A LIGHTWEIGHT AND PRIVATE MOBILE PAYMENT PROTOCOL

TAN SOO FUN

THESIS SUBMITTED IN FULFILLMENT FOR THE DEGREE OF MASTER OF SCIENCE

LABUAN SCHOOL OF INFORMATICS SCIENCE
UNIVERSITI MALAYSIA SABAH
2009
DECLARATION

I hereby declare that the material in this thesis entitled "A lightweight and Private Mobile Payment Protocol" is the result of my own research except for quotations, excerpts, equations, summaries and references, which have been duly acknowledged.

1 June 2009

Tan Soo Fun
PI20078017
CERTIFICATION

JUDUL: A LIGHTWEIGHT AND PRIVATE MOBILE PAYMENT PROTOCOL
IJAZAH: MASTER OF SCIENCE (COMPUTER SCIENCE)
SESIS PENGAJIAN: 2007 – 2009

Saya, TAN SOO FUN mengaku membenarkan tesis sarjana ini disimpan di perpustakaan Universiti Malaysia Sabah dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hak milik Universiti Malaysia Sabah.
2. Perpustakaan Universiti Malaysia Sabah dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. TIDAK TERHAD

Disahkan oleh

Penulis: TAN SOO FUN
Alamat: 48, Taman Wijaya, 84700, Grisek, Muar, Johor

Penyelia: Assoc. Prof Dr. Hj Rozaini Roslan
Penyelia: En. Mohd Yuszren Yusak
Penyelia: En. Jonathan Likoh Juis

Tarikh: 2009
NAME : TAN SOO FUN
MATRIC NO : PI20078017
TITLE : A LIGHTWEIGHT AND PRIVATE MOBILE PAYMENT PROTOCOL
DEGREE : MASTER OF SCIENCE
VIVA DATE : 31 MARCH 2009

DECLARED BY

1. SUPERVISOR
   (Assoc. Prof Dr. Hj Rozaini Roslan)

2. CO-SUPERVISOR
   (En. Mohd Yuszren Yusak)

3. CO-SUPERVISOR
   (En. Jonathan Likoh Juis)

4. INTERNAL EXAMINER
   (Assoc. Prof. Assoc. Prof. Dr. Patricia Anthony)

5. DEAN/DIRECTOR
   (Dr. Ag Asri Hj Ag Ibrahim)
ACKNOWLEDGEMENT

In preparing this valuable piece of work, I received much excellent encouragement, guidance and advices from many people. These people certainly have contributed toward me achieving this. Firstly, I would like to express my deepest gratitude to Dr. Hj. Rozaini Roslan, Mr. Mohd Yuszren Yusak and Mr. Jonathan Likoh Juis as my thesis supervisors for giving me fully support and faithfulness in all guidance, advices and commitment upon on effort since the beginning of this thesis. Besides, I also would like to present my special thanks to all the lectures that have given me theirs guidance and advices. I also would like to express my sincere appreciation for my family members who always encourage and give me fully support for doing this research. Finally, I am also very thankful to my friends for their supports and assistances at various occasions. Indeed, the encouragement and support are deeply appreciated.

Tan Soo Fun
1 June 2009
Mobile commerce (m-commerce) has undoubtedly become an omnipresent and an active area in electronic payments. It allows mobile user to buy and pay for things, pay his bill or make a bet via mobile phone when on move, anywhere and at any time. However, several challenges in accountability and privacy properties have emerged with the widespread of mobile payments in recent years. Consequently, many public-key cryptography based mobile payment protocols have been proposed. However, limited capabilities of mobile devices (poor computation power, low battery capacity and limited storage memory), limitation of wireless networks (less bandwidth and reliability, and higher latencies), and higher wireless networks connection cost make these protocols unsuitable for mobile network. In this paper, a lightweight and private mobile payment protocol involving mobile network operators (MNOs) and employing symmetric key operations is proposed. It is unrealistic to expect all payers and all payees to have accounts with multiples MNOs. Therefore, the proposed protocol supports the interoperability among multiple MNOs, each with its own customer (payer) and merchant (payee), allowing customers of one MNO to make purchases from merchants of the other MNO. The symmetric cryptographic technique applied into the proposed protocol not only reduces the number of cryptographic operations and communication passes between the involved parties, but also achieves completely privacy protection of payer and satisfies all the criteria of end-to-end security property, party's requirements including non-repudiation. The proposed mobile payment protocol is analyzed with Kungpisdan et al. accountability logic (KP Logic). The result shows that the proposed protocol satisfies all security requirements in electronic payment transaction, enhances privacy protection and reduces the number of cryptographic operations in existing mobile payment protocols.
ABSTRAK

