A Secure SMS Model in E-Commerce Payment using Combined AES and ECC Encryption Algorithms

Abdolghader Pourali

Student of Department of Computer Engineering

Islamic Azad University, UAE branch, Dubai, UAE

Pourali_ghader@yahoo.com

Dr. Mohammad V. Malakooti

Faculty and Head of Department of Computer Engineering

Islamic Azad University, UAE branch, Dubai, UAE

malakooti@iau.ae

Dr. Muhammad Hussein Yektaie

Faculty of Department of Computer Engineering

Islamic Azad University, Abadan branch, Abadan, Iran

mh.yektaie@gmail.com

ABSTRACT

Mobile commerce is whatever electronic transfer or transaction via a mobile modem through a mobile net in which the true value or advance payment is done for goods, services or information. A mobile payment system should be beneficial for all related persons. For a payment system to be a Successful system, End-user, seller, exporter and operators should see a additional value in it. End-user prefers simplicity, available speed, convenience, security and suitable cost. Sellers want to cover many customers powerfully a mobile payment system. They are attending to obtain additional money by mobile payment services by increasing security and reducing the risk of denying the transaction. There are various mobile payment technologies which some of them are successful, unsuccessful and gradually disappeared. In this article the various mobile electronic commerce payment models are studied by the aim of choosing the ideal model .After the application of hybrid AES Symmetric and ECC Asymmetric Algorithm coding, an SMS based model is presented in electronic commerce.

KEYWORDS

Mobile payment, security, Mobile E-commerce, Encryption.

1 - INTRODUCTION

Progress of technology and development of mobile technologies led to formation of a new type of e-commerce as mobile commerce. Mobile commerce can be defined as performance of commercial transactions using mobile devices such as mobile phones, PDAs and computers without mobile system. E-payment means the process which enables two parties to exchange financial value of a product or service using a mobile system [1],[2]. E-payment is expected to be one of the best applications of e-commerce. Generally, a payment system should be able to fulfill security conditions such as authentication, confidentiality, data integration, Non Repudiation, etc. for this reason, the presence of standard and generalized procedures seems to be necessary to expand mobile commerce. Today, different methods have been provided for e-banking particularly e-payment, which have tried to make e-payment transactions in the shortest possible time and with suitable security. Different methods of payment can be classified based on different criteria such as the used technology, type of used account and type of business model and the like. In this paper, we discuss types of e-payment methods, business models, and the used technology and finally, we present a safe model based on SMS and application of security mechanisms based on AES and ESS algorithms for performing interactions.

2 - E-payment business models

Different types of e-payment business models are being completed. Difference of these models is caused by response to this question: who establishes relation (payment of fund, bill payment, opening accounts et) with end user, bank, operators and other non-bank companies. One of the other differences is hidden in nature and rules between bank and non-bank companies and agencies. But there are four potential models for payment of mobile phone: Operator – Centric model, Bank-centric model, Peer to peer model and Collaboration model.

2.1 Operators-Centric Model

In Operator-Centric Model, mobile phone operators act independently for performance of e-payment and financial institutes don't participate in payment process. In this model, operator is production authority and e-payment manager. Many of the developed Operator-Centric models have been challenged due to no connection with present payment networks. Some examples have been commissioned with this model in the newly emerging countries but they don't cover e-payment services methods and e-payments have been limited to payment of fund and purchase of mobile phone charge. Here, payment can be made with two methods: payment with credit card and payment through telecommunication phone bill. Therefore, major payments are not supported in this model. Operator also can create a mobile wallet independent of user account [3][4]. Communication scenario between beneficiaries in Operator-Centric Model is shown in Figure 1.

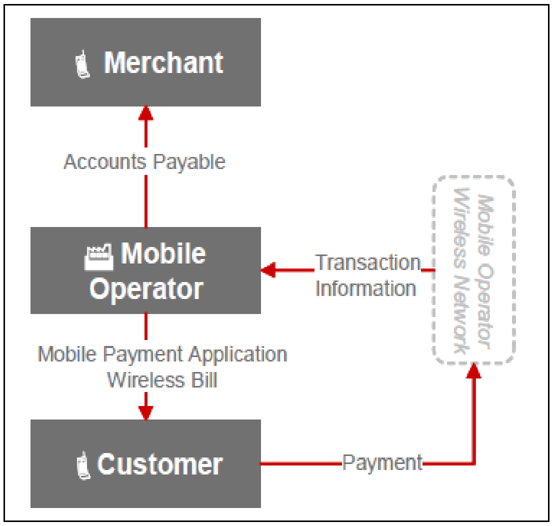

Figure 1: Operator-Centric Model: Stakeholder Scenario [5]

Operator-Centric Model faces different challenges. The first problem which this model faces is presentation of a set of products and services for payment and also presentation of a solution which can be accepted as the safe and reliable method [5]. The second challenge is collective acceptance of this model by merchant and consumers which will be difficult due to:

- Problems of privacy and imitation
- The absence of commercial relation between merchants and operator
- Centralization of POS equipment toward seller
- Challenge of billing and the required services of customer for operator

Considering the above cases and type of communication among beneficiaries in Operator-Centric Model, the presence of each of these people in this model will bring different profit and risk for them. Figure 2 graphically shows risk and profit rate for each one of the beneficiaries.

