Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(10):652-654

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

E-commerce "identity" — — a digital certificate

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 describes the principles of digital certificates and the digital certificates in e-commerce applications, such as what is the digital certificate, the principle of 'digital certificate, a digital certificate type, authentication process, also points out role of digital certificate.

Keywords: E-business; digital; certificate.

INTRODUCTION

With the rapid development of internet, e-commerce has become a new business model. Because of the internet's an open and all other factors, security has been the electronic commerce development bottlenecks, and many people don't want to make online shopping and pay the main reasons[1]. To be on the network security in electronic commerce activities, must take encryption and digital signatures, the key management, firewalls and other security. Of digital certificate used to verify a user's identity and access network resources, the electronic transactions, if both sides produced their digital certificate and deal with them, both parties do not have to worry about the status of truth[2,3].

EXPERIMENTAL SECTION

What is the digital certificate

Internet transactions is one of the problem of identification, this involves two issues ： if it is an identity, the third party will deal of counterfeiting and to destroy, corrupted by such party's reputation or misappropriation by such party of the product. An identity to identify, both parties to prevent "suspicious of each other". second, "non-repudiation", both parties should be responsible for his actions must be the responsibility of information to the sender and accepter cannot be denied. in the capacity to identify, if there is to deny, it is the basis of. So on the internet and digital certificates for identification of individual or organization's identity provide a means.

Digital certificate authentication and certification, usually short, for the certificate with the driver driving licence or other similar routine id card, it includes a public key and the corresponding private key for the ca and the identity of the content of the digital signature. The signature of the ca certificate can ensure the integrity and truthfulness, certificates are generally follow the format of TTU (the international telecommunication union) make x 509 standards. it can give you a confirmation. an e-mail message or a page from they claimed that the place. a digital certificate actually a few figures in the file is used to the figures on the internet users of the confirmation or resources, it also ensure that online exchange of both parties to the security and mutual trust。

Digital certificates to be done in two and it can be used to validate its owners — — an individual and the web site,

the network resources is really their ； Second, to protect the online exchange data are not to steal or tampered with. a digital certificate and identification process is similar, we made a trusted third parties institutions to provide your personal information, and then follow the procedures to obtain the certificate. the third party organization is known as the center of the ca. The centre to confirm your personal information is sent to you are a digital certificate. a digital certificate contains a number of information, such as the issuance of certificates, certificate issuer, etc. as a digital certificate used to authenticate a document or software that the identification information are safe in the certificate to the other party to establish a trust relationship.

The principle of 'digital certificate

Digital certificate that the public key cryptography system, with each other matching the key for encryption and decryption. a key like a single encryption device, not two keys are the same, this is why a key can be used to identify a user's identity. The key only with their work can is called, a private key and another is public key. The public key encryption, only with the corresponding private key to decrypt, and vice versa. Anybody can get your public key, but your private key can only do you have and never let the others have. in public-key password system, common the RSA system.

Digital certificates to the public key publications and exchange of information technology process more automatic. When you on your computer or server to install digital certificates, your computer or web site would have his own private key. with the private key corresponding public key figures as part of the certificate on your computer or web site, anybody can get. When a new computer trying to your computer to exchange information, it will be able to access your digital certificate and get your public key. The computer uses of your public key to identify you and security socket floor SSL to encrypt it would like to send your information. only your private key can open this information, so when this information on the internet can be seen on sending or tampered with.

A digital certificate type

The present definition of certificate and a lot, such as x. 509 certificates, certificate and the WAP WTLS PGP certificate, etc. but most of the certificate is the use of x. 509 v3 public key and the public key certificate application is very wide, according to the scope of application, divided into five categories.

Personal digital certificate

Certificate containing any personally identifiable information and personal the public key used to identify the holder of the personal identity certificates. the number of security and the corresponding private key Ikey IC card or storage in which individuals on the internet for the contract sign the bill, order, and input audits, operation, information permission for such activities. an identity.

