would be mandated for the cards (ID cards, PKI, building access), Department-wide applications such as manifesting, e-purse and food service, basic data on the card, and space allocation for components. Decentralized aspects of the program were to include: component specific applications, physical access authorization, system access authorization, Defense Enrollment Eligibility Reporting System (DEERS), Real Time Automated Personnel Identification System (RAPIDS) workstation operations, applications hardware and business process re-engineering.[6]

The DoD also developed a Mission Need Statement (MNS) that quantified the requirement for smart cards. Citing the fact that "computers are increasingly used for planning, control and analyzing the military's operational, administrative, personnel, medical and logistic support functions. To a large degree, the effectiveness of computers is a function of the quality of the provided input data. To derive maximum benefit from DoD's vast installed computer base, timely and accurate data collection and retrieval is required."[7]

The MNS specified the initial target audience for smart cards would be as outlined in Secretary Hamre's memorandum—DoD active duty and Reservists. Key applications that would be supported by using the smart cards were identified as identification and tracking of personnel within a secured area, in-transit visibility (ITV) of personnel (as is related to mobilization activities and the movements of military personnel into and out of a theater of operation), tracking time and attendance, health care applications, training records and a validated electronic signature.[8]

A core aspect of the DoD smart card initiative centers around interoperability. As used here, interoperability refers to the cooperative processing of an application using specific software, hardware, various generations of cards and terminals, and a plethora of administrative and operating procedures. To this end, DoD strove to establish an interoperable environment for smart cards, which would enable flexibility at all levels of service delivery. It was hoped from the beginning that PKI held the mechanism for achieving government-wide interoperability, especially at the higher application level. With this as a backdrop, the Navy developed several documents that were to become the foundation for the smart card effort in DoD.[9]

The Navy, lead agency for smart cards, developed a Memorandum of Understanding (MOU) with the General Services Administration (GSA), and also drafted a Strategic Plan for implementing smart cards. The MOU between the GSA and the Navy established a Multiple Agency Program (MAP) which intended to provide economies of effort as smart cards were being tested and implemented within DoD. Specifically, the MAP allowed economies of scale when purchasing smart card software and hardware, ensured interoperability across DoD and leveraged each agency's investment towards common software applications.[10] The Navy's Strategic Plan also contained a key provision that not only sought to provide smart card

technology to all Navy personnel, but encouraged collaboration with other DoD agencies and civilian industry to "establish a common standard to achieve interoperability." This groundwork having been laid, testing would begin in earnest throughout various DoD agencies to ensure this new technology would work.[11]

Notes

[1] Department of Navy Smart Card Strategic Plan, FY 2000-2002
[2] Deputy Secretary of Defense memorandum dated 10 Nov 99
[3] IBID
[4] IBID
[5] IBID
[6] DoD Smart Card Implementation Brief, OSD web site
[7] www.afca.scott.af.mil/ip/comsec/caw/smartmns.htm
[8] IBID
[9] DoD Report to Congress "Use of Smart Card Technology in DoD", pages 4-5
[10] smart.gov/information/navy/mounavy.html
[11] Department of Navy Smart Card Strategic Plan, FY 2000-2002

Chapter 3

Smart Card Initiatives and Tests in the DoD

> "The Marine Corps issued more than 4,000 (smart) cards to military members during a joint military exercise called Cobra Gold '98. The card cut personnel deployment processing from eight hours to 45 minutes"
>
> —Donald E. Illich, Commander, 23 Jul 99[1]

The DoD has been enamored with smart cards since about 1993. Two aspects of the card especially intrigued the DoD: the card's ability to monitor access to secure computer networks (of which the Air Force has a preponderance), and that the card could also minimize the discomfort military members typically felt when participating in mobility processing. The military began a battery of field tests using smart cards from various contractors that employed many software applications in their search for what worked, and what would not. These early tests allowed the DoD to examine in depth the various capabilities of smart cards such as electronic purse, computer network access and mobility processing. What follows in this chapter is an examination of this process and in particular how smart cards have impacted both the Air Force, and the Air Force Reserve.[2]

The DoD began its first major test of smart cards when they were used in 1998 during a large, bilateral exercise between the United States and Thailand known as Cobra Gold. This exercise is designed to ensure regional peace in a large geographic area, and as such, one of the key exercise components involved mobilization of active duty and RC military personnel. The

exercise was conducted from 19 May to 1 June 1998, and served as the first in-depth measure for how successful smart cards would or would not be. Since the crux of this exercise would be the movement of large amounts of personnel in to and out of Thailand, smart cards were used primarily in aircraft manifesting to determine if they would prove to be beneficial.[3]

