A SECURITY PAYMENT MODEL FOR FINANCIAL PAYMENT USING MYKAD

NURUL HUDA BINTI AHMAD ZAHARI

A thesis submitted in
fulfillment of the requirement for the award of the
Master of Information Technology

Faculty of Information Technology and Multimedia
Universiti Tun Hussein Onn Malaysia

APRIL, 201I

ABSTRACT

The Malaysian Government has created smart national identity card named MyKad for every citizen aged 12 and above since September, 2001. In the following year, the National Registration Department of Malaysia (JPN) has embedded the latest application of MyKad, which is known as Public Key Infrastructure (PKI). It allows secure electronic transactions over the Internet. The electronic transactions include online submission of tax returns, secure email and e-commerce. In parallel with the emergence of e-commerce payment system, a new MyKad Payment Model (MPM) is proposed in order to introduce to the public another function of MyKad that is not only for identification purposes, but also in e-commerce transactions. However, to make this payment model accepted by the public, the focus should be made on two issues; trust/security issue and performance issue. A system with security technique named Arbitrary Random Security Algorithm (ARSA) and a one-to-one multithreading model need to be developed in order to accelerate the authentication response time of MPM. ARSA will automatically change its security algorithm based on times and attacks. If there is no attack or intrusion detected, MPM will wait for the scheduled switching within 30 minutes. However, if attack or intrusion is detected in less than 30 minutes, ARSA will automatically change the security algorithm to a new one. The evaluation of the MPM performance is measured with HP LoadRunner testing tools from which it is found that the response time of MPM with multithreading is better compared to the single thread model and credit card authorisation system. Moreover, the development of ARSA makes this model more secure and safer for the customers.

ABSTRAK

Kerajaan Malaysia telah memperkenalkan kad pengenalan diri pintar untuk semua warganegaranya yang berumur 12 tahun dan ke atas sejak September 2001. Pada tahun berikutnya pula, Jabatan Pendaftaran Negara Malaysia (JPN) telah melancarkan aplikasi terbaharu MyKad yang dikenali sebagai Infrastruktur Kekunci Awam (PKI). Aplikasi terbaharu ini membolehkan pengguna melakukan transaksi elektronik dengan menggunakan kemudahan Internet. Transaksi yang dimaksudkan adalah seperti penghantaran borang cukai pendapatan dalam talian, emel yang selamat dan e-dagang. Seiring dengan perkembangan e-dagang kini, Model Pembayaran MyKad (MPM) yang baharu dicadangkan untuk diperkenalkan kepada masyarakat umum bahawa MyKad bukan sekadar digunakan untuk tujuan pengenalan diri tetapi juga untuk transaksi e-dagang. Walau bagaimanapun, untuk membolehkan model ini diterima pakai oleh rakyat Malaysia, terdapat dua isu yang perlu difokuskan iaitu isu kebolehpercayaan/keselamatan dan isu prestasi. Oleh itu, satu sistem yang menggunakan teknik keselamatan yang dinamakan sebagai *Arbitrary Random Switching Algorithm (ARSA)* dan model multijalur satu-dengan-satu perlu dibina untuk mempercepat tempoh respon untuk transaksi MPM. ARSA akan menukar algoritmanya secara automatik mengikut masa dan serangan. Jika tiada sebarangan gangguan atau serangan dikesan, MPM akan menunggu proses penukaran yang dijadualkan dalam masa 30 minit. Namun, jika gangguan atau serangan dikesan dalam tempoh kurang daripada 30 minit, ARSA akan menukar algoritma keselamatan yang baharu secara automatik. Prestasi tempoh transaksi MPM dinilai dengan menggunakan perisian HP LoadRunner dan didapati sistem MPM mempunyai tempoh transaksi yang lebih cepat berbanding model jalur tunggal dan sistem pengesahan kad kredit. Tambahan pula, ARSA membolehkan sistem ini digunakan oleh pengguna dengan lebih selamat dan terjamin.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AES -	Advanced Encryption Standard
ATM -	Automated Teller Machine
CA -	Certification Authority
CAPICOM -	Microsoft security algorithm pack
DES -	Data Encryption Standard
3DES -	Triple Data Encryption Standard
EEPROM -	Electrically Erasable and Programmable Read Only Memory
GSM -	Global System for Mobile
iVEST -	Virtual Environment for Secure Transaction
i -	Starting of Thread
JPJ -	Road Transportation Department
JPN-	National Registration Department
LRT -	Light Rail Transit
LHDN -	The Inland Revenue Malaysia
MAMPU-	Malaysia Administrative Modernization and Management Planning Unit
MD -	Message Digest
MEPS -	Malaysian Electronic Payment System
MIMOS -	Malaysian Institute of Microelectric Systems
n -	Number of concurrent threads
NIC -	National Identity Card
NIST -	National Institute Standard Technology
NITC -	National Information Technology Council
SIM -	Subscriber Identity Module
PDRM -	Traffic Police Officer of Royal Malaysian Police
PIN -	Personal Identification Number
PKI -	Public Key Information

RC - Rivest Cipher

RSA - Rivest Shamir Adleman

SHA - Secure Hash Algorithm

T - Thread response time

UML - Unified Modeling Language

VUGEN - Virtual User Generator

VU - Virtual User

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of Study

A lot of changes had occurred in the development of smart card since it started to be patented in early 1970's. It started with a magnetic stripe card to the latest version, contactless smart card. Until now, smart cards have been used to store small amount of money, as a debit card to pay telephone bills, photocopy, pay transportation to tickets and many more. After the launch of the smart-based Subscriber Identity Module (SIM) card in the Europe in 1990's, the use of this card has finally made sense to the public. This smart-based SIM card is used in Global System for Mobile (GSM) for mobile phones in the European countries (Henry, 2007). Smart card is widely used as an identification card in several countries such as Germany, South Korea and Malaysia. A lot of information can be encoded in the chip card such as health status, driving license, insurance and other important details about oneself.

