International Journal of u- and e- Service, Science and Technology
Vol.7, No.3 (2014), pp.45-52
http://dx.doi.org/10.14257/ijunesst.2014.7.3.05

Analysis and Solution for Virtual Personal Payment System of Online Banking

Jing Liu, Quan Cheng, Yihui Qin and Lei Feng

Beijing polytechnic, IBM (China) Investment Company Limited,
College of Beijing Union University, Beijing polytechnic
liujing0523@yahoo.com.cn

Abstract

Virtual personal payment system solution of online banking is proposed based on well known Public Key Infrastructure (PKI) in this paper. It will cover how to build a PKI architecture and online payment procedure on top of PKI. "Virtual" means the system solution will simulate online payment system design and implementation in real world. Mean while, the detail analysis will be given.

Keywords: *Electronic-Commerce, On-line Payment PKI*

1. Introduction

E-Commerce is booming increasingly these years, however, both merchant organization and consumer still remain concerns about security issue in online payment applications. As a result, the requirement to build a more secure and fast-response online payment system, which also safeguards confidential information, is becoming a hot issue for end user, including consumer and merchant. This paper will start from analyzing PKI architecture and individual payment procedure, and finally propose a "virtual" online personal payment solution for online banking, and "virtual" here refers that it will simulate the design and implementation of online payment system in real world.

2. Security Architecture

2.1. Transaction Security Requirement

The transaction security requirement for online payment system includes the following:

- Validation of transaction, in real world transaction activity, in order to ensure the legal justification, besides legal regulation, how to identify those who perform transaction need to be addressed technically; Also technical procedure need to apply to ensure data integrity in the whole transaction, so the data in transaction can be traced legally, which means the sender of the transaction cannot repudiate he/she is the digital transaction issuer, while same apply to the receiver.
- Security of transaction, the openness of the internet will potentially bring danger on online transaction. In a summary, it should fulfill following security requirements (ACIN).
  - Authentication: Prior to the transaction, first both entity who conduct transaction need to be identified to ensure both sides cannot be disguised.

ISSN: 2005-4246 IJUNESST

- Confidentiality: To cipher the sensitive information in transaction, so that it is useless even the data is captured by other party.
- Integrity: To ensure the data is received by receiver completely, and there should not be modified during the transportation, so to safeguard the fairness of the transaction.
- Non－Repudiation: Once the transaction is submitted. Both sides cannot deny the data they ever processed.

2.2. Key Technology Introduction for Online Security

Public key Infrastructure, PKI is the technology which popularly used currently in network security and its security services, and detail description is listed as following:

A)PKI

PKI is a common security infrastructure. It uses asymmetric cryptographic algorithm (public key algorithm) theory and techniques to provide network security service. It follows the rules of public key encrypting techniques to provide a set of security infrastructures for the transaction of electronic commerce, electronic government, on-line banking and on-line bond trading. Utilizing the security services provided by PKI, the users can make on-line transactions safely. PKI is a standard key management platform, which can be applied to all WEB applications, and it provides key and certification management, which includes encryption, decryption and digital signature request. Hence, PKI can be viewed as a combination of software and hardware system that can create issue, manage and revoke the public key certifications, and it also includes the whole process of security policy specification, the law and the personnel who are working with it. The certification is the core element of PKI, and CA is the core executor of PKI.

B)CA

CA, Certificate Authority, is an essential component of PKI. In a broad sense, CA should also include RA (Registration Authority), which is responsible for the registration, issuing and management of digital certification.

The main responsibilities of CA are as follows:

To validate and identify the identities of applicants; to guarantee the correct bindings of certification and user's identity by examining the applicant's credit, aim of appliance and non-deceptive identity;

To ensure the quality and safety of Asymmetric Key which is applied to signature certification, the length of private key applied to signature certification of CA must be over 1024 bits in case of not being decrypted, and private key must be generated by hardware and applied within it;

To ensure identification certificate subject is unique by reusing of certification name;

To issue and maintain the certificate recycling list (CRL) for on-line querying;

To monitor the whole process of issuing certifications;

To keep the records in log files which will be used as evidence in arbitration when transactions are in conflicts.

