Pre-paid Petrol Refill Smart Card for Petronas Stations

By

Faizad Bin Nik Abdul Aziz

Dissertation submitted in partial fulfillment of
the requirements for the
Bachelor of Technology (Hons)
(Information Technology)

DECEMBER 2004

Universiti Teknologi Petronas
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

Prepaid Petrol Refill Smartcard for Petronas Stations

By

Faizad B Nik Abdul Aziz

A project dissertation submitted to the
Information Technology Programme
Universiti Teknologi PETRONAS
in partial fulfillment of the requirement for the
BACHELOR OF TECHNOLOGY (Hons)
(INFORMATION TECHNOLOGY)

Approved by,

_____

(Mr. Low Tan Jung)

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK
December 2004

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

(Faizad B Nik Abdul Aziz)

ABSTRACT

This document represents the final dissertation for the Final Year Project. The purpose of the dissertation is to present the documentation of the project.

The title in question is Prepaid Petrol Refill Smartcard for Petronas Stations. The title itself explains the general idea behind the project is to provide an advanced stored value of money in electronic card for paying petrol refilling at Petronas stations. It is also to promote a cashless environment at all Petronas stations.

In the problem statement section, discussion will be concerning problem identification and the significance of the project, which is to provide a more efficient and reliable payment system for petrol refilling.

The scope of study will focus on smartcard technologies and its realization into a prepaid system. With that in hand it is hopeful that a workable prototype will be able to be produced to demonstrate its usefulness in a real world environment.

Methodology will be based on the Waterfall model which consists of five steps which are planning, analysis, design, and implementation and testing.

Findings and its relevancy to the objectives of the project will conclude the report based on the discussions mentioned above. Also, additional information will be included where seemed appropriate.

In Results and Discussion, topics will be about the critical segments of a smartcard technology implementation and some of the issues in using smartcard in today's electronic commerce.

ACKNOWLEDGEMENTS

Naturally, my utmost gratitude goes to Allah S.W.T. for all his Grace and Blessings which have made this project possible.

My warmest regards goes to Mr. Low Tan Jung who acted as my supervisor. His patience and guidance were exceptional in standing by me through thick and thin. My appreciation also goes to Ms Vivian Yong Suet Peng and Mr. Mohd Noor Ibrahim who, as Coordinators for the Final Year Project subject, oversaw the entire progress and running of the course through out the entire semester.

A reserved thank you for both of my parents who have stood by me and cheered me on, giving moral support when things have gone tough and acknowledged me in times of success.

Last but not least, a heartfelt gratitude for my colleagues and friends who have always been there when I was in the need of help and kept me focused in completing this project.

TABLE OF CONTENTS

ABSTRACT			**iii**
ACKNOWLEDGEMENTS			**iv**
CHAPTER 1:	**INTRODUCTION**		**1**
	1.1	BACKGROUND OF STUDY	**1**
	1.2	PROBLEM STATEMENT	**5**
	1.3	OBJECTIVE AND SCOPE OF STUDY	**7**
CHAPTER 2:	**LITERATURE REVIEW AND THEORY**		**8**
CHAPTER 3:	**METHODOLOGY**		**12**
	3.1	PROCEDURE.	**12**
	3.2	TOOL	**16**
CHAPTER 4:	**RESULTS AND DISCUSSION**		**17**
	4.1	TECHNOLOGY AND PLAYERS	**17**
	4.2	SMARTCARD ARCHITECTURES	**19**
	4.3	STANDARDS AND SPECIFICATIONS	**21**
	4.4	SMARTCARDS AS A PAYMENT SYSTEM	**23**
CHAPTER 5:	**CONCLUSION**		**26**
	RECOMMENDATIONS		**30**
REFERENCES			**32**

CHAPTER 1

1 INTRODUCTION

1.1 Background of study

It was during the 1980's that France's Public Telephone and Telegraph System introduced a coinless public telephone system. The system used a "smart" card to hold prepurchased value and when inserted into the telephone card reader, it can be used to activate a call and cost will be deducted from the card.

As this new trend began to grow, a new generation of smartcards began to emerge using an embedded microprocessor to control and safeguard the "exchange" of electronic currency. Apart from being a substitute for cash, these smartcards also provide other benefits such as fraud control for credit and debit cards, storage of emergency medical information and ticketless travel on airlines, subways, buses or trains.

Smart cards growth in Different Industries

The telecommunications industry currently deploys the majority of smart cards for use in GSM (global system for mobile communications) digital cellular, mobile radio and emerging PCS (personal communication services) systems. These digital cellular technologies use a smart card, or smart card chip, within the telephone handset to enable secure identification and payment of phone calls.

Insurance and health care companies around the world have also adopted smart card technology. In Germany, for example, 78 million chip cards are used to store health care insurance data, including demographic information, payment responsibility and entitlement benefits. Considering that there are hundreds of millions of potential users for each of these applications, a multibillion-dollar smart card industry will shortly be a reality.

Electronic commerce

Electronic commerce is defined as any monetary transaction that occurs electronically as opposed to the physical exchange of money or checks. In an electronic transaction, e-money is exchanged at the point of interaction after secure information is transmitted across communication lines. Tangible currency is eliminated and accounts are adjusted electronically to reflect the effects of the transaction. For example, an electronic commerce point of interaction may be a pay-per-view or on-demand cable program or a TV connected via modem to the Internet, providing access to a virtual shopping mall. Within this framework, the smartcard becomes the electronic key that will unlock a universe of services.

