Association for Information Systems
AIS Electronic Library (AISeL)

Eleventh Wuhan International Conference on e-Business

Wuhan International Conference on e-Business

5-26-2012

Research on Authentication Technology of E-Commerce

Hongwei Hui
Management Department, The Engineeing Technical College of Chengdu University of Technology, Sichuan Leshan, China, 25560317@qq.com

Ying Zhang
Management Department, The Engineeing Technical College of Chengdu University of Technology, Sichuan Leshan, China, 1914877248@qq.com

Research on Authentication Technology of E-Commerce

Hongwei Hui [1], *Ying Zhang* [2*]

[1] Management Department, The Engineeing Technical College of Chengdu University of Technology, Sichuan Leshan, China

[2] Management Department, The Engineeing Technical College of Chengdu University of Technology, Sichuan Leshan, China

Abstract: With the continuous development of society and the requirements of economic integration, E-commerce is becoming a major economic model in the market , But it is facing a huge security problem in the course of its development。 In this paper it is starting from overview on e-commerce and problems to be solved on development of e-commerce :authentication is a technology of the most basic to ensure the e-commerce transactions, Then it is discoursed the development of e-commerce authentication technology, It is a digital certificate, And center of the digital certificate is a CA technology , Main technical departments and their function for CA technology is PAA,RA,CP and PKI, Third it is discoursed main basis technology of the CA system technology,Including digital envelope and digital signature and dual digital signature , Detailed analysis their working principle ,In the end I analyze direction for future research of e-commerce authentication technology: The dynamic password of the mobile phone software is most likely to be one of the large-scale popularization of the next generation of internet authentication technology.

Keywords: e-commerce1, authentication2, CA technology3， future directions4

1. INTRODUCTION

With the continuous progress and development of society, Recently electronic technology as the core of the trade is becoming increasingly popular in virtual network. And it also continue to be recognized by various sectors of the community. However, in the process of development of e-commerce, But inevitably there is a problem of authentication, And this issue has become the current development process of e-commerce solutions and the most difficult problems to be solved.

2. E-COMMERCE OVERVIEW AND PHASE OF THE DEVELOPMENT PROBLEMS IN ITS PROCESS

2.1 Overview on e-commerce

E-commerce base on electronic technology as a core technology, It change the original way of direct transactions between people, To break the existing national and regional obstacles and barriers between by them,To produce a global, integrated, networked existence. Simply, E-commerce is the way through low-cost operation, Allows buyers and sellers to achieve efficient operation by electronic business and trade activities.

The most striking feature of e-commerce is a computer network as a platform and infrastructure, It can be permitted by law and regulations to conduct business activities within the scope.

With the continuous development of e-commerce, The biggest problem is the security problems in the whole process. In many cases, E-commerce security problems are solved by authentication technology. Therefore, With the continuous advance of e-commerce, Authentication technology for its increasingly has becoming high requirements and more in-depth。

* Hongwei Hui. Email: 25560317@qq.com , Ying Zhang. Email: 1914877248@qq.com

2.2 Problems to be solved on development of e-commerce

In the course of the entire operation in e-commerce, The whole process from the buyer selection of goods to commodity trading depend on electronic data to display transaction information,and the exchange of transaction information between buyers and sellers. That is, All of l factors about exchange of information on Commercial trade in the traditional , liquidity factors and product delivery as well as last sale realize becase of network platform,Therefore , Establishment of an effective payment platform, Authentication system and logistics system for quick and easy are directly restricting the development of e-commerce. Of course, this is the stable development of e-commerce plays a decisive three key factors.

On the above cited factors in these constraints, Authentication is the most basic of a technology to guarantee the security of e-commerce transactions, Becase of only perfect authentication technology systems can really ensure the Smooth operation and completion of the e-commerce[1,2]. The existence of the authentication technology can effectively guarantee that the integrity, confidentiality, and controllablethe of transaction information .

3. THE DEVELOPMENT OF E-COMMERCE AUTHENTICATION AND KEY TECHNOLOGY DEPARTMENTS

3.1. The development of e-commerce authentication

It needs Identification and recognition of identity like the identity of human communication on the Internet , The sign about security of online transactions in the passports and identification is the digital certificate[3]. Function of the digital certificate is to provide proof of identity of both parties for transactions on the network. The so-called digital certificates mainly refers to a public key files, This key documents is authorized by Digital Licensing Center.

E-commerce over the Internet is to achieve a simple and efficient trading, Guarantee their safety is mainly through a series of encryption to achieve and guarantee,Of course, Embodiment of the security need to use to help identify the status of digital certificates, While the digital certificate is a CA certificate technology.

CA technology is the abbreviation of certificate authority, It is the hub of the digital certificate authentication, The main working principle of this technique is Through third-party authentication to achieve certification of their status, This service center.'s mainly task is a management of trading parties about application and acceptance as well as issue[4,5] . checking the information and cancel the digital certificate. The operation of Certification Center is mainly through this series of GPS to achieve operational certification procedures. CA technology has a very important role in E-commerce, It can be verified by the number of its special function testing the legal authentication whether buyers or sellers in online transactions , And who holds a valid certificate issued by a certificate, Such measures can prevent and contain some malicious tampering wanted for illegal business practices and business fraud in time[6] .

