Research Journal of Applied Sciences, Engineering and Technology 7(12): 2589-2595, 2014
DOI:10.19026/rjaset.7.572
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: September 09, 2013 Accepted: September 24, 2013 Published: March 29, 2014

Research Article

The Architecture of Mobile Wallet System Based on NFC (Near Field Communication)

Xiaohua Ma and Wenxue Wei
College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China

Abstract: The study presented mobile wallet system architecture, in order that people can consume more convenient and efficient in life. Nowadays, existing mobile banking applications require real-time online and its tedious steps have been unable to meet needs of users. With the emergence of smart phones continues to heat up in the world, more and more payment methods use mobile payment. In addition, with the continuous improvement of mobile hardware devices, it will be possible that people can use mobile NFC (Near Field Communication) tags for payment. This study realized the prototypical system of this architecture in the android environment. Consumer uses this application to achieve proximity payments, without networking. Consumer simply closes to the POS (Point of Sale) devices gently, then the payment can be completed.

Keywords: Digital certificate, NFC technology, offline consumption, proximity payment, safety verification

INTRODUCTION

Mobile payment is a service mode that it allows mobile users to pay for the consumption of goods or services using mobile. Payment methods mainly include remote payment and proximity payment. The current mobile bank is achieved by using remote payment, it combines mobile communication field with financial services and becomes a new banking model after the bank card, ATM and online bank, bringing great convenience to users. But when mobile bank consumer makes payment, it requires the mobile real-time online and also its complex payment procedures, it is not easy to be grasped and is not conducive to be spread (Xu, 2012a; Yi, 2009; Kemp, 2013).

This study will achieve proximity payment, with NFC technology. Proximity payment is a mode that mobile device completes the transaction in the manner of online or offline payment through terminal device at trading site. Online trading is communicated with the bank host directly or indirectly, for business processing by calling business service. Offline trading is not communicated with the bank host, completing the transaction processing through the terminal device and the mobile terminal, When it get to end-of-day, business system progresses trading data, which terminal equipment sends to. NFC means Near Field Communication. NFC mobile inside places NFC chip, which is a part of the RFID (Radio Frequency Identification) module. NFC chip can be used as passive RFID tag for paying and also can be used data exchange and acquisition as a RFID reader (Wu and Yang, 2013; Chen, 2011; Xu, 2012b).

In order to solve the drawbacks of existing mobile banking and make people consume with mobile more convenient and efficient, this study presented NFC-based mobile wallet system. With the mobile wallet, people can complete the payment easily. For the way of micro-payment, the consumer deposits the funds of debit card account or cash to mobile wallet before consuming. When people pay the money, simply holds the mobile to the POS device, then will complete the payment without needs networking (Zhou and Zhang, 2007; Yi, 2009).

MATERIALS AND METHODS

The system architecture based on NFC mobile wallet includes system overall architecture and security architecture. The overall architecture of the mobile wallet system analyzed the various components and researched the business of the system. As mobile communication wireless network easily being intercepted and tampered, in addition, user identity is easy to impersonate, this study also researched the security architecture.

The overall architecture: Mobile wallet system involved mobile wallet platforms, bank counter system, acquiring system, account management system and mobile client software. With increasing mobile wallet application, mobile wallet platform adds online and offline accounts. Online account is a temporary account for mobile wallet cash, using for temporary save the funds of returned goods mainly and its balance does not write into the mobile wallet accounts. The balance of the

Corresponding Author: Xiaohua Ma, College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China