Shoppers in an electronic commerce system do not sign a charge ticket or show a photo ID while shopping; they are viewed as anonymous bits and bytes as opposed to familiar faces at a town store. Within this environment, the smart card takes over the role of consumer identification, electronically secures the link between the merchant and the customer, and authenticates the form of payment.

As the electronic world becomes larger and more impersonal, we will need newer, more efficient technologies to provide reliable identification. Security must improve to lower the risk of fraud without decreasing the performance of the card system.

Implementations of electronic commerce continue to leave the laboratory and enter the pilot-testing stage. Consumer banking services have been enhanced through the introduction of branded financial products, such as Visa Cash and MasterCard Cash, to electronically replace the coins and dollar bills used for purchasing small items such as newspapers and sodas. These stored-value card systems, also known as *e-cash* or *electronic purse*, are being implemented around the world and include, for example, NETS in Singapore, NET/1 MegaLink in South Africa, SEMP in Spain, and Proton in Belgium, The Netherlands, Switzerland, Sweden, and the Philippines.

Successful Smart Card Applications

There two types of smartcards; contact and contactless.

Contact cards

The contact card smartcard is the most common. For the data inside the card to be read, it has to be inserted into a card reader, hence the contact. Contact cards are further divided into two; microprocessor cards and memory cards. For memory cards, they are straight memory, segmented memory and stored value memory. For microprocessor, they range from the 8-bit low performance OS to the 32-bit high performance OS.

Example

First Union's "Spot Card" for the NFL's Jacksonville Jaguars

Among the newest franchises in the NFL, the Jacksonville Jaguars have introduced a disposable, stored-value chip card produced by Schlumberger. The card, with a value of $20, $50, or $100, was implemented in concession and souvenir stands throughout the stadium to speed payment time, reduce errors caused by direct cash transfers and limit theft. The plan also allows for a general issuance of the card to First Union Bank customers as a reloadable debit card for various retail and transportation use throughout the community.

Contactless cards

The contactless card uses Radio Frequency (RF) signals to communicate with its reader. The first type of contactless card is very close proximity (less than 1 millimeter) cards, in which the reader/writer coupling devices in the card and the terminal must be very precisely aligned. Now, contactless cards allow remote coupling. Remote-coupling cards can operate within distances of a few centimeters to as many as 3 to 5 meters.

Example

Hong Kong's Contactless Transit Card

ERG Ltd., an Australian systems integration firm, created a potential model for future transit applications with its automatic fare-collection pilot for Hong Kong's various independent public-transport divisions. The system will involve the production and distribution of 3 million reloadable, contactless cards (cards "waved" in front of the reader rather than inserted into it) for use in 400 fare-collection sites located in14 mass transit stations.

Initially, directed by Creative Star Ltd. (a joint venture formed by Hong Kong's Mass Transit Railway Corporation, Kowloon Canton Railway Corporation, Kowloon Motor Bus Company, City Bus, and Yaumati Ferry), the system allows access to all modes of public transit. Its flexible design will allow stored-value upgrades for use in city parking lots, retail stores, and pay phones.

1.2 Problem statement

1.2.1 Problem identification

- Presently, people who come to Petronas stations to have their vehicles refueled have two ways to pay for the commodity, which is either by cash or credit card.
- Customers would normally have to worry the amount of cash they are carrying should they wish to refill petrol.
- Payment by credit card will also include all the hassle associated with credit card use such as interest rates.
- Probably the direct comparison that can be made with a prepaid smart card is a credit card.
- Payment by credit card will also include all the hassle of clearing your outstanding debt.
- Annual fees, current interest rates, finance charges and cash-advance fees are some of the main concerns for credit card users.

1.2.2 Significant of the project

- The community today prefers to bring less cash with them when moving around as practicality is proving to be the new way of life and the prepaid system would certainly fits this agenda.
- The system will be implemented in all Petronas stations and customers would have the opportunity to experience a new mean of payment that will be more secure, reliable, faster and more efficient than before.
- Prepaid smart cards are more direct in conducting financial transactions. They do not require fees or interest rates which have proven to be troublesome.
- Prepaid smart cards require purchasers to pay the amount of stored-value and when the credit finishes, the trade ends there. If the users wish to continue using the system, they may rightly do so.
- With prepaid smart cards, there are no carry-on-balance or future debts involved. The user only spends the amount he/she had already paid for.

1.3 Objective and scope of study

1.3.1 The relevancy of the project

The primary objective of the project would be to introduce a new form of payment for petrol refilling at Petronas stations. The system will be based on a smartcard where users can purchase petrol by using the smartcard and paying it electronically. Smartcard readers will be designated all petrol pumps and the purchasing and topping up of the cards could be done at any Petronas station.

1.3.2 Feasibility of the project within the scope and time frame

The ultimate goal of the project would be to come up with a prepaid system that could be immediately introduced into the real world environment. However, with the time frame of a few months and tight budget along with the amateurish level of knowledge associated with smartcard technology of a university student, the most realistic target would be to come up with a workable prototype that is able to perform the most basic and primary function of the system, which is to handle electronic payment of petrol refilling.

The idea behind this project is to design an efficient and cost effective electronic prepaid system which can be produced locally for the process of refilling petrol at Petronas stations. This project would be reminiscent to that of the Touch 'n Go payment system, which is widely used nationwide, in terms of function and purpose but with a smaller scope in mind. It will be used primarily for the payment of petrol refilling and it is exclusively to be used at Petronas stations only. Purchase of new cards and topping up could only be done at Petronas stations.