The exercise itself included joint and combined air/land/sea operations, with the United States Marines acting as lead agent. Total participants in this exercise was about 10,600, and included elements of US Marine Forces, Pacific; US Army, Pacific; US Pacific Air Forces; US Pacific Fleet; Special Operations Command, Pacific; Air Mobility Command; Military Sealift Command; and RC units from the Army, Navy, Air Force and the Marines. Of these total numbers, some 500 Reservists were issued smart cards to determine if they could be easily melded into the process.[4]

The objectives to be tested during Cobra Gold were many. In particular, the DoD wanted to:

- Learn overall smart card performance
- Develop lessons learned to improve smart cards use for the future
- Evaluate reductions in the cost of logistics products
- Identify any increased value of logistics products
- Determine any long-term infrastructure savings from using smart cards as a business process improvement[5]

The methodology to collect data during this test was varied. Surveys, interviews, observations and specific diagnostics were run to determine the success of smart cards during the exercise. Particular tools used would also hopefully shed light on the usefulness of smart cards. These tools were business case analysis, activity based costing, process flow mapping and business process improvement. Constraints in the test were specific as to resources, times and

locations. Events used during the test included mass issuance, tracking, access control and manifesting. The actual participants included cardholders, system users, process experts database managers, commanders, end users of the products and technical representatives. The final result, overall performance, cost reduction (if any), quality and value assessment, lessons learned, data collection and implementation methods would all be captured in the hopes that this exercise would serve as the benchmark for continued use of the cards.[6]

Cobra Gold also allowed for the smart card test team and the participants to review the following applications and products:

Applications	**Products**
Card issuance	Strength accounting reports
Manifesting/movement tracking	Liberty and leave (ad hoc)
Manpower database	Red Cross messages
Access control to headquarters	Lost and found
	Mail forwarding
	Blood donor database[7]

Cobra Gold provided the DoD with the spark it was looking for with regard to the success of smart cards. What was originally a tedious, labor intensive process (manifesting military personnel for deployment), went from a previous six to eight hour job to approximately 30-45 minutes total. Other savings were equally as impressive. Previously, daily manpower reports required a lot of "hands-on" administrative work; in this test, smart cards were found to reduce the man-hour "cost" by as much as 50 per cent. Similarly, logistics products also improved. Accuracy rates went from 80 percent to 100 percent, and allowed for real-time information,

widespread availability and visibility, but perhaps most noteworthy was the intrinsic value of quality of life for the warfighter.[8]

Smart card use during Cobra Gold also provided other tangible savings through specific business process improvements. For example, there were reduced administrative overhead costs. The Tanker/Airlift Control Element (TALCE) saw a three to five person billet reduction due to smart card use, and similar savings of up to three billets were realized in the personnel area. There were also cost savings noted in the logistics area through reduced support and equipment costs, and most noteworthy was the reduced "in-transit" time afforded by smart cards. During Cobra Gold, the participants noted they spent less time overall but received the same training value, and estimated they would save a minimum of eight to twelve hours per unit per exercise.[9]

Smart cards also allowed for savings specifically in the manifest process, typically allowing for the manifest time to be within the mechanical turnaround time of the aircraft. This factor itself was so significant that it allowed for reduced rental charges for support equipment, improved the quality of life for those previously waiting long periods of time, and most importantly, allowed for more training time, not time spent in a business process. There were also improvements noted in the raw logistics information collected. Smart card data allowed for increased flexibility in dealing with aircraft cancellations and schedule changes (exercise or real), provided real-time in-transit visibility of the personnel assets, and afforded the ability to react to changes as in this exercise when a non-combatant evacuation was tasked. As with other areas already noted, the logistic community expected these process improvements could reduce the number of billets required in future exercises.[10]

The savings that were discovered by using smart cards during Cobra Gold, however, were not expeted to manifest themselves with only one use per year. Rather, real savings would occur

if such a program were applied across the DoD. Data from Cobra Gold provided estimates indicating that if ten similar exercises were conducted, DoD would realize over $2,000,000 in cost avoidance over five years due to reduced travel, per diem and rental costs. These savings could be achieved primarily due to the reduced number of personnel required to accomplish aircraft manifesting, personnel tracking, and report preparation. Overall manpower savings (per similar event) was estimated to be eleven.[11]