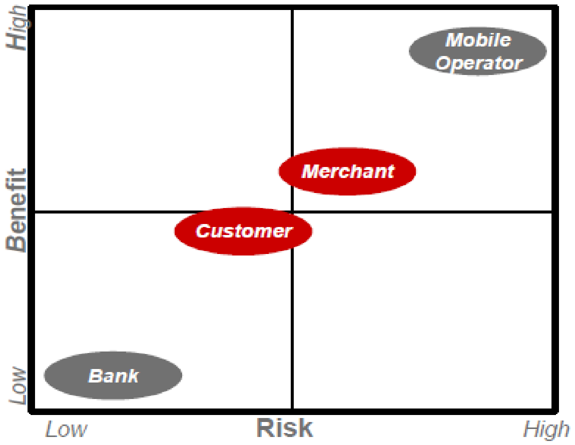

Figure 2: Risks and Benefits for Operator-Centric Model Stakeholders [5]

2.2 Bank-centric model

In this model, bank is responsible for production and management of e-payment service like the present credit card system. Operators don't participate in this payment process. Banks produce e-payment plans or provide e-payment devices for customers and guarantee communication point between customer and sellers. In this model, mobile network operator is used as a simple authority. However, there is benefit of operator in this model when banks use SimCard-based software technology for the mobile tools. In these cards, banks should pay rental to operators. Operators also provide their experience for guaranteeing QOS. In this model, since payments are made through bank accounts, both major and minor payments should be supported [3],[4]. Figure 3 shows communication scenario between beneficiaries in the Bank-Centric Model. One of the known systems which use Business Model is Pay Box method.

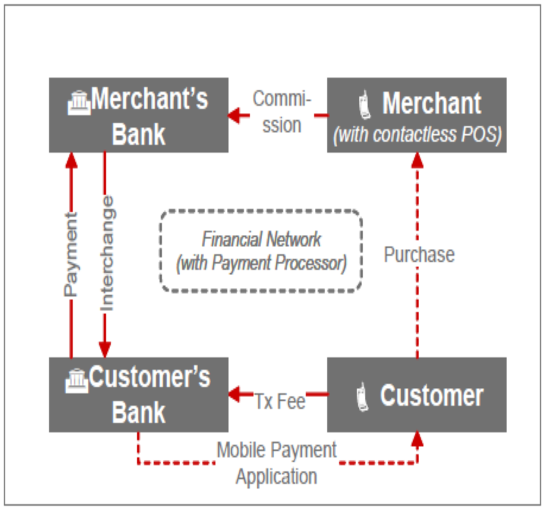
Merchant's Bank
Commi-ssion
Merchant (with contactless POS)
Payment
Interchange
Financial Network (with Payment Processor)
Purchase
Customer's Bank
Tx Fee
Customer
Mobile Payment Application

Figure 3: Bank-Centric Model: Stakeholder Scenario [5]

Considering these cases, there are some barriers for execution of a successful bank-centric model. First, all banks may be forced to support different and special standards of operators due to dependency of mobile phone operators. Second, banks act with trade for investment in e-payment considering that they are producing contactless debit and credit cards. Figure 4 shows risk and benefit for each one of the beneficiaries in bank-centric model.

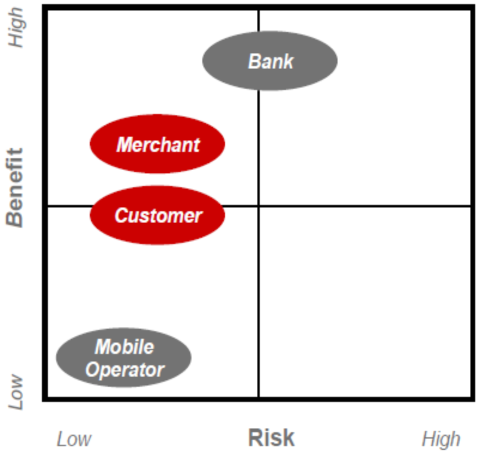

Figure 4: Risks and Benefits for Bank-Centric Model Stakeholders [5]