Continuous development of e-commerce is continuing to set new and higher requirements for network security. Because of e-commerce can continue to push forward the construction of the Internet trading environment, Of course, in the creation of their trading environment, But also for enterprises unexpected commercial profits. In 1999 China established the China Telecom CA security certification system, This is our first CA Certification Center, To June 2006, China Financial Certification Authority is formed, This indicates that China has started work on the CA's certificate. Since then, CA certification behavior is expanding growth. the "People's Republic of China Electronic Signature Act" are also awarded in 2004. This makes e-commerce transactions in authentication technology have more strict legal norms, It is to operate more normative.

3.2 The mainly technical department of CA system technology

- CA system technology policy approval body is the PAA, Its main function is to create a variety of PKI

Policy, And it (PCA is a specific department of PAA policy) issued a public key certificate to subordinate PCA, It create various forms of PKI security policy,CA monitor the behavior of PCA activities . In connection multiple PKI trust domains, Bridge Certificate BAC is the core , It is a bridge between all trusted domains, Helping in different regions of the CA issuing a certificate, And it establish a cross-trust certificate policy, Forming to-one mapping relationship beween Trust Domain Policy and Bridge CA Certificate Policy.

- Audit authority departments of CA systems technology is RA,The abbreviation of Registry Authority, RA is exists as part of CA authentication technology system, It has the following functions: Application for a certificate, download and approval,It can provide authentication services for the entire system .
- The Certificate of operating departments of CA system technology is CP, The abbreviation of Certificate Processor，As a part of CA system technology, Its existence primarily service for the readers who have been authorized to apply for , It undertake all the consequences that will bring about at the course of their operations may produce . Of course, including those applications who have been compromised by a certificate issued.
- The public key Infrastructure of CA systems technology is PKI, The abbreviation of Public Key Infrastructure, PKI is a functional departments primarily Providing such as digital signatures and encryption services for all users of e-commerce, It is generally the key management in accordance with established in the Operation and function of the implementation process[7]. Simply, PKI is the infrastructure to provide security servic, Of course it is the core of information security technology in the whole system, It is a Basic and critical technology in e-commerce. PKI-based technologies including the following forms:they are encryption, digital Signature , digital envelope ,double figures and so on.

3.3 The main basis for technical of CA system

3.3.1 Digital envelope

- Digital envelope technology is not a simple type of technology, But it combine with the advantages of public key technology and a secret key technical to integrated to form a new technology, It can effectively solve distribution of difficult problems which the secret key occurred during its the release occurred , It also avoids consumption of public key encryption in the length of the question, It also avoids time-consuming public key encryption issues It also avoids time-consuming of the public key encryption issues[8]. When it combine with the advantages of public key technology and a secret key technical, It can effectively play its comprehensive and efficient performance, it is effective to ensure the safety and reliability of information. It is divided into the following main steps when the digital envelope technology is to help to achieve authentication: First, it first generate a symmetric key when the sender sent the information to be built, Then it use this symmetric key to send messages by encryption way; The second step, The sender encrypt symmetric key generated in the first step by the recipient's public key and it generate digital envelope, The third step, It transfer he digital envelope the newly generated and the structure of the sending message to the recipient; The fourth step, when the recipient receives the envelope, They decrypt the password through their own private key, Finally, They get the transmission key has been encrypted, Followed by the symmetric key is to effectively interpret their messages,They get the information by the sender at last[9].
- Digital envelope technology get real information conveyed in the dual interpretation of public key and symmetric key , In the use of public key encryption technology, It can play itself effectively because the public key has flexibility of technology, The symmetric key has the relative short features , And making it in a very short period of time will be conveying information and interpretation. And the demand of this technology, It uses a different symmetric key when the delivery of information every time, Thus this greatly increases the safety performance of the system.

3.3.2 Digital signature

- The mainly use of digital signature technology is to ensure the integrity of its information y during transmission on the one hand, The other hand, it provide sender authentication for the Information receiver[10,11]. In the digital signature technology has the signature key and private key. The former is used to verify the legitimacy of the key, It has the openness, Thus it ,become the public key; The latter is used to keep secret, It has some kind of function to keep secret. The main steps in the implementation process and the steps are as follows in the digital signature technology[12]: First, the message sender who must use a certain algorithm organized the information being sent into summary information , And the sender uses the private key to sign its written summary of information at this time, Second, the message sender r will send the summary information has been signed; Third, when Any receiver with the sender using the same hash function can be reduced to summary information, By using the public key the recipients to verify the information received, To achieve to confirm the identity of the sender and to check whether the information during transmission is being changed.
- A digital signature is the most feasible means of using to communicate information and to ensure the validity of the information in e-commerce era,It form based on the traditional signature of extension and development . Therefore, in this sense, Digital signature technology has some kind of writing, the legal norms of the original itself, However as the digital signature itself owning the characteristics is as same as the written signature, And with the limitations.

