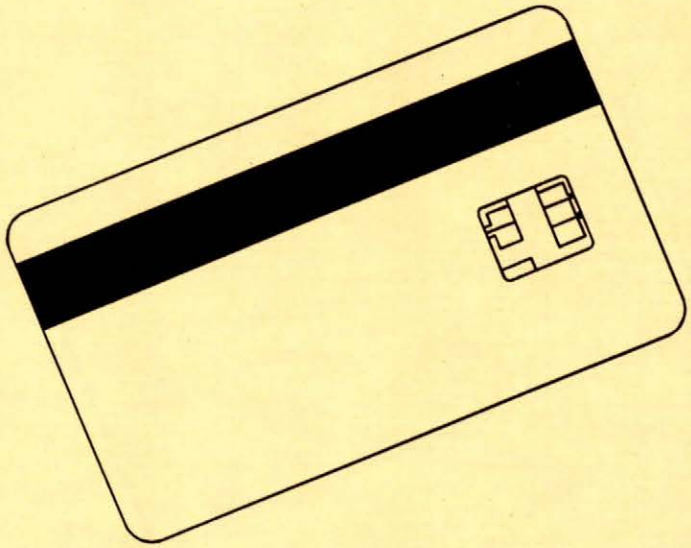
February 1993

Smart Cards in the Public Service: The Department of Communications Experience



The Department of Communications Smart Card Group

TABLE OF CONTENTS

SMART CARDS IN THE PUBLIC SERVICE
The Department of Communications Experience

EXECUTIVE SUMMARY

Advanced Card Technologies (ACT) have evolved out of the modern day need to have highly convenient portable data storage media. In looking at the available Advanced Card Technologies (ACT) of magnetic stripe cards, optical cards, large memory cards, memory cards and smart cards, the Department of Communications (DOC) was interested in a data storage medium that offered very good data security, could house multiple applications on a single card, was reusable, and was very portable. The smart card was identified as the ACT that could best meet these demands.

A smart card is a plastic card which resembles a credit card and contains an imbedded computer chip capable of storing, retrieving and processing information stored on the chip. The arrival of this technology to the electronic data processing (EDP) sector has provided users of EDP technology with a very portable and highly secure information medium. The smart card has the capabilities to eliminate paper, provide secure portability of information, improve systems integrity, improve the quality of life in the workplace, facilitate workplace integration of people with special needs, and enable distributed processing at the individual level. These capabilities allow the creation of a wide range of applications that can be used to increase the productivity of all functional areas of government.

Recognizing the potential advantages that such a technology offered, DOC decided, in 1988, to experiment with smart card technology to determine its potential use within the Department. Successful smart card trials paved the way for more involvement and by 1992, Senior Management support for accelerated development of smart card technology was given.

In the four year period between 1988 and 1992 DOC's Smart Card Group gained a lot of experience in the fields of smart card physical and technical design. One of the earliest targeted uses for the smart card was to create a smart card that would double as the Departmental ID card. This combined card would be able to provide visual verification of an employee's status through the ID portion of the card, while also providing important user information such as computer access password codes and building access privileges through the smart card portion of the card.

Experiences gained in the area of physical design helped determine the basic components DOC required of a combined ID/smart card. These components were identified as smart card designated components, namely the computer chip and the magnetic stripe, and ID card components, which consisted of the Departmental and Federal Government headers, a Departmental ID number, the expiry date of the card, and the cardholder's photograph, name, signature and security clearance code.

The Smart Card Group's work with developing smart card applications uncovered valuable information used for technical design considerations. Important findings included identifying a high quality smart card operating system which would ensure DOC's flexibility to deal with different smart card vendors, provided an easy to use application development system, and made maximum use of the smart card's limited memory capacity. The Smart Card Group's experience with magnetic stripe technology led to the decision to use highly durable magnetic stripes which also provide better data protection for data stored on the magnetic stripes.

Throughout its experiences, the DOC Smart Card Group relied on DOC employee feedback to refine designs and create a better overall product. It was this feedback that helped determine the final components of the ID portion of the combined ID/smart card. Also, employee feedback has been instrumental in assessing smart card durability and data integrity in real life working environments.

The DOC experience with smart cards has shown that this information medium has the potential to become an indispensable tool for the Federal Government both in its internal workings and in providing client services. DOC, while focusing on internal administrative applications, is committed to the pursuit of realizing the full potential of the smart card.

1.0 INTRODUCTION

1.1 PURPOSE

This report documents DOC's involvement and experience in the conception, development and delivery of smart cards and smart card technology. This document will serve three main purposes:

1) It will serve as a DOC reference guide for revisiting the rationale behind the development of smart cards within the Department;

2) It will provide DOC senior management with high level information that will facilitate understanding of the development and impact of smart cards at DOC; and,

3) It will serve as a reference guide for Other Government Departments, Committees and working groups in the creation of an interdepartmental smart card.

1.2 A PRIMER TO ADVANCED CARD TECHNOLOGIES

The smart card represents one available technology within the ACT umbrella. ACT are information storage/processing/retrieval technologies which are implemented on a plastic medium and which resembles a credit card in physical dimensions. The products which are considered to be ACT include:

1. The magnetic stripe card
2. The optical card
3. The large memory card
4. The memory card
5. The smart card

A brief description of each card technology follows.

The magnetic stripe card is undoubtably the most recognizable ACT. Anyone who uses a credit card or an automated teller banking card is using a magnetic stripe card. This type of card is distinguishable by the dark stripe of magnetic material which is placed on one side of the card. The magnetic stripe is capable of storing 400 bytes (characters) of information. Its very limited information storage capabilities require that systems utilizing this technology store only essential information, such as cardholder identification codes to the card. Although the magnetic stripe card has gained massive acceptance throughout the world, it is widely recognized that its limited data storage capability and the data's susceptibility to fraudulent alteration will severely limit the future uses of the

technology.

The second ACT, the optical card incorporates optical data storage technology (such as high-capacity optical disks) to portable credit-card sized plastic cards. Data is stored and retrieved using laser beams in essentially the same manner as used for optical disks. Unlike some ACT which allow data to be written, erased and re-written, optical cards employ a write-once technology, ie. the media can be written to only once and it cannot be altered without destroying the card. Under the proper circumstances this unerasable write-once system is desirable (eg. medical records). The main advantage of this technology is its high data storage capacity, typically in the 3 to 4 megabyte range (equivalent to 1200 to 1600 typewritten pages of text). A disadvantage of this technology is its relatively weak capability to prevent unauthorized users from reading data stored on the card.

The large memory card is another ACT which under the right circumstances can be a very useful product. Physically, the card's length and width conform to credit card standards, however these cards are considerably thicker than a credit card or other ACT products. The large memory card is basically an electronic computer memory board shrunken to the length and width of a credit card. The memory capacity of this media can be as high as 2 megabytes (equivalent to 800 typewritten pages of text) depending on the type of memory that is used. A drawback associated with this ACT is that it is not very portable, that is one cannot carry a large memory card in one's wallet.

The small memory card's memory storage capacity of 2 kilobytes to 64 kilobytes of memory (2,000 to 64,000 characters) is much more limited than that of the large memory card. The small memory card's credit card like appearance, source of memory and memory capacities are very similar to that of a smart card. It is often referred to as a smart card without the intelligence of a microprocessor.

The final ACT, the smart card, is perhaps the most promising ACT of all. A smart card is a credit card sized plastic card that contains an imbedded computer chip which possesses computer logic and is capable of storing and retrieving information loaded onto the chip. Although memory storage capacity is limited to a maximum of 16 kilobytes, the smart card's microprocessor offers functionality that is not available with any other ACT. The smart card's microprocessor is able to employ sophisticated encryption/decryption techniques to prevent unauthorized users from viewing data stored on the card. Also, the smart card's microprocessor is capable of performing computer logic functions such as addition, subtraction, multiplication, division, conditional branching, etc. In fact, these functions are used by the smart card's microprocessor to monitor access attempts and to shut off the smart card when the number of incorrect access attempts reaches a predefined number.

It is the smart card's extensive data protection capabilities that has attracted the attention of DOC and made it the focus of a number of applications under development. A technical comparison of the ACT is provided in appendix A.

Smart card technology has been in use around the world for several years in a variety of applications. France, where the smart card was invented, has made heavy use of the technology in a wide variety of service, industrial, and leisure industry sectors. In France, smart cards were first used to revolutionize the public pay telephone system, as their ability to store and manage pre-paid funds replaced the cash payment method previously used.

