2014

ISSN : 0974 - 7435 Volume 10 Issue 24

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(24), 2014 [16492-16499]

Study of structure and security of online banking u shield for human information security problem

Tao Xu, Yukun Ma, Zengyong Shi
Henan Institute of Science and Technology, Xinxiang 453003, Henan, (P.R.CHINA)
E-mail: 327188324@qq.com

ABSTRACT

In this paper, we propose a solution for Human information security problem. In the process of conducting e-commerce, the security of online banking system is particularly critical, and all banks take U shield to protect the security of online transactions. In this paper, the composition of U shield commonly used in all domestic banks, encryption algorithm, the safe design of design principles were studied and analyzed, so as to illustrate that U shield can fully guarantee the confidentiality of authenticity, integrity, and non repudiation online transactions.

KEYWORDS

Online banking accounts; Digital certificates; Electronic signature; Digital envelope.

INTRODUCTION

Along with the rapid proliferation of PC and rapid development of Internet technology, people increasingly concern about personal message security issues, especially e-commerce security issues. The core of e-commerce security is the user's online banking account security, financial security, which is to say that, when user account security issues are resolved, the core issue of the online trading security is resolved in the meantime. With the development of computer networks, e-commerce is rapidly developed, the three representatives of the area of electronic commerce: Alibaba (B2B), Dangdang (B2C) and Taobao (C2C), the rapid development of which are inseparable from the development of online banking system of all major banks (hereinafter referred to as online banking), and the security has also become the focus of attention.

FUNDAMENTAL CONCEPTS

At present, in the domestic online banking system, banks provide customers with the high-level security tool for dealing with online banking business - U shield, that is, the client certificate USB key launched by banks.

U shield is a physical hardware com intelligent chip, the shape of which is similar to flash, always protecting your online banking capital security. In addition to the USB interface circuit, on this product the world's leading message security technology was adopted, in the core hardware module, the CPU chip of an intelligent card was used, the internal structure consists of five parts, such as the CPU and encryption logic, RAM, ROM, EEPROM and I/O, as shown in Figure 1.

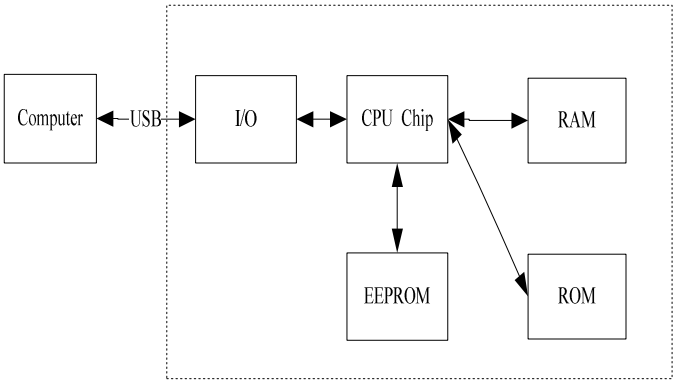

Figure 1 : System hardware structure

Code protection of hardware PIN

U Shield is a kind of tool for electronic signature and digital certificate. The miniature smart card processor is built-in inside of U shield, and before the delivery of the CPU chip of the smart card in the hardware module, the manufacturer writes an e-label on the chip, which can not be tampered with PKI technology, and 1024 non-symmetric key algorithm to realize on-line data encryption, decryption and digital signature so as to ensure the confidentiality, authenticity, integrity, and non repudiation of online transactions.

Safe key system

The dual-key cryptosystem adopted in U shield ensures security. When the initialization is realized, the cryptographic algorithm procedure is reserved by firing in ROM, and then, by generating public and private key program, generates a pair of public and private keys, which can be exported out of the U shield, while the private key is stored in a key district, which does not allow external access. When digital signatures and asymmetric decryption are realized, any cryptographic operation in which participates the private key can only be completed inside the chip, in the whole process, private key will not get out of U shield media, in the external public key, the certification center CA of certificate issuing based on the PKI technology implement the signature of the digital signature certificate, the holder's identity message and files bound by public key, guarantee the safe certification of digital certificate, which utilizes U Shield as the storage medium.

U shield has hardware true random number generator, with the key generated entirely in hardware, and stored in hardware, the user can not directly read from the external and must utilize the corresponding programs, called by CPU inside U shield, for reading and modifying the key document, accordingly, from the outside of the U shield port, any instruction can read and modify the contents of the key area, nor modify, update and delete, ensuring that the key will not get out of hardware, and that hackers can not use illegal program to modify the key.