CHAPTER 2

2 LITERATURE REVIEW AND THEORY

2.1 Smartcard applications

According to Dr. David Everett (2002) they are two types of smartcard applications that exist today. They are prepayment and authentication. Our focus will be more on prepayment where it further falls into two types which are open and closed systems. Closed systems are when the smartcard is issued by a particular service provider which in this case would be Petronas. These closed systems smartcards use simple memory chips and can be produced by a relatively low cost, typically about 50 cents or less. Dr. Everett also stated that he sees an increase in the closed prepayment schemes in the near future.

2.2 Smartcard growth

Soon Yong Choi and Andrew Whinston (1998) wrote that it is estimated 2.8 billion smartcards are issued annually around the world and 70% of these cards will be used in Western Europe and Asia (p.133 – 134). So it seems that even a small country like Malaysia has the potential to greatly increase the use of smartcards in our daily lives compared to more developed countries like the United States. It is neither a dream nor a fantasy to say that the electronic persona in the digital world will be indeed in the form of a smartcard and therefore, no enterprise solutions should ignore its potential impact on business.

2.3 The Relation between Smartcards and E-Commerce

There is hazy definition on how exactly does smartcards play its role in e-commerce. Gladly to elaborate on this topic is Randy Franklin Smith, CEO of Monterey Technology Group, (1999). He teaches Monterey Technology Group's Ultimate Windows Security course series and is an SSCP and a CISA.

Smart cards enable public key infrastructure (PKI), which in turn facilitates e-commerce. PKI lets you achieve a level of trust for electronic transactions that equals or surpasses that of the paper- and signature-based world. PKI can provide message integrity, privacy, and nonrepudiation. You can't deny you sent a message if you've signed it with your digital certificate because your public key verifies your signature. If a public key successfully verifies a signature, the only person who could have sent the message is the person with the private key. The cornerstone of PKI security is that the private key associated with a digital certificate must remain private. An intruder can use a private key to easily forge transactions.

How Smart Cards Work

Smart cards protect private keys, which are so crucial to PKI. Without smart cards, private keys reside on the local workstation, where they're vulnerable to intruder and physical-access attacks. When you store your certificate on a smart card, the processor inside the smart card generates the corresponding private key directly and permanently inside the smart card. The smart card processes any information that you need to encrypt by using your private key.

This procedure might sound impractical if you need to encrypt and email a file of several megabytes—how can a smart card's relatively slow resources accomplish that encryption? Because, in keeping with PKI's strategy, you don't encrypt actual data with private and public keys. Instead, the system generates a much faster symmetric *session* key to encrypt the file. The system sends the session key and the file, which the smart card first encrypts with the private key. The recipient decrypts the session key with your certificate's public key, then decrypts the data. This way, you're pushing a fairly small amount of data through the smart card.

Smart cards also let you take your private key with you. If you move from one workstation to another without a smart card, you might not have access to your certificate, depending on the PKI software you're using. With a smart card, however, you can go to any system that has a smart-card reader and log on, initiate transactions, sign and encrypt email, and so on. Eventually, when truly public PKI exists, you might perform the same actions at Internet kiosks in an airport. By sequestering the private key within the smart card, you sidestep many risks. In "Protect Your Passwords," October 1998, I described the many ways to steal Windows NT passwords that are stored on the local system. As intruders turn their attention to PKI, I anticipate similar incidents of intruders stealing locally stored private keys.

Smart cards also reduce password risks. Users often neglect to create quality passwords; therefore, intruders can easily guess those passwords. Passwords are also vulnerable to network eavesdropping and intruder programs. Smart cards provide much stronger two-factor authentication: The user must physically have the smart card and must know the card's personal identification number (PIN). Even when a user misplaces the smart card, an intruder has only a few chances to guess the correct PIN before the smart card permanently locks itself. As soon as the user reports the lost card, the PKI software can revoke the certificate and render it invalid even if the intruder discovers the PIN.

2.4 Electronic Purse

The following is from Dr. Keith M. Jackson explaining the concept of electronic purses and the virtues of smartcards in the conundrum.

What is an Electronic Purse?

I'm sure that various people working on the several different purse systems that are being implemented would come up with slightly different definitions. That would be reasonable. However I want to discuss electronic purses in general, so I've tried to stay system independent. Apologies in advance if I have failed in this laudable aim.

In very general terms - an electronic purse is a software application that controls how much value is available to be used by the owner of the purse.'

Note that the insertion of the words 'software application' immediately requires that an electronic purse is controlled by its own processor.

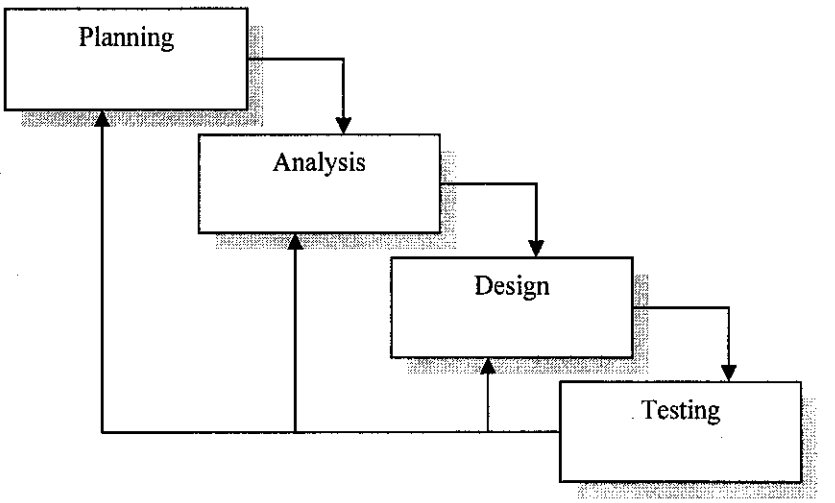
Note also that the definition does *not* include any mention of a Smart Card. Although many (most? currently all?) electronic purse systems are being implemented using Smart Cards, this is not a *requirement* for making an electronic purse available.