1.3 THE SMART CARD VERSUS THE MAGNETIC STRIPE CARD

The portable plastic magnetic stripe card has become a common device used for portable information storage and application access. Plastic cards are everywhere and are used for financial transactions (credit cards, automated teller cards, debit cards), club membership identification (eg. Club-Z, Price Club), cheque authorization (supermarket customer cards), access to health care (provincial health cards, Blue Cross), and a myriad of other uses. In 1991 there were over 2.4 billion plastic magnetic stripe cards in use throughout the world. Clearly the plastic card has become the medium of choice for portable information. Through plastic cards, cardholders wield considerable financial power and gain instant access to valuable goods and services.

This proliferation of plastic cards however, has exposed various drawbacks of the technology. First, the cards are typically limited to one application per card, for example you cannot combine your health card with your bank card. Second, plastic cards are fixed in structure, data areas can only be used for very specific purposes. Finally, the relative ease with which fraudulent plastic cards can be manufactured and magnetic stripe information can be altered or copied has created new opportunities ripe for exploitation by organized crime.

The smart card is able to address these limitations while taking advantage of the popularity of plastic cards. The attributes which demonstrate the smart card's superiority to the plastic magnetic stripe card include:

1. Multiple applications capability
2. Protection from fraud/counterfeiting
3. Encryption/decryption of all card data
4. Personal privacy of sensitive data
5. Ability to co-exist with magnetic stripe technology
6. Flexible data structure

2.0 THE ROLE OF THE SMART CARD

The smart card's arrival has opened up a new avenue of application possibilities. As this chapter will show, the card's capabilities will facilitate productivity gains across the entire spectrum of government. The application possibilities that are highlighted in section 2.2 illustrate the wide range of opportunities suited to the smart card's abilities.

2.1 SMART CARD CAPABILITIES

2.1.1 Eliminating Paperwork Burden

While the arrival of the microcomputer has transformed office procedures substantially, it has not been able to reduce our heavy reliance on pre-printed forms, letters and memoranda. In most procedures, the paper serves three purposes:

1) Provide the service or product supplier with a record of a transaction. This requirement can be met adequately with central computer systems that are developed for and operated by service providers. Since the service provider will be controlling the information that is placed on such systems, they do not require separate paper records.

2) Provide the receiver of the service or product with a record of the transaction. Since the receiver of the product does not control the information that is placed on supplier based computer systems, paper is used to provide the receiver with transaction authentication. Smart cards can meet this authentication requirement through their storage ability and protection of data.

3) Provide an approval process mechanism. A manager's signature is often used on paper forms to indicate approval for a particular request or action. The smart card's authentication routines and PIN entry requirements provide an electronic means of meeting this requirement.

2.1.2 Provide Secure Portability of Information

Floppy diskettes are frequently used by people to store electronic information in a portable format. While this medium performs reasonably well under circumstances where the information stored on the diskette is not sensitive in nature, it is unable to provide rigorous data protection for conditions where data is sensitive.

Another drawback of using floppy diskettes concerns their size. At 3.5 inch and 5.25 inch diameters, these information storage devices are certainly portable, but not convenient. While people can carry diskettes around in a shirt pocket, pant pockets, or even some larger purses, they cannot be placed inside a wallet, which is the accessory that most people associate with information portability and convenience.

The smart card is able to address both of these drawbacks. The sophisticated data protection mechanisms employed by the smart card's internal computer offer rigorous data protection for sensitive data while the smart card's credit card size allows it to be carried around in a wallet thus making it a truly portable and convenient information storage medium.

Security of data is provided in a number of ways:

1) The smart card's design prevents unauthorized users from using special electronic equipment to probe or tamper with the contents of the smart card. Any such attempt typically results in a smart card shutdown which locks the card and renders it useless.

2) Data that is stored on smart cards is encrypted using sophisticated encryption/decryption algorithms. This encryption therefore ensures that data cannot be read unless proper access has been established.

3) Proper access to the smart card is established by the entry of the valid Personal Identification Number (PIN) by the owner of the smart card. Access to the smart card is not possible without the entry of this PIN. To prevent an unauthorized user from "guessing" the correct PIN, the smart card keeps an internal count of the number of incorrect PIN entry attempts and once the internally set limit is reached, the smart card will lock up, rendering it useless, until the smart card programmer resets the card.

4) The smart card allows the smart card programmer to set up tamper-proof employee profiles, so that even the smart card's authorized user may be prevented from accessing or altering certain data areas of the card. For example, the DOC stockroom application will have the finance section loading authorized money amounts to a employee's smart card. By implementing employee profiles, DOC can insure that the employee will only be able to view the monetary information, not alter it.

2.1.3 Improving Systems Integrity

The smart card's data protection facilities make it possible to easily incorporate high-level protection systems that limit access to computers and the information which is stored on them. It has been shown that computer systems that require password input by keyboard are not difficult to break since the perpetrator need only possess knowledge of the password. With a smart card however, a second level of security is added, the possession of a smart card. Computer systems that incorporate smart card technology work only if the individual inserts the smart card into a smart card reader and then inputs a password, hence possession of the smart card or knowledge of the password alone are insufficient to provide access.

2.1.4 Improving Quality of Life in the Workplace

The smart card's multi-application ability means that many different facilities such as physical access, computer access, personal information, financial information, etc. can reside on a single smart card. This capability greatly simplifies the day-to-day work of an individual as the smart card becomes the single access mechanism to a multitude of services available to the employee thereby contributing to greater job satisfaction and higher productivity.

2.1.5 Facilitating Workplace Integration of People with Special Needs

The smart card's ability to store the profile of an employee presents opportunities for better accommodating people with special needs. In such instances the smart card could be used to pass information about the employee's special needs to allow the system to adjust itself to that employee's needs.

2.1.6 Enabling Distributed Processing at the Individual Level

As personal computers have become more powerful and cheaper in price, they have changed the electronic data processing field. Many giant centrally controlled computer systems have been replaced by smaller computer systems which serve a single organizational group or even a single individual. This change in computing structure, called distributed processing, has allowed these smaller groups to directly harness the power of the computer and control the information that they choose to place on the computer.

It is widely recognized that there are many advantages to distributed processing, including:

1) More reliability - under distributed processing, since each organization will have its own computer, the organization will not be paralysed by failures of a central computer or computer access links.

2) Less cost - the total equipment cost for a distributed system is usually cheaper than the pro-rata cost of a centralized computer system.

3) More flexibility - each organization has control to determine how to best use their computer system resources. If priorities change, the distributed system resources can easily be altered to address the needs. Under a centralized system this flexibility is not possible.

The smart card enables the concept of distributed processing to be realized at the individual level, in a uniquely convenient format. Utilizing smart card technology, information which is pertinent to a single individual can be stored on and processed directly to that person's smart card. In addition, the smart card's unique portability allows the individual to carry this portable data processing centre anywhere, storing it in his/her wallet. This represents the ultimate form of distributed processing.

2.2 APPLICATION POSSIBILITIES FOR THE FEDERAL GOVERNMENT

Previous sections have shown that the smart card is a very versatile and unique information processing and storage tool that is capable of addressing many challenges facing the federal government in the 1990's. Smart cards will have an impact on every function of government and will be used as a tool for increasing productivity and performance while controlling costs. The following sub-sections will illustrate the types of smart card applications that may be developed for various government functions. Further examples of application possibilities are listed in Appendix B.

2.2.1 Administration

The government administration function is one of the more obvious areas where the smart card can be used to eliminate paper and increase productivity. The administration function includes daily work that forms a part of every public servant's day. These operations include office services, materiel management, technical services, facility accommodation services

and library services.

Some examples of possible smart card applications could include:

1. Records management tracking of files, correspondence, cabinet documents, etc. - With this type of application, the smart card would be used to replace the current loan-form that employees must complete in order to borrow such documents. When a document is loaned out, the employee's smart card would be "charged" with responsibility for that document while a corresponding entry would be made electronically to the central tracking system. To ensure full accountability this entry would have to be confirmed by the employee through the use of his/her smart card and PIN. Additionally, multiple document transactions could be stored on the employee's smart card, thus resulting in a substantial reduction in the production of paper as well as decreasing the transaction turn around time.

   The above example could easily be adapted to apply to a library system, where books are loaned instead of records.

2. Inventory management - With this type of application, inventories of furniture, office equipment, computer software and computer hardware could easily and accurately be tracked. Using the single multi-purpose smart card, these inventory managers could assign furniture, equipment, computer software and computer hardware to employees via the employee's smart card. Once the acceptance of an inventory item is confirmed and a transaction is accepted and recorded to the employee's smart card, that employee would assume full responsibility for that item until the item is returned. When the item is returned, the existing item entry on the smart card would be electronically removed from the smart card item list, thereby releasing the employee's responsibility for that item. Entries on the employee's smart card would be the ultimate form of proof of employee responsibility for an inventory item. Such a system would eliminate the need for the inventory manager or the employee to complete and keep track of the prodigious amounts of paper forms that would be required to track an employee's holdings.