The Malaysian Government has used smart card as identification card for Malaysian and permanent residents aged 12 and above since its official launching on the 5th September 2001. It incorporates an ATMEL 64K Electrically Erasable and Programmable Read Only Memory (EEPROM) microchip. This chip contains several items of data including biometrics. The Malaysian Government Multipurpose Card or also known as MyKad is a multipurpose card that enables its user to access public and private services. It is regarded as the world's first smart identity card (Knight, 2001).

According to the National Information Technology Council (NITC) (2009), the objective of MyKad is to provide a secure ID platform for private and Government transactions. To date, MyKad project has attracted many private applications but the uptake of public applications has been minimal. The council also reported that roughly RM900 million has been invested in MyKad project, including RM600 million for the purchase of 22 million smartcards. In order to ensure that MyKad application achieves its full potential, various agencies such as Malaysia Administrative Modernisation and Management Planning Unit (MAMPU), National Registration Department (JPN), Pos Malaysia Berhad and NITC itself are required to cooperate. After spending such an amount on developing the project, the use of MyKad is not limited to identification purpose only, but it is also developed to perform different access to Government agencies. Figure 1.1 presents the information contained in the chip of MyKad.

Based on the figure, there are about eight more applications that can be carried out by using MyKad. The applications include driving license information, passport information, health information, frequency traveller card, Automated Teller Machine (ATM) application, Malaysian Electronic Payment System (MEPS) cash (MEPSCASH), Touch ‘n Go and the latest one, Public Key Infrastructure (PKI). For the driving license application, MyKad replaces the paper-based laminated cards and functions as a regular driving license. The users for this application are the Road Transportation Department (JPJ) enforcement officers and the Police Traffic Officers of the Royal Malaysian Police (PDRM). The passport application in MyKad supplements Malaysians to facilitate efficient exit and re-entry from Malaysian Immigration check points. Health information in MyKad stores basic and critical medical information. Another application in MyKad, MEPSCASH facilitates payment of small purchases and enhances the efficiency and quality of public and payment services. For transportation, MyKad can be used for the payment at the toll gates, parking fees, bus and Light Rail Transit (LRT) fares. For banking application, MyKad provides easy and convenient transaction that acts like an ATM card. The functions include cash withdrawal, balance inquiry, and fund transfer. Finally, the latest application implemented, PKI provides confidentiality, integrity, non-repudiation and authentication.

Out of eight applications mentioned earlier, by far, the application that is emphasised in this research is the PKI application. PKI enables the users to conduct

secure electronic commerce and transactions using digital certificate over the networks such as the Internet. The authenticity and integrity of the data are protected and inaccessible to anyone, except from the relevant Government agencies and the owner of MyKad (Clarke, 2005).

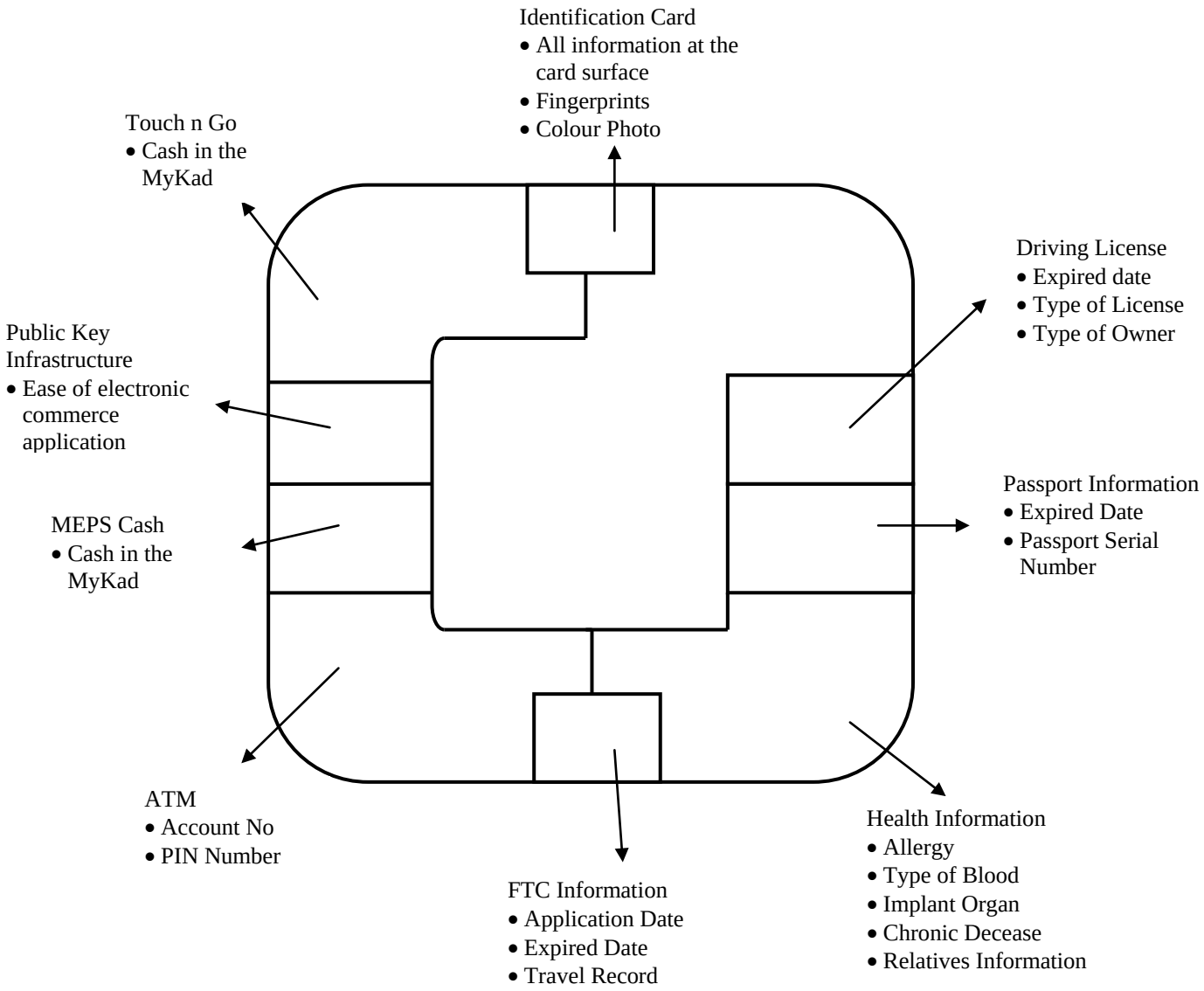

Figure 1.1: Allocated Space for Various Applications in MyKad chip (JPN, 2007)

