UNIVERSITI PUTRA MALAYSIA

SMART CARD IMPLEMENTATION MODEL

LEE CHIN HUAT

FSKTM 2000 10

SMART CARD IMPLEMENTATION MODEL

LEE CHIN HUAT

IN PARTIAL FULFILMENT OF THE REQUIREMENT
FOR THE MASTER OF INFORMATION TECHNOLOGY
UNIVERSITY PUTRA MALAYSIA

NOVEMBER 2000

ACKNOWLEDGEMENT

One of the most pleasant part in writing this dissertation is the opportunity to thank those who are have contributed towards the success of this dissertation. I would like to thank the person, without their support, I may not have succeeded in completing this dissertation.

Firstly, I would like to express my sincere gratitude and appreciation to my Dissertation's Supervisor, Professor Madya Mohamad Hasan Selamat for his invaluable advice on various issues discussed in this paper.

My special thanks also to my other friends and course-mates who have given me helps and resources throughout the dissertation. These also included all the lecturer who are imparting their knowledge and guidance during the road to success of this dissertation.

Last but absolutely not mean least, a sincere thanks to all the members and staff of University Putra Malaysia, which provides me the facilities and most of the resources and equipment in making this dissertation a successful one.

ABSTRACT

Smart card (intelligent card) systems evolved in the 1970s and progressed through the 2000s, however, their globalization and potential has not yet been achieved. In some countries, France for example, they have been accepted and implemented to a very high degree, while in others the technology is just emerging.

The present research analyses these underlying principles from a business perspective and proposes a set of procedures (a implementation plan) for the design of smart card applications. These procedures are based on the market overview and market prospective from the previous cases as a guideline to implement a smart card.

I describe a generic, scalable plan that may be applied to future smart card operating systems, interfaces, and implementation schemes.

TABLE OF CONTENT

LIST OF FIGURE

CHAPTER 1

INTRODUCTION

1.1 OBJECTIVE

The objective of this research is mainly to review the current local government and worldwide government smart card projects in order to form a methodology for developing a smart card implementation model as well as the literature support from reading materials. From the previous leading smart card companies showcase the latest in solutions based on Sun's Java Card technology and the Berlin Smart Card Transit System. And from the latest technologies the methodology for smart card implementation plan can be achieved by any agencies.

1.2 DEFINITION OF SMART CARD

According to Gold (1996), *Smart Card Technology Background Paper* , identical in size and feel to credit cards, smart cards store information on an integrated microprocessor chip located within the body of the card. These chips hold a variety of information, from stored (monetary)-value used for retail and vending machines, to secure information and applications for higher-end operations such as medical/healthcare records. New information and/or applications can be added depending on the chip capabilities.

Different types of cards being used today are contact, contactless and combination cards. Contact smart cards must be inserted into a smart card reader. These cards have a contact plate on the face which makes an electrical connector for reads and writes to and from the chip when inserted into the reader.

Contactless smart cards have an antenna coil, as well as a chip embedded within the card. The internal antenna allows for communication and power with a receiving antenna at the transaction point to transfer information. Close proximity is required for such transactions, which can decrease transaction time while increasing convenience.

Defined at its highest level, a smart card is a credit-card sized plastic card with an embedded computer chip. The chip can either be a microprocessor with internal memory or a memory chip with non-programmable logic. The chip connection is either via direct physical *contact* or remotely via a *contactless* electromagnetic interface.

1.2.1 Characteristics

As in other computers, the main elements of a smart card are processing power, data storage and a means to input and output data and a power source.

ISO 7816 outlines the basic standard characteritics of the smart cards. The key elements include:

Microcomputer: This is a small computer with no peripheral devices computer with no peripheral devices or SPOM (Self-Programmable One-chip Microcomputer). Specified not to be more than 25mm in width or length under ISO 7816 standard, it is to fit onto

any typical credit card. The 8 metallic pads provide serial transfer of data between card reader and the card's microcomputer.