3. Materiel acquisition from stockrooms - An application that could eliminate substantial paperwork is the use of the smart card to replace all paper procedures required for acquiring materiel from stockrooms. This application is under development within DOC and is scheduled to be operational by mid-1993. It is planned that this

application will utilize the smart card as a form of electronic money, that is funds to purchase stockroom materiel will be loaded to the smart card and decremented by the stockroom as goods are passed over to the cardholder.

2.2.2 Personnel

Smart cards can be used in the personnel function to eliminate the overhead required to respond to employee leave queries, superannuation queries and health plan information as well as simplifying the procedures involved in employee transfers, training and development, official languages and classification.

Smart card personnel applications generally focus on improving the access and quality of personnel information available to the employee. Productivity gains are usually realized through the Personnel Branch's reduced service requirements. Some of the possibilities for the utilization of smart cards in the personnel area would include:

1. Distributed leave reporting - Experience has shown that the typical personnel branch devotes significant resources to responding to queries from employees in regards to their leave credit balances, how much leave has been taken, how much special leave is available, etc. With this smart card application, leave credits would be periodically downloaded to employee smart cards. This set-up would benefit both the employee and the personnel branch. Employees would benefit from being able to query their smart cards leave balances at will and no longer having to depend on personnel branch resources to answer their leave credit queries. The personnel branch would benefit because the elimination of this service requirement would free up resources which could be used to support other areas of operation.

   The second part of this application would see the employee and his/her supervisor using the smart card to allow the electronic submission and approval/rejection of leave requests. This system would typically be tied to a central application run through personnel branch so that all records are kept up to date. On approval of any requests, the employee's smart card and the personnel system would be simultaneously updated so as to ensure that all participants have accurate records available. The benefits accruing to this part of the application would include productivity improvements through quicker transaction turn around time and the

elimination for the need to generate paper leave request forms.

2. Interdepartmental Transfers - The current procedure for transferring an employee's file from one government department to another is slow, paper-intensive, and very complicated. A possible smart card application could be to enter the employee's personnel record on the employee's smart card. When a transfer is required, a transfer code could be entered by the home department. This code would allow the new department to pick off the employee's personnel record from the employee's smart card, including the information regarding offices to contact vis-a-vis the transfer. Such an application could greatly speed up the time required to transfer an employee as well as resulting in a reduction in personnel resource overhead and paper creation.

3. Electronic Overtime Tracking - This type of application could greatly improve overtime accountability, tracking, completion and submission. Under such an application, the smart card would be used to replace all employee overtime requests. All overtime worked by an employee would be recorded to the employee's smart card, but only after authorization through a supervisor smart card. Once the supervisor approves the request for overtime, a centralized computer overtime system would record employee overtime to the employee's smart card. Without the supervisor smart card approval, access to the overtime system would be denied and the employee would not be authorized to put in the overtime. At the end of the month, the employee would use the central overtime system to submit the overtime hours, at which point the central system could automatically calculate the payments due to the employee and forward the request for approval to the employee's supervisor.

2.2.3 Finance

Although smart card applications involving aspects of government finance have been detailed in the administration function section above, smart cards can also be used in specific finance procedures through electronic signature and electronic wallet applications.

1. Electronic Signatures - The smart card can be used in financial applications as a valid electronic signature. The federal government Financial Management Manual stipulates that two conditions must be met before electronic signatures can be considered valid. These conditions are; 1) that a password is required for use of the

electronic signature, and 2) that the individual entrusted with financial signing authority holds the valid electronic signature on a protected storage token.

The smart card easily meets both conditions thus making it a natural candidate for storage of an electronic signature. The ability to store and release an electronic signature can result in productivity gains, faster transaction completion times, and a reduction in the creation of paper.

2. Electronic Wallet - The smart card's sophisticated data protection, processing, and storage mechanisms make it an ideal candidate for use as an electronic wallet. The stockroom application outlined in section 2.2.1 is an excellent example of how a smart card could be used as an electronic wallet. Another example could be to load money onto smart cards for use in requesting by-hand service. Whenever a request for a by-hand is made, the by-hand section could deduct a monetary amount from the requester's smart card, until the money on the card is emptied and needs to be refilled.

3. Acting Position Delegation - Currently, whenever a delegation of signing authority is required, forms need to be completed to provide accountability. Frequently, the same individuals are called upon to assume this acting authority thus resulting in a continuous cycle of paper generation. Using the smart card, an individuals profile can include the ability to assume an acting authority upon approval by his/her superior's smart card, thus eliminating the need for the previously mentioned paper creation. Once enacted by the employee's superior (specifying a range of valid dates) the employee's smart card would be recognized as a valid signing authority.

2.2.4 Security

The smart card's data protection abilities make it an ideal tool for use in various departmental security functions. One of the smart card's primary uses is that of authentication. In the departmental security function this authentication feature can be exploited in controlling physical access to restricted sites and controlling logical access to computers.

1. Physical Building Access During Silent Hours - Smart card technology would allow the traditional register sign-in/sign-out procedures for building access to be replaced by electronic

equivalents. With a smart card system the employee would slip the smart card into a card reader upon entering the building and then again upon leaving the building. This application would eliminate the need for sign-in/sign-out registers while providing the employee (via the smart card) and the department with accurate building access records.

2. Interdepartmental Building Access - The use of the smart card as an interdepartmental Security/ID card could simplify interdepartmental government employee visits. When a federal government employee currently visits another federal government department, he/she must go through a labour intensive procedure that requires the employee to sign-in at a front desk and establish his reason for visiting the building. With an interdepartmental Security/ID smart card and a supporting smart card system, a visiting employee's status and time entering the building could be identified and recorded quickly and easily, thus reducing the front desk resource support needs while speeding up building access approval for that employee.

3. Computer Access - The smart card can be used effectively in applications that are intended to limit access to computers or computer systems. By incorporating hardware and/or software applications that use the smart card, it becomes possible to prevent an employee from accessing any part of a computer or computer system without the use of a valid smart card and knowledge of the appropriate PIN for access to that smart card's databanks. This application would greatly enhance the protection capabilities afforded to sensitive databases of information.

2.2.5 Informatics

The informatics function involves the provision of all EDP equipment, software and systems to a department's employees. The objective of the informatics function within a government department is to provide tools/systems that will simplify the work of the department while increasing the productivity and effectiveness of its employees. Smart cards can be used by informatics organizations to increase portability of data, establish custom user profiles (to determine systems that various employees can access and maintain) and administer multiple passwords for access to various information systems.

1. Distributed Databases - As identified in section 2.1.6, the smart card can facilitate distributed processing. An example of a distributed

database application could be a distributed pension benefits system for employees. Each employee's smart card could contain the data to allow employees to track their pension benefits and perform queries to determine pensions upon immediate retirement, pension at age 60, annual allowance amounts, last 6 years salary, average salary over the last 6 years, etc. Another example of a distributed processing application would be for an employee to use the smart card for project management, tracking of milestones, and delivery dates. Another distributed processing application might be to develop and produce onto an employee smart card, an individualized long-term training program, including target courses, course dates, course codes, etc.

2. User Profiles - User profiles embedded into employee smart cards can be used in a variety of ways. The user profile typically would identify what computer systems and access rights would be granted to a smart card holder. This feature would improve computer security as the smart card would be used to prevent access to restricted computer systems. In addition, this feature would benefit the employee as it would tailor what the employee's sees on a computer screen to his/her specific needs as identified by the smart card profile.

   A novel use for user profiles would be to custom tailor the way an employee uses the computer. In such an application the user profile could be used to determine the preferred language of the employee and bring up application screens in that language.

   For people with special needs, the user profile may be used to activate special interfaces. An example might see the user profile for a near-sightless person automatically signal the loading of a computer interface to greatly increase the size of all computer screen text or the user profile for a sightless person may automatically load a computer speech generation interface.

3. Maintain and Administer Multiple Passwords - The multi-application potential of the smart card can be effectively used to simplify the maintenance and administration of multiple passwords. The ever expanding network of information systems which are available to employees means that there is an ever increasing number of passwords that the employee needs to remember. The smart card can be used to maintain all information systems passwords securely and automatically, thus relieving the employee of the burden of remembering and maintaining numerous passwords.

Using the smart card, the employee would gain access to information systems by possession of the smart card and knowledge of the PIN. Once this multiple password maintenance function is established, password security can be further enhanced by programming the smart card and the information systems to generate and pass random passwords.

3.0 SMART CARD USE AT DOC

Smart Cards have their roots in the roles of identification and authentication. Like their predecessors, the Financial Transaction Card (Automated Banking Machine Cards), industry initially saw smart cards as devices which could be used to provide authorized personnel with secure access to protected environments.