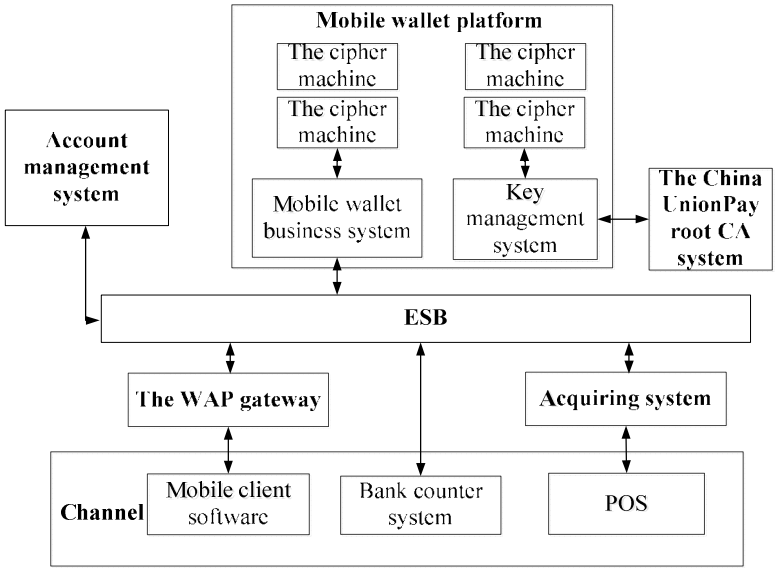

Fig. 1: The logical architecture of mobile wallet system

offline account is written into mobile wallet account for offline consumption. Mobile wallet account is a virtual concept at the mobile terminal, that is to say, it is the limit counter in the mobile wallet software.

Mobile wallet account deducts the corresponding funds when people consume offline payments. Pos terminal sends the consumer records to the acquiring system, then the acquiring system sends it to the mobile wallet platform in the bank. When the records are validated by mobile wallet platform, the offline account will deduct the amount. Mobile wallet platform sends the request to the bank account management system, when users use transaction of load. Then the bank account management system processes the transaction accordingly. As a result, the sum of offline account in mobile wallet platform is increased. If the operation makes successful, the system will notice the client software, the amount of mobile wallet account has been increased finally. The logical architecture of mobile wallet system is as shown in Fig. 1.

Account management system: Responsible for managing the ledger of banking institutions.

ESB (Enterprise Service Bus): Responsible for routing control, changeover message and exception handling.

Mobile wallet business system: Responsible for managing the ledger of mobile wallet system, liquidating the account of offline consumption, checking the account with peripheral systems and bank account management system.

Key management system: Mainly responsible for continuously generating asymmetric keys, also responsible for managing user information, issuing certificates, revoking certificates, updating certificates and so on.

The China union pay root CA system: Responsible for issuing the bank's certificates.

The WAP gateway: Responsible for protocol conversion between the WAP and WWW.

Acquiring system: Responsible for generating and send the offline transaction information and collecting, collating and submitting billing data etc.

Bank counter system: Responsible for increasing or canceling mobile wallet service, reporting the loss or relieving the loss reporting of mobile wallet, loading cash and so on.

According to the logical architecture of system, this study showed the functional distribution of mobile wallet system in Fig. 2.

Loss reporting or relieving the loss reporting: Realize to manage the online account in mobile wallet system when the phone is lost.

Parameter modification: Realize the function of modifying parameters of mobile wallet and parameters include: balance limit, single spending limit, the amount of automatic load, the minimum balance of automatic load and so on.

Load: Including cash load, binding load and non-binding load, realize to deposit cash or the funds of debit account in mobile wallet account.

Automatic load: According to the agreement which is signed in advance, the system will automatically