While this was the first real opportunity to have Reservists from various service branches participate in smart card issuance, many Reservists still showed up for the exercise without a card. It was determined that many of them (or their unit) never got notified of the new procedure. Despite these minor setbacks, the summary report from the exercise stated that the "smart card proved to be the enabling tool for process improvement and to create cost savings, improve quality of life, and enhance mission readiness". It was also felt that were smart cards to continue their foray into other applications such as food service, medical and dental, similar returns on investment would be realized.[12]

The Air Force has had success with smart cards as well. Two programs in particular have allowed the Air Force to determine first-hand whether or not smart cards will meet the demands placed on them by subjecting them to real tests in an operational environment. The first is called the Supply Asset Tracking System (SATS). SATS is a front-end application used in conjunction with the standard base supply system. In this application, smart cards are used by providing real-time visibility over assets located within base supply. Currently, SATS at Shaw AFB, South Carolina, Eglin AFB, Florida, Aviano Air Base, Italy, and Ramstein Air Base, Germany are using smart cards. In each case and at each location, smart cards are providing the electronic authentication and authorization required of the cardholder to receive the assets from base

supply. Previously, a labor intensive, paper based system performed the function now being done with smart cards. Thus far, it appears to be successful.[13]

The second area where smart cards are in use by the Air Force no doubt came into being as a result of the positive results realized from Cobra Gold '98. The Air Force Expeditionary Battlelab (AFEB), located in Mountain Home, Idaho, is attempting to integrate smart cards into the Air Force readiness process. The overall goal of this process is to use smart card technology to demonstrate the AFEB's Deployment Personnel Accountability and Readiness Tool (DPART) initiative. The basic premise of this initiative is very similar to that proved in Cobra Gold; to provide timely and accurate information to unit commanders and deployment managers on their unit's state of readiness. DPART is expected to interface with existing Air Force systems that contribute to personnel readiness, but again to be leveraged through the use of smart cards. In testing DPART, it should be noted that the Air Force involved both active and Reserve units. To date, no significant problems have been discovered in using DPART, and in fact, similar cost/personnel savings that surfaced in Cobra Gold are being confirmed.[14]

The current thrust in implementing smart cards in the Air Force is focused now on beta testing set for February through March 2001 at Langley AFB, Virginia, Lackland AFB, Texas, Hurlburt Field, Florida, Osan Air Base, Korea, and Ramstein Air Base, Germany. The plan is to begin issuing cards at these locations, with the idea that other Air Force commands and all military personnel flights (MPF's) will follow suit. Full implementation of the CAC is expected to begin as early as April, 2001, with nearly all personnel (including Reservists), receiving new ID cards within the next two years. Total cards to be issued should exceed nearly four million units.[15]

The Air Force also fully intends to integrate the Reserves into the smart card initiative. Essentially confirming the DoD implementation plan for smart cards, the Air Force Reserve has specified in its Reserve Component Employment Study 2005 that smart cards would be critical to any future mobilization action involving the Reserves. The expectation is that once the technological hurdle of issuing this many ID cards is completed, smart cards will have matured to the point that particular issues and concerns of the Reserves can be addressed. The intent is to leverage the lessons learned in the issuing of this plethora of new ID cards with the increased capability smart cards will offer in the very near future.[16]

The challenges facing the Reserves are many. While allowing the Reserves to have new ID cards via the DEERS/RAPIDS databases is a good idea and complies with the Deputy Secretary of Defense's guidance, this represents the "low hanging fruit". There are many other issues that need to be resolved to ensure the Reserves are an active player in the smart card effort. For example, if a Reservist is also a DoD contractor, only the CAC that most accurately depicts the capacity in which the individual will operate with respect to a particular facility, will be activated for that facility. Similarly, when an Air Reserve Technician (ART) is not serving in a uniform status, they are a member of the federal civil service. Certainly, this could lead to confusion, and this issue of "multiple affiliations" currently has the attention of DoD policy makers. Similarly, many records that active duty personnel have inherent in digital form today are not necessarily available for Reserve personnel. While the DEERS and RAPIDS systems contain many records on Reservists, specific deployment data such as immunization, medical and training information for the individual Reservist may not be as available or as current. Also, the various categories of Reservists (unit, Individual Mobilization Augmentee - IMA, ART) drive their participation requirements. While the unit they are assigned usually has no trouble contacting each

