International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.119-128
http://dx.doi.org/10.14257/ijsia.2015.9.7.11

Research on Mobile E-business Security Model based on WPKI Technology and its Application

Yongsheng Luo

Department of Electronic and Information Engineering, Shunde Polytechnic, Shunde 528000 China

Abstract

Information has become the important and strategic resource, and social informatization has become the developing trend and core. The information safety will play an extremely important role in the information society. It is directly related to the national security, business and the normal life. Wireless Public Key Infrastrcture(WPKI) is a technology of wireless networks security, which is applied to transform the E-Business and the Internet for shopping, banking and transacting with one another in anywhere at anytime by using the wireless devices of mobile phone, PDA, IPAD and so on. Wireless application protocol (WAP) can ensure the secure e-business services and wireless applications. So the structure, principle, security infrastructure, application model and environment of WPKI are described in detail. Then the mobile E-business security model based on WPKI Technology is proposed in this paper. It will analyze and demonstrate how the WPKI technology can provide the security services to mobile E-business with similar security requirements and provide the reader with a high level technical application of the WPKI technology. And a application system provided an excellent example for demonstrating the effectiveness, and the secrecy, identity authentication and non repudiation are studied and analyzed.

Keywords: *WPKI, WAP, Mobile E-business, Security service, Certification authority*

1. Introduction

With the quick development of mobile communication technology and the wide application of intelligent mobile terminal, huge amounts of information are moved daily from one network to another. Today, individuals and businesses rely on this way to conveniently exchange information. The consumers can achieve many things on line, such as shopping, banking, transacting and so on. And mobile E-business is one of businesses. It has become a new approach to individuals and enterprises on businesses [1-2]. This approach is based on combining the wireless network technology and traditional business application. Various suppliers can provide various customers with the more convenient, real-time and humanized services by using the new business way. Mobile E-business refers to process electronic business online activities based on combining PDA, mobile phones, palm computers and Internet. In recent years, mobile E-business has made considerable development. However, due to the sensitive information transmitting via wireless network, the safety is always the key technology to affect the development of the mobile E-business. The mobile E-business security is more vulnerable than the traditional E-business model [3-4]. Therefore, the Public Key Infrastructure (PKI) security mechanism is introduced into the wireless network in order to construct Wireless Public Key Infrastructure (WPKI) security technology, which can provide security services of encryption and digital signature for all kinds of applications on the wireless network. The goal is to protect the legal information of the mobile users (account, password and so on) from the invasion and meet the safety requirements of mobile E-business.

ISSN: 1738-9976 IJSIA

In recent years, in allusion to the mobile E-business model, many researchers have deeply studied and explored new models from the different views. Anderson *et al.* [5] proposed a model checking for the verification of complex software systems. As the use of the Internet for conducting e-business extends the reach of many organizations, well-designed software becomes the foundation of reliable implementation of e-business processes. Lee *et al.* [6] proposed a wireless PKI that provides the similar security level as the wired PKI supporting mobile phone. And the implementation result of the proposed wireless PKI technology is illustrated on the newest mobile phone. Chen *et al.* [7] proposed an organisation structure-based access control (OSAC) model based on a task-role-based access control (T-RBAC) model. The proposed model extends the concepts of static separation of duty (SSD), dynamic separation of duty (DSD), prerequisite, and cardinality constraints in the role-based access control (RBAC) model to present department and role relations that identify the cooperative interactive relations among roles across department boundaries to facilitate resource sharing among roles and simplify enterprise resource management. Jiang and Yang [8] proposed an E-commerce online payment system based on ensuring the security of online payments confidential information. Fang Chung and Fang Chen [9] explained the PKI structure including the different types of cryptosystem and PKI technology such as digital signature and PKI components, the way of the components operate, and the four main services provided by PKI. And a Cross Platform Layer (CPL) as a communication interface is proposed for facilitating secure PKI interoperability. Ou and Ou [10] proposed an adaptation of proxy certificates to non-repudiation protocol of agent-based mobile payment systems. Muniyal *et al.* [11] used the hierarchical PKI of the most popular PKI trust models to construct the security infrastructure. Benson *et al.* [12] proposed the Partner Key Management (PKM) as a mechanism which sufficiently addresses security and liability concerns of businesses performing high-value online transactions, and uses wholesale banking as the motivating example. And this paper justifies the security of PKM and its flexible revocation models; and illustrates the justification with proofs through formal logic. Ryu *et al.* [13] investigated the effect of alignments between service innovation strategy (*i.e.*, service creation-focused [SCFS], service delivery-focused [SDFS], and customer interaction-focused [CIFS] strategies) and business strategy (*i.e.*, cost leadership [CLS], innovative differentiation [IDS], and focus [FS] strategies) on firm performance, which is assessed using both nonfinancial and financial measures.