ISBN: 978-0-9891305-5-4 ©2014 SDIWC

2.3 Peer–to–peer model

This model is different from the above models. The third company commissions e-payment service using infrastructures of banks and operators and acts independently of financial institutes and network operators. The third company acts as a route among customers, sellers and banks. Transaction is performed peer to peer between customer and seller. This model changes the present payment ecosystem by reducing role of banks and payment networks. In addition, money can be transferred from a person to another person in this method. Therefore, this model affects business of money transfer. One of the known e-payment services which follow this business model is Pay Bal [3][4]. Figure 5 shows communication scenario between the beneficiaries in peer-to-peer model

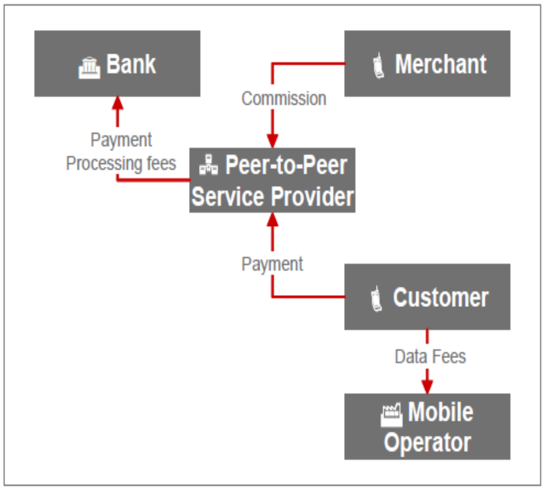

Figure 5: Peer-to-Peer Model: Stakeholder Scenario [5]

Peer to peer model is interesting for the merchant who seeks to reduce processing costs of payment credit and debit cards for non-bank customers and those who can use traditional cards. It is also suitable for the customers who seek to send money to friends and family out of their country.

However, the following cases and problems should be removed by the beneficiaries for survival of this model.

- Supporting considerable number of commercial places which can be used for customers.
- Providing sustainable income for banks so that they guide transactions toward this direction.
- Ensuring that transactions are suitable whether in POS or on line.
- Dominating over report of negative media on money laundering and security
- Settling dispute between beneficiaries

Figure 6 shows risk and benefit for each one of the beneficiaries in peer to peer model.

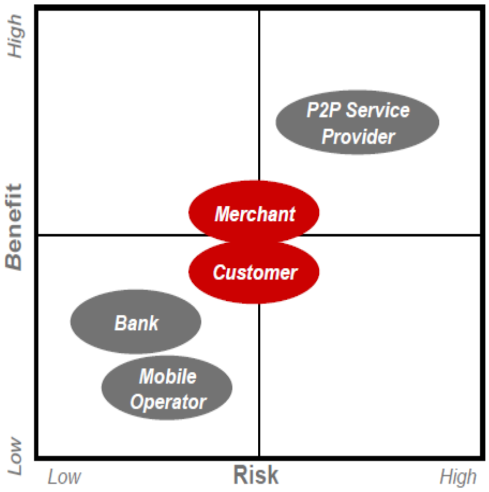

Figure 6: Risks and Benefits for Peer-to-Peer (P2P) Model Stakeholders [5**]**

2.4 **Collaboration Model**

Collaboration model includes collaborations between the trusted banks, operators and the third company. Service manager is responsible for management of all payment and collaboration processes among the operators and banks. This model allows beneficiaries to concentrate on their main capabilities, open door for earning new income from gradual services, direct retention and loyalty of customer and fulfill main demand of customers. Therefore, it is more possible to implement and establish collaboration model. In the survey which was performed in smart cards union, 86% of the respondents supported this model because it has the highest capability for long-term position [4]. Despite relations between actors of this model, their collaboration is very complex. ISIS and Google Wallet and Square Wallet are the payment services which follow this business model [3],[4]. Communication scenario between the beneficiaries is shown in collaboration operator model in Figure 7.

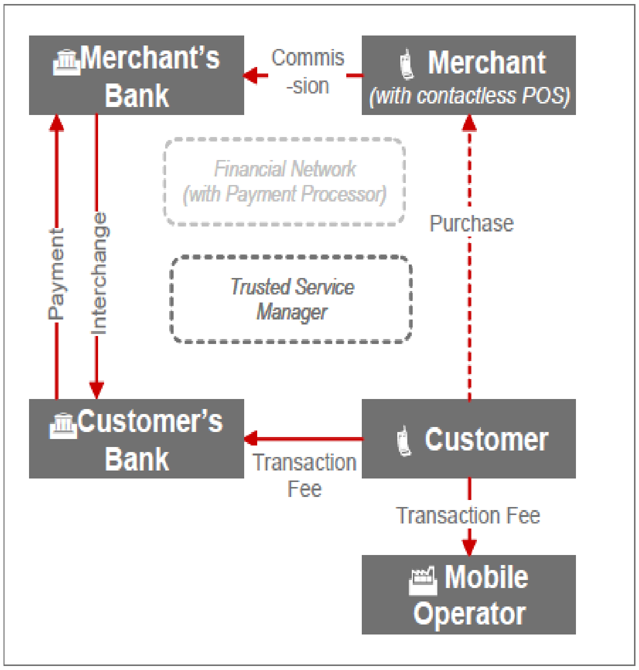

Figure 7: Collaboration Model: Stakeholder Scenario [5]

Figure 8 shows risk and benefit for each one of the beneficiaries in collaboration model.