- Memory: Memory allows data to be written to it and/or read from it. In most smart card applications memory is in the form of non-volatile memory, retaining data when power is switched off. Memory in smart cards can be categorised into types; ROM (Read Only Memory), RAM (Random Access Memory) and PROM (Programmbale ROM). ROM is non-volatile and the content is embedded into the chip during manufacture. RAM is volatile and is used as temporary storage space. Data can be written, altered, read and deleted from it. While EPROM (Electrically Programmable ROM) cannot be reprogrammed, EEPROM (Electrically Erasable Programmable ROM) is reprogrammable.
- Input/Output: Input and output of data varies with the type of card. The metallic surface of contact card provides the link when inserted in a read/write device while a contactless card utilises a method of radio frequency transmission and receptio of data which requires the card to be held on or near a read/write device.
- Power Source: The power source for smart cards could either be from a current generated through contacts on the card, by transmitting power or by a battery embedded in it.

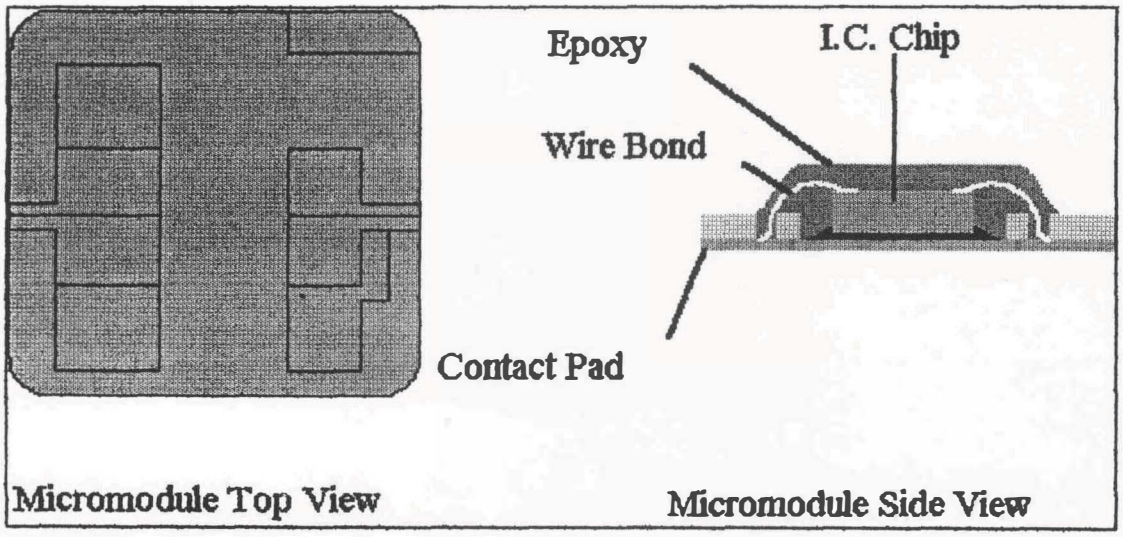
1.2.2 Contact Smart Card

There are two general categories of smart cards: contact and contactless smart cards. A contact smart card requires insertion into a smart card reader with a direct connection to a conductive

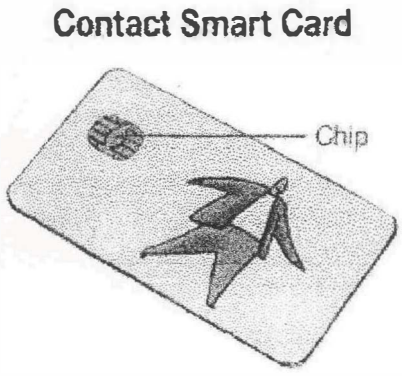
micromodule on the surface of the card (typically gold plated). It is via these physical contact points, that transmission of commands, data, and card status takes place.

A contact smart card requires insertion into a smart card reader with a direct connection to a conductive micromodule on the surface of the card (typically gold plated). It is via these physical contact points, that transmission of commands, data, and card status takes place.

Figure 1.2.2 A contact micromodule which is embedded into a plastic substrate.



Contact Chip Diagram



This diagram shows the micromodule embedded into the plastic substrate or card. Prior to embedding, a cavity is formed or milled into the plastic card. Then either a cold or hot glue process bonds the micormodule to the card.

1.2.3 Contactless Card

A contactless card requires only close proximity to a reader. Both the reader and the card have antenna and it is via this contactless link that the two communicate. Most contactless cards also derive the internal chip power source from this electromagnetic signal. The range is typically two to three inches for non-battery powered cards, and this is ideal for applications such as mass transit which require very fast card interface.

