# New mobile payment protocol: Mobile pay center protocol (MPCP)

**Conference Paper** · April 2011

CITATION
1

READS
74

**3 authors**, including:

Mohammad Vahidalizadehdizaj
Pace University
**16** PUBLICATIONS **37** CITATIONS
SEE PROFILE

Reza Askari
University of Tehran
**72** PUBLICATIONS **390** CITATIONS
SEE PROFILE

# New mobile payment protocol: Mobile Pay Center Protocol (*MPCP*)

Mohammad Vahid Alizade
Computer Department
Payame Noor University
Tehran Iran
m_alizadeh@irib.ir

Reza Askari Moghaddam
Computer Department
Payame Noor University
Tehran Iran
askari@pnu.ac.ir

Samad Momenebellah
Deputy Secretary of TCI
Tehran Iran
smbfard@yahoo.com

***Abstract*—Growing of wireless networks and popularity of handheld devices such as Personal Digital Assistants (PDAs), Smart phones, mobile phones and wireless tablets represents an incredible opportunity to give power to mobile devices as a payment device. Unfortunately, some problems hindering the widespread acceptance of mobile payment for example: accountability properties, privacy protection, limitation of wireless networks and mobile devices. Recently, many public-key cryptography protocols are presented for mobile payment. However, limited capabilities of mobile devices and wireless networks make these protocols unsuitable for mobile network. Moreover, these protocols were designed to preserve traditional flow of payment data, which is vulnerable to attack and increase the user's risk. In this paper, we propose a private mobile payment protocol which is based on client centric model and works by employing symmetric key operations. The proposed mobile payment protocol not only minimizes the computational operations and communications between the engaging parties, but also achieves a completely privacy protection for the payer, avoid repudiating transaction from each of them and decrease risk of replay attacks.**

Keywords—Mobile Network Operator, Mobile Payment Protocol, repudiation, Encryption.

## I. INTRODUCTION

Mobile payment is any transaction that is executed via mobile devices, involves either direct or indirect exchange of fiscal values between parties. An interesting aspect about mobile payment is that mobile phone can be used as payment device for all types of payment situations. Optimists believe that the new world economy will witness the transition of mobile devices from a simple communication device to a payments mechanism [4, 9, 10, 12, and 17].

Nowadays, many mobile payment protocols were presented; however, most of them are based on PKI (Public Key Infrastructure) which are inefficiently applied to wireless networks. Some of them are keeping information about the engaging parties' credit card on their mobile devices or used it in the transaction without protection, which makes it vulnerable to attack. Most of these payment protocols were designed to preserve the traditional flow of payment data (Client - seller - seller's Bank), transaction which is carried out between client and seller. Therefore, it is vulnerable to attacks like transaction or balance modification by seller. Also it increases the user's risk which their credit or debit cards can be captured and used for accessing to customer's account illegally. Besides that, there is no notification to the client from the client's bank after the successful transfer. The user has to check his/her balance after logging on to his/her bank's website again [2,6,9,10,11,13,14,15,18, 19,20].

Additionally, design schemes of some mobile payment protocols are not worried about customer's privacy. Customer's privacy such as customer identity and transaction details are revealed not only to seller, but also to the payment gateway and the banks [3, 9, 10, 11, 14, 19].

In according to these problems, this paper's objective is to create a private mobile payment protocol that involves mobile network operator which is employing symmetric key operations. The rest of this paper is organized as follows. Some existing mobile payment protocols are briefly explained in section II. Section III is about details of proposed protocol. Section IV presents comparison on privacy protection and repudiating among several existing mobile payment protocol regarding to proposed protocol. Finally, section V concludes this research.

## II. RELATED WORK

In this section, existing payment protocols will be explored. These payment protocols composed of five principals, client (C), merchant (M), issuer (client's financial institution), acquire (merchant's financial institution) and payment gateway (PG) which are a medium between them and client and merchant. Three primitive payment transactions that have occurred within these payment protocols are as below:

1) Payment:

ISBN: 978-960-474-258-5

Client makes a payment
2) Subtraction:
Client requests issuers or payment gateway to debit his account.
3) Value Claim:
Merchant requests acquirer or payment gateway to credit transaction amount into his account [1, 21].