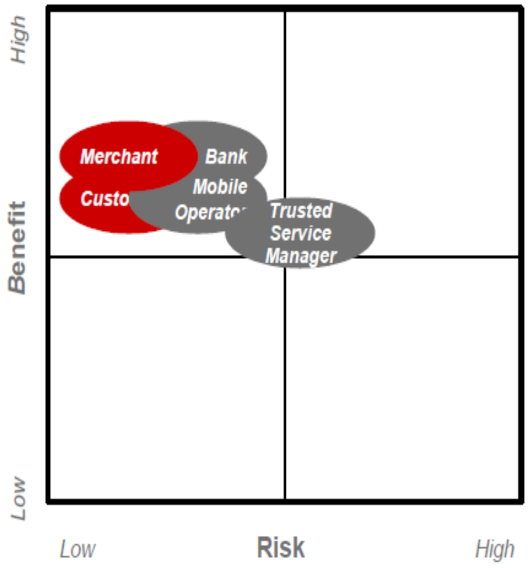

Figure 8: Risks and Benefits for Collaboration Model Stakeholders [5]

3 REVIEW of THE EXISTING E-PYMENT METHODS

Today, abundant methods have been presented in the world. Although each one of the methods may conform to one of the business models which have been presented, it has its own methods. In this Section, we study several current and active payment methods in the world.

3.1 A-Boku

This company was commissioned in 2009 and grew with two Mobillcash and Paymo companies which were active in e-payment services. Boku is active with mobile phone operators all over the world. Merchants and publishers use their main services called Paymo in 65 countries of the world. Focus of this company is first on purchaser and transactions for social games and virtual goods. Transfer of money has not been studied [6]. For purchase through Boku, user doesn't need only mobile phone and also needs credit card, bank account and other accounts and even internet. This company communicates with customer, seller , operator and bank of seller with this method. Technology used in this method is SMS and e-payment business model is almost similar to Operator- Centric-model [7].

3.2 Pay Pal

Pay Pal is a global e-business which has been created for payment and transfer of money through internet. Pay Pal Mobile is a specific solution belonging to Pay Pal and is usually used in USA and Canada. Pay Pal acts as a trusted third party between customer and seller. Pay Pal only charges receiver and sender doesn't pay cost for payment service. Interaction of participants is shown in Figure 9[8].

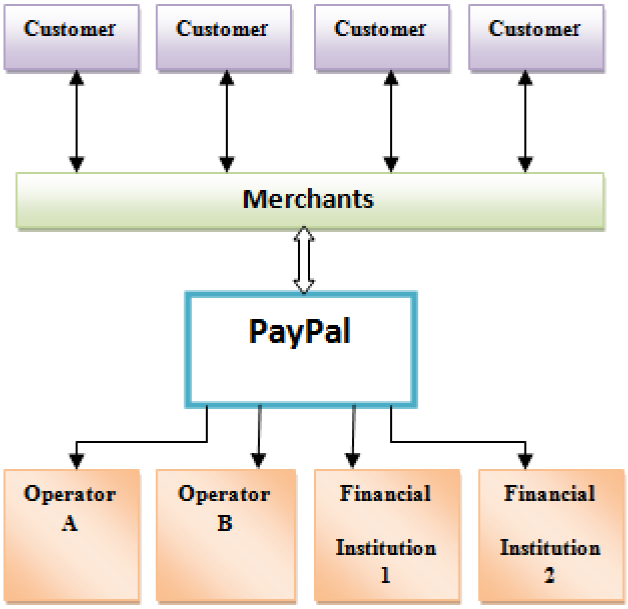

Figure 9: Business Model – PayPal Mobile

For shopping with this method, user only needs a mobile phone and a Pay Pal account with this method and hardware is not needed. To create a Pay Pal account, a credit or debit card is required to activate account. At time of purchasing operations, the phone should be connected to internet. For other communications, SMS and WAP are used. Pay Pal Mobile acts based on peer to peer model.

3.3 PayBox

Pay Box Company provides different services for trading mobile phone such as content, marketing and payment. For payment through Pay Box, user only needs a mobile phone and a bank account and also should be registered in Pay Box. Actors of business model in this project include customers and sellers of Pay Box and interaction between these actors is shown in Figure 10[8].