Currently, MyKad's PKI application allows secure electronic transactions over the Internet. The transactions include online submission of tax returns, secure email and electronic commerce. Based on JPN's website, there are three agencies

that use PKI application but not in MyKad. They are e-Perolehan system by the Ministry of Finance (MoF), e-filling system by The Inland Revenue Board of Malaysia (LHDN), and e-business card and tender registration by the Malaysian Institute of Microelectronic Systems (MIMOS). As presented by Wan Ibrahim (2005), the use of MyKad's PKI needs to be a mandatory application in five years to ensure the implementation of MyKad can achieve its Return on Investment (ROI). However, only National Identity Card (NIC) application is loaded into MyKad by default while other applications are loaded voluntarily (Loo et al., 2009). The Government faces difficulties in convincing all MyKad users to acknowledge MyKad's full potential and capabilities. Therefore, this research aims to close the gap and to propose that the MyKad's PKI to be embedded in e-commerce application.

1.2 Problem Statement

Nowadays, the Internet helps and facilitates online business to be more flexible. With the pressure from the fluctuated economic growth, Malaysians are turning more towards the online business. This kind of business is beneficial to both merchants and consumers as the company needs low cost to build its business while the customers can easily deal with the company. There are, however, a number of problems with the current online business model. According to a survey by Rahman and Masrom (2010), these online business systems do not provide legal binding proof of the business transaction. Normally, consumers are asked to bank the required amount of money for the item they want to buy. However, there is no legal evidence that the money transferred to the merchant's account is a payment for that particular item. Hence, there is no way for the customers to prove that they have made the payment in accordance to any electronic order form prior to the transaction. In addition, since the transferred money is in the merchant's account, it is not guaranteed that the merchant will ship the product to the consumer. Based on these situations, the customers are likely not to make the purchase as they do not will to risk losing their money.

Therefore, this research proposes a new payment model that is suitable and acceptable in Malaysia. In order to overcome the issues mentioned earlier, MyKad will be used as the medium of payment since the PKI in MyKad is recognised by the authority as legally bonded. Besides, this research introduces to the public another use of MyKad that is not only for identification purpose but also in e-commerce transactions. Hence, the new payment model will introduce to the Malaysians the secure usability of PKI application in MyKad that can be used as an alternative payment method. In order to make this payment model acceptable by the public, the proposed model needs to overcome these issues:

(a) Trust and Security issues

Trust has been found to have an influence on a customer's willingness to purchase online (Gefen et al., 2006). For example, an entity can be said to trust a second entity when the first entity makes the assumption that the second entity will perform exactly as the first entity expects. In this proposed research, the use of PKI will gain the trust from the public because if anything happens during the transaction, the evidence generated from the PKI is admissible in the court of law since it is recognised as legally bonded. With the PKI, the public will find that their transaction and money are secure even if something happens during the transaction.

Other than the trust issue, security has always been considered as an essential and critical area of research (Rahman and Masrom, 2010). It is crucial for a payment model to have its own security framework. This research intends to propose the security of payment model for financial transaction using MyKad.

(b) Performance issue

In this issue, it emphasises on real-time performance especially regarding authentication response time because it can affect the users' behaviour whether they want to use the system or not due to its performance. For example, in a credit card system during peak hours, credit card transaction takes longer time for authorisation process. The performance of the system is affected whenever the authorisation process is increasing. Hence, users will try to avoid using the system during the peak

time. However, Siti Hafizah et al. (2008) proposed a credit card authorisation system using multithreading technique to improve its response time since modern operating systems with advanced multi-core processors have a good support of multithreading implementation. Based on the comparison between single and multithread using the proposed system, the performance of the multithread system has increased almost two-fold than the single thread system. It proves that multithreading can give better response time to the users and also allows users to execute the tasks simultaneously while running the process.

1.3 Research Questions

From the earlier discussion, research questions have been formulated as follows:

(i) What are the elements involved in MyKad payment model?
(ii) What security frameworks can MyKad payment model implement to secure customers during transaction?
(iii) Does the new payment model with security and multithreading technique perform better than the credit card?

1.4 Research Objectives

Based on the research background and other related issues, the objectives of this research are as follows:

(i) To identify all the elements of the payment model related to MyKad based on the study of payment model.
(ii) To design a payment model with security and multithreading technique as proposed in the research.
(iii) To evaluate the model based on response time of the transaction with the proposed techniques.

1.5 Research Hypothesis

In order to determine whether the new payment model named MyKad Payment Model (MPM) performs as good as the credit card system, the following null hypothesis was tested.

Null Hypothesis 1. There is no difference between MyKad Payment Model (MPM) and credit card authorisation system response time.

1.6 Thesis Outline

(i) **Chapter 1** presents a brief explanation about the background, research problem statements, research questions, research objectives and research hypothesis.

(ii) **Chapter 2** discusses an overview of smart card, MyKad and their applications. Related payment models are compared in this chapter in order to identify the players involved in a transaction for a basic model. Besides that, this chapter discusses a general idea on security and multithreading parts.

