Wireless Pers Commun (2015) 85:289–304
DOI 10.1007/s11277-015-2738-y

P2PM-pay: Person to Person Mobile Payment Scheme Controlled by Expiration Date

Rafael Martínez-Peláez[1] · Homero Toral-Cruz[2] · Joel Ruiz[3] · Pablo Velarde-Alvarado[4]

Published online: 22 May 2015

Abstract In this paper, we propose P2PM-pay scheme which provides two key points. The first key point is related with the mobile cash. In P2PM-pay scheme, the mobile cash is controlled by the expiration date. The expiration date is embedded into the mobile cash by partial blind signature during the withdrawal date, and the bank does not hold information about the operation. Moreover, we have considered the effective date and deposit date for administrative purposes. The effective date is when customers use their mobile cash to pay for products, and the deposit date is when merchants receive the funds in their bank account. The other key point is related with the authentication process among participants. Although P2PM-pay uses WTLS protocol, we propose a wireless public key infrastructure with an efficient certificate path validation. Furthermore, the design of the proposed scheme achieves successfully the security requirements described in previous works. Consequently, P2PM-pay is secure against well-known attacks and efficient in terms of processing time.

Keywords Date attachment · Hash functions · Micropayments · Mobile cash · Mobile commerce · Partial blind signature

✉ Rafael Martínez-Peláez
rafael.pelaez@uacj.mx

Homero Toral-Cruz
htoral@uqroo.edu.mx

Joel Ruiz
joel.ruiz@ues.mx

Pablo Velarde-Alvarado
pvelarde@uan.edu.mx

[1] Department of Electrical Engineering and Computing, Autonomous University of Ciudad Juarez, Ciudad Juarez, Mexico

[2] Department of Science and Engineering, University of Quintana Roo, Quintana Roo, Mexico

[3] Department of Software Engineering, Sonora State University, Navojoa, Mexico

[4] Area of Basic Sciences and Engineering, Autonomous University of Nayarit, Tepic, Mexico

1 Introduction

The advances of wireless network technologies and mobile devices' computational power have created a new technology to pay for products and services in any place and at any time you require. This new technology is called mobile payment or m-payment, and it is a key component for increasing confidence in mobile commerce [1, 2]. Mobile payments can be defined as the process of exchanging financial value between two entities using mobile devices to pay for a product or services [3].

Mobile payment schemes proposed in the literature [4–23] can be classified in three types [24]. The first type of schemes is based on credit/debit cards. These types of schemes require high computational power to verify the authenticity and integrity of payment information because many cryptographic operations are computed. For example, the schemes proposed in [5, 10, 14, 15, 18, 22, 23] compute many public key cryptography operations to validate the digital signature. The second type of schemes is based on direct mobile phone bill. These types of schemes require a connection with the background infrastructure, such as Global System for Mobile communication (GSM), Universal Mobile Telecommunications System (3G) or Long-Term Evolution (4G), to charge the total amount of the purchase in the users' mobile phone bill. However, these types of schemes do not provide privacy because the mobile network operator or carrier knows the users' transaction. For example, the scheme proposed in [9, 21] requires a Short Message Service (SMS) in order to the mobile network operator or carrier accept the transaction. The last type of schemes is based on mobile cash. The mobile cash is the digital representation of the paper cash, and it is issued and controlled by a trusted third party such as bank. Mobile payment schemes based on mobile cash [4, 6–8, 12, 13, 17] provide strong privacy with low computational power, and they are suitable for micropayments. In this paper, we focus on mobile payment schemes based on mobile cash.

A mobile payment scheme based on mobile cash contains three participants (customer, merchant and bank) and consists of four phases (withdrawal, purchase, payment and deposit) [25]. The main security requirements for such schemes are [26, 27]: confidentiality, mutual authentication, integrity, and anonymity. Moreover, in terms of performance the schemes should require low computational power, low storage capacity and low administrative cost. Although many proposals of mobile cash or electronic cash can be found in the literature, few of them [28–33] prevent the bank's database grows very fast. However, these schemes do not take into consideration the authentication process among participants.

In order to contribute in the field of mobile commerce, we propose a person-to-person mobile payment scheme (P2PM-pay) based on mobile cash. The mobile cash is controlled by expiration date preventing the bank's database grows very fast. The mobile cash's design is inspired in the partially blinded signature scheme introduced in [34]. Moreover, the scheme considers the effective date and deposit date of the mobile cash as security parameters. Furthermore, the public key infrastructure is efficient in terms of execution time because the certificate path validation process have been improved in [35, 36].

The paper is organized as follows. In Sect. 2, we explain the architecture of P2PM-pay scheme. The mobile payment scheme is proposed in Sect. 3. We evaluate the proposed scheme in Sect. 4. Finally, conclusions are given in Sect. 5.

2 P2PM-pay: Architecture

In this section, we give an overview of technologies used in the design of P2PM-pay scheme.

2.1 PKI-enabled SIM Card

A PKI-enabled SIM card [15] is a SIM card integrated with the Wireless Identity Module (WIM) making possible the use of certificates. PKI-enabled SIM cards are suitable for computing a public key algorithm such as RSA, and it takes advantage of security mechanism. Technically, it allows the implementation of Wireless Transport Layer Security (WTLS) protocol [37] to provide end to end security communication in mobile devices. The PKI-enabled SIM card can store private/public key pairs.