So why are Smart Cards used?

I mentioned previously that an electronic purse requires a processor, but this processor must operate *exactly* as it has been designed to do. It needs a secure environment. A Smart Card is just the cheapest way of obtaining a processor that is executing in a secure environment.

Based on those reasons, it is decided that the project will be based on the Waterfall model. The model's four phases are:

- Planning
- Analysis
- Design
- Testing



3.1.1 Planning

System planning begins with a formal proposal or request for the project. In this phase, the purpose is to identify clearly the nature and scope of the business opportunity or problem by performing preliminary investigation or also called as feasibility study. The outcome from this study is project scope.

As my project deals with smartcards, the initial step for me is to gather information and find out more about smartcard technology. The first question that needed answering is "What is a smartcard?". There are various types of smartcards depending on their functions and security level desired. The next question is on how does one come up with his/her own smartcard system. Various issues have to be covered including the architectures and the level of security algorithms to ensure reliable transactions.

The university's resource center would be my main destination for information gathering. I would have to go through books, articles from magazines and newspapers and not to forget research journals. I have also gone online for resources on the Internet.

3.1.2 Analysis

The purpose of this phase is to understand the requirements and build a logical model for the system. The end product of this system analysis phase is the system requirement.

For this next stage, data gathering is performed concerning smartcards. The main areas covered are the smartcard architectures, where the physical architecture of the single-chip microprocessor card is studied. Among the areas of concerned are the smartcard hardware, including size and type of memory needed, necessity of a coprocessor for dynamic security authentication, processor clock speed, and proper testing methodologies to ensure that the software works as designed. Standard and specifications are not forgotten where analysis will include the standards for cards and card interfaces in addition to the mergence of industry-specific specifications. Lastly, the security and cryptography is looked into on how smartcards has introduced an entirely new approach toward securing information and financial transactions, much of which will be done through dynamic authentication using cryptographic signatures.

3.1.3 Design

In this phase, all necessary outputs, inputs, interfaces, and processes were identified. The storyboard was developed during this phase as it was done concurrently with system analysis phase.

The author would have to look at the design considerations for implementing a smart card system which include the complex design process and tools available to facilitate the development effort.

System Implementation Considerations; discussions will focus on the tools available to the developer, including off-the-shelf operating systems and component toolboxes and emulators.

Functional Design and Data Layout Considerations; a matrix of possible data elements is outlined to help identify the data that is important to specific implementations. Also discussed is the relative importance of the technical components that must be developed or purchased in order to store and retrieve data, as well as the importance of the design and layout of card memory in sizing the right type of card for the system.

Operating Systems and the Card-To-Terminal Interface; it is known that the number of operating systems available today is limited. Choosing one over another may dictate the chip manufacturer, the security capability, and the card acceptance device (CAD) type for the proposed application or system.

System and Data Integrity; to examine ways to back up card-based information and describes some strategies that can be used to preserve the system's integrity.

3.1.4 Testing

The final step in the methodology is the testing phase of the application. This step is to ensure that the application is functioning as it is supposes to. I have failed in securing a card and reader package that was planned earlier in the project timeline. However, I did manage to download a few source codes from the internet and construct a decent application which is also able to perform a reloadable card system.

The application has a few flaws that require attention in order to make it work. The testing phase is specifically to eliminate that problem and deliver a workable application.

3.2 Tools (Equipment, hardware, etc.) required

Personal Computer

⇒ Pentium 4 2.8GHz, 256 MB of RAM, Windows XP Professional

Smartcard Development kit:

- Smartcards
- Smartcard reader
- Software Development Kit

CHAPTER 4

4 RESULTS AND DISCUSSION

In this chapter, discussion will focus on how to design, build, and manage a smartcard system. Also a few issues will be discussed regarding on the smartcard technology and is critical segments and smartcards to be used as a mean of payment in today's economy and living trend.

4.1 Technology and Players

For smart cards to carry out applications, several components must come together. The technology of smart cards includes four critical segments.

4.1.1 Card Manufacturers

A smart card begins with a micro-controller produced by semiconductor manufacturers such as Siemens, Motorola and Thomson. This integrated circuit chip is attached to an electronic module by inserting into a cavity on the module. Then, terminals between the chip and the electronic module are interconnected. Finally, the chip-embedded electronic module is glued to a plastic card. The global leader in card manufacturing is Schlumberger who sold about half of all smart cards in use in 1997. A close second is Gemplus followed by Bull and De La Rue of France.

4.1.2 Card Terminals and Readers

Smart cards may be read by conventional card reader or by wireless terminals. New devices similar to a floppy disk allow smart cards to be read by PC disk drive. Suppliers of POS and ATM card readers have expanded into smart card readers for their product lines, where some worldwide consolidation is occurring. For example, a market leader Grupe Ingenico is buying another player De La Rue of France.

