Study on Security Based on PKI for E-commerce of Statistics Information System

Min Liu
Northwestern Polytechnical University
(Xian University of Finance and Economics)
127 Youyi West Road, Xi'an, Shaanxi Province, People's Republic of China, 710072
86-029-85583871
minliu_0@126.com

Shudong Sun
Northwestern Polytechnical University
127 Youyi West Road, Xi'an, Shaanxi Province, People's Republic of China, 710072
86-029-88494371
sdsun@nwpu.edu.cn

Miaotiao Xing
Xian University of Finance and Economics
64 Xiaozhai East Road, Xi'an, Shaanxi Province, People's Republic of China, 710072
86-029-82332652
mt_xing@126.com

ABSTRACT
In this paper, issues about the trend of statistics information merchandizing, and the present situation of statistics information network and statistics information system security, are analyzed. Security construction scheme is put forward, which is appropriate to e-commerce of statistics information system. In the scheme, first, system framework of hierarchy PKI with three levels is established, and system composing elements and their function are studied, as well as flow chart of user certificate generation. Second, adoptable security protocols and hybrid key cryptosystem, are discussed, and one encryption way of providing confidentiality, integrity, and authentication is set forth. Finally ideas of key management for e-commerce of statistics information system are proposed. Security is the foundation of e-commerce of statistics information system, and PKI is the most feasible and effective approach to ensure statistics information security in open network, so the study is significant.

Keywords
Statistics information; E-commerce; Security; PKI

1. INTRODUCTION
In developed countries, such as America**,** Canada[1], statistics information is real merchandise. Giant statistics information databases in the e-commerce center of State Stat Bureau are linked to consumers who can get statistics products at any time via network, and added value and utilizing efficiency of statistics information resource have been greatly improved. E-commerce of Stat department is prospering. IDC predicted that trade volume of e-commerce would reach over 600 hundred million dollars in China last year[2]. The rising of e-commerce supplies a new method of getting statistics information to governments, enterprises, and users, who can access statistics products over online services and Internet/Intranet. So it is inevitable to develop economic commerce in China statistics department.

Statistics information network, formed by linking backbone of State Stat. Bureau to 31 provincial and 32 metropolitan statistics bureaus, and its 64 notes extended respectively to make it covering over three fourth of boroughs and countys, supports statistics transaction running. Sites facing-society built in 14 province statistics bureaus, and the one of State Stat. Bureau becomes more influential.

Statistics information network set up on China public network certainly exists security-hidden trouble. Statistics information system has built self-contained security system to ensure security on three layers of network, system and application. On network layer, computer house management, integrative wiring, secure equipment install and management enhanced, all kinds of security facilities including firewall and security evaluation system installed, original X.25 network changed into internal network to separate from external network. On system layer, regular upgrade and secure reinforce of patches made for all OS platform, user management policies, inbreak detection facilities, and network management software used to ensure system reliability and stability. On application layer, virus prevention systems installed, and PKI[3] with one layer built mainly to provide issuing of digital certificates and authentication of secure data transmission for direct reports of 5000 industry enterprises and 3000 real estate corporations, fifth census, third agriculture survey, and second general investigation of basic units[4]. All above lay well security foundation for e-commerce of statistics information system.

2. SECURITY SCHEME of E-COMMERCE of STAT. INFORMATION SYSTEM

2.1 PKI System Framework
State statistics department consists of 4 levels of statistics bureaus of state, province, borough and county, and its branches spread over China. Hierarchy PKI system should be established to ensure the security of e-commerce of statistics information system.

Statistics PKI system for e-commerce should be hierarchy of three levels. Root CA is built in State Stat. Bureau, responsible for certificate application, signature and issue and management of the next lower level CAs, and its own certificates are self-signed. The second level CAs should be built in each provincial and municipality statistics bureau with their certificates signed and issued by Root CA, and user certificates signed and issued by CAs of their provincial or municipality statistics bureau. RAs should be built in each provincial and municipality statistics bureau, and register sites where users register and

ICEC'05, August 15–17, 2005, Xi'an, China.

apply certificates built in all statistics bureaus except for subordinates of counties. Showed in Fig.1. All levels of CAs store and issue certificates by accessing LDAP servers.

