Université du Québec à Chicoutimi

Mémoire présenté à
L'Université du Québec à Chicoutimi
comme exigence partielle
de la Maîtrise en informatique

offerte à

l'Université du Québec à Chicoutimi
en vertu d'un protocole d'entente
avec l'Université du Québec à Montréal

par

TONG-XUE

DESIGN OF A SECURE E-BUSINESS APPLICATION

JUNE 2010

ABSTRACT

The present economical situation in China asks the enterprises to change the traditional transaction style and implement e-business. The most important problems the e-business is facing are: the information confidentiality, the data availability, the data integrity, the user's identity, the non-repudiation of the data's original sender and the legal user, etc.

The subject of this thesis analyzes the basic concepts, the security infrastructure and payment system of electronic commerce, makes a thorough and comprehensive research on the security technology, authentication and transaction process, points out some deficiencies in Secure Electronic Transaction (SET) protocol. Then an improved method is given out with the data flow and data structure, finally a secure electronic commerce payment system and its software based on the improved SET model are designed. This thesis brings forward the improved method for improving the speed of transaction, and strengthening the security of protocol and adapting it to any circumstance easily.

Key words: Electronic Commerce, Secure Electronic Transaction protocol, Secure Sockets Layer, electronic payment system, message security

ACKNOWLEDGEMENTS

I would like to thank my supervisor Qiao-Mei and co-supervisor Dong-Yutao. I have learned a lot from their serious attitude toward studying, their deep knowledge on the subject, which has helped me in understanding the subject.

I would like to thank Prof.Ning-hongyun who helped me with the subject and also on the personal level.

I would like to thank my classmates, with whom I often had interesting discussions, which has broaden my view and increased my knowledge on the subject.

I would also like to thank all of my teachers and classmates in MCS, they give me such colourful days of these three years.

Last but not the least, I would like to thank my parents and my husband. Their love and encourage have made this thesis possible!

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

DES	Data Encryption Standard
ASN.1	Abstract Syntax Notation
ASNA	ATM-based Signaling Network Architecture
CA	Certification Authority
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DTS	Digital Time Service
EC	Electronic Commerce
EDI	Electronic Data Interchange
ICC	International Chamber of Commerce
IEFT	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
PAN	Personal Account Number
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
RSA	Rivest, Shamir , Adleman
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer

CHAPTER 1

INTRODUCTION

1.1 Electronic Commerce and Security Protocol [11]

1.1.1 An Overview of Electronic Commerce

Electronic commerce first appeared in 1960s, and developed in 1990s. There were two phases in the development of electronic commerce: one is based on EDI (Electronic Data Interchange), and the other is based on the Internet [22].

After 1990s, with the popularity and mature of computer as well as internet, the common applications of credit cards, the designing of electronic security transaction protocol, and the support and promotion of the government, electronic commerce which is based on internet has been developed quickly. Especially when SET (Secure Electronic Transaction Protocol) was introduced, it was recognized and supported by most companies. It provides a key and secure environment for developing electronic commerce on internet, which is significant for the development of electronic commerce. Internet has covered more than 150 countries and regions, which connects more than 15000 networks with 2.2 million host computers. It has become the biggest network in the world. Because of the low-cost, wide covering surface, full developed function, and flexibility of the

internet, electronic commerce becomes the hotspot of the world.

Experts believe that electronic commerce will be the important application of the 21st century economy, whose function will be as significant as the industry revolution 200 years ago. Worldwide services organizations and enterprises such as government sectors, public service mechanism, telecommunications enterprises, banks, etc, as well as billions of personal users are widely participating electronic commerce activities. The average speed of growth of electronic commerce a year is 150%, which make it the fastest growing area. At present, electronic commerce has become one of the key elements to consider when countries make their economic strategies.

Electronic Commerce, abbreviated as EC, contains two components: one is electronic model, and the other is commercial activities.

In November 1997, International Chamber of Commerce (ICC) held the The World Business Agenda for Electronic Commerce in Paris. The conference expounded the concept of electronic commerce authoritatively: electronic commerce is to realize the application of electronic IT on the whole trade and commercial activities. From the perspective of scope, electronic commerce means participants finish any kind of business transaction through electronic way instead of physical exchange or direct physical contact on computer network, especially on internet. Here electronic method includes electronic data interchange (EDI), electronic payment, electronic ordering system, e-mail, fax, network, bulletin board system bar code, image processing, smart card. from the technological perspective, electronic commerce is a multi-technological aggregation, including data

interchange (such as electronic data interchange , smart card, etc.), data acquisition (such as sharing database, Bulletin Board System, etc) and automatic data acquisition (bar code). In summary, electronic commerce is a new mode of commercial activity. Based on computer network, especially internet, it uses simple, quick, and low-cost electronic means of communication to realize various commercial activities through skills such as data encryption, data signature, and authentication, in which participants don't have to see each other.

There are various kinds of electronic commerce. And they can be classified into different types according to different standards. [32]

(i) According to the contents of electronic commerce

Direct electronic commerce: activities such as ordering of intangible goods, services or payments.

Indirect electronic commerce: activities such as ordering of tangible goods, services or payments.

(ii) According to whether electronic commerce involves payment

Non-payment electronic commerce: this kind of electronic commerce does not involve on-line payment and goods delivery. The contents such as: releasing, information inquiry, on-line negotiation, the forming of contract wording, which do not involves banking payment. In this kind of electronic commerce, there are only flows of goods, material, and information. The flow of funds is not included.

Payment electronic commerce: this kind of electronic commerce involves on-line payment and goods delivery. Its contents includes: All contents of non–payment electronic commerce, banking payment, delivery, and goods delivery, etc. This kind of electronic commerce includes flow of goods and information as well as funds.

(iii) According to the transaction entity it involves

Internal electronic commerce: to deal with and exchange commercial information among the branches. Intranet is an effective commercial tool. Enterprise can separate its intranet from internet by firewall. It can be used to automatically deal with business operation and workflow, strengthen the access to important system and key data, share experiences, solve customers' problems jointly, and keep in touch among branches. Intranet can increase the agility of operation of business activity, react quickly to the market situation, and provide better services to customers.

Business to customer (B2C for short, which means enterprises to personal customers or business organization to consumers) electronic commerce. Nowadays, there are various kinds of commercial center on internet, which provide different kinds of goods and services, including flowers, books, computers, cars, etc.

Business to business (B2B for short, which means business to business or business organization to business organization) electronic commerce. Business organization to business organization electronic commerce means business organization (enterprise or company) use internet or various business networks to make orders or payment to supplier (enterprise or company).

Business to government electronic commerce (BtoG or B2G). Electronic commerce between enterprise and government can cover many businesses between enterprise and government organizations.

Consumer to government electronic commerce (C2G). Government will expand the electronic commerce to the providing of welfare, self-assessment of tax, and the collection of personal tax.

Commonly, only two kinds of electronic commerce models, B2C and B2B were mainly used.

(iv) According to the network type of electronic commerce

Electronic Data Interchange (EDI) network electronic commerce: it standardize and format commercial papers according to a recognized standard and agreement, and do electronic commerce through computer network.

Internet electronic commerce: it uses internet to do electronic commerce activities. It is the main form or electronic commerce now.

Intranet electronic commerce: it uses intranet to do electronic commerce activities. Intranet is a kind of network inside the company based on internet.

1.1.2 Electronic Commerce Safety Protocol

Electronic commerce is an inter-relationship among Client, Merchant, Bank and trusted third party (Certification Authority) about information flow, logistics, and fund flow,, it uses simple,

convenient, and low cost electronic communication method to do various trading activities. Electronic commerce is usually done in the internet environment. Because of the open and insecurity of internet, if electronic commerce wants to go well, the first thing is to solve the security problem. In electronic commerce trading model, the interrelationships among various participants have certain rules to follow in order to ensure the security of participant's interests and control risks, these rules are various security protocols.

Electronic commerce protocols are different in convenience, security, and risk. At the same time, their application environment, realization aim, and costs demands are also different. However, all electronic protocols must conform to some common standards when they are designed.

(i) Anonymity

In transaction process, the customer usually keep his identity, purchasing habit, and purchased goods secret, that must be guaranteed in electronic commerce, so more customers can join in the transaction. We have to point out that although anonymity is a requirement in business transaction; there are still some countries regard anonymous transaction as illegality. One compromising method is to purchase through trusted agency, private information such as customer's identify is kept by agency, and the tracking of fund flow is also stopped at the agency.

(ii) Security

To the electronic commerce, the most important thing is security. Only with the guarantee of security protocol, online transaction can go well. It ensures that data won't be changed and leaked

in transmitting process, and interests of participants won't be violated. Electronic commerce involves the problem of mutual trust, which is closely related to security. Some protocols are supposed to trust the third party, some others are supposed not to trust related members.

(iii) Non-repudiation

The process of electronic commerce involves interests of various members, and certain ways must be used to ensure the non-repudiation of participants' action. The popular skill is to use digital signature to ensure information sent by participants.

(iv) Atomic nature

The atomic nature of electronic commerce is developed from a database concept by T.D. Tygar. It is used to regulate information flow, logistics, and fund flow in transaction , and it can be divided into three layers:

a) Atomic nature of money: it defines that fund flow is conservation in electronic commerce, that is to say, fund will not increase or reduce in the process of flow in transaction.

b) The atomic nature of goods: it ensures that once customer pays, he will get the goods. If he gets goods, he must have paid. , No payment no goods and no goods no payment. The atomic nature of goods is very important for information goods or digital goods sold through internet.

c) Atomic nature of ensuring sending: It ensures the seller and buyer of the contents and quality of goods, that is to say, customer gets some goods he buys with some quality, and merchant do send the goods ordered by customers, this is always guaranteed by a third party. Atomic nature

of ensuring send is significant in occasions where customer and merchant do not trust each other. The protocol which is satisfied by atomic nature can ensure the contents and quality of sent goods.

The above three atomic nature is in upward containing relation, the latter contains the previous one, that is to say, if atomic nature of goods is satisfied, atomic nature of money must be satisfied, if atomic nature of ensuring sending is satisfied, the previous two must be satisfied.

1.2 The Significance and Major Work of This Thesis

Because of the popularity of internet, electronic commerce is recognized as new growth point with best potential in IT industry. The core problem of electronic commerce is secured payment mechanism, how to make electronic commerce operate in highly active environment is the key of research. Therefore, electronic business researchers of the world analyzed many payment protocols, and realized some of them such as Digicash, FirstVirtual, Netbill, SSL and SET.

In business, Secure Electronic Transaction protocol is supported by major credit card brand such as VISA and MASTER and in technique it is supported by computer companies such as IBM, Microsoft, HP, and Netscape. It is now the most widely supported payment protocol; in fact, it is also the standard of electronic commerce. Future commerce competition is the competition of network economy, and the security problem of network is more and more serious. It has become a hot spot to analyze security protocols such as SET.

However, there are quality problems in the designing of SET protocol, which limits its

application. Its contents are too complicated, and the transaction cost is too high, the encryption it uses is no longer secure. The research on encryption algorithm to replace the encryption algorithm in original SET protocol and improvement on SET protocol reduces transaction cost, and raises new proposals, which realizes the popularity of SET.

Analyzing, completing and improving SET protocol is significant in promoting the development of China's electronic commerce, solving electronic business security problem and pushing further development of electronic commerce, and China's own version software development.

1.3 The Structure of the Thesis

This thesis discusses the working theory of SET protocol. Through analyzing its process, the thesis finds out its shortcomings, and offers corresponding improving solutions according to these shortcomings. On this basis, this thesis constructs a secure electronic commerce payment model which is based on improved solution, and provides the data flow, data structure and software module of this model.

The main structure of this thesis is as follows:

Chapter One: Introduction.

This chapter introduces the developing situation of electronic commerce and related contents of security protocol, and the main work of this thesis.

Chapter Two: Research on SET protocol of secure electronic transaction.

Introduce in details on SET protocol of secure electronic transaction, and analyze its theoretic foundation, technical specification, secure algorithm, working procedure, certificate, and application environment.

Chapter Three: Analysis of SET protocol shortcomings and method to improve it.

This chapter first introduces another widely used protocol in electronic commerce—SSL, and does on-stream analysis on SSL. After that, SSL and SET are compared, the shortcomings of SET are discussed, and the improving solutions are suggested.

Chapter Four: The design of SET protocol payment system based on improving solutions.

Design the improved SET according to the improvement solution suggested in chapter three, and offer new working procedure, data flow and data structure.

Chapter Five: Research and design on secure electronic commerce payment system software module. This chapter offers a realization model for improved SET protocol payment system. This model can be divided into company service module, customer module, payment gateway module, certificate module and security module. The design theory and working procedure of these modules are also introduced.

CHAPTER 2

RESEARCH ON SET PROTOCOL OF SECURITY ELECTRONIC COMMERCE

Set protocol is released by VISA and MasterCard together, which is the security protocol based on credit card online payment. SET protocol is mainly used in BtoC electronic commerce system. It not only defines electronic protocol, but also sets strict formulations on the management of certificate and trading process. Its security is mainly realized through ID authentication skill, information encryption skill, digital signature skill, etc. At present, SET protocol has been approved by internet engineering task force (IETF) standards, which enables it as an industry standard.

2.1 The Technique Standard and Theory Foundation of SET Protocol [13]

2.1.1 The Technique Standard of SET Protocol

In the year 1995, the union which included MasterCard, IBM, and Netscape began to develop security electronic payment protocol (SEPP), and the union of VISA and Microsoft began to develop security trading technique (STT). The two biggest credit card organizations

MasterCard and VISA support independent network payment solutions separately, which influenced the development of network payment. In 1996, these companies declared that they would jointly develop a standard, which was called security electronic trade (SET). In 1997, SET protocol 1.0 version was introduced jointly by VISA and MasterCard. Many important organizations in Internet payment industry, such as IBM, HP, Microsoft Netscape, GTE, ViriSign, etc. all declared to support SET.

- **The application standard of SET**

SET standard consists of the following three parts:

(i) Business Description: Include the background information and processing flow of SET. It is used to provide the overall business description of SET.

(ii) Programmer's Guide: Include data information and processing flow. It is used to provide the technique standard of SET protocol. This guide can be divided into three parts and appendix:

a) Part one: System Design Considerations. Include considerations in developing saddlebag of SET and its application. It provides the background information and characteristics and marks in programmer's guide.

b) Part two: Certificate Management. It defines certificate's requiring structure, protocol and the certificate concept in used in SET.

c) Part three: Payment System. This part provides the description and processing

information of the payment system in SET protocol, and all the information related to certificate, cash requirement, and payment system management.

The appendix part: this part provides the side information related to SET protocol.

(iii) Formal Protocol Definition: This part includes the formal definition of protocol. It also provides the strictest description of SET information and data area.

In addition, External User Interface Guide offers the programming guide which adopts actual transmission mechanism.

- **The industry standard supported by SET**

In addition to SET's own standard, SET has to support standard, algorithm, and certificate of industry, internet, and international organizations, based on which SET is designed. These standards are defined in ISO, IEFT, PKCS, and ANSI.

(i) ASN.1 (Abstract Syntax Notation) is a symbol for SET to define information.

(ii) DER (Distinguished Encoding Rules) realizes the protocol data and code in payment information and certificate (defines in X509) with clear form.

(iii) DES (Data Encryption Standard) is used for data Encryption. DES key is distributed with encryption. This encryption is a digital envelop which adopts public key encryption.

(iv) HMAC is key hash mechanism.

(v) HTTP is World Wide Web's transport protocol.

(vi) ISO 3166:1993 represents the code standard of nation names.

(vii) ISO 4217:1995 represents code of currency and fund.

(viii) ISO 7812:1985, it is card ID, which is used to identify the number of issuing bank, including algorithm and parity bit.

(ix) ISO 8583:1993, the definition of starting information and exchanging information of financial transaction card.

(x) ISO 9594-8:1997, X.509 (1997) standard recommended by international telecommunication union-telecommunication sector (ITU-T), it supports the interconnection of information technology and open system, which is used in catalog identification system .

(xi) ISO 9834-7, object identification provides international registration authority.

(xii) MIME (Multipurpose Internet Message Extension) is used in the encapsulation code of payment information, which enables browser to support and identify payment information. It can also support commerce with e-mail.

(xiii) PKCS (Public Key Cryptograph Standards) is used to define PKSC and PKCS.

(xiv) RFC 1766, language standard.

(xv) SHA-1 (Secure Hashing Algorithm) is proposed jointly by The National Institute of Standards and Technology (NIST) and National Security Agency (NSA), SET adopts SHA-to for all digital signature.

(xvi) TCP/IP, it supports the protocol set of internet communications.

(xvii) X. 509 (1997) recommended by ITU-T is the coding standard of public key

certificate. Certificate format definition supported by SET is defined in ISO standard X.509 version 3, ANSI X9.57.

2.1.2 The Theoretic Foundation of SET Protocol

- **The structure of electronic commerce system**

A complete electronic commerce system can be viewed as a three-layer frame construction [34], as is shown in Figure 2-1.

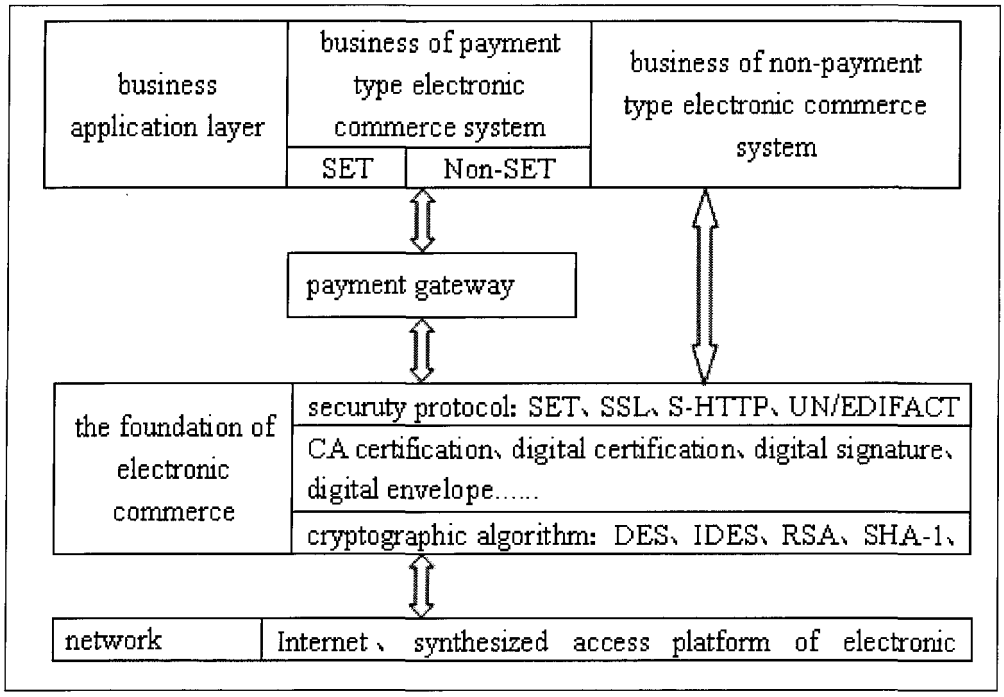


Figure 2-1 the system architecture of electronic commerce

In this figure, the bottom layer is network layer, specifically the network layer in ISO OSI/RM (Open System Interconnection Reference Model). This layer addresses and routing IP packets over Internet.

The middle layer provides the foundation for electronic commerce. It consists of 3 sub-layers. The first sub-layer is algorithm layer, which encrypt and decrypt data. These algorithms include DES, RSA, DSA, MD5, SHA-1, etc. the second sub-layer is security infrastructure layer. This layer uses non-symmetric algorithms (such as RSA, DSA) and Hash functions (such as MD5, SHA-1) to realize digital signature, or uses other algorithms to realize digital envelope. It can also provide digital certificate by mean of CA. The third sub-layer is security protocol layer. Protocols, such as SSL, SET protocol, HTTP over SSL functions on this layer, providing up-level applications with secure communication.

