Research on the security of online payment

Huang Hanyan

School of Information Technology Jiangxi University of Finance & Economics

Nanchang, China

huanghany@126.com

Keywords: online Payment, Secure Electronic Transaction, E-business,

Abstract. The secure payment on network is the core of E-business, because the security of the network payment has a direct effect on E-business. So, how to guarantee the data-transmission security on the network has become one of the most important factors in popularizing E-business. The payment mode of the improved Secure Electronic Transaction researched by the Paper can effectively solve the payment problem, and it also can provide the strongest support for the secure transaction of users.

1. Introduction

The network payment is to realize the online electronic payment via the open internet, which makes the users realize the synchronous online payment and settlement without the limitation of the time and space. The network payment is the basics of E-business which is just an electronic market information or electronic contract without the real-time network payment. Due to the openness of the Internet, the confidential information of the users has become the major target for illegal invaders or hackers during the process of online transaction. So, how to protect the security of the online payment and the confidential information of the users, verify the legal identity of the users and guarantee the data integrity and transaction authenticity and others have become the bottleneck to restrict the E-business development. However, the SET is emerged for solving the problem. At present, the SET is one of the main online payment modes for E-business and the most complex standard among all modes, but the process is so complex and slowly. The high procedure fee limits the promotion of SET to a certain degree. The payment mode of the improved SET can effectively solve the payment problem, and it also can provide the strongest support for the secure transaction of users[1].

2. SET Introduction

The SET, issued by MasterCard International and VISA, is a security standard to protect the online payment of credit card on the Internet. With support of IBM, HP, Microsoft, NetScape, VeriFone, GTE, VeriSign and other famous companies, the SET has become an actual industrial standard and currently gained the approval of IETF [2]. The SET, as an online payment based on the credit card, is suitable for B2C E-business, which can realize the ID identification, information confidentiality, integrity and authenticity of the users during the process of online payment. The SET has some core technologies (such as encryption technology, asymmetric encryption technology and Hash) to meet the requirements of the secure payment[2].

3. SET Application of E-business

3.1 Functions of SET

(1) Information Confidentiality. To realize the online transaction, the seller and the bank must make their customers believe that their provided bank information is protected and only the specially authorized person can see their information. Moreover, to prevent the account, password

© 2015. The authors - Published by Atlantis Press

and transaction date from being gained by the illegal person, the seller and the bank must guarantee that the settlement account and relevant information are protected by the secure measures. What’s more, the SET also adopts the corresponding technology to prevent the seller from seeing the customer’s account information to increase the transaction security. Besides, the SET guarantees the security of information transmission with an encryption technology, digital envelope, etc.

(2) Data Integrity. Based on the SET, the receiver can confirm whether the information is revised or not in the transmission, and the transaction cannot be processed smoothly if any information is revised. To get rid of the hidden frauds, the SET will compare the transmitted information with the built information by the digital signature technology for ensuring that the received information is the same as the sent information.

(3) Identity Authentication. The identification of each side must be checked before each online transaction. The identification check includes bank-card account and password of the buyer and the creditworthiness of the seller. All these abovementioned requirements can be met by the digital certificate and CA.

(4) Wide Application. The SET is a formal industrial standard, which can be operated in different hardware and operation-system platforms and be used in many kinds of network environment.

(5) Instantaneity of Online Transaction. All payment must be online, which meets the requirements of E-business[3,4].

3.2 SET Flow

The following flow is based on the payment-data flow of SET:

