The Security Model of Electronic Cash under Abnormal Situations

Liping Zeng, Lina Zhao, Xuefei Yan
Zhejiang University of Technology, Hangzhou, 310023, China
email: 373450303@qq.com

Keywords: Electronic Commerce; Electronic Cash; Security Model; Abnormal Situations

Abstract. As the development of social economy and information technology, electronic cash has appeared on the social stage. E-cash is not only a new kind of electronic currency, but also an innovative and modem payment device. E-cash payment systems are the heart of electronic commerce. How to achieve safe electronic transactions is the key to the development of electronic cash payment systems. In order to solve the security problem of electronic cash in electronic commerce, the paper presented the security model of e-cash under abnormal situations. The dynamic and uncertain problem of e-cash demand is analyzed qualitatively by considering influencing factors and system complexity. The presented solution can promote the development and effective e-cash regulation and control of e-cash with the purpose of perfecting the fundamental theory of e-cash and research methods.

Introduction

Electronic commerce, commonly referred to as "e-commerce", may be defined as the application of information and communication technologies in support of all the activities of business. Commerce constitutes the exchange of products and services between businesses, groups and individuals and can be seen as one of the essential activities of any business. Electronic commerce focuses on the use of communication technologies to enable the external activities and relationships of the business with individuals, groups and other businesses. Electronic business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers.

In practice, e-business is more than just e-commerce. While e-business refers to more strategic focus with an emphasis on the functions that occurs using electronic capabilities, e-commerce is a subset of an overall e-business strategy. E-commerce seeks to add revenue streams using the World Wide Web or the Internet to build and enhance relationships with clients and partners and to improve efficiency using the Empty Vessel strategy. Often, e-commerce involves the application of knowledge management systems.

E-business involves business processes spanning the entire value chain: electronic purchasing and supply chain management, processing orders electronically, handling customer service, and cooperating with business partners. Special technical standards for e-business facilitate the exchange of data between companies. E-business software solutions allow the integration of intra and inter firm business processes. E-business can be conducted using the Web, the Internet, intranets, extranets, or some combination of these.

Usually paired with a transaction account or current account, cards with an electronic cash logo are only handed out by proper credit institutions. An electronic card payment is generally made by the card owner entering their PIN (Personal Identification Number) at a so-called EFT-POS-terminal (Electronic-Funds-Transfer-Terminal). Comparable debit card systems are Maestro and Visa Electron. Banks and credit institutions who issue these cards often pair electronic cash debit cards with Maestro functionality. In order to solve the security problem of electronic cash in electronic commerce, the paper presented the security model of e-cash under abnormal situations. The dynamic and uncertain problem of e-cash demand is analyzed qualitatively by considering influencing factors and system complexity. The presented solution can promote the development

Copyright © 2016, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

and effective e-cash regulation and control of e-cash with the purpose of perfecting the fundamental theory of e-cash and research methods.

Electronic cash

Electronic cash is in fact a technology in the form of electronic cash. Electronic cash systems attempt to replicate the characteristics of cash for online transactions in many ways: convenience, low cost, anonymous, and other properties. But not all of the electronic cash system to meet these characteristics, most of the electronic cash system can provide fast and convenient for small online transactions.

Electronic cash payment process

The following is a detailed description of the process of electronic cash in the actual transaction process, as shown in Figure 1.

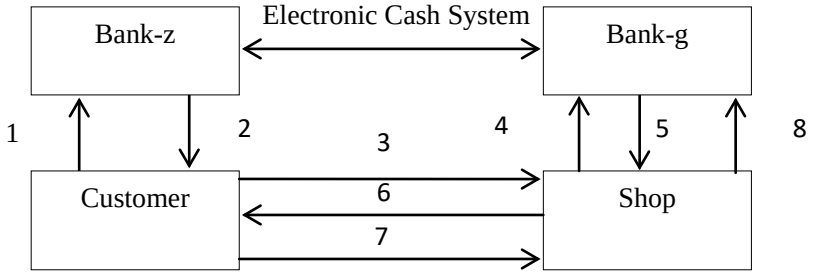

Figure 1 Electronic cash payment process

1) Customers from the bank to extract electronic cash applications. Customers are required to enter the correct credit card number and password.