WPKI offers many security services such as authentication, digital signatures, data integrity, encryption and non-repudiation. With this in mind, it would be very interesting to look at some of the issues that would arise when looking at WPKI to secure E-Business primarily on mobile phone terminals. Thus, this paper provides the reader, initially with a concept of Wireless PKI and also an abstract example of how WPKI can secure a particular E-Business.

2. Basic Method

2.1. Mobile E-business

With the rapid development of modern information technology, the influence scope of E- business is expanded, mobile phone technology is increasingly mature. These technologies provide strong technical support for the mobile E- business based on combining E-business and mobile communication. Mobile operators, value-added services, banks and smart card technology cooperate actively to construct the mobile security trading platform with powerful function and broad channel. Internet, mobile networks and wireless PKI technology are used to achieve the organic combination in virtue of message mechanism and STK technology, in order to provide a strong security guarantee for the online business. Mobile E-business is a new E-business mode in mobile information period. It takes full advantage of 3A property of the mobile terminal (Anywhere/Anytime/Anything) to extend E-business from Internet to the phone for forming a broader E-business platform. The information system platform of mobile operators introduces the credit control system and accounting system of operators into the mobile payment system by using the flexible and efficient interface, in order to make more convenient payments. The mobile payment system is applied to the field of mobile value-added services, as an application is loaded onto a mobile peroration network for providing the trading means of mobile phone to consumers. This way will gradually change people's shopping habits and greatly reduce the social transaction costs. It is unlike the wired E-business with PC-based interface, mobile E-business activities mainly rely on the portable terminal of mobile phones, personal digital assistants and so on to carry out business activities. So mobile E-business must ensure that these transactions can be carried anywhere. The mobile E-business is the inevitable result of the integration and development of the wired E-business.

2.2. WAP Protocol

WAP 2.0 [14] uses the same general protocol with the Internet. It can directly log on the Internet by using mobile phone. At the same time, WAP 2.0 has the direct HTTP communication, friendly mobile technology, markup language XHTMLMP and WML 1.0, which can obtain better graphics display and control ability. WAP 2.0 can more easily make the corresponding content optimization for different terminals. It can transmit streaming media by wireless network. The cache is used to obtain faster processing speed. The large file downloads are more quickly. WAP 2.0 will really realize the seamless connection between the Internet and mobile phone. The mobile phone has become a miniature computer terminal. WAP 2.0 uses all kinds of technologies to enhance the business performance, including data synchronization, multimedia messaging service (MMS), permanent storage interface, provisioning, transmitted pictograms of graphic symbols and so on. In addition, WAP 2.0 further improve for the wireless telephone application, Push and the user agent profile and so on.

WAP defines an open global wireless application framework and network protocol standard. The application and the service on the Internet are introduced into the wireless terminal, such as mobile phones and so on. The aim is to the mobile user can not be limited by network type, network structure, the bearing business of carrier operator and terminal devices. The mobile devices are used to easy access and obtain the business information and all kinds of services of the Internet or the enterprise internal network. The WAP model consists of agent mobile devices of users, WAP gateway and WAP server. The model is shown in Figure 1.