2.2 Bluetooth

Bluetooth [38] is a wireless technology to interconnect mobile devices with each other or with other devices via point-to-point or point-to-multipoint links. This technology transfers voice, data and video in real time. The transmission area is omni-directional and its transfer rate is 1 Mbps. The maximum distance between the data origin (source) and receiver is around 10 m. Bluetooth technology transmits and receives on frequency band 2.45 GHz. Bluetooth technology is a key element in mobile commerce because it enables mobile devices to pay for products. According with results presented in [3], Bluetooth is a valid option for wireless communication in mobile payment schemes.

In our scheme, the communication is via Bluetooth between customers-merchants and customers-loading centre (e.g., kiosk or ATM machine).

2.3 Wireless Public Key Infrastructure (WPKI)

We use WPKI certificates and WTLS protocol [37] to provide mutual authentication and to establish a secure channel among all the mobile users in an open network [39], where the transmitted and received signals travel over the air. The authentication process using certificates requires that the customer and the merchant start WTLS protocol. Authentication using certificates implies the validation of certification paths [40].

A certification path is a chain of Public Key Certificates (PKCs) through which a user can obtain the public key of another one. The primary goal of a path validation is verifying the binding between the entity and his/her public key. Then the verifier must check the signature and validity of each certificate in the path to trust in the public key of the target entity. Validity of certificates implies to verify the expiration date of each certificate and their revocation status. A trust anchor is the Certification Authority (CA) verification key used by the client application as the starting point for all certificate validation. Thus, the path is traced from the verifier's trust anchor to the CA key required to validate the target entity's certificate. So, the certification path length is equal to the number of certificates in the plus one: a CA certificate per each intermediary CA and the target entity's certificate. Since, the verifier knows and trusts the public key of his/her trust anchor, the trust anchor's certificate is not included in the path.

Certificate revocation is the mechanism under which an issuer can revoke the binding between an entity and a public key before the expiration of the corresponding certificate. A certificate can be revoked because of the loss or compromise of the associated private key, a change in the relationship with the issuer, etc. The standard certificate revocation mechanisms are Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP).

Based on previous research [36, 41, 42], we design a WPKI in where the mobile devices require low computational power to perform the mutual-authentication process using

WTLS. Figure 1 describes the structure of the WPKI. The structure defined has the following characteristics:

1. A governmental organization such as national bank or department of the treasure is the Root Certification Authority (RCA), and it is responsible for issuing certificates to banks.
2. Banks participate as Certification Authority (CA), and they are responsible for issuing certificates to customers and merchants.
3. The size of certificates for RCA and CAs are 473 bytes [40].
4. The size of certificates for customers and merchants are 425 bytes [40].
5. The certification path length is $L = 1$, when the customer and merchant belong to the same CA, and $L = 2$, when the customer and merchant belong to different CAs.
6. The verifier use OCSP to verify the revocation status of certificates.

3 P2PM-pay

3.1 Participants

The mobile payment architecture includes the following entities:

- *Customer*-person who owns a mobile device to pay for products.
- *Merchant*-person or vendor machine that accepts mobile payments.
- *Bank*-entity that dispenses and validates mobile cash, and deposits funds in the merchant's bank account.

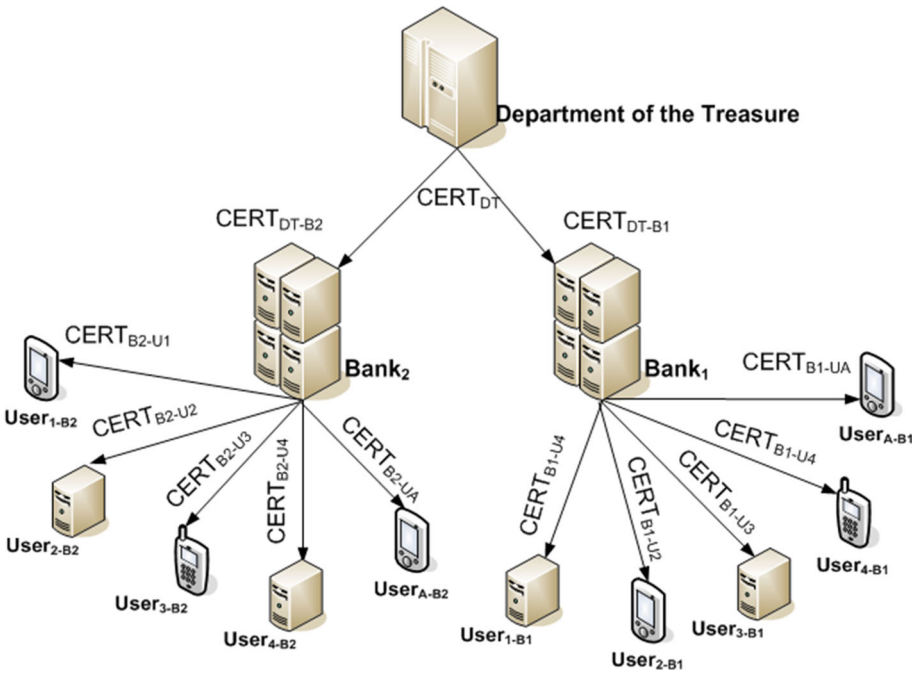

Fig. 1 Structure of the WPKI

The notations used in this paper are given in Table 1.