participating Reservist, many Reservists still do not perform military duty with any regularity (beyond that which is required to ensure their continued participation in the Reserves). The point here is that if essential data is needed from these Reservists for inclusion into databases that will be accessed by smart cards, a serious effort will be needed to ensure the information is made available in a timely manner. An example of this concern is illustrated in the existing effort to modify/upgrade the current Logistics Module (LOGMOD) database that is used in the Air Force's mobilization process. Here, as in other areas, the Air Force intends to update critical databases to include information on Reservists. Although still very early in the development stages, everyone involved realizes that smart cards will need concise, current and correct data from many databases, and that Reservist's data will need to be updated and uploaded as well to ensure the accuracy of their information.[17]

Notes

[1] Quick Look Report: Smart Card in Cobra Gold '98
[2] DoD Report to Congress "Use of Smart Card Technology in DoD", page 7
[3] IBID
[4] IBID
[5] Quick Look Report: Smart Card in Cobra Gold '98
[6] IBID
[7] IBID
[8] IBID
[9] IBID
[10] IBID
[11] IBID
[12] IBID
[13] DoD Report to Congress "Use of Smart Card Technology in DoD", pages 12-13
[14] IBID, AEFB DPART Brief
[15] DEERS Homepage, Randolph AFB
[16] www.defenselink.mil/pubs/rces2005_0799g.html
[17] IBID, CAC application from HQ SSG/ILX

Chapter 4

Conclusion and Summary

Smart cards began their life as most technological inventions have. Originally patented and basically thought of as having some utility, their real capability has come to light as the technology matured and eventually satisfied a need. Early versions of smart cards could barely hold identification data, but advances in miniature circuitry and computer processing power has allowed smart cards to literally invade our lives.[1]

The most pervasive influence of this technology has come from the banking and financial industries. Seeing the utility of the security and cost benefits that could be garnered from such technology, France, Germany and the United Kingdom literally "dumped" smart cards into the public's hands to foster their acceptance. The sell was relatively easy; rather than fishing in pockets, purses and briefcases for currency, the consumer could now use a smart card for many of his everyday financial transactions. Consumers quickly fell in love with them due to their utility and security, and banks liked the inherent fraud protection offered by the cards. With so many positive aspects inherent in smart cards, it was not long before they attracted the attention of United States industries, and soon after, the DoD.[2]

The DoD began using smart cards slowly, intent on taking advantage of two key components. First, they wanted to explore all aspects of the card's capability, and second, they wanted to ensure compatibility through the Department. The DoD soon appointed the U. S.

Navy as lead agent for smart cards, and laid basic ground rules for its implementation. Testing followed suit and the technology has not disappointed. As previously indicated from the Cobra Gold exercise, despite some minor setbacks, smart cards offered the DoD significant savings in business processes, dollars and personnel. As expected, the DoD is on-track to issue nearly four million smart cards to active duty personnel and Reservists.[3]

Smart cards can be viewed as a force enabler for today's Total Force. With the vast drawdown in personnel making the inclusion of Reserve personnel in many of the global missions of the Air Force a must, smart cards will allow all military personnel significant quality of life improvements. For anyone who has ever had to endure what seemed like an eternity in a processing line for mobilization, smart cards should minimize that wait by some 90 percent. Most significantly, though, is in the smart card's future potential. As technology improves, smart cards will be used for a myriad of processes that will further reduce the need for human intervention. But herein lies a caution: as noted in this paper, we need to ensure from the beginning that the databases smart cards will access are updated and current. For example, there will have to be a concerted effort to ensure Reservist's information, in whatever form is needed, is input into the various databases used by smart cards. As we saw in the Cobra Gold test from several years ago, many of the Reservists never received a smart card for the test as word never reached them or their unit. Similarly, the unique participation requirements of each reservist puts them potentially at risk for being excluded in the smart card implementation effort. Each program manager at each command and unit must be aware of this initial implementation effort, and see this as a "call to action". It is imperative that RC personnel data is checked for accuracy, and that each RC member is fully aware of the intent of this new program. Similarly, program managers and Air Reserve Personnel Center (ARPC) staff must work diligently with the Air