4.1.3 Interface between Card and Terminal (API)

Electronic modules embedded in smart cards have contacts by which messages are exchanged between the card's IC chip and the card reader. International standards such as ISO 7816 have specified which contact handles what type of data but applications must be programmed to manage message exchanges that can be used by networked processors. An interoperable and multi-platform application programming interface (API) is critical for smart cards to carry out diverse functions. Open standards such as Java smart card API provides one of several proposed interfaces. Java Card API in particular offers a development tool for flexible, multi-platform applications–"Write Once, Run Anywhere"–for devices ranging from Network Computers, Web TV, smart phones and other consumer appliances. The industry leader Schlumberger, for example, has introduced EasyFlex and FastOS based on Java API.

4.1.4 Applications

The ultimate utility of smart cards is in the functions they carry out–for example, payment process, identification, network computing, health care management, benefits distribution and so on. Application programs handle data read by smart card readers and forward them to central computers located at the other end of the smart card infrastructure such as payment servers in banks, traffic control centers or mobile phone centers, credit card companies, transit authorities, governments, Microsoft and other service providers. Market players and stake holders in this end game for smart cards include a wide variety of firms and institutions including card issuers, content providers, Visa and MasterCard, banks, government agencies, security implementers such as Lucent Technologies, electronics manufacturers such as NEC, and service providers who want to exploit advantages of smart card technologies.

4.2 Smartcard Architectures

A smart manager will certainly analyze the overall architecture of the smartcard, terminals, and card readers that make up the system. The issues facing the manager involve the type and use of memory, communications protocols, and speed, the need for dedicated coprocessors, and the choice of operating system and mask (the part of the application written into ROM). In order to gain maximum functionality within the physically small smartcard, trade-offs must be made. These trade-offs occur because the physical limitations of the chip force smartcard programs and systems to be written and implemented in slightly different ways than those developed for PCs.

Smartcard systems have typically been implemented using assembly-level or low-level language to program the applications that are loaded inside the cards and terminal readers. These programs allow the card and the reader to communicate with programs written with a higher-level software, such as COBOL or C, on host computers. Improvements in software technology and in the smartcard themselves should encourage the development of more smartcards effective ways of creating smartcard programs by using interpreters, applets (such as Java), and application development toolkits.

Let us look more closely at today's smartcard architecture and the layout of single chip microcomputers.

4.2.1 Memory cards

Memory cards and all smartcards for that matter, have some form of memory storage. Memory cards are primarily designed for storing information or values and are commonly used for applications such as disposable prepaid telephone cards used in public telephones. These cards are already in use in over 100 countries around the word.

Three major telephone companies in the United States and Bell Canada in Canada are deploying third-generation disposable telephone cards that contain no computing power whatsoever. They are designed only to provide information to a telephone equipped with a special card acceptance device (CAD) or reader. The card provides the telephone as

identification number, which may be or may not include an embedded PIN number. The PIN ensures that only the telephone operating company that is entitled to take money from the card can read and authenticate the card. The card also stores value that is decremented as telephone calls are made.

General characteristics of memory cards

Memory cards have product options such as register size and memory access time that need to be considered when developing smartcard applications. Larger registers allow more data to be accessed or processed at one time.

General protocols for communicating with memory cards do not exist. There are no international standards that regulate the communications protocol between the cards and the terminals. In addition, there are no standards for laying out memory on the cards. The memory can be allocated in any form that the hardware and application designers deem necessary. There is also no uniform definition for the security procedures required to decrement the value of the card or authorize the value remaining on the card. The lack of standards almost guarantees that cards deployed for one system will not work for another.

Memory cards, sometimes referred to as *synchronous cards*, communicate through a defined set of pathways. The synchronous communications process is under the control of the terminal.

EEPROM (Storage-Only) Memory Cards

An EEPROM memory card is a storage card with rewritable memory. These cards are used to store information such as buyer profile for loyalty card programs or database information that might be carried from one application to another. EEPROM memory can be designed as free memory in any format since no standards regulate the allocation of data space inside the card.

Memory card with Registers

These second and third-generation cards, with very limited memory sizes, use an abacus-style counting method. The abacus method uses a limited-intelligence-register approach. The registers use hard-wired logic to decrement a large number through a series of counter stages with decreasing values. When all the counter stages have been exhausted, there is no money or value left on the card. Since these cards are not rewritable, they are discarded.

4.3 Standards and Specifications

According to the International Standards Organization (ISO), "Standards are documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose." Standards can be anything from a two-page document to a 1500-page volume. A standard will specify tasks that a piece of equipment must be able to perform or describe in detail in apparatus and its safety features.

Typically, a specification is a narrowly defined interpretation of a standard. The formation of a specification usually starts with an existing standard. Certain decisions are made about the various technical alternatives authorized for implementation. The specification defines in detail the technological parameters for the intended application.

4.3.1 Standards

Plastic card standards

The application developers adopted the existing standards for cards with magnetic stripes and embossing as their reference points. These standards established the physical characteristics of plastic cards and fixed the location of the magnetic stripe on the back and the embossing on the front of the cards. The chip and module can be positioned on the card without violating existing standards, thus allowing a smooth migration from magnetic stripe card to chip card.

Smartcards are embossed (i.e., having a raised surface on the card showing a name or other information) or equipped with a magnetic stripe can be used in any of the three modes. The information on the card can be accessed by reading the chip, swiping the magnetic stripe, or making an imprint from the embossing.

ISO 7810 establishes a baseline for the magnetic stripe cards used worldwide for credit and debit applications. This standard defines the location for both the embossing and the magnetic stripe.