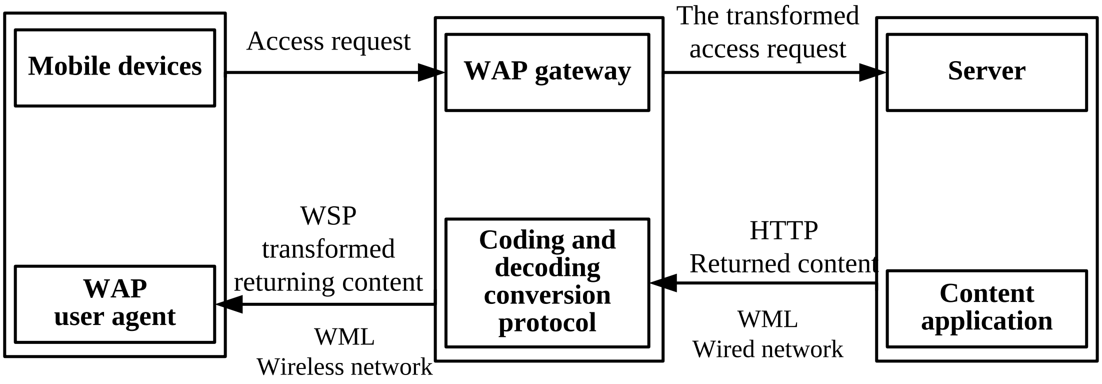


Figure 1. The WAP Model

2.3. WPKI Technology

The WPKI technology [6] is a key management platform based on the established standards. It is not a new standard, PKI technology in the traditional wired environment is optimized and extended for applying in a wireless environment. Because PKI technology is very difficult to be applied in the wireless environment and has very high system requirements, the WPKI technology based on PKI technology is improved, optimized and extended to adapt to the wireless network environment bandwidth, low wireless device computing ability and so on. The WPKI has perfect key and certificate management system, it most concerned policies and standards in order to manage E-business, provide security services by using WTLS WML Script under the wireless application environment. It can meet the safety requirements of mobile E-business, which are confidentiality, integrity, authenticity and non-repudiation. The WPKI technology uses optimized ECC algorithm, compressed X.509 digital certificates, and the third trusted organization of certified authority to validate user ID, in order to realize the secure transmission of information in the wireless network and reduce the risk of the transactions.

In the actual application, the WPKI components mainly include entity application (EA), PKI directory, registry centre (RA), certification authenticity (CA), certificate repository, interface and so on. However, in the WPKI, the end device applications and registration is a little different for implementing, and a new component based on the PKI Portal is also required. In the WPKI model, the EE is implemented as optimized software that runs in the WAP device, depends on the WTLS WML Script API for realizing the key services and cryptographic operations. The PKI portal is a new device in the WPKI. It is just a networked server (WAP Gateway), it is to realize the RA, and is responsible to translate requests by the wireless device client to the RA and CA in the PKI. The PKI Portal will typically be embed the RA functions and interoperate with the WAP devices on the wireless network and the CA on the wired network. The basic structure of the WPKI is shown in Figure 2.