3.2 P2PM-pay Protocol

The proposed mobile payment scheme consists of the following phases: enrolment process, withdrawal process, payment process, and deposit process. Figure 2 describes the interaction among the participants, and Fig. 3 shows the transmitted messages among the customer, merchant and bank during the execution of the proposed scheme.

3.2.1 Enrolment

In this phase, the customer and merchant must be registered by the bank in order to get the security parameters and be part of the system. The security parameters include a pseudonym identity and certificate. The process is as follows:

Step 1 Customer and merchant disclose their personal information to the bank. Then the bank verifies the information. If the information is valid, the bank creates a bank account number BAN_A for each one. Finally, the customer and merchant must deposit w euros, dollars or pesos in their bank account

Step 2 The bank concatenates and hashes the user's real name and identity number of SIM card using a one-way hash function to get the pseudonym identity $(PI = H(RN \parallel ID_{SIM}))$

Step 3 The bank computes the public (d_C, p_C, q_C) and private (e_C, n_C) key pairs

Step 4 The bank stores the users' RSA public key pairs and certificate, and its public key in the PKI-enabled SIM card

Step 5 The bank publishes a one-way hash function $H()$

Table 1 Protocol notation

Notation	Meaning
$CERT_{BB\text{-}UA}$	Certificate of user A issued by bank B
BAN_A	Bank account number of participant A
PI_A	Pseudonym identity of participant A
$AEPO$	Agreement of electronic payment order
$a \parallel b$	Concatenation of value a and b
(e_A, n_A), (d_A, p_A, q_A)	Public and private keys of participant A
R	Blind factor
$H()$	One-way hash function
$H^n()$	n Times one-way hash function
$\Delta_1, \Delta_2, \Delta_3$	Expiration date, effective date and deposit date
S	Seed of the hash chain
i	Units of mobile cash
y_i	Start point of the mobile cash
y_{TP}	Total payment
y_x	Spend x units of mobile cash

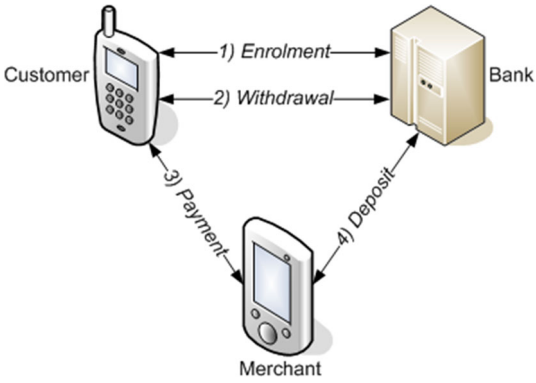

Fig. 2 Mobile payment scenario

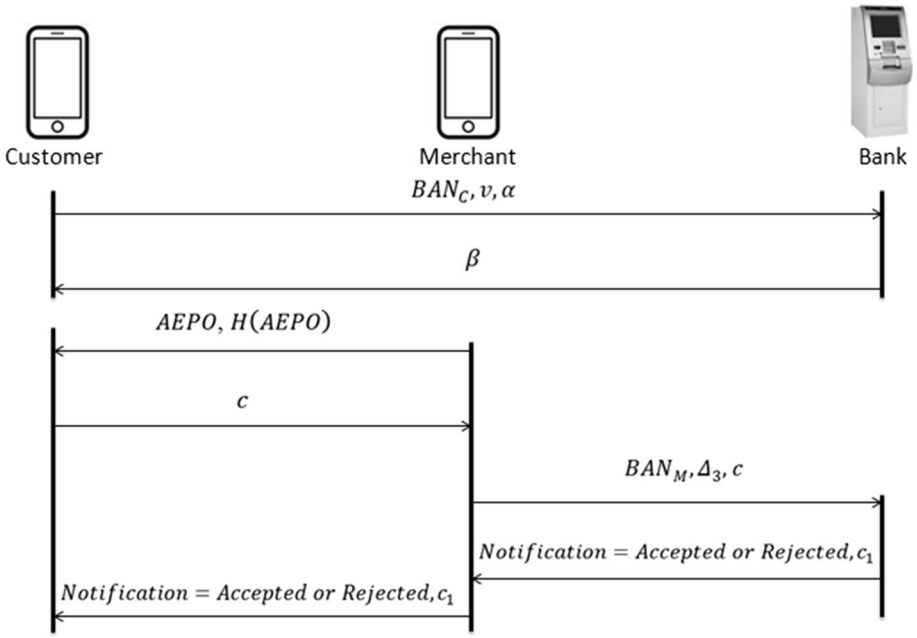

Fig. 3 Messages exchange during the execution of the proposed scheme

3.2.2 Withdrawal

When customers want to obtain mobile cash, they need to establish a communication with an authorized loading centre such as kiosk or ATM machine. The communication between mobile devices and loading centre is via Bluetooth. The process is as follows:

Step 1 The customers and authorized loading centre verify the identity of each other by means of WTLS protocol [40]. After the WTLS protocol finish, customers and authorized loading centre know the session key and cryptographic algorithm to encrypt messages

Step 2 The customers carry out the following process:

1. CREATE $v = \Delta_1 \parallel i$
2. CHOOSE RANDOMLY *S and R in* Z_n^*
3. COMPUTE $y_i = H^i(S)$
4. COMPUTE $h_1 = H(y_i)$
5. BLIND h_1 COMPUTING $\propto \equiv h_1 \times R^{e_C * v} (\mathrm{mod} n_C)$
6. SEND BAN_C, v, α to *Bank*

Step 3 After the bank receives the message, it carries out the following process

1. VERIFIES *format of v*
2. VERIFIES $i \leq$ *balance account*
3. If both verifications are approved, the bank deducts w euros, dollars or pesos from customer's bank account and stores the operation in its transactional history
4. SIGNS α COMPUTING $\beta \equiv \alpha^{d_B * v} (\mathrm{mod} n_B)$
5. SENDS β to *Customers*

Finally, customers compute $\varepsilon \equiv \beta R^{d_C * v} (\mathrm{mod} n_C)$ and get their mobile cash (y_i, ε, v).

3.2.3 Payment

When customers want to pay for a product using mobile cash, they and merchants perform the following steps:

Step 1 Perform the cryptographic operations required in WTLS protocol. After the protocol finalized, each participant can encrypt and decrypt messages

Step 2 Merchants compute and sends the *AEPO* to customers. The process is as follows:

1. COMPUTE the *AEPO*. *The AEPO includes the identification of the product, price, quantity, pseudonym identity of the merchant, transaction date, identification of the transaction, and total payment*
2. COMPUTE *H*(*AEPO*)
3. SEND *AEPO*, *H*(*AEPO*) to *Customers*

Step 3 After customers receive the message, they perform the following process

1. VERIFY *format of AEPO*
2. STORE *the total payment information into the variable* y_{TP}
3. COMPUTE $y_x = y_i - y_{TP}$ *such that* $H^{i-TP}(S) = y_x$
4. COMPUTE $h_2 = H(\Delta_2 \parallel (y_i, \varepsilon, v) \parallel y_x \parallel y_{TP})$
5. ENCRYPT $c \equiv (\Delta_2 \parallel (y_i, \varepsilon, v) \parallel y_x \parallel y_{TP} \parallel h_2)^{e_B} (\mathrm{mod}_{n_B})$
6. SEND c to *Merchant*

3.2.4 Deposit

In this phase, the bank deposits the funds in merchant's bank account (BAN_M). The merchant and the bank must perform the following steps:

Step 1 After the merchants receive the payment information, they carry out the following process

1. SEND BAN_M, Δ_3, c to *Bank*

Step 2 After the bank receive the deposit requirement, it performs the following process,

1. DECRYPTS $\Delta_2 \parallel (y_i, \varepsilon, v) \parallel y_x \parallel y_{TP} \parallel h_2 \equiv (c)^{d_B} (\mathrm{mod}_{n_B})$
2. COMPUTES $h_2^* = H(\Delta_2 \parallel (y_i, \varepsilon, v) \parallel y_x \parallel y_{TP})$
3. VERIFIES $h_{2=}^{*?} h_2$
4. VERIFIES *format of v*
5. CHECKS $\Delta_2 \leq \Delta_3 \leq \Delta_1$
6. VERIFIES ε COMPUTING $\varepsilon^{e_B v} \equiv H(y_i)^{d_B v} (\mathrm{mod} n_B)$
7. VERIFIES $y_{TP} \leq i$
8. SEARCHES *vandy*$_i$ *to prevent double spending*
9. COMPUTES $y_i = H^{TP}(y_x)$
10. DEDUCTS $y_i^{'} = i - TP$
11. DEPOSITS y_{TP} *into* BAN_M
12. COMPUTES
    $h_3 = H\left(y_i^{'}\right),\ \varepsilon' \equiv h_3^{d_B v} (\mathrm{mod} n_B)$ *and* $c_1 \equiv (Notification, h_3, \varepsilon')^{d_B} (\mathrm{mod} n_B)$
13. STORES v and y_i
14. SENDS *Notification* = *Accepted or* Re*jected*, c_1 to *Merchant*

Step 3 After the merchants know the status of the deposit phase, they deliver the product and

1. SEND *Notification* = *Accepted or Rejected*, c_1 to *Customer*

Step 4 After the customers receive the response message, they know the status of the transaction and have the remainder of mobile cash. The process is as follows

1. DECRYPT *Notification*, h_3, $\varepsilon' \equiv (c_1)^{e_B} (\mathrm{mod} n_B)$

The customers get their remainder of mobile cash *by means of* $y_i^{'}$, ε', v.

4 Evaluation

In this section, we analyze the performance, security and usability of the proposed scheme. Moreover, we compare P2PM-pay with related works in terms of performance, security and usability.