C)Digital Certificate

The file of a digital certification contains public key and the information of the public key owner which is also authorized by CA. As an authoritative, reliable, judicial third party, CA provides all kinds of digital certification services. The certifications from CA follows strictly open standard, *i.e.*, X.509 V3. X.509 certificate-based authentication technology for open network environment authentication is widely

applied and many web applications are implementing the X.509 certification. A standard certification of X.509 includes the following elements:

- Version of the certification;
- Serial number of certification, every user has a unique number of certification;
- Signature algorithm of certification;
- Issuing organization of certification, and naming rules follows the format of X.400;
- Validity of certification, common certification implemented the format of UTC time, which is from 1950 -2049.
- Name of certification owner, naming rules follows the format of X.400.
- Public key of the owner's certification (For more information on public key, see asymmetric cryptographic algorithm);
- Signature of the publisher's certification.

D)Secure Certification Architecture Based on CA

In the aspects of modules, CA consists of several functions, such as: RS, RA, CP and CRL.

RA is responsible for examination and approval of certificates. And it makes decision on issuing the certificate to the applicants, and also takes the full responsibility for the wrong issued certificates to the unqualified applicants.

CP is the organization of issuing certificates, which makes issues and manages certificates for the authorized applicants. And it is responsible for the consequences caused by mis-operation of the certificates, such as: confidential information disclosure, certificates issued to unauthorized applicants, *etc.*,.

RS is a recipient of certificates. It receives applications from users, and transfers them to CP and RA.

CRL takes records of the serial number of user's expired certificate for querying on them.

Recipient is working as an interface of CA services. And it provides face to face services of issuing and applying certificates. In the meantime, it can audit the certificates issued to the users, examine the data submitted by them and decide whether they can be issued with certificates.

3. PKI Implementation(Self-built CA based on the Bouncy Castle Open Source Framework)

To develop the functions of building CA, certification issuing and signed the certification by Bouncy Castle Open Source framework.

A)Building CA：

1)Generate public key and private key of CA

GeneratePairKeys.generaKeyPairByAlgorithm(keysize,ca_algorithm);

2)Generate certificate which contains CA public key and private key.

X509Certificate caCer = CertificateUtils.createCACert(caPubKey, caPrivKey, DN, validMonths, "SHA1withRSA");

3) Store certification objects into keystore.

caStore.store(caPfxOut,ca.getCapassword().toCharArray());

B)Issuing user certificate

1) Acquire the public key and private key of CA

```
PrivateKey caPrivKey = (PrivateKey) (keystoreCA.getKey("CApriv",null));
X509Certificate caCer = (X509Certificate) (keystoreCA.getCertificate("CA"));
PublicKey caPubKey = caCer.getPublicKey();
```

2) Generate key pairing of users

KeyPair pairKeysUserCer = GeneratePairKeys.generaKeyPairByAlgorithm(keysize, sign_algorithm);

PrivateKey userPrivKey = pairKeysUserCer.getPrivate();

PublicKey userPubKey = pairKeysUserCer.getPublic();

3) generate the users' certification object.

X509Certificate userCer = CertificateUtils.createCert(userPubKey,caPrivKey, caPubKey, caDN, DN, serialno, validMonths,"SHA1withRSA");

4. The procedure of "virtual" personal payment of on-line banking

1) Users are browsing products on online shopping web site.