The motivation for use of the smart card within DOC first originated within DOC's Security Branch in 1988, in response to a need to control access to DOC buildings during silent hours. A pilot group of approximately 80 employees were identified and issued smart cards which contained personal information about the cardholder. Each employee was required to use the card to log in or out of the building during silent hours by inserting their card into a smart card reader. The reader displayed cardholder information on a computer screen and recorded the information on the computer's hard disk for audit trail purposes. The cost of the pilot project, which included a card reader, 100 cards and custom designed software, was approximately $15,000. The software and hardware were provided by Clientel Systems in Vancouver. The hardware was built by Honeywell Bull of France, and the cards were manufactured by Micro Card Technologies International (MCTI), a subsidiary of Honeywell Bull, located in Dallas, Texas.

The pilot was very well received by the employees as well as the guard staff as it automatically provided a record of all building access by cardholders. During the course of the pilot, a number of problems were revealed which precluded DOC from making more extensive use of the technology at that time:

1) The smart cards were prone to high chip failure rates, in excess of 5%. These failures rendered the smart cards unusable and new cards had to be re-issued as replacements.

2) Support for the software and hardware, from Clientel Systems and MCTI was inconsistent.

3) Prices for components, such as card readers were extremely high, about $800 Canadian, with no apparent price relief on the horizon despite the fact that in France, readers were available for as little as $100 Canadian.

4) DOC's original intent for the use of smart cards was to create an "all-in-one" departmental ID card which not only contained the smart card chip but also displayed cardholder information such as a photograph, name and signature. This information had to be laminated to the smart card to increase the card's durability while providing protection from fraud. At the time, there were no lamination processes available at reasonable cost that would not damage the smart card chip.

These observations made it apparent that the North American smart card infrastructure was too fragmented and underdeveloped. Bearing this in mind, the DOC Security Branch's Smart Card Group decided to place a moratorium on smart card development, and instead, monitor the market and technological developments until the North American market infrastructure was better developed and offered more choice, a better product, and more competitive pricing.

The decision to re-enter the smart card development arena came in 1992, on the heels of a new awareness across the government vis-a-vis the potential benefits of smart cards and an announcement by the Canada Employment and Immigration Commission (CEIC) to launch a smart card project with a pilot community of 2000 Unemployment Insurance (UI) claimants in regards to the processing of UI benefits.

In the two-year period between 1990 and 1992, the DOC Smart Card Group found that the North American smart card infrastructure had been strengthened considerably and a much wider array of products were available. Also, the technology had advanced considerably. The advent of commercially available EEPROM (Electronically Erasable Programmable Memory) smart card chips, coupled with lower costs, better operating systems, and improved programming language support opened up a new world of opportunities for the smart card. Finally, it was possible to envisage a multi-function smart card which could be used in a wide variety of creative ways. This new technology would allow a single smart card to perform the functions of multiple single-use cards.

Based on this renewed enthusiasm, Senior Management threw its support behind smart card development and the Smart Card Group. The Smart Card Group immediately went about researching the new offerings, contacting various suppliers and manufacturers, and purchasing and testing promising systems.

Within DOC, the Smart Card Group identified initial pilot smart card applications and recruited managers willing to participate in testing the smart card technology. As of January 1993, pilot projects that have been established include:

1) An in/out employee status board for use at the Canadian Conservation Institute. Employees use their smart cards to indicate to the central computer whether or not they are in their office and replaces the in/out status board that previously existed.

2) An inventory control system for the loan of expense tools and apparatuses from the Plant Engineering Tool Crib at the Communications Research Centre (CRC). Technicians have access to a central set of work tools supplied by the Department. These high-tech tools and apparatuses can be very expensive and therefore a paper based loans/returns system was previously used to monitor who had borrowed which tool. The smart card application has allowed these systems to be replaced by a new system where all tool loans are written to a central

database and the employee's smart card. User satisfaction with this application has been very high and has resulted in more rapid processing and tracking of tools and apparatuses.

3) An inventory control system for the loan of expense tools and apparatuses from the Model Shop Tool Crib at the CRC (similar in operation to the Plant Engineering Tool Crib mentioned above).

Developments which are progressing include:

1) An application to use smart cards as electronic money in DOC stockrooms. This application will eliminate the majority of paper currently required to obtain stockroom materiel while maintaining and improving the necessary financial controls. The smart card will be loaded with financial amounts (like an electronic wallet) which the cardholder will then use to go to the stockroom and acquire goods. Amounts will be decremented from the smart card's monetary balance field and all transactions will be recorded on a stand-alone microcomputer.

2) An application to provide log-in and log-out by smart card at the CRC guardhouse. In conjunction with the above mentioned Tool Crib applications, employees with authorized smart cards will also be able to use their smart cards to gain access to the CRC without a requirement to sign an in/out register.

3) An application to use smart cards to maintain multiple employee profiles and passwords to facilitate access control for microcomputers to various computer systems. With the growing number of computer systems that can be accessed by computer, comes a growing number of passwords that must be remembered. This application will store all of the employee's passwords on his/her smart card and access all systems using only the smart card PIN. System passwords will be protected by the smart card's encryption capabilities.

At the same time Federal Government awareness regarding the potential use of smart cards led to the establishment of an interdepartmental Treasury Board Information Technology Standards Working Group, whose objective was to propose standards for the government-wide use of smart cards. As a leader in the use of smart cards in the Federal Government, DOC was asked to participate in this working group.

On an interdepartmental level DOC sees many possibilities for gains in productivity, efficiency and effectiveness through the use of smart cards. One possible interdepartmental application would be the development of a standard government wide ID/Security smart card that would allow authorized government employees to gain access to other government department buildings. This process could be achieved through the smart card's ability to validate the employee's employment status and security clearance level.

In 1993, DOC's support for the smart card initiatives will see the Smart Card Group actively pursue the development of new applications in the fields of physical/logical access security in addition to the new focus on streamlining or eliminating time-consuming paper intensive office procedures.

4.0 PHYSICAL DESIGN EVOLUTION

The evolution of DOC's current smart card initiatives did not come about by chance. From the start of the project, DOC has strived to follow certain basic rules of development:

1. Keep the design simple and the costs as low as possible.
2. Incorporate, wherever possible, established industry standards.
3. Try to avoid proprietary design components that would force DOC to deal with only one supplier.
4. Observe Government of Canada standards and guidelines.

By following these rules, the DOC has been able to keep its smart card design reflective of employee and Departmental needs. These changes have evolved through constant attention to employee feedback, changes in smart card uses and improvements in technology.

The upcoming sections document DOC's experience in determining the physical design of DOC's smart card.

4.1 BASIC COMPONENTS OF THE ID/SMART CARD

The determination of the basic components of the smart card were dictated by the intended use of the smart card. Initially, as previously explained, the DOC smart card was introduced to electronically control silent hours access to DOC buildings. Since the technology was new and the project was a pilot, no attempt was made to produce a combined Departmental ID/smart card. As such, the first DOC smart card only included the Department of Communications identifier, an embossed three digit card number, the smart card computer chip and a signature line for the cardholder. Figure 4.1 shows what the original DOC smart card looked like.

The next step in the current smart card evolution came in April 1990, when DOC purchased electronic Id card equipment from National Business Systems (NBS) of Orlando, Florida. While seemingly unrelated, the intent of the purchase was to provide an ID card system that would be compatible with the production of smart cards, to allow the achievement of a combined ID/smart card.

The general design philosophy behind any ID card is to authenticate an individual's membership to a particular organization. As such, most ID cards have these common elements; the organization identifier, the individuals photograph and name of the individual. This philosophy is followed in the requirements for DOC's ID card.

