I.J. Wireless and Microwave Technologies, **2011, 1, 1-6**
Published Online February 2011 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2011.01.01

Available online at http://www.mecs-press.net/ijwmt

Application of PKI in Encrypting Communications and Verifying Identities of Users in the Internet Banking

Xingyu Gong[a], Shangfu Gong[a *]

[a] *School of Computer, Xi'an University of Science and Technology, Xi'an 710054, Shanxi ,China*

Abstract

This paper analyzes and researches the theories of the encryption communications and identities authentication over the Internet banking based on the PKI technology. Combined with the specific Internet banking system, this research tries to design Internet banking system communication encryption and identities verification and the workflow and main functions. Implementing application to enhance confidentiality of the information transferred by the network communication, this research solves the problems of encrypting Internet banking data and verifying the identities of users and Internet banking. Finally, this paper explores the key technology more in-depth in the designing.

Index Terms: Internet Banking, Certificate, PKI, SSL, CFCA

1. Introduction

With the development of banking and IT industries, a lot of banks have built Internet banking, opening up an exhibition on the Internet banking business. Internet banking is the emerging banking business system that provides customers with information service and the finance service with the help of the Internet technology, the divided commonalty edition system and the specialty edition system. The special edition system requires that the user applies his digital certificate at the branch network of the bank, and the commonalty edition system permits the user to transact on the Internet with the ID card, account number and password. The commonalty edition system can only provide fundamental functions such as inquiry, micro-payment; however, the specialty edition system can provide transfer of accounts payment serves and so on [1]. This paper is emphasizing on the modality of digital certificate to introduce the safe application of PKI technology in the Internet Banking.

2. PKI technology

PKI (Public Key Infrastructure) is a kind of technology and norm that abides by a standard and makes use of the public key encryption technology, which provides Electronic Commerce a set of safe basic platforms. The

* Corresponding author:
E-mail address: gongsf@xust.edu.cn

users could make use of the service that PKI platform provides to carry out safe communication. In real application, great majority of commercial PKI systems only have Certification Authority (CA) [2] that provides issuing and verifying kinds of digital certificates.

The communication between server and consumer could make use of the server and personal digital certificate or corporation digital certificate issued by the CA, to build SSL communication. SSL (Secure Sockets Layer) is the safe protocol brought forward by Netscape Company based on the application of the WEB. The SSL protocol has one especially safe layered data system, which applies between the application program protocol (as HTTP , Telnet , NMTP, FTP and so on) and the TCP/IP protocol , and which provides TCP/IP that TCP/IP connections with data encryption, server verification , information completeness and optional client verification[3]. The SSL protocol is an optional protocol situated between HTTP protocol and TCP protocol; and the communication principle of SSL is shown in Figure 1.