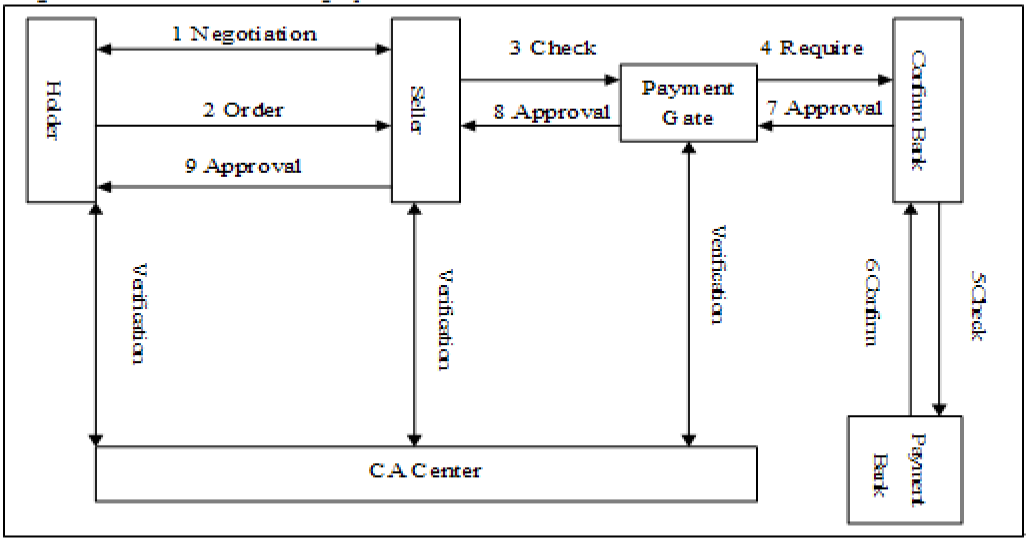

Figure 1 Payment Data Flow of SET

The whole process can be divided into following seven steps according to the flow of the SET:

1. The buyer can buy the goods online, and then input the list of the selected goods via the computer. The list should include the name of the online shop and purchased goods, quantity, delivery time, address and relevant information.

2. The seller will tell the buyer via the E-business server and online information and confirm whether the buyer wants to change the information about the unit price of the purchased goods, pay, delivery method and others or not.

3. The buyer selects the payment method, confirms the order, signs the payment tips, and then the SET begins to work.

4. Based on the SET, the buyer must do digital signature for the order and payment tips, meanwhile, the SET can make the seller not see the account information of the buyer via the double signature technology.

5. The seller will require the permit of the order payment after received the order, the information will be passed to the bank via the payment gateway, and then the electronic-currency

issuing company will confirm the information. After the transaction confirmed, the seller will get the confirmed information.

6. The seller will send the order information to the buyer, and the terminal software of the buyer will record the transaction information for the future query.

7. The seller sends the goods or provides services to the buyer, and the bank will transfer the payables from the buyer's account to the seller's account. Sometime the payables will be paid via the issuing bank after getting the payment information.

4. Payment Mode of Improved SET

Based on the SET, the seller not only handles the order information but transmits the payment information (including credit card account and other confidential data) from the buyer to the payment gateway. However, the payment information is encrypted, but partial information may be left to the seller, so it is very unsafe to the partial information. Thus, the E-business payment mode of the SET is improved for solving the problem.

In this way, the electronic seller mainly shows their goods online and issues invoice while the buyer makes an online order. The final payment and other functions (like higher technological security and creditworthiness) will be done by the third party (it is regarded as Payment Center). So the buyer doesn't send the payment information to the seller and then the seller will transmit it to the payment gateway, but just send to the entrusted third party (it is regarded as SET Payment Center) which is confirmed by the seller and buyer. Now, the seller can not see the information of the buyer and the bank cannot get the information of the card holder, which effectively guarantees that only the direct receiver can be authorized to see the relevant information, and promote the confidentiality and security of real-time information and fund online transmission.

The improved payment mode is as follows:

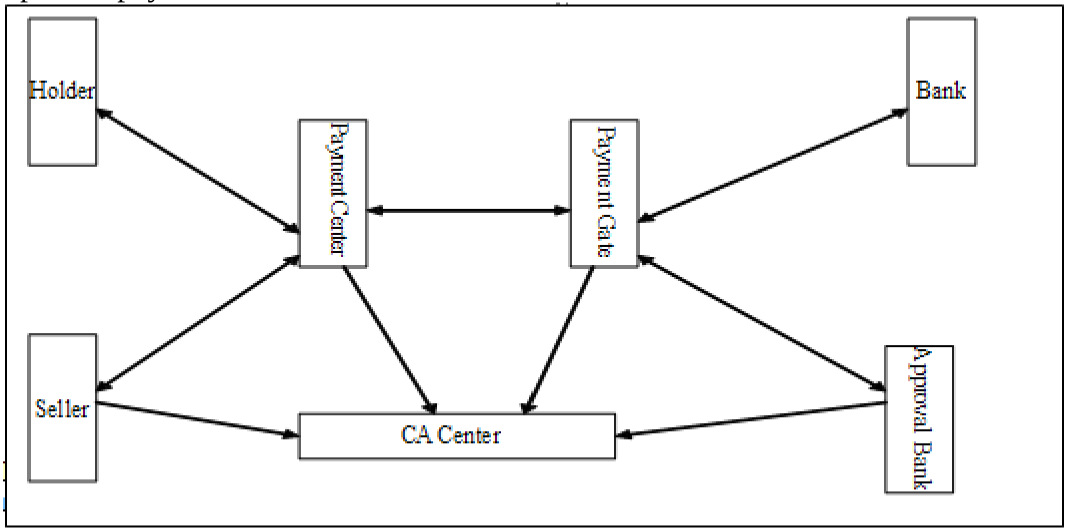

Figure 2 Payment Mode with A Payment Center

The improved payment flow with a payment center makes the payment flow be different from the previous one, and the main difference is the finished initial response. The whole flow is as follows.