# LIST OF CONTENTS

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TITLE</td>
<td>i</td>
</tr>
<tr>
<td>DECLARATION</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td>v</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>vi</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF CONTENTS</td>
<td>viii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xii</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>xvi</td>
</tr>
<tr>
<td>LIST OF NOTATIONS</td>
<td>xvii</td>
</tr>
<tr>
<td>LIST OF APPENDIX</td>
<td>xxi</td>
</tr>
</tbody>
</table>

## CHAPTER 1: INTRODUCTION

1.1 Overview

1.2 Background And Problem Statements

1.3 Aims And Objectives

1.4 Scopes

1.5 Methodology

1.6 Outline

## CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

2.2 Overview Of Mobile Payment Protocol

2.2.1 Actors

2.2.2 Model

2.2.3 Method

2.2.4 Transaction Flow of Payment Data

2.3 Security Requirements For Payment Transactions

2.4 Cryptography Techniques For Payment Transaction

2.4.1 Symmetric / Asymmetric Key

2.4.2 Symmetric Key Exchange

2.4.3 Key Generation Techniques

2.4.4 Hash Functions

2.4.5 Message Authentication Code

2.4.6 Nonce

2.5 Analysis Techniques For Payment Protocol

2.5.1 BAN Logic

2.5.2 Kaliar's Logic
7.3 Security Issues Of Proposed Mobile Payment Protocol
7.3.1 Authentication
7.3.2 Message Integrity
7.3.3 Confidentiality
7.3.4 Anti-Replay Protection
7.3.5 Anonymity
7.3.6 Privacy Protection
7.3.7 Authorization
7.3.8 Non-Repudiation
7.4 Summary

CHAPTER 8: CONCLUSION
8.1 Introduction
8.2 Research Contributors
8.3 Future Works
8.4 Summary