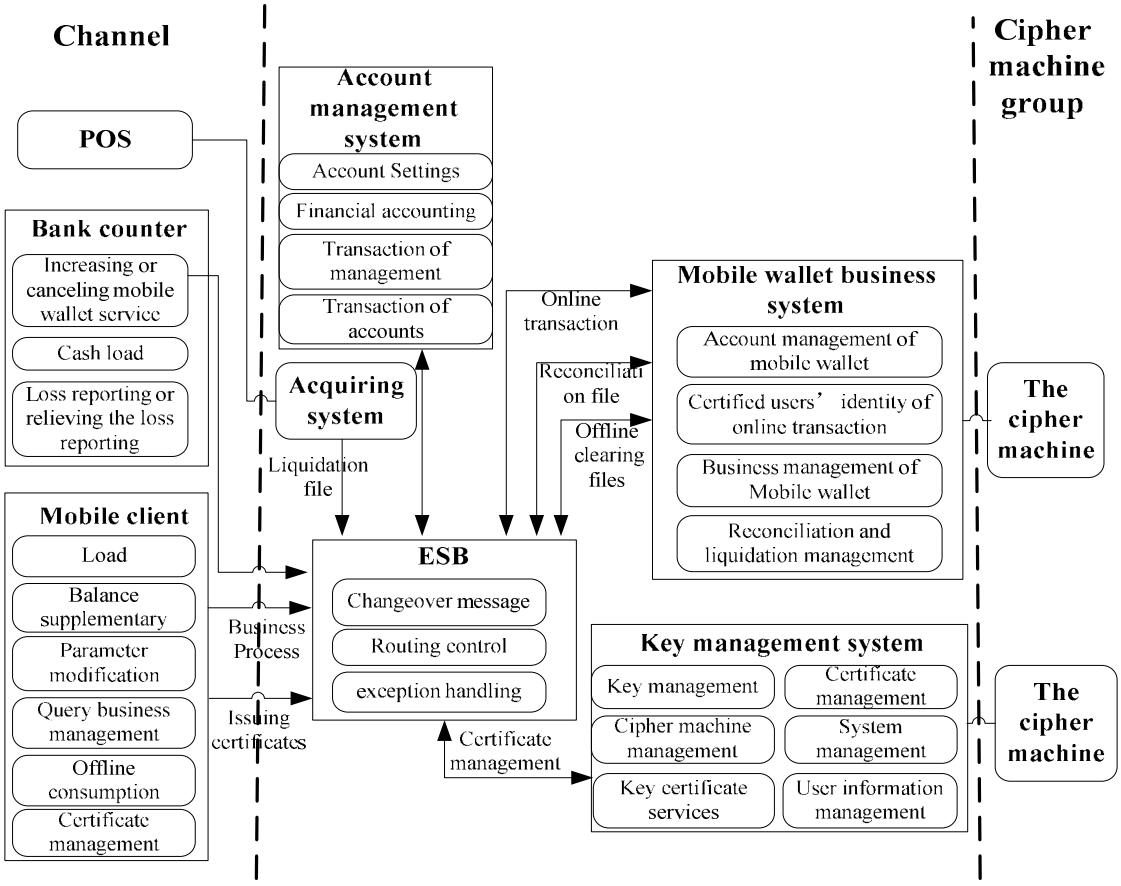

Fig. 2: The functional distribution of mobile wallet system

touch off load transactions when the balance of mobile wallet is less than the minimum balance of automatic load.

Balance supplementary: Realize to deposit the funds of online account in mobile wallet account.

Load reverse: When the load operation is not accomplished, the accounting will be automatic rollback.

Revoke load: Revoke the operations of cash load which are done by a teller.

Reconciliation: Check the account which is produced by load or unload with bank account management system and check the account which is produced by consumption through the Union Pay channels with peripheral systems.

Accounting booking including offline consumption and returned goods: Record the accounting information which was produced by offline consumption or returned goods through the Union Pay channels and send back the ledger of mobile wallet to the bank account management system. Record the accounting information which was produced by offline consumption or returned goods through the indirect POS channels, send back the ledger of mobile wallet to the bank account management system and send back the ledger of merchant to indirect POS system.

The security architecture: The security architecture is at the core position in the mobile wallet system. The study used identity authentication, information encryption, data integrity verification, digital signature technology in the security architecture, ensures the security of end-to-end data transmission.

The security design as a whole: The security architecture of mobile wallet system was divided into three parts in general: the China Union Pay root CA (Certificate Authority), the security system in the bank and the insurance in mobile client software. The overall security architecture of mobile wallet system is shown in Fig. 3.

China Union Pay root CA is responsible for issuing public key certificate to the bank. It also is responsible