The top layer is application layer. It is business logic layer of secure electronic commerce. This layer provides 2 types of applications: Payment and non-payment. Payment-type applications, such as secure electronic commerce in SET require payment gateway to transform Internet protocols to/from internal bank protocols. Otherwise, non-payment-type ones don't require payment gateway.

Up-level protocols depend upon down-level protocols. On the contrary, down-level protocols serve up-level protocols.

- **Electronic commerce module based on SET**

Electronic commerce module based on SET is shown in the following Figure 2-2:

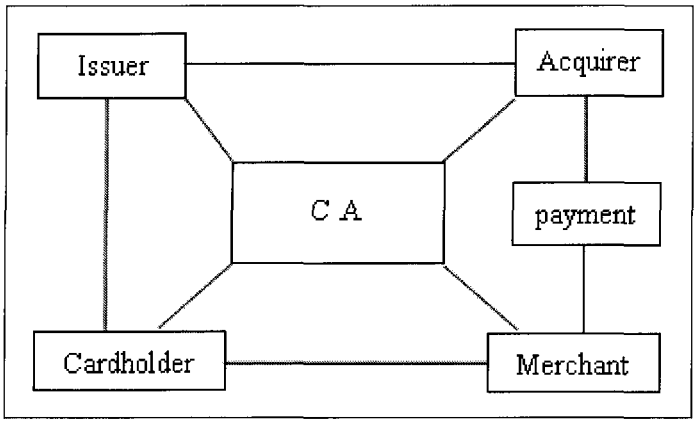


Figure 2-2 The electronic commerce module based on SET protocol

The involved participants in SET protocol include Certification Authority (CA), Issuer, Acquirer, Payment Gateway, Cardholder and Merchant [13]. The descriptions on these participants are as follows:

CA: It is usually an authorities organization trusted by all participants. It is the certificate management organization. Its main function includes the issuing, saving, catalog services, declaring the lost and renewal of the certificate, the renewal and reversion of the key, and the authentication of the certificate.

Issuer is a financial organization which issues credit card to cardholder, and verify cardholder when he or she applies for SET digital authentication.

Acquirer is a financial organization where merchant open account. It verify merchant when the merchant applies for SET digital certification.

Payment Gateway is used to realize the transformation of payment information from internet to the inner network of bank, and very the merchant and cardholder.

Cardholder is purchaser of internet goods. He or she choose the goods of certain merchant

by browsing the internet, and purchase them on-line with payment software.

Merchant: services provider which provides goods or services.

2.2 The Security Technology of SET Protocol [2] [23] [22] [34]

In SET protocol, encryption techniques and digital certification, digital signature, and authentication techniques are used to guarantee the security of SET payment system. At present, there are two widely used encryption techniques, secret key encryption system and public key encryption system. SET perfectly combines symmetric key's quickness and low-cost with non-symmetric key's effectiveness. In SET, secret key encryption system adopts DES cryptographic algorithm, and public key encryption system adopts RSA cryptographic algorithm. Non-financial data's encryption should use DES cryptographic algorithm, and card data's encryption should use DES cryptographic algorithm and RDA algorithm to strengthen the encryption.

2.2.1 Symmetric and Asymmetric Key Cryptography

Symmetric Key Cryptography is also called Private-key Encryption which means that the sender and the receiver of the message use one key to make both encryption and decryption [21]. Its biggest advantage is its high speed for doing the above job. It is suited to make encryption on a large scale of data. However, the management of it is difficult.

The appliance of the Symmetric Key Cryptography will simplify the process of encryption as every participant need not to study and exchange the encryption algorithms of the dedicated

device but to utilize the same encryption algorithms and exchange the shared dedicated key only [12]. If the communication of the two sides could ensure the non-leak of the dedicated key in the key-exchange process, the confidentiality and the integrity of the message could come into being by encrypting the credential messages through digest or hash with the message transmission.

The most famous Symmetric Key Cryptography is the Data Encryption Standard.

Asymmetric Key Cryptography is also called Public-key Encryption. A pair of keys is needed to finish the operation of encryption and decryption respectively. One of the keys is released to the public, namely the public key. The message sender uses the public key to make encryption while the receiver uses the private key to make decryption. The mechanism of the public key is flexible but with a slower speed than the Asymmetric Key Cryptography. [21]

In the system of Asymmetric Key Cryptography, the key is divided into a pair. Either key of the pair could be used as the public key (encryption key) to be released to the public in a non-private way while the other is kept as the private key (decryption key). The private key could only be held by the trader who generates the key pair while the public key could be widely released. [21]

The process of the message exchanges of the plan is like this: Merchant A produces a pair of keys and makes one of them the public key opened to the other merchants; merchant B who gets the public key uses it to make message encryption which will be sent back to merchant A. Then, merchant A makes decryption with the dedicated key to the encrypted message.

Asymmetric Key Cryptography mainly contains RSA, DSA, DiffieHellman. Etc.

2.2.2 Message Digest

Message digest is also called finger print; it is a value correspondent to an only message or text. A uni-directional hash encryption function acts on message, and generates a hash code, and it is hardly to be restored. Hash function can accept longer input data, and then finish it to a small data (usually 128-512bits). When inputted the same data, it can always generate the same output value. Output data is smaller then input data, therefore, one output data can correspond to several input data.

A good message digest algorithm should have the following two characteristics. First, this algorithm is unpredictable and unreasonable (i.e. the corresponding input value can be restored through experiment). Second, a slight change in input data may results in obvious changes in output data. For example, a changing of data bit in input data will results in changing of half of data bits in output data. This is actually a corollary of the first characteristic.

Message digest is designed to ensure the integrity of information.

2.2.3 Digital Signature

Digital signature is to use cryptographic algorithm to encrypt the primed data, and generates a section of data digest information, which will be attached in the original text. This section of information is similar to signature or seal. The receiver will verify it, and judge the

truthfulness of the original text.

The main way of the digital signature is like this: the sender of the message generates a message digest from the message. The sender uses his private key to encrypt the message digest to form the sender's digital signature. And then, this digital signature will be sent with the message as message's attachment to the receiver. There are mathematical relationships between public key and private key, data encrypted by one key can only be open with one key. The receiver of the message first calculates the message digest from the received original message, and then uses public key to decrypt the attached digital signature. If two message digests are same, then the receiver will make sure that the digital signature is the sender's.

Through verifying the signature, the following three things were make sure :

(i) This message is sent by the sender

(ii) The signature is generated by the sender

(iii) The message received by receiver is complete.

2.2.4 Digital Envelop

Digital envelop is also called digital packet, its main function is to guarantee the confidentiality of the data. In SET, when data is passed confidentially, first, there need to generate a symmetric key by random, and then use this symmetric key to encrypt data. After that, encrypt the public key of this symmetric key's receiver, which is called "digital envelop", and

send it with data to the receiver. This "digital envelop" can only be "unlocked" by receiver, because only receiver has the key to decrypt. When decrypting, receiver first uses his private key to decrypt digital envelope, and obtains key, then uses symmetric key decryption data, and gets the final data. The advantages of digital envelop is that it can speedup the encryption, and avoid the distribution of symmetric key.

2.2.5 Digital Time Stamp

In electronic commerce, there need to protect the security of trading document's data and time information, during which process there adopt the technique of digital time stamp. Digital time stamp is a kind of variant of digital signature technique. DTS (Digital Time Service) is used in providing security protection in electronic document's issuing time. Time stamp is an evidence document which is encrypted, it consists of three parts: abstract of document which needs to use time stamp, data and time when DTS receives document, and DTS's digital signature.

Generally speaking, the generation process of time stamp is as follows: users first uses Hash algorithm to encrypt document which needs to use time stamp to form the abstract, and then send this abstract to DTS. After adding data and time information when receiving the document, DTS will encrypt this document (digital signature), and send it back to user.

2.2.6 Double Digital Signature

Double digital signature means in some occasions, senders need to send two related

information to two receivers, one receiver can only understand one group of these related information, and another group will be transmitted to the other receiver. In this situation, sender should encrypt these two groups separately, and makes two digital signatures, which are called double digital signature.

Double digital signature is a new application of SET protocol's digital signature. It guarantees user's important information such as account is concealed from the merchant. For example, when cardholder provides ordering information to merchant, he also provides payment information to bank, which is convenient for him to authorize bank to pay. However, cardholder won't let merchant know his account's information ; Also, he won't let issuing bank know the concrete content of consumption. He just needs credit or debt according to money amount.

The concrete implementation methods are as follows: first generating abstracts of two messages, and linking two abstracts to generate a new abstract, which is called double signature. Then encrypt it with sender's private key. In order to let receiver verify the double signature, there must send the other message's abstract. In this way, any message's receiver can verify the truthfulness of the message according to the following method: generating abstract of the message, linking it with the other message's abstract to generate new abstract. If it is equal to double signature after decryption, then can guarantee that this message is true.

The working process of double signature is shown in the following Figure 2-3:

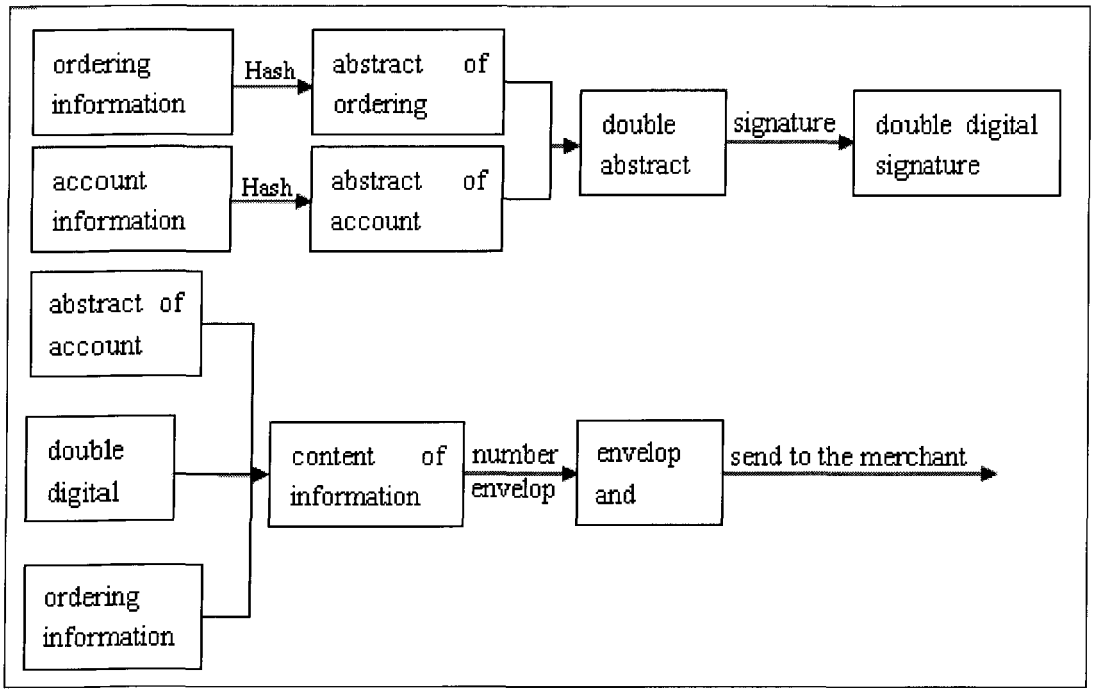


Figure 2-3 Customers' generation double digital signature

Merchant verifying digital signature is shown in the following Figure 2-4

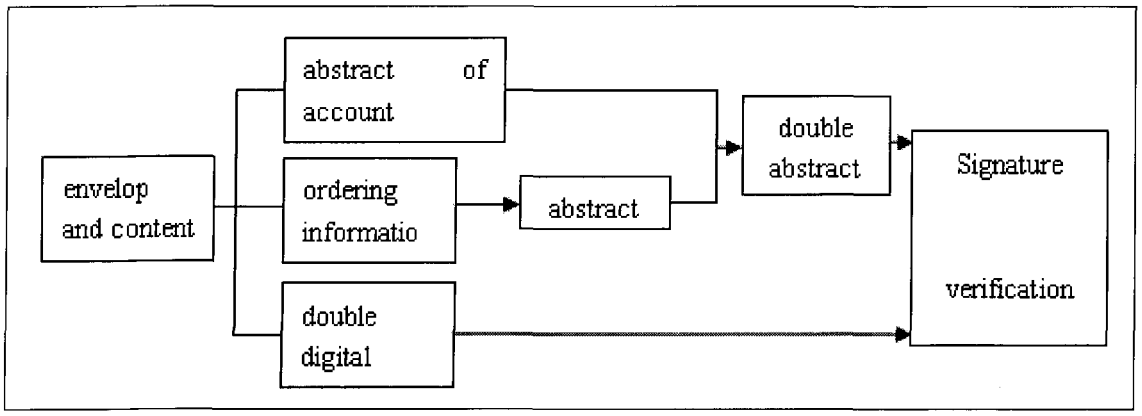


Figure 2-4 Merchant verification double digital signature

In SET, each user at least has two pairs of keys, one is signature key and a pair of encryption key, each pair of key has the corresponding digital certificate. Private key is kept by user, and public key is kept by CA center.

2.2.7 Digital Certificate

Digital certificate is also called digital evidence, memory or certificate; it is legal identity certificate of participants in transaction. It includes all encryption and signature public key, and can be proved its effectiveness through verifying in root CA. it uses electronic way to verify the identity of a user and the limits to right of visiting internet resources. In online electronic trading, participants show their digital certificate for counterpart to verify their identity, and use it to do business.

There are two kinds of digital certificates, one is signature certificate, which has signature public key to verify the identity of the sender; the other is encryption certificate, which has exchanging public key to encrypt symmetric key.

The simplest certificate includes a public key, name and digital signature of certificate authorities' center. In general situation, certificate also includes the effective time of key, name of certificate authorities center, serial number of this certificate, etc. the format of the certificate should conform to ITUT X.509 international standard.

2.3 The Payment Processing of SET Protocol [25][26]

The typical processing procedure of payment based on SET protocol is shown as follows:

(i) Cardholders apply for opening an account in a bank, and install correspondent software and digital certificate.

(ii) Cardholders (consumers) send initialization request to electronic merchant, and electronic merchant has initialization reply. Then cardholders receive and check this initialization reply. If there is nothing wrong with it, cardholders will send purchasing request to electronic merchant. Initialization request appoints transaction circumstances, transaction ID, the form of transaction card (payment form), etc. purchasing request includes payment information and ordering information of cardholders.

(iii) Electronic merchant receive and check cardholder's purchasing request, if there is nothing wrong with it, electronic merchant will send payment authentication request to payment gateway to verify the truthfulness of cardholders' payment information.

(iv) Payment gateway receive and check payment authentication request, and contact bank to verify payment information according to what are provided by cardholders.

(v) After verifying payment information, bank sends the results to payment gateway.

(vi) Payment gateway sends authentication reply to electronic merchant. The replying information includes authentication result of payment information and payment evidence.

(vii) Electronic merchant receives and check the payment reply of payment gateway, if there is nothing wrong, then send purchasing reply to cardholders. And contact payment gateway and request payment according to payment situation. Cardholders receive purchasing reply, and save purchasing evidence.

The authentication center of SET payment system is responsible for generating,

distributing and managing all participants' electronic certificate, and issuing certificates for all participants. Each participant can identify counterpart through checking their certificates.

2.4 SET Certificate and CA Hierarchy [36][38]

2.4.1 SET Certificate

Digital certificate is each entity's identity evidence online in electronic commerce. It proves matching relationship between entity's declared identity and its public key, which binds entity's identity and public key, from the mechanism of public key management, digital certificate is part of the key management in public key mechanism, that is to say, the distributing, sending is realized by certificate mechanism. Therefore, digital certificate is an authoritative electronic document; it is issued by a third-party organization which is authoritative, trustworthy and fair.

- **The type of SET certificates**

In SET protocol, there are cardholder's certificate, merchant's certificate, payment gateway certificate, bank certificate, issuing organization certificate, etc, in which cardholder's certificate, merchant's certificate, and payment gateway certificate is important.

Cardholder's certificate: it is for cardholder to use card (debit card, credit card) issued by card issuing organization to purchase and settle up the bill on line.

Merchant's certificate: it is for merchant to sell goods or services through internet, and

links with payment gateway to realize capital allocation.

Payment gateway certificate: it is for services provided by payment gateway, and the transformation between various security protocols on internet and bank's current network data format.

- **The structure of the certificate[13]**

The format of SET protocol of digital certificate usually adopts X.509 international standard. X.509 is part of X series of international standard suggested by ITU and ISO. It is now the most widely used public key system in the world. X.509 defines the concrete requirements of standard field and expanded field in digital certificate.

Authentication center generates user's certificate by sign on a group of information. These information includes the user's recognizable name and public key, and additional information. The following is the format of X509V3 format:

Version number	Serial number	Signature algorithm	issue	validity	subject	subject public key infor	issuer Unique ID	subject Unique ID	extension

The ASN.1 data type used by this certificate is shown as follows:

```
Certificate::=SEQUENCE{
    Version                 [0]Version DEFAULT v1 ,
    serialNumber            Certificate SerialNumber,
    signature               AlgorithmIdentifier,
    issuer                  Name,
    validity                Validity,
    subject                 Name,
                            SubjectPublicKeyInfo,
```

```
subjectPublicKeyInfo          [I] IMPLICIT Uniqueldentifier OPTIONAL,
                               //If present, version shall be v2 or v3
issuerUniqueldentifier        [2] IMPLICIT UniqueIdentifier OPTIONAL,
                               //If present, version shall be v2 or v3
subjectUniqueldentifier       [3] Extensions OPTIONAL
                               //If present, version shall be v3
                               }
extensions
```

Some fields' are defined as follows:

```
Version                        ::=INTEGER{v1(0), v2(1), v3(2)}
Certificate SerialNumber       ::=INTEGER
AlgorithmIdentifier            ::=SEQUENCE{
algorithm                      ALGORITHM.&ID({SupportedAlgorithm}),
parameters                     ALGORITHM. & Type ({ SupportedAlgorithm}
                                                  {@algorithm})OPTIONAL
                               }
Validity                       ::=SEQUENCE{
notBefore                 Time,
notAfter                  Time
                               }
Time                           ::=CHOICE{
utcTime                    UTCTime,
generalizedTime            GeneralizedTime
                               }
Uniqueldentifie           ::=BIT STRING
SubjectPublicKeyInfo      ::=SEQUENCE{
    Algorithm                  Algorithmldentifier,
    subjectPublicKey           BIT STRING
                               }
Extensions                ::=SEQUENCE OF Extension
Extension                 ::=SEQUENCE{
    extnID                     OBJECT IDENTIFIER,
    critical                   BOOLEAN DEFAULT FALSE,
    extnValue                  OCTET STRING
                               }
```

The explanation of each field in certificate:

Version: version field indicates the X. 509 version number (1,2, or 3) of certificate's format,

and prepares for new version in the future.

Serial number: in one domain, each certificate issued by CA must has a unique digital symbol, this digital symbol is saved in serial number field.

Signature: it indicates signature algorithm used to certificate by CA, including public key encryption algorithm and message digest when CA give signature to certificate.

Issuer: issuer field means X500 name of CA which issues certificate.

Validity: validity field offers the period of validity of certificate, including effective date and expiry date. When using certificate, application software will check the date of certificate to make sure it is validity.

Subject: subject field indicates the name of entity (service or user) that holds the certificate.

SubjectPublicKeyInfo: this field includes two parts of important information, the public key value of certificate holder and algorithm symbol of encryption which the public key uses.

IssuerUniqueID (Version 2.3 only): this field is added into certificate in X. 5.9 version 2, it is a selective field. Considering certificates are issued continuously, the same X. 500 name may be used in more than one CA, therefore, this field is added for issuer to provide a unique X. 500 name.

SubjectUniqueID (Version 2.3 only): this field is also added into certificate in X. 509 version 2. it is also a selective field. It is the unique ID of certificate holder.

Extensions: including Authority key ID, subject key ID, key application, extended key

application, CRL distribution points, another name of subject, and another name of issuer, etc.