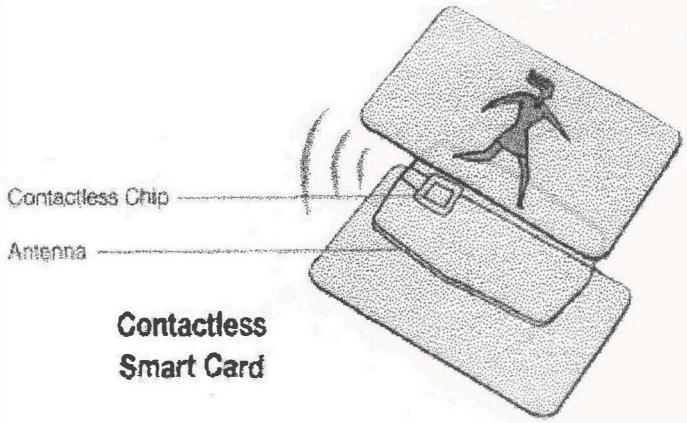


Figure 1.2.2 This diagram shows the top and bottom card layers which sandwich the antenna/chip module. The antenna is typically 3 - 5 turns of very thin wire (or conductive ink), connected to the contactless chip.

1.2.4 Hybrid Card & Combi Card

Two additional categories, derived from the contact and contactless cards are Combi cards and Hybrid cards. A Hybrid card has two chips, each with its respective contact and contactless interface. The two chips are not connected, but for many applications, this Hybrid serves the needs of consumers and card issuers.

Just emerging is the Combi card which in a single chip card with a contact and contactless interface. With Combi cards, it is now possible to access the same chip via a contact or contactless interface, with a very high level of security. The mass transportation and banking industries are expected to be the first to take advantage of this technology.

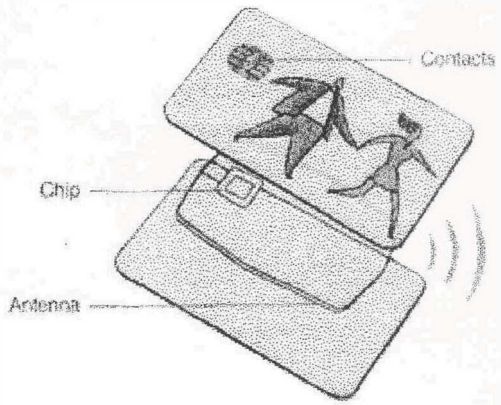


Figure 1.2.4 This shows both the contact and contactless elements of the card. A Combi Card has only one chip while a Hybrid card has two.

The chips used in all of these cards fall into two categories as well: microprocessor chips and memory chips. A memory chip can be viewed as small floppy disks with optional security. Memory cards can hold from 103 bits to 16,000 bits of data. They are less expensive than microprocessor cards but with a corresponding decrease in data management security. They depend on the security of the card reader for their processing and are ideal when security requirements permit use of cards with low to medium security.

1.3 PRIVACY CONCERNS

Today's society is often characterized as an "information society". Technological developments, particularly in the areas of computers, telecommunications and miniaturization, have meant that "greater quantities of information can now be stored and transmitted by a greater number of people, at higher speeds, at lower costs, to multiple remote locations." This ability has fundamentally changed the character of the modern organization and the society in which it is

embedded.(134) As noted by Ursula Franklin, Professor Emeritus at the University of Toronto, in her CBC Massey lecture on "The Real World of Technology", modern realities have been restructured through technological activities.

The information society has been described by many in rather bleak and almost sinister terms: More transactions will tend to be recorded; the records will tend to be kept longer; information will tend to be given to more people; more data will tend to be transmitted over public communications channels; fewer people will know what is happening to the data; the data will tend to be more easily accessible; and data can be manipulated, combined, correlated, associated and analyzed to yield information which could not have been obtained without the use of computers.

1.3.1 The Used of the Smart Card

This concern is not limited to smart cards, but rather reflects the general concerns about information technology noted above. It is acknowledged that smart cards have the potential to provide benefits in terms of improved customer service, operational efficiency and security, for both the public and private sectors. However, smart cards also have the potential to become a technology of surveillance and control.