4.1 Performance Evaluation

In this sub-section, we present a performance analysis in terms of cryptographic operations executed by each participant in P2PM-pay. By means of this evaluation, we want to know the number of cryptographic operations computed by each participant. Moreover, we want

Table 2 Computational cost in P2PM-pay

Phase	Participant	Hash function	RSA encrypt	RSA decrypt	Symmetric encrypt/decrypt
Withdrawal	Customer	1	1	1	2
	Merchant	0	0	0	0
	Bank	0	1	0	2
Payment	Customer	1	1	0	2
	Merchant	1	0	0	2
	Bank	0	0	0	0
Deposit	Customer	0	0	1	1
	Merchant	0	0	0	3
	Bank	2	2	2	2

to know the size of each message exchanged during each phase. We assume the use of SHA-1 [43] as hash function and each data size is 6 bytes.

The number of cryptographic operations computed by each participant is presented in Table 2. The cryptographic operations computed during the WTLS protocol are not considered in this evaluation. We suggest to readers review related works [36, 41, 44–48]. Table 3 shows the number and size of messages exchanged by each participant during the different phases.

Table 2 and Table 3 show the performance of the proposed scheme. The number of cryptographic operations is low for merchants because they must compute several transactions every day. On the other hand, customers compute many operations during the withdrawal phase, but in the payment and deposit phases they compute low cryptographic operations. The bank computes more cryptographic operations because it verifies the validity and legacy of mobile cash.

In order to know the energy cost of cryptographic operations, we computed the energy cost of each cryptographic operation computed by the participant during the P2PM-pay scheme. We assume the energy consumption presented in [23]. Figure 4 shows the differences among three symmetric algorithms and provides an overview of their implementation. Moreover, Fig. 5 shows the energy consumption of RSA algorithm.

Table 3 Messages exchange between participants

Phase	Participant	Messages send	Size in bits
Withdrawal	Customer	1	$3400 + 96 + 1024 = 4520$
	Merchant	0	0
	Bank	1	1024
Payment	Customer	1	1024
	Merchant	1	608
	Bank	0	0
Deposit	Customer	0	0
	Merchant	2	$80 + 48 + 1024 = 1152$
			$16 + 1024 = 1040$
	Bank	1	$16 + 1024 = 1040$

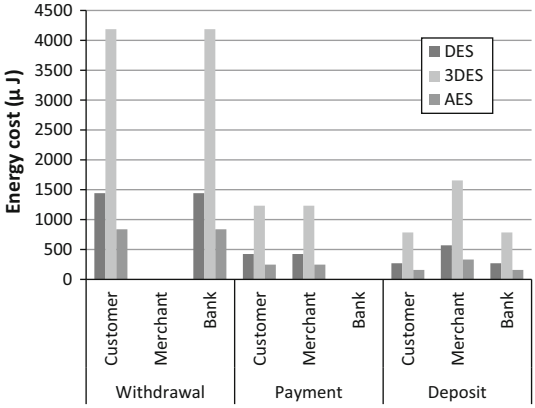

Fig. 4 Energy cost of symmetric encryption/decryption using DES, 3DES and AES

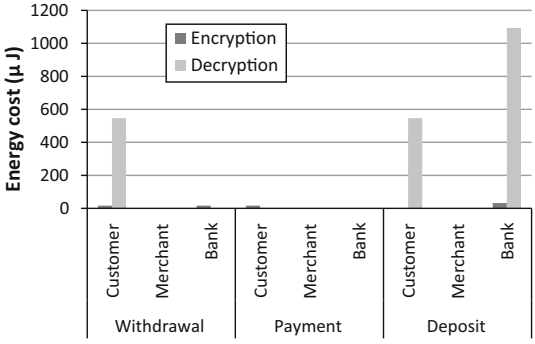

Fig. 5 Energy cost of encryption/decryption using RSA algorithm

According with the results presented in Figs. 4 and 5, P2PM-pay is suitable for mobile devices because the number of cryptographic operations does not required high energy cost. The evaluation in terms of energy cost demonstrated that the cryptographic operations carried out by merchants do not required high consumption of energy. This point is very important because merchants can compute several times the protocol during every day, so the energy cost must be low. Although customers' devices compute four cryptographic operations during the payment phase, the energy cost is very low. Because the bank has more resources than customers and merchants, it computes more cryptographic operations requiring more energy cost. In brief, the energy cost is available for mobile devices, and it is not a limitation.

4.2 Security Analysis

P2PM-pay offers robust security because the scheme provides mutual authentication, payment authorization, confidentiality, and integrity.

Authentication: Mobile payment schemes must offer the option to authenticate each participate to prevent the participation of illegal participant.

- Mutual authentication. Customers and merchants use digital certificates to authenticate each other by means of WTLS protocol.

Integrity: Mobile payment systems must guarantee that sensitive information have not been modified by an attacker.

- Protection against eavesdroppers. The communication among participants is secure against attackers because the information is encrypted using the secret master key computed during the WTLS protocol.
- Protection against physical exposure. The PKI-enabled SIM card protects sensitive information (e.g., private key, seed, blind factor) from unauthorized access.
- Protection of payment information. By means of one-way hash function participants of the transaction can detect any modification in the payment information.

Privacy: Mobile payment systems must avoid eavesdroppers have access to the sensitive information.

- No disclosure of real name. Customers and merchants do not reveal their real name.
- No disclosure of personal information in the payment phase. Customers do not share private information with merchants.
- No disclosure of customers' purchase. The bank does not know the products purchased by customers.