### *A. Secure Electronic Transaction (SET) Protocol*

This protocol is the most famous credit card payment protocol, which consists of request/response message pairs. All principals in SET payment protocol are required to acquire public key certificates. SET protocol's transaction consists of five steps, payment initialization, purchase order, authorization, and capture payment at the end card inquiry phase [9, 10, and 14].

### *B. Internet Key Protocol (iKP)*

iKP protocols are based on public key cryptography. They are different from each other with number of principals that posses their own public key pairs. This number is indicated by the name of the individual protocols for example: 1KP, 2KP and 3KP. The greater number of principals that hold public key pairs, the greater the level of security it provided. Principals of iKP are customer, merchant and payment gateway (acquirer) [2, 10, and 14].

### *C. KSL Payment Protocol*

SET payment protocol and iKP payment protocols are good payment protocols, which are executed successfully for e-commerce in fixed network like Internet. However, Tellez et al. and Kungpisdan et al. argued that both payment protocols are unsuitable for mobile payment transactions via wireless network because of theirs heavy computational operations and communications between them. Kungpisdan et al. enhanced SET and iKP payment protocols by reduce the number of principals who posses own public key pairs. All principals exclude client are required to have their own certificates. Therefore, client side's computation is reduced. KSL payment protocol consists of two subprotocols, which are merchant registration protocol and payment protocol. Both client and issuer share $Y_i$ before they starts making payment. Client is required to register with merchant and share symmetric key Xi with merchant [9, 11, and 19].

### *D. Tellez et al. Anonymous Payment Protocol*

Tellez et al. proposed anonymous payment protocols is based on client centric model. It employs a digital signature scheme with message recovery which was using self-certified public keys. It consists of five principals, which are client, merchant, acquirer, issuer and payment gateway. This payment protocol also consists of two-sub protocols, which are merchant registration protocol and payment protocol [19].

### *E. Kungpisdan et al.'s Mobile Payment Protocol*

Kungpisdan et al. suggested another secure account based mobile payment protocol to improve his KSL protocol. This payment protocol is employing symmetric key operations which require lower computation at all engaging parties. There are five principals involved in this protocol, which are client, merchant, issuer, acquirer and payment gateway. Kungpisdan et al.'s protocol includes two-sub protocols, which is merchant registration protocol and payment protocol. Before payment, client is required to register with merchant by running merchant registration protocol. After completion of registration protocol, client and merchant share a set of secret key Xi. The client also shared secret Yi with issuer and secret Zj is shared between merchant and payment gateway [9, 11].

## III. RECOMMENDED PROTOCOL

The suggested mobile payment protocol is presented in order to protect payer's privacy, resolve the problem of traditional flow of payment data, resolve repudiating problem and resolve replay attacks problem. The protocol is based on client centric model, where the payee does not have a direct communications with payer's MNO. In this protocol transaction flow is completely controlled by Payer. The proposed mobile payment protocol is composed of four principals, including payer, payee, payer's MNO and payee's MNO. The proposed protocol is working with set Xi, where i = 1,…,n and only is shared between payer and payer's MNO. Also set Yi is only shared between payee and payee's MNO. The following symbols are used in proposed mobile payment protocol:

TABLE I
NOTATIONS

| | |
|---|---|
| {payer, payee, payer's MNO, payee's MNO} | A set of engaging parties, which includes Payee, Payer, Payee's MNO and Payer's MNO |
| Paycenter | Time Stamp and Digital Sign center |
| $PN_P$ | Phone Number of Party *P* |
| $PIN_P$ | Party *P* selected this password identification number |
| $ID_P$ | Identity of Party *P*, which identifies Party *P* to *MNO*, computed as *IDP= PNP+ H(PNP, PINP)* |
| $AI_P$ | Account Information of Party *P*, which including credit limit for each transaction and type of account (postpaid or prepaid account) |
| $R_1$ | Random Number and timestamp generated by Payer act as Payer's pseudo-ID, which uniquely identifies Payer to Payee |
| $R_2$ | Random Number and timestamp generated to protect against replay attack |
| DATE | Date of payment execution |
| AMOUNT | Payment transaction amount and currency |
| DESC | Payment Description, which may includes |