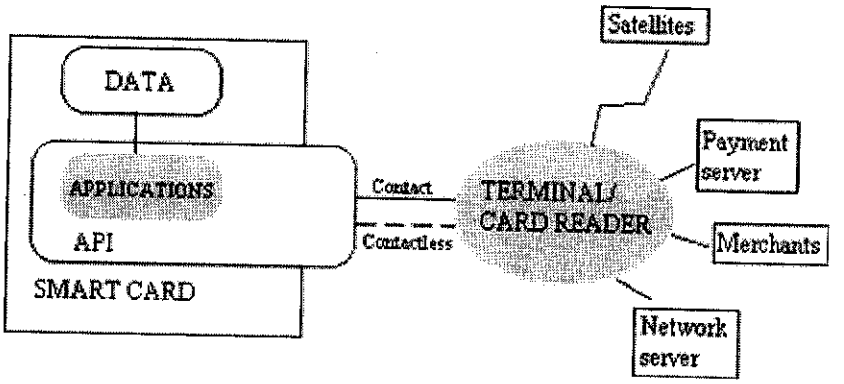
Contact Card standard

The second major reference standard for smartcards is ISO 7816, which addresses cards embedded with either microcontroller or memory-only chips. The standard describes the location of the contacts for both types of cards. In the case of the memory cards, however, the standard does not describe the operation of the wires and connections.

ISO 7816 consists of a number of parts (distinct sections). Each part contains specific minimum requirements for the physical characteristics, layout, data access techniques, data storage techniques, numbering systems, and registration procedures.

4.3.2 Specifications

The first and perhaps most significant of the specifications that have been developed is the EMV specification. EMV is an acronym for Europay, MasterCard, and Visa, the three global card franchise associations representing the 22000 financial institutions that issue credit cards around the world. EMV-1, describing the card and chip environment. EMV-2, described the terminal environment. EMV-3, describes the specific manner in which cards and terminals will authenticate each other, identify the applications on the card and exchange data between each device.



4.2 Smart Cards as a Payment System

A payment function is an integral part of most smart card applications because most services accessible by smart cards must be paid one way or the other. But before smart cards are widely used as a preferred payment method in electronic commerce, two outstanding issues must be resolved:

- legal protection for loss and fraud
- demand and supply for microtransactions

4.2.1 Legal Protection and Liability

Currently, a cash balance stored in, for example Touch N Go, is not insured or protected against loss or theft. In comparison, a credit card user is liable only to a minimum determined by legislation. Being a cash equivalent, however, a stored value on a Touch N Go card is not recoverable if the card is lost or stolen. Several electronic cash payment systems guard against such losses by an elaborate encryption mechanism or a required authentication in each transaction. They, however, add significant transaction costs minimizing their advantages over cash or checks. A cost effective guarantee or assurance on stored values must be established to protect consumers. But legal opinions regarding the liability and rights of issuers and users of electronic cash vary widely. In general, online stored value systems which do not rely on smart cards may be protected by existing federal regulations as long as the funds are considered to be in consumer deposit accounts. Offline systems are left to voluntary arrangements between card issuers or financial institutions and consumers.

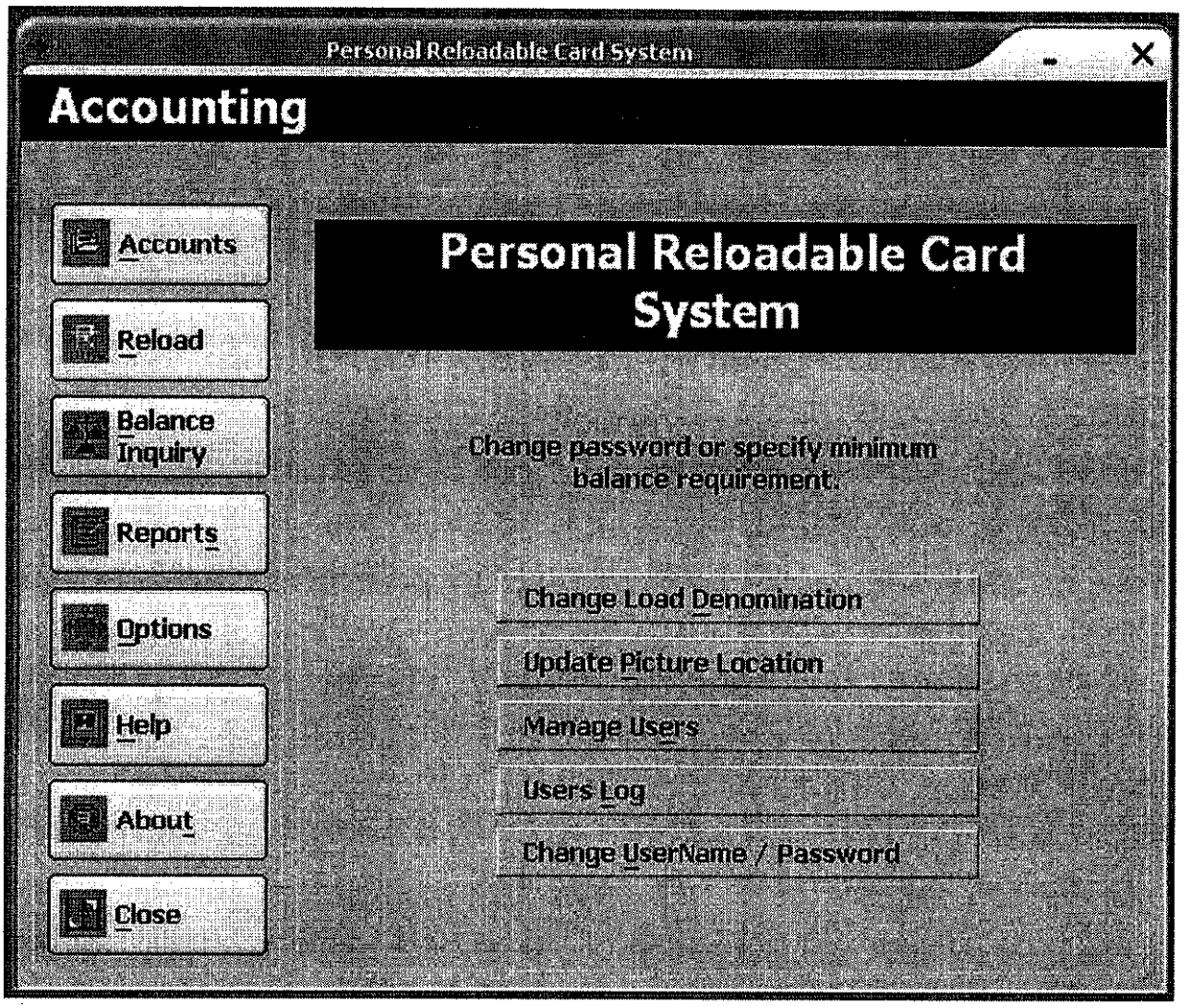
4.2.2 Microtransactions and Micropayments