Meanwhile, in relation to the U shield CPU built-in or smart card chip, in the process of realizing data digest, data encryption and signature, as well as other various algorithms, the encryption algorithm is connected with the E-label and key, which can not be modified in the CPU chip; accordingly, this operation is not reversible. The entire encryption and decryption algorithm run totally within the cryptographic hardware to ensure the security of the process of encryption and decryption of transaction data.

Software operation system

In addition to hardware, the realization of security depends entirely on the smart card chip operating system (COS) with high technical content, the operating system, like DOS, WINDOWS and other operating systems, manages a variety of data, message security and the key files closely related to message security.

FILTERING DRIVING MODEL DESCRIPTION

The filtering driving technology is a currently hot technology, which is more stable and powerful than the HOOK technology. Hierarchical structures are adopted for the driving model of Windows NT Kernel operating system, which respectively drives the file system, intermediate and device, as shown in Figure 2. In this structure, the I/O package-(I/O Request Packet) administrated by the I/O administrator transmits to the inferior devices according to the objects created by driver, meanwhile the driving programs corresponding to the objects of every layer process by order this request packet.

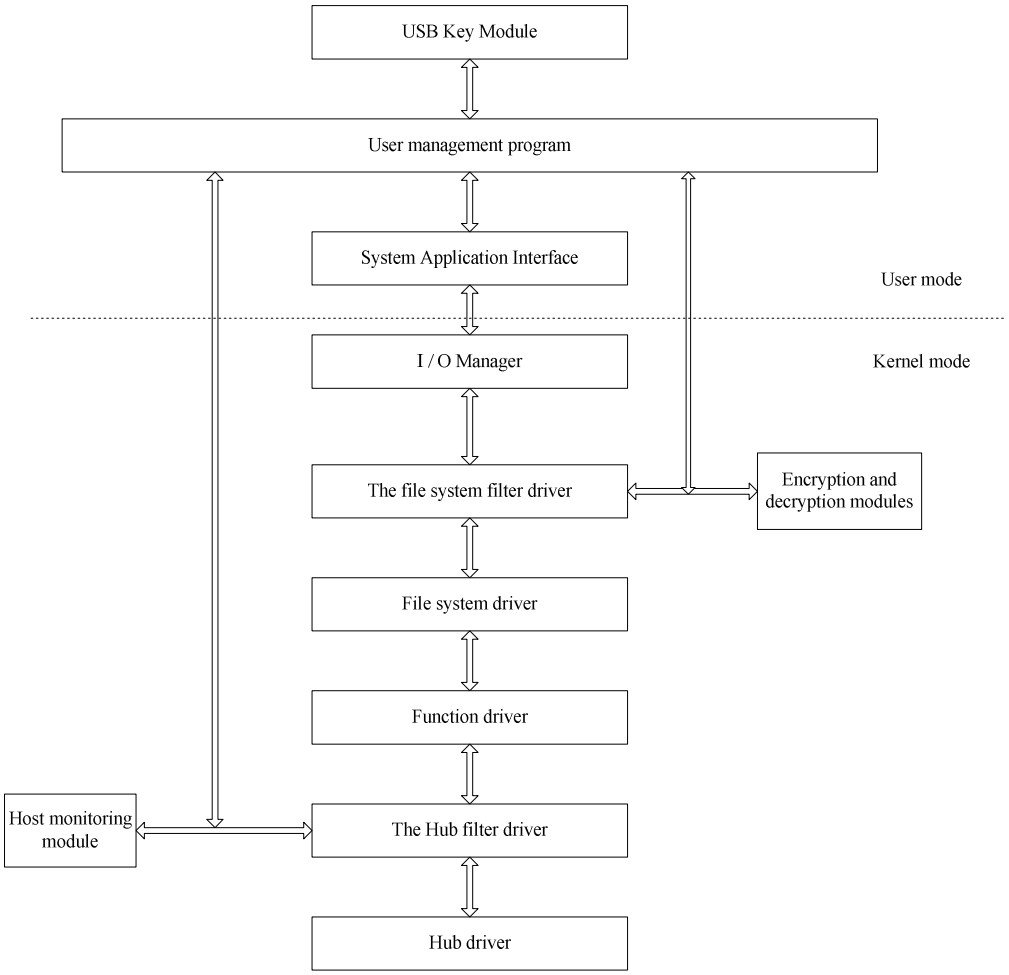

Figure 2 : Description of filtering driving model

After the process, the programs return to the application layer respectively. Based on this model, the filtering driver can intercept all data and process the relevant IRP, prior to the operation of document system driving of the same system, in the process of application programs reading data, as well as the corresponding encryption and decryption operations.