(iii) **Chapter 3** starts with the introduction of the basic payment model and followed by the details of the proposed model. The chapter continues by describing how the model has been formulated and designed. It also discusses the two techniques proposed, which are ARSA and multithreading.

(iv) **Chapter 4** describes the details of MPM model along with its module, techniques proposed, architecture design of the proposed model and its prototype with detailed explanation on the system architecture. In the last section in the chapter, the performance testing of the MPM is conducted by using HP Load Runner.

(v) **Chapter 5** summarizes the analyses and findings of the MPM. The findings discussed in this section are the multithreading result. The response time between the proposed technique, multithread and single thread are compared in seconds (sec). MPM multithreading results are compared with credit card

authorisation system to give some insights regarding MPM performance compared to credit card authorisation system.

(vi) **Chapter 6** summarizes the key results of the thesis and recommends the topics for the future work.

CHAPTER 2

ELECTRONIC PAYMENT MODEL – DATA SECURITY AND PERFORMANCE

2.1 Introduction

MyKad contains multiple applications for users' convenience, with the latest one is Public Key Infrastructure or PKI in short. As it is PKI-ready, MyKad is capable to store digital certificate that can be used to digitally sign and encrypt Internet transactions. Based on its security features, MyKad gives more secure and protected e-commerce transactions where it can be used as a medium of payment in purchasing everyday items. In order to develop a new security payment model for MyKad named MyKad Payment Model (MPM), four types of payment model are discussed in this chapter, which are:

(i) Electronic Credit Card
(ii) Electronic Cash
(iii) Electronic Check
(iv) Smart Card Payment

As mentioned in Chapter 1, the issues on security and performance will be focused. In security issue, several algorithms will be discussed in this chapter in order to find the suitable algorithm to be put in the model. The algorithms include the encryption/decryption and hashing process. The performance of MPM is determined on how the MPM would react to the time taken for authentication process

for MyKad transaction. Therefore, multithreading technique will be used instead of single threading.

2.2 Smart Card

Smart card is an intelligent card with a built-in chip capable of storing information in its memory (Awad, 2007). The card contains a programmable chip, a combination of RAM and ROM storages and an operating system. Turban and McElroy (1998) identified two main categories of smart cards. The first category of smart card is a memory card that contains only non-volatile memory storage components, and perhaps some specific security logic. For example, the users can spend this type of smart card on pay phone, retail, vending machines and other related transactions. The second category is a microprocessor or intelligent card that contains volatile memory and microprocessor components. Most of the intelligent cards offer read and write applications, and new information can be added and processed (Turban and McElroy, 1998; and Maher, 2004).

Since smart cards have been around for about 20 years, the demand for public key smart cards in the last four years has been increasing (Raihi, 2001). The demand includes the Government sector, banks and insurance institutions. The popularity of Internet recently also contributes to the increas of e-commerce applications and this will affect the growth of smart cards application in the Internet (Guthery and Jurgensen, 1998). Hence, this chapter will describe more about MyKad with its application in e-commerce. Table 2.1 summarizes the history of smart cards.

Table 2.1: Summary of smart card history (Cardwerk, 2009)

Year	Inventor	Description
1968	Jurgen Dethloff & Helmutt Grupp	An automated chip card, patent approved in 1982 and first used with France pay phones.
1970	Dr. Kunitaka Arimura	Filed the first and only patented the smart card concept.
1974	Roland Moreno	Filed the original patent for the IC card, later dubbed the “smart card”.
1977	Bull CP8, SGS Thomson, and Schlumberger	Three commercial manufacturers began developing the IC card.
1979	Motorola	Developed the first secure single chip microcontroller for use in French banking.
1982	French Telecommunication Company	Field testing of serial memory phone cards took place in France, the world’s first major IC card test.
1984	Bank	Field trials of ATM bank cards with successfully conducted chips.
1986	Bull CP8	Distributed smart cards to its clients such as Bank of Virginia, Maryland National Bank, First National Palm Beach Bank and Mall Bank.
1987	U.S. Department of Agriculture’s nationwide Peanut Marketing Card.	First large-scale smart card application implemented in the United States.
1991	Wyoming Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).	First Electronic Benefits Transfer (EBT) smart card project launched.
1993	Telecarte (for public phones)	Field test of multifunction smart card applications in Rennes, France, enabled in a Smart Bank Card.
1994	Europay, MasterCard, and Visa (EMV)	Published joint specifications for global microchip-based bank cards (smart cards). Germany began issuance of 80 million serial memory chip cards as citizen health cards.
1995	Mobile Phones Companies	Mobile phone subscribers worldwide began initiating and billing calls with smart cards. The first of 40,000 multifunctional, multi-technology MARC cards with chips were issued to U.S. Marines in Hawaii.
1996	Atlanta Olympics MasterCard and Visa	Over 1.5 million VISACash stored value cards were issued at the Atlanta Olympics. MasterCard and Visa began sponsorship of competing consortia to work on solving the problems of smart card interoperability. Two different card solutions were developed: the JavaCard backed by Visa, and the Multi-Application Operating System (MULTOS) backed by MasterCard.

Table 2.1: (continued)

Year	Inventor	Description
1998	U.S. Government's General Services Administration United States Navy Microsoft	Joined forces and implemented a nine-application smart card system and card management solution at the Smart Card Technology Center in Washington, D.C. Announced its new Windows smart card operating system.
2001	Social Security IDCard, Spain.	Full scale introduction in progress. Card gave access to medical benefit.
2001	**Malaysian Government**	**Compulsory national ID scheme included different applications and was rolled out for 18 million users.**
2006	Axalto and Gemplus	Merged and became Gemalto.