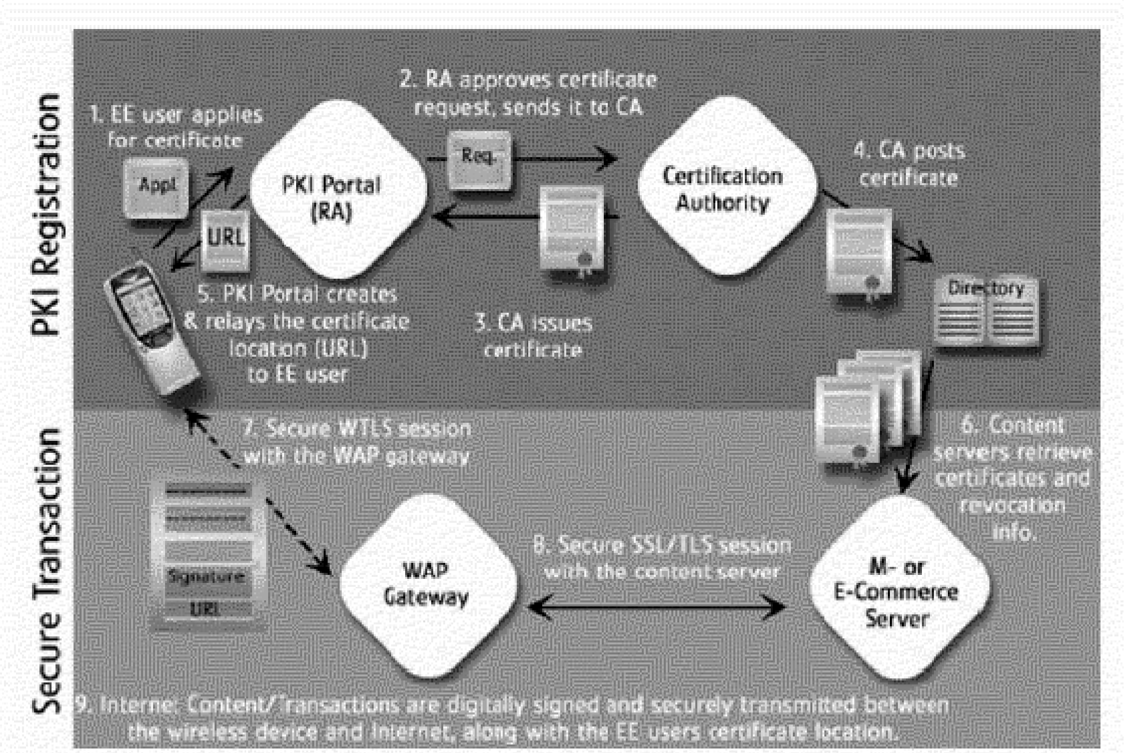

PKI Registration
1. EE user applies for certificate
Appl
URL
PKI Portal (RA)
2. RA approves certificate request, sends it to CA
Req.
Certification Authority
3. CA issues certificate
4. CA posts certificate
Directory
5. PKI Portal creates & relays the certificate location (URL) to EE user
Secure Transaction
6. Content servers retrieve certificates and revocation info.
7. Secure WTLS session with the WAP gateway
Signature
URL
WAP Gateway
8. Secure SSL/TLS session with the content server
M- or E-Commerce Server
9. Interne: Content/Transactions are digitally signed and securely transmitted between the wireless device and Internet, along with the EE users certificate location.

Figure 2. The Flow of WPKI Technology

3. The Security Architecture of Mobile E-business

The security architecture of mobile E-business is to ensure a complete logical structure of data safety in the mobile E-business. The security architecture consists of five layers, which include the mobile bearing layer, encryption layer, security authentication layer, network security protocol layer and application system layer. The functions of mobile bearing layer mainly provide bearing network and soft, hardware platform and so on. The functions of encryption layer mainly complete data encryption and decryption from the mobile terminal to the WAP gateway and from the WAP gateway to the Web server. The functions of security authentication layer mainly complete the identity authentication of the mobile terminal users, Web server users, the third party financial institutions and so on. The network security protocol layer mainly includes WTLS protocol, security protocol TLS, SSL on the transport layer under the wired environment. The application system layer mainly completes a variety of processes of mobile E-business. The security architecture of mobile E-business can interrelate the unified and interdependent entirety in order to realize mobile E-business security. The security architecture of mobile E-business is shown in Figure 3.