ISBN: 978-960-474-258-5

| | |
|---|---|
| | delivery address, purchase order details and so on. Payer will include only the information that he/she wish to exposure to Payee. |
| TID | The Identity of transaction |
| $TID_{Req}$ | The request for *TID* |
| $PayeeID_{Req}$ | The request for payee identity. |
| {M}X | The message M encrypted with key X. |
| H(M) | The one way hash function of the message *M* |
| i | Used to identify the current session key of *Xi* and *Yi* |
| $K_{P-P}$ | The secret key shared between Payer's MNO and Payee's MNO. |
| Success/Fail | The status of registration, whether success or failed |
| Yes/No | The status of transaction, whether approved or rejected |
| Received | Payment receivable update status, which may includes the received payment amount |
| $Pr_P$ | Private key of party P |
| $Pu_P$ | Public key of party P |
| Ck | client key: a key that is necessary for decoding $X_i$ and $Y_i$ sets on client side |
| t | Current date and time |
| $ck_{Req}$ | Request for client key |

Suggested mobile payment protocol consists of two-sub protocols, which are registration protocol and payment protocol. Both payer and payee must register with their own mobile network operator (MNO) before any transaction could take place. Payer and payer's MNO generate session key, *K*1 by running Diffie-Hellman Key Agreement protocol. Then payer encrypts registration details such as account information, payer identity and phone number, and sends them to payer's MNO.

Payer -> Payer's MNO: $\{PN_{Payer}, ID_{Payer}, AI_{payer}\}K_1$

During the registration process, payer has to set his password identification number, PINpayer, for accessing his mobile wallet application. This implementation uses two factor authentication, that is an important principle for mobile devices access control. The two factor authentication is authenticating users in two steps to access mobile wallet system. First step is mobile device with mobile wallet application (something he has). Second step is password (something he knows only). Then the $ID_{payer}$, is computed by hashing the $PN_{Payer}$ and $PIN_{payer}$ [16] .

$ID_{Payer} = PN_{Payer} + H(PN_{Payer}, PIN_{Payer})$

Payer's MNO decodes message with shared session key, K1 to retrieve payer's information. Payer's MNO stores necessary information into their database. If registration process is successful, payer's MNO sends confirmation message to inform payer. Confirmation message is encrypted with the session key K1.

Payer's MNO -> Payer: $\{Success/ Failed\}K_1$

After registration, payer receives mobile wallet application through email or downloading from payer's MNO site. The mobile wallet application contains symmetric key generation and payment software. After successful installation, a set of symmetric key $X = \{X_1, X_2, \ldots, X_n\}$ is generated, store into payer's mobile devices and send to payer's MNO and payee must go through the similar registration process with his/her MNO. This enables his/her to receive payment from payer. The payee generates a set of symmetric key $Y = \{Y_1, Y_2, \ldots..Y_n\}$ with payee's MNO and store into his/her terminal and MNO's database. In this protocol if someone catch payment message, he or she can't use that message because all messages are encrypted and include timestamp generated numbers. If someone steals payment device, Stealer can access X or Y keys, therefore, stealer can decode the payment messages and use them for illegal payment. For solving this problem all X and Y keys are encrypted in client side with client key that is only available in P's MNO. Client for gaining client key does these steps:

First P request the key from P's MNO, second P's MNO give P client key and P use this key. Finally client delete client key. These steps are shown below. In addition, request encrypts with public key of P's MNO and reply encrypt with P's public key.

P -> P's MNO: $\{ PN_P, t, ck_{Req} \} Pu_{P's\ MNO}$

P's MNO -> P: $\{ ck \} Pu_P$

The proposed payment protocol consists of seven phases as illustrates in Fig. 1.