2.3 MyKad

MyKad is a multipurpose card that will enable Malaysians to access public and private services since the data stored in it include personal identification, driving license number, passport information, medical data and financial information. Some of the services provided for MyKad holder are highway tolls, parking fees and public transportation such as bus fares and LRT fares. According to Knight (2001), MyKad is regarded as the world's first National Identification Smart Card. MyKad supports eight types of applications such as identity card including fingerprint and photo, driving license, passport, e-cash, ATM card integration, Touch 'n Go, as well as MyKad PKI application.

This study is on one of the applications of Mykad, which is the Public Key Infrastructure (PKI) supported by the 64 Kb version of MyKad. It has been implemented since February, 2003. With it, PKI allows easy securing of private data over public, thus allowing secure electronic transactions over the Internet, which include online submission of tax returns, Internet banking and secure email. However, at this moment these functions are still not widely used by Malaysian because they are not widely promoted and this causes the Malaysian to be unaware of this application. MyKad's PKI will be explained further in next section.

2.3.1 MyKad's PKI

The driving force behind the security of MyKad is Virtual Environment for Secure Transactions (iVEST), while the PKI is developed by a subsidiary of MiMOS Bhd of the same name (Swinburne, 2009). MyKad has an embedded PKI that supports security mechanisms such as encryption, message authentication and digital signatures (Phan, 2003). The PKI in MyKad performs encryption and digital signatures by making use the public-key techniques. Such techniques make use a pair of keys, namely a private key, which is kept secret, and a public key that is "widely broadcasted to the public". The two keys are generated such that when one key is used to transform some information into an unintelligible form (encryption), the only way to reverse the process is by using the other key (via decryption).

The MyKad PKI uses X.509 Version 3 (v3) certificates (Mykad Guidelines, 2005). The structure of the X.509 v3 certificate is illustrated in Figure 2.1. The certificates contains the owner's public key, some forms of the principal's identity, algorithms used in the certificates, digitally signed and issued by Certification Authority (CA), and has a finite validity period (Norbik, 2006). In particular, Figure 2.2 shows how the certificate may be extended with optional extension fields. These certificates are digitally signed using the private key of the issuing CA. A part of the PKI implementation focuses on MyKad physical requirements as set by the National Registration Department. All registered MyKads with the identities of every individual shall fit for the registration and usage of the digital certificates. The characters of the basic requirements, but not limited to MyKad, are as follows:

(i) Card Operating System
(ii) Support international standard, ISO 7816 Part 3 and 4.
(iii) Cryptographic Module
(iv) Higher security features and accelerators.
(v) Secure protection of private keys
(vi) Digital signature support
(vii) Minimum of RSA 1024 bits processor
(viii) Certification

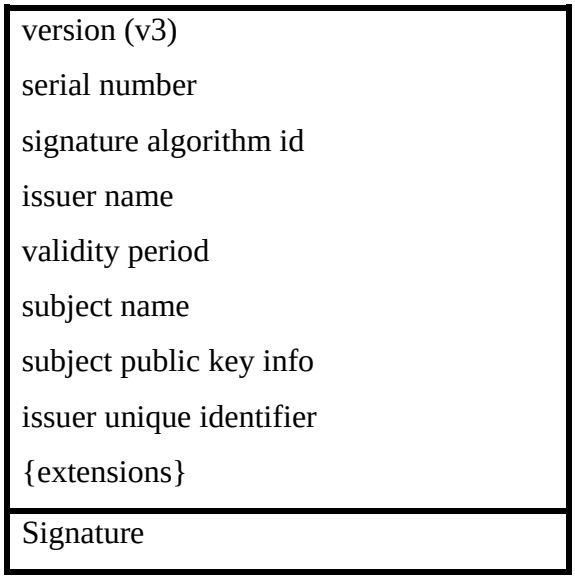

Figure 2.1 Certificate Format (Norbik, 2006)

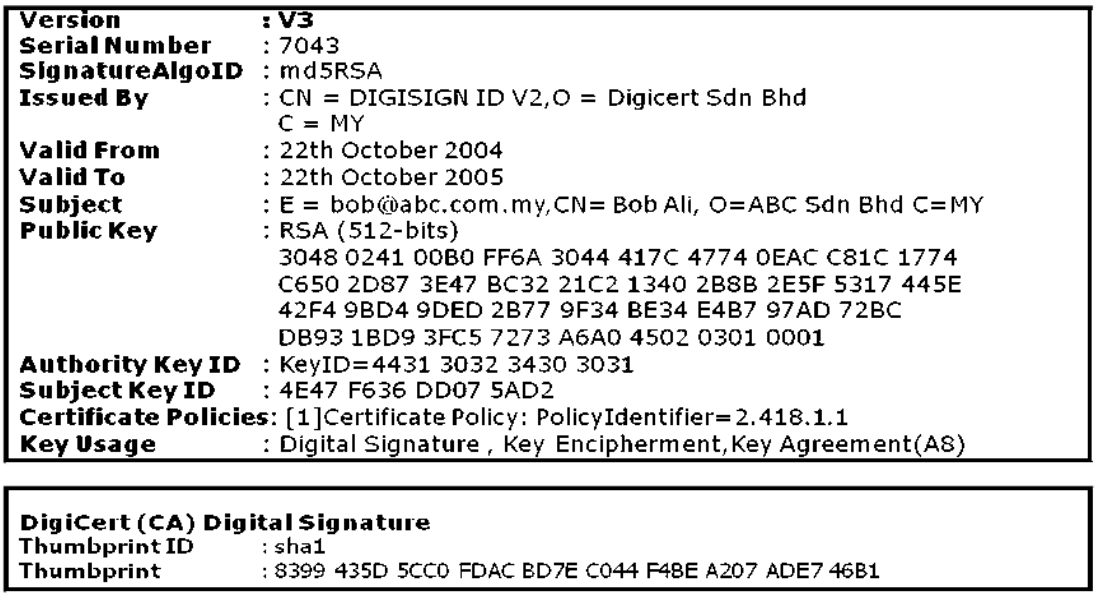

Figure 2.2 Example of Digital Certificate (Norbik, 2006)

The implementation of PKI capabilities into MyKad along with the usage of Digital Certificates shall provide a few key benefits (MyKad Guideline, 2005). There shall be two sets of digital certificates in MyKad. Each certificate shall have its own functions to be performed in accordance to Digital Signature Act 1997 and Digital Signature Regulations 1998. The first set of digital certificate is used for digital signature and the cardholder uses the private key to carry out the function

while the second set of digital certificate is used in authentication and encryption function (Mykad Guidelines, 2005).