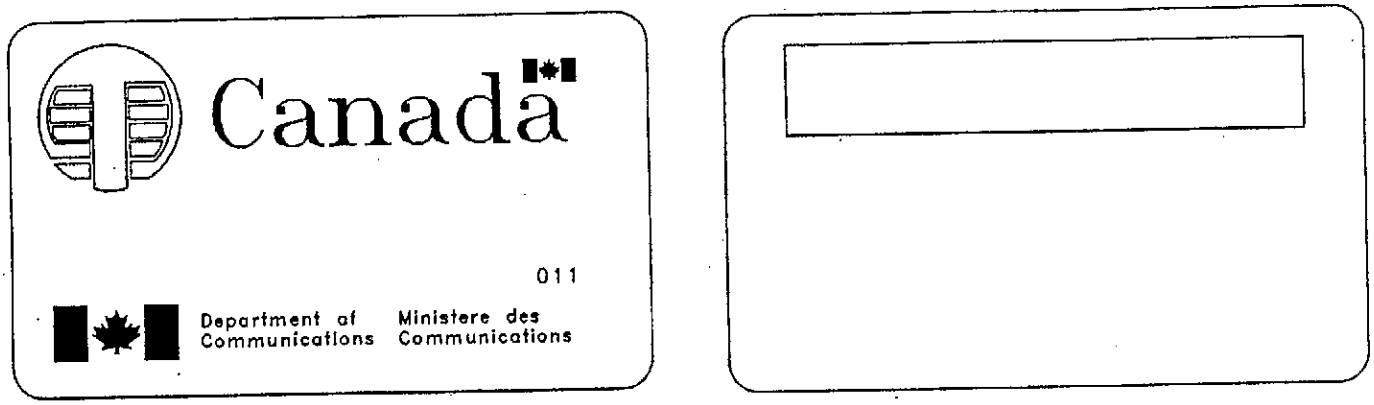


fig. 4.1 - Original DOC Smart Card

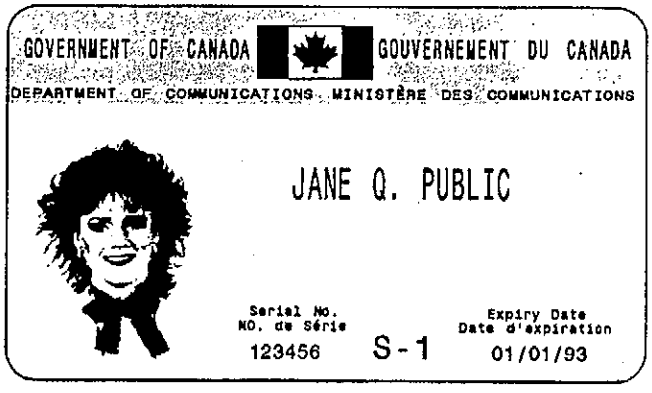


fig. 4.2 - NBS ID face for DOC

In addition, however, DOC chose to include four additional pieces of information, namely; the individual's signature, an ID card control number, the expiry date of the card, and the security clearance of the individual. The following descriptions of each component explain the rationale for inclusion of that component to the ID portion of the ID/smart card.

1. Government of Canada and Department of Communications headers - these headers identify the organization and parent organization to which the individual belongs.

2. Photograph of the Individual - the photograph provides visual confirmation that the individual producing the card is the authorized cardholder and has access to the rights and privileges of the card.

3. Name of the Individual - can be cross-referenced to other forms of identification for positive identification of a valid cardholder both within and outside the organization.

4. Signature of Individual - useful when a cardholder uses his/her signature in a transaction. Prevents signature fraud.

5. Departmental Identification Number - for card numbering control purposes.

6. Expiry date of Card - this entry ensures that all cardholder information is updated on a regular basis (ie. before the expiry date) and is useful to prevent access by individuals whose cards expire and no longer have access rights (especially important for identification and control of temporary employees of the department).

7. The Security Clearance Code - to identify cardholders who have special access privileges to information files.

Since the NBS ID system stores the entire ID face (including photograph and employee signature) electronically (see figure 4.2), automated production of a combined card becomes a feasible task.

With the 1992 renewal of the smart card initiative, the DOC Smart Card Group was determined to produce the elusive combined ID/smart card. Research into the North American smart card market identified two leading smart card vendors; DataCard Corp., located in Mississauga, Ontario, and PC3 Corporation of Lakeland, Florida. Both companies produced smart cards based on the same set of ISO standards, therefore compatibility of peripherals was not an issue. For

evaluation purposes, smart cards were ordered from both suppliers. The DataCard smart card is shown in figure 4.3 while the PC3 smart card is shown in figure 4.4. Because of the similarities of design and price, DOC chose the Canadian company, DataCard Corp. to supply the smart cards for use in the DOC pilot smart card applications.

Note that the smart cards in figures 4.3 and 4.4 include the provision of a magnetic stripe. DOC's Smart Card Group wanted this stripe included as a source of data storage for less risky and simpler applications that can take advantage of the economies of cheap magnetic stripe equipment and technology. Also the reader will note that space is available for the future inclusion of a bar code for future bar code applications.

4.2 PLACEMENT OF THE ID/SMART CARD COMPONENTS

This section details the constraints, decisions and rationale that led to the configuration for the current iteration of the DOC ID/smart card. The first section will deal with the placement of the smart card related components, that is the smart card computer chip and the bar code. The second section will describe the rationale that determined the inclusion and placement of information present on the ID portion of the combined card.

4.2.1 Smart Card Component Placement

In looking at the placement of the magnetic stripe and the smart card computer chip, DOC's Smart Card Group did not want to "Re-invent the Wheel". It was decided that to ensure the greatest cross-compatibility amongst different suppliers and manufacturers of smart cards and smart card peripherals, DOC would build its smart card utilizing the most popular International Standards Organization (ISO) standards for smart cards and card related items.

The ISO is a world-wide organization whose goal is to collaboratively achieve consensus amongst leading nations in the development of similar technologies with regards to standards of design and use. Adherence to ISO standards generally increases a company's ability to market a product world-wide and ensures that all developing industries work towards a common design goal.

With regards to smart cards, the ISO standards are the deciding factor in the determination of the physical dimensions of the smart card (IS 7810), embossing of characters on the card (IS 7811), the look, placement and pin

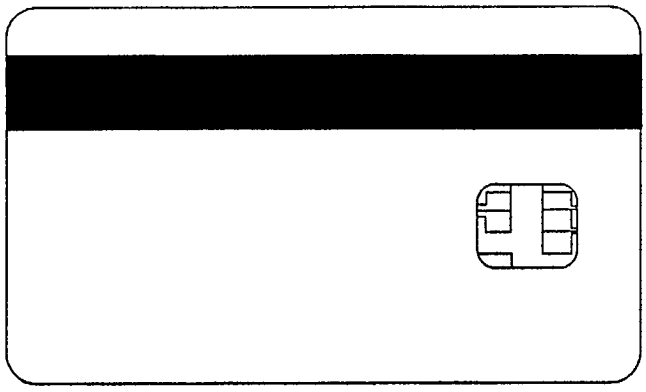


fig 4.3 - DataCard Corp Smart Card

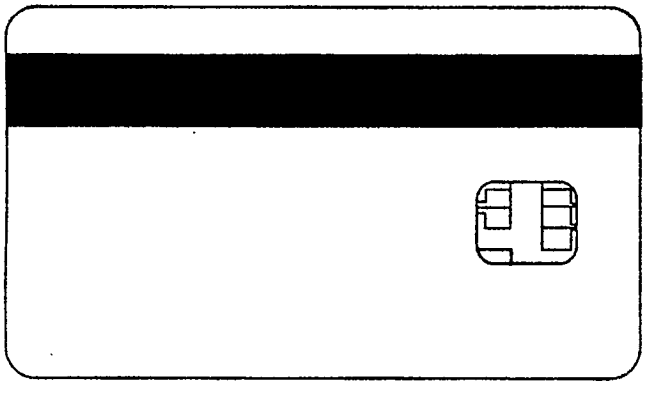


fig 4.4 - PC3 Corp Smart Card

assignment of the smart card CPU (IS 7816), and the location of the magnetic bar stripe (also IS 7811). So, although DOC technically could decide on custom placement of the smart card components, such a decision would have exacted a very high cost in terms of price, supply, cross-compatibility and flexibility to switch suppliers at any time in the future.

4.2.2 ID Card Component Placement

In looking at the placement of the various components of the ID card, DOC's Smart Card Group had to consider the following general factors:

1. All written information presented on Government of Canada ID cards must be presented in both official languages;

2. It was considered good practice that for the identification of organization, both official languages should be given equal consideration and therefore appear side-by-side rather than one above the other.

3. The delicacies of the smart card chip dictated that no information should be printed in the area backing the chip as the printing process could damage the chip and make the smart card inoperable.

4. It was determined that to allow maximum writing area, the ID card components would be placed on the opposite side of the smart card chip and magnetic stripe such that smart card chip would be located backing the right portion of the ID side of the card. This placement would allow the individual's photograph to be placed in the lower left hand quadrant of the ID side of the card (a preferred photograph location, since people habitually scan objects from left to right).

The ID card layout, as shown in fig 4.2 meets all of the above criteria. Note that the inclusion of the Canadian flag across the Government of Canada header provides an immediate visual reference to a symbol of the Government of Canada. The prominent position of the individual's photograph, name and signature ensure quick and easy visual confirmation of the individual. Finally, note that the placement of secondary information such as the serial number, security clearance, and the card expiry date is in the less important lower right quadrant of the card.

