Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(10):660-662

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Safety technology is set in the agreement of the application

Xiang-dong Wu[a] and *Jian Zhou[b]

[a]*School of Computer and Information Engineering, Central South University of Forestry and Technology, Changsha, P. R. China*
[b]*Machinery and Electrical Engineering College of Centre South University of Forestry and Technology, Changsha, P. R. China*

ABSTRACT

This article is illustrated in e-business SET, including the payment of the security agreement, few common safety technology, SET security, etc.

Key words: SET agreement; Safety technology; Application.

INTRODUCTION

Online payment security in electronic commerce is the core and complex Visa and Mastercard[1]. The joint development of the agreement, is SET for B2C mode of e-commerce, based on credit card payment agreement, it can achieve both parties to the identification and confidentiality of information, integrity and undeniable[2].

EXPERIMENTAL SECTION

Symmetric key for encryption
Symmetric key encryption algorithm is for a message encryption and the sender and receiver are in the same key encryption and decryption process. Its greatest advantages is encrypted and decrypted faster pace for about a lot of data encrypted, but the key management difficulties.

Asymmetric keys for encryption
Asymmetric encryption algorithm is an encryption and decryption using different keys, usually has two keys, called "public key and private key". If the public key to encrypt only by the corresponding private key to decrypt ； and vice versa. The greatest advantage is a symmetric encryption technology in key transport of the security problem, but they are very slow, only applicable to small amounts.

The hash algorithm
The hash algorithms produce information "fingerprints" that figures is one of the data is changed, the hash algorithms have three characteristics：One is able to deal with any size of information and a fixed length (160bit) summary of information. Second, has to be proactive. Three is a not reversal .

A digital signature
Digital signatures to be transmitted through the hash algorithm of a summary of information, then use the sender's private key encrypted and the results to the original message, that the information. In digital signature set in a special service, when sending order to cardholders business information OI and payment instruction PI, must ensure that the PI, and OI.

Figures envelope
Figures in order to solve the envelope is to replace the key issues of technology, combined symmetric encryption and asymmetric encryption. Use the sender random the symmetric key encrypted data, and will generate the cipher text and the key itself with a recipient's public key encryption （called an envelope） and send ； Receivers first with his own private encryption key to decrypt an envelope, and then get a symmetric key using a symmetric key to decrypt data. This will ensure that every time the transmission of data can be selected by the sender of a symmetric key.

Digital certificate：
In exchange for the parties to prove their identity, the third party is the center for authentication and digital certificate. It is the center of the parties to the identity of the documents, it is a digital signature of the CA certificate (the public key holders) personal information and the public key file.

RESULTS AND DISCUSSION

Confidentiality
SET in the transmission of data encrypted data processing, to protect confidentiality of sensitive information and personal information to prevent intentionally or unintentionally attack or leakage. In a network of the security environment, to ensure data security, the need for the encryption technology and key management. set in a number of the use of symmetrical and asymmetric encryption and the two types of algorithms to provide data to the confidential nature.

Authentication sexual
To ensure the data is really from that of the sender, receiver can use of digital signatures and digital certificate to authenticate, such as follows.

Entity authentication
Digital signature requirements for a trusted third parties participant (CA) provide digital certificates to ensure that public key of an entity of the electronic (CA certificate by the digital signature) kept in the entity in the computer. Receivers use of books to verify that the sender's public key, it is true that original information ： not (data integrity) ； information is only by the private key of the owner to prove the signature (entity) ； a third party for the signing of the information is key to the legitimate owners. Therefore, a digital signature of the uniqueness, the hash value with the public key to the sender and the sender is a sign of the sender.

Cardholders authentication
Cardholders certification issued by the ca cardholders public key and the corresponding order. mail and telephone, and the specific to verify the identities of the cardholders and account the effectiveness of the theft. Similarly, the effective card account number and expiration of the unauthorized individuals may try to make electronic commerce transactions, the user and the mechanism will reduce the accounts with the possibility of fraud and payment processing costs.

Merchant authentication
In special need to verify the businessmen's certificate request and if, through the merchant CA (MCA) a certificate to provide business, the certificate with the specific effective agreement for cardholders and the payment gateway by verifying the signature of the business certificates and certificates to prove the effectiveness of the chain business. By the certificate, can confirm a merchant. business sponsorship.

Payment gateway authentication
Payment gateway of the certificate is from the payment gateway CA (PCA) issue, cardholders use the payment gateway of the public key to encrypt a symmetric key, cardholders system need to be able to verify the payment gateway. try to cardholders provide the payment gateway encryption system, cardholders need to verify the certificate and make sure that the payment gateway is illegal, so as to guarantee the payment of the cardholders that the confidentiality.

Data integrity
Data integrity guarantees from the data is actually making use of all the data from the transmission of data integrity(is the hash value) to materialize. The integrity of the data values from the sender and receiver to the recipient to verify the completeness by comparing the value data are manipulated. A digital signature is defined as an additional data element and allows the recipient to verify the data source and integrity and tamper with. to prevent counterfeiting. On SET, a digital signature is encrypted with sender make of the hash value for the hash value in the

source data integrity.

CONCLUSION

In short, set agreement with encryption and digital certificate, a digital signature for, can verify the authenticity of the cardholders and to provide information of a confidential nature and guarantee its payment of integrity.

Acknowledgements
Project of teaching innovating of Centre South University of Forestry and Technlogy(2011);Project of postgraduate students teaching innovating of Centre South University of Forestry and Technlogy(2012J003); Conditional innovating project of science and technology department of Hunan province (2012TT2048); Open Lab Project of Centre South University of Forestry and Technology of China (KFXM 2012029).

REFERENCES

[1].Jian ZHOU,Lijun LI, Ye Xue. *Advance Journal of Food Science and Technology*, **2014**, 6,130-134.
[2]. Jian Zhou, Lijun Li,Lei Lei. *Journal of Chemical and PharmaceuticalResearch*,**2014**,6,153-155.
[3]Lin Feng.E-business technology and application security.1st Edition,Beijing aerospace university press,Beijing,**2013**,30-40.
[4] Zhou Hua-xiang.Safety net and e-commerce.1st Edition,China power press,Beijing,**2012**,56-64.