MyKad's PKI architecture contains security measure that involves certificate registration. The process of certification creation involves a lot of encryption and decryption of sensitive data (SANS Institute, 2001). The encryption and decryption of the data are done by applying any strong security algorithms so that the data cannot be decrypted easily by third party. Every encryption and decryption process will have an assigned public key and private key in which they are only known to the authorised party.

The security features such as public key and digital signatures included in MyKad's PKI enable more secure and protected e-commerce transactions. Malaysians whom have converted their old national identity card to MyKad can use it as a medium to purchase everyday items, to pre-pay for any services requested and to do online transactions with any of the e-commerce merchants using the MyKad's PKI e-commerce application. Currently, there is still lack of e-commerce applications that are compatible with MyKad's PKI. Therefore, in the next section further discussion on how MyKad's PKI can be enhanced to support the e-commerce application with minimal fuss, the risk and other major considerations that need to be considered for the development of MyKad e-commerce applications.

2.3.2 MyKad's PKI in e-Commerce Application

One application that can be looked upon when researching for the success of developing MyKad's PKI in e-commerce application is smart card e-payment. In smart card e-payment, smart cards are used either to store money or enhance e-payment security. In many cases, smart cards are more secure than credit cards and they can be extended with other payment services (Turban et al., 2008). For example in retail field, smart cards are used where payments are usually done by cash such as stores, gas stations, cinemas, transit fares and others. To use smart cards, it is necessary to have smart card reader, a hardware device that communicates with the chip on the smart card. The reader can be attached with, for examples, personal computers and electronic cash register.

According to Thomas (2004), the benefit of smart card is highly dependent on the availability of smart card reader. Both the customer and the merchant must possess the smart card reader. For instance, Barclay Bank has introduced a card reader to its customer since 2007 to perform transactions. The bank reported that almost one million of its customers are using it (Bielski, 1999). It shows a good response since it was launched. Hence, the user has the control on the validity of identification by using the card reader. Due to that, the use of smart card reader is seen as a reason that widens the acceptance of smart card (Chege, 2002).

2.4 Overview on Electronic Payment

There are several electronic payment systems and models proposed that depend on their application or transaction requirements. Generally, there are four major categories of electronic payment system, which are online credit card payment, electronic cash, electronic checks and small payment (Wayner, 1997). However, Meng (2003) classified the electronic payment model into three payment models, which are similar to the models proposed by Wayner (1997) except the small payment. Table 2.2 shows the summary of the payment models and Table 2.3 shows the comparison of the characteristics of the models.

Table 2.2: Summary of reviewed payment models

Model	Description	Players
Electronic Credit Card	1. The payer must have credit card account. 2. Payer provides credit card account information upon paying and sent to merchant bank's processor. 3. Merchant's bank sends issuing information to the user's bank. 4. User's bank approves/declines the transaction. 5. User sends the transaction status to the merchant's bank. 6. Merchant's bank sends the result to the merchant.	Payer (user), Payee (merchant/store), Payee's (merchant/store) bank, Payer's (user) bank.
Electronic Cash	1. User must purchase the electronic cash from the issuer bank. 2. User uses the electronic cash in data format to pay and send to merchant. 3. Merchant sends the electronic cash to his bank for clearing. 4. Both user and merchant's bank verify the electronic cash. 5. Bank sends the verified electronic cash to the merchant.	Payer (user), Payee (merchant/store), Payee's (merchant/store) bank, Electronic cash issuer bank.
Electronic Check	1. User creates an electronic check that includes check information. 2. The signed electronic check is sent to payee. 3. Payee verifies the signatures and sends the payment to the intended account for clearing. 4. Bank verifies the signature and accounts and make sure it is valid and not duplicate. 5. Bank sent the check to the payee's account.	Payer (user), Payee (merchant/store), Payee's (merchant/store) bank, Payer's (user) bank.
Smart Card Payment	1. User loads some money into the smart card. 2. User inserts card reader to pay for the transaction. 3. Card issuer authenticates the owner. 4. Merchant fills in the total amount. 5. Payment is deducted from the user account	User Card issuers Merchants

Table 2.3: Comparison of characteristics of electronic payment model

Characteristics	Electronic Credit Card	Electronic Cash Payment	Electronic Check Payment	Smart Card Payment
Authority	Security number + PIN	PIN	Digital Signatures + Digital Certificates	PIN / Digital Signatures + Digital Certificates
Actual Pay Time	Later	Before	Later	Pay Before
User	Legitimate Credit card user	Anyone	Bank Account Holder	Smart Card Account / Bank Account
Transaction Risk	Most risks are borne by bank	Risk of electronic cash to be stolen, lost or misused	User responsible most of the risk, however the payment can be stopped by user	Risk of smart card to be stolen, lost or misused.
Micro Payment	No	Yes	No	Yes
Large Payment	Yes	No	Yes	Yes
Transfer Limitation	Depends on limit of the card	Depends on the prepaid	No limit	Depends on how much money is saved

Based on both tables, the users of the electronic credit card payment need to provide three security numbers at the back of the card and PIN number for authorisation. Electronic cash payment only uses PIN number for authentication. Electronic check payment provides strong authentication, which is digital signatures and digital certificates. For time settlement, electronic credit card and electronic check payment are paid after the statements are sent to the users while the electronic cash is paid before the payment is made because the users need to buy the electronic cash before spending it.

