A PROPOSAL FOR PAYMENT MODEL FOR FINANCIAL TRANSACTION USING My Kad

NURUL HUDA AHMAD ZAHARI
ZURINAH SURADI

A Proposal for Payment Model for Financial Transaction Using MyKad

Nurul Huda Ahmad Zahari[a], Zurinah Suradi[b,*]
Faculty of Information Technology & Multimedia, Universiti Tun Hussein Onn
Malaysia, 86400 Parit Raja, Batu Pahat, Johor
zurinah@uthm.edu.my

ABSTRACT

The Public Key Infrastructure (PKI) application in Mykad will enable users to conduct e-commerce using a digital certificate. PKI allows for easy securing of private data over the public network and allowing secure electronic transactions over the Internet which include online submission of tax returns and internet banking. Hence, this research presents the basic elements of electronic payment model that related to MyKad PKI because there still no model or system to conduct this transaction to date. In order to identify these elements, we reviewed three payment models which are PayCircle, PayWord and PayPal. PayPal is widely used in making payment all over the world while PayWord is one of the payment models that used public key in their transaction. For PayCircle, this model described the simplest possible electronic payment models which can be the basis for all other models. Hence, we proposed a new payment model to include a digital certification authority as one of the necessary players in electronic payment for smart card.

Keywords: The Public Key Infrastructure (PKI), digital certificate, electronic payment, internet banking

1. Introduction

For more than 20 years, one of the main purposes of smart card is to store small amount of money. This value of money can be used to pay for simple business transaction. Examples of payments are telephone bills, photocopying purposes, and transportations fare and so on. Besides that, smart card is also widely used as identification cards as in several countries especially in Malaysia. The information in the chip of the smart cards may include demographic information, health status, driving license, insurance and many others. For Malaysia, the government has been using smart cards as identification purpose for Malaysian citizen since September 5, 2001. The data contains including biometrics. This card is known as MyKad.

MyKad is a multi-purpose card that will enable Malaysians accessing public and private services since the data stored in MyKad would include personal identification, driving license number, passport information, medical data and financial information. It is regarded as the world's first smart identity card (Knight, 2001). One of the applications of Mykad, is Public Key Infrastructure which is supported by the 64Kb version and implemented in February 2003. This application will enable users to conduct e-commerce transaction over the Internet. This is the latest feature in the smart card environment. With this feature, users can easily perform business transactions. However, till to date this feature is still not available in Malaysia because

there is still no platform or public portal provided to conduct such transactions. Another reason may be due to lack of promotion on the application itself even it has been launched five years ago. Hence, this paper proposes an e-payment model for financial transactions using Mykad. The model will illustrate the flows of the transaction process and hopefully the users will felt secured to use this application. In turn, it will further enhance the usability of MyKad as a payment mechanism.

This paper is organized as follows. In section 2, several existing payment model will be discussed and in section 3, the proposed payment model developed by highlighting the basic model. Section 4, justifies the method that will be used and proposed the expected result of the study and finally, section 5 presents the conclusions.

2. Related Work

There are several electronic payment models proposed which depend on its application or transaction requirements. For example, PayCircle (2003) introduced a simple electronic payment model. The components involved are customer, merchant, payment service provider (PSP) and Financial Service Provider (FSP). This simple model assumed that only one PSP involved in the transaction that has relationships with both customer and merchant. This shows that for merchant and customer, they will have to share one PSP which is responsible for the settlement.

On the other hand, Fadi and Ezz (2004) proposed a payment model that support person-to-person transactions with a limited intervention of a third party. This payment model can be viewed from smart card or e-cash perspectives. This model has three major players which are issuer (bank), payer (individual uses credit card, debit-card or bank account to purchase goods) and the payee (seller). The e-cash will be transformed from the issuer to the customer and later it will be transferred from the payer to the payee for the payment.

For Rivest (1996) model's which known as PayWord, uses cryptographic properties of digital signature in e-cash generation with a simple scenario. The process included three main players which are broker, customer and vendor. A user is a person who purchased the goods and makes payment, a vendor who sells the goods and also collects the payment while the broker will keep the accounts for user and vendor. In this model, both user and vendor must share the same broker in order for any transaction to take place.

One of the most successful examples of the payment model can be found in consumer friendly payment systems, called PayPal (Gonzalez, 2004). PayPal acts as a third party that organizes the money transaction among the users (Fadi, 2004). In PayPal model, there arc three main players which are sender, receiver and PayPal itself. PayPal users will send and receive money to or from each other by using emails. For this model, users should provide their credit card information.