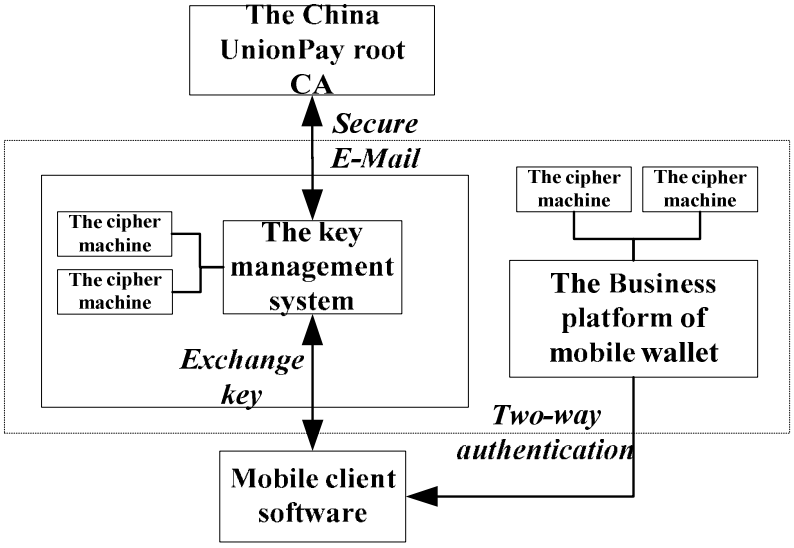

Fig. 3: The security architecture mobile wallet system

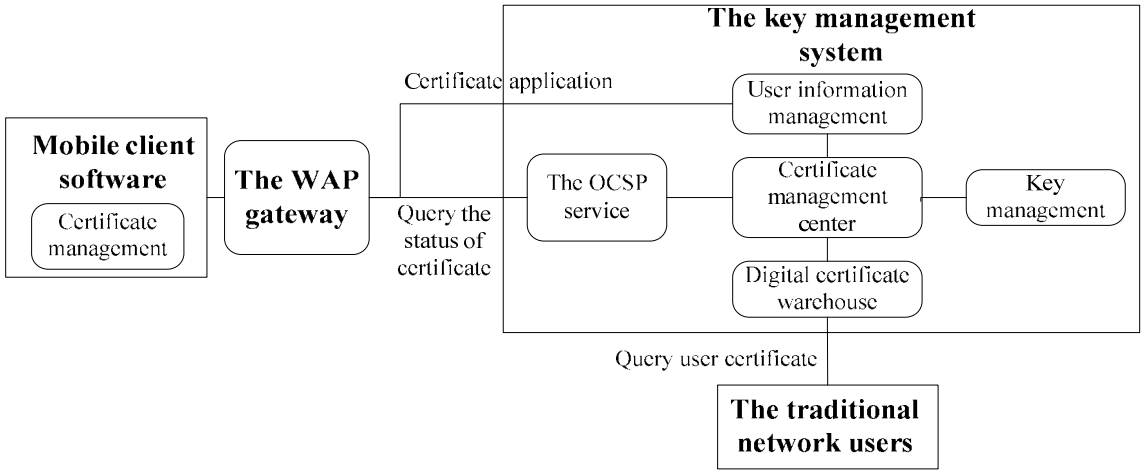

Fig. 4: Security architecture based on WPKI (Wireless Public Key Infrastructure) of mobile wallet system

for generating, storing, maintaining the private key and public key. In addition, China Union Pay root CA is responsible for transmitting the public key certificate of root CA to each bank and acquirer.

Key Management system is responsible for accessing to the Union Pay. After registering strictly, though the system people can apply for the bank certificate or transmit data by way of secure E-Mail. In addition, the system have to bear the work of the constantly generating the asymmetric key and bulk issuing the certificate. Key Management system also exchange data with the mobile client software by the way of appointing exchange key.

Security system based on WPKI: WPKI (Wireless Public Key Infrastructure) is used to manage the public key and digital certificate in mobile communication network environment and effectively establish a secure and trusted wireless communication network environment. The Security architecture based on WPKI as shown in Fig. 4 (He *et al*., 2008; Yin and Wei, 2007).

Through the WAP (Wireless Application Protocol) gateway, the mobile client software access to key management system which in mobile wallet platforms. Key management system provide functions of user information management, certificate management, key management, the status of certificate query and the certificate directory download and so on to users.

User information management: Audit user information and register user information.