The same technology that can help financial institutions reduce credit card fraud, can also censor the cardholder's actions by reporting itself "potentially stolen" when it detects unusual purchases. The same technology that processes tolls for thousands of cars per hour, can be used to track a vehicle's movements. The same technology that allows a shopper the convenience of directly

debiting a bank account, allows the retailer to record that consumer's purchasing preferences for direct marketing purposes. The same technology that enables employers to offer employees the convenience of an electronic wallet for the staff cafeteria, can be used to monitor employees' movements. The same technology that allows a government to facilitate the delivery of programs and services, can be used to monitor and control its citizens.

Professor Franklin noted that promises of "liberation" through technology can become "tickets of enslavement". What turns the promised liberation into enslavement is not the products of technology per se, but the structures and infrastructures that are put in place to facilitate the use of these products.

1.3.2 The Storage of Smart Card

The purpose of a smart card system will largely determine what information will need to be stored on the card. For some systems, such as electronic purse applications, there may be no need to include any personal information on the card. However, many applications will require the smart card to be personalized. This may be limited to just adding the cardholder's name and an identification number, or it may involve the loading of large amounts of personal information onto the card.

A cardholder (i.e., data subject) may expect a smart card to contain personal information relating to the reported purpose of the card (e.g., a health card). However, a smart card system can be designed to prevent the cardholder from determining the full extent of the card's holdings or the purposes for which the personal information is being used. Issued for one purpose with full

knowledge and consent of the data subject, a smart card can be instructed to collect additional personal information, or to use the personal information collected for the original purpose in a manner completely unknown to the cardholder. Features like encryption and secret memory zones prevent the data subject from having access to information on the smart card that the issuer does not want that individual to access.

The three memory zones of a smart card make the location of the data storage of critical importance when personal information is involved and/or when there are multiple users or applications. For example, there are no access restrictions to a smart card's open zone. Therefore, any data, including personal information, stored in that zone will be accessible to all users.

1.3.3 The Information Access in Smart Card

This is a complex question from which many problems relating to the protection of informational privacy arise. The first is, who should be authorized users of the smart card? Although data subjects may be issued smart cards, their role can be designed as one of custodian only. Without conscious and deliberate action on the part of the issuing body to include the data subject as a user, a smart card system can be designed without providing the cardholder with access. For example, if the purpose of the smart card system is to give health care providers access to medical information about a patient, it may not be seen as necessary to provide that patient with a means of accessing the same information. In situations like this, the security features of the smart card would actively work to prevent access by the cardholder.

Authorized users of the smart card are generally designated by the issuing body. Such designation may be done entirely without the consent of the data subject. Cardholders may be required to relinquish the smart card on demand to various authorized users, but can be excluded from the process of determining who should have access to their cards and personal information. Another question is, what exactly does "access" mean? Within a smart card system, there are many variables. Some authorized users will only have the ability to "read" limited information; others will have unrestricted access to all information on the card and be able to "write" to as well as "read" from the card. Here again, the cardholder may not be party to the decisions about the levels of access provided to each authorized user, as these are generally made prior to individual smart cards being issued.

When refusal of a necessary service or benefit is the alternative, the cardholder may not be in a position to question whether it is necessary for a particular individual to use the smart card, or to have access to certain information it contains. This issue speaks to the nature of consent (i.e., a voluntary agreement, or the act or result of coming into accord, free from fraud or duress).(151) If a system is designed so that a service or benefit can only be provided through the use of a smart card, the perceived or stated consequences of refusal to turn over the smart card (e.g., denial of a service or benefit), places the cardholder under duress, thereby making consent meaningless. The data subject's ability to refuse access to their personal information is abrogated. In addition, as complex smart card systems may be confusing to the layperson data subject, "informed" consent should not be assumed (i.e., even if a data subject consents, the full implications of that consent may not be fully realized at that time).

Under the larger question of "who has access to what" on a smart card, there are a number of additional issues that should be addressed:

- **The Personal Information each user**

  Technological improvements in information-handling capability generally have been followed by a tendency to engage in more manipulation and analysis of recorded data. This, in turn, has motivated the collection of data pertaining to a larger number of variables, resulting in even more personal information being collected from individuals.