2.4.2 CA Hierarchy

For the convenience of certificate's management, SET protocol defines a set of complete certificate trust chain system, and CA, as the authority to manage certificate and main executor, realizes its function through this trust chain.

As the cornerstone of certificate management, the trust chain of certificate establishes an abstract hierarchical model which is based on practical application. Through the frame is describe (Figure 2-5), there can find the hierarchical relationships among participants' certificates.

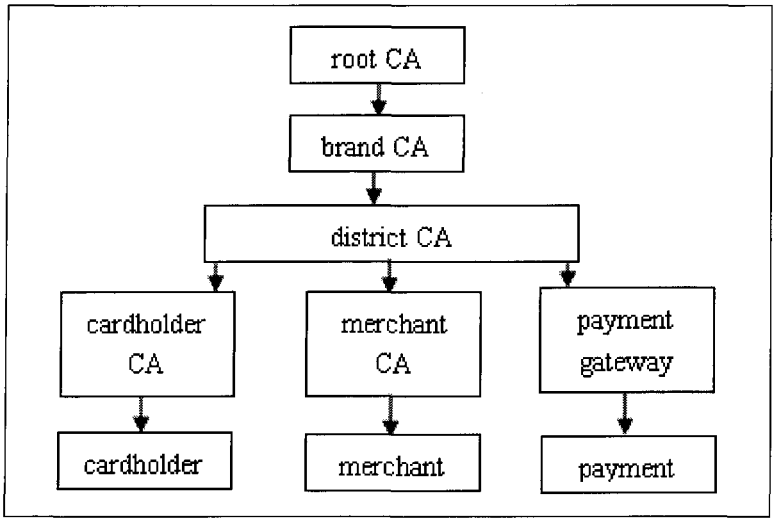


Figure 2-5 the CA hierarchy of SET protocol

The hierarchy of certificate management is composed by 9 parts, in four layers, in which each layer is generated by its upper layer. The paramount is root CA; it is the foundation of low level CA certificate. It can generate brand CA, and brand CA will generate district CA, payment

gateway CA, merchant CA and cardholder CA. And certificates of cardholder, payment gateway and merchant are issued by corresponding CA. Because of the importance of root CA in SET protocol, it is usually settled in area which is protected strictly and securely, and it is always in off-line situation. Only when new brand CA needs to be issued, root certificate is renewed, and CRL is generated, it will work on-line. In general situation, root CA is hardly to be attacked by outside. Also, band CA, district CA, payment gateway CA, merchant CA and cardholder, as the functional module of CA, are protected in the same way. The difference is that they are always on line; users can obtain correspondent certificates directly through Web or Email.

The certificate trust chain which is reflected by hierarchy of certificate's management, determines ways to verify the validity of certificate. Each certificate is related to its issuer's signature certificate. In communication process between transaction participants, each will trace back counterpart's certificate to the root certificate along the trust chain to testify the validity of this certificate. For example, the validity of customer A's certificate is verified by CA in its issuer's district, and district CA's certificate is verified by the corresponding brand CA, and finally CA's validity is guaranteed by root CA. In this way, according to views in logic, customer A's certificates is verified.

2.5 SET's Operating Environment

SET does not define how SET information is transmitted among entities. SET information

can transmit among mechanism agreed between receiver and sender. However, For encouraging the interaction among the developers, when using internet, the communication between SET entities is used by standard transmission in Internet, so the SET environment is divided into two parts:

(i) Interaction environment. There is certain retardation time in messages exchanging communication among entities, such as WWW (World Wide Web).

(ii) Non-entity environment. There is long retardation time in messages exchanging communication among entities, such as e-mail.

2.6 Summary

This chapter introduces in details about the technique standard and regulation, security mechanism, payment processing procedure, certificate mechanism and objective of SET protocol. The security mechanism of SET protocol adopts combinations of many security mechanisms such as DES algorithm, digital signature, and digital envelop and double digital signature, digital time stamp. Double digital signature is the new application of digital signature promoted by SET protocol, it ensures that important information such as customer's account is hidden from merchant, this chapter introduces in details about the procedure and characteristics of double digital signature. There are five parts in the payment processing procedure of SET protocol: cardholder registration, merchant registration, purchasing request, payment request, and payment

authorization. This chapter also introduces SET certificate structure and CA level structure. In SET protocol, there are cardholder certificate, merchant certificate, payment gateway certificate, bank certificate, and issuing organization certificate, etc. the digital certificate's format of SET protocol usually adopts X.509 international standard.

CHAPTER 3

ANALYSIS ON THE DEFICIENCY AND IMPROVEMENT OF SET PROTOCOL

This chapter mainly discusses SET protocol's working procedure. At the same time, and this chapter also discuss another commonly used security protocol SSL in electronic commerce, and compare these two protocols, find the deficiencies of SET protocol, and raise corresponding improvement proposal.

3.1 Secure Sockets Layer (SSL) [32]

SSL (Secure Sockets Layer) protocol was first developed by famous Netscape Company. And now it is widely used in ID authentication on internet, and the data safe data communication between Web server and user side browser. SSL protocol is located in the session layer, on top of the TCP/IP protocol. It is used to encapsulate the upper protocols. It provides services from the following three aspects: the validity authentication of user and server; encrypt data to hide the transmitted data; and keep the completeness of data.

3.1.1 The Transaction Process Based on SSL Protocol

SSL protocol is composed by SSL recording protocol and SSL handshake protocol.

SSL recording protocol includes regulations on recording head and data format. In SSL protocol, all transmitted data is encapsulated in record. Record is composed by recording head and the recording data whose length is not 0. SSL's recording data includes three parts: MAC data, actual data, and attached data. all SSL's communication includes handshake message, safe blank record and application data, which use SSL's recording layer.

SSL's handshake protocol includes two phases: the phase is used to construct private communication channel (from the first step to the fourth step), the second phase is used for user authentication (from the fifth step to the eighth step).

(i) The initiation phase of communication, user send a greeting message to server and server must send back a server greeting message to reply. This information includes certificate, encryption rule and linkage symbol held by the server. These greeting messages are used to make sure whether it is necessary to have a new key. If not necessary, both sides come into the second phase of handshake protocol;

(ii) If a new a key is needed, then user generated a new key through server's greeting message.

(iii) User and server exchange codes which are recognized by both sides and generate the discussion code which is used in discussion. Therefore, four keys are need in one link, they are: user's reading key, user's writing key, server's reading key, and server's writing key.

(iv) Checking code.

(v) Server send authentication requesting message to user.

(vi) When user receives the authentication requesting message from the server, he will send his authentication certificate and monitor the result send from the counterpart.

(vii) Server check user's certificate.

(viii) User and server exchange the ending messages.

When the above actions are finished, both sides begin to transmit information. SSL adopts key technique to guarantee the privacy and completeness of the data. Sender transmits the information after encrypting it with public key, and receiver uses private key to decrypt obtained information. Even the intruder gets encrypted information on the internet, if they don't have the key, they can not read the information. SSL make sure that user's inputted credit card number and other information can be obtained by merchant which provides services for them only. User can also print the authorized order shown in the screen, in this way, he can get the written evidence of this transaction. Most online merchants show the evidence after receiving user's credit number, which is user's reliable evidence to show he has paid. According to SSL protocol, the purchasing information of user is first sent to merchant, and then merchant transfers it to bank. After verify the validity of user's information, bank will notify merchant the success of payment. Then merchant will notify user that the purchasing is successful, and send the goods to user.

3.1.2 The Safety Advantages of SSL Protocol

The encryption algorithm and authentication algorithm adopted by SSL protocol have certain safety, which can stop some attacks.

(i) Monitor and man-in-the-middle attack

SSL uses an encryption algorithm and key which are determined by both sides of communication. Applying them on different safe level, there can find out different encryption algorithm which can be used in encrypting data. Its key management is better. It generates a temporary conversation key by producing a hash function. In addition to using different keys in different linking, each transmitting direction in one linkage uses independent key. Although SSL protocol provides many rules for listeners-in, it has better key protection for it adopts RSA exchanging key, so they can change the key frequently. Therefore, to monitor and man-in-the-middle attack, it has high precaution.

(ii) Data flow analytic attack data on flow

The core of data flow analytic attack is trying to attack by checking the clear fields of data packet or the attribute of unprotected packet. In general situation, the perniciousness of this attack is relatively small. However, SSL can not stop this attack.

(iii) Intercepting and jointing attack

When encrypting stronger links, it considers this kind of security. Basically, SSL3.0 can stop this kind of attack.

(iv) Message resending attack

Message resending attack can be easily stopped, SSL can stop this attack by including "serial number" in MAC data.

3.1.3 Flaws in SSL Protocol

(i) Key management problem

a) User's computer and server use rules to transmit the encryption algorithm which is supported by them. It can be attacked and revised, which makes them to use algorithm whose encryption digit is the shortest.

b) In order to be compatible to previous versions, SSL 3.0 may reduce its security.

c) All conversation key will generate master-key, and the security of handshake protocol totally depends on the protection of master-key. Therefore, in communication, its had better not use master-key too many times.

(ii) Conditionality

According to the regulation of America's Ministry of Interior, Netscape uses key with 40 digit in its international browser and server. If the key is too short, it is easily to be decoded.

(iii) The problem of digital signature

SSL protocol does not have the function of digital signature, that is to say, it does not have counter-denying function. User can not guarantee that merchant can keep his credit card

information as a secret, neither can he guarantee that merchant is the appointed merchant of this card; at the same time, merchant can not make sure whether this cardholder is legal or not.

First user's information goes to merchant, and merchant read it, in this way, the security of user's information can not be guaranteed. SSL can only make sure the security of transmitting process of the information. It can not guarantee whether it is deceit in transmitting process. Therefore, SSL can not realize the secrecy and completeness required by electronic payment. What's more, cross acceptance is very difficult.

SSL protocol can only keep data secret, and merchant can not make sure who fills this document. In addition, the settlement problem of bank has not been solved. Therefore, SSL protocol is only suitable for small scale transaction with common secure level.

The encryption link provided by SSL has very big loophole. SSL provides no other safety assurance except in transmitting process. SSL make users believe that merchants are authorized to receive payment by credit card. On internet, there are always some strange shops. Just because of this, there is larger chance for online merchant to cheat than ordinary shops. If an honest merchant does not adopt good method to ensure the security of user's credit card information, then this information can be easily stolen by hacker and the server of merchant.

3.1.4 The Comparison of SET Protocol and SSL Protocol [30]

Payment system is key to electronic commerce. SSL protocol and SET protocol are two important communication protocols. They both provide payment methods through internet.

Although they are both used in electronic commerce, because of the different aims in their original designing, except for they all use RSA public key algorithm, they have nothing in common in technique perspective.

The encryption applied in SSL includes secret-key cryptography and public-key cryptography. Before the data switching between client and server, they need to exchange the initial handshake information which is encrypted with all kinds of cryptographies to guarantee its confidentiality and the completeness of data, and is identified by digital certificate. So that it is impossible for illegal user to break.

In SET protocol, the security of payment environment needs to put secret-key cryptography and public-key cryptography together. Here the secret-key cryptography applies DES, while the public-key cryptography applies RSA. The joint of these two different cryptographies is vividly called digital envelope. RSA is just like the seal of the envelope, first, the information is encrypted by 56byte DES, and then put into digital envelope encrypted by 1024 byte RSA, at last it is transmitted between buyer and seller. The combination of these two cryptographies keeps the data information confidential in trading.

SSL provides the safe linkage between two machines. The payment system is usually constructed through transmitting credit card number in SSL linkage. Online bank and other financial systems are also always constructed on SSL. The reason why SSL is widely used is that it is internally installed in most web browser and web server, which enables it to be used easily.

SET is a protocol which is based on information flow. It is also a message protocol in many ways. It defines required message rules among bank, merchant, and cardholder. At the same time, SSL simply build the security linkage between both parties. SSL is connection-oriented, and SET's allowing of message exchanging among parties is not real-time. SET message rule can be transmitted in internal network and other networks, and the card payment system based on SSL can be bound only with web browser.

To consumers, SET guarantees the validity of merchant, at the same time the credit card number of user won't be stolen. On the other hand, SSL protocol is lack of the authentication of the merchant. SSL is used in many electronic commercial servers. It provides the security of conversation level, which means as long as a secure conversation is built; all communications on internet will be encrypted. And when data is transmitted to merchant's server, all data will be decrypted. Using SSL, consumers can not guarantee that merchant can have on their credit card information confidential, there is no guarantee of the payment card merchant is a freelance merchant.

SET defines interoperation interface for each member in the transaction, one system can be composed by products from different companies. One advantage of SET is that it can be used jin part of the system all the whole system, some merchants are considering using SET in connection with bank, and using SSL in connection with customers. This method avoids installing stored value card in customer's machine, at the same, it gets advantage of SET.

3.2 The Procedure Performance Analysis of SET Protocol [24][31]

3.2.1 The Working Procedure of SET Protocol

SET protocol uses DES symmetric key algorithm, RSA non-symmetric key algorithm to provide functions such as data encryption, digital signature, digital envelop. The cost of this protocol is very big, and customers, merchants, and bank should install corresponding software.

There draw into the following symbols for convenience:

C	customer
M	merchant
P	paying bank
I	issuing bank
SK	private key
PK	public key
E	encryption
D	decryption

The payment procedure of SET protocol is shown in Figure 3-1 as follows:

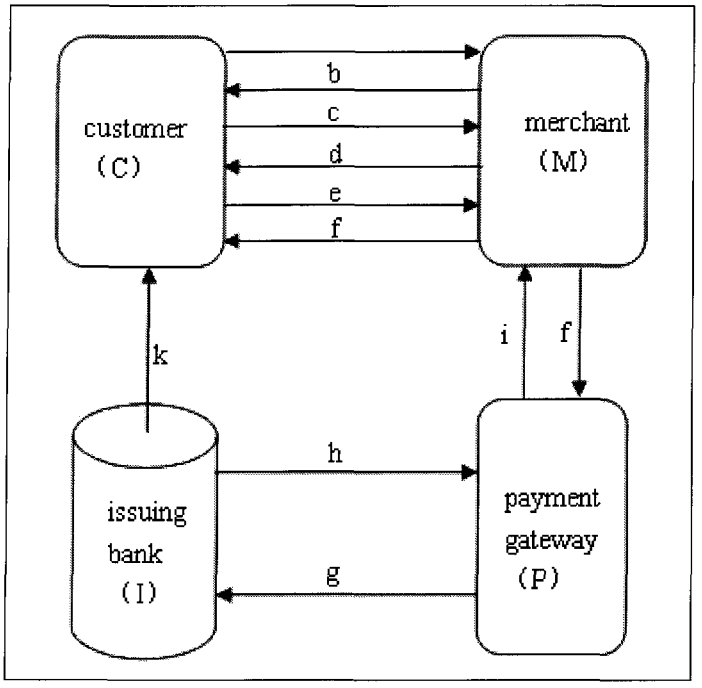


Figure 3-1 Payment procedure of SET protocol

(i) Customer send purchasing request to merchant (message a);

(ii) Merchant send the catalog to customer (message b);

(iii) If customer agrees to buy, then make digital signature to OI (Order Instruction):

OI'=ESKC(OI)

ESKC(OI)=Encrypt OI with Customer's Private Key, namely, customer make digital signature to OI with his/her private key.

And send signed OI' to merchant (message c);

(iv) Merchant decrypt received OI':

OI=DPKC(OI')

DPKC(OI')=Decrypt OI' with Customer's Public Key, namely, merchant verify the

customer's authenticity.

Make sure OI is sent by this customer;

Merchant do digital signature to his own digital certificate CerM (certificate of merchant), digital certificate of payment gateway CerP (certificate of payment gateway) and payment requirement Pay:

$$Y=ESKM(CerM,CerP,Pay),$$

Then send it to customer (message d);

(v) Customer receives Y, and decrypts it:

$$(CerM, CerP, Pay)=DPKM(Y)$$

Make sure Y is sent by the merchant, and make sure the identity of merchant and payment gateway.

Customer generates PI (Payment Instruction) which is required by Pay, and do digital signature:

$$PI'=ESKC(PI)$$

Encrypt PI with customer's private key, namely, customer make digital signature to PI.

Customer generates randomly a symmetric key K, and encrypts PI with K:

$$PI''=EK(PI')$$

Encrypt PI' with secret key K.

Encrypt customer's account information PAN and K with public key in payment gateway:

PA=EPKP(PAN,K)

Because customer has certificate of payment gateway at this time, he/she can make digital envelope to PAN and K with public key of payment gateway. EPKP(PAN,K)=encrypt(make digital envelope) PAN and K with public key of payment gateway. PA is digital envelope of PAN and K.

Do digital signature to customer's digital certificate CerC. PI and PA:

Y1=ESKC(CerC,PI",PA)

Encrypt Certificate of Customer, PI" and PA with Customer's private key, namely, customer does digital signature to CerC,PI",PA. Y1 will be given to merchant. PA is digital envelope to payment gateway, only payment gateway can unseal it, merchant can't open and read it. So customer's account number and secret key K is secure. PI" is secret text encrypted with secret key K, merchant can not also read it, which prevents merchant from getting customer; payment information. There call Y1 as dual signature. Purposes of dual signature are both to pass account/payment information to payment gateway and to prevent merchant from knowing customer's account information.

Then send it to merchant (message e);

(vi) Merchant decrypt Y1:

(CerC,PI",PA)=DPKC(Y 1)

Make sure it is sent by this customer.

Do digital signature to CerC, PI, PA and merchant's digital certificate CerM:

Y2=ESKM(CerM,CerC, PI",PA)

Then send it to payment gateway(message f);

(vii) Payment gate decrypt received Y2:

(CerM,CerC, PI",PA)=DPKM(Y2)

Make sure it is sent by this merchant.

Decrypt PA, and make sure it is sent by this customer:

(PAN,K)=DSKP(PA)

And decrypt PI" with key K:

PI'=DK(PI")

And then decrypt PI:

PI=DPKC(PI')

Send payment order PI to the issuing bank (message g);

(viii) Issuing bank verify the message, make sure the account of customer is valid, and then send verified PI to payment gateway (message h). Therefore, funds movement occurs between customer account and merchant account.

(ix) Payment gateway send finished message Mrg to merchant and encrypt it (message i):

Mrg'=ESKP(Mrg)

ESKP(Mrg)=encrypt message with private key of payment gateway, namely, payment gateway does digital signature to message.

(x) Merchant receives payment finishing message and decrypt it,

Mrg=DPKP(Mrg')

Merchant does un-sign to message.

Finally send goods to customer and provides receipt (message j);

(xi) Issuing bank provides consuming receipt to customers regularly (message k).

From the transaction process of SET, There can conclude that SET is strict in designing, and considerable in each step, which solves the secure problem of customer's information. Merchant can not see the credit card account of customer, and bank can not see the ordering information of customer; SET also solves the authentication problem between, customer and merchant, customer and bank, merchant and bank, which can effectively prevent the occurring of fake problem; all transaction process is on line, which guarantees the real-time of on-line transaction; it ensures the security of electronic commerce information with encryption technique, Hash algorithm, digital signature, digital envelop, the third organization CA, etc.

On the other hand, SET is a complicated protocol. It endures the security of information through encryption, signature, etc. from a certain perspective, SET's emphasis on security is realized through sacrificing performance, sometimes it is unworthy for some small-scale transaction, because the sacrifice is too much. Here can count the times of encryption, signature, certificate transmission, and certificate authentication in SET, to further verify the complexity of its application.