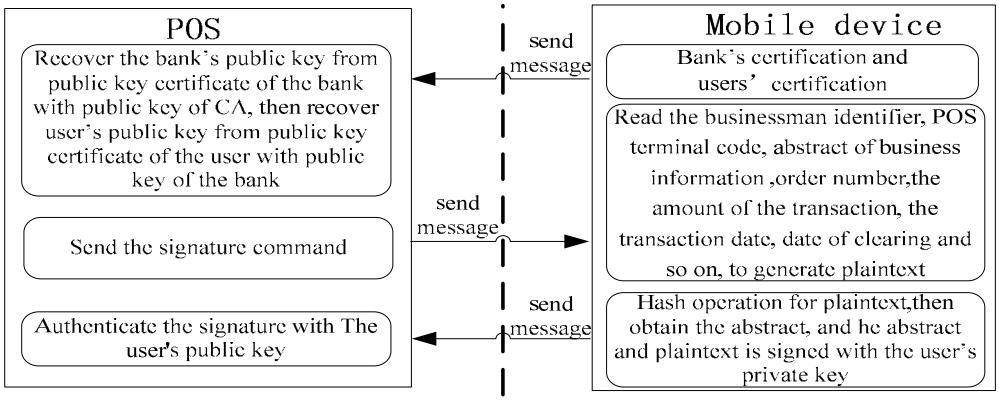

Fig. 5: The safety verification process of offline consumption

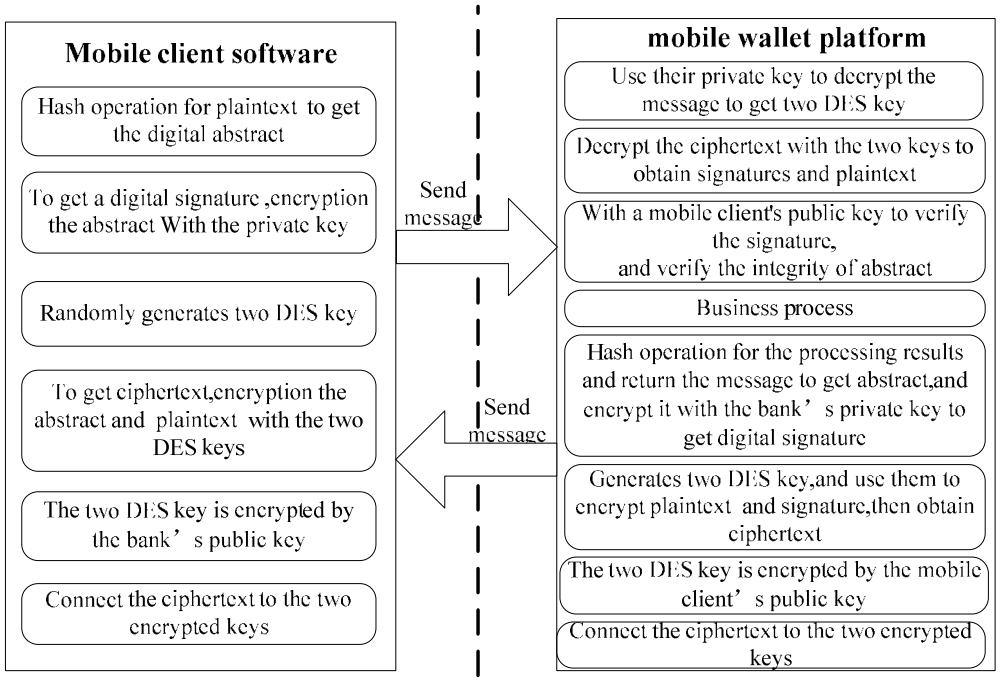

Fig. 6: The safety verification process of online consumption

OCSP (Online Certificate Status Protocol) service: Provide the services of real-time querying certificate status to mobile network users.

Certificate management center: Responsible for signing, updating, canceling the certificates, recovering the key and issuing the certificate list (CRL Certificate Revocation List).

Key management: Responsible for key generation, key recovery, key backup, etc.

Digital certificate warehouse: Store certificates which have been issued.

Design of the identity authentication: The public and private key pairs are generated in mobile client software and private key is stored in an encrypted file in phone memory. The bank's private key is generated in the cipher machine; it is encrypted by master key in cipher machine and stored in the system database. The bank's certification is generated by the bank's public key is signed with the private key of Union Pay certification authority. The user's certification is generated by the user's public key is signed with the private key of the bank. In order to ensure the legitimacy of the user, need to authenticate their identity when they are consuming online or offline.

The identity verification of offline consumption: Mobile device and POS terminal need to authenticate mutually when people use the mobile device to consume. The safety verification process of offline consumption as shown in Fig. 5.

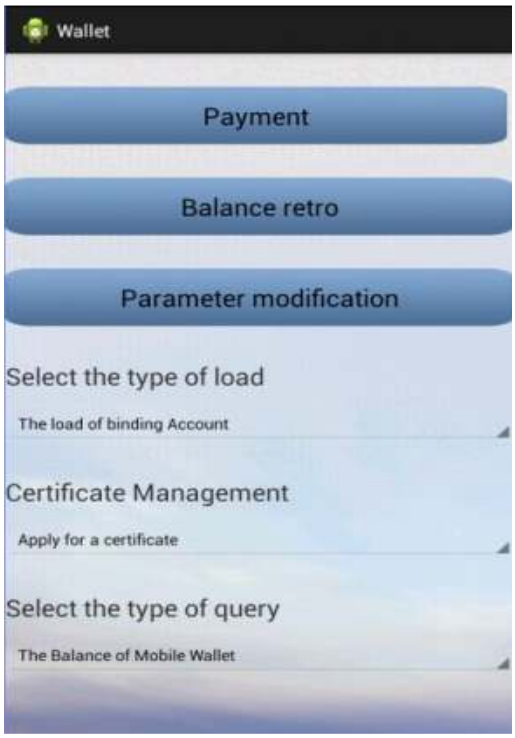

Fig. 7: The main interface of mobile wallet

The data of counter value is included in message. The counter value is used to ensure the uniqueness of consumer records and the value plus 1 when a transaction completes successfully.