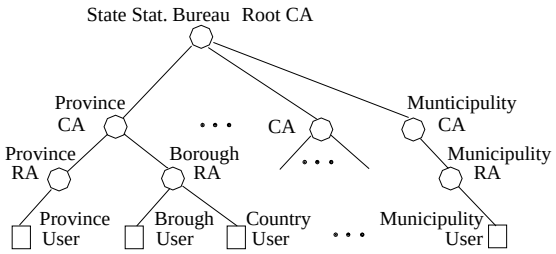

Fig.1 Statistics PKI System Framework

2.2 PKI System Composing and Procedure of User Certificate Generation Title and Authors

According to common composing of a PKI system [5], PKI system for e-commerce of statistics information system consists of:①Security policies: Methods and principles of encryption algorithm, defined by state statistics department, such as how to deal with keys and important data, and provide control grades corresponding to specific risk ones. State statistics department can develop its own CPS (Certificate Practice Statement), which specifies implementation procedure of security policies, and how to construct and run CA, and how to issue, validate, revoke, store and apply certificates. ② CA: A core in PKI system and a trustworthy entity that issues and revokes public key certificates and CRLs.③RA: An entity that is trusted by the CA to register or verify identity of certificate applicants and help to decide whether CA can issue them certificates or not.④ Key management: A system that supplies services like key generation, storage and backup, revocation, recovery and escrow.⑤Certificate issue system: A LDAP system from which certificates and CRLs are issued, updated and retrieved. ⑥ Application interface based on PKI: PKI must provide friendly API, which supplies all kinds of PKI services and functions of public key and private key, as well as operation interface of certificates and CRLs, in order to interact with e-commerce system about statistics information securely and trustworthily.

The procedure of user certificate generation is:① User comes to local register site and submits identity information to apply for certificate.②The register site accepts certificate request with entering registered information, and submits it to RA.③RA sends the certificate request to CA after verifying it.④CA signs signature certificate and encryption certificate after key pairs generated according to security policies and user type in different ways—customers may be provided with key generation software to generate their own key-pairs, and the key-pairs for employees may be generated by CA's trusted administrator. ⑤ CA sends user certificates (including the private keys for employees) to RA, and issues them via certificate issue system. ⑥ RA accepts user certificates and sends them to local register site. ⑦ Local site sends user certificates to user (Mainly by off-line). ⑧ User can inquire certificates from certificate management system, and apply to certificate revocation system for revoking certificates if something occurring. Showed in Fig.2.

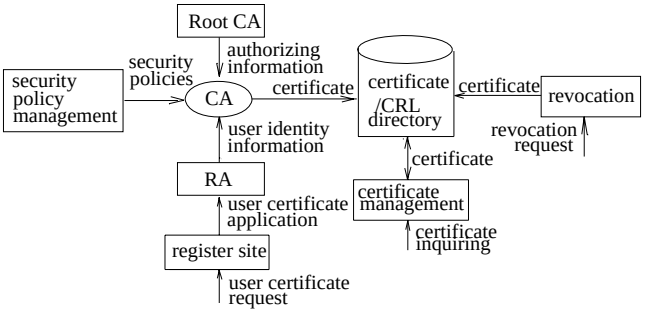

Fig.2 PKI system composing

2.3 Network security protocols

SSL[6] is an open protocol on TCP/IP transport layer to establish secure connection by key encryption. Encryption techniques, such as DES and MD5, are adopted in SSL to achieve confidentiality and integrity, and X.509 certificates are used to make authentication. From e-commerce application viewpoint, SSL benefits to merchant server, but can not ensure security of customer information. SET[7] is an open protocol on application layer to support secure finance payment by using cryptography. SET uses PKI and X.509 certificate standard, and defines format of encryption data and rules of transmission data during a process of card payment trading, and support authentication among consumers, merchants and banks, ensuring confidentiality, authentication, integrity and non-repudiation, especially ensuring not to expose credit card account information to merchants. Though SET has greater capabilities than SSL, it cannot be implemented without installing corresponding software in bank network, merchants' server and customers' PC, and its related costs are much more than that of SSL.