REFERENCES

GLOSSARY

APPENDIX
<table>
<thead>
<tr>
<th>Table 2.1</th>
<th>Mobile Network Operator Penetration Rate and Subscriber</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2.2</td>
<td>iKP Party’s Authorization Requirements</td>
<td>21</td>
</tr>
<tr>
<td>Table 2.3</td>
<td>Formulae of KP Logic</td>
<td>39</td>
</tr>
<tr>
<td>Table 4.1</td>
<td>Notations of Proposed Mobile Payment Protocol</td>
<td>73</td>
</tr>
<tr>
<td>Table 7.1</td>
<td>Comparison of Cryptographic Operations</td>
<td>116</td>
</tr>
<tr>
<td>Table 7.2</td>
<td>Comparison on Privacy Protection</td>
<td>118</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1</td>
<td>Operational Steps and Research Methodology</td>
<td>7</td>
</tr>
<tr>
<td>Figure 2.1</td>
<td>Traditional Payment Data Flow scenario</td>
<td>18</td>
</tr>
<tr>
<td>Figure 2.2</td>
<td>Client Centric Model</td>
<td>19</td>
</tr>
<tr>
<td>Figure 2.3</td>
<td>Cryptographic Techniques for Payment Transaction</td>
<td>22</td>
</tr>
<tr>
<td>Figure 2.4</td>
<td>Operation of a Symmetric Cryptosystem</td>
<td>23</td>
</tr>
<tr>
<td>Figure 2.5</td>
<td>Operation of Public-Key Cryptosystem</td>
<td>24</td>
</tr>
<tr>
<td>Figure 2.6</td>
<td>Public Key Distribution for Symmetric Key</td>
<td>26</td>
</tr>
<tr>
<td>Figure 2.7</td>
<td>Diffie-Hellman Key Agreement</td>
<td>27</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>Primitive Transaction</td>
<td>47</td>
</tr>
<tr>
<td>Figure 3.2</td>
<td>Communication Sequence of SET Payment Protocol</td>
<td>48</td>
</tr>
<tr>
<td>Figure 3.3</td>
<td>Communication Sequence of i KP Payment Protocol</td>
<td>51</td>
</tr>
<tr>
<td>Figure 3.4</td>
<td>Communication Sequence of KSL Payment Protocol</td>
<td>53</td>
</tr>
<tr>
<td>Figure 3.5</td>
<td>Communication Sequence of Kungpisdan <em>et al.</em> Payment Protocol</td>
<td>56</td>
</tr>
<tr>
<td>Figure 3.6</td>
<td>Communication Sequence of Tellez <em>et al.</em> Payment Protocol</td>
<td>59</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>Key Generation Techniques of Proposed Mobile Payment Protocol</td>
<td>69</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Registration Protocol for Proposed Mobile Payment Protocol</td>
<td>76</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>Diagram of Proposed Mobile Payment Protocol</td>
<td>77</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>Communication Sequence of Proposed Mobile Payment Protocol</td>
<td>78</td>
</tr>
<tr>
<td>Figure 5.1</td>
<td>The Pseudo code of Proposed Mobile Payment Protocol</td>
<td>88</td>
</tr>
<tr>
<td>Figure 5.2</td>
<td>Payer Initiates Payment</td>
<td>89</td>
</tr>
<tr>
<td>Figure 5.3</td>
<td>New Payment Request Alert For Payee</td>
<td>89</td>
</tr>
<tr>
<td>Figure 5.4</td>
<td>Payer Issues a Payment</td>
<td>Page</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Figure 5.5</td>
<td>Payer Sends a Payment Request</td>
<td>90</td>
</tr>
<tr>
<td>Figure 5.6</td>
<td>A Confirmation Alert for Payer</td>
<td>91</td>
</tr>
<tr>
<td>Figure 5.7</td>
<td>Hash Function</td>
<td>91</td>
</tr>
<tr>
<td>Figure 5.8</td>
<td>The pseudo code of Hash Function</td>
<td>91</td>
</tr>
<tr>
<td>Figure 5.9</td>
<td>The Pseudo Code of Encryption and Decryption Symmetric Key</td>
<td>92</td>
</tr>
</tbody>
</table>
**LIST OF ABBREVIATIONS**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G</td>
<td>The second generation of wireless technology. Usually identified as GSM</td>
</tr>
<tr>
<td>2.5G</td>
<td>Between the second and third generations of wireless technology. Usually identified as GPRS</td>
</tr>
<tr>
<td>3G</td>
<td>Third generation of wireless technology. Usually identified as UMTS</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CCI</td>
<td>Credit Card Information</td>
</tr>
<tr>
<td>CLDC</td>
<td>Connected Limited Device Configuration</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>Electronic Commerce</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data for GSM Evolution</td>
</tr>
<tr>
<td>EFTPOS</td>
<td>Electronic Funds Transfer at Point of Sales</td>
</tr>
<tr>
<td>FSP</td>
<td>Financial Service Providers</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Services</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile communication</td>
</tr>
<tr>
<td>HMAC</td>
<td>Keyed-Hash Message Authentication Code</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTP over SSL (secure socket layer)</td>
</tr>
<tr>
<td>IrDA</td>
<td>Infrared</td>
</tr>
<tr>
<td>IrFM</td>
<td>Infrared Financial Messaging</td>
</tr>
</tbody>
</table>
POS  Point-of-Sale
PSP  Payment Service Providers
RFID  Radio Frequency Identification
RTT  Radio Transmission Technology
SAT  SIM application Toolkit
SET  Secure Electronic Transaction
SHA-1  Secure Hash Algorithm Version 1, also called as Secure Hash Standard (SHS)
SIM  Subscriber Identity Module
SMS  Short Message Service
TSC  Time Stamp Center
TTP  Trusted Third Party
WAP  Wireless Application Protocol
UMTS  Universal Mobile Telecommunication System
W-CDMA  Wideband Code Division Multiple Access
WIM  Wireless Identity Module. Usually associated with SIM
WTLS  Wireless Transport Layer Security
WWW  World Wide Web
LIST OF NOTATIONS

\{ \Phi, \Psi \} \quad \text{A set of statements that derived from messages}

\rightarrow^K Q \quad \text{The symmetric key } K \text{ can be used to refer } Q

A_l \quad \text{Account Information of Party } P, \text{ which including credit limit for each transaction, type of account (post-paid or prepaid account)}