Based on the literature, electronic payment model should have at least three main players involved in a certain transactions which are customer, merchant and payment provider. One of the players in each payment model maybe differs by their names, however their roles are similar in nature. For example, PayCircle, PayWord and.

PayPal respectively used customer, user and sender as one of their main player. All these actually play the same role as a person who accesses a service or buying goods that needs to be paid. Hence, we classify customer, merchant and payment provider are the basic players for our payment model.

Model & Author	Year	Attribute Components	Purpose
PayCircle	2003	Customer, Merchant, PSP and FSP	Propose simple and basic electronic payment model.
Fadi and Ezz	2004	Issuer(bank), Payer and Payee	Support person-to-person transaction with a limited intervention of a third party.
Rivest, R.L (PayWord)	1996	Broker, Customer and Vendor	Making small purchases over Internet uses cryptographic properties of digital signature.
PayPal	1999	Sender, Receiver, PayPal itself	Allows individuals and businesses to transfer funds electronically

Table 1: Summary of Model Attributes and Purposes

3. The Payment Model

In this section, we describe the proposed payment model in detail.

3.1 Payment Overview

The aim of this paper is to identify all the payment model elements and variables that will enable MyKad to make payment for financial transactions. With PKI and digital certification availability, a payment model is formulated for MyKad.

In this payment model, four players were identified to be involved for given transactions which are customer, merchant, payment provider and certification authority. The three players were based on the previous work and can be considered as the basic players of any payment models. The Certification Authority was added as a fourth player because of the PKI properties in MyKad. This will let the user have control of the card electronic payment.

The preparation procedures of our model can be summarized as follows: The customer must register with his local certification authority and get his digital certificate and secret keys. Digital certificates are the electronic counterparts to MyKad. With this model, digital certificate can be presented electronically to prove customer's identity or right to access online services. This certificate will binds an identity to a pair of electronic keys that can be used for encrypting and signing digital information. With this application inserted in MyKad, it will enable individuals to secure business and personal transactions across communication networks. In this payment model, the customer who wants to purchase goods will needs digital certificate to ensure his identity is secured before making the transactions.

Thus, it will ensure the transaction is safe to be performed. The flow of digital license is summarized as in *Figure 1* below.
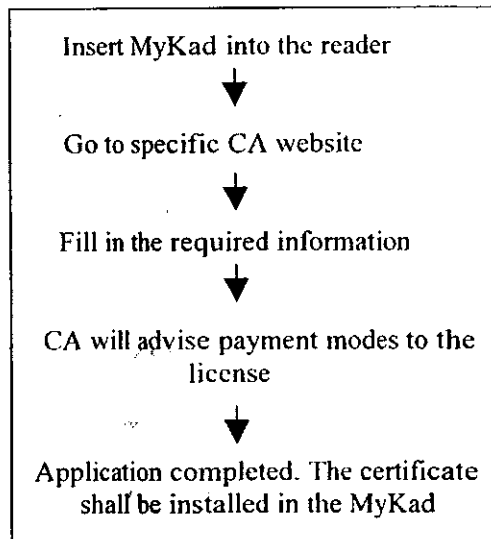

Figure 1: Flows of issuance digital license.

3.2 The proposed model
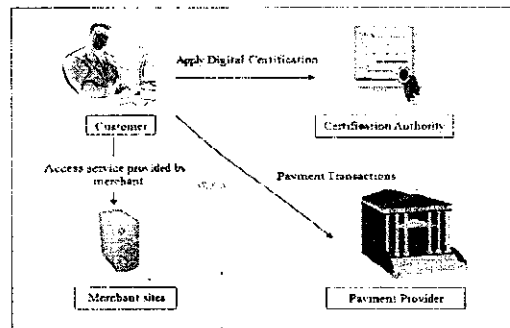
Figure 2 shows the basic proposed model of Mykad.

Figure 2: Basic Proposed Model of MyKad.

Customer

The customer is an individual who owns a MyKad and is a Malaysian citizen. The customer will use it to pay for goods or services they purchased from the merchant sites.

Merchant Sites

The merchant sites are the place where the customer can access and may take a look at the content provided before they purchased something. These merchant sites also become service or goods provider for the customer. Merchants also will request how the payment can be made from the customer and on delivery of goods.