Overall, DOC feels that this is a very well thought out ID card, which presents all required information in a format that facilitates smart card integration.

fig. 4.5 - Current DOC Cold-laminate Combined Card

4.3 PRODUCING THE COMBINED ID/SMART CARD

Until recently (mid-1992) DOC's Smart Card Group has not been able to identify a North American company that was able to produce the combined ID/smart card at a reasonable price nor has it been able to find a process for self-production that could be bought. The main problem lies with the fact that the smart card computer chip is sensitive to heat and pressure, the two main components used in the manufacture of most ID cards. Therefore, in order to manufacture a combination ID/smart card, expensive equipment needs to be used. While a solution was known to exist in Europe and Japan where smart cards are widely used, North America companies who have access to a relatively tiny smart card user network have not been able to cost justify purchase of the proper equipment.

Based on the current availability of smart card products, DOC has experimented with two procedures for producing this combined ID/smart card. The first procedure called thermal dye transfer is produced by DataCard Corp.

The procedure requires DOC to send DataCard the electronic ID file that is captured by DOC's NBS ID card system. This file is then fed into the DataCard system which then digitally reproduces all the components of the Departmental Id card directly onto a smart card (even the photograph).

The trial run using this process however, failed to produce an acceptable quality output. The digital imprinting produced poor resolution photographs and "fuzzy" characters and graphics. In addition, it was noted that the imprinting process vertically compressed photographs by about 25 % thus distorting the appearance of the individual to look more stout than in actuality. DataCard has stated that with development work and equipment improvements an acceptable (for DOC) quality combined card is feasible, although the per unit cost to produce such a card would be quite high initially.

Not satisfied with the DataCard product, DOC's Smart Card Group looked for another way to produce the combined ID/smart card. This search led to the discovery of an interim solution that on a small scale of card production, can meet the DOC requirements. The process involves purchasing and applying cold laminate covers to "sandwich" the NBS ID Card paper outputs to a blank sided smart card. Although the process is very labour intensive, the result is a professional looking, durable product which is forgery resistant. The combined card is shown in figure 4.5.

DOC's Smart Card Group acknowledges that the cold laminate process is only an interim solution and therefore has continued its search for a permanent solution to this problem. Indeed, recent developments indicate that a viable solution may be close at hand, as the recent North American surge in interest for smart cards

has resulted in a whole new wave of excitement and product announcements on all fronts, including a rumoured solution to the combined ID/smart card problem. Based on this new wave of advancements, DOC's Smart Card Group believes that an economical and viable solution will manifest itself before the end of 1993.

4.4 FEEDBACK VIS-A-VIS DESIGN AND APPEARANCE

DOC employees have played an important role in the design of the combined ID/smart card. To start, one of the underlying reasons for producing the combined ID/smart cards stemmed from DOC employees desire to eliminate the need to carry multiple Departmental special purpose cards and to replace these multiple cards with a single card that could handle the provision of all their Departmental privileges.

An area where employee feedback has altered the appearance of the card is in the removal of the Date of Birth indicator from the ID card portion. Initially, the Departmental ID Card included the individual's date of birth. This piece of information was included because it was identified as being a unique piece of information that could be cross-referenced to other records for authentication purposes for an individual. DOC employees argued that the provision of a photograph, name and signature was more than enough to allow positive identification of an individual. Also, inclusion of the Date of Birth was argued to be an invasion of the privacy of the individual. The employees concerns and logic were acknowledged and the date of birth was removed from the card.

Overall however, DOC employee satisfaction with cards has been very high with regards to design and appearance.

5.0 TECHNICAL DESIGN RESEARCH

Since the start of the smart card project in 1988, the DOC Smart Card Group has been very happy with the results achieved and knowledge gained in the area of technical design. This achievement is doubly rewarding when one appreciates the underdeveloped state of the North American smart card market and the limited DOC resources available for research.

Indeed, in many instances evolution has come about through hard-won, hands-on experience rather than through esoteric analysis. DOC's experience has taken it from using the Honeywell Bull CP8 smart card to today's smart card which uses the PC3 Operating System. The following sections detail DOC's findings and observations in relation to the technical aspects of smart cards.

5.1 OPERATING SYSTEM AND DEVELOPMENT SYSTEM SELECTION

One of the first realizations which DOC research uncovered was the importance of Operating System (OS) selection. Since the OS is the central piece of computer software used to control the use of the computer chip, the decision of selection of an OS was as important as the selection of a smart card manufacturer. However, unlike the Personal Computer (PC) market, where practically all PC's use the Microsoft MS-DOS OS, no standard for OS's exists in the smart card market.

In fact DOC's experience showed that most smart card manufacturers were marketing their own proprietary OS along with their smart card and were not interested in licensing the technology to other third party companies. From DOC's point of view, this meant that the smart card and OS went hand-in-hand, the two could not be separated. Once one of these proprietary systems was adopted, the user was forced to purchase that manufacturer's products; no flexibility was available. In the event of company bankruptcy, such an arrangement would leave DOC without third party support for such a system. Experience also showed that with proprietary systems, as company support for the product waned so too did user support and product availability.

DOC's Smart Card Group decided that in the event of vendor bankruptcy, it would be desirable to have the flexibility to change vendors. Thus it was desirable to find a company that produced a smart card OS that was available for licensing to other companies. That way, if the company that DOC chose to deal with were to become insolvent, DOC would be able to continue to acquire support and make compatible equipment purchases with other licensed companies. To DOC's knowledge, as of January 1992, PC3 Corp. was the only North American company whose OS was available for licensing to other

companies.

With this knowledge DOC's Smart Card Group decided to look at the PC3 smart card OS and decided to test the PC3 smart card system vis-a-vis the Honeywell Bull smart card system. The results of DOC's testing and relationships with PC3 support staff allowed for some interesting comparisons with the Honeywell Bull experience, both in similarities and differences.

One of the first differences noted was in the structure of the OS. The Honeywell Bull OS required programmers to specify all parameters involved in any smart card operation, hence great flexibility was present, although at a cost of making programming more onerous and complex. The PC3 OS on the other hand, was more compact and less complex to program and retained most of the functionality that was available with the Honeywell Bull OS. The relative ease of use of the PC3 OS vis-a-vis the Honeywell Bull OS can be seen in the following example which provides the programming code to perform the function of submitting a PIN to a smart card:

Code for submitting a PIN : Honeywell Bull OS (using C language)

```
#include "MCLIB.H"
BYTE pinbuffer[4];
BYTE commandstatus;
BYTE cardstatus;
main()
{
mcdevice = &mc5202;
mcportid = 0x3F8;
mcdvinit();
mcmask = &mcssm;
mcon (&commandstatus,&cardstatus);
pinbuffer[0] = 0x11;
pinbuffer[1] = 0x11;
pinbuffer[2] = 0x11;
pinbuffer[3] = 0x11;
mcpin (pinbuffer,1,&commandstatus,&cardstatus);
}
```

Code for Submitting a PIN: PC3 OS (using C language)

```
#include "scdisk.h"
char p_str[4];
main()
```

```
{
call_scdisk ("COMM", &retcode, "1", "8", &null_str);
p_str = "1111";
call_scdisk ("SUBMIT", &retcode, p_str, "", &null_str);
}
```

As can be seen the PC3 code is much shorter and easier to follow.

Another important factor in assessing an OS concerns determining the breadth of programming language and applications support provided by the OS. Typically, DOC's Smart Card Group found that most smart card OS's supported only one programming language, Microsoft C and very little in the way of turn-key applications. This was true in the case of the OS's provided by Honeywell Bull, Toshiba, and GEMPLUS Card Int'l. PC3's OS however, showed itself to be a richer environment for programming languages and applications as it supported Microsoft C and Microsoft QuickBasic. In addition PC3 is currently developing a supporting DLL library for Visual Basic that will allow the production of Windows applications that can interact with the smart card (DOC is currently Beta testing this library).

The advantages of PC3's expanded programming language support are apparent when one revisits the above programming code example and notes the further program efficiencies that are achieved by using Microsoft's QuickBasic:

Code for Submitting a PIN: PC3 OS (using QuickBasic language)

```
DECLARE SUB SCDISK CDECL (P1$, RETCODE%, P3$, P4$, DATA$)
CALL SCDISK("COMM", RETCODE%, "1", "8", "")
P$ = "1111"
CALL SCDISK("SUBMIT", RETCODE%, P$, "", "")
```

A final area of comparison between smart card OS's concerns company support for the product. In this area DOC's Smart Card Group can only relay experiences gained through working with MCTI (representing Honeywell Bull) and PC3 corporation. Smart card OS's are complicated to deal with, and DOC's Smart Card Group found itself requesting company support and assistance often.

The experience with MCTI in obtaining support proved frustrating, as replies to requests for information were difficult to get over the telephone. With regards to PC3 Corp., however, DOC's Smart Card Group was able to deal with staff on hand who had either participated in the development of the smart card OS or had detailed knowledge of it. A typical reply to requests for information from these people was, "Hi, I worked on the OS. Your problem is that you did a Reset Card after the Submit PIN". Such direct support allowed the DOC Smart Card Group

to avoid many crises in dealing with client support or in instituting programming corrections.