AMOUNT \quad \text{Payment transaction amount and currency}

AuthReq \quad \text{Authentication Request message}

AuthRes \quad \text{Authentication Response message}

BrandID \quad \text{Brand of card that will be used in the payment, such as VISA}

CapAmt \quad \text{Payment Capture Amount}

CapID \quad \text{Payment Capture Message ID}

CapCode \quad \text{Payment Capture Code}

CapReq \quad \text{Payment Capture Request message}

CapRes \quad \text{Payment Capture Response message}

Cap_Token \quad \text{Payment Capture Token}

Cert \quad \text{A certificate of party } P \text{ which contains } \{ ID, K_P \}

Chall_C \quad \text{Client's Challenges variable used in the merchant's to guarantee the freshness of the communication}

Chall_M \quad \text{Merchant's Challenges variable to guarantee the freshness of the communication}

\{ C, M, PG, I, A, Payee, Payer, Payee's MNO, Payer's MNO, TSC \} \quad \text{A set of engaging parties, which are Client, Merchant, Payment Gateway, Issuer, Acquirer, Payee, Payer, Payee's MNO, Payer's MNO and Time Stamp Center respectively.}
<p>| <strong>DATE</strong> | Date of payment execution |
| <strong>DESC</strong> | Payment Description, which may includes delivery address, purchase order details and so on. Payer will include only the information that he/she wish to disclosure to Payee. |
| <strong>E_{p,p'}</strong> | Message $X$ singed and encrypted by the user $ID_p$ to a specified received $ID_{p'}$. |
| <strong>H(M)</strong> | The one way hash function of the message $M$ |
| <strong>ID_p</strong> | Identity of engaging party $P$ |
| <strong>InqReq</strong> | Inquiry Request message |
| <strong>InqRes</strong> | Inquiry Response message |
| <strong>i</strong> | Used to identify the current session key of $X_i$, where $i = 1, 2, ..., n$ |
| <strong>K-is-decrypting-key-for-{M}K</strong> | The symmetric key $K$ can be used to decrypted ${M}<em>K$ |
| **K</em>{p,p}** | The secret key $K$ shared between Payer’s MNO and Payee’s MNO. |
| <strong>K_p</strong> | Public key of Party $P$ |
| <strong>K_{p^{-1}}</strong> | Private key of Party $P$ |
| <strong>LID_C</strong> | A local ID for the transaction |
| <strong>MAC(M,K)</strong> | The Message Authentication Code (MAC) of the message $M$ with the key $K$ |
| <strong>MID_{req}</strong> | The request for $ID_M$ |
| ${M}_K$ | The message $M$ encrypted with the public key of the party $P$ |
| ${M}_K^{-1}$ | The message $M$ signed with the private key of the party $P$ |
| ${M}_K$ | The message $M$ symmetrically encrypted with the shared key $K$ |
| <strong>NID_C</strong> | Nick Name of Client |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONCE</td>
<td>Random number and timestamp generated to protect against replay attack, that is ensure old communication cannot reused in replay attack.</td>
</tr>
<tr>
<td>Order Information</td>
<td>OI</td>
</tr>
<tr>
<td>$P \leftarrow^k Q$</td>
<td>The symmetric key $K$ is the shared key between party $P$ and party $Q$</td>
</tr>
<tr>
<td>PayeeIDReq</td>
<td>The request for ID of payee.</td>
</tr>
<tr>
<td>PI</td>
<td>Payment Information which contains Credit Card Information (CCI)</td>
</tr>
<tr>
<td>$PIN_p$</td>
<td>Party $P$ selected Password Identification Number ($PIN$)</td>
</tr>
<tr>
<td>PInitReq</td>
<td>Payment Initialization Request message</td>
</tr>
<tr>
<td>PInitRes</td>
<td>Payment Initialization Response message</td>
</tr>
<tr>
<td>PReq</td>
<td>Payment Request message</td>
</tr>
<tr>
<td>PRes</td>
<td>Payment Response message</td>
</tr>
<tr>
<td>$P$ believes $\Phi$</td>
<td>A party $P$ believes that the statement $\Phi$ is true by doing some actions.</td>
</tr>
<tr>
<td>$P$ has $M$</td>
<td>A party $P$ possesses a message $M$. Party $P$ can send $M$ to other parties or use it for further computations.</td>
</tr>
<tr>
<td>$P$ says $M$</td>
<td>A party $P$ has sent a message $M$.</td>
</tr>
<tr>
<td>$P$ sees $M$</td>
<td>Some party has sent a message $M$ to party $P$ and party $P$ is able to read $M$.</td>
</tr>
<tr>
<td>$P$ CanProve $\Phi$ to $Q$</td>
<td>A party $P$ can prove to party $Q$ that statement $\Phi$ is true by sending a message $M$ to party $Q$. After party $Q$ receives $M$, he believes that the statement $\Phi$ is true.</td>
</tr>
<tr>
<td>$P$ authorized Payment ($P$, $Q$, AMOUNT, DATE)</td>
<td>A party $P$ has authorization on making the payment amount (AMOUNT) to party $Q$ on the date of transaction (DATE).</td>
</tr>
</tbody>
</table>
A party \( P \) has authorization on requesting party \( Q \) to deduct the amount \((AMOUNT)\) from party \( P \) account on the date of the transaction \((DATE)\).