- **The Controls to restrict unauthorized use, disclosure and copying**

When the cardholder gives his/her smart card to another person to use, the cardholder relinquishes control over the personal information it contains. If a smart card system is not designed with the proper controls, it is conceivable that a user may decide to "download" the information from the smart card to another database, and then use that information for purposes unknown to the data subject.

- **The Integrity of the Smart Card**

Given that any number of users may have access to a smart card, some of whom may have the ability to modify or delete information, there is a concern that data may be modified or destroyed inadvertently or deliberately. An additional concern relating to multiple users/applications is that there may not be a central control to ensure that all the information contained on a smart card is appropriate, valid and accurate.

- **The Level of Security**

It is in the area of security that smart cards excel and can actually function to protect personal privacy. However, the authentication protocol and all the other security measures outlined earlier

in the paper, are not standard features of every smart card. Smart card systems can be designed without security, thereby making them vulnerable to unauthorized access.

1.3.4 The Role of the data subject in the smart card system

The design of any computer system can mitigate against control of personal information by the individual to whom the information relates. With smart cards, by the time a person is issued a card, the entire system has already been designed and operationalized. It is the card issuer, rather than the data subject, who controls the functions and parameters of the system, and determines what information will be collected, retained, used, or disclosed.

It is conceivable that an organization may think that, as the issuing body, it owns the smart card and, therefore, all the information it contains. However, when a smart card contains personal information, the data subject must be considered to be at least an equal partner. This places an ethical obligation on the issuing body to ensure that the data subjects are party to, and notified of, all decisions affecting the collection, retention, use, disclosure and security of their personal information.

CHAPTER 2

THE CARD TECHNOLOGY

2.1 THE TECHNOLOGY

According to Dice (1994), *Chip Architecture for Smart Cards and secure Protable Devices*, in order to fully understand the significance and potential of smart cards, it is necessary to put the technology into context. Smart cards represent but one of a number of different types of plastic cards that fall under the umbrella term of "advanced card" technologies.

2.1.1 Embossed Plastic Cards

The embossed plastic card represents the first step in the development toward advanced cards. The essential functions of this type of card can be understood from a visual inspection. The issuer is generally identified through the print and card colour. The embossed lettering usually shows the name of the holder, as well as other significant data such as identification or account number. Sometimes there is a signature stripe on the back which shows a typical signature of the cardholder in order to allow for personal identification.

The card is essentially a personalized record. Though one could conceive of adding more information (presumably by embossing more letters), the card is essentially static. The information which is recorded is intended to remain the same in each use, and any calculation or manipulation that needs to be carried out in order to complete a transaction must be done elsewhere. The card is a memory but not a processor.

Introduced in the late 1940s, and achieving broad-based acceptance and usage in the 1960s and 1970s, embossed plastic cards are familiar to Canadians who possess social insurance number cards, hospital identification cards, health club membership cards, or even library cards.

2.1.2 Magnetic Stripe Cards

The magnetic stripe card, adopted by major credit card companies in the late 1970s, consists of a plastic card with a thin stripe of magnetic material embedded in its surface. Small spots along the stripe are magnetized in varying degrees to form a code representing the stored data. A magnetic stripe card can store up to 240 characters of information. The magnetic stripe is divided into three tracks, according to international standards, each of which has been designed for different applications. One of the tracks is designated a read/write track and, with appropriate terminal equipment, can be updated.

The magnetic stripe card has proven to be exceedingly successful over the years. It is widely used in the world of banking for credit and debit cards, and to provide access to automated banking machines. In addition, the magnetic stripe card has been adopted for many different non- financial applications (e.g., club membership identification and health cards). Its two main

strengths are low production costs and established standards. However, there are also several drawbacks:

1. the magnetic stripe can be damaged by scratching or exposure to a magnetic field,
2. the cards are easy to counterfeit, and the cards are typically limited to one application per card.

Generally, magnetic stripe card systems use personal identification numbers (PINs) in order to authenticate cardholders. It is unusual to store extremely sensitive information on a magnetic stripe card as the data can be easily read by unauthorized means, although for additional security, it is possible for a limited amount of information to be encrypted.