Another characteristic compared is the risk of transaction where the risk of electronic check highly depends on the users. For electronic credit card, bank is responsible for most of the risks and the other part for the user. There is a risk with electronic cash if the electronic cash is stolen lost or misused. Both electronic credit card and electronic check do not support micro payment due to high cost of this kind of payment. Because of that, both of them are suitable for macro payment. On the other hand, electronic cash supports micro payment but is not suitable for macro payment because if anything happens, the electronic cash is not replaceable. Users

can freely enter any amount of money without limits if they use the electronic check while the other two models depend on their card or prepaid limit.

Because smart card also provides an access to valuable assets or secret information such as electronic cash and banking information, they must be secured against any threats. Some smart cards show the account number of the owner and some others are required to enter a PIN number that must match the card. However, currently most of the cards use encrypted form to store information in the smart cards. That is why Turban et al. (2008) classified smart cards hacking as "class 3" attack because the cost for attacking exceeds the benefit.

Therefore, to ensure the implementation of MyKad Payment Model (MPM) succeeds, the model should be secured and offers good performance in term of time such as quick and less authentication time for authorisation. In order to achieve these criteria, the MPM should be developed with the tightest security as it holds critical information of the users and the capability to provide shorter waiting time for authentication. Next section discusses further on security.

2.5 Security Features of Payment Model

Computer security technology is constantly improved from time to time, as new technologies are being introduced almost every day. However, for all the new technologies that are being introduced to the computer world, the obsolete technologies are used as reference points. These obsolete technologies are replaced with the new ones. This can be seen by taking the chronological scenario of mobile phone General System of Mobile (GSM) network. From the Second Generation (2G) band that only supports the normal usage of voice call and text message to the evolution of multimedia messages that can enclose images and sounds. Next, Third Generation (3G) band that supports video call, internet broadband, and live video streaming is introduced. The evolution of 3G band improves the method of process in the 2G band. Pertinent to the evolution, it is similar to the proposed advanced security features of MPM. In MPM, the most secured safety measures will be employed during the authorisation of merchant and certification process. This process will involve a lot of security algorithms to do encryption, decryption and

hashing of the transaction. In order to achieve this requirement, MPM will propose a new security feature named Arbitrary Random Switching Algorithm (ARSA), which is the evolution and enhanced security of a well-known Microsoft security algorithm pack, or CAPICOM. CAPICOM is a security technology from Microsoft that is used as part of this research project. It enables to do digitally signed data with a smart card or software key, verifies digitally signed data, graphically displays certificate information, and encrypts and decrypts data using public keys and certificates (Lambert, 2001).

Basically, CAPICOM is a library that contains various types of Hashing and Encryption/Decryption algorithms. For encryption process, five different types of algorithms are used such as Data Encryption Standard (DES), 3Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Rivest Cipher 2 (RC2) and Rivest Cipher 4 (RC4), while in hashing Message Digest 2 (MD2), Message Digest 4 (MD4), Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) are used.

2.5.1 Encryption/Decryption Process

Encryption is a process of transforming a plaintext to a ciphertext. In a normal context, encryption can be referred to as a football playing strategy. For example, a coach will refer a playing strategy to simple codes such as 4-4-2 strategy or 4-3-3 strategy, and the players will automatically know that this strategy is devised from the details of four defence player, 4 midfielders player and 2 strikers being for the former. Besides, in this strategy, the coach already includes all playing methods such as ball wasting, passing mode, tackling mode and others that the players are already aware of. It is important so that when the coach wants to change the strategy, he only mentions the simple code to avoid any leak of information to the opponent.

In cryptography, a message in human language referred as plaintext, while ciphertext is a message that has been disguised by encryption process. The main reason of encryption is to hide the message or text from anyone for whom it is not referred for. On the other hand, decryption is a process of reversing a ciphertext to its original plaintext. Decryption is a method used to get the original message back

from the disguised message. Encryption and decryption processes need to be employed in MPM due to the amount of sensitive data that MPM holds. MPM holds and transmits a lot of sensitive information that can be stolen such as customer information and account information. These data need to be masked before the transaction can take place so that, even though it is stolen during the transaction, the thief will not be able to use the stolen data because it is encrypted. So, in order to be able to encrypt and decrypt all the data, an algorithm will be used. This algorithm can be referred as a medium and process of encryption and decryption. Therefore, MPM introduces ARSA as its main security feature.

ARSA is a random switching algorithm technique. It has the capability to randomly switch the algorithms based on time or network attack to the system. Most of the algorithms used in ARSA are either taken directly from the CAPICOM or replaced with the newer version that is known to offer the latest security features. Like the football strategy, ARSA can be seen like the technique used by the football coach during football match. For example, when the team is in attacking mode, the coach will automatically use the attacking technique. When the team is in defence mode, the coach will use defence technique. When the game is nearly over and the team is winning, the coach will revert to the time wasting technique. Same goes to ARSA of MPM, when the system is being attacked, ARSA will switch to the algorithm that is known to be immune to the attack. All algorithms in ARSA have their own strength and weaknesses and the algorithms used in ARSA are specifically designed to counter each other's weaknesses. The details of these algorithms such as its history, process, strength and weaknesses will be explained further in the next paragraph.