2) Bank card numbers, passwords and balances to determine whether to give electronic cash. If it is true, then return the electronic cash serial number and the random key. If it is false, return to the customer to withdraw cash failure tips.

3) When customers shop to pay electronic cash, first available to businesses.

4) The serial number of businesses to send electronic cash provided by the customer to the bank to check authenticity.

5) The bank returns the check results. If it is true, continue the next step. If it is false, the prompt input is error, and the cash does not exist or have been used, businesses should not accept the electronic cash.

6) If it is true, request the customer to provide electronic cash serial number, that is, to request the customer to pay electronic cash. If it is false, return to the implementation of the third step.

7) The key customer, that customer agrees to pay electronic cash.

8) The merchant provides password to the bank to obtain funds, the original electronic cash failure, businesses can generate new electronic cash, can also choose to deposit the amount in the ordinary account, deposit cash equivalent.

Problems of security

A business successfully submitted application for checking, the bank should be labeled as "the electronic cash is checked, mark time is T, this time in T, on the other cash check for the return to" temporarily unable to identify, please wait "to prevent the repeated use of cash.

In this step, the customer submits the key, it is agreed to pay electronic cash. So here to take measures to prevent businesses to deny, a non-repudiation mechanism.

If there is a certain number of wrong key to input in time T, is considered to be illegal trial, this time mark T cannot return to the identification results; and the business into the black list, after treatment.

According to the data of the intermediate transmission, different encryption methods can be used according to the security requirements, and the data encryption standard and the various variants of DES are commonly used.

The security model of electronic cash

The security electronic cash model contains bank, customer, shop, central bank and supervision department, which uses the group signature and blind signature technology, as shown in Figure 2.

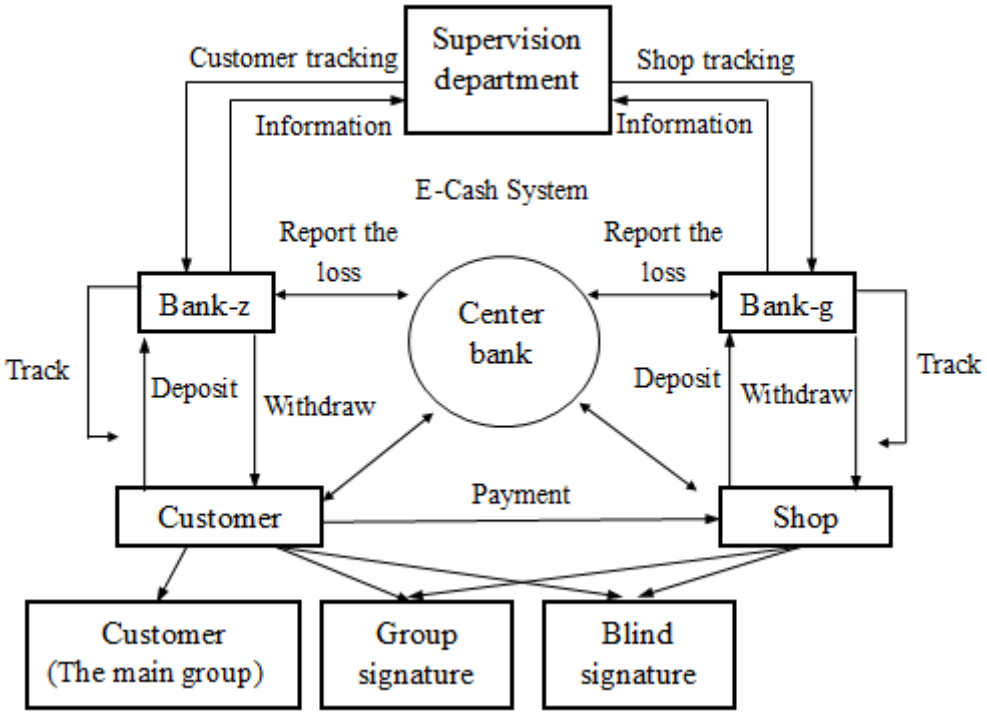

Figure 2 The security model of electronic cash

User register

The registration phase is a process for a user to join the group. The user of the platform in TPM on the identity certificate public key information and their identity information is sent to the main group, and the information with the group public key encryption, so that only know the private key can decrypt the main group, so as to ensure the security of information in the transmission. The main group received the information sent by the user after the first group of the private key to decrypt, and then determine whether the user has a valid TPM, if the user has the legal TPM group will randomly choose a large prime number as the identity of the user code, and then calculate the user identity of another public key. The private key generated by the group sent to the user, while the user information is saved to a specialized database to find.