In order to ensure that transaction data can only be utilized by authorized users, in the user mode service process monitoring on USB key and related operations: When the user inserts the USB key, the server process sends the IRP package, the file system filter driver program constitutes a new IRP package, to complete the certification of USB key. After the user unplugging the USB key, the service process still informs file system filter driving layer, through the I/O administrator, in the form of IRP, meanwhile the layer cancels the relevant content in the memory.

U SHIELD AUTHENTICATION AND KEY MANAGEMENT MODULE

Nowadays all banks utilize CA security certification system, developed by the People's Bank of China. Based on practical application of authentication mode of PKI digital certificates, especially on the online banking, the system can be adopted to ensure the safety of their users' online transactions through issuing digital certificate to users.

Authentication mode of digital signature based on PKI

PKI (Public Key Infrastructure) consists in a public key system, namely, with the use of a pair of matched keys to encrypt and decrypt a public key and a private key. The basic principle is the following: the message content encrypted by a key can only be decrypted by the other key paired with the initial one. A public key can be widely distributed to the communicators relevant with their private key reserved by firing in ROM when U shield is initialized.

Every U shield user has a private key which can only be dominated by the user, and used for decryption and signature; also has a public key used to encrypt transactions. When a transaction occurs, the sender uses the recipient's public key to encrypt the data, while the receiver uses his own private key to decrypt the message, consequently, message can safely and unmistakably arrive at the destination, even if intercepted by a third party, because there is no corresponding private key, it's not possible to decrypt.

The "digital certificate authentication method" based on PKI can effectively guarantee the security of user's identity and data transmission. A digital certificate is a group of data structure that contains the user's identity message (key) issued by the Digital Certificate Authentication Center (Certficate Authority, CA). The PKI system builds a perfect process to ensure the security of the digital certificate holder's identity, through the use of encryption algorithm. USB Key can protect the digital certificate from being copied, all the key operations can be realized in the USB Key, the user key do not appear in the computer's memory, nor be spread in the network, only the USB Key holder can operate the digital certificate, accordingly security is assured. The USB Key has many advantages, such as being safe, reliable, easy to carry, easy to use, and of low-cost, coupled with the data protection mechanism of the PKI system, the use of authentication method of USB Key store digital certificate has become a major online banking digital signature authentication mode.

Digital signature based on the PKI technology

Theory of digital signature

U shield system is based on digital signatures and key management, additionally; the application layer service program realizes audition of USB key, including access time, user identity, and authentication level, etc. Its core content is the digital signature module, on which a dual encryption method is adopted for security. The basic principle is shown in Figure 3:

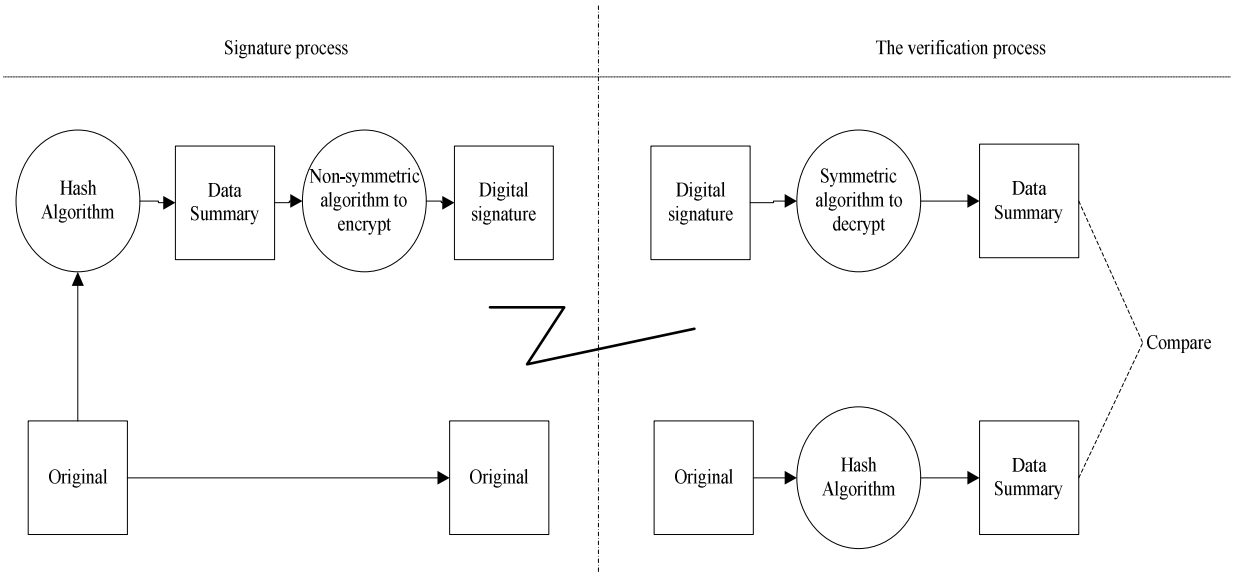

Figure 3 : Theory of digital signature

Detailed algorithm for digital signature and signature verification

For a typical online banking digital signature system, it must contain two important integral parts, one is the signature algorithm (the Signature Algorithm.) and the other one is authentication algorithm (Verification Algorithm.), which has a complete set of the process as shown in Figure 4. In order to meet the two requirements mentioned above, the digital signature system must meet two basic assumptions: A. the signing key is safe, and can be only used by its owner; B. It is the only way to generate a digital signature using the signature key.

When the digital signature technology starts the specific work, first of all, the sender realizes mathematical transformation to the message, the message obtained corresponds to the original message; when the recipient realizes inverse transformation, the original message will be obtained. Many domestic famous mathematicians demonstrated excellent function of hash, DES, RSA mathematical transformation method, through rigorous mathematical calculations. The message

transformed has a strong security in transit, and is difficult to decipher and modify. This process is called encryption, and the corresponding inverse transformation process is called decryption.