Table 3-1 Certificate transmission and verifying times statistics

	Transmission times	Authentication times
cardholder	1: cardholder's signature certificate 1	3: merchant signature certificate 2;gateway encryption certificate 1
Merchant	5: cardholder signature certificate1;gateway encryption certificate1;merchant encryption certificate1; merchant signature certificate 2	3: cardholder signature certificate1; gateway encryption certificate 1: gateway signature certificate 1
Gateway	1: gateway signature certificate 1	3: cardholder signature certificate1; merchant signature certificate 1;merchant encryption certificate 1

Table 3-2 Signature and authentication times

	Times of signature	Times of authentication
cardholder	1	2:merchant signature
merchant	3	2: cardholder signature; gateway signature
gateway	1	2: cardholder signature; gateway signature

Table 3-3 Encryption and decryption times

	Times of encryption		Times of decryption	
	symmetry	Non-symmetry	symmetry	Non-symmetry
cardholder	1:merchant; gateway	1:merchant; gateway		
merchant	1:gateway	1:gateway	2:merchant; gateway	2:merchant; gateway
gateway	2:merchant	2:merchant	2:merchant; gateway	2:merchant; gateway

From the above analysis, shows that, SET protocol is complicated, this involves several entities. Both merchant and bank need to improve the system to realize interoperation, which is

troublesome. SET requires installing corresponding software on bank's network, merchant server, and customer PC, and sending certificate to each member. It cost very much. In addition, SET transaction model can be used in BtoC business model only. It can not be used in BtoB business model, and its application in BtoC business model is very limited, only some restricted card payment business.

3.2.2 Performance Deficiency in SET Protocol

SET is a security protocol standard of on-line transaction through internet. It is designed to solve customer, merchant, and bank's payment through credit card, which can ensure the secrecy of payment information, the completeness of payment process, the valid identity of each member and it's undeniable, etc. although there are many advantages in SET protocol, its application is not very popular. It has the following problems:

(i) SET only supports credit card consumption. SET protocol mainly transmit the account information of cardholder, code PIN is not used. But in China, debit card is mainly used.

(ii) SET transaction process only guarantees the atomic nature of money. The atomic nature of sending and merchant are not guaranteed. That is to say, it cannot guarantee that customers receive the goods, and the received goods are what they have ordered. If good provided by merchant is not qualified, or customer declares that the goods are not qualified, and refuses to receive the goods, even blackmails the merchant, how to umpire this kind of dispute [26].

(iii) SET's message is too complicated. SET defines message of payment process and data definition. Because its normalized aim is worldwide application, therefore, main elements considered are American payment pattern. To other countries, the message is too complicated, which makes SET application software complicated in design, high in price. The popularity of SET is influence.

(iv) SET protocol is too complicated. It requires too many installed software packages. And it is slow in processing and expensive. To small-scale transaction, the low efficiency and high cost brought by high security are unworthy. At the same time, SET involves too many entities. In order to realize SET payment, cardholder, merchant, payment gateway and CA must support SET at the same time, therefore, the construction and coordination among each member lead to poor interoperation.

(v) SET does not solve the problem of generating and maintaining data in transaction. SET protocol only solves the authentication of payment information. SET technique standard does not mention how to safely save or destroy these data after finishing the transaction; this loophole may suffer potential attack afterwards.

(vi) For each payment, time term is key information, which is especially important in network transaction process. Time and signature are the same key contents in preventing fake and falsifying. It is easy to change the time stamp of a document in computer. Therefore, in electronic transaction, there should adopt corresponding measures to documents' data and time information.

There must be unified time control, arbitration of transaction time by the third party. These measures can prevent denying afterward.

3.3 Expansion and Improvement Proposal for SET Protocol

In the previous two sections, introduced SSL protocol, another common used protocol in electronic commerce; and through analyzing SET's working procedure, there point out the deficiencies of SET protocol. These deficiencies are all basic reasons which influence its popularity. Therefore, only expand and improve it to enable its security, high efficiency and low cost can be achieved.

3.3.1 SET Protocol's Support to the Debit Card

The original SET protocol is designed on the basis of credit card transaction. It uses credit card as payment tool. The main difference between credit card payment and debit card payment is that the credit card to be not had the overdraw function. As for debit card, customer must deposit first. Overdraft has a certain limit, and debit card should has PIN to identify.

In China, the personal credit system is not built. In comparison with developed countries, credit system does not nearly exist, which hinders electronic payment based on credit. At present, people transact by hand-to-hand payment mainly. Debit cards are more popular than credit cards.

There is a PIN (Personal Identification Number) in a debit card. This number is equivalent to a password. User must input the correct PIN to login transaction system. PIN is built on

authentication mechanism. On the other hand, a credit card has only a PAN (Personal Account Number), not a PIN. User should not input any password-like information.

SET 1.0 is designed to support credit card transaction only. In order to let SET protocol support debit card, the SET protocol should be revised. However, the revision should be done on the premise of not influencing commonality of SET protocol.

- **Suggested structure of supporting debit card**

Because at present in China, debit card payment needs to input PIN, and SET 1.0 standard is mainly used in credit card. It only needs PAN information (credit card number), but not defines the processing method of PIN. In SET protocol, the identity of cardholder is guaranteed by certificate of cardholder and PAN of payment card, PAN is the key data of cardholder. And PIN and PAN should have the same security requirement, so there consider using the same encryption process of PIN.

Online PIN encryption mechanism is shown in the following Figure 3-2; PIN is inputted into computer through keyboard and other equipment. PIN data is in RSA/OAEP (Optimal Asymmetric Encryption Padding) module of SET protocol, which is protected by payment gateway public key and symmetric encryption. The encrypted PIN in SET protocol is transmitted to payment gateway through merchant, and payment gateway uses private key to unlock the envelop, and then uses symmetric key to decrypt PIN data. If needed, the PIN data should be transfer into other PIN module format, adopts symmetric key to re-encrypt, and then send re-encrypted PIN data to

payment card network.

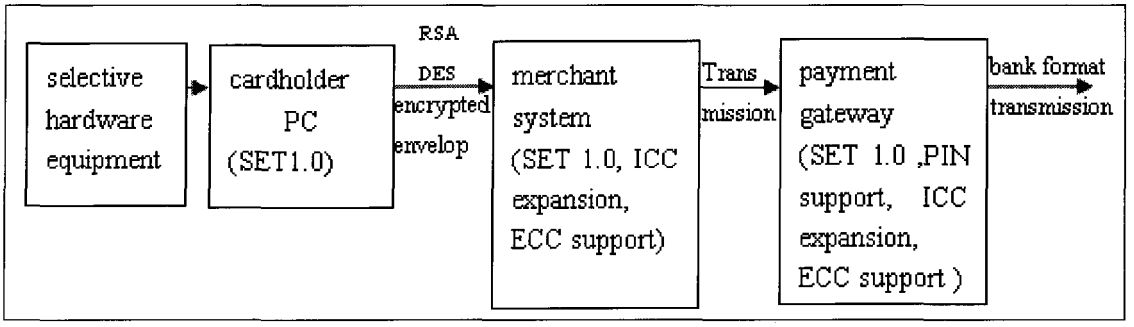


Figure 3-2 SET's support to debit card

PIN's format should conform to IS09564-1 Format0, PIN module uses eight bytes. In formatting operation, a binary system exclusive-OR of a rule's PIN data area and account number data area should be done. The purpose of exclusive-OR is to strengthen the relevance of PAN and PIN data, and to prevent exchange and attack.

The format of PIN is as follows:

C	N	14-12 tetrads , if no enough, fill it with 1111	F	F
0	1	2	14	15

C=controlling data, generally uses to represents "Format 0".

N=PIN length , Obit binary number from 0100 to 1100.

PIN's value is number from 4 to 12; each number represents four digit binary numbers. They are listed from left to right, if no enough, fill it with binary system 1111.

F=occupation number, C、 N、 PIN area use PIN's first 14 number, the left 2 numbers is set up as 1111

Account number data area's format is shown in figure 4-2, each of the first four Obit number

contains binary system 0000.

Other 12 binary system numbers is ordered on the basis of the right one, if not enough, fill it with binary system 0 from the left side.

0	0	0	0	12flush right

- **Cardholder and payment gateway's support to PIN**

In order to let cardholder know whether a certain card needs PIN, we need to increase a expanded item in certificate, to mark whether PIN should be input. At the same time, there can use the mark bit of id-set-PIN-Secure-Source and id-set-PIN-Any-Source to distinguish whether it is necessary to use secure PIN inputting equipment.

Cardholder's PIN process is as follows:

(i) After customers selecting paying card, cardholder software needs to know which payment card should have online PIN. Through the expansion item of this card's corresponding certificate to decide whether this card need to input PIN. If needed, then obtain PIN with inputting equipment, build message's PIN data area. Cardholder software does not keep PIN, once PIN is encrypted, and PIN message information in memory must be cleared.

(ii) Build account data area, SOR rules' PIN data and account data area. Use symmetric key to encrypt PIN data area after SOR.

(iii) Encrypt symmetric key with RSA public key of payment gateway. The encrypted PIN data is transmitted to payment gateway through merchant, and payment gateway uses private key.

The processing of payment gateway is as follows:

(i) Implement standard RSA/OAEP process, use payment gateway private key to decrypt, which will decrypt symmetric encrypted key;

(ii) Decrypt PIN encrypted data with symmetric key;

(iii) Rebuild PAN's data area, and XOR with PIN data module, which will get PIN;

(iv) Send PIN data to bank for verifying after transferring the format accordingly.

In China, for debit card, the main way of SET' payment is "authorizing, approving, and transferring". This function is necessary for debit card. The SET payment procedure of Chinese debit card is as follows:

(i) When purchasing goes into the paying phase, cardholder first sends purchasing requesting message PReq to merchant;

(ii) Merchant receives PReq requesting message and confirms the identity of cardholder, then sends authorizing requesting message AuthReq to payment gateway;

(iii) When merchant generates authorizing requesting message AuthReq, he should set "Capture Now" sign in this message.

(iv) Because it is needed to be paid immediately, therefore, after payment gateway receives AuthReq, it links issuing bank and acceptance bank. Issuing bank first check the identity of cardholder, and then check whether cardholder's account balance is less than what to be paid, then transfer the fund from issuing bank and acceptance bank.

(v) If refund is needed after transaction, there can send refund message to deal with.

3.3.2 SET Protocol's Satisfaction on Atomic Nature

SET protocol regulates in details about the identity authentication of each member of transaction. At the same time, it guarantees the balance of fund in each direction, money amount paid by customer is equal to what obtained by merchant. And funds transferred by payment gateway must be equal to what is received by merchant. The amount of fund won't appear or vanish from nothing, that is to say, SET realizes money's atomic nature.

However, SET has not satisfied the atomic nature of goods, which means merchant receives money, but he does not send goods; on the other hand, customer may receive goods, but does not send the money to merchant. However, the later phenomenon almost never happens in current SET mechanism; because SET's procedure is started from merchant getting money from payment gateway, then merchant will send the goods, which makes customer become the weaker part in the originally fair transaction.

At the same tine, SET does not satisfy atomic nature of sending. In SET transaction, customer purchases goods on a virtual network shop through internet. They can not see and try the real goods. They can only know about various kinds of goods by pictures and description words, then they decide whether to buy them or not. Therefore, the following problems are existing: there are differences between the goods they buy and what they see on the internet, or there are quality problems; on the other hand, if sometimes customer does not want to buy the goods, and demands the return of goods. For these problems, SET protocol does not has corresponding solutions. There

is no third party which both sides trust to do arbitration.

In previous introduced SET protocol working procedure, when merchant send message of requesting payment to bank, there is a time item attached to it, that is, Y2=DSKM (CerM, Cerc, PI'', PA, Tim). The time item includes merchant sending time T and predicted arriving time. It is written by merchant according to his own situation of goods supply, service ability, customer's area and goods' characteristics.

The concrete writing mode is as follows:

On the online purchase website provided by merchant, when customer fills the detailed shopping list, there are some essential options, customer address, purchased goods and amount. After customer checks the list, he submits the form.

Then merchant classify their goods according to current logistics situation such as merchant service ability, goods sending channel, kinds of goods, nature of goods, customer address, etc. this kind of classification can be rough. The purpose of classification is for software of merchant server to offer delivering time of some goods. When merchant server receives purchasing information list submitted by customer, server background processing system calculates delivering time and predicted arriving time of goods according to information provided by customer and goods' classified information provided by merchant. This kind of calculation can be estimate to some extent. And then return needed time to customer through browser immediately. Common software can easily realize this function.

After merchant sending Y2 to payment bank, payment bank gets the time item data through decrypting Y2, and then saves it in a special database. At the same time, other SET transaction steps are still going on. After issuing bank verifying customer's account number, payment bank notifies merchant to pay. After receiving message from payment bank, merchant sends goods or provide corresponding services to customer.

Here, payment bank transfers the money from customer's account, but the money won't be transferred to merchant's account immediately, instead, it will be kept in temporary database of payment bank's server, waiting there for a while. This waiting time is from delivering time to arriving time, until customer receives the goods. If there is no dissatisfaction from customer after he receives the goods, which means customer gets what he purchases. Then, payment bank will transfer the money to merchant's account. If merchant has not delivered goods on time, or the goods customer get are not what he ordered, then after customer waiting for time Tb, he can reports to payment bank, the payment center has the authority to conceal the transaction, and sends message to both customer and merchant. Merchant's responsibility is not in the range of SET protocol, merchant and customer should negotiate or solve related problem by legal means.

Moreover, if customer receives his ordered goods, but lies to the payment center about, merchant can prove his action through delivering system or document in postal system. Usually, post office requires signature when customer receive his goods to make sure the goods are sent to the right customer, this is the responsibility of the post office, which not belongs to the contents of

SET protocol. At the same time, the cheating of customer is legal problem involved by SET.

The above methods are to protect more customers' interests. In this way, previously weak customer becomes stronger, which enables SET protocol to satisfy the atomic nature of sending and goods. the following phenomenon won't occur: customer pays for goods, but cannot receive it; or what customer gets are not what he ordered.

3.3.3 Solution to the Problem of High Cost of SET Protocol

SET is a security electronic transaction protocol on the basis of online credit card payment. Before the transaction, it requires cardholder, merchant, payment gateway to install corresponding software and apply their own digital certificate to CA. in transaction process, there are many certificate's passing and verifying, and many encryption, decryption, and digital signature. The operation is very complicated, the price is very high, the operation efficiency is very low, and the adaptation is very poor.

Although the purpose of the above design is to guarantee the security of transaction process, there pointed out in previous that this kind of security is on the basis of sacrificing efficiency and cost. For small-scale transaction, this kind of spending is unworthy. What's more, sending certificate to each potential customer is not realistic. At present, install SET customer software on each computer which is linked to internet is not realistic either. For some customers, they purchase without applying certificate or their computers do not have SET customer software. All these are

hindrances to the development of SET.

The solution offered here is to do security level treatment to SET.

The so-called security stage treatment is increasing security level options when customers order goods. Here preliminary divide the security level of SET into: low level, SSL level, middle level, and high level. Customer can choose corresponding transaction level when they order goods.

(i) If customer chooses low level transaction mode, then customer and merchant do not need to verify each other. And the information of goods needs not to maintain secrecy. This is suitable for those customers who do not have certificates or whose computers do not have SET customer software. Of course, it is suitable to small-scale transaction too. Customer's PIN code of certain debit card or credit card is encrypted through payment bank's public key, which omit the certificate sending and inter-verifying between customer and merchant. the security verifying between merchant and payment bank should be guaranteed. At the same time, transaction information data is not required to be kept in file center; it will be destroyed after transaction.

(ii) For SSL level security level, merchant and customer need SSL link, and merchant and payment bank are linked by SET. SET is internally installed in many browsers; customer's computer also does not need to install SET software, but customer need to have his own certificate. Merchant will verify whether a customer is legal identity of a certain issuing bank according to SSL's procedure, which is introduced in previous part. Merchant and payment still exchange information according to SET.

(iii) For middle level security mode, all links among customer, merchant, and payment bank use SET protocol, then customers' computer must install corresponding SET software, and they must have their own certificate.

(iv) For high level transaction mode, in order to satisfy requirement of middle level security mode, operate according to normal SET protocol, at the same time, save various data information in file center for future use. If customer chooses high level service, he must pay for certain fees. The file center will be discussed in detail in 3.3.4.

In previous section, it is mentioned that time item is added in payment request generated by merchant, this time item is sent to customer and payment gateway at the same time. If merchant is dishonest, if the time value he sends to customer (Tim -C) is not equal to the time value he send to payment gateway (Tim_ P), that is Tim C>Tim_ P, then merchant can make use of this time difference, to achieve the purpose of deceiving. When customer has not received the goods, and has not report the goods' quality, merchant has obtained the transferred money.

In order to solve this problem, when customer chooses high level security, customer will send the time item to customer, that is Tim-C, at this time, customer uses his private key to send the signature to merchant, merchant will encrypt it with private key, and then send it to the payment gateway, payment gateway will verify and ensure this information is from merchant, and ensure that it is time item received by customer, then, compares it with time item Tim-P which is sent by merchant, if these two are equal, then it concludes that the merchant is not cheating.

Adopting the way of transaction scale level to reduce SET' high cost in some transaction, to improve its efficiency, this is a must in customer's ordering process. This method enables customer security; it is also helpful for customer without certificate and computer without SET customer software. However, low level security is only suitable for small-scale transaction.

3.3.4 Processing of Various Data in SET Protocol Transaction

In transaction process, there are large amount of information exchange among customer, merchant, payment bank and issuing bank, each data must be kept secret strictly, and can not be leaked. Some important data must be saved accordingly. SET protocol does not offer suggestion in this respect.

Add a file center in the server of payment bank, the file can be divided into two parts: 1) goods information file: various data related to goods information, including customer's ordering time, type of the goods, amount, delivering date and arriving date; 2) fund information file: various data related to fund information, including transferring time, transferring amount, customer and merchant's account.

One of the principles of electronic commerce is that merchant can not see information such as customer's account, and payment bank can not see customer's purchasing information. Then the files should be kept with encryption separately, goods' information file is encrypted by merchant with public key, and fund information file is encrypted by payment bank with public key. Partly link

the encrypted two files, and adds time stamp, encrypted them with public key in CA center to avoid cheating.

From the analysis of SET protocol's procedure, there can see that merchant can not obtain any customer's information which is related to fund, and payment bank can not obtain any information related to goods, because they lack corresponding private key which can decrypt. In this way, their authority is limited, and customers' benefits can not be damaged.

Let us suppose that the adding of file center can not only add security, but also increase the expense. In this point, the additional expenses should be negotiated by customer and merchant, and paid by customer. Just like sending package in post office, if you support value , you must fill in the value of the goods, you should pay some insurance fee according to the value. For some important transaction, it is worthy to save some important data.

3.3.5 Processing of Time Item in SET Protocol Transaction Process

From the previous analysis, can see that changing a time symbol of a certain file on computer is very easy. Therefore, we must adopt corresponding security measures of data and time information involved in each transaction in electronic commerce, to prevent participants denying the transaction afterward.

A doable method is to increase the function of authentication center, which provides DTS service as the third party organization in electronic commerce. In electronic commerce, once the

transaction between customer and merchant is successful, then both sides can not deny the validity of this transaction. Authentication center has the authority of arbitration when members of transaction argue before transaction is confirmed to be successful, that is to say, whether the transaction can be canceled or it is valid.