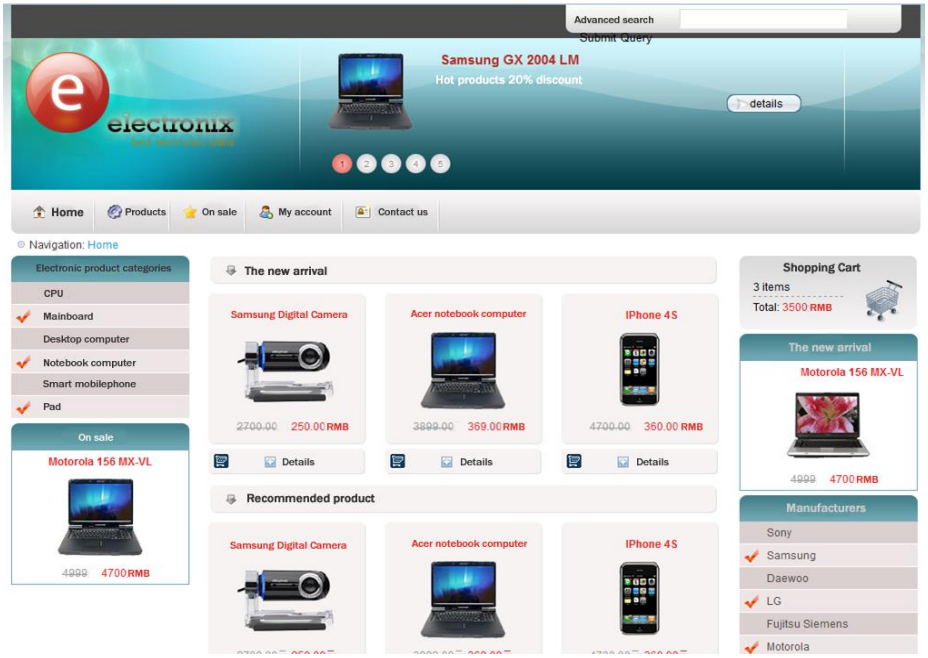

Figure1. Online Shopping Web Site

2 users are placing orders and make payment on the web site;

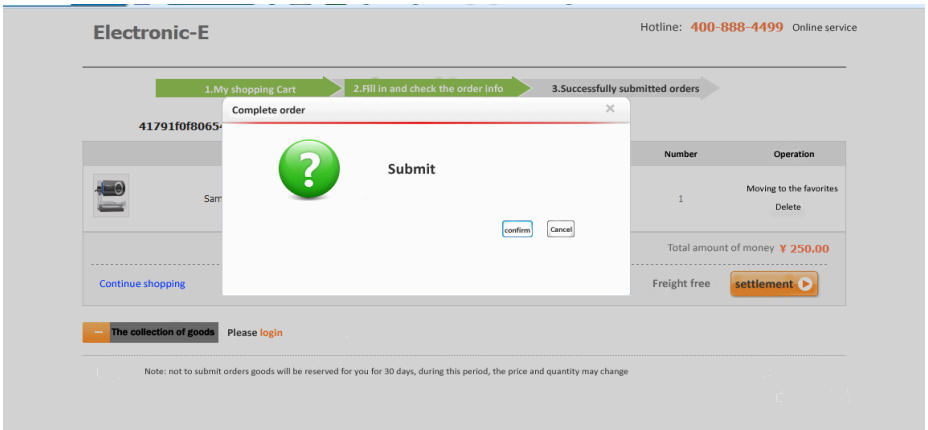

Figure2. Orders and Payment

3 users digitally signed on their orders and then transfer to the gateway of on-line banking payment system.

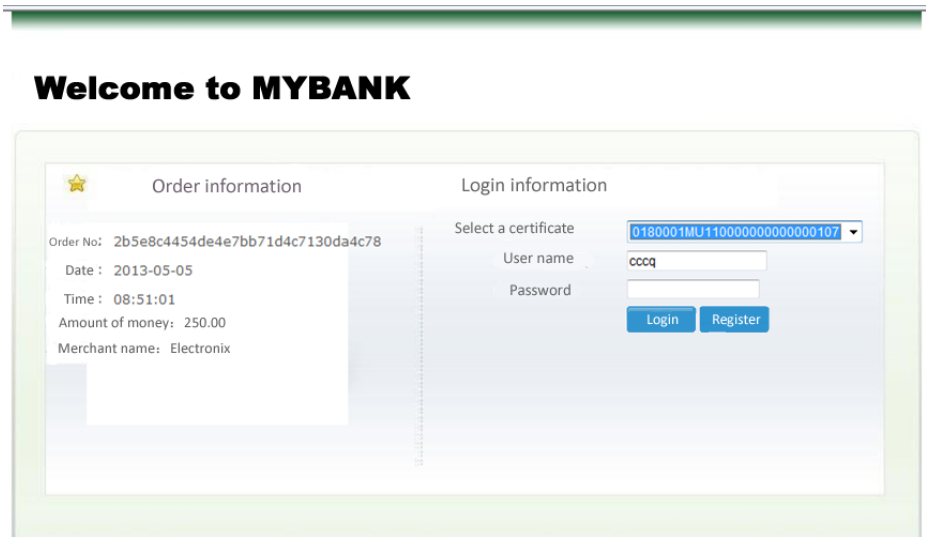

Figure3 On-line Banking Payment System

4 users login in the online payment gateway, and the gateway signed on the users' information.