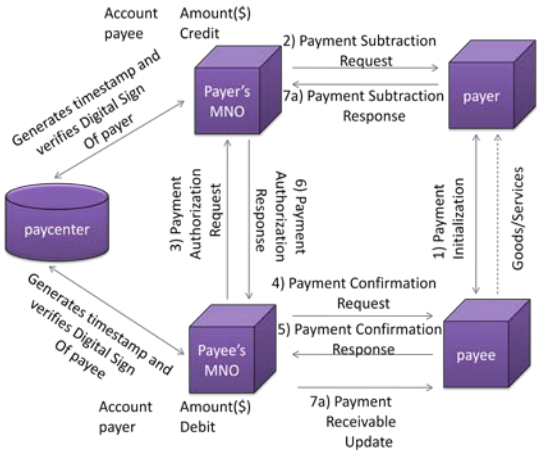


Fig. 1 Proposed mobile payment protocol

Phase 1 Payment Initialization:

Payer -> Payee: $R_1$ , $TID_{Req}$ , $PayeeID_{Req}$

Payee -> Payer: { $ID_{Payee}$, TID, $ID_{MNO}$ }K2

Phase 2 Payment Subtraction Request:

Payer -> Payer's MNO: { $ID_{Payee}$, $ID_{MNO}$, $R_1$, TID, AMOUNT, DATE, $R_2$, H ($ID_{Payee}$, $ID_{MNO}$, $R_1$, TID, AMOUNT, DATE, $R_2$ ), { $R_2$, DESC } $K_2$, { TID } $Pr_{Payer}$ } $X_i$, i, $ID_{Payer}$

Payer's MNO -> paycenter: H [ { $ID_{Payee}$, $ID_{MNO}$, $R_1$, TID, AMOUNT, DATE, $R_2$, H ($ID_{Payee}$, $ID_{MNO}$, $R_1$, TID, AMOUNT, DATE, $R_2$ ), { $R_2$, DESC } $K_2$, { TID } $Pr_{Payer}$ } $X_i$, i, $ID_{Payer}$]

Paycenter -> Payer's MNO: generates TimeStamp1 and verifies Payer's digital sign

Phase 3 Payment Authorization Request:

Payer's MNO -> Payee's MNO: $R_1$, $ID_{Payee}$, TID, AMOUNT, DATE, { $R_1$, DESC } $K_2$, { TID } $Pr_{Payer}$

Phase 4 Payment Confirmation Request:

Payee's MNO -> Payee: { $R_1$,TID, AMOUNT, DATE, { $R_1$, DESC } $K_2$, $R_2$, H ( R,TID, AMOUNT, DATE, { $R_1$, DESC } $K_2$, $R_2$ ), H ( $K_{P-P}$ ), { TID } $Pr_{Payer}$ } $Y_i$ , i

Phase 5 Payment Confirmation Response:

Payee -> Payee's MNO: { Yes, No, $R_2$, H ( $K_{P-P}$ ), H ( $R_1$, TID, AMOUNT, DATE, { $R_1$, DESC } $K_2$, $R_2$ ), { Yes/No, TID, AMOUNT, DATE } $K_2$, { { TID } $Pr_{Payer}$ } $Pr_{Payee}$ } $Y_{i+1}$

Phase 6 Payment Authorization Response:

Payee's MNO -> paycenter: H ({ Yes, No, $R_2$, H ( $K_{P-P}$ ), H ( $R_1$, TID, AMOUNT, DATE, { $R_1$, DESC } $K_2$, $R_2$ ), { Yes/No, TID, AMOUNT, DATE } $K_2$, { { TID } $Pr_{Payer}$ } $Pr_{Payee}$ } $Y_{i+1}$)

Paycenter -> Payee's MNO: generates TimeStamp2 and verifies Payee's digital sign

Payee's MNO -> Payer's MNO: Yes/No, TID, AMOUNT, DATE, { { TID } $Pr_{Payer}$ } $Pr_{Payee}$, { Yes/No, TID, AMOUNT, DATE } $K_2$

Phase 7 Payment Subtraction Response:

Payer's MNO -> Payer: { Yes/No, $R_2$, H ( $K_{P-P}$ ), H ( $ID_{Payee}$, $ID_{MNO}$, $R_1$, $R_2$, TID, AMOUNT, DATE ), { Yes/No, TID, AMOUNT, DATE } $K_2$, { { TID } $Pr_{Payer}$ } $Pr_{Payee}$ } $X_{i+1}$