3.3.3 Dual digital signature

Dual digital signature technology is a major technology to effectively transfer information among buyers, merchants and banks. Its use ensures the integrity of information and the reliability of authentication in the process of information transfering, And it can effectively prevent denial the case occurred during the transaction. Specifically, In a trade, When buyers purchase goods, He needs to send business-related information about purchasing and payment to seller (The buyer's payment account in the bank), But buyers do not want to be seen directly the the payment account information through information by the seller, At the same time, Buyer is not willing to allow banks to see the related to purchase history information, In this case, You can use dual digital signature technology to implement and complet of the above requirements. Dual digital signature technology include the main steps like this, The first step, the buyer were to send a message to banks and the seller, Information summary 1 and information summary 2 were generated respectively, After it finished, Buyer use information Summary 1 and information Summary 2 to generate information Summary 3, And at this time buyer use the private key to encrypt the information summary 3; The second step, the buyer will send information summary 1 ,information summary 2 and information summary 3 to the seller and bank at the same time, Sellers can not see the information summary 2, The bank can not see the information summary 1, The third step, when the seller receives information, Summary of new information are generated form information summary of information 1and information summary 2 , This is a summary of information 3 to verify using the public key, Through this form to verify whether the information was changed during transmission is being changed and the identity of the sender information. The bank also used the same method.When it receives the information,

4. TRENDS OF CA SYSTEM FOR E-COMMERCE AUTHENTICATION TECHNOLOGY

Development of electronic commerce will inevitably provide a wider space of development and development of the market for authentication technical CA system. . With China's accession to the WTO, Development of domestic and foreign economies are growing rapidly，The degree of cross-development is deepening, Only the form of e-commerce trade is in line with international requirements when they integrate with each other to a certain extent, which will require the development and support of CA systems In this course. Thus, The development of China's e—commerce CA system will show the following characteristics :

4.1 Trend for internationalization

With the rapid development of China's economy and China's accession to the WTO, The tightness of China's economic development and the world economy is more and more in-depth, We can not but take into account international users in the development of e-commerce in China, Thus e-commerce must walk the road of international development. This is bound to the development of CA systems show cross-development trends: Domestic and foreign CA system technology are in cross-development .

4.2 Trend for commercialization

Network is a virtual world, Thus it is not easy to establish a trusted trading platform, As a CA system technology, it is different from the constraints of legal, and also it is different from the mandatory of government's management, It has characteristic of contract , The existence of this feature is the use of mode of commercial operation. Thus, CA system technology is necessary to the development. of commercial operation.

4.3 Directions for future research

Popular authentication technologies have its advantages and disadvantages: PKI technology is mature, But it subject to the constraints of cost and ease of use, Its difficult to become a popular program.

Mobile dynamic password is an installation of the client software on the phone, With the development of mobile Internet and the growing popularity of smart phones, More and more mobile phones can be able to install the software , Users will cultivate a good habit to use the mobile client software, Mobile dynamic password is a program of high security, low cost and easy access , Mobile dynamic password technology will be the direction of future development, It can not be said to be the most perfect solution, The dynamic password of the mobile phone software is most likely to be one of the large-scale popularization of the next generation of internet authentication technology.

REFERENCES

[1] Guan Jun. (2010).Applied Research on the Mechanism of Digital Certificate Authentication, Informatization Research

[2] Cao Wang.(2010). Design and Implementation of the General Rights Management on Digital Certificates,Coputer System and Application

[3] He Fang,Wang Ruchuan.(2009). Authentication Technology of P2P Based on PKI, Computer Technology and Development

[4] Xu Xiaoping,Yin Yingyu.(2006). A Program of Authentication Model Based on Digital Signature, Computer Technology and Development

[5] Li Yuku,Zhang Deyun,Zhang Yong.(2001). Analysis of Authentication Mechanism and its Security,Application Research of Computers

[6] Gao Jianhua. (2007).Analysis and Research of E-Commerce technology: Computer and Digital Engineering

[7] Zhao Wenqing,Wang Dewen,Song Yu.(2003). Implementation of Digital Signatures and Digital Envelopes on PKI , Journal of North China Electric Power University

[8] Feng Dengguo.(2001). Public Key Infrastructure - Concepts, Standards and Implementation:Beijing:Qinghua University Press:5-36

[9] Chen Bangwen,Chen Xu,Guo Wenping,Chen Ying.(2010). Design of Secure communications program on Digital Envelopes and Digital Signatures , Journal of TAIZHOU College

[10] Qing Sihan.（2001). Cryptography and Computer Network Security:Beijing:Qinghua University Press:65-72

[11] Yang Bo.(2002). Network Security Theory and Applications: Beijing:PHEI:145-160

[12] Xie Hongyan. (2007). Security problems and countermeasures of e-commerce: Journal of Harbin University of Commerce（Natural Science）