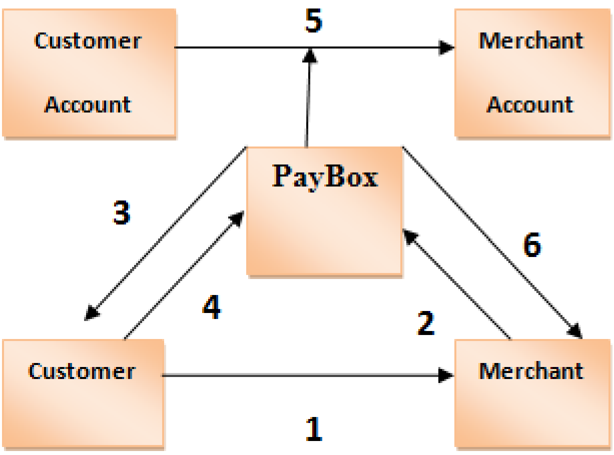

Figure 10: Interaction of participants in mobile payment with paybox

3.4 PayforIT

It is a company which provides mobile phone payment services which has been supported by all mobile phone operators of England and has been designed for easy mobile payments. Pay for IT has potential access to more than 52 million users in England. It supports micropayments (usually below 10 pounds) for purchase using mobile phone and simple and rapid methods of bill charging for payment. Since May 2007, Pay for IT supports web transactions as an income flow. For payment with this method, there is no need for bank account or special hardware and only one mobile phone is required. In addition to users, operators and merchants include a layer of participants called valid payment intermediary as described in Figure 11. Business model is in operator- centric Pay ForIT and WAP technology is used for performance of operations [8].

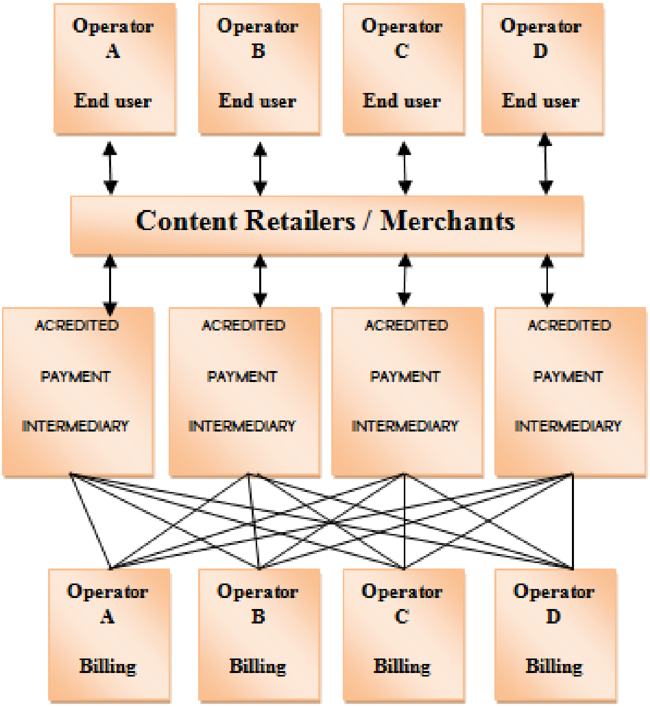
Operator A End user
Operator B End user
Operator C End user
Operator D End user
Content Retailers / Merchants
ACREDITED PAYMENT INTERMEDIARY
ACREDITED PAYMENT INTERMEDIARY
ACREDITED PAYMENT INTERMEDIARY
ACREDITED PAYMENT INTERMEDIARY
Operator A Billing
Operator B Billing
Operator C Billing
Operator D Billing

Figure 11: Business Model – PayforIT

3.5 **I-mode Mobile Payment - Osaifu-Keitai**

Osaifu-keitai mobile payment service has been introduced by the transferred NTTDoCoMo which is currently presented by all of three mobile operators in Japan to their users. Osaifu-keitai which principally means wallet allows use of smart cards for mobile payment. The user needs a mobile phone which supports i-mode card reader using this method. In this method, all purchase expenses are transferred to NTTDoCoMo after purchase by user and then registered beside other network expenses. Payment business model is operator –centric I-mode as shown in Figure 12.