Payee's MNO -> Payee: { Received, $R_2$, H ( $K_{P-P}$ ), H ( $R_1$, TID, AMOUNT, DATE, { $R_1$, DESC } $K_2$, $R_2$ ), { { TID } $Pr_{Payer}$ } $Pr_{Payee}$ } $Y_{i+1}$

If all the transaction processes completed successfully, payee will release or deliver the purchased goods or services to payer. To prevent replay of the secret key from payer and payee, both payer's MNO and payee's MNO make sure that the symmetric key Xi and Yi have not been used before processing the payment transaction. The MNO will keep a list of generated secret key by expiring used symmetric key Xi and Yi from the list. If symmetric key Xi and Yi were compromised, there must be revoked. Both payer and payee may receive an update notification from MNO when their key was expired. To update their secret key, they connect to their MNO to generate a new session key, $K_1$ by running Diffie-Hellman Agreement protocol. Then, offline generates a new set of secret key X and Y with a new session key $K_1$.

## IV. COMPARISON ON PRIVACY PROTECTION AND AVOID REPUDIATING BY DIGITAL SIGN

In this section, the proposed mobile payment protocol is comparing with five existing payment protocols from some aspects such as privacy protection and avoids repudiating with digital sign. Privacy protection includes identity privacy protection and transaction privacy transaction. Table II presents comparison of privacy protections and avoid repudiating by digital sign of proposed mobile payment protocol with five existing payment protocols.

TABLE II
COMPARISON ON PRIVACY PROTECTION AND AVOID REPUDIATING BY DIGITAL SIGN

| | SET | IKP | KSL | Tellez et al. | Kung-Pisdan et al. | MPCP |
|---|---|---|---|---|---|---|
| Identity Protection From Payee | No | No | no | yes | No | Yes |
| Identity Protection From Eavesdropp | Yes | Yes | yes | yes | Yes | Yes |
| Transaction Privacy Protection From Eavesdropp | Yes | Yes | yes | yes | Yes | Yes |
| Transaction Privacy Protection From TTP or Related Financial Institution | No | No | no | No | No | Yes |
| avoid repudiating transaction by Digital Sign | No | No | no | No | No | Yes |

ISBN: 978-960-474-258-5

Attainment of payer's privacy protection and avoid repudiating are two significant security issues of the proposed mobile payment. Note that, five existing mobile payment protocols and proposed mobile payment protocol are provide basic privacy protection for payer, that is protecting payer's identity and transaction details from eavesdropper. However, only Tellez et al. protocol and proposed protocol achieve payer's identity protection from payee. In Tellez et al. protocol, payer (client) only reveals temporary identity or called Client's Nickname to Payee (merchant) when sending the request for the transaction identity. The proposed mobile payment protocol protects payer's identity by sending a random generated number, $R_1$, to payee when requesting the transaction identity from payee. $R_1$ represents one-time payer's identity together with regarding transaction identity (TID) uniquely identifies payer to payee. This avoids revealing the real payer's identity ($ID_{Payer}$) to payee. Comparison results also show that only the proposed mobile payment protocol provides the transactions privacy from trusted third parties or related financial institution. Also only the proposed mobile payment protocol provides avoid repudiating from each one of them. The payment subtraction request that was sent from payer to payer's MNO consist of transaction details, which is {R, DESC} $K_1$. Note that, the transaction details for example which stock the payee interested in or delivery address is protected from both payer's MNO and payee's MNO. Also they are encrypted with payer and payee shared session key, $K_2$. Hence, only the corresponding payee can decrypts and retrieves the transaction details. Besides that, both payment subtraction request message and payment confirmation response message are applied a hash function before sending it to paycenter. This prevents revealing of any payment transaction details to paycenter. In the nutshell, after comparing the proposed protocol with five existing payment protocols, it is revealed that only the proposed mobile payment protocol satisfies all privacy protection and avoids repudiating requirements.

## V. CONCLUSION

So far many mobile payment protocols have been presented, but none of them has taken dominant position as yet. This paper suggests a private mobile payment protocol that involves MNO of Payer and Payee. This protocol is based on client centric model. In the proposed protocol one time Payer's identity, transaction details that are encrypted with the Payer and Payee's shared session key and digital sign of Payer and Payee can provide complete privacy protection for the payer and avoid repudiating transaction from each of them. The proposal method seems to improve mobile payment's security.