E-commerce system in state statistics department can link with banks by SET protocol, and with customers by SSL protocol. In addition, in statistics PKI system, SSL can be used during transmission of messages between CA and RA, as well as CA and LDAP directory server, to provide security in transport layer and to ensure secure transmission of PKI messages. This scheme not only obtains strongpoint of SET protocol, but also avoids installing electronic wallet software in customers' computers to make them more complicated.

X.509 certificates include a public key, identity of entity holding corresponding private key and CAs' signature, and its structure can be defined as following:

```
#define KEY_LEN 128

typedef struct _CERT

{       char    m_Version[2];
        char    m_Serial[10];
        char    m_Sign_alg_hash[10];
        char    m_Sign_alg_encry[10];
        char    m_Issuer[32];
        char    m_Validity_begin[20];
        char    m_Validity_end[20];
        char    m_Subject[32];
        char    m_PKey_N[KEY_LEN];
```

```
    char        m_PKey_E[KEY_LEN];
    char        m_Signature[KEY_LEN];
    char        m_Sdomin[20];
    char        m_Department[60];
    char        m_Signman[10];
}CERT,*PCERT;
```

2.4 Cryptosystem

Cryptosystem[8] can be categorized into two types of symmetric cryptosystem and public-key cryptosystem. In symmetric key system, both encryption and decryption share a common secret-key, and security rests on the secret-key rather than encryption and decryption algorithms. In public-key cryptosystem, each communicating entity has a key pair—a public key and a private key, algorithms and public key can be open, and security depends on private key that must keep secret.

Considering that public-key cryptography is not as efficient as symmetric method, such as DES with encryption at least 100 times [7] much faster than RSA, but the sharing and dissemination of secret keys presents implementation problems in keeping the shared secret-key confidential, a hybrid key cryptosystem can be adopted by e-commerce system in state statistics department. Rather than encoding the entire message with the slower public-private key pairs, it is encoded with a faster session key which itself is encoded with public-private key encryption. One way of providing confidentiality, integrity, and authentication is presented in Fig.3.

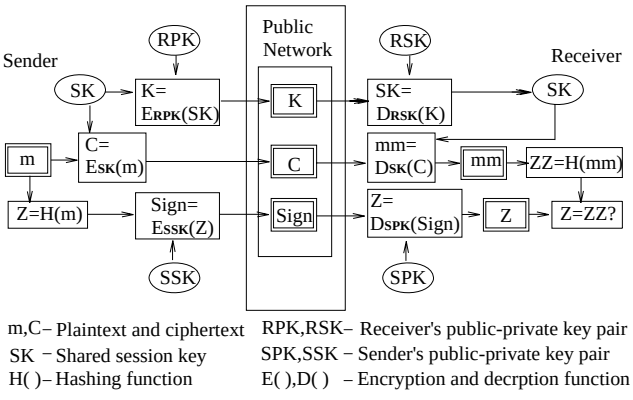

Fig.3 One Encryption Way

Main encryption ways in java are as follows:

```
// encryption by public key
  byte[] Endata=RSAEncrypt(publickey,src_byte);
  fos=new java.io.FileOutputStream("public_endata");
  fos.write(Endata);
//decryption by private key
    byte[] Dedata=RSADecrypt(privatekey,Endata);
//encryption by private key
  Endata=RSAEncrypt(privatekey,src_byte);
  fos=new java.io.FileOutputStream("private_endata");
  fos.write(Endata);
// decryption by public key
  Dedata=RSADecrypt(publickey,Endata);
```

One design scheme based on PKI showed in Fig.4.