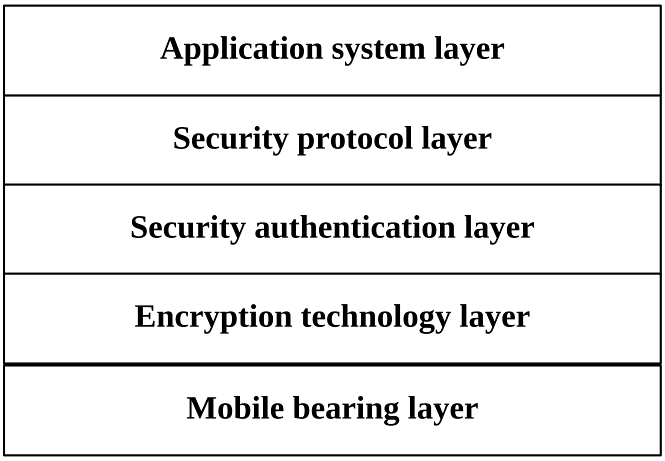


Figure 3. The Security Architecture of Mobile E-business

4. The Security of Mobile E-business based on WPKI Technology

4.1. The Security Model of Mobile E-business

The WPKI technology is a comprehensive security platform based on the public key technology. It will introduce the PKI security mechanism of Internet E-business into wireless network environment, including the needed hardware, software, personnel, policies and procedures, such as generation, management, storage, distribution and revocation certificates and so on. In E-business, how to realize the online, real-time and secure payment is the core of implementation techniques, especially in mobile E-business, it need accurately identify the persons, determine account, and safely achieve funds transfer processing. Currently, the most mobile equipment processing capacity is low, a mobile E-Business security model based on WPKI technology is proposed in this paper. A complete WPKI system must include the following elements:

(1) End entity application (EA)

The EA takes on the application of the PKI function. This application is used to WIM card in the WAP devices.

(2) Registry authority (RA)

The RA provides an interface between the user and the CA, which is regarded as the calibration in the certification authority in order to determine the identity of the users, put forward the certificate request and process the other requests of the users to the CA. Of course, the certification processing quality depends on the trust level in the certificate.

(3) Certification authority (CA)

The CA system is based on the PKI trust and the WPKI system. It is responsible for the generation, distribution and verification of digital certificates, determining the validity of the certificate, issuing and revocation the certificate list.

(4) Certificate repository

It is used to deposit certificate directory and access these certificate.
The transaction process of mobile E-business is shown in Figure 4.

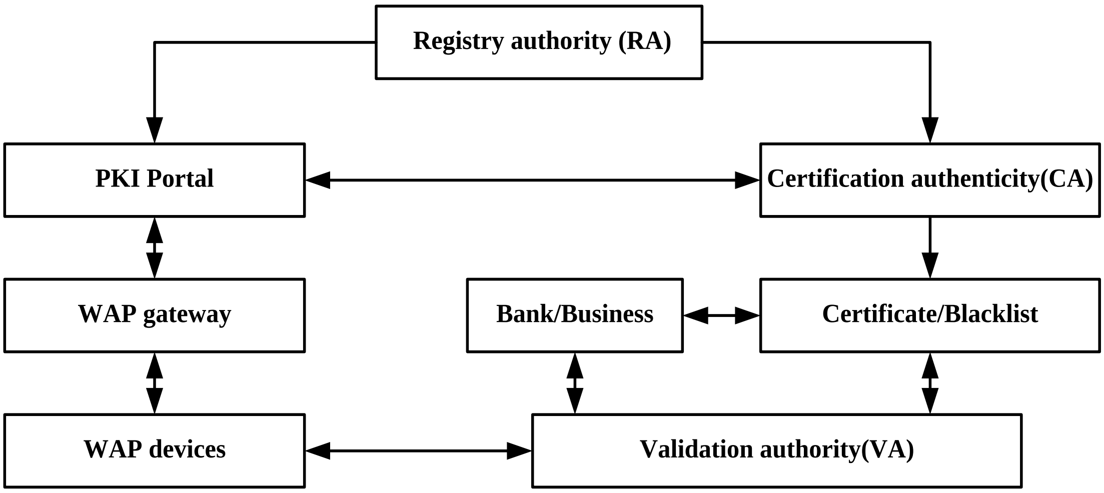


Figure 4. The Transaction Process of Mobile E-business

In the WPKI architecture, WAP gateway is the key component for accessing the Internet by using wireless network. Because mobile network resources are limited, the security connection between the mobile terminal and WAP gateway uses WTLS protocol. WTLS protocol is a secure transport protocol in the WAP protocol stack for mobile E-business. It can ensure the security of WAP communication. So a complete processing operation of WPKI has the following steps:

Step1. The mobile terminal submits the requests of user information, the certificate application, certificate revocation, updating application and so on to the PKI entrance.

Step2. The PKI Portal checks the submitted application. Then request the certificate to the CA after qualified checking and confirmed ID.

Step3. The CA will generate the server certificate. The PKI Portal is used to restore the key, the mobile terminal certificate URL and so on.