## REFERENCES


[1] Abad-Peiro J. L., Asokan N., Steiner M. & Waidner M, *Designing a generic payment service*, IBM System Research Journal, Vol.37(1), 1998, Pp. 72-88

[2] Bellare, M., Garay, J., Hauser, R., Herzberg, A., Steiner, M., Tsudik, G.,
Van Herreweghen, E., and Waidner, M, *Design,Implementation, and Deployment of the iKP Secure Electronic Payment system*, IEEE Journal of Selected Areas in Communications, 2000, pp. 611-627.

[3] C. Wang & H-f. Leung, "*A Private and Efficient Mobile Payment Protocol*", London: Springer-Verlag, LNAI, 2005, pp.1030-1035.

[4]E. Valcourt, J. Robert, & F. Beaulieu, (2005). "*Investigating mobile payment: supporting technologies, methods, and use.*" IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, (WiMob'2005), Aug. 2005 Page(s):29 - 36 Vol. 4 Digital Object Identifier 10.1109/WIMOB.2005.1512946

[5]*http://www.setco.org/set_specifications.html*

[6] J. Rao, P. Rohatgi, H. Scherzer and S. Tinguely [2002]. "*Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards.*" Proceedings of the 2002 IEEE Symposium on Security and Privacy.

[7] Jun Liu, Jianxin Liao, Xiaomin Zhu, "*A System Model and Protocol for Mobile Payment*", Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'05), 2005.
[8] Krueger, M, *"The future of M-Payments–business options and policy issues*", Seville. Spain, 2001.

[9] Kungpisdan, S., Srinivasan, B., and Phu Dung, L, "*Lightweight Mobile Credit-Card Payment Protocol*", Berlin Heidelberg: Springer –Verlag, 2003a, pp. 295-308.

[10] Kungpisdan, S., Srinivasan, B., and Phu Dung, L., "*A Practical Framework for MobileSET Payment*", Proceedings of International ESociety Conference, 2003b, pp. 321-328.

[11] Kungpisdan S., Srinivasan B., and Phu Dung Le, "*A Secure Accountbased Mobile Payment Protocol*", Proceedings of the International Conference on Information Technology: Coding and Computing, Vol. 1, Las Vegas, USA, 2004a, pp. 35-39.

[12] M. Ding and C. Unnithan, "*Mobile Payments (mPayments) –An Exploratory Study of Emerging Issues and Future Trends"*, Deakin University, 2002.

[13] Mobile Payment Forum of India *http://www.mpf.org.in/*

[14] Mohony D.O., Peirce M. and Tewari Histesh, *"Electronic Payment Systems for E-Commerce*", Artech House, United States of America, 2001.

[15] M. Rieback and A. Tanenbaum [2006]. "*Is your cat infected with a computer virus?"* 4th Annual IEEE International conference on Pervasive Computing and Communications.

[16] Panko R. R, Corporate "*Computer and Network Security*", Prentice Hall, Upper Saddle River, New Jersey, 2004.

[17] Pousttchi, K, "*Conditions for Acceptance and Usage of Mobile Payment Procedures*", Proceedings of the M-Business Conference, 2003.

[18] S. Karnouskos & F. Fokus (2004). *"Mobile Payment: a journey through existing procedures and standardization initiatives*", IEEE Communications Surveys and Tutorials. 6(4) 44-66.

[19] Tellez J. & Sierra J, "*Anonymous Payment in a Client Centric Model for Digital Ecosystem*", IEEE DEST, 2007, pp. 422-427.

[20] Tiwari, A., Sanyal, S., Abraham, A., Knapskog, J. S. & Sanyal, S., "*A Multi-factor Security Protocol for Wireless Payment-Secure Web Authentication Using Mobile Devices*", IADIS International Conference Applied Computing, pp.160-167, 2007.

[21] X. Zheng & D.Chen (2003). "*Study of mobile payments systems"*. IEEE International Conference on E-Commerce, CEC 2003, June 2003 Page(s):24 – 27 Digital Object Identifier 10.1109/COEC.2003.1210227

ISBN: 978-960-474-258-5 