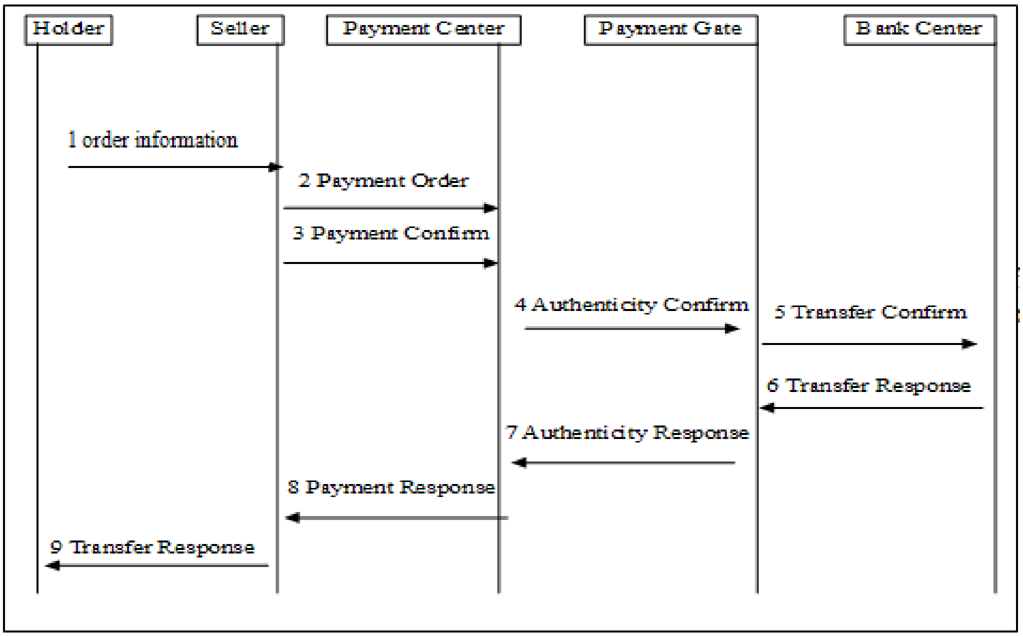

Figure 3 Improved SET Flow

5. Security Analyses on Improved SET

With adopting the payment center, the payment information of the card holder will not be transmitted by the seller, which can greatly enhance the transaction security. The order information transmitted from the card holder and the seller will be compared in the payment center, which effectively prevents the illegal card holder or seller from revising the order information or payable amount. All information sources adopt the digital signature technology to guarantee that the final receiver can check the information sources. Moreover, all confidential transmission adopts the digital envelope technology to guarantee that even if the relevant information being gained by the illegal person, they cannot be decoded. Adopting the encryption algorithm and hash function, the improved SET is very safe than the previous SET.

6 Conclusion

The verification of E-business for the buyer, seller and bank has the advantages like safety, completeness, stability and authenticity during the process of online transaction, so it is regarded as an international safety standard for the credit card and debit card. SET is very popular during the process of online transaction, but the process is so complex and slowly. The high procedure fee limits the promotion of SET to a certain degree.

Based on the improved SET, the payment mode adopts perfect system, advanced encryption algorithm, the applicable card type and authenticity function, which greatly perfects the payment flow and then promote the payment security and practical applicability.

References

[1] What is E-business? http://www.g369.net/pswt—13479-17000-24214.html.2005-08.

[2] Luo Jing, Zhang Youchun. Simple Analysis on the SET Application in E-business. Modern Computer, 2003,(2):15-19.

[3] Xu Rongsheng, Jiang Wenbao. Security and Privacy of E-business, China Electronics Press, 2001.

[4] Song Ling, Opportunity and Challenge of E-business in 21st Century, Electronics and Industry Press, Beijing.

[5] Eric Armstrong. The Java Web services tutorial. Beijing: Higher Education Press, 2003