Non-repudiation: Mobile payment systems should avoid refuting operations.

- Prevent the rejection of the withdrawal. Customers are authenticated by the bank through their certificate. In addition, the bank stores the operation in the transactional history.
- Prevent the rejection of the payment. The bank verifies the authenticity of the mobile cash before the merchant deliver the product.

Fraud detection: Mobile payment systems must detect any attempt of fraud.

- Detection of double spending attack. The bank verifies the mobile cash in each transaction.
- Detection of forgery attack. The seed of hash chain is known only by the consumer, nobody can create two equal y_i.
- Detection of illegal user. When a customer starts a commercial transaction with a merchant, they must exchange certificates and each participant can determine whether the certificate is valid or not.

4.3 Usability

In this sub-section, we evaluate P2PM-pay from the following factors [49]: cost, convenience and commercial scenario. Table 4 summarizes the common factors that influence in the success of mobile payment systems.

P2PM-pay scheme is feasible for person-to-person and real point of sale scenarios because the computational cost, energy cost and messages exchange for each participant are very low. Moreover, the communication among entities does not require extra cost. Furthermore, customers and merchants can establish a secure communication wherever and whenever they want. Finally, the mobile cash's validation is carry out by the bank. This type of mobile payment is useful for small stores.

Table 4 Evaluation criteria for successful mobile payments

Parameters	P2PM-pay
Scenario	
Real POS	Yes
Virtual POS	No
P2P	Yes
Cost	
Transaction fees	No, customers use short link wireless technology
Convenience	
Permanent Connectivity	No, customers does not require permanent connectivity
Rounds in withdrawal phase	2
Rounds in payment phase	2
Withdraw for each payment	No
Fast processing	Hashes and partial blind signature operations
Verification process	Online

Table 5 Comparisons between P2PM-pay and others

Characteristic	[8]	[13]	[28]	[29]	[30]	[34]	P2PM-pay
Effective date	No	No	No	Yes	Yes	No	Yes
Expiration date	Yes	No	No	No	No	Yes	Yes
Deposit date	Yes	Yes	No	No	No	No	Yes

4.4 Comparisons

We compare P2PM-pay with other mobile payment schemes based on mobile cash [8, 13, 28–30, 34]. We summarize the functionality of our proposal with others in Table 5.

The first characteristic of comparison is the effective date which represents the date of payment. This characteristic is incorporated in [29], [30] and P2PM-pay. By means of this characteristic customers and banks controls the spending of mobile cash. The second characteristic is the expiration date which represents the date of validity of each mobile cash. The expiration date is used by the bank to delete mobile cash with invalid date. This characteristic is included in [8], [34] and P2PM-pay. The third characteristic is the deposit date which represents the date when the merchants receive the payment in their bank account. This characteristic is included in [8], [13] and P2PM-pay. At this point, P2PM-pay is the unique scheme which includes the three characteristics related with the date.

In terms of security, P2PM-pay provides anonymity, integrity, mutual authentication, non-repudiation, and privacy as explained in [26, 27]. As a consequence, the scheme is secure against eavesdropping and malicious users. Security is the main requirement for mobile payments because the information exchange among participants is money, and participants do not want to lose money. The number of cryptographic operations is very similar to related works [8, 13, 23, 30–32] which means that P2PM-pay is efficient in terms of processing time.

5 Conclusions

In this paper, we have proposed a practical mobile payment scheme for person-to-person scenario which contributes in two aspects. First, the mobile cash prevents the bank's database grows uncontrolled by means of the expiration date providing better performance during the verification process. The expiration date is added to the mobile cash using concatenation operation and partial blind signature scheme introduced by Abe and Fujisaki. The second aspect is related with the wireless public key infrastructure (WPKI). In P2PM-pay the WPKI provides an efficient certification path validation reducing the computational cost and making feasible the adoption of digital certificates. In brief, the computational cost to compute the mobile cash is low and easily applied to mobile devices because it is based on hash chain and one digital signature operation, and the adoption of digital certificates is feasible under the WPKI proposed.

From security point of view, P2PM-pay achieves the essential security requirements. The scheme provides anonymity to customers during the withdrawal and payment phase. Although customers and merchants exchange digital certificates, their identities are not exposed. The payment information does not contain data about the product; as a consequence, the bank does not obtain information about the customers' habits. The communication among participants is encrypted avoiding eavesdropping.

Acknowledgments We thank the anonymous reviewers for their constructive comments which helped us improve the presentation and quality of this paper. Moreover, we would like to thank Leslie Cedeño and Monica Padilla for their support. This work was partially sponsored by SEP-CONACyT CB-2011-01 Project 167859.