Step4. The CA will also generate user public key certificate, which are issued in the directory server for providing the query and download.

Step5. The PKI entrance provides the restored key to the mobile terminal, and preserves the certificate of the mobile terminal. It will send the certificate URL of the mobile terminal. This certificate URL is the URL addresses of these certificates in the directory server.

Step6. The network server can submit query certificate request to the directory server. The directory server will send the certificate URL to the wired network server.

Step7. The security WTLS connection is established between mobile terminal and WAP gateway by using the certificate of the CA.

Step8. The WAP gateway will send the request message of the mobile terminal to the wired network server. Then the wired network server can be returned to the mobile terminal. Thus, the SSL connection is established between the WAP gateway and the wired network server.

4.2. The Security System of Mobile E-business

In order to illustrate the performance of the proposed security model of mobile E-business based on WPKI technology, Construction Bank of China is selected in this paper. Construction Bank of China transaction is taken place on a mobile phone by using the proposed security model, shown in Figure 5.

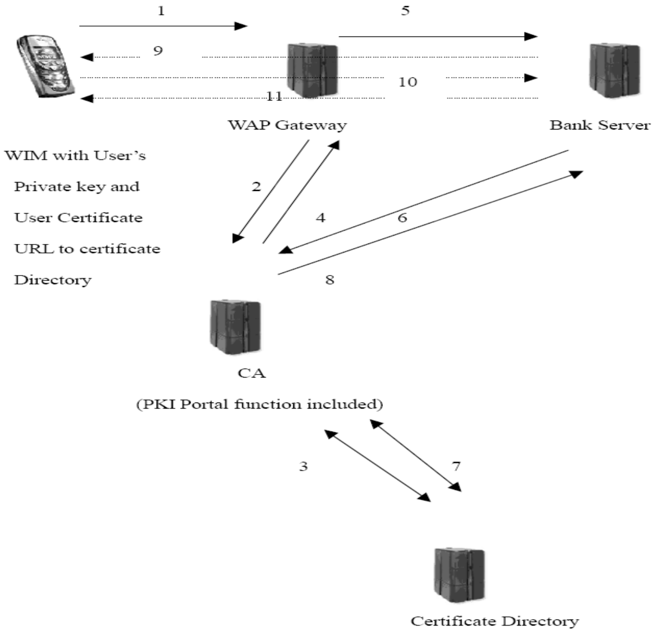


Figure 5. A Technical of Mobile E-Business based on the Security Model

5. Safety Analysis

5.1. The Secrecy

The communication uses a WTLS handshake protocol in the wireless network, and traditional SSL cryptographic protocol in the wired network, so that the information channels between every module is safe. As a businessman, he only know the customers to buy merchandise information, does not know the privacy of the identity information and account information of customers. As the banking system, it, he only know the account information of customers, does not know the information of goods of customers. Each operation in the transaction, the key is used to encrypt the transmitted sensitive information. All the parties of the transaction only know that they should know the information, so as to ensure the confidentiality of sensitive information.

5.2. The Identity Authentication

All the parties of the transaction in the system use the certificates come from the CA. The sender uses its private key to sign the data, and the receiver uses the public key in the certificate to verify the signature information, order to realize the authenticity of the identity authentication of all the parties of the transaction.

5.3. Non Repudiation

The system uses the sent private key in all the parties of the transaction to signature, and received public key in all the parties of the transaction to decrypt and verify. The goal is to ensure that only the two parties of transaction can sign the data. In addition, the security transaction platform of the system records and saves historical data and payment information for all the parties of the transaction, in order to guarantee to deny the signature of the payment. Thus it can guarantee the non repudiation of the transaction in future.