The generation of digital time stamp can be divided into two steps. First, does Hash algorithm to file which need digital time stamp, and generate this file's digital digest, then send this digest to authentication center? Second, authentication do digital stamp to the file after adding data and time information to received file digest, then return it to the sender. The process of DTS is shown as follows in Figure 3-3:

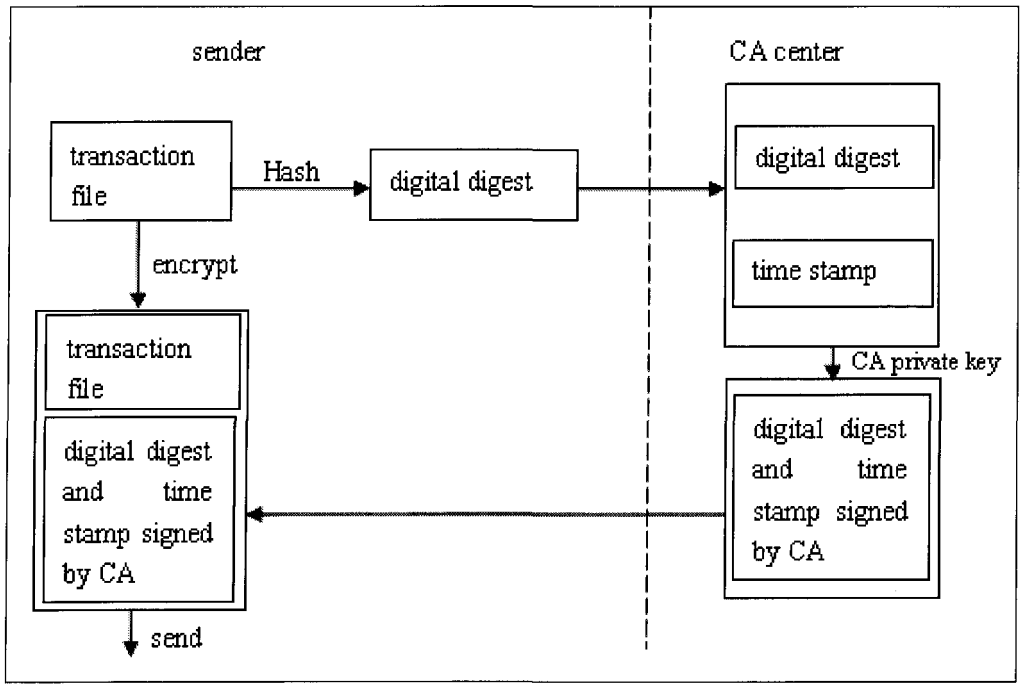


Figure 3-3 CA center provides time stamp service

3.3.6 SET's Processing to Network Transmitting Error

SET protocol's work is done by making use of internet. All data flow is transmitted in the network, once network is wrong or receiver does not receive information sent by sender immediately, then the imbalance of electronic fund flow may happen, and results in lost. In order to prevent the happening of such problems, one solution is to generate a data head from data flow involved by SET protocol through software.

Original port	Objective port	Sending serial number	Receiving serial number	ACK	RST	SYN	(data)

In such a information heading, original port and objective port are used to fix on both service ports, and find corresponding receiving place; sending serial number marks the sending order of data flow, and receiving serial number marks data's serial number of data which is expected to be received next time. Through verifying two serial numbers in each software, there can ensure whether there is error data flow; ACK is the affirming bit, when ACK=1, affirming serial fields are significant, when ACK=0, affirming serial number is insignificant. RST is reconstructing bit, when RST=1, it means that there is something wrong, for example, server might be broken, or there are other reasons, in these cases, there must release previous data, and reconnect. RST is also used to refuse an illegal message or refuse to open a link; SYN is a synchronize bit, which is used in linking, when SYN=1, and ACK=0, it means this is a linking request message fields, if the other one agrees to link, then should make SYN=1, ACK=1 in returned message, therefore, if SYN=1,

then it means this is a linking request or linking message, and ACK's value is used to distinguish messages.

Information heading is generated by software; it is given when software generating each data flows. Any data flow, no matter customer or merchant's server, or payment gateway, each of two build a link, they must use information heading, do three times handshaking with counterpart, to make sure the existence of the other, and only link is successful, SET protocol's corresponding steps can be proceeded, which is used to prevent network interrupting or danger brought by error. One error appears; SET protocol software will cancel this operation, and send new request link. When request mounts to certain times (the amount of times should be found suitable value in practice), then cancel the transaction, and send information of transaction fails.

3.4 Summary

This chapter introduces security SSL, describes the transaction process of SSL protocol, and compares it with the performance of SET protocol, and points out its advantages and disadvantages. Next will be introduced in details about the deficiencies of SET protocol, include:

- SET only supports credit card consumption.
- SET transaction process only guarantees the atomic nature of money. The atomic nature of sending and merchant are not guaranteed.
- SET's message is too complicated.

- SET protocol is too complicated. It requires too many installed software packages. And it is slow in processing and expensive.
- SET does not solve the problem of generating and maintaining data in transaction.

For each deficiency, this chapter offers corresponding improvement proposal. For example, offers a new data structure to solve the problem supporting debit card; raises SET security level processing to solve the problem of high cost of SET protocol, that is, when customer order goods, add security level option, and customer can choose corresponding level according to his own situation; consider to add a file center to keep various information related to goods and fund in payment bank server for various data generated in SET protocol transaction process.

CHAPTER 4

PAYMENT SYSTEM DESIGN BASED ON IMPROVED SET PROTOCOL

This chapter discusses the designing of a payment system based on improved SET protocol. From the perspective of working procedure, this system designing uses ASNA (ATM-based Signaling Network Architecture) data structure language to describe, and offers detailed design proposal.

4.1 Payment System Procedure of Improved SET Protocol

The payment system described by SET protocol is composed by customer, merchant (merchant payment server) and payment gateway. As an option, it is possible to has a business gateway between merchant and payment gateway. The main function of business gateway is to realize counting, and management of payment transaction in electronic commerce.

In this payment system, SET protocol only offers the message definition and description of payment model which is participated by customer, merchant, and payment gateway, that is, the message definition and description of payment type. This payment system protocol is a point-to-point protocol between merchant payment server and payment gateway. In the perspective

of business and security, business gateway and its related information are transparent to payment gateway. Therefore, the existence of business gateway does not influence the transaction dealing process ruled in this protocol and security authentication mode among request/reply grammar definition, grammar format of protocol message, merchant payment server, and payment gateway. The existence of business gateway will not reduce the security of payment system. All payment sensitive information in transaction process and information is hidden from business gateway. Protocol request information can include fields related to business gateway. However, payment gateway should not explain and process about this field. Merchant payment server can support customer's electronic commerce application. In payment system, merchant payment server is an independent authentication entity.

Realizing a complete SET transaction on internet mainly include cardholder registration for obtaining certificate, merchant registration for obtaining certificate, purchasing request, payment authorization, obtaining for detaining fund, etc, in which the obtaining of cardholder's certificate and merchant's certificate are finished at the beginning of purchasing. Here I would tell how to realize online purchasing payment processing (including purchasing request, payment authorization, and obtaining retaining fund).

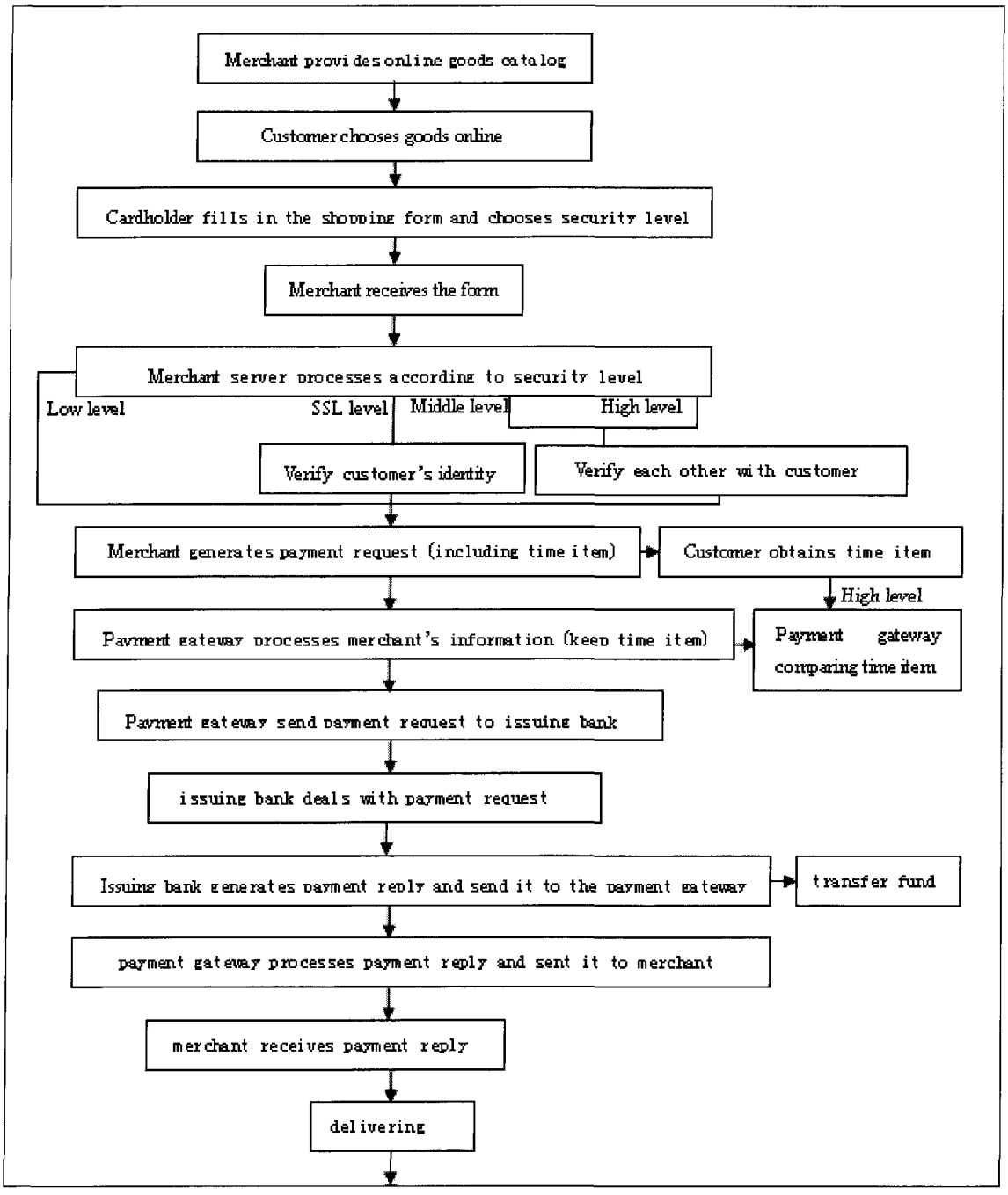
Payment procedure can be divided into payment procedure and reversal procedure. Payment procedure starts from customer sending payment initialization request to merchant, to merchant returning payment reply to customer. Messages involved in payment procedure include payment

initialization request, payment request, authorization request, cash request, authorization cash request, payment initialization reply, payment reply, authorization reply, cash request reply, and authorization cash reply. reversal procedure includes reversal procedure and refund request: after merchant notify business system the failure of transaction, he send reversal request to payment gateway, and receive payment gateway's reversal answer; refund is business system sending merchant refund notice, merchant send refund request to payment gateway, and receive payment gateway's refund answer.

Concrete payment procedure can be divided into three types according to differences of payment gateway payment messages sent by payment server: the first one is for customer with certificate, which can finish payment transaction with authorization cash request; the second one is for customer with certificate, which can finish payment transaction with two steps, authorization and cash request; the third one is for customer without certificate, which is finished with direct payment.

4.1.1 Payment Flow Chart

In chapter three, discuss the deficiencies of SET, and offer solutions to them. There can obtain the following payment system mode procedure according to improved SET protocol reference proposal.



(to be continued)

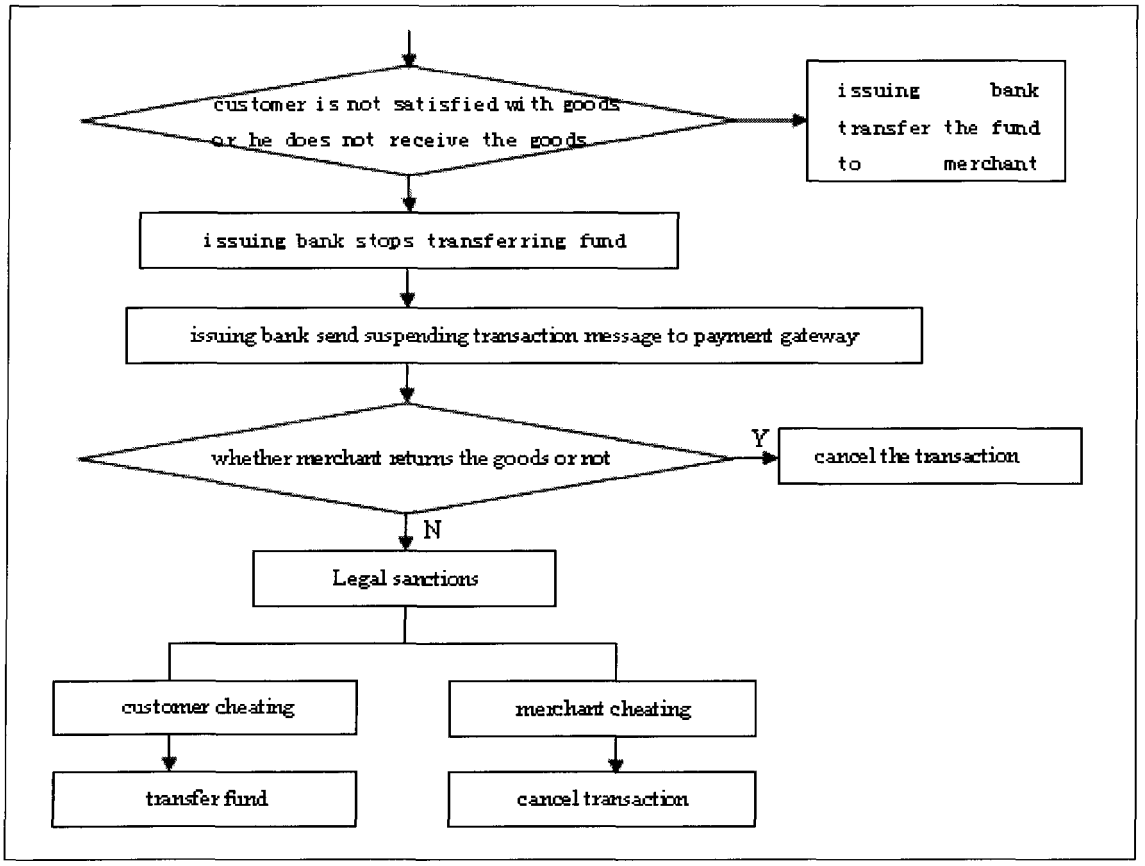


Figure 4-1 Improved SET payment flow chart

4.1.2 Step-by-step Description of Payment System Data Flow

The event tracking chart of data flow is as follows:

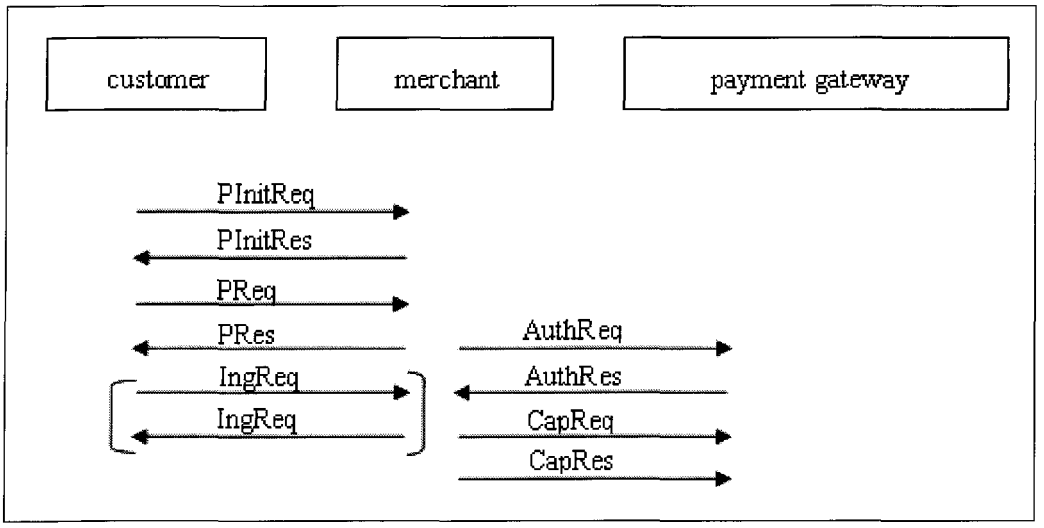


Figure 4-2 SET protocol data flow chart

From the perspective of SET protocol data flow, and combined previous SET improved proposal, its offer data flow's realization and processing in detail.

- **Transaction initialization data flow-- PInitReq/PInitRes**

PInitReq/PInitRes message is the original exchanged message flow when cardholder and merchant build transaction relationship, the purpose is for cardholder to obtain certificates of merchant and payment gateway, and ensure the feasibility of transaction.

(i) Customer checks the online catalog provided by merchant through browser and chooses merchant, fills in the shopping form, and at the same time chooses security level.

(ii) If security level is low, or SSL level, then browser will generate initialization request

PInitReq; if middle level or high level is chosen, then start SET customer software, and send PInitReq request.

(iii) Merchant receives initialization request, and judges through security level

If it is low-level security, then skip the authentication, and go to the payment request directly;

If it is SSL-level security, then send verifying request to customer.

If it is middle or high level security, then merchant software generates reply, encrypts merchant certificate, payment gateway certificate with merchant's private signature key, and generates replying message PInitRes, then send it to the cardholder.

- **Purchasing instruction data flow-- PReq/Pres**

PReq/Pres message provide the basic transaction processing between cardholder and merchant. Cardholder uses PReq (purchasing request) to transfer payment instruction and ordering information, and merchant replays customer's purchasing request with Pres, then gives the result of this transaction.

(i) Customer receives PInitRes. If security level is SSL, then sends certificate to merchant; if security level is middle or high, then tracks to root key to verify merchant's certificate and payment gateway's certificate according to trust chain.

(ii) Customer links ordering information and payment instruction with Hash, and encrypts it with his own private key, and forms double digital certificate.

(iii) Cardholder software encrypts with a symmetric key (#1) which is generated randomly,

and then encrypts #1 key and cardholder account information with payment network public key, generates PReq, and sends it to merchant.

(iv) Merchant tracks to root key to verify customer's certificate and payment gateway's certificate according to trust chain.

(v) Merchant decrypts double digital certificate, and compares and verify customer's signature, and at the same time obtains ordering information.

(vi) Merchant software calculates time item, encrypts it, and generates purchasing reply Pres, and sends it to customer.

(vii) Customer verifies merchant's signature and the validity of certificate, and at the same time keeps purchasing reply.

- **Authorize request data flow --AuthReq/AuthRes**

AuthReq/AuthRes is used to complete payment authorization between merchant and payment gateway. Merchant will verify cardholder's payment information to payment gateway, and payment gateway replies bank the verifying result. With the payment authorization of cardholder's issuing bank, merchant can do transaction with cardholder.

(i) Merchant does digital signature to customer's certificate, payment instruction, customer's account information, and time item with merchant's private key, merchant software generates stochastic code #2 and encrypts it, then encrypts code #2 with payment gateway public key, and generates authorization request Auth Req, and sends it to payment gateway. For high level security

mode, payment gateway will also receive the time item with signature sent by customer. Payment gateway compares two time items.

(ii) Payment gateway tracks root key to verify merchant's certificate and customer's certificate according to the trust chain.

(iii) Payment gateway decrypts payment instruction and authorization separately with private key, and verify customer's double signature.

(iv) Payment gateway creates authorization replying message, generates authorization reply's information digest and generates digital signature by encrypting with signature private key. Payment gateway encrypts authorization reply with a new stochastic symmetric key #3, and then encrypts this symmetric key by exchanging merchant key with public key.

(v) Payment gateway sends the encrypted authorization reply to merchant AuthRes.

(vi) Merchant verifies payment gateway certificate and keeps AuthReq.

- **Payment instruction data flow-- CapReq/CapRes**

CapReq/CapRes realizes the function of fund settlement. This step is done by payment gateway, cardholder then transfer the goods' fund from issuing bank to merchant's acceptance bank.

(i) After merchant finishing authorization verifying, he will send payment information CapReq to payment gateway. Then payment gateway will send payment instruction to issuing bank through financial security channel.

(ii) Issuing bank verify the validity of customer's account. If it is valid, payment gateway

will transfer the fund from customer's account, and keep it in temporary data base, and notify payment gateway that customer's account is verified to be valid.