2.1.3 Memory Cards

There are a number of different types of memory cards -- cards that function solely as data storage devices. The magnetic stripe card is one type. A more advanced memory card has a microchip or integrated circuit with fixed memory functions, but no intelligence or processing power. Further developments in the memory card technology have lead to the development of the optical or laser card.

The size of a standard plastic card, it uses a technology similar to that used to produce optical discs; whereby information is written onto the card using a laser to burn millions of microscopic holes into a thin sheet of optical material (the optical stripe) on the surface of the card. Information is retrieved from the card by a low-powered laser mounted inside a reader/writer connected to a computer.

2.1.4 Smart Cards

Having described a variety of other card technologies, what then is a smart card? Unfortunately, there is no one internationally recognized definition. In fact, there is no agreement on the correct term, as "smart card", "integrated circuit card", "microcomputer card", "intelligent memory card" and "chip card" are often used synonymously.

Some think that the term "smart card" has become a "catch-all phrase for microprocessor-based, card-shaped, data-carrying devices". Others think that the term is a misnomer as formats are not limited to card form, and not all portable data-carrying devices contain microprocessors.

A particularly succinct description is that a smart card is "a credit-card-sized personal computer". However, for the purpose of this paper, a smart card is defined as a credit-card- sized device containing one or more integrated circuit chips, which perform the functions of a microprocessor, memory and an input/output interface. Other devices which perform the same type of functions as a smart card, but which are not standard credit card size, will be referred to as "smart tokens" or "tags".

The microprocessor is the component that makes a smart card "smart", and distinguishes it from integrated circuit memory cards designed to simply store data. The microprocessor and its associated operating system, enable the smart card to respond to external events, to "make its own decisions" concerning where it will store data in its memories, and under what circumstances it will transfer information through its input/output interface.

A smart card may be equipped with three types of memory which are used for different purposes:

- Read Only Memory (ROM) - non-volatile memory containing information loaded at the manufacturing stage, which cannot be altered.

- Random Access Memory (RAM) - volatile memory which retains its contents only while power is applied.
- Programmable read-only Memory (PROM) - non-volatile memory, the contents of which can be altered.

The ROM is used to hold the card's operating system. This consists of all the operations to be executed by the central processing unit (CPU), the management of the PROM, the security rules, the communication protocol and the encryption/decryption functions.

The RAM is used by the CPU for the management of internal or temporary data and for storing intermediate results. When the card is disconnected from the power supply this information is lost.

The PROM has both erasable and non-erasable memory. The PROM memory is able to retain information without a power source, and is the key to the smart card's flexibility. With PROM, information can be stored, retrieved or altered in the memory. The PROM in smart cards is regarded as being composed of three memory "zones" -- open, working, and secret.

The open zone is used to record information available to all, such as the cardholder's name and address. Although this area can be read by anyone, it cannot be overwritten.

The working zone is more secure and can only be accessed under the microprocessor's control. This area may contain information specific to the cardholder, such as authorization limits and transaction details.

The secret zone is strictly confidential and controlled by security logic in the 'chip'. The cardholder cannot access it and it is therefore used for storing information such as a cardholder's Personal Identification Number (PIN).

Generally, a smart card system contains a card, a reader/writer device, a terminal, a host computer, and the connections necessary to interface these components. A smart card works under the control of its microprocessor which requires a power source. Once connected to a terminal, it is powered on and is able, by accessing the operating system and instructions stored in ROM, to function as a computer.

A smart card communicates to external terminal devices through its input/output functions which may use either metal contacts on the face of the card, or inductive coils or high-frequency antennae (known as contactless smart cards).

The microprocessor's CPU controls the internal channels through which it can access all the memories. The CPU also manages the communication line enabling the microprocessor to communicate with the outside world through a smart card reader. No direct access to the memory of the smart card is possible from the outside.

The amount of memory available varies from card to card. The majority of smart cards offer eight kilobyte (K) memory, but 24K and 64K cards are now commercially available, and one megabyte cards are in development. Although these memory capacities are available, many current applications operate on two and three kilobyte cards, with the pre-paid applications in telephone systems generally operating on less than one kilobyte.

In order to understand why smart cards can be used in such a wide variety of applications (discussed in the next section of the paper), it is necessary to understand that the fundamental operations of the card are various forms of information transmission, manipulation and recording. Several critical information management functions are discussed below. This