A more convenient, low-cost payment method is necessary for low-value transactions. There are many examples of micropayments already in use: toll and bus fare collections, copy machine payments, parking meters and vending machines. Coins and tokens used in all of these examples can be substituted by smart cards. However, will there be substantial demand for microtransactions and micropayment methods in electronic commerce? The answer will depend on how information and other digital products are sold online. Bundling and subscription plans are based on aggregating small charges into a periodic bill that is large enough to utilize conventional credit card payments. If sellers and consumers prefer to aggregate products and services, there will be little need for a flexible payment system. On the other hand, unbundling and customizing products require a payment system which can facilitate small charges, for example one or two cents for a Web page. Before smart cards and electronic cash are used widely, the demand for, and supply of, microproducts and microtransactions must precede.

Even when these issues are resolved and smart cards become a preferred payment method for electronic commerce, the excitement over smart card technologies and the ready embrace by many developers of these technologies are due more to the explosion of applications than to being a convenient form of payment. The smart card platform has already expanded into the mainstream computing and commercial arena as a versatile technology to implement innovative services in a mobile network.

4.3 The Application

The final output for this project is an application named the Personal Reloadable Card System. The application is compatible with Microsoft Visual basic 6.0 running on Windows XP. It is a point of sale program that uses reloadable card (which can be the user's ID) instead of cash. The Accounting feature supports the reloading and managing accounts. The reports use data dynamics reporting engine. The whole application is included in the CD accompanying this report.



Main page screenshot

CHAPTER 5

5.1 CONCLUSION

5.1.1 The Future of the Industry

Credit, debit, ATM, loyalty and membership cards have changed our lives and the way we conduct business. We use them to obtain cash, track frequent flyers miles, and gain access to secure areas. I anticipate the formation of entirely new business organizations based on smart cards to be launched in this millennium.

The smart card industry is quickly maturing, moving from an analog physical card environment to an electronic one. As a consequence, an entirely new type of commercial landscape is being created. This environment will be far more secure than today's magnetic-stripe and paper-based transactions. Future trends that the world would expect to see include:

- Electronic commerce
- Improved technologies
- New time constraints
- New skill sets
- Easy-to-use applications
- A merging of disciplines
- An increased role of biometrics
- A growing array of appliances
- More sophisticated security
- A greater diversity in the development and innovation of smart card applications

Electronic Commerce

New kinds of information-access scenarios will be available in which the consumer and the merchant will not have to be physically present at a car dealership, grocery store, or restaurant. The consumer, not the merchant, will assume electronic control in many future transactions. Some scenarios predict that as many as 85 percent of the new terminals and card accepting locations under development will be user-driven.

Our TV sets (with over a billion manufactured) and telephones (over a billion phone lines) of the future will have the ability to accept smart cards to enable electronic commerce. There are already millions of digital cellular telephones that accept these cards today. New personal reader devices, such as the Visa viewer, can display your electronic cash balance and your last 10 or so electronic cash transactions. Other devices will evolve as more sophisticated personal commerce and information-access devices become available.

All these devices will be our "PCs" of the future. They will be more than just entertainment devices (like TV sets), points of communication (like telephones), or places to work (like personal computers). These "smart" devices will become points of interaction and electronic transaction in tomorrow's economy. A securable device like a smart card will be important in enabling this vision to become reality. We are at the beginning of a new awareness and a new environment.

Improved Technologies

In setting for future opportunities, you should expect the unexpected (that is, "future-proof" yourself). The smart card industry today is fairly well defined by existing levels of computer technology. We expect to see smart card technology define a path and evolution similar to that of the PC. For example, today's smart cards and those being designed for use through the end of the decade operate at half-duplex. They can either transmit data or receive data, but they cannot do both simultaneously. Tomorrow's smart cards will become full duplex cards with the capability of transmitting and receiving data simultaneously.

These future cards will also run at higher speeds, be ale to perform more secure functions at lower voltage, and have greater storage capabilities – much like the personal

computer of today. More and more of today's features and functions will grow and mature into far more sophisticated systems. Technology and time constraints will be linked in the future.

Merging Disciplines

Electronic commerce will require merging disciplines in several areas, the most important of which is security, as these new transactional systems will increasingly rely on more sophisticated devices. These devices will have various formats and form factors, ranging from contact and contactless chip cards to PCMCIA cards and other personal electronic tokens such as advanced automobile keys, keyless entry systems, or secure identification technologies.