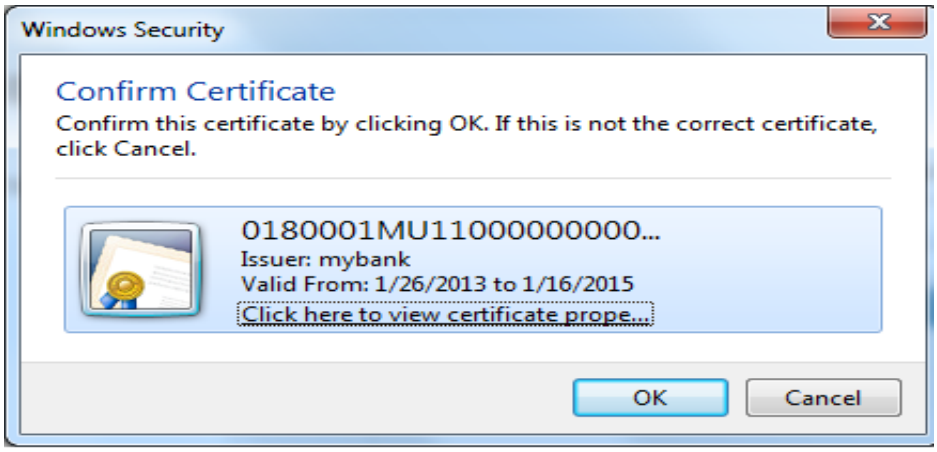

Figure4 Login Confirm Certificate

5 After logging in successfully, users enter home page of the payment gateway. Users submit their payment information (credit card number and password), and then the gateway will sign on the payment information.