References

1. Leavitt, N. (2010). Payment applications make e-commerce mobile. *Computer, 43*(12), 19–22.
2. To, W.-M., & Lai, S.-L. (2014). Mobile banking and payment in China. *IT Professional, 16*(3), 22–27.
3. Martínez-Peláez, R., et al. (2008). Performance analysis of mobile payment protocols over the Bluetooth wireless network. In *6th CollECTeR Iberoamérica*.
4. Tracz, R., & Wrona, K. (2001). Fair electronic cash withdrawal and change return for wireless networks. In *ACM international workshop on mobile commerce*.
5. Kungpisdan, S., Srinivasan, B., & Le, P.D. (2003). Lightweight mobile credit-card payment protocol. In *4th International conference on cryptology in India, progress in cryptology-Indocrypt'03*. Springer-Verlag.
6. Abbadasari, R., Mukkamala, R., & Kumari, V. (2004). Mobicoin: Digital cash for m-commerce. In *International conference on distributed computing and internet technology*. Springer-Verlag.
7. Hu, Z.Y., et al. (2004). Anonymous micropayments authentication (AMA) in mobile data network. In *23rd Annual joint conference of the IEEE computer and communications societies*. IEEE Press.
8. Song, R., & Korba, L. (2004). How to make E-cash with non-repudiation and anonymity. In *International conference on information technology: Coding and computing*. IEEE Press.
9. Fong, S., & Lai, E. (2005). Mobile mini-payment scheme using sms-credit. In *Computational science and its applications*. Springer-Verlag.
10. Lee, B.-K., Lee, T.-C., & Yang, S.-H. (2005). A MEP (mobile electronic payment) and IntCA protocol design. In *1st International conference on high performance computing and communications*. Springer-Verlag.
11. Téllez, J., et al. (2006). Anonymous payment in a kiosk centric model using digital signature scheme with message recovery and low computational power device. *Journal of Theoretical and Applied Electronic Commerce Research, 1*(2), 1–11.
12. Zhang, L., Yin, J. P. & Zhan, Y. B. (2006). An anonymous digital cash and fair payment protocol utilizing smart card in mobile environments. In *5th International conference on grid and cooperative computing workshops*.

13. Hwang, R. J., Shiau, S. H., & Jan, D. F. (2007). A new mobile payment scheme for roaming services. *Electronic Commerce Research and Applications, 6*(2), 184–191.
14. Téllez, J., & Sierra, J. (2007). A secure payment protocol for restrictred connectivity scenarios in m-commerce. In *EC-WEB*. Springer-Verlag.
15. Hassinen, M., Hyppönen, K., & Trichina, E. (2008). Utilizing national public-key infrastructure in mobile payment systems. *Electronic Commerce Research and Applications, 7*(2), 214–231.
16. Lin, P., et al. (2008). A secure mobile electronic payment architecture platform for wireless mobile networks. *IEEE Transactions on Wireless Communications, 7*(7), 2705–2713.
17. Martínez-Peláez, R., Rico-Novella, F., & Satizabal, C. (2008). Mobile payment protocol for micro-payments: Withdrawal and payment anonymous. In *International conference on new technologies, mobility and security*. Tangier, Morocco. IEEE.
18. Ahamad, S. S., Udgata, S. K., & Sastry, V. N. (2012). A new mobile payment system with formal verification. *International Journal Internet Technology and Secured Transactions, 4*(1), 71–103.
19. Deya, A.-P. I., et al. (2012). Anonymous, fair and untraceable micropayment scheme: Application to LBS. *IEEE Latin America Transactions, 10*(3), 1774–1784.
20. Chen, C.-L., & Chien, C.-F. (2013). An ownership transfer scheme using mobile RFIDs. *Wireless Personal Communications, 68*, 1093–1119.
21. Wakadha, H., et al. (2013). The feasibility of using mobile-phone based SMS reminders and conditional cash transfers to improve timely immunization in rural Kenya. *Vaccine, 31*, 987–993.
22. Yang, J.-H., Chang, Y.-F., & Chen, Y.-H. (2013). An efficient authenticated encryption scheme based on ECC and its application for electronic payment. *Information Technology and Control, 42*(4), 315–324.
23. Javan, S. L., & Bafghi, A. G. (2014). An anonymous mobile payment protocol based on SWPP. *Electronic Commerce Research,*. doi:10.1007/s10660-014-9151-6.
24. Leavitt, N. (2012). Are mobile payments ready to cash in yet? *Computer, 45*(9), 15–18.
25. Martínez-Peláez, R., Rico-Novella, F., & Satizabal, C. (2010). Study of mobile payment protocols and its performance evaluation on mobile devices. *International Journal of Information Technology and Management, 9*(3), 337–356.
26. Putland, P. A., Hill, J., & Tsapikidis, D. (1997). Electronic payment systems. *BT Technology Journal, 15*(2), 32–38.
27. Kadhiwala, S., & Muhammad, S. (2007). Analysis of mobile payment security measures and different standards. *Computer Fraud and Security, 2007*(6), 12–16.
28. Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology—Crypto'82*. Springer.
29. Fan, C. I., Chen, W. K., & Yeh, Y. S. (2000). Date attachable electronic cash. *Computer Communications, 23*(4), 425–428.
30. Chang, C.-C., & Lai, Y.-P. (2003). A flexible date-attachment scheme on e-cash. *Computers and Security, 22*(2), 160–166.
31. Juang, W. S. (2007). D-cash: A flexible pre-paid e-cash scheme for date-attachment. *Electronic Commerce Research and Applications, 6*(1), 74–80.
32. Martínez-Peláez, R., Rico-Novella, F., & Satizabal, C. (2010). TOMIN: Trustworthy mobile cash with expiration-date attached. *Journal of Software, 5*(6), 579–584.
33. Fan, C.-I., Sun, W.-Z., & Hau, H.-T. (2014). Date attachable offline electronic cash scheme. *Hindawi Publishing Corporation,*. doi:10.1155/2014/216973.
34. Abe, M., & Fujisaki, E. (1996). How to date blind signatures. In *International conference on the theory and applications of cryptology and information security: Advances in cryptology*. Springer-Verlag.
35. Satizabal, C., Páez, R., & Forné, J. (2005). PKI Trust Relationship Using Hash Chains. In *International conference on advances in the internet, processing, systems and interdisciplinary research, (IPSI'05)*. Carcassonne, France.
36. Satizabal, C., et al. (2007). Reducing the computational cost of certification path validation in mobile payment. In *4th European PKI workshop: Theory and practice on public key infrastructure*. Palma de Mallorca, Spain. Springer-Verlag.
37. WAPForum. (2001). Wireless transport layer security, specification WAP-261-WTLS-20010406-a.
38. Bruno, R., Conti, M., & Gregori, E. (2002). Bluetooth: Architecture, protocols and scheduling algorithms. *Cluster Computing, 5*, 117–131.
39. Assora, M., Kadirire, J., & Shirvani, A. (2007). Using WPKI for security of web transaction. In *E-commerce and web technologies*. Springer-Verlag.
40. Satizabal, C., Paez, R., & Forne, J. (2007). WAP PKI and certification path validation. *International Journal of Internet Protocol Technology, 2*(2), 88–95.