A party \( P \) has authorization on requesting party \( Q \) to transfer the amount \((AMOUNT)\) to party \( P \) account on the date of transaction \((DATE)\).

\[ P \rightarrow Q \]

Party \( P \) sends a message to party \( Q \)

Payment receivable update status, which includes the received payment amount

Payer’s nick name, random number and timestamp generated by payer act as payer’s pseudo-ID, which uniquely identifies payer to payee

The registration status, whether the registration process is success or failed

The type of card used in the purchase process, \((TC=\{Credit, Debit\})\).

Optional list of certificates \((Thumbs)\) already stored by the cardholder software. This list consists of a thumbprint \((SHA\ hash)\) of each certificate held

Identity of transaction

The request for \( TID \)

Payer’s public value used in the signature process

\( A \) is a fingerprint of \( B \)

The status of transaction approved/rejected
# LIST OF APPENDIX

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPENDIX A</td>
<td>Gantt Chart</td>
<td>151</td>
</tr>
<tr>
<td>APPENDIX B</td>
<td>Source Code: Proposed Mobile Payment Protocol Simulator</td>
<td>152</td>
</tr>
<tr>
<td>APPENDIX C</td>
<td>Source Code: Java Cryptography</td>
<td>160</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Overview

The increasing development of wireless networks and the widespread popularity of handheld devices such as Personal Digital Assistants (PDAs), mobile phones and wireless tablets, have led to numerous applications ranging from mobile banking, location-based tracking to mobile advertising. According to Durlacher (1999), mobile commerce (m-commerce) refers as any transaction with a monetary value that is conducted via a mobile telecommunications network. Mobile payment is defined as any transaction that is carried out via mobile device, involves either direct or indirect exchange of monetary values between two or more parties involved (Krueger, 2001; Pousttchi, 2003; Jun et al., 2005). Wolco (2008) predicts that the rapidly evolving market for money transfer and remittances via mobile phones resulting more than 100 million global users will use their mobile phones to make international money transfers by 2013.

According to Malte (2001) and Wolco (2008), two basic forces indicate a positive future of mobile payments. Firstly, the increasing spread of mobile phones and technologies. The number of worldwide mobile phones users will reach 4.5 billion on 2013 (Business News and Technology News 2009). The mobile device's storage, computing and data transmission capabilities have made mobile phone an ideal device to store everything that is normally carried in wallet, including coins, cash, ATM cards, debit cards and credit cards. Secondly, mobile payment can be accepted as universal payment method for daily financial transactions such as web store-front payment, physical Point-of-Sale (POS) purchase, Person-to-Person (P2P) payment, and payment for mobile commerce application. Muller-Veerse (2000) and Vilmos and Karnouskos (2003) highlighted the attractiveness of m-commerce and mobile payment such as ubiquity, reachability, personalization, localization, convenience and coverage. These allow great flexibility and creativity for
businesses to increase their volume of transactions and offer their volume of
transactions and offer customers more ways of making payment.