(iii) Payment gateway uses merchant's public key to encrypt payment reply, and notify merchant to deliver the goods CapRes.

(iv) After waiting for delivering time, if there is nothing wrong, then transfer the fund into merchant's account.

(v) For high-level security mode, payment gateway keeps the purchasing information signed by merchant, and fund information is signed by payment gateway, and encrypts them with CA public key.

- **Transaction inquiring data flow --InqReq/InqRes**

InqRe, InqRes enable cardholder to inquire about transaction situation. After cardholder send purchasing request PReq, he can send inquiring information at any time.

(i) Customer send inquiring information InqReq which is signed by private key.

(ii) Merchant verify customer's identity, and signs customer's inquired information with merchant's private key, and sent it to customer InqRes.

For high level security mode:

(i) Customer sends inquiring request to merchant, and signs it with private key.

(ii) Merchant agrees about inquiring, and signs the inquiring request sent by customer with his own private key, and sends it to the payment gateway.

(iii) After verifying identities of customer and merchant, payment gateway sends inquiring request to CA, and CA decrypts file information.

(iv) Payment gateway sends inquiring result to merchant and merchant sends the inquiring result to customer.

- **Error message data flow --Error**

Error provides a processing method for situation with error in transaction process of in message transmitting process. Generally, error code and this error message will return to the sender of message. This message is unilateral.

4.2 The Data Structure Description of Payment System

The data structures involved in the whole payment system include:

(i) Security data structure: it mainly defines various security methods in transaction process, including encryption/decryption, signature/authentication, and code algorithm, etc.

(ii) Public data structure: it is mainly used to describe transaction steps in payment process, including the beginning of transaction (PInitReq/PInitRes), purchasing instruction (PReq/PRes), authorization request (AuthReq/AuthRes), payment instruction (CapReq/ CapRes), cardholder inquiring instruction (InqReq/ InqRes).

4.2.1 Abstract Syntax Notation (ASN.1) [5]

ASN.1 is used to describe the high-level format/structure of data to be transferred

between the Application Layer and the Presentation Layer of the Open Systems Interconnection (OSI). Thus, the sending computer would transform the data to be sent into ASN.1 syntax and send it to the destination computer. Upon receiving the data, the destination computer would transform the data from the ASN.1 syntax back to the native format, and make it available to the actual application.

ASN.1 is meant to provide a mechanism using which the Presentation Layer can use a single standard encoding mechanism to exchange any arbitrary data structure with other computer systems, while the Application Layer can map this standard encoding into any type of representation or language that is appropriate for the end user. ASN.1 does not describe the content, meaning, or structure of the data, but only the way in which it is specified and encoded.

ASN.1 is defined jointly by ISO/IEC along with ITU. ASN.1 defines two important aspects: type and value. The types can be primitive or constructed.

4.2.2 Security Data Structure

(i) AlgorithmIdentifier

```
AlgorithmIdentifier::=SEQUENCE{
    algorithm       OBJECT IDENTIFIER,
    parameters      ANY DEFINED BY algorithm OPTIONAL,
     }
```

(ii) DigestedData

```
DigestedData::=SEQUENCE{
   Version              INTEGER DEFAULT ver(0),
   digestAlgorithm      AlgorithmIdentifier,
   contentInfo          ContentInfo,
   digest               Digest,
}
Digest:: =OCTET STRING
```

In business data description, DigestedData is shown in the short form DD(t), which means digested data without rules.

(iii) Contenttnfo

```
ContentInfo::=SEQUENCE{
  contentType              ContentType,
```

```
    content                 [0] EXPLICIT ANY DEFINED BY contentType
                            OPTIONAL,
  )
ContentType::=OBJECT IDENTIFIER
```

(iv) Linkage

```
Linkage::=SEQUENCE f
        Ti              ANY,
        t2              DigestedData
  }
```

In business data description, Linkage is shown in the short form L (t1, t2)={ti, DD (t2)}, in which it is member one of the Linkage, and t2 is the digested rule of Linkage's member two.

(v) SignedData

```
SignedData::=SEQUENCE{
  Version                 INTEGER DEFAULT v1(1),
  digestAlgorithms        DigestAlgorithmIdentifiers,
  contentInfo             ContentInfo,
  certificates            [0] IMPLICIT Certificates OPTIONAL,
  signerInfos             SignerInfo
}
DigestAlgorithmIdentifiers::=SEQUENCE OF AlgorithmIdentifier

Certificates::=SEQUENCE OF Certificate

Certificate::=OCTET STRING

SignerInfos: : =SEQUENCE OF SignerInfo

SignerInfo::=SEQUENCE{
        Version                     INTEGER,
        issuerAndSerialNumber       IssuerAndSerialNumber,
        digestAlgorithm             AlgorithmIdentifier,
        digestEncryptionAlgorithm   AlgorithmIdentifier,
        encrptedDigest              EncryptedDigest/
}

EncryptedDigest::=OCTET STRING
```

```
        IssuerAndSerialNumber::=SEQUENCE{
        Issuer          Name,
        serialNumber    INTEGER
}
```

In business data structure description, SignedData is shown in the short form S(s, t) and SO (s, t), in which SO (s, t) is the digital signature with rule (uses t to do signature to t and then seals t in the signed data structure), SO (s, t) is the digital signature without rule (uses t to do signature to t but t is not sealed in signature data structure), content is the signature rule, and s is the signature certificate.

(vi) EnvelopedData

```
    EnvelopedData::=SEQUENCE{
        Version                 INTEGER,
        recipientInfo           RecipientInfo,
        encryptedContentInfo    EncryptedContentInfo
          }
    RecipientInfo::=SEQUENCE{
        version                 INTEGER,
        issuerAndSerialNumber   IssuerAndSerialNumber,
        keyEncryptionAlgorithm   AlgorithmIdentifier,
        encryptedKey            EncryptedKey
}

    EncryptedKey:=OCTET STRING (SIZE (1....128))

    EncryptedContentInfo::=SEQUENCE{
        contentType         ContentType,
        contentEncyption    Algorithm AlgorithmIdentifier,
        encryptedContent    [0] IMPLICIT EncryptedContent OPTIONAL
  }

    EncryptedContent::=OCTET STRING
```

In business data structure description, EnvelopedData is shown in the short form Enc(s, r, t)

and Env (r,t), in which Enc(s, r, t) is the digital envelop of rule signature, and Env(r,t) is the digital envelop of rule, s is the signature certificate, and r is the encrypted certificate. EnvelopedData is shown with function E(r,t), its meaning is to encrypt t with symmetric key k, and dissymmetric encrypt k with r's public key. Enc(s, r, t)=E (r, S (s,t)); Env (r, 0=E(r, t) .

(vii) EnCBData

```
EncBData::=SEQUENCE(
  enc EnvelopedData,
    baggage Baggage
  }
  Baggage::=OCTET STRING
```

In business data structure description, EncBData is shown in the short form for EncB(s, r, t, Baggage)=(Enc (s, r, L(t, p)), p), in which s is the signature certificate, and r is the encrypted certificate, t is the encrypted information, Baggage is the information which do Linkage with t.

(viii) EX

```
EX::=SEQUENCE{
  env       EnvelopedData,
  append    OCTET STRING
}
```

In business data structure description, EX is shown in the short form EX(s, r, t, p)={Env(r, L(t, P)), P cryption}, in which s is the signature certificate, r is the encrypted certificate, t is the encrypted information. P encryption is the information obtained from dissymmetric encrypting P with r's public key.

4.2.3 Public Data Structure

(i) TranslDs

```
TransIDs::=SEQUENCE{
```

```
        lid-C    LocalID,   // customer's local ID, in initialization request, customer
                                                    will generate local ID
        lid-M   LocalID,    // merchant's local ID, that is, business system ordering
                                                    number
        xid      XID,       //ID of the whole situation, it is the ID of merchant payment
                                                    server payment transaction.
        pReqDate    Date //transaction request time, generated by merchant payment
                                                    server in initialization reply
    }
      LocalID::=OCTET STRING size (1....20))
      XID::=OCTET STRING size (1....30)
      Date:: =GeneralizedTime   //time fuction
```

(ii) RRTags(request reply ID)

```
    RRTags::=SEQUENCE{
            rrpid RRPID,          //new request, reply, matching mark for each request and
                                                    reply
            currentDate Date      //generating time of request
  }
    RRPID:=OCTET STRING (size(20))
```

(iii) Bin(bank mark)

```
    Bin::=SEQUENCE{
            Bid        BID,   //bank mark
            region     REGION,   //region mark
            pgid       PGID OPTIONA L   //gateway mark, which is used only between
                                                    merchantserver and payment
                                                    gateway
  }
      BID::=NUMERIC STRING
      REGION::=NUMERIC STRING
      PGID::=NUMBERIC STRING
```

(iv) OIData (0I data)

```
  OIData::=SEQUENCE{
     transIDs      TransIDs,
            rrpid          RRPID,   //request, reply, customer payment request, reply's
                                                    matching mark
            chall-C        Challenge,     //marking message stochastic number, which
```

```
                                                    copy the chall-c in initialization
                                                    request
            hod         DD{HODInput},  // HODInput data's digest constructed by
                                                    customer
            odSalt      Nonce  //ordering adjustment value generated by customer,
                                                    merchant server is used to
                                                    reconstruct HODInput data
            chall-M     Challenge,     // mark message stochastic number
            bin         Bin,
            odExtOIDs   [0] EXPLICIT OIDlist OPTIONAL,// OID chain from in
                                                    extension item, which is in the
                                                    same order with the extension item
                                                    in HODInput
            oiExtensions  [1] EXPLICIT Extensions OPTIONAL//extension item
}
OIDList::=SEQUENCE OF OBJECT INDETIFIER
Challenge::=OCTET STRING (size(20))
```

(v) HODInput(merchant's ordering information)

```
HODInput::=SEQUENCE(
            Od              OD,    //ordering description
            purchAmt        CurrencyAmount,       //ordering fund
            odSalt          Nonce,          // stochastic number which is used to
                                                    prevent guessing
            extensions      [0] EXPLICIT Extensions OPTIONAL    //extensions
}
OD::=SEQUENCE{
        id          OBJECT IDENTIFIER,//
        value       OCTET STRING//
}
CurrencyAmount:=SEQUENCE
            currency    Currenc.
            amount      Amount
}
Currency:;=INTEGER (1...999)
Nonce::=OCTET STRING(SIZE(20))
Amount::=INTEGER
```

(vi) PANData(account information)

```
PANData::=SEQUENCE{
        cardType        CardType,       //card type
        pan             PAN,            //account number and credit card number
        password        [0] EXPLICIT Password OPTIONAL,         //password
        idNumber        IDNumber, //ID number
        expiry          [1] EXPLICIT CardExpiry OPTIONAL, // expiry
        panSecret       [2] EXPLICIT Nonce OPTIONAL,    // stochastic number
                                                        shared by customer, payment
                                                        gateway, and CA.exNonce
        Nonce           //new nonce which is used to prevent guessing on pin
}
CardType:=INTEGER (0..MAX)
PAN::=NUMERIC STRING (size (1..10))
Password::=OCTET STRING (size (1..12))
IDNumber::=NUMERIC STRING (size (1..20)
CardExpiry::=NUMERIC STRING (size (6))
```

(vii) PIHead(PI head information)

```
PIHead::=SEQUENCE{
        transIDs        TranslDs,       //transaction ID
        inputs          Inputs,         //structure composed by HODInput's digest
                                        message and ordering information
        merchantID      MerchantID,     //merchant ID
        extensions      [0] EXPLICIT Extensions OPTIONAL     // extensions
}
MerchantID:=VisibleString (size (1..19))
Inputs::=SEQUENCE{
        hod             HOD,    // HODInput data's digest constructed by customer
        purchAmt        CurrencyAmount      //ordering fund
}
HOD::=DD { HODInput}
```

4.2.4 Flow data structure

(i) Payment initialization request PInitReq

```
PInitReq::=SEQUENCE{
        rrpid       RRPID,      //it is used to mark request/reply flow
        lid –C      LocalID,    // it is generated by customer and is used to mark this
```

```
                                        transaction
        lid –M      LocalID,        //it is generated by merchant and is used to mark
                                        purchasing order
        chall- C    Challenge,      //it is generated by customer and is used to defend attack
        brandID     BrandID,        //payment card selected by cardholder
        bin         BIN,            //the first 6 number of the card
        security    Security        //security level controlling option
}
RRPID:=OCTET STRING (SIZE (20))         //20 bit character type
LocalID:=OCTET STRING (SIZE (20))       //20 bit character type
Challenge::=OCTET STRING (SIZE (20))    //20 bit character type
BIN::=NUMERIC STRING (SIZE (6))         //6 bit integer
BrandID::=SETString         //set
Security::=Char
```

(ii) Payment initialization reponse PInitRes

```
PInitRes: : =S(M, PInitResData)     //S(m, t) is signing operation, which means sign unit
                                        t with entity m's private key, here
                                        M is merchant certificate, which is
                                        issued by bank.
PInitResData::=SEQUENCE{
        transIDs        TransIDs,       //transaction ID
        rrpid           RRPID,          //mark request and reply
        chall_ C        Challenge,      //mark generated by cardholder which can
                                            prevent attack
        chall- M        Challenge,      // mark generated by merchant which can
                                            prevent attack
        tim             Tim             //time item generated by merchant
}
TransIDs::=SEQUENCE {
        lid –C          LocalID,        //it is generated by cardholder to mark this
                                            transaction
        lid -M          LocalID,        //it is generated by merchant to mark
                                            purchasing order
        xid             XID,            // it is generated by merchant to mark this
                                            transaction
        pReqDate        Date            //time in which merchant generating
                                            message
}
```

```
LocalID:=OCTET STRING (SIZE (20))        //20 bit character type
XID::=OCTET STRING (SIZE (20))           //20 bit character type
Tim::=SEQUENCE{
        dateA       Date        //delivering time
        dataB       Date        //arriving time
}
```

(iii) Payment request PReq

```
PReq::=SEQUENCE{
        E(M, OIDualSigned)      //encryption and digital envelop sent to merchant
        E(G , PIDualSigned)     //encryption and digital envelop sent to bank's gateway
}
```

E (c, t) is digital envelop operation, which is divided into two steps:

a) Generates stochastically a symmetric key k, and encrypts unit t with this key;

b) Encrypt key k with public key provided by receiver, and to form a digital envelop.

Here M is merchant's certificate, and G is payment gateway's certificate,

```
PIDualSigned:: -SEQUENCE{           //double digital signature of payment
                                                instruction
        PiHead      PIHEAD      //head information of payment instruction
        panData     PANData,    //account information of customer's credit card
        hOIData     HOIData,    //Hash digest data of ordering instruction
                                                information
        dualSign    DualSign    //double digital signature of PI and OI
      }
HOIData::= DD( OIData)      // Hash digest data of ordering instruction
DualSign::=SO( HOIData, HPIHead)        // double digital signature of PI and OI
OIDualSigned::=SEQUENCE {               //double digital signature of ordering
                                                instruction
        oiData      OIData,             //ordering instruction information
        hPIHead     HPIHead,    //Hash digest information of payment instruction head
                                        information
        dualSign    DualSign    // double digital signature of PI and OI
}
HPIData::=DD (PIData)           //Hash digest information of payment instruction
```

```
                                                    information
    DualSign: : =SO (HOIData, HPIHead)   // double digital signature of PI and OI
    OIData::=SEQUENCE{                   // ordering instruction information
            TransIDs      TransIDs,      //transaction ID
            rrpid         RRPID,         //it is used to mark request and reply
            chall_ C      Challenge,     //mark generated by customer which is used
                                                to prevent attack
            chall_ M      Challenge,     // mark generated by merchant which is
                                                used to prevent attack
            bin           BIN,           //the first 6 number of the card
            merInfo       OrderInf       //merchant 0pp's information
}
    PIHead:: -SEQUENCE{                  //head information of payment
                                                instruction
            transIDs      TransIDs,      //transaction ID
            hOD           HOD,           //Hash digest data of ordering
                                                information
            money         OrderInfo,     //total amount of purchasing goods
            merchantID    MerchantID     //merchant's mark
)
```

(iv) Payment reponse PRes

```
    PRes::=S (M, PResData)
    PResData::=SEQUENCE{
            T    ransIDs      TransIDs,        // transaction ID
            rpid              RRPID ,          //mark request and reply
            chall             C Challenge,     // mark generated by customer which is
            used to prevent attack
          completionCode      CompletionCode,  //completion code mark
          errorCode           ErrorCode        //error code mark
}
```

(v) AuthReq

```
    AuthReq: : =EncB (M, P, AuthReqData, PI)    //EncB is the extended envelop
                                                encryption
    PI::=E (G, PIDualSigned                     //payment information generated by
                                                cardholder
    AuthReqData::=SEQUENCE {
```

```
        authTags        AuthTags,          //authorization request mark
        checkDigests    CheckDigests,      //verifying digital signature
        captureNow      BOOLEAN,           //whether pay immediately or not
        authReqPayload  AuthReqPayload,    //including payment amount, etc.
        security        Security           //security level controlling option
        tim             Tim                //time item generated by merchant
}
AuthTags::=SEQUENCE {                      //authorization request mark
        transIDs        TransID,           //transaction mark
        rrpid           RRPID              //mark request and reply
}
CheckDigests::=EQUENCE {                   //verifying digital signature
        hOIData HOIData,                   //Hash digest data of ordering instruction
                                           information
        hod2 HOD                           // Hash digest data of ordering
                                           information
}
HOIData::=DD(OIData)                       // Hash digest data of ordering instruction
                                           information
HOD:=DD(OD)                                // Hash digest data of ordering
                                           information
Tim:=SEQUENCE{
        dateA           Date               //delivering time
        dataB           Date               //arriving time
}
```

(vi) Authorization reponse AuthRes

```
AuthRea: : =Enc (P, M, AuthResData)        //signature and digital envelop
AuthResData::=SEQUENCE{
        authTags        AuthTags,          //authorization request mark
        capResPayload   CapResPayload,     //pay
                                           immediately information
        authAmt         AuthAmt,           //authorized fund
        authCod         AuthCode,          //authorization code mark
        errorCode       ErrorCode          //error code mark
}
```

4.3 Summary

This chapter puts emphasis on the detailed design of payment system based on improved SET protocol. First it introduces improved SET payment processing procedure, including: transaction initialization data flow, purchasing SET does not solve the problem of generating and maintaining data in transaction. Data flow, authorization request data flow, payment instruction data flow, transaction inquiring data flow and error message data flow. Then introduce in details about various data structure in new payment system:

- Security data structure
- Public data structure
- Procedure data structure

CHAPTER 5

RESEARCH AND DESIGN OF PAYMENT SYSTEM SOFTWARE MODULE

This chapter mainly analyzes SET's modules, and offers realization methods.