5.2 PARTITIONING MEMORY

Another important area of technical design concerns the memory partitioning structures used by the various manufacturers. The memory partitioning setup is an area of concern because it determines how the limited card memory gets used, modified and rewritten.

By examining different OS's, DOC's Smart Card Group found that there were three primary means of partitioning card memory.

The first means is exemplified by the Honeywell Bull OS which employs a hierarchical tree file system. Branches on the hierarchy can share access properties. Files within these branches further share certain sub-properties. This design structure seems to dictate that a branch would be devoted to a particular application, or family of applications.

The second means, as employed by the PC3 OS, does not employ a domain, or hierarchical tree file structure. Files are not subordinated to any structures or to other files. In other words, all files are at "root".

The third category is "other". These models either do not employ a file type structure and treat the memory as one file (something certainly undesirable for multi-application cards) or rely upon the external application to enforce file separation which is not acceptable if any card security is required.

The difference for the developer is whether a hierarchical file structure is required or whether it will be an encumbrance. With regards to comparison between the hierarchical structure versus the non-hierarchical structure, what is given up in organization is more than retrieved in flexibility of use of memory. Also, the organization of branches in a hierarchical model requires additional memory overhead which is not required in a non-hierarchical model. When looking at the limited memory available on smart cards, this overhead becomes a concern.

The non-hierarchical model was deemed preferable for DOC since it allowed easy deletion and addition of files without having to resort to "pruning and grafting" of file branches. This setup also allowed for a more flexible set of file read/write privileges. Also, the non-hierarchical model did not require giving up precious memory space for overhead.

In the final analysis, each model has its merits based on user requirements. The lesson is that there is a distinct difference between the models and that requirements can mistakenly assume one model over the other.

On a non-specific level another important memory partitioning discovery made by the DOC Smart Card Group was the importance of determining users exact program requirements and how these requirements affected memory allocation. The nature of the smart card memory structure is rigid and once determined, cannot be changed without the requirement to recall and reprogram affected smart cards or alter applications for smart cards that need updating.

This restriction was experienced first hand in a particular instance where an application that was developed according to the client specifications had to be modified at a later date (due to client request for additional information storage). In the end, this so-called simple modification required the DOC Smart Card Group to reformat all the client smart cards before the client modification could be implemented, thus making the modification process complicated and tedious.

5.3 MEMORY USAGE EXPERIENCE

The current smart card used by DOC provides only 2 kilobytes of memory and represents the most economical smart card size available. Although smart cards providing as much as 16 kilobytes of memory are available, they are currently prohibitively expensive to purchase in small quantities. As such, the DOC Smart Card Group has had to work as efficiently as possible with the available smart card memory (much like programming in the 1960's, and 1970's when memory for computers was very expensive).

Working with only 2 kilobytes, the DOC Smart Card Group has focused on defining what type of information should be stored on the smart card and what type of information should be stored externally. Also the DOC Smart Card Group has worked towards developing innovative processes to stretch the usefulness of the available memory.

One such innovation has been to replace voluminous hard data with codes which are used to access external data tables containing the actual hard data. A second DOC Smart Card Group innovation which has greatly increased the usability of smart card memory involved the successful development of a methodology to compress data on a PC3 OS smart card. For example, using the data compression methodology, numeric data can be compressed to 50% of its original size.

An example of the difficulties involved with memory restriction concerns the experiences learned with providing smart cards with various support modules, such

as smart card rebuilding routines and smart card reformatting tools. Accommodating these routines into the 2 kilobyte smart card proved to be quite a challenge but was eventually resolved through a series of precisely executed program calls which were developed through experimentation.

5.4 CARD SECURITY

One of the often touted benefits of using smart cards has been the protection that the smart card offers over its data. Various integral parts of the smart card Chip, such as the OS are protected by encrypted keycodes which prevent unauthorized tampering. As such, maintaining the integrity of the smart card was a paramount issue in the eyes of the DOC Smart Card Group.

One area which challenged smart card security concerned the rebuilding of smart cards which had failed (which means the smart card had stopped functioning and/or the entire data contents had been wiped out). In such instances, the DOC Smart Card Group was placed in a precarious situation. It was not possible to rebuild the cards centrally since the data resided at the client site, yet the DOC Smart Card Group did not wish to disclose the Initiating Key (IKey) to the clients. The IKey is required to format new cards and is installed at manufacture, and cannot be reset like an Application Key (AKey) or PIN. Clearly, releasing the IKey to the clients would compromise the security of the smart card.

A number of alternatives to solve this dilemma were explored. One alternative involved making an executable program within which the IKey was embedded, but this alternative was found to still leave the IKey vulnerable. Another alternative which proved to be acceptable, was to provide pre-formatted cards loaded with an executable program which required a supervisor's card be present to rebuild a failed smart card. While still not ideal, this second solution did manage to preserve the security of the smart card. The very important lesson that DOC's Smart Card Group learned was that the IKey must be reserved for formatting cards whereas an AKey should be used for file creation and as a prerequisite for writing to protected files.

5.5 USE AND PLACEMENT OF MAGNETIC STRIPE

Due to the wide availability and relatively cheap costs of production, equipment, and use of magnetic stripes, DOC's Smart Card Group decided that there was still a role for this medium for simple applications such as physical building access to low security areas. In working with magnetic stripes DOC's Smart Card Group found that there were basically two types of magnetic stripes on the market, low coercivity and high coercivity stripes.

The main difference between low coercivity and high coercivity stripes is that high coercivity stripes provide more protection from data erasure due to spurious magnetic fields than low coercivity stripes. Also, the high coercivity stripe has been shown to last longer. These advantages are available for a slight premium over the cost of a low coercivity stripe.

The DOC Smart Card Group also looked at a variety of magnetic stripe widths that were available and found out that most magnetic stripe readers had no problems reading data off any of the stripe widths.

Interestingly, the DOC Smart Card Group found it difficult to find a North American manufacturer who could actually place a magnetic stripe on a smart card, due to the fact that the smart card stock (type of plastic) used by smart card manufacturers differs and these differences affect the magnetic stripe application process.

A final area of note is that currently, smart card readers do not incorporate magnetic stripe reading capabilities. In instances where it would be efficient to use both magnetic stripe and smart card memory areas, both a smart card reader and a separate magnetic stripe reader would be required. Also, in a phase-out scenario where smart cards replace magnetic stripes, it would be beneficial to be able to replace the magnetic stripe reader with a combination smart card/magnetic stripe reader so that uninterrupted utilization can occur. Recognizing this possible limitation, the DOC Smart Card Group has been working with a vendor to produce a smart card reader which will also be able to simulate a magnetic stripe reader so that the magnetic stripe reader can be replaced without redesigning the entire access system.

5.6 FEEDBACK VIS-A-VIS TECHNICAL ASPECTS

As in the case for physical design, DOC employees have played an important role in providing feedback vis-a-vis running applications. Employee input has been very important throughout, and has often resulted in the creation of elegant and simple solutions to problems which were often considered very difficult to solve. Employees have been instrumental in bringing to the Smart Card Group's attention concerns that the group had thought trivial but by no means were, and by de-emphasizing areas which the employees thought trivial but the Smart Card Group interpreted as critical.

In pilot tests, employees communicated quickly that card failure or slow replacement of failed cards was not acceptable. As the applications became part of the way they did business, they came to rely on the smart cards heavily.

With regards to procedures, employees preferred interfaces that matched existing system procedures. For example, a preference was shown for two-slot card readers for "in/out" type applications, even though a one-slot card reader would have been sufficient. By responding to these requests and dealing quickly with employee concerns, the DOC Smart Card Group facilitated the cooperation and support of the employees.

The staff members required to perform administrative smart card application tasks (e.g. commissionaires at in/out applications) came to terms with the system and understood its intricacies far faster than anticipated. Training requirements for these people were much less than expected. In situations where these staff were encouraged to "play without fear of breaking" the application prior to implementation, the training requirements were further reduced.

Employee feedback has also had an influence in the establishment of point form operating procedures lists and a smart card hotline support number. The DOC Smart Card Group and employees both agree that these enhancements have proved to be very useful in averting minor employee problems.

6.0 SUMMARY

The North American smart card market has only recently shown the signs that significant use and presence is at hand as evidenced by the increase in general public interest and awareness coupled with the expansion of the North American market of companies involved in supplying the smart card industry.

This document has attempted to document the trials and tribulations that the DOC Smart Card Group has experienced in its smart card program. The past four years have shown that this information medium can and should play a vital role in the overall information strategy of a modern organization.

DOC is committed to advancing the Government of Canada's state-of-the-art in this field and welcomes participation from other government departments in developing a common set of standards for smart cards. At the same time, the DOC Smart Card Group also remains committed full time to internal development and application of the smart card.