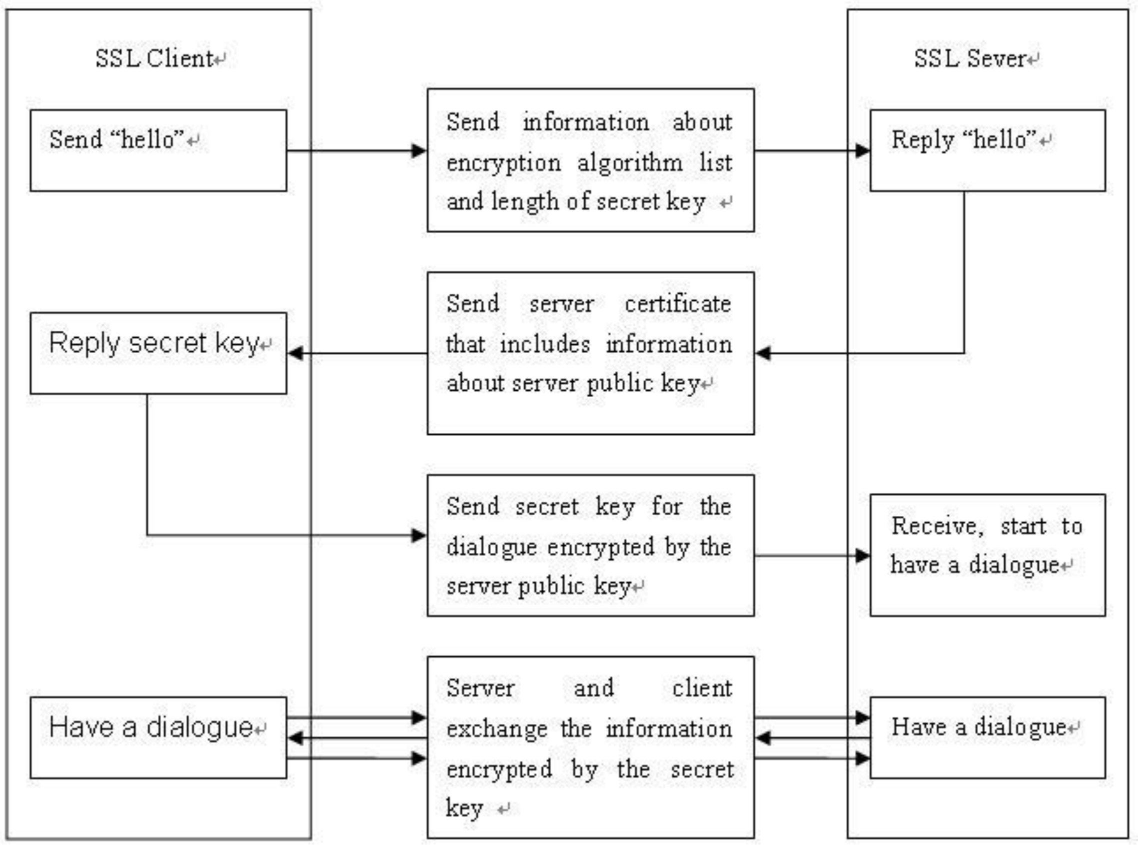
SSL Client
SSL Sever
Send "hello"
Send information about encryption algorithm list and length of secret key
Reply "hello"
Reply secret key
Send server certificate that includes information about server public key
Send secret key for the dialogue encrypted by the server public key
Receive, start to have a dialogue
Have a dialogue
Server and client exchange the information encrypted by the secret key
Have a dialogue

Fig. 1. SSL communication theory

In addition, CA also issues personal digital certificates and corporation digital certificates, and the function of the two kinds of certificates is confirming the identities of individuals and corporations on the Internet, and meanwhile, the function of the above-mentioned server certificate is to establish the SSL server. The digital certificate adopts a private key and public key system, namely making use of a pair of matching each other's keys for encryption and decryption. Each user has a private key issued by the CA and only he knows it, using it for encryption, decryption and digital signature. At the same time, the user shares a public key issued by the CA to a group of users, used for encryption and digital signature. When sending a confidential document, the sender encrypts the data with the receiver's public key, while the receiver decrypts the data with his own private key, so that the data can reach the destination safely. The encryption process with digital means is a reversible process, and can only be decrypted by the private key. The RSA is common in public-key cryptosystem, and its mathematical theory is to break a large number into a product of two prime numbers, composed of the public key and the private key based on the two prime numbers. It is difficult to induce the private key in calculation even if the original data, encrypted data and the public key are known. It needs one millennium to decipher the current 1024 digits RSA key according to our present computer technology [5]. The public key technology has solved the problem of key management issues, in which a business can be shared in its public key, and can retain its private key. Customers can use the business's well-known public key to encrypt messages, and transmit it to the business securely, and then the business can decrypt with its own private key.

The user also can encrypt the data with his private key, and he could generate documents that others can not, because the key only the user has the key, and it could form the digital signature. There are two points that could be affirmed if adopting the digital signature:

(1) The guarantee information is signed by the signer's digital certificate, so that the signer can not deny or be difficult to deny;

(2) Till guarantee information does not go through any modification from signing to receiving, so that the signed document is a true document.