Security

The new security threats caused by the evolution of technology have been anticipated by existing applications developers and card system operators, who are using colleges and universities as testing labs to study the nature of these attacks and how to thwart them. Often, the main threat of attack to defeat or interrupt the operation of the system is not from the causal hacker. The greatest threat is from high-tech organized crime (organized crime has tried repeatedly to penetrate monetary and other high yield systems). Therefore, card and terminal design must have more sophisticated logic and security capabilities, such as certificate authentication and mutual authentication procedures.

Even the personal reader devices would have smart card-complementary logic in order to provide part or the entire authentication between the card and the card-reading device. This implies that the number and complexity of readers will, at a minimum, have the same capabilities as the complex cards in the market. From a system design and architectural perspective the readers will have to be treated as discrete units in the commercial operating environment and may have their own unique cryptographic and addressing methodologies.

This approach is not all that dissimilar to the Internet system architecture of today. However, we must take care to allow sufficient ways top assign unique identification

numbers or addresses, as evidenced in today's Internet and other large, connected, network environments.

5.1.2 Future Applications

Smart cards will quietly revolutionize most sectors of the company. Many cards will find a core application, with additional applications being built on to the primary delivery system, such as an electronic driver's license with state and federal welfare programs launched on top of it. A comprehensive bank card may have applications ranging from merchant loyalty programs and electronic purses to debit, credit, and possibly consumer finance and lending. We should also expect to see ticketless travel and frequent flyer/driver/sleeper programs on multiple-branded cards. Only our imaginations limit innovative applications of the future.

At a certain point, though, the competition and demand will dictate the applications that are developed and implemented. From the technical side, it is a question of making the appropriate trade-offs between the future systems and technologies will evolve on-line (or off-line).

When considering the trade-offs, we must also take note of the increased risk of putting too much information onto a single card.

The risk here is not a technological one, but rather a business and logistical one. The competitive information contained on such a card from members of the airline industry or the retail merchant sector will make a lost, damaged, or expired card very expensive to reissue. The presence of more than one application on a card will make it difficult for the individual cardholder to reconstruct the information on a reissued card. Furthermore, the problem of accessing the enormous numbers of cards is daunting as they proliferate to meet the requirements for products and services of individual cardholders.

5.2 RECOMMENDATION

At the beginning, the main objective of this project is to develop a prepaid smartcard for purchasing petrol refilling at Petronas stations. Regrettably, this project has fall short of that objective. The desired output of a workable system could not be developed. Time and financial constraints could prove to be decisive factors in this failure but as not as much as my own incompetence. Nevertheless, I have gained a lot of valuable knowledge and experience regarding smart card technology and its scenario in Malaysia. One thing for sure, this would not undermine me in undertaking a similar topic in the future.

Even though smart card technology has been around for quite a while, it is limited in Malaysia in terms of resources. Usage over the years has been extraordinarily encouraging especially in the telecommunications and banking industry. However, for a smart card developer, resources are scare. One of the main reasons being that there are very few companies in the country which are involved in smart card development. The most famous two are probably IRIS and Tricubes. In the local smart card industry these are arguably the monopolizing companies. Being that, it is inevitable that they are very strict regarding sharing of information and resources. Information and services that they are willing to hand out to the interested parties are charged at a very high price. It is almost discouraging. For students who are interested in this branch of technology would be disappointed with this outcome as I have. Smart card resources are very exclusive in Malaysia even by normal standards. It is highly suggestive that these types of information and resources be more readily available. This is just so to spark the enthusiasm that this industry needs from young and energetic people.

As far as my project is concerned, the difficulty in securing a smartcard package (i.e. the smartcard and its reader) is one of the factors contributed to my failure in achieving the project's objective. Purchasing such a package would cost in the region of thousands of Malaysian Ringgit. A feasible alternative was to borrow the package from the suppliers. Even so, the approval process takes weeks and that is before the borrower opens and explores what the package actually contains. Usually, the features that came with it are restricted and limited. It would be most pleasing if smart card solution companies in

Malaysia would make their products and expertise more accessible for individuals who are interested in this type of technology.

REFERENCES

1. Dreifuss, Henry &, Monk, Thomas J., (1998), 'Smartcards: A guide to building and managing smart card applications', Wiley.
2. Attali, Isabelle &, Jensen, Thomas (Eds.), (2001), 'Smartcard Programming and Security (International Conference on Research in Smartcards, E-Smart 2001 Cannes, France, September 2001 Proceedings), Springer.
3. Smith, Randy Franklin, (October 1999), Secure E-Commerce with Smartcards, http://www.winnetmag.com
4. Jackson, Dr. Keith M, Security Design for the Electronic Purse, http://www.smartcard.co.uk
5. Everett, Dr. David B, Smartcard Technology: Introduction to Smartcards, http://www.smartcard.co.uk
6. January/February 2002 (Vol. 6, No. 1) p p. 18-24 Building Trust in **E-Commerce** Yacine Atif
7. Soon-Yong Choi, Andrew B. Whinston: The Future of E-Commerce: Integrate and Customize. IEEE Computer 32(1): 133-134 (1999)
8. Soon-Yong Choi, Dale O. Stahl, Andrew B. Whinston: Intermediation, Contracts and Micropayments in Electronic Commerce. Electronic Markets 8(1): (1998)
9. http://www.smartcardbasics.com
10. http://www.iris.com
11. http://www.tricubes.com