Appendix A - Advanced Card Technologies Technical Comparison

Characteristic	Magnetic Stripe Card	Optical Card	Large Memory Card	Memory Card	Smart Card
Medium	Magnetic	Laser Optics	Electrical	Electrical	Electrical
ROM Capacity	400 bytes	4 megabytes	2 megabytes	64 kilobytes	16 kilobytes
Multi-Write	Yes	No	Yes	EPROM (No) EEPROM (Yes)	EPROM (No) EEPROM (Yes)
Reproducible	Yes	Yes - costly	Yes - protection available	No	No
Information Security	Very Poor	Okay, if encryption used	Poor	Good	Very Good
Fraudulent Use	Yes, very high risk	Yes	Yes, some	Low risk	Very low risk
Durability	3 yrs	5 to 10 yrs	5 to 10 yrs	5 to 10 yrs	5 to 10 yrs
Base Reader Price	$150	$5000	$300	$200	$200
Card Price (>5000 cards)	$1	$20	$30	$3	$10
Environmental Vulnerablilites	Magnetic	Dirt, humidity, heat	Static, dirt, humidity	Static, humidity	Static, humidity

Appendix B - Compendium of Possible Applications for Smart Cards

The following list of application possibilities is presented for illustrative purposes and is intended only to give the reader an appreciation of the wide variety of applications where smart cards may be used effectively. Please note that analysis has not been conducted to determine the feasibility or return on investment potential for these applications.

ADMINISTRATION

Records Management - use the smart card to track files, correspondence, cabinet documents, etc. Smart card replaces loan agreement forms, increases accountability of the individual and is non-repudiable.

Inventory Management - use the smart card to assign responsibility for furniture and equipment to individual employees. Multiple forms get replaced, accountability increases, and maintenance of system is greatly simplified.

Materiel Acquisition from stockrooms - the smart card is used as electronic money to acquire materiel from stockrooms. A monetary amount is loaded onto the employee's smart card, each time the card is used the purchase amount can be decremented from the card until the card balance is zero. When the electronic money is depleted, the employee can re-load money onto the card.

Electronic Overtime Tracking - the smart card could be used to replace employee overtime request forms as all overtime could be recorded to the card. As an added bonus the implementation of smart card technology allows the development of a two card smart card system where a supervisor uses his/her smart card to approve overtime requests. This set-up would increase the accountability of overtime systems significantly while at the same time simplifying the process through elimination of paper requests.

Electronic Project Management - use smart card to enhance project management by tracking time utilization vis-a-vis project milestones. Reports can include individual employee time spent per milestone, project time vs. down time, salary costing of project, etc.

Acting Position Delegation - user profile on smart card can be triggered to allow employee to assume a delegated signing authority, once authorized by his/her superior through their smart card.

Senior Management Overtime - the smart card can be used by Senior Managers to track the amount of overtime hours worked by managers. This feature can be of use to these managers to help them to assess how effective they have been in handling their workloads, determining if their workloads are too great, re-evaluating what this overtime has been accomplishing, etc.

Fleet Management - Smart cards can be issued for fleet vehicles and used to track all vehicle expenses and uses thus increasing the ability to monitor and control fleet vehicle expenses.

PERSONNEL

Leave System on Smart Cards - use smart cards to store employee leave credits. Employee can query smart card directly and use smart card to submit requests for leave. Supervisor uses smart card as authorizing token for subordinate's leave request. When approved, leave amount gets deducted from employees smart card balances.

Interdepartmental Transfers - store employee personnel record on smart card. Use this record to speed transfers between government departments as employee brings all pertinent data with him/her to the new department.

Electronic Training Register. Use smart card to load training itinerary and money for employees, based on career development goals agreed upon by both employee and employer. Training money loaded onto card can only be used for authorized courses.

Government wide competition poster system - system would use user profile off the employee's smart card to search for competition list for which the employee is qualified to compete. Search parameters such as clearance level, language profile, education, special physical/mental requirements, current classification level, etc.

Access to Performance Appraisals - the smart card user profile can be used to determine access rights to performance appraisals, or protect electronic appraisal files from unauthorized probing/tampering. If the smart card holder is identified as an employee with no subordinate employees then that employee would only be able to view and approve his/her appraisal. If the smart card holder is identified as a supervisor/manager then he/she would have access to viewing all subordinate employee appraisals, creating new appraisals, viewing his/her own appraisal, signing off appraisals, etc. The controls that were put in place would satisfy and surpass current data privacy/sensitivity requirements.

Electronic Medical Profiles - The employee's medical profile can be placed on the smart card to aid in ensuring that special employee needs are met or to be used for health insurance purposes.

FINANCE

Access Control to Financial Systems - use the user profiles capability of smart cards to define employee access rights to various levels of financial control systems, ie. commitments, expenditures, budgets, OPF's, MYOPS.

Electronic Signatures - the smart card can be used as a valid electronic signature for use with automated financial, leave, travel, etc.

Electronic Travel Itineraries - loading travel itineraries onto the smart card. Using the smart card to keep track of all travel expenses and transactions.

SECURITY

Physical access to buildings - the smart card can be used to replace sign-in, sign-out registers while improving the tracking capabilities of such applications.

Computer Access - smart cards can be used to restrict computer access only to valid holders of smart cards. Furthermore, the card holder's smart card user profile could be used to determine what systems can be accessed.

Maintain and Administer multiple passwords - the smart card's multi-application ability can be used to store and maintain multiple passwords for various computer systems, thus simplifying the employee's use and access to computers while maintaining existing security standards.

OTHER

Distributed Printing of Radio Licences - Issue smart cards to companies that require access to selected Communications Canada computer systems on a frequent basis. The smart cards could store company profiles that would direct access to allowable and strictly defined portions of Communications Canada's computer systems. This automation would remove the current support service overhead that is required to assist these companies in their dealings with the Department.

Smart Cards for travelling art exhibits - smart card travels with piece of art. Information on smart card indicates condition of artwork when it left. Through on the road updates to a central expert system, answers given by the employee regarding the condition state of the artwork can be checked against the original state of the artwork as recorded to the smart card. After a certain point of deterioration, the expert system can red flag a piece of art, indicating that restoration is required.

Electronic Filing of Tax Returns - this application could yield huge savings in processing time, assessing costs, mailing costs, and turn around time to file tax returns. One roadblock to implementation of this application has been authentication of the individual dialling in to Revenue Canada. Smart cards issued to Canadian Taxpayers can be used to authenticate such individuals and allow access to electronic tax return filing.

Electronic Unemployment Insurance Benefit Claims - EIC is currently working to go forward with development of this large application which promises to overhaul the current process. U.I claimants will be able go to ATM type machines, complete their UIC claim and receive immediate payment for that claim. Savings in mailing costs alone is estimated at over 10 million dollars. Further savings in administrative overhead will likely exceed mailing cost savings.

Electronic Vote Casting for Elections - Using the smart card to overhaul the Elections Canada voting system shows great promise. The same smart card that is used for electronic tax return filing and UIC claims can be used to provide access to electronic voting during elections or votes on referenda. The individuals smart card profile will alert the computer systems as to whether or not the individual is eligible to vote (ie. profile could include the individuals age, citizenship, and mailing address). Once valid access has been established, the individual could enter his/her vote electronically (note that such a system would essentially eliminate the possibility of spoiled ballets). This system could save the overhead required to canvas voters, set up voting booths, count the results, etc.

Appendix C - Bibliography

1. Svigals, Jerome, "SMART CARDS, The Ultimate Personal Computer", Macmillan Publishing Company, New York, 1987.

2. Bright, Roy, "SMART CARDS: Principles, Practice, Applications", R. Bright/Ellis Horwood Limited, Chichester, 1988.

3. Price-Francis, Stephen D., "Philosophy and Benefits of Optical Cards", Canon Canada Inc., Toronto, 1992.

4. Gane, Chris and Sarson, Trish, "Structured Systems Analysis: tools and techniques", Prentice-Hall Inc., New York, 1979.

5. ACT Canada Conference Proceedings, "Advanced Card Technologies", Private, Toronto, 1992.

6. Supply and Services Canada, "Software Exchange Service Catalogue", Supply and Services Canada, Ottawa, 1991.

Appendix D - References

Bastien, Rene
Nova Consulting Services
Montreal, Quebec

Bloor, Barbara
Assistant Deputy Minister
Corporate Management Branch
Communications Canada, Ottawa

Price, Linda
President, ACT Canada,
Toronto, Ontario

Taylor, Colin
Director
Facilities Management and Planning
Communications Canada, Ottawa

Young, Greg
Chief, Advanced Card Technologies
Smart Card Group
Communications Canada, Ottawa