Here, the main assumption is credible, trusted third party is not in need, thereby reducing the interaction process, improve the efficiency of the system.

Deposit

The following steps should be carried out when the user wants to withdraw money at a bank.

The user sets the amount of money to withdraw and operates.

The user selects a blind factor for the blind operation of the information to be sent. Send the result of the calculation to the bank.

After the bank receives the user's information, according to the value of information in the first check whether there is enough balance in the user's account. If yes, deduct the corresponding amount from the user account.

After the user receives the information, the user verifies the information. If correct, would have operation; get the bank to e-cash signature.

Payment

Merchant first send the payment information to the user, waiting for the user to confirm.

After receiving the information, the user can calculate and confirm the operation, and then send the reply signal to the merchant. If the user's environment platform and TPM binding, then it will also be sent to the merchant and the information sent by the bank to get the information to

determine the receiver.

Businesses receive the user's information, check the amount of the transaction and the validity period, if the signature of the electronic cash has expired will refuse to receive the user's payment. Otherwise, businesses believe that the user's electronic cash to send a legitimate, and then to determine whether it is valid. If the electronic cash and TPM binding, businesses also verify whether the information sent by the user is consistent with the original information. If a series of operations are verified successfully, businesses will successfully receive the user's electronic cash, the end of the transaction between the two sides.

Withdraw

This process for the business to the user to submit the electronic cash stored in the own account. First, the business will be electronic cash data and the signature of the information sent to the bank, and then check whether the bank cash effective, and then verify the signature of electronic cash. After all the inspection, the bank has been spent in the electronic cash database to find, if there is no corresponding record corresponding to the electronic cash into the business account. Otherwise, the bank believes that the user repeat consumption, refused to receive, and can be found through the appropriate parameters of the user to repeat consumption.

Conclusion

With the development of social economy and information technology, electronic cash has appeared on the social stage. It is not only a new electronic currency, but also an innovative and modern payment device. Electronic cash payment system is the heart of electronic commerce. How to realize the secure electronic transaction is the key to the development of the electronic cash payment system. In order to solve the security problem of electronic payment in electronic commerce, in this paper, the abnormal situation of the security model of electronic cash is put forward. The dynamic and uncertain problem of e-cash demand is analyzed qualitatively by considering influencing factors and system complexity. The proposed solution is aimed at improving the basic theory of electronic cash and research methods, and promoting the development of effective electronic cash management and control of electronic money.

Acknowledgement

This research is supported by Zhejiang University of Technology Undergraduate Training Program for Innovation and Entrepreneurship.

References

[1] Songjie Gong, Liping Zeng, The Solution of Safety of Electronic Cash in E-Commerce under Cloud Computing Environment[J]. Advanced Materials Research, 2014, 989-994:4314-4317.

[2] Okamoto T, Ohta K. Universal Electronic Cash[C]// Advances in Cryptology - CRYPTO '91, International Cryptology Conference, Santa Barbara, California, Usa, August 11-15, 1991, Proceedings. 1991:324-337.

[3] Popescu C. An Electronic Cash System Based on Group Blind Signatures.[J]. Informatica, 2006, 17(4):551-564.

[4] Chen Y, Chou J S, Sun H M, et al. A novel electronic cash system with trustee-based anonymity revocation from pairing[J]. Electronic Commerce Research & Applications, 2011, 10(6):673-682.

[5] Xiaoya Liu ,Xiaolong Xin . Improved blind signature electronic cash scheme [J]. Computer Engineering and Applications ,2011,47:114-116.

[6] Ziba Eslami , ehdi Talebi . A new untraceable off-line electronic cash system [J]. Electronic Com- merce Research and Applications,2011, 10:59-66.

[7] Varadharajan V, Nguyen K Q, Mu Y. On the design of efficient RSA-based off-line electronic cash schemes[J]. Theoretical Computer Science, 1999, 226(1-2):173-184.