The establishment of a digital certificate

Certificate contains corporate information and the public key used to identify the certificate is a corporate identity. the number of security and the corresponding private key card, and stored keynet for business on the internet for the contract sign the bill, the stock exchange, exchange information. Making.

The signing certificate

Certificate containing any personally identifiable information and personal signature of the private key used to identify the holder of the personal identity certificates. the signature of the private key to the storage keynet to individuals on the internet for the contract sign the bill, order, and input audits, operation, information permission for such activities. an identity.

The establishment of the signing certificate

Certificate contains corporate information and the signature of the private key used to identify the certificate, a corporate identity. the signature of the private key to the storage keynet to the internet for the contract sign the bill, the stock exchange, exchange information.

Equipment, and digital certificate

Certificate contains a server information and the server's public key used to identify a server certificate of identity. the number of security and the corresponding private key card, and stored keynet the server to index, are used chiefly deal, for the purpose of web server to client and server have to pay for business information, make sure that both sides of the truthfulness and security.

RESULTS AND DISCUSSION

Authentication process
X.509 contains. specifying single, double and three to three alternatives such as authentication procedures.

One-way authentication
One-way process involving the news from a user a to b another user for one-way. received by the news made a check ： 's a rank, that information is made from a second test. The news was transmitted to b. three is to ensure the integrity and the information.

Dual authentication
For two-way authentication, b in addition to the need to verify the one-way authentication three content, a, b responses received news that we should examine the following three content： a, b's and b generated in response to the news is true. The second is the validation message is sent to a. three is to ensure the integrity and the response messages.

Three to the user authentication
A and B for two-way authentication, if B also need to verify a definite received his response message will be three, the authentication. In order to prove this point A to B to sign a copy. Sending。

Role of Digital certificate
Data encryption technology is the role of information security is very important, but a digital certificate is quite new. in conventional log, even if a man with password access and sends the encrypted message to you, you still do not know the man. A digital certificate, you can identify and verify that your exchange information, and use of conventional password authentication way can steal against others your password and tamper with data, and it is very difficult to know who did it. And other forms of security measures, the more secure digital certificate. Ago and have already mentioned, a digital certificate is a third-party certification issued by the centre to center. The authentication of the background, employment, credit and other materials to audit. a digital certificate or a passport, driver's license as easy as it was forged, so it is safer. Use digital certificates to send the electricity, like to sign papers, plus appropriate PKI, a digital signature even more than a handwritten signature more secure. Some of the big corporation or institution, for example, the bank will issue of digital certificates. Thus, the organization itself becomes the center, they may set up a stringent authentication procedures to ensure the credibility of the registration process.

CONCLUSION

Identification authentication and digital certificate technology development and application for internet transactions to provide security. a digital certificate used depends on the ca and the construction and development, because the machine ca is to verify, so only to build an authority of the ca and efficient system can improve the efficiency and to better guide the development of e-commerce applications. However, because of the ca certificate of administrative bodies in a set of commercialization, so as a commercial, and prone to various ca the contradiction between a client authenticates the multiple questions, will seriously impede the planning and development of e-commerce. Therefore, in our country, as a digital certificate main applications of electronic commerce certification system, the government should strengthen guidance and co-ordination of the CA and the construction of more effective, pragmatic to the direction of china, thereby promoting E-business fast, healthy and orderly development.

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

REFERENCES

[1] Jian Zhou, Lijun Li,Lei Lei. *Journal of Chemical and PharmaceuticalResearch*,**2014**,6,153-155.
[2] Zhang Zhuo-qi,Shi Ming-kun.Online payment and the internet to financial services,1st Edition, Chinese northeast financial university press, Haerbing, **2011**, 55-59.
[3] Lei Xin-sheng.E-commerce safety technology,1st Edition,National defense industry press,Beijing,**2012**,35-40.