3. Application of PKI in Internet Banking

3.1. China Financial Certification Authority

China Financial Certification Authority (CFCA) is a special organization to issue the digital certificates in Chinese financial circles. The CFCA is the state-class authoritative financial certification organization, which is led by People's Bank of China and is cooperating with fourteen countrywide commercial banks. And the CFCA is the only one authoritative third party online certification service organization that supports Electronic Commerce safety payment transaction. The CFCA specializes in providing various kinds of digital certification services for Electronic Commerce, to build the trusting each other system for providing both sides of online business with information safety Safeguard, and finally to achieve the privacy protection , authenticity , completeness and non-denial of the online Electronic Commerce. Meanwhile, the CFCA takes part in shaping the regulation of online safety business and criterion of technology and operation.

There are three kinds of certificates issued by the CFCA: The corporation digital certificate, individual digital certificate, and server digital certificates. And these three kinds of certificates are respectively used for verifying the identities of the corporation and individual, and building-up the SSL server. The bank can apply for the server digital certificate from the CFCA directly; while the corporation and individual apply for the digital certificate only after being verified by the bank.

3.2. Specific Application of Internet Banking

(1) Server Certificate

The CFCA global server certificate is sent for the global website, and the root-certificate has already established in browsers. The server certificate is equal to "network ID card" of the website, and can used to verify the identity of the website and ensures that the website has high-level encryption safety. It can ensure that the user communicates or trade with the trusting website (not the suspicious website), furthermore, the information sent to the website can not be intercepted or decrypted by any other on the halfway, and consequently can effectively guard against network safety problem such phishing, scamming, wiretapping and tampering. The application for the CFCA global server certificate is shown in Figure 2.

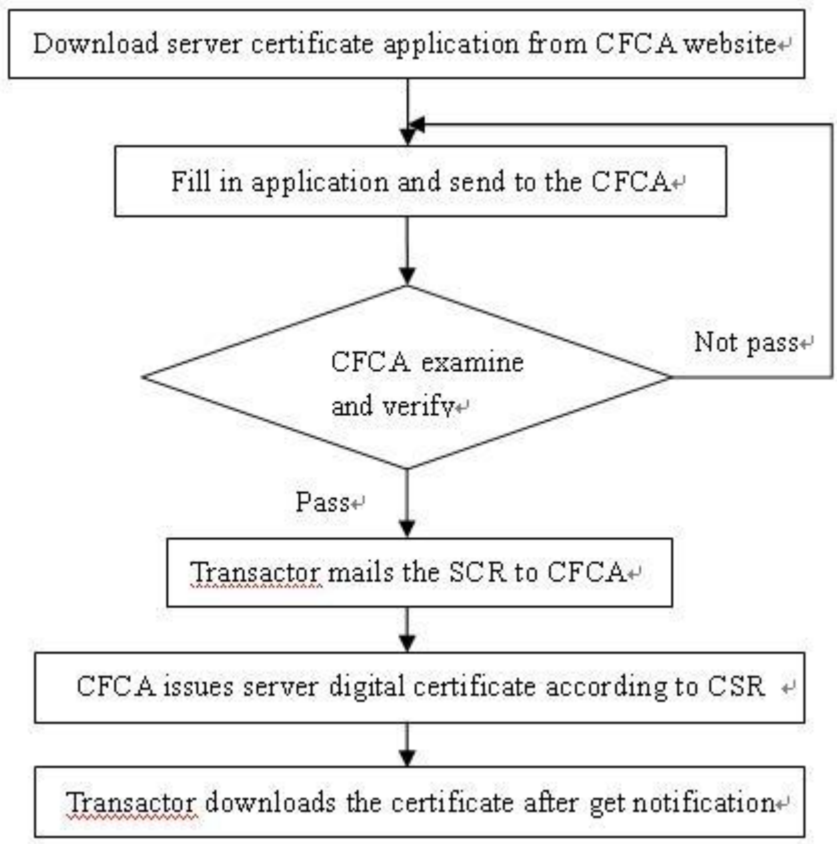
Download server certificate application from CFCA website
Fill in application and send to the CFCA
CFCA examine and verify
Not pass
Pass
Transactor mails the SCR to CFCA
CFCA issues server digital certificate according to CSR
Transactor downloads the certificate after get notification