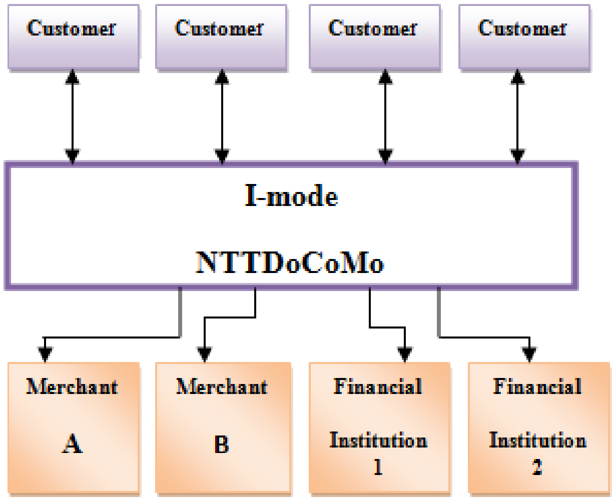

Figure 12: Business Model – Osaifu-Keitai

4- TYPES of MOBILE PAYMENTS

Mobile payments can be classified into two major groups based on its rate and volume.

1- Micropayments: includes payments of ten dollars below and means the payments in mobile medium such as cost of downloading video clip and games.
2- Macro payments : includes payment of high volume transaction cost such as online shopping and proximity payments such as park card but mobile payments can be classified from another perspective which is information transfer in mobile transactions . Based on this classification, two major groups of payment can be identified.
3- Mobile payments which are based on SMS/MMS technology or WAP crawlers based infrastructures.
4- Proximity payments which include use of message transfer protocols in limited distances such as (Contact Less Chip, Radio Frequency Identification (RFID), Infrared, Bluetooth, Near Field Communication, (NFC) for payment of price of goods and services.

5 - INTRODUCTION to ENCRYPTION

Encryption means use of mathematical techniques for hiding information [13]. Main goal of encryption is to enable sender and receiver to communicate with each other with a safe channel so that another person cannot understand or alter information. This communication channel can be telephone line, computer networks or wireless interfaces [14]. Cryptography techniques are mainly classified into two classes: symmetric and asymmetrical techniques [15]. In symmetric encryption, sender and receiver have equal key. When sender wants to send a message to receiver, he encrypts it with key and then sends the encrypted information. After receiving the information encrypted by receiver, the password will be recovered and information will be returned to the primary state and used [15]. In asymmetric encryption, each participant has two keys in communication: public key and private key. Private Key only belongs to sender and public key is given to receiver by sender. For decryption, receiver should use public key which is presented by sender along with private key [16].

6-PROPOSED MODEL

As illustrated in figure 13, the protocol includes six elements:

1-User (costumer): The owner of mobile device who buys goods or services via payment system.

2-Electronic (Digital) wallet: It is software installed on costumer's mobile device and consists of certain codes causing interactions between costumer, seller and bank. In plain English, user can interact bank and seller using this software. Besides, this software exploits cryptographic protocols to encrypt messages. This software is delivered to mobile user when he/she subscribes for using mobile services. Also, it might be provided for user in the form of a specific subscriber's services in expense of a monthly payment.

3-Merchant (seller): A person who sells electronic goods such as e-books, MP3, Downloads, software or search results in a digital library. Additionally, seller may provide some services for customers.

4- Trusted Third Party (TTP):
This element plays two main roles:
 As the reference for issuing certificates for banks (sellers' and costumers' bank)
 As a clearing house between banks. It settles payments between banks.

5- Costumer's bank: The bank where costumer has an account. It is responsible for authentication, controlling costumer's bank account; withdraw from costumer's account (debit) and communication with seller's bank.

6- Seller's bank: The bank where seller has a bank account. It communicates with costumer's bank and credits seller's bank accounts
Prior to entering this system, banks should register in TTP so that digital certificate is issued for them.

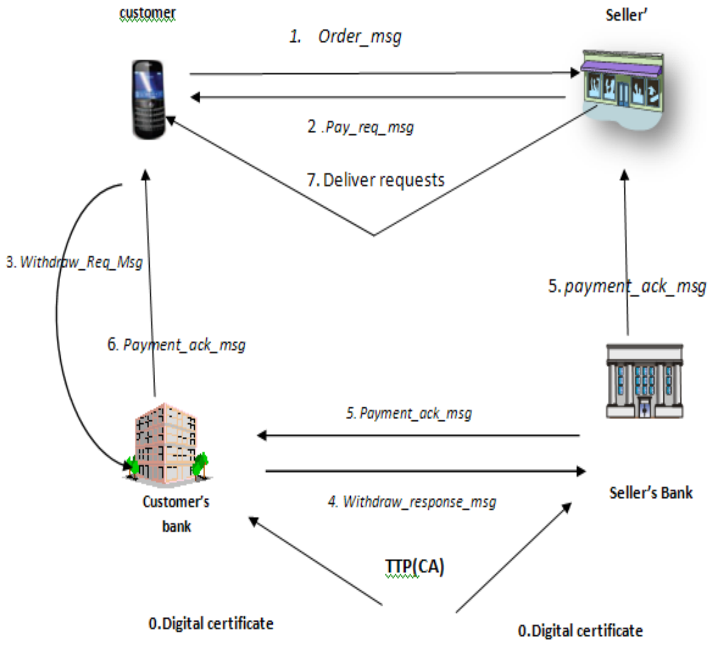

Figure 13: Main elements and their interactions

1

In proposed model

selects desired product. Then “product order” message (Order_msg) is generated and sent to seller by costumer. This message includes properties of selected product (name, identification number, number of products and etc)