Payment Provider

The payment provider is responsible for the payment process and in this model the payment provider can be of financial institutions for example a bank. The bank is where the card holders registered an account with that particular bank.

Certification Authority

Certification Authority is the entity given the authorities to perform the certificate authorization management. MyKad holders can apply and purchased the certificates from two Malaysia's certification authority, which are MSCTrustgate.com Sdn. Bhd and Digicert Sdn. Bhd.

In this proposed payment model, customer will access services provided by the merchant. The customer can purchased any information or goods provided by the merchant. If the customer wants to make a transaction, he needs to insert his MyKad into the MyKad reader and enter his Personal Identification Number (PIN). Then, the customer can perform a secured online transaction. With this model, customers will easily authenticate themselves, besides that they also can sign on the transactions made.

Although this process seems cumbersome, nevertheless the Barclay Bank has implemented it since 2007. The bank reported that almost one million of their customers are using it. This shows a good response since it was launched. Hence, the user will have control on the validity of identification using the card reader. This will encourage user to use electronic payment in their future transactions.

3.3 Tools Requirement

MyKad Reader FT SCR2000

FT SCR2000 smart card reader is designed for multiple uses of smart card applications and it is also applicable for credit card sized. This reader is developed to suit any computers with an availability of a standard USB port. A built-in dual-color LED indicator will communicate messages to users for status indication. The slim shape makes it easy to carry and plug without additional space required to your desktop.

Operating System

There are multiple operating systems supported for this reader such as Windows 98SE/Me/2000/Server 2003/XP, Linux and Mac OS. So, it will depends on the user choice or selection.

Hardware

Minimum hardware requirements include personal computer with a Pentium or higher microprocessor, 64MB of RAM, 5MB free Hard Disc space and the most important is 64K MyKad.

4. Method Proposed

This study will use case study method where literature on existing payment model were reviewed and analyzed as in Section 2. Based on the reviewed model, the basic elements of the model were identified and the basic payment model as proposed in Section 3. In addition, an interview will be conducted soon with key Malaysian players to perform electronic commerce transaction.

4.1 Proposed System

To develop the prototype transaction base application using MyKad, we proposed to use VB.NET programming as the language for this system. The system is developed to show how the process of the transaction and also to validate if the model is really works. .NET is familiar because of its advantages where the programmers or developers can create applications using various used languages and development tools such as Visual Basic. The prototype developed will be tested with MyKad and MyKad reader attached to the system in order to give the flow of the system and in addition to make sure the proposed model is works using the prototype.

All card systems depend on a central database in some form (Henry, 2007). Currently, the use of large scale databases is strongly expanding and offers some scope of abuse. If the programmers or developers are managed to implement the card system to the databases, it will give the card holders more power of their own data and control the access to the data.

5.0 Expected Result

Based on this study, the expected result will be a model for electronic payment that is applicable in the context of MyKad. With this, financial transactions can be perform online using MyKad. This in turn will encourage more Malaysian to perform e-commerce transaction in the future.

6. Conclussion

Many elements should be considered when developing this payment model which includes the MyKad type, the flow of the digital license application and so on.This model should be tested against internet based business transactions available in e-commerce and other business services. This is to ensure that this payment model is reliable and valid in fulfilling its purposes. Hence, if the payment model demonstrates high effectiveness, it can be the basis of other payment model.

Acknowledgement

We would like to thank all staff and members who were involved in this research either directly or indirectly and also for their valuable supports and contributions.

REFERENCES

[1] Card Technology Today, Volume 20, Issues 7-8, July-August 2008, Page 1.

[2] Fadi Abdulhamid and Ezz Hattab 2004. A Model for Person to Person Electronic Payment System. Working Paper

[3] Gonzalez, A.G. 2004. PayPal: The Legal Status of C2C Payment Systems. *Computer Law & Security Report Vol. 20 No. 4 2004.*

[4] Hendry, M. 2007. Multi-application Smart Cards: Technology and Applications. Cambridge: Cambridge University Press, 2007

[5] Knight, W. Malaysia Pioneers Smart Cards with Fingerprint Data, *New Scientist,* September 21, 2001.

[6] Rivest, R.L. and Shamir, A. 1996. PayWord and Micromint, Two Simple Micropayment Schemes. *RSA '96 Conference.*

[7] MyKad retrieved on May 3rd, 2007 from http://www.jpn.gov.my/

[8] www.paycircle.org retrieved on Jun 10th, 2008.

[9] http://www.mykadpro.net/ retrieved on August 20th, 2008.