The identity verification of online consumption: Online transaction is the interaction between mobile wallet platform and the mobile client software. The bank and the user need to authenticate each other, to ensure data integrity and accuracy. The safety verification process of online consumption as shown in Fig. 6 (Hsiang and Shih, 2009; Zhang *et al*., 2013; Al-Fayoumi and Aboud, 2007).

The data which need to be signed in the alternating process between mobile wallet platform and the mobile client software include: mobile user ID, user account, bank identification, transaction code, transaction parameters and so on. The encrypted and decrypted operation is finished by the encrypted and decrypted device which belongs to sender or recipient.

RESULTS AND DISCUSSION

In order to prove the designed architecture in this study, this study designed and developed the prototypical system of this architecture in the android environment. The system realized some transactions such as: offline consumption, load, balance supplementary, parameter modification, query

Fig. 8: The interface of binding load

management, certificate management and so on. When people first use the mobile wallet application need to register to set a password. If login successfully, you will see the main interface of mobile wallet. The main interface of mobile wallet as shown in Fig. 7.

In the drop-down box of load type, people select the load of binding account and the interface will jump to the interface of the binding load and it as shown in Fig. 8.

The bank's systems communicate each other through the Web Sphere MQ, Web Sphere MQ is composed mainly by Queue Manager, Queues and Channel. When one system sends messages to a queue and the other one will remove the messages from the queue.

The interface field of load request message include: Tx Code (Transaction Code), ESerNo (ESB Serial Number), E_date (ESB transaction Date), E_time (ESB transaction Time), Teller (Teller's number), Brc (Trading institutions), WalletSta (Status of the mobile wallet)\, Card No (Debit Card Number), Circlesavetype (the load Type), Circleamount (the amount of load), ELcashincard (Balance of the mobile wallet), Eleccashon (balance limit of mobile wallet).

CONCLUSION

The mobile wallet system based on NFC use a micro-payment method. The money in wallet cannot be spent if the mobile phone is lost meanwhile there is no mobile client login password. It can reduce the number of interactions between the mobile wallet system with the banks' system and reducing the burden of banks. In addition, when users consume offline, they need not to enter a password so that it can save much time and bring a lot of convenient for users.

But the user's certificate and private key exist in the encrypted files; this has not yet meets the requirement of safety. With the further development of

mobile phone hardware, if the smart card is integrated in mobile phones, public and private key will be generated in the smart card, this will make the security of mobile payment greatly improved.

REFERENCES

Al-Fayoumi, M.A. and S.J. Aboud, 2007. Identity authentication and key agreement schemes for ad hoc networks. J. Appl. Sci., 7: 1638-1642.

Chen, W., 2011. The implementation of android system based NFC technology. M.A. Thesis, Dalian University of Technology, Dalian, China.

He, R., Z. Qin and X. Qin, 2008. A secured mobile access scheme for SMS message. Inform. Technol. J., 7: 261-268.

Hsiang, H.C. and W.K. Shih, 2009. A secure remote mutual authentication and key agreement without smart cards. Inform. Technol. J., 8: 333-339.

Kemp, R., 2013. Mobile payments: Current and emerging regulatory and contracting issues. Comput. Law Secur. Rev., 29: 175-179.

Wu, S.H. and C. Yang, 2013. A study on designing the new near field communication technology-NFC-micro SD technology. Inform. Technol. J., DOI: 10.3923/itj.2013 (In Press).

Xu, H., 2012a. The development and application research for E-wallet in mobile payment. M.A. Thesis, Beijing University of Posts and Telecommunications, Beijing, China.

Xu, H.Y., 2012b. The study on mobile payment business based on China unionpay model. M.A. Thesis, Tianjin University, China.

Yi, L., 2009. The trend of mobile payment. Radio Freq. Ident. Technol. Appl., 1: 75-76.

Yin, C.J. and Z. Wei, 2007. Design of PKI-based mobile bank security system. J. Chongqing Univ., Posts Telecommun. Nat. Sci. Edn., 19: 381-385.

Zhang, D.D., Z.F. Ma, X.X. Niu and Y. Peng, 2013. Anonymous authentication scheme of trusted mobile terminal under mobile internet. J. China Univ., Posts Telecommun., 20: 58-65.

Zhou, C.Y. and C.R. Zhang, 2007. A trusted smart phone and its applications in electronic payment. J. Electron. Sci. Technol. China, 3: 206-211.