41. Martínez-Peláez, R., et al. (2008). Efficient certificate path validation and its application in mobile payment protocols. In *International workshop on frontiers in availability, reliability and security*. IEEE Press.
42. Satizabal, C., et al. (2010). Reducing the computational cost of the authentication process in SET protocol. *Ingeniería y Desarrollo, 27*, 1–24.
43. NIST. (1995). Secure hash standard (SHA), FIPS PUB 180-1. National Institute of Standards and Technology. http://www.itl.nist.gov/fipspubs/fip180-1.htm.
44. Daswani, N. (2000). Cryptographic execution time for WTLS handshakes on palm OS devices. Certicom Public Key Solutions.
45. Gupta, V., et al. (2002). Performance analysis of elliptic curve cryptography for SSL. In *3rd ACM workshop on wireless security*. Georgia, USA.
46. Levi, A., & Savas, E. (2003). Performance evaluation of public-key cryptosystem operations in WTLS protocol. In *8th IEEE international symposium on computers and communication*. IEEE.
47. Argyroudis, P.G., et al. (2004). Performance analysis of cryptographic protocols on handheld devices. In *3rd IEEE International symposium on network computing and applications*.
48. Tillich, S., & Grobschädl, J. (2004). A survey of public-key cryptography on J2ME-enabled mobile devices. In *19th International symposium on computer an information sciences*. Antalya, Turkey.
49. van der Heijden, H. (2002). Factors affecting the successful introduction of mobile payment system. In *Proceedings of 15th bled electronic commerce conference eReality: Constructing the eEconomy*.

Rafael Martínez-Peláez received Ph.D. degree from the Technical University of Catalonia in 2010. He is an associate professor in the Department of Electrical Engineering and Computing at Autonomous University of Ciudad Juarez, Mexico. He has served as TPC member of many international conferences and workshops. He is a member of the National System of Researchers (SNI) of the National Mexican Science Council (CONACYT). His research interests include authentication technologies, smart cards, and security issues on electronic services.

Homero Toral-Cruz received M.Sc. and Ph.D. degrees in Electrical Engineering, Telecommunication option from Center for Research and Advanced Studies of the National Polytechnic Institute (CINVESTAV), Jalisco, Mexico, in 2006 and 2010, respectively. He received the B.Sc. degree in Electronic Engineering from "Instituto Tecnológico de la Laguna", Coahuila, Mexico in 2002. He is currently an Assistant Professor at Sciences and Engineering department in University of Quintana Roo, Mexico. His research interest includes VoIP technologies, QoS and network measurements, convergent networks, Internet technologies, IP traffic modeling, network performance evaluation, network security and WSN. He has served as Guest Editor of some international journals and TPC member of several international conferences and workshops. He has been awarded a national recognition as a researcher (SNI level C) by CONACYT and has been elected as member of the Mexican Academy of Sciences (AMC).

Joel Ruiz received M.Sc. and PhD degrees in Electrical Engineering from Ensenada Center for Scientific Research and Higher Education (CICESE) in 2006 and 2011, respectively. Currently, he is Full time professor at Sonora's State University (UES) in the Department of Software Engineering. His research interests include Wireless Sensor Networks' protocols design, Medium access and routing protocols for wireless networks.

Pablo Velarde-Alvarado is a Research-Professor at the Area of Basic Sciences and Engineering of the Autonomous University of Nayarit. He received the B. Tech. degree in electronics engineering from the Autonomous University of Guadalajara (UAG), in 1993, and the M.Sc. and Ph.D. degrees in electrical engineering from the Center for Research and Advanced Studies (CINVESTAV-IPN) in Guadalajara City, in 2001 and 2009, respectively. He is a member of the National System of Researchers (SNI). His research interests include IP-Traffic Modeling and design of concise behavior models for Entropy based Intrusion Detection Systems.