1.2 Background and Problem Statements
Some issues hampering the widespread acceptance of mobile payment such as ease of use, expenses, security, universality and technical feasibility. According to Cervera (2002), Kungpisdan et al. (2003a) and Pousttchi et al. (2007), security issues are very fundamental of critical success factor in making mobile payment a reality. However, designing secure mobile payment protocol is more challenging than Internet payment protocol due to the constraints of wireless network and mobile devices. Firstly, the limitations of mobile devices such as lower power, computational and storage capabilities. Secondly, the constraints of wireless network such as lower bandwidth, less reliability and higher latencies than wired network. Furthermore, the cost of wireless network connection is higher than wired network (Cimato, 2002; Halonen, 2002; Tellez et al., 2007). These resulting existing Internet payment protocol such as Secure Electronic Protocol (SET) and Internet Payment Protocol (A(P) cannot be directly adopted in wireless environments as they designed for wired network and do not meet all the challenges of wireless environments (Chari et al., 2001; Marvel, 2001; Cimato, 2002; Halonen, 2002; Tellez et al., 2007).

Currently, several mobile payment protocols have been proposed. However, most of them (Bellare et al., 2000; Vilmos and Karnouskos, 2003; Tellez et al., 2007) are based on Public Key Infrastructure (PKI) which are inefficient to be applied into wireless networks. The PKI is a technology and management needed for a certificate authority (CA) to create public key and private key pairs, distribute private keys, issue digital certificates, and maintain certificate revocation list. With public key encryption, client needs to perform high computational operations, and his mobile device is required to have sufficient storage to store public-key certificates (Ramfos et al., 2004; Jun et al., 2005; Li and Hu, 2008). Although some mobile devices are equipped with special processors (VISA, 2007), performing such operations on them still requires longer procession time (Kungpisdan et al., 2004a). Furthermore, during a transaction, each certificate sent to the payer has to be
verified by a Certificate Authority (CA) located in a fixed network, which results in an additional communication passes between engaging parties (Kungpisdan et al., 2004a; Wang and Leung, 2005; Tellez et al., 2007; Li and Hu, 2008).

To solve the PKI problems, Kungpisdan et al. (2003a) proposed KSL payment protocol by reducing computational tasks at payer’s wireless devices. Tellez et al. (2007) proposed a digital signature scheme with message recovery using self-certified public keys to solve PKI problem. Although some payment schemes (Kungpisdan et al., 2003a, 2003b; Tellez et al., 2007), public-key cryptography have been reduced to certain degrees, these schemes are still impractically feasible apply into mobile payment (Kungpisdan et al., 2004a; Wang and Leung, 2005; Li and Hu, 2008). Hence, Kungpisdan et al. (2004a) proposed another mobile payment protocol to enhance their KSL payment protocol (2003a) by employs symmetric key operations not only for payer side but also for all engaging parties.

Wang and Leung (2005), Tiwari et al. (2007) and Li and Hu (2008) further pointed out several limitations of existing mobile payment protocol. Firstly, the privacy of the payer is not protected during the transaction. The payer’s identity and the transaction details are revealed not only to the payee, but also to the payment gateway and the banks. Secondly, some existing mobile payment protocols (Mastercard and Visa 1997; Bellare et al., 2000; Kungpisdan et al., 2003a, 2004a) are based on full-connectivity scenario as stated by Tellez et al. (2007), which does not consider the situation of payee who is not under the coverage of communication connection, or is unaffordable due to the inconvenience and costs. Thirdly, some payment schemes ( Mastercard and Visa 1997; Bellare et al., 2000; Kungpisdan et al., 2003a, 2004a) were designed to preserve the traditional flow of payment data (Payer - Payee- Payee’s Bank). Therefore, it is vulnerable to violation like transaction or balance modification by payee and gaining illegal access to payer’s account. These increasing the payer’s risk which their credit or debit cards can be captured and used later to access a payer account without authorization. Besides that, there is no notification to the payer from the payer’s bank after the successful transfer. The payer has to check his balance again. Lastly, some of
REFERENCE


Mickan, S. 2004. Paybox Makes Credit Cards Mobile in Belgium and Iceland, Paybox solutions AG. (Online) 

Mint.2007.Mobile Payments . (online)

Mobilewallet2u. 2008. *What is Mobile Wallet*. (Online)

Mobipay. 2007. (Online)


MovieTickets. 2007. (Online)


Trivent, 2008.(Online)


Valista, 2008. (Online)


VISA. 2007. *Mobile Visa Wave: Visa’s Contactless Payment Program for Mobile Phone in Malaysia*. (Online)