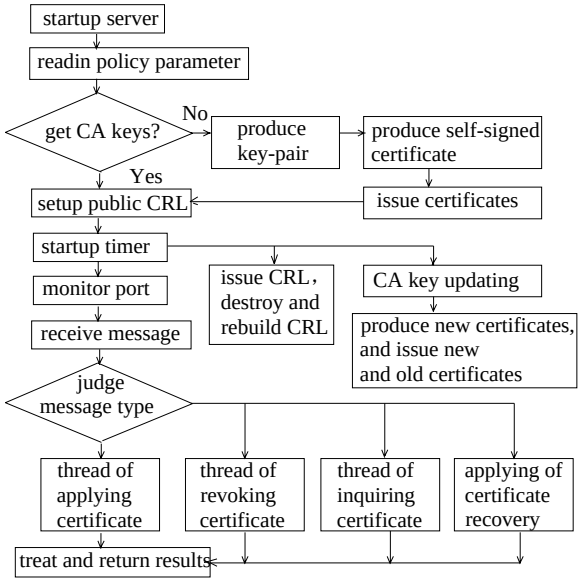

Fig.4 One Design Scheme Based on PKI

Encryption can also be made by Hardware technology in order to improve its intensity and firmness. Encryptor, product of integration of packet filter firewall and encryption, equipped many network cards and core software to realize combination of physical and logical network sections, is not only capable of high-speed network encryption, but also network security protection and control management. It adopts symmetric cryptosystem to achieve information transmission with confidentiality and authentication, and independent of any other application system.

2.5 Key Management

Key pairs can be classified into two types of signing and encryption according to their purposes, and there are different management policies.

A signing key pair is used for digital signature. The private key can never be copied and stored, since more than one copy makes non-repudiation and authentication impossible. If the private key is lost, a new key pair needs to be generated, and a copy of old public key can remain available to authenticate previously signed messages. This type of key pairs may have longer life.

An encryption key pair is used for encrypting and decrypting messages. A copy of the private key should be maintained to prevent loss of data if the private key is lost, and to decrypt previously encoded messages at any time. The public key needn't to be copied and stored. If the key pair is lost, a new key pair needs to be generated. This type of key pairs is usually used to send session keys, so they should be replaced frequently and have shorter life.

Customers should be allowed to generate and maintain their own key-pairs in order to achieve non-repudiation. But the private keys of employees should be placed in escrow with CA

because the system may need to decrypt data in emergency. Private keys can be also in escrow by key escrow agents, private key escrow[9] is the trend of security policies in e-commerce.

3. EPILOGUE

E-commerce of statistics information system will promote utmost development and utilization of statistics information resources. Security is its foundation, and PKI system is the most feasible and effective approach to ensure statistics information security in open network. Security model for Economic commerce of statistics information system cannot completely copy that in other industries. A lot of issues need to be further studied carefully, such as hidden security trouble, an appropriate security scheme including actual cipher algorithm and processing flow, technique of Internet EDI/VPN, XML, Agent[10] by adopting technology of network, software, and modern cryptology, etc. It's significant to study security based in PKI for e-commerce of statistics information system.

4. REFERENCES

[1] Mei Haiyan. *Enlightenment of Canada Statistics Information Industry on Developing China Statistics Information Industry* (In Chinese). Information Research. 2001.4:10-13

[2] 'Research on Statistic of E-commerce and Its Application' Project Team. *Series of Investigation Report of Statistic of E-commerce and Its Application* (In Chinese). China Statistics. 2002.12-2003.7

[3] Tom A. *PKI*. New York: John Wiley & Sons Inc, 2001

[4] Xu Tiefu, Zhao Mingxia. *Security of Statistics Information System in 21 Century* (In Chinese). Information Security and Communication Secrecy. 2001.12:20-23

[5] Ray Hunt. *Technological Infrastructure for PKI and Digital Certification*. Computer Communications, 2001,24: 1460-1471

[6] Frier A, Karlton P, Kocher P. *The SSL 3.0 Protocol*. Netscape Communication Corp, 1996.11.18

[7] Marilyn Greenstein, Todd M. Feinman. *E-commerce: Security, Risk Management and Control*. New York: McGraw-Hill, Inc, 2000

[8] Schneier B. *Applied Cryptography: Algorithms, Protocols and Source Code in C*. New York: John Wiley & Sons Inc, 2001

[9] Phoenix S J D. *Cryptography, trusted third parties and escrow*. BT Technology Journal, 1997, 15(2):45-62.

[10] Hu Chunguang, He Qi, Chen Mingyu. *A PKI System Based on Agent* (In Chinese). Microelectronic and Computer. 2002,11:29-32