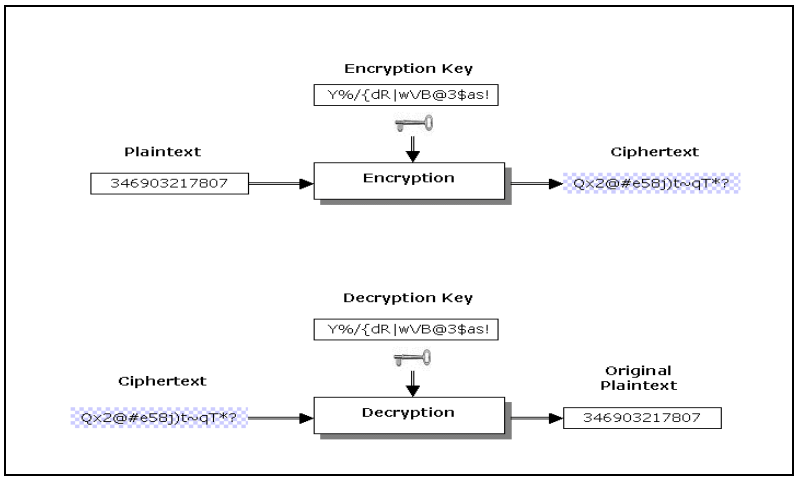

Figure 2.3: Encryption and Decryption Processes

There are two types of encryption process. They are Symmetric and Asymmetric Encryptions. The differences between Symmetric and Asymmetric Encryptions are shown in Table 2.4**.**

Table 2.4: The differences between Symmetric and Asymmetric Encryptions

Symmetric	**Asymmetric**
Private key encryption	Public key encryption
Only one key is used to encrypt/decrypt data	Uses public and private keys
Key should be distributed before transmission between entities	No need to distribute the keys because they are already defined as public and private keys.
The strength depends on the key size. The longer the key, the harder to break than the small one.	Based on mathematical function and computationally intensive.
Examples: DES, 3DES, AES, Blowfish.	Examples: RSA and DSA.

As mentioned earlier in previous section, CAPICOM mainly uses DES, 3DES, AES, RC2 and RC4 for encryption process. However, some of the algorithms used in CAPICOM have their own weaknesses and they are not suitable to be implemented in MPM security module.

DES is the first encryption standard to be recommended by National Institute Standard Technology (NIST) and it contains 64 bits block size. Based on small key size, DES is opened to many attacks and threats that make it an insecure block cipher (Stallings, 2005; Coppersmith, 1994). According to Abuzineh (2004), it is possible to crack a DES in less than three and half hours and some experts nowadays no longer consider DES to be secure against all attacks and due to that the 3DES is

proposed. However, the entrenchment of DES within the communities such as banking will make it difficult to switch to a different encryption algorithm even if NIST does not recertify DES (Scheneir, 1994).

3DES is the improvement from weakness of the DES. This algorithm was proposed as a replacement for DES due to the advances in key searching (Nadeem & Javed, 2005). It is a 64 bits block size but with 192 bits key size, which is three times higher than DES. It is applied three times from DES encryption algorithm to increase the encryption level and the average safe time (Elminaam et al., 2008). However, because it applies three times, 3DES is known as slower than other block cipher method (Stallings, 2005) but it is more secure if used properly.

AES became the U.S Government standard in 2002 and has been approved for use with classified information. AES was proposed because clearly a replacement for DES was needed at that time (NIST, 1997). AES encryption is fast and flexible and can be implemented on various platforms especially in small devices (Naik & Wei, 2001). In addition, AES has been carefully tested for many security applications (Stallings, 2005; Daemen & Rijmen, 2001). The known attacks against AES to date have involved timing, where the keys are guessed by analysing how long particular steps require. Some cryptographers worry that there might be attacks on the algorithm itself, but none have publicly emerged to date. Moreover, in terms of power consumption and throughput, AES has an advantage over 3DES, DES and RC2 (Elminaam et al., 2008).

RC2 and RC4 were invented by Ronald Rivest for RSA Data Security, Inc. RC2 is known to have two weaknesses that are vulnerable to differential attacks related to key attack (Elbaz & Bar-El, 2000). A study also showed that RC2 still has low performance among of these algorithms. On the other hand, the disadvantage of RC4 is the weak key-mixing phase. Obviously, 1 over 256 of the keys belongs to a class of weak keys and they are detectable. Based on the algorithms above, only two algorithms are selected in ARSA library, which are 3DES and AES. The other three algorithms will be replaced with the latest algorithms, which are RC6, Blowfish and Rivest Shamir Adleman (RSA).

Due to the weaknesses of RC2 and RC4, RC6 is implemented. RC6 is considered to be strong algorithm with fast and easy hardware implementation. Moreover, in MPM system, MyKad reader is required. In addition, the advantage of RC6 is that this algorithm is quite simple and will allow a compiler to produce well-

optimised code resulting in good performance without hand optimisations (Rivest et al., 2000). A study done by Elminaam et al. (2008) also showed that RC6 required less time than all algorithms, except Blowfish.

As a replacement for the DES algorithm, Blowfish is applied. Blowfish takes a variable length key, ranging from 32 bits to 448 bits and it consumes a lot of time to break. The Blowfish is designed to resist all known attacks on block cipher and it is known for its security and availability in common encryption products (Elbaz & Bar-El, 2000). In performance simulation done by Elminaam et al. (2008), it was also concluded that Blowfish has a better performance than other common encryption algorithms used, followed by RC6.

As stated earlier, one of the basic requirements in MyKad is the minimum of RSA 1024 bits processor. For that, RSA scheme is implemented in ARSA library. RSA algorithm is based on the factoring of very large prime numbers and demand as the easiest public key algorithm that works for encryption. The advantage of RSA comes from the fact that, while it is easy to multiply two huge prime numbers together to obtain the product, it is computationally difficult to do the reverse. RSA is still the most widely used encryption algorithm. However, while other standards such as DES are faster to decrypt, RSA remains as an industry-favourite for encrypting data with many believing its 2048 bit key encryption is virtually unbreakable. This is because factoring is such a slow process, and because of this combination of the slowness of factoring and an asymmetric encryption process, that make RSA so powerful and revolutionary compared to previous systems of encryption. Below is the general algorithm encryption step:

(i) Plain text is ready to be converted (plain text here is any information that needs to be transmitted).

(ii) Plain text is converted by the algorithm to mask its original information.
General algorithm key is used here.

(iii) The masked data is transmitted.

(iv) Receiver will decrypt the masked data using the same algorithm to reveal the original information.