2. When merchant received Order_msg from costumer, generates purchase bill for costumer and encrypts it using public key and sent them to the costumer. This message includes some details regarding price, currency and a description of selected product (to make sure that costumer has selected correctly) and time of request. Costumer checks product description and price field to ensure accuracy of his/her selection.

3. The costumer receives seller's message, decrypts it and generates Withdraw_Req_Msg message. Using this message the customer pays the desired price from his bank.

4. Receiving Withdraw_Req_Msg, the bank authenticates the costumer using private key and checks whether costumer's account has enough amount of money or not. Afterwards, it debits costumer accounts as much as requested price and generates “withdraw response” message. This message is signed by private key of the bank. In addition, it is encrypted using public key of seller's bank to avoid manipulation. The encrypted message is sent to seller's bank while a acknowledgement message is sent back to the costumer.

5. The seller's bank, decrypts received message, authenticates it, and checks accuracy of costumer's bank signature and expiration time of the message. Subsequently, the seller's account is credit and payment validation (acknowledgement) is sent to costumer and costumer's bank.

6. Costumer's bank sends a validation message to the costumer as soon as they received acknowledgement message from seller's bank.

7. The seller gives the requested product to the costumer, when he receives acknowledgement message.

6.1 The prominent security principals in our model are proved as follows:

Data integrity:
It guarantees that content of messages is not manipulated and the message is unchanged.
In this protocol, sender generates a summary of message (for example using SHA-1 algorithm) and encrypts it with its private key. Then it adds this summary to the message and sends it to the client. The client separates summary of message and decrypts it using public key of sender. Subsequently, the client compares derived summary to a summary which is generated by it. If these summaries match, the sender is the claimed one and data integrity is met.

Non-Repudiation
This characteristic prevents fake claim of a person who has not performed any transactions Signatures provide non-repudiation of performed operations Thus, in this protocol seller and costumer should sign the receipt in order to avoid denial of trade by merchant or costumer. This occurs in second step of protocol.

Authentication
Message authentication means proving consistency of receiver’s original identity. Authenticating person's identity is proving that the person is the same person who claims. In this protocol, authentication is provided by digital signature secure cryptography mechanism. Sender should sign the message with its private key. The client checks signature accuracy using sender's public key. If the signature is valid the sender is authenticated.

Confidentiality
It prevents unauthorized people to access sensitive payment information which may lead to abuse in future. In this protocol when the seller receives (Order_msg) message from costumer, sends the bill to costumer and encrypts it by their shared key. The costumer receives seller’s message, decrypts it and generates (Withdraw_Req_Msg) message to pay the price of product by its bank.

6.2 Efficiency and security considerations of the provided model are as follows:

1- Symmetric encryption is performed very rapidly in mobile devices and it is not time-consuming operation because only one key is used for encryption and decryption. Therefore, efficiency of the system will be suitable.AES method is suitable for micropayment.

2- Asymmetric encryption and digital signature are time-consuming in mobile devices and may affect efficiency of the system but its security is higher than the symmetric method because it uses two public and private keys for encryption and decryption.

3- Use of asymmetric encryption and digital signature is not suitable for micropayment but it is completely logical in micropayment because it needs high security [17].

4- Selection of ECC asymmetric encryption among asymmetric encryptions improves efficiency and speed of encryption calculation because digital signature is calculated and data is decrypted with very high speed in ECC method and its security is higher than that of other asymmetric algorithms [18].

5- Use of asymmetric encryption requires bank or two involved parties to use digital certificate. In case certificates are provided to bank and users, use of this encryption is very useful for authentication and can be easily applied in the system.

6- Digital signature also requires application of public key and more suitable non- repudiation, confidentiality and authentication by adding it to the proposed method.

7-Wherever signature was required, we used asymmetric encryption i.e. ECC method but symmetric encryption method, AES method was used in the messages which only shared key had been used.

7 - CONCLUSION

In this paper, four mobile payable business models were studied. For this purpose, participants used mobile payment business models and position of each beneficiary was determined in these models and risk and benefit of each participant were studied in these models and their positive and negative points were mentioned. Based on these studies and collaboration mode, because beneficiaries have almost equal risk and benefit and each one of the beneficiaries acts in his/her specialized field, it is better than other models. 10 payment methods in the world were currently studied and it was evident in this study that new methods have used collaboration model and wireless technology. In Table 1, 10 important methods along with business models applied in each one of the payment methods are shown.