Fig. 2. Apply for global server certificate

When the bank generates a CSR request document, it will generate a keystore document, and then get server certificate; the server will be used just after importing the server certificate into the keystore file. Taking TOMCAT as an example, put the keystore file in the folder named conf, and then add the path and password of the keystore into the server.xml file, and finally restart the server to complete configuration of the SSL server.

(2)Corporation and individual digital certificates

The CFCA corporation and individual digital certificate are sent for global corporation and individual, The certificate is equal to "network ID card" of corporation and individual, and can used to verify the identity of the website and ensures that the website has high-level encryption safety. In the Internet banking system, there is a RA server specifically handling application of users' certificate, the application process of the CFCA corporation and individual digital certificates as shown in Figure 3.

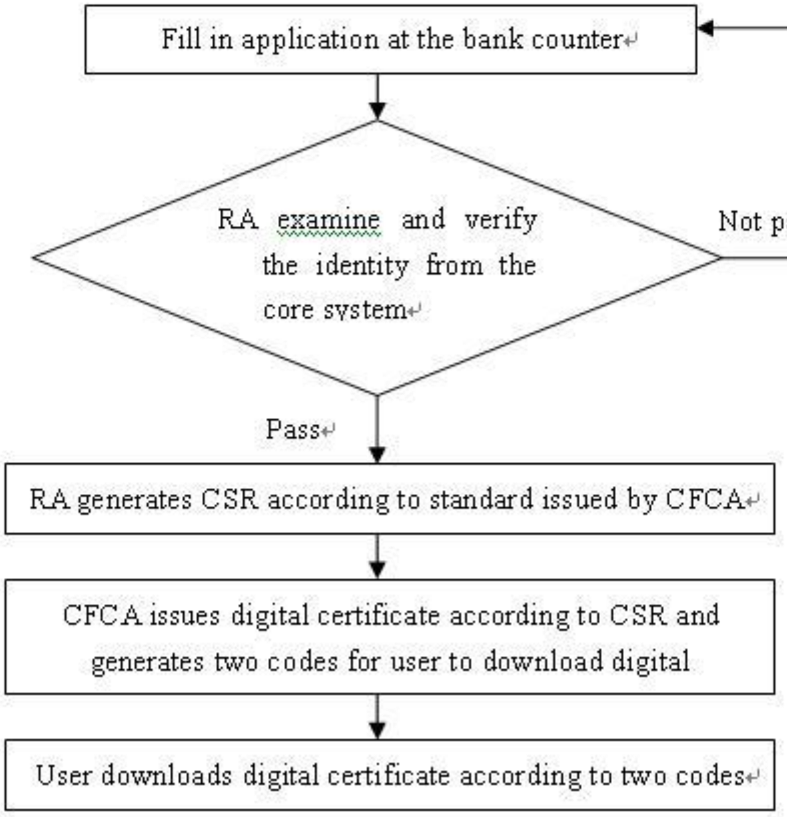
Fill in application at the bank counter
RA examine and verify the identity from the core system
Not pass
Pass
RA generates CSR according to standard issued by CFCA
CFCA issues digital certificate according to CSR and generates two codes for user to download digital
User downloads digital certificate according to two codes

Fig. 3. Apply for digital certificate of corporation and individual

The two codes generated by RA server are the application code and the verification code, and the user can download a digital certificate on the CFCA website according to the two codes on the personal computer, and also use the more secure USBKEY to store a certificate. The B/S pattern needs to call active/component to achieve signature operation, the client can call Microsoft CAPICOM by script; and also can call self-develop ActiveX application active.