Force Personnel Center (AFPC) to ensure future smart card applications are built with RC forces in mind. Without a concerted effort on the part of management, Reservists may well be left behind as newer, even more elaborate uses for smart cards are introduced.[4]

The Air Force is making incredible strides with this technology, and it does appear aware of the concerns addressed here. As evidenced by the many field tests of smart cards where Reservists were included as a key component, the Air Force is also intent in including them in all aspects of the implementation effort, ever mindful of their specific concerns. As long as this same attitude remains, and reaches down to the functional management levels in the Reserve hierarchy, we can rest assured that this vital force enabler will also remain at the forefront of tomorrow's Air Force missions.[5]

Notes

[1] www.scia.org
[2] IBID
[3] Quick Look Report: Smart Card in Cobra Gold '98
[4] IBID
[5] Deputy Secretary of Defense memorandum dated 10 Nov 99

Glossary

ACSC	Air Command and Staff College
AFIT	Air Force Institute of Technology
AFPC	Air Force Personnel Center
ARPC	Air Reserve Personnel Center
ART	Air Reserve Technician
AU	Air University
CAC	Common Access Card
DPART	Deployment Personnel Accountability and Readiness Tool
DoD	Department of Defense
DEERS	Defense Enrollment Eligibility Reporting System
GSA	General Services Administration
ICC	Integrated Circuit Chip
ID	Identification Card
IMA	Individual Mobilization Augmentee
ITV	In-transit visibility
LOGMOD	Logistics Module
MPF	Military Personnel Flight
PKI	Public Key Infrastructure
RAPIDS	Real Time Automated Personnel Identification System
RC	Reserve Component
SATS	Supply Asset Tracking System
USAF	United States Air Force
USAFA	United States Air Force Academy
USCENTCOM	United States Central Command

Common Access Card. A smart card designated by the DoD as having the required elements to be used in multiple applications. The DoD CAC is a smart card with one or more embedded memory and/or microprocessor integrated circuit chips (ICC). The CAC also contains a linear bar code, two-dimensional barcode, magnetic stripe, color digital photograph, and printed text.

Public Key Infrastructure. A key and certificate management infrastructure designed to support confidentiality, integrity, availability, authentication, non-repudiation, and access control in computer networks.

Bibliography

The Craft of Research, Booth, Colomb and Williams
Defense Information Systems Agency, on-line at www.knowledgenet
DEERS/RAPIDS/CAC homepage, on-line at www.afpc.randolph.af.mil
Message DTG 261829Z Oct 00, SUBJ: DoD Smart Card Technology Implementation
Reserve Component Employment Study 2005, on-line at www.defenselink.mil
AIT Technology Briefing, Air Force AIT Management Office, Aug 2000
Smart Card Industry Association, on-line at www.scia.org
DoD Common Access Card Fact Sheet, on-line at www.dmdc.osd.mil
Deputy Secretary of Defense memorandum dated 10 Nov 99
DoD Smart Card Implementation Brief, on-line at www.dmdc.osd.mil
Scott AFB Communications Mission Need Statement, on-line at www.afca.scott.af.mil/ip/comsec/caw/smartmns.htm
DoD Report to Congress on the Use of Smart Card Technology in DoD, June 1999
General Services Administration, on-line at smart.gov/information/navy/mounavy.html
Department of the Navy Smart Card Strategic Plan, FY 2000-2002
Quick Look Report: Smart Card in Cobra Gold '98 on-line at www.dmdc.osd.mil
Air Force Times Smart Cards could Put an End to Paperwork, 3 May 99
Design News, Vol. 49, Issue 8, 25 Apr 94, Flash Memory card Targets Harsh Military Environment
Program Manager, Vol. 28, Issue 5, Sep/Oct 99, PKI Moves On-board with DoN Smart Cards
Army Logistician, Vol.32, Issue 3, May/Jun 2000, Smart Cards Will Replace Traditional ID Cards
Federal Times, Vol. 35, Issue 45, 13 Dec 99, GSA Nears Smart Card Procurement
ABA Banking Journal, Vol. 40, Issue 11, Nov 98, Smart Cards, Coming Up to Bat
Air Force Journal of Logistics, Vol. 23, Issue 2, Summer 99, Just the FAQ's—Smart Cards
Smart Card Technology for Joint Food Service, USCENTCOM Briefing, 25 Apr 2000
DPART Technology, AEFB Briefing, Aug 2000