TABEL 1: Ten important methods along with business models

Method of payment	Business model	Payment technology	Mode of payment	Disadvantages
BOUK[7],[6]	Operator-Centric	SMS	Micro payment	Non macro payment, Non –non repudiation
PayPal[8]	peer-to-peer	SMS,WAP	Micro & Macro payment	Authentication method dialog[4]
pay Box[8]	Bank- Centric	SMS	Macro payment	Non Authentication, Not suitable for micro payment
PayforIT[19],[8]	Operator-Centric	WAP	Micro payment	Non macro payment, High cost in application of WAP technology
Osaifu-Keitai[8]	Operator-Centric	RFID	Micro payment	Non macro payment, Non Payment remote
Google Wallet[9]	Collaboration	NFC	Micro & Macro payment	Non Payment remote
ISIS[10]	Collaboration	NFC	Micro & Macro payment	Non Payment remote
Square Wallet[20]	Collaboration	WAP	Micro & Macro payment	High cost in application of WAP technology
Jiring [11]	Operator-Centric	USSD	Micro mini payment	Non macro payment
Paypaad [12]	Collaboration	SMS,USSD	Micro payment	Non macro payment, Non Authentication
The proposed method	Collaboration	SMS	Micro & Macro payment	

In addition, one evaluation was done by Ms. Asghari et al [5]. in Iran based on which collaboration model was selected in the business model in Iran. In the proposed method, attempt was made to use collaboration model for business and transactions and micropayment and micropayment and also payment through SMS were provided through symmetric and asymmetric encryption of a secure payment which has all security specifications.

8-REFERENCES

[1] M.A. Tehrani, A.A Amidian, J. Muhammadi, and H.R. Rabiee , "A survey of system platforms for mobile payment", The 4th international conference on data management on E-commerce and E-Government (ICMECG),2010, PP.367-381.

[2] J. Ondrus, "A Tool Kit For A Better Understanding Of The Market". University of Lausanne2003

[3] F. Asghari, A.A Amidian, J. Muhammadi, H. R. Rabiee, "A Fuzzy ELECTRE Approach For Evaluating Mobile Payment Business Models" Management of e-Commerce and e-Government, International Conference ON PP.353-355, Oct, 2010.

[4] G. Ruijun, Y. Juan, W. Jiacai "Research on Mobile Payment Technology and Business Models in China under e-Commerce Environment" school of information science, Nanjing Audit University ,Nanjing,china,2010

[5] Smart Card Alliance, "Proximity Mobile Payments Business model Research Report", White Paper 2008.

[6] http://www.boku.com.

[7] Kuganeswari, Li Minyong, Nguyen Duc Duy, Nguyen Hung,Tan zeng Yi Adrian “USA Mobile payment Target company Baku”, Boku,2012.

[8] O. Santolalla, “MOBILE PAYMENT AS KEY FACTOR FOR MOBILE COMMERCE SUCCESS”, Helsinki University of Technology, 2008.

[9] O. Ghag, S. Hegde, “ A Comprehensive Study of Google Wallet as an NFC Application”, International Journal of Computer Applications, Volume 58– No.16, November 2012, PP. 37-42.

[10] “Towards a ubiquitous mobile payment solution: Exploring NFC mobile payment business models A case study on Google Wallet and ISIS” Master’s Thesis, Copenhagen Business School, 2012 International Journal of Engineering and Technology Volume 2 No. 9, September, 2012.

[11] http://www.jiring.ir.

[12] http://www.paypaad.ir.

[13] A. Jmenezes, P.C. van Oorschot, and S.A Vanstone. Handbook of Applied Cryptography, volume 6 Of Discrete Mathematics and Its Applications.CRC PRESS, 1996.

[14] C, stinson, Cryptography: Theory and practice .CRC Press, Boca Raton, Florida, second edition, 2002 .

[15] Cryptography for _mobile security. Mitchell, Chris J. Security for Mobility. Ed. Chris J Mitchell. IEE Press, 2004

[16] W. Stalling, Cryptography and Network Security: Principles and Practice (6th Edition), March 16, 2013.

[17] B.K. Alese, E.D. Philemon, S.O. Falaki, “ Comparative Analysis of Public-Key Encryption Schemes”.

[18] Dr. (Mrs). G.Padmavathi, Ms. B. Lavanya “Comparison of RSA-Threshold Cryptography and ECC-Threshold Cryptography for Small Mobile Adhoc Networks”, Int. J. Advanced Networking and Applications, 2012.

[19] Bearing point, “Mobile Money - The future of the payments market”, Bearingpoint White paper 2012.

[20] http://www.squareup.com/wallet