6. Conclusions

Mobile E-business has become a new approach to individuals and enterprises on businesses. It is based on combining the wireless network technology and traditional business application. Various suppliers can provide various customers with the more convenient, real-time and humanized services by using the new business way. Due to the sensitive information transmitting via wireless network, the safety is always the key technology to affect the development of the mobile E-business. The WPKI technology is a comprehensive security platform based on the public key technology. It can provide the similar security level as wired PKI supporting mobile phone. The wireless PKI technology is proposed for constructing the mobile E-business security model through wireless communication in this paper. The security architecture of mobile E-business is given to ensure a complete logical structure of data safety in the mobile E-business. And the transaction process of mobile E-business is described. The applications also need to justify the on going costs of using proposed the mobile E-business security model, and the Construction Bank of China application provided an excellent example for demonstrating. And the secrecy, identity authentication and non repudiation are studied and analyzed.

The proposed security model can be utilized not only E-business but also diverse wireless data communication such as mobile hospital and government, based on mobile phone through wireless internet.

References

[1] K.Y. Lam, S.L. Chung, M. Gu, J.G. Sun, Performance of PKI-based security mechanisms in mobile ad hoc networks, Computer Communications, vol. 26, (**2003**), pp. 2052-2060.

[2] D. Critchlow and N. Zhang, “Security enhanced accountable anonymous PKI certificates for mobile e-commerce”, Computer Networks, vol. 45, (**2004**), pp. 483-503.

[3] T. Walter, “Secure mobile business applications framework, architecture and implementation”, Information Security Technical Report, vol. 9, no. 4, (**2007**), pp. 6-21.

[4] H. Marko, H. Konstantin Hyppo and T. Elena, “Utilizing national public-key infrastructure in mobile payment systems”, Electronic Commerce Research and Applications, vol. 7, (**2008**), pp. 214-231.

[5] B. B. Anderson, J. V. Hansen, P. B. Lowry and S. L. Summers, “Model checking for e-Business control and assurance”, IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews, vol. 35, no. 3, (**2005**), pp. 445-450.

[6] Y. Lee, J. Lee and J. S. Song, “Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce. Computer Communications”, vol. 30, no. 4, (**2007**), pp. 893-903.

[7] T. Y. Chen, Y. M. Chen, C. B. Wang and H. C. Chu, “Flexible authorisation in dynamic e-business environments using an organisation structure-based access control model”, International Journal of Computer Integrated Manufacturing, vol. 22, no. 3, (**2009**), pp. 225-244 .

[8] H. Jiang and J. Yang, “Security technology support system on the electronic commerce online payment”, WSEAS Transactions on Computers, vol. 6, no. 5, (**2007**), pp. 813-820.

[9] Y. U. Fang Chung and H. U. I. Fang Chen, “Cross platform layer for public key infrastructure interoperability”, International Journal of Innovative Computing, Information and Control, vol. 5, no. 6, (**2009**), pp. 1699-1709.

[10] C. M. Ou and C. R. Ou, "Adaptation of proxy certificates to non-repudiation protocol of agent-based mobile payment systems", Applied Intelligence, vol. 30, no. 3, (**2009**), pp. 233-243.

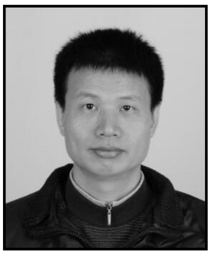
[11] B. Muniyal and P. K. V. Reddy, "An efficient method to merge hierarchical public key infrastructures", International Journal of Computers and Applications, vol. 32, no. 4, (**2010**), pp. 442-446.

[12] G. Benson, S. K. Chin, S. Croston, K. Jayaraman and S. Older, "Banking on interoperability: Secure, interoperable credential management", Computer Networks, vol. 67, (**2014**), pp. 235-251.

[13] H. S. Ryu, J. N. Lee and B. Choi, "Alignment between service innovation strategy and business strategy and its effect on firm performance: An empirical investigation", IEEE Transactions on Engineering Management, vol. 62, no. 1, (**2015**), pp. 100-113.

[14] Wireless Application Protocol Forum, Ltd. Wireless identity module specification [EB/OL]. 2006. Http://technical.openmobilealliance.org/Technical/wapindex.aspx

Author



Yongsheng Luo, he is an associate professor, received the Bachelor degree in Computational mathematics and application software from Wuhan University in 1992, Wuhan, and Master degree in Computer Science from Fuzhou University in 2006,Fuzhou China. The main research directions: Software framework, Information system and security, Educational technology.