(3)Main Function

As soon as the client and server install a digital certificate issued by the CFCA and verify the dignities of both sides, the bidirectional SSL communication will be built, in addition to the user's account number and password, which makes online business especially safe. The bidirectional SSL protocol not only verifies the user and server's identities, but also keeps sensitive data safe in the communication process, which means that it supports overall non-denial. Application of a CFCA digital certificate can avoid cheating on the Internet effectively; and verification identities is the most important problem in finance. The Internet banking system structure is shown in Figure 4.

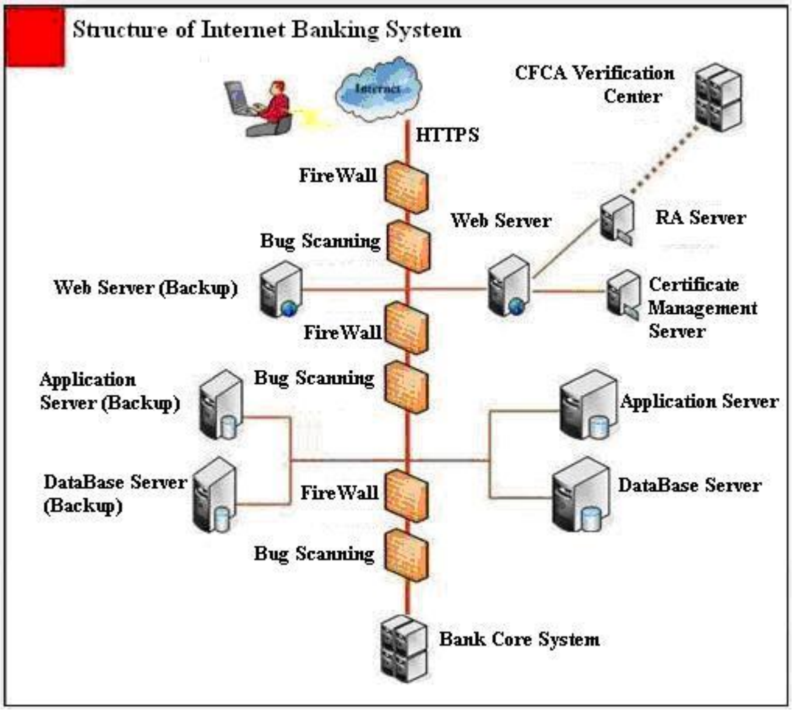

Fig. 4. Structure of Internet Banking System

4. Conclusion

The paper is mainly expatiating on the operation principles and functions of PKI technology in the Internet banking system, and discusses how to issue a digital certificate and its function. The CFCA digital certificate not only enhances the security of the Internet Banking system based on the PKI, but also enhances the usability and transparency of Internet Banking, which has improved the promotion and application of Internet Banking.

References

[1] Huang J H, Li J T. Key Factor of Internet Banking [J]. Systems Engineering, 2008,8:32-16
[2] Liang J, Wan C Y. Design and Application of PKI in the Internet Banking[J]. Computer Engineering.2004
[3] Eric Rescorda. SSL and TLS Designing and Building Secure Systems [M]. Addison Wesley Longman, Inc.2002.
[4] Gao Z X, Tu Y Q, Li Z X. Design and Implementation of PKI and RBAC-authorized Digital Certificate [J].Computer Enigeering.2006,8:34-2
[5] The OpenSSL Project [EB/OL]. http://www.openssl.org/
[6] Zhou Q, Yi C E. Key indicators for online-bank service quality[J].China Credit Card,2002,8:49-52.
[7] LiuJiayao, Zheng Xiaochuan, Yan Guillan. Core Java/Java programming Instances[M]. Wuhan: Wuhan University Press,2009
[8] Yang Dongyu. Syntax and Paradigm Dictionary of JavaScript[M]. Beijing: China Electric Power Press,2009