5.1Payment System Module of SET Protocol

5.1.1 Module Chart of SET Payment System

SET protocol is defined on network, and serves for security data flow, it involves fund flow and logistics relationship among customer, merchant and payment gateway. Based on such consideration, the designing chart of SET system module is shown in the following Figure 5-1:

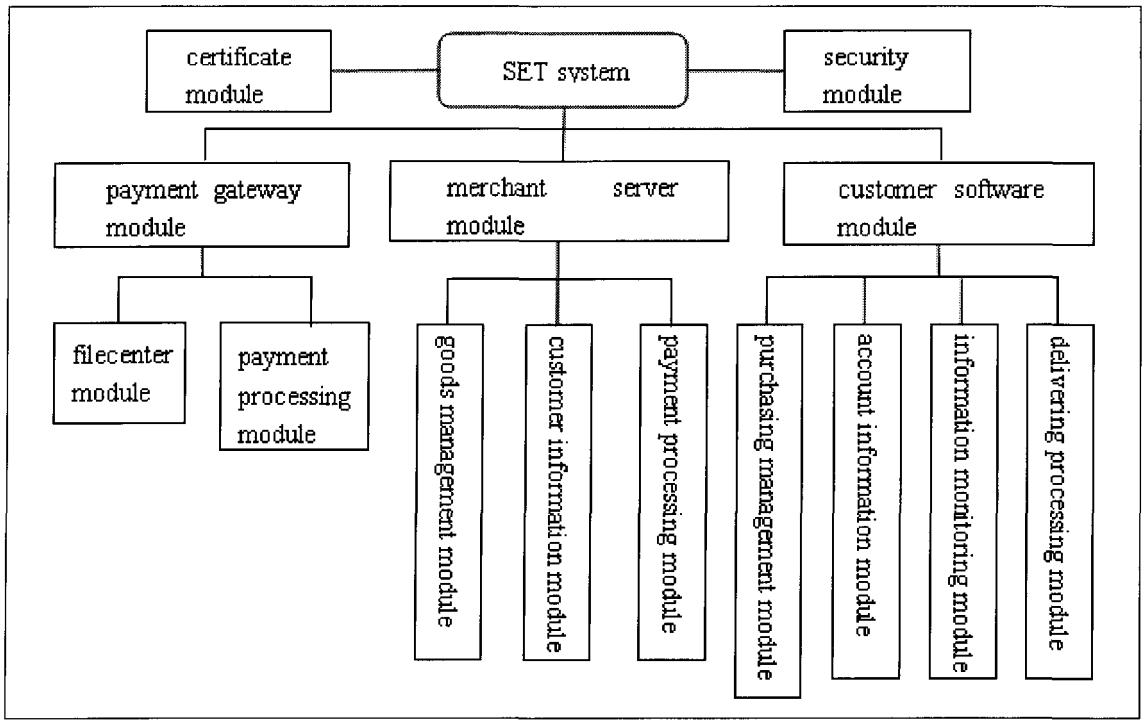


Figure 5-1 System module chart

5.1.2 Introduction of Each Module in Payment System

From the module chart of SET payment system, there can see that the whole SET protocol is an organic system, which is composed by five parts:

(i) Certificate module: certificate module is a public module. It defines functions such as supplication, approval, renewal, drawback, abolishing, and resuming of certificate. This module serves customer module, merchant server module and payment gateway module, like a public interface. What should point be out is that the operation of this module should has the support of matched PKI/CA system. The concrete regulation and interface definition designed by it should conform to CA's related rules.

(ii) Security module: security module is the same with certificate module, they are both public modules. Security module is used to define various encryption algorithms in SET system, such as RSA, DES, IDEA, and message digest Hash function, such as MD-5, SHA-1, etc. security module also provides services in interfacing way. With the coming of developed encryption method, there need only renew the related contents in this mode to provide more secure service for SET protocol. As long as they have the same interface, security module is independent and offer SET better extension.

(iii) Customer software module: customer software is mainly used in the computer terminal which is connected with internet, connects server through it with SET. It has the controlling power of security level. There are four modules in customer module:

Information monitoring module: consistently monitor messages sent by merchant server. Determine whether activate SET protocol or not according to security level.

Account information module: considering customer may used different kinds of cards, including credit card, saving card, debit card. This module is used to identify and manage different cards, and offer corresponding output according to different card with SET's processing mode. Each is processing is one-off, no information related to card is maintained.

Purchasing management module: this module is used to manage customers' information, which enables customer to inquire local record to know about purchased goods' information.

Payment processing module: transaction processing module is directly used to generate

various data flow related to SET protocol, including generating PInit Req, PReq, Ing Req and receive and process PInit Res, PRes,Ing Res. In the working process, it will transfer code algorithm and digest generating algorithm in security module.

(iv) Merchant server module: Merchant server is like a online shopping center, which provides services to customers who is connect to it. it includes three sub-modules:

Customer information module: this module is used to manage information of each different customer, and record this customer's purchasing situation.

Goods' catalog module: this module is used to manage the goods' situation of this merchant, including goods' information such as saving, sailing, and prices, that is, the shopping list of merchant.

Payment processing module: this module processes data flow related to SET protocol directly, which is used to generates PInitRes, PRes, IngRes, Auth Req, CapReq and receive PInitReq, PReq, IngReq, AuthRes, CapRes, to finish various encryption, decryption, signature, and authentication. (theses are all data structure .mentioned in 4.2)

(v) Payment gateway module: payment gateway module's function is to provide security electronic method which is used to exchange goods or services to customer, merchant and financial organization, transfer payment information to bank securely through network, complete payment function such as ordering processing, transferring application, transaction confirmation with customer software through merchant virtual cash register and bank's payment gateway software, etc.

Files center module: this module is used to keep high level security transaction module's purchasing file, which provides evidence for inquiries afterwards.

Payment processing module: this module is used to process data flow related to SET protocol, including generating Auth Res ,CapRes and receiving Auth Req, CapReqo.

5.2 The Working Theory of SET Protocol's Payment Processing Module

5.2.1 Customer Software Module

When customer browses goods on website provided by merchant, through consistently monitoring messages, customer software receives browsing order sent by browser, transmits website needs to be browsed by browser, and receives information sent back by website, and at the same time monitors contents on the website, to activate SET transaction. On the other hand, except for choosing whether needs to link SET and merchant from website provided by merchant, SET customer software can choose security level. If choosing low level or SSL level security, then SET is not activated, if not, SET is activated.

The working theory of customer message monitoring sub-module is as follows:

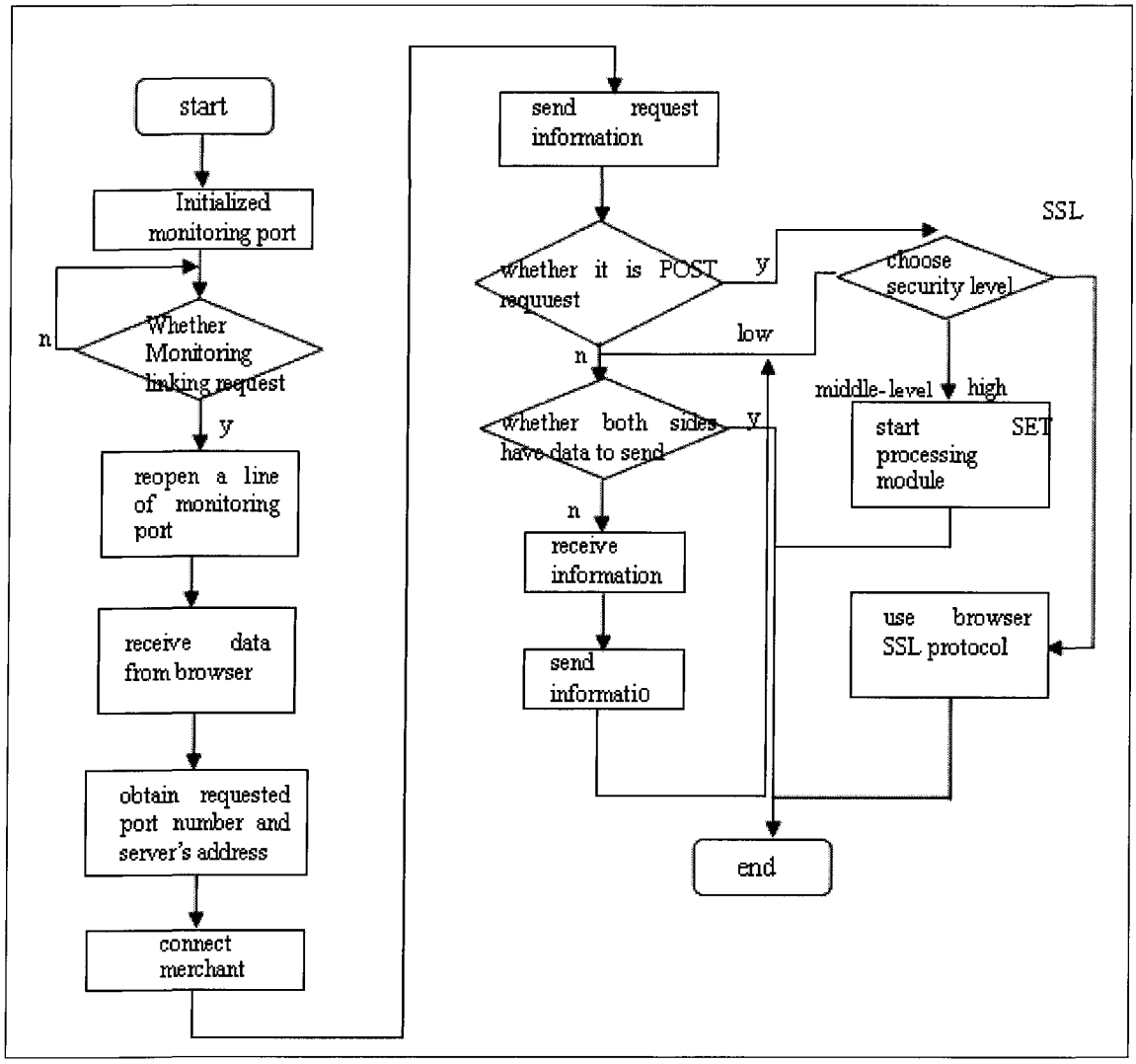


Figure 5-2 Description of customer monitoring module

When customer chooses middle or high level security module, SET payment processing module is started. This module is used to have SET dialog with merchant server. SET transaction module uses various encryption methods provided by encryption function to realize cardholder's function in SET transaction process. It is responsible for sending data flow such as Auth Req, Cap Req, receiving and processing answering data flow such as PInitRes, PRes. Its working theory is shown in the following Figure 5-3:

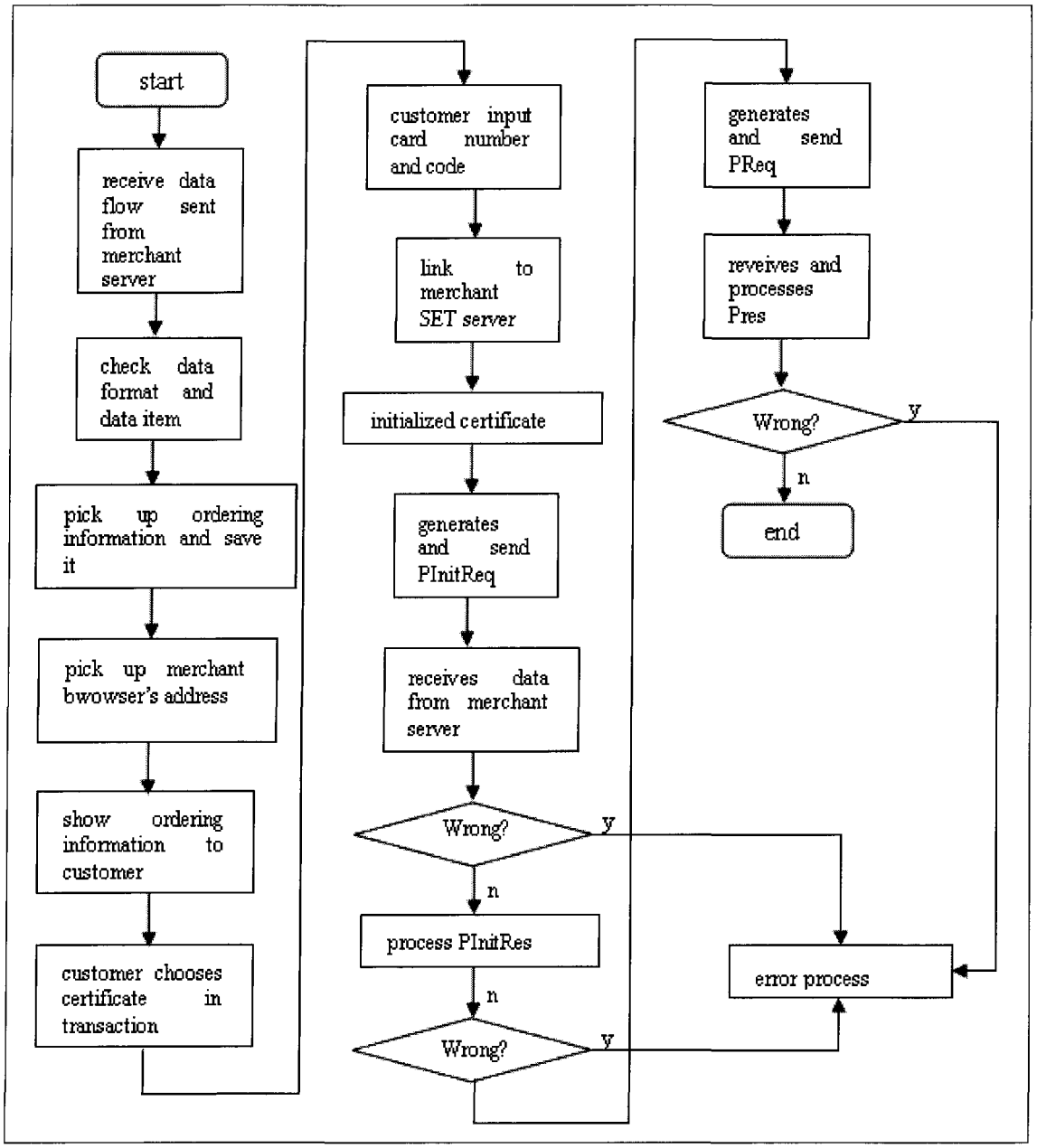


Figure 5-3 Description of customer payment processing module

It must be pointed that customers without SET customer software choose low level or links with merchant directly through SSL do not need customer module.

5.2.2 Merchant Software Module

Merchant SET server is a conjunction between cardholder and payment gateway. It is also an important part of SET transaction process. It is responsible for receiving data flows such as PInitReq, PReq, AuthRes, CapRes, and generating data flows such as PInitRes, PRes, AuthReq, CapReq. Merchant server first consistently monitoring customer's message, and answer correspondingly according to security level setting. Its working theory is shown in the following Figure 5-4:

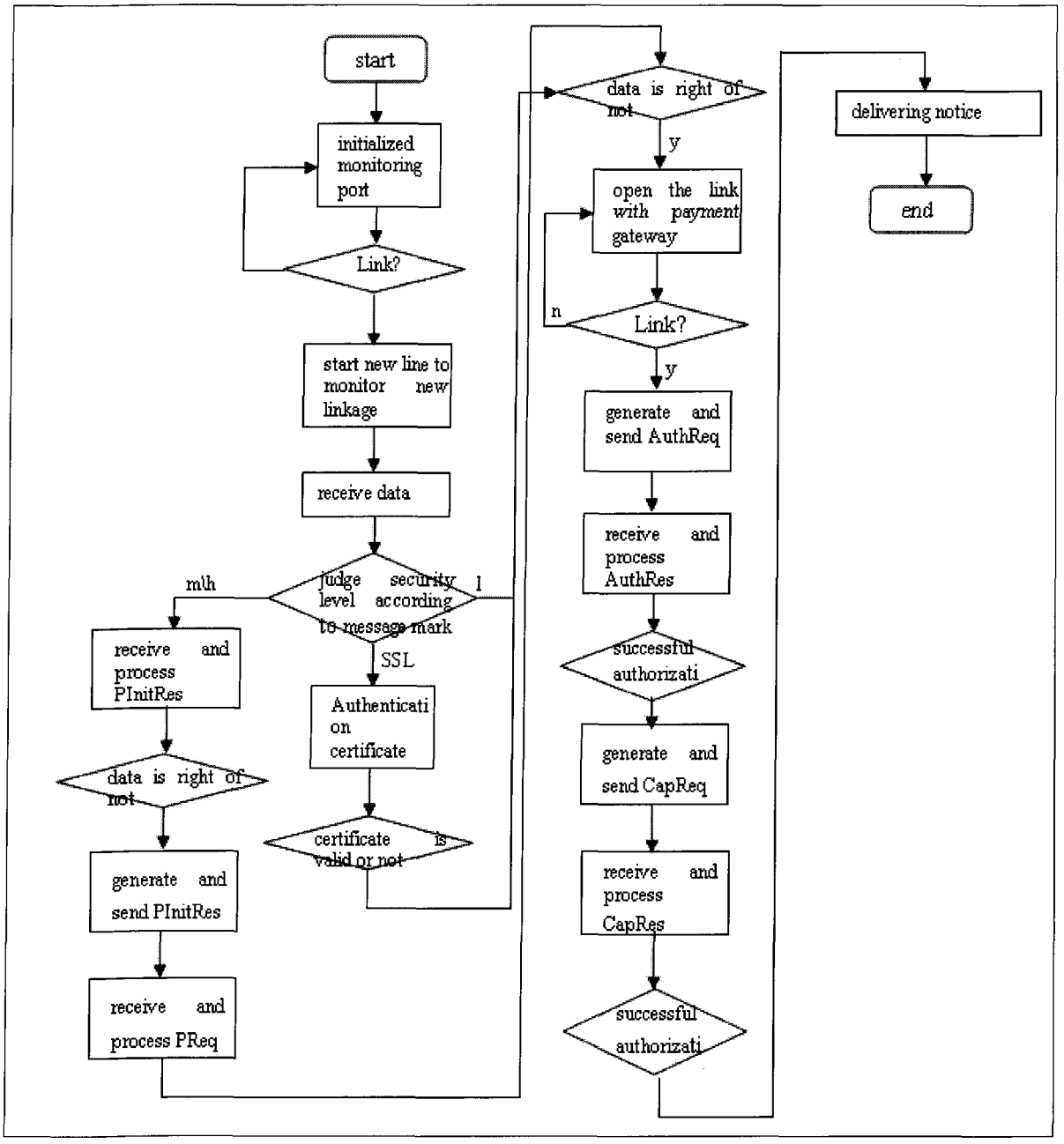


Figure 5-4 Description of merchant server payment processing module

In Figure 5-4 if each data check fails, it should do error processing.