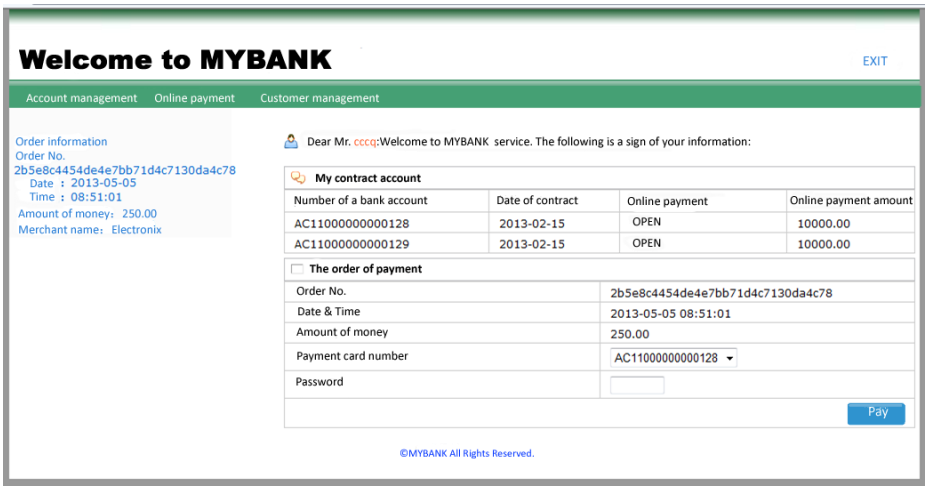

Figure5 MYBANK Welcome Page

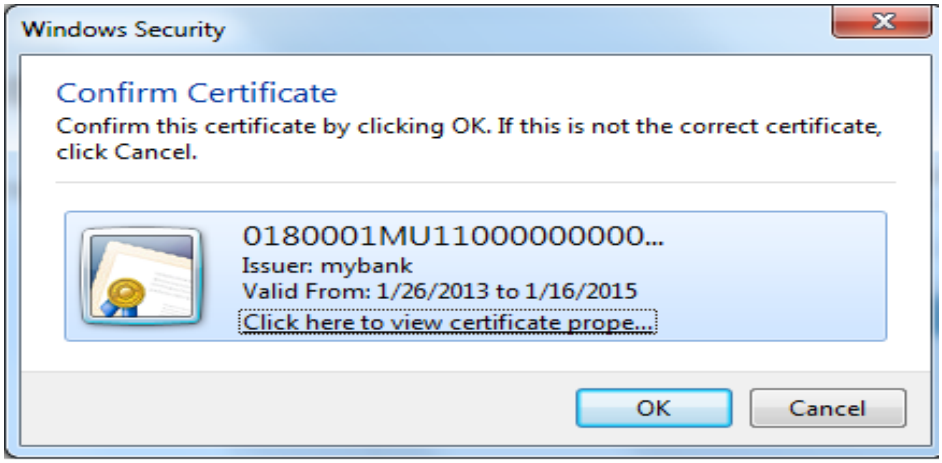

Figure6 Payment Confirm Certificate

6 users complete the transaction of on-line payment.

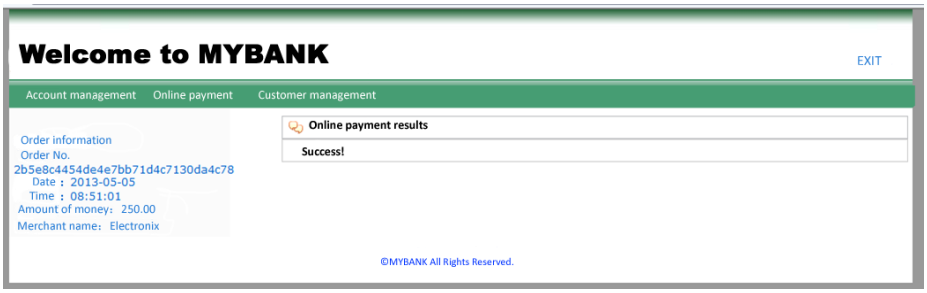

Figure7 Payment Success

5. Conclusion

The security issue of on-line payment is the bottleneck of the development of e-commerce. This paper introduces PKI security system in detail, furthermore, it analyze

common personal payment procedure, through which hopefully readers will understand how currency flow, business flow and information flow are combined to apply in E-Commerce. Based on the study of on-line banking payment in real world, a virtual environment is proposed to facilitate E-Commerce teaching.

References

[1] G. Horng, T. Chen and D.-S. Tsai, "Cheating in Visual Cryptography", Designs, Codes and Cryptography, no. 2, **(2006).**
[2] W. Diffie and M. Hellman, "Multiuser cryptographic techniques", Proceedings of the AFIPS National Computer Conference, **(1976).**
[3] B. Diffie, "New Directions in Cryptography", IEEE Transactions on Information Theory, **(1996).**
[4] C. Yeun and B. Mitchell, "How to identify all Cheaters in Pinch' s scheme", JWIS, **(1998).**
[5] D. Chadwick, "Smart Cards Aren' t Always the Smart Choice", IEEE Computer, **(1999).**
[6] T. Seideman. "Bar Codes Sweep the World", Invention and Technology, **(1993).**
[7] R. Housley, W. Ford and T. Polk, "Internet Public Key Infrastructure-X. 509 Certificates and CRL profile.

Authors

Jing Liu, she was born in Beijing in 1979. Her research areas cover the economics profession of E-Commerce, E-Banking, E-Marketing, logistic and Website design practice.

Quan Cheng, he received B. Eng degree in Space Craft Design and M. Eng degree in Software Engineering in Beijing BeiHang University in 1998 and 2007 respectively. He is a software engineer of IBM (China) Investment Limited. His current interest is Enterprise Content Management.

Qin Yihui, he was born in Beijing in 1978. His Research areas include electronic business and software architecture.

Lei Feng, he received his B. Eng degree in Electronic Information Science and Technology and the M. Eng degree in Computer Network from Beijing University of Chemical Technology (BUCT), China in 2004 and 2010 respectively. He is a teacher to teach the course of computer network.His current research interests on Computer Network Applications and E-commerce.