5.2.3 Payment Gateway Module

Payment gateway is between merchant and acceptance bank. Merchant and payment gateway is linked through internet or special net, and payment gateway and acceptance are linked through financial special network. Payment gateway should process SET transaction's data flow such as AuthReq, AuthRes, CapReq, CapRes, authentificate card number for customer, and transfer fund. At the same time, it also involves repack the data package sent by internet according to banking system's inner communication protocol; receives replying message's work which is feed backed by banking system. Its working principle is shown in the following Figure 5-5:

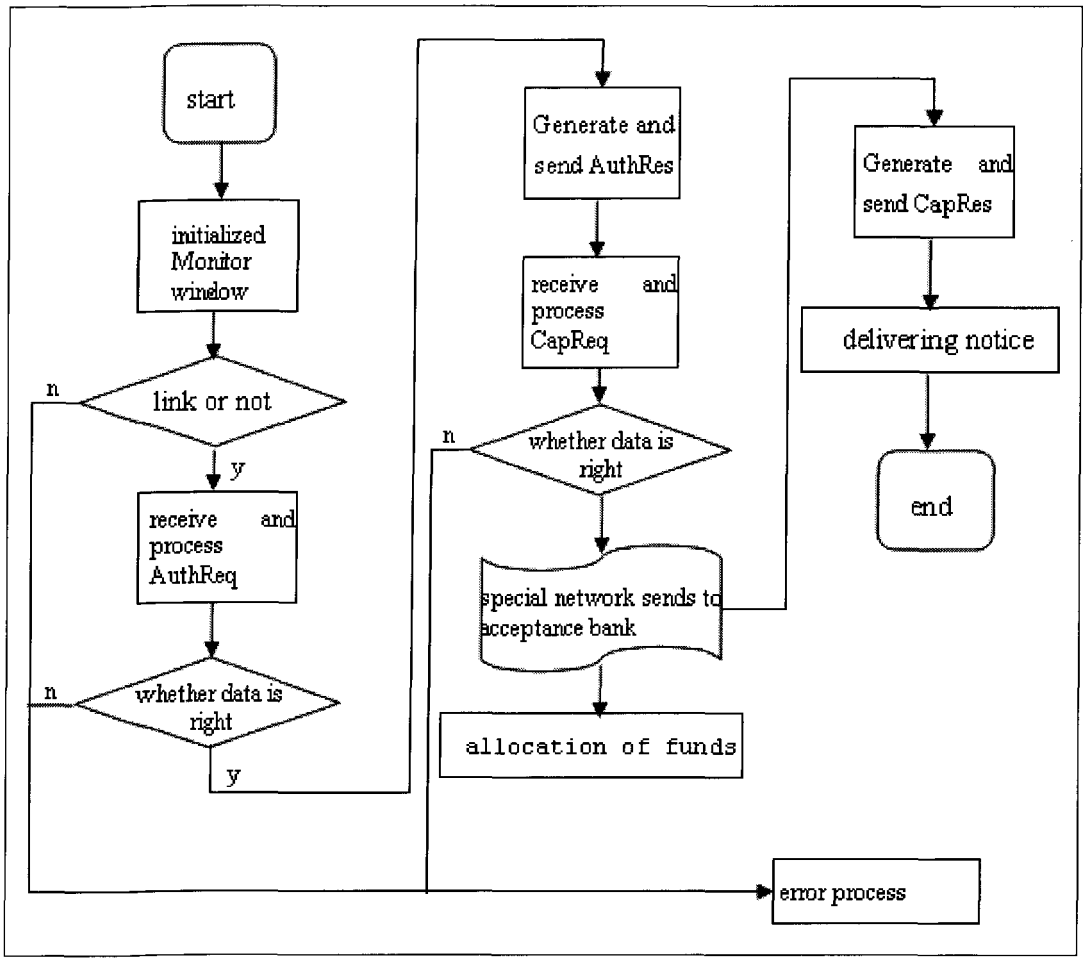


Figure 5-5 Description of payment gateway processing module

5.2.4 Security Module

Security module is a module provides public service. It's designing idea is to seal various encryption, decryption, signature, authentication, and hash function, etc, which is involved in SET protocol, provides public interface for merchant, customer, and payment gateway. Because security is independent of SET's other design, then just need to renew this module if there is securer algorithm to replace the current one in the future. This is kind of design accords with the idea of

current software development which is based on module and group ware. Its basic structure is shown in the following figure 5-6:

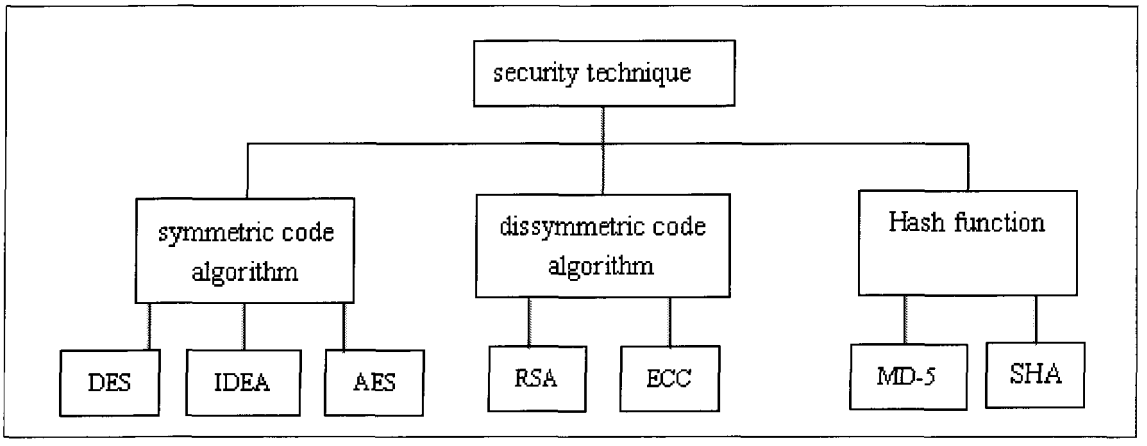


Figure 5-6 Security module

5.3 Analyses on Security of Payment System

5.3.1 Security of Core Algorithm

In SET protocol, currently there are DES, RSA, and SHA-1. These algorithms are key to the secure operation of SET. Their security is important in designing and using of SET.

(i) Security analysis of DES

DES is an algorithm which is used to encrypt the binary data. Data group length is 64 bit (8 byte), encryption group length is 64bit, no data extension, and key length is 64bit, in which there are 8 bit verifying of odd and even number. The whole mechanism with effective key length 56 bit DES is open, and system's security is kept by key. DES adopts traditional exchanging and replacing way to encrypt, its algorithms include: original replacing, product changing of 16 round iteration

and generator of 16 sub-keys.

DES algorithm has relatively high security. Till now, except for enumerating searching method's attack to DES algorithm, there is no other more effective method. However, with the growth of computer's operating speed, the ability to decrypt is improving a lot. In SET, DES algorithm adopts 56 bit key, the encryption intensity of this method is not very strong. According to data in the year 1997, it can be broken through in 58 days. In SET protocol, when bank and cardholder's information exchanging need to through merchant, and also need CDMF method to encrypt the information. This method's encryption intensity is correspondent to a 40 bit's DES algorithm. Such encryption intensity can be broken through in 78 seconds with strong attack.

Therefore, longer key is necessary. The other way is to change code algorithm, and use three times DES to replace DES, or uses AES algorithm.

Micheal Wiener found that it is proportional between machine's cost and breakthrough time for DES.

Table 5-1 Key length and breakthrough time statistics

Cost (million dollars)	Key length					
	40	56	64	80	112	128
0.1	2 sec.	35 hr.	1 year	70000 years	10^{14} years	10^{19} years
1	0.2 sec.	3.5 hr.	37 days	7000 year	10^{13} years	10^{18} years
10	0.02 sec.	21 min.	4 days	700 year	10^{12} years	10^{17} years
10^2	2 ms	2 min.	9 hr.	70 year	10^{11} years	10^{16} years
10^3	0.2 ms	13 sec.	1 hr.	7 year	10^{10} years	10^{15} years
10^4	0.02 ms	1 sec.	5.4 min.	245 days	10^9 years	10^{14} years
10^5	2 us	0.1 sec.	32 sec.	24 days	10^8 years	10^{13} years
10^6	0.2 us	0.01 sec.	3 sec.	2.4 days	10^7 years	10^{12} years
10^7	0.02 us	1 ms	0.3 sec.	6 hr.	10^6 years	10^{11} years

(ii) RSA's security analysis[30]

RSA algorithm is named after his initiator's name: Rivest, Shamir, Adelman. This algorithm was raised first in the year 1978, and until now it has not serious security leak. RSA algorithm is based on mathematics problem: decompounds big number and examine the prime number's theoretical foundation.

RSA uses two keys: public key and private key. When encrypting, it will divide rules into blocks, and the size of blocks can change, but it cannot surpass the length of key. RSA translate rule blocks into encryptions which length is the same.

The security of RSA algorithm depends on decompounds of big numbers. But whether it is equal to big numbers decompounding has not proved in theory yet. It is not proved that breaking through RSA must need compound big number. If the third-party is listening-in, he will get several numbers e, n(=pq), m 1, m2 ....., if he wants to decode, then he must get d, so, he must do

factorization to n. to prevent factorization, the most effective way is to find two very big prime numbers p and q, which will make third party's factorization be difficult, to guarantee the security of data.

In SET, information sent from root CA is encrypted by 2048 bit's RSA algorithm, and other information exchanging is encrypted by 1024 bit's RSA algorithm. With the improvement of decompounding technique and computer ability, and of computer's cost, RSA's security is threatened. At present, most decompounding is difficult. However, with the development of number theory and calculating ability, it will become easier. In the development of SET from now on, algorithm with higher reliability might appear to replace RSA.

In addition, because RSA is used in big number's calculation, which make fastest RSA is ten times lower than SEA, no matter it is realized by software or hardware. Speed is always the deficiency of RSA, therefore generally it is used in encryption of small amount of data. It is troublesome for RSA to generate key, because it is restricted by the generating technique of prime number, then it is hard to achieve one time an encryption. The group is too long. In order to ensure the security, n is at least 600 bit, which increases the cost of operation, especially the slowing down of speed, which slower a lot than symmetric code algorithm; and with the development of bug number's decompounding technique, this length is increasing, which is not good for the standardization of data format.

(iii) SHA's security analysis

In SET protocol, all Hash calculation adopts SHA-1 algorithm, the typical application of SHA-1 is on digital signature, generates message digest of a field of information to avoids being changed.

For any length's message, SHA-1 will generate a 160 bits' message digest. If there is one bit changing in the message, then about half data in message digest may change. The chance of two messages' digests is the same is 10-as (nearly 0). Therefore, it is impossible to do direct attack to SHA-1.

However, in August 2004, an international cryptogram conference in California America, Professor Wang Xiao-yun, from Shandong university, has proclaimed that she has already deciphered MD5, HAVAL-128, MD4, and RIPEMD, provoking a great disturbance in cryptogram field. MD5 and SHA1 were once considered as the most secure algorithms, but through using "Mod Difference" produced by Prof. Wang, there can find "Collision" result of MD5 on common computers only in two hours. And the kernel principle of that method is how to choose an advanced cryptogram algorithm to keep the key secretly.

5.3.2 Security Analysis of Transaction Protocol

The purchasing request data flow sent by customer to merchant using double digital signature ensures merchant won't obtain credit card information and payment gateway won't get goods' information. It is pointed out in Chapter Four that TransID is used in the transaction process to

mark only the whole transaction process, TransID includes a stochastic number, which can ensure the uniqueness of each transaction. The use of stochastic numbers Chal-C and Chall-M can avoid attack.

Suppose, if customer is a cardholder who owns an acceptance bank, the inter-verifying of he and merchant and payment gateway has no problem. When this customer sends purchasing request to merchant, merchant can not read payment information, at this time, if customer wants to changing payment money and wants to pay less, merchant can not find out. However, when payment gateway verifying the payment request sent by merchant, it can verify and compare account payable sent by merchant and payment money generated by customer, cheating can be found out. The same, if merchant wants to revise account payable to obtain more money, he can also be found out by payment gateway's verifying. Payment gateway can also avoid merchant or customer revising goods' information through verifying messages sent by customer and merchant, for example, customer wants to change purchased goods or amount, these are not valid.

In the improved proposal of SET protocol, each transaction has files in the situation of high level security, and for each member in transaction, because authentication center signs time stamp, he can not revise its contents, which avoids dissension after transaction.

In improved SET protocol, after receiving payment order and verifying it, issuing bank will not transfer the money to merchant's account, but waiting for customer to get the goods, if there is nothing wrong, the money is transferred. Suppose customer gets his goods, but lies by saying that

he does not get them, merchant can verify his action through inquiring post or delivering channel. The difficult situation is that customer receives goods but lies that what he gets are not what he orders. At this time, the third party is needed to research and check each one's responsibilities.

5.4 Summary

This chapter offers the system realization which is based on improved SET protocol. The system is divided into five parts, this chapter introduces their working theories in details, the five modules are:

- Certificate module: certificate module is a public module. It defines functions such as application, approval, renewal, drawback, abolishing, and resuming of certificate. his module serves customer module, merchant server module and payment gateway module .
- Security module: security module is the same with certificate module, they are both public module s. Security module is used to define various encryption algorithm in SET system, such as RSA, DES, IDEA, and message digest Hash function, such as MD-5, SHA-1, etc.
- Customer software module: customer software is mainly used in the computer terminal It has the controlling power of security level. There are four modules in customer module: Information monitoring module, Account information module, purchasing management module, and Payment processing module.
- Merchant server module: Merchant server is like an online shopping center, which can be

divided into three sub modules: Customer information module, Goods' catalog module, and Payment processing module.

- Payment gateway module: payment gateway module's function is to provide security electronic method which is used to exchange goods or services to customer, merchant and financial organization, transfer payment information to bank securely through network, complete payment function such as ordering processing, transferring application, transaction confirmation with customer software through merchant virtual cash register and bank's payment gateway software, etc., it has two sub-modules: Files center module and Payment processing module.

At last, this chapter analyzes and concludes on the core algorithm involved in SET protocol, such as DES, RSA, SHA's security and transaction protocol's security.

CHAPTER 6

CONCLUSION

At present, internet is applied commonly and developing fast. It has reached to various aspects of people's life because of its low cost, popularity, complete function, and agile application. Electronic commerce as a new business activity mode has become a hot internet application. However, openness of internet brings great security problem to the wide development of electronic commerce. And developing efficient and secure electronic commerce protocol becomes the researching direction, and SET protocol appears in such a background, and it is now in fact the standard.

SET protocol is a security electronic transaction protocol based on card payment. SET protocol adopts encryption system which combines symmetric key algorithm and dissymmetric key algorithm. It uses fully the speed of symmetric algorithm and the convenience of dissymmetric key algorithm in key exchanging, and better guarantees the confidentiality of network information sending.

SET adopts techniques such as X.509 digital certificate, digital signature, message digest, digital envelop and double signature to make sure the validity of merchant and customer's identity, and authentication and undeniable of business action. SET solves security problem which holds the

development of electronic commerce through making standards and adopting various technique methods, and provides more trust, and more complete transaction information, higher security, and less possibility of cheating in electronic transaction chain.

This thesis analyzes SET protocol's security technique, authentication system, and transaction procedure, and points its existing deficiency. SET protocol is complicated, costly, unsatisfying protocol, not strict regulation to data's processing, etc... All these bring difficulty in the popularity of it. To these deficiencies, this thesis offers corresponding solutions. In customer's part, set security level according to fact, and reduce cost; add file center in payment gateway, and provide copy service for high level security, at the same time uses signature of authentication center and provides time stamp service, avoids revising and cheating; in order to avoid merchant cheating, add time item in requesting payment data flow; after receiving payment message, acceptance bank adopts the method of temporarily transferring fund by controlling this time item, to avoid merchant getting money and not delivering goods. In addition, SET is originally designed for the use of credit card, and it can be extended to be suitable for the debit card.

These proposals have been practiced on our prototype system. The result shows that our improved solutions almost work well and follow the expectation, which proves suitable for situations of China. Next, the author plan to cooperate with government and e-commerce authority to extend experiment extent to gain more experience.

In the prototype experiments, there can also found that some data structures and relevant

processing are a bit unnecessary complex, such as digital timestamp processing. It will be revised in the future.

After discussing the improved proposal, this thesis describes the working procedure of improved SET protocol, and offers each message's data structure, and public data structure and security data structure that might be involved. At last, the thesis offers the payment module of the whole SET protocol system, which describes the whole module's working principle and its security from realistic perspective.

However, SET protocol is a complicated protocol, which involves complicated things. With the improvement of computer's calculation ability, it is necessary to have more convenient and securer protocol proposal, therefore, make SET protocol easier and securer is the researching direction of future. Here are some ideas:

From the current research on software area, software system is developing toward reusing, and concepts of module and groupware are more and more realized in the software system. Through consistently reusing, reconstructing, and upgrading of original system, making use of other software's code and module to construct new software product. The future software will not be wise result of several programmers; they are also the union of millions of sub-software. With the idea of software development, there can also apply the concepts of groupware and module to code area. Suppose it can be divided into different parts of the secure system, and make them to be independent "black box", which only provides certain services, data interface, and become a kind a

infrastructure like power source. The original design of PKI is like this. When it is needed to change a security algorithm, or changing a certain authentication system, just change the related "black box" will be ok. On the other hand, some module design of the system is selectable, users may buy or install some parts, then they can obtain the corresponding service, this is similar to the Office software developed by Microsoft, which is convenient for the popularization of individualization of the protocol.

Another assumption is that for different acceptance banks, they lack enough authentications among them. How to build authentication relation network among them is also the research direction of electronic commerce development. From the perspective of database, customer, merchant and bank are the mode of many to many, merchant and merchant, customer and customer do not have certain relation and restriction, there should find an authentication channel, which unites each chain of electronic commerce to a big network through banks' relations, this is the future direction of electronic commerce.

LIST OF REFERENCE

[1] Adams, Carlisle, *Understanding public key infrastructure*, New Riders publishing, 1999

[2] Andrew S.Tanenbaum, *Computer Networks(Third Edition)*, Translated by XIONG gui-xi WANG xiao-hu , Tsinghua University Press , 1998.7

[3] Ahuja, Vijay, *Network and Internet Security*, AP Professional, 1996

[4] Amor, Daniel, *The E-business Evolution*, Prentice Hall, 2000

[5] Atul Kahate, *Cryptography and Network Security*, Beijing, Tsinghua University Press,2005

[6] Black, Uyless, *Internet Security Protocols*, Publishing House of Electronics Industry, 2000

[7] CHEN Yong, *Research and Development of a New Single Route Programmable Adjuster*, Bejing University of technology, 2003

[8] DONG Xiao-hong, *A Thermometer System for High Temperature Resistance Furnace*, Xinijang Industrial College, 2003

[9] FANG Mei-qi, *An Introduction to Electronic Commerce*, Beijing, Tsinghua University Press, 1999

[10] Garfinkel, Simson and Spafford, Gene, *Web Security, privacy and commerce*, O'Reilly, 2002

[11] Howard, Michael and LeBlanc, David, *Writing Secure Code*, WP Press, 2002

[12] JIANG Hong-bo, *Introduction to E-Commerce*, Beijing, Tsinghua University Press, 2009

[13] Kaufman, Charlie et al., *Network Security*, Publishing House of Electronics Industry, 2002

[14] Kosiur, David, *Understanding Electronic Commerce*, Microsoft Press, 1997

[15] Liang jin,Wang yu-min, *Core Technologies of E-Commerce—Theory and Design fo Secure Electronic Transactions Protocols*,XIDIAN University Press,2000

[16] Oaks, Scott, *Java Security*, O'Reilly, 2001

[17] Pistoia, Marco et al., *Java 2 Network Security*, Publishing House of Electronics Industry, 2001

[18] SET Specification Book 1:*BusinessDescription*.Version 1.0, May 31 1997

[19] SET Specification Book2:*Programmer'sGuide*,Versionl.0, May 31 1997

[20] SET Specification Book3:*Formal Protocol Definition*, Version 1.0,May31 1997

[21] Schneider, Gary and Perry, James, *Electronic Commerce*, Thomson Learning, 2001

[22] Smith, Richard, *Internet Cryptography*, Publishing House of Electronics Industry, 1999

[23] Stallings, William, *Network Security Essentials*, Publishing House of Electronics Industry, 2002

[24] Steve Burnett, Stephen Pains, *Password works in English Guide to Practice* , Translated by FENG deng-guo,Tsinghua University Press , 2001.10

[25] TAO Min-fang, *The Security of Information and Electron Business*, YanHuang New Star Net Company, 2003

[26] Visa International and MasterCard International, *SET Secure Electronic Transaction Specification*: Book 1. Business Description, Version 1,1997

[27] Visa International and MasterCard International, *SET Secure Electronic Transaction Specification*: Book 2, Part 1. Programmer's Guide: System Design Considerations, Version 1, 1997.

[28] ISO/IEC International Standard, *Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems*: Part1~Part7, 1996

[29] Yu jian-bin, *Focus on Hacker*, Post and Telecom Press, 1998

[30] Li la-yuan,, *National Defense*, Industry Press,1997

[31] Lin xiao-dong, *a kind of DNS Network Public Key System*, China Information Security, 2001.2

[32] Liu chun-yue, *Security Analysis on Network Payment Based on SET Protocals*, Telecommunications Network Technology,2001.12

[33] Wang ai-ying, *Smart Card Technology*, Tsinghua University Press, 1996

[34] Wang chan,Yao chi-dan, *Comparison of SSL/SET Protocols and Improved Model*,,Modern Computer 2002.8

[35] Wang yu-min,He da-ke,Cryptology-Basic and applied,XIDIAN University Press,1990

[36] Xu jing, *Security Analysis on Network Payment Based on SET Protocals*,WUHAN University of Technology,2003.3

[37] Zhou da-shui, *E-commerce and Security*, China Information Security, Part3, 2000.5

[38] Zheng xue-xue, *Data Security and Software Encryption Technology*, Post and Telecom Press, 1995

[39] Zhang huan-guo, *Computer Security Technology*, Peking University Press, 1994

[40] Zhao yi-ming, *the usage of Public Key Mechanism in Digital Signature*, China Information Security, 2004

[41] Zhou jian-peng, *E-C Technology*, China Information Security, 2005