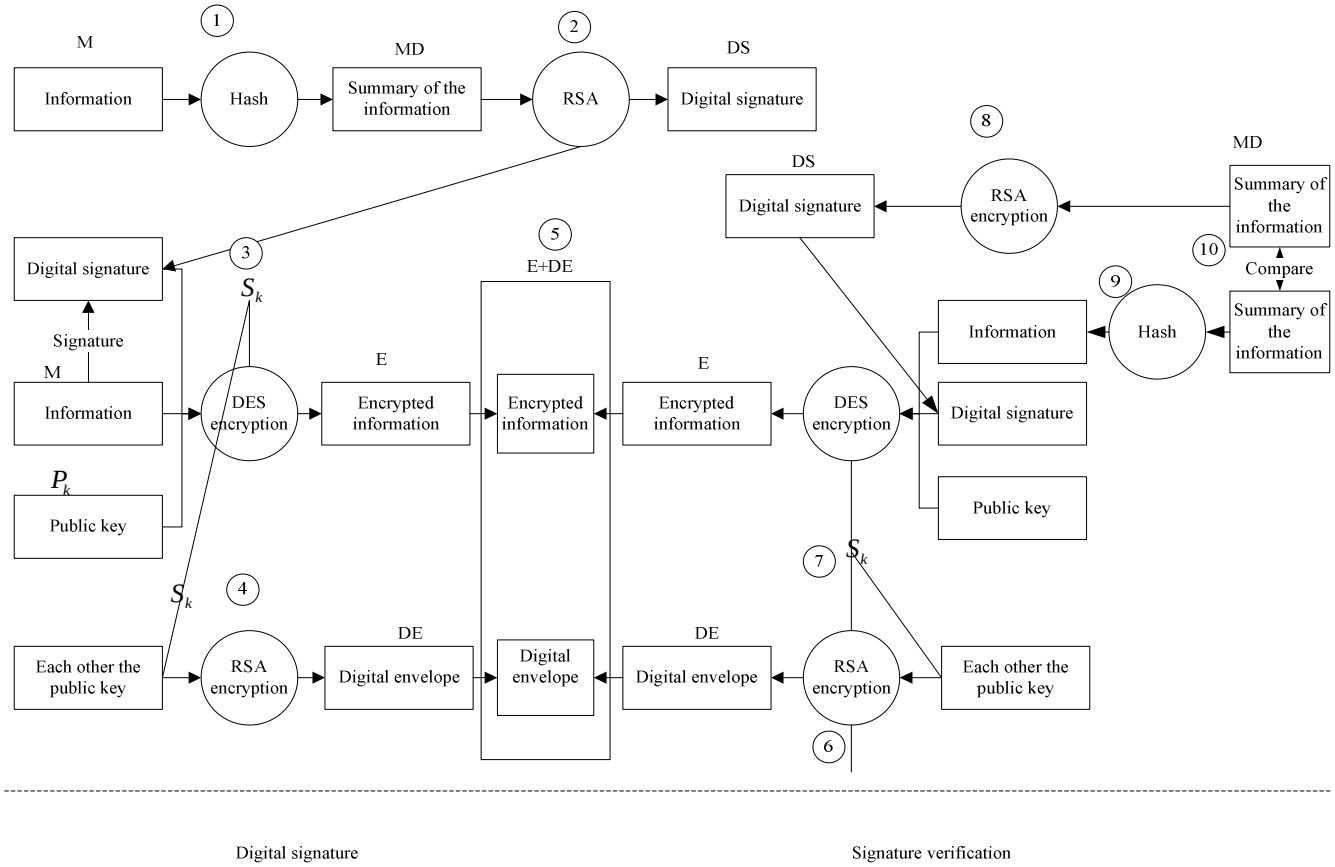

Figure 4 : Digital signature and signature verification algorithm

Hash function encryption algorithm

This algorithm aims at message M transformation of different length to 128 codes, and return to a unique and length-fixed string, which becomes a Message Digest, or Hash value, h = H (M), by comparing this value to determine legal communication between two parties, which is also called digital signature. After data transmission, by comparing the hash value you can confirm whether message has been intercepted or modified on the way, or from a legitimate sender sending or legitimate recipient receiving. Its irreversible operation from plaintext to ciphertext, in which only encryption can not realized instead of recovery, besides, the digest of different message can not be the same, consequently the hash function encryption algorithm has the function of complete verification, password table encryption, digital signature, authentication., etc. Currently MD4, MD5 and SHA are used.

Detailed hash operation is the following: Define Φ as a cycle function, TV is the initialization value of message length L_2. In case of the hash function stipulated by the standard GBT18238.3-2002, for a given loop function Φ, the value of TV should be fixed.

Hash code H of the message M should be calculated in accordance with the following four steps.

Step 1 (To fill)

Fill in the message M to ensure that its length is a multiple of L_1.

Step 2 (To separate)

The filled version of the message M is separated into block $M_1,M_2.....M_q$ of bit L_1, among which M_1 indicates the 1st bit L_1 after M is filled, M_2 indicates the 2nd bit L_1, and so on. It is a process of filling and separating.

Step 3 (iterative)

Set $M_1, M_2,...M_q$ by filling and separating, to be data blocks with a length of bit L_1.. Set H_0 a string equal to TV. bit string L_2 $H_1, H_2,...,H_q$ should be calculated in the following method:

For i from 1-9:

$$H_i = \Phi\left(M_i - H_{i-1}\right)$$

Step 4 (truncated)

By taking the most left bit L_H of output string Hq of which the length is L_2 to export hash code H.

Symmetric encryption algorithm

DES is the Data Encryption Standard of the United States (Date Encryption Standard), an iterative block cipher, in which both the plaintext and the cipher text are 64 bit. By using 56 bit key and additional 8 bit parity. This algorithm is allowed in the cipher text operations of secure messaging MAC mechanism.

One of the most commonly used 3-DES encryption refers to the use of double length (16 bytes) key K = (KL||K) and classification and encryption of 8-byte plaintext data into data packet, as follows:

$$E = DES(P_K)\left[DES^{-1}(S_K)\left[DES(P_K)[M]\right]\right]$$

The decryption method is as follows:

$$M = DES^{-1}(P_K)\left[DES(S_K)\left[DES^{-1}(P_K)[E]\right]\right]$$

Asymmetric encryption algorithm

RSA refers to a reversible algorithm, approved to be used to encrypt and generate digital signature. The key length 512 bit, on which a pair of matching keys are adopted for encryption and decryption. Each key performs a one-way data processing, and each function is precisely contrary to another, if one is used to encrypt, the other would be used to decrypt. The public key is to be open by its owner, while the private key has been produced by firing in ROM when initialization of U shield is realized.

In order to send a confidential transaction message, the sender must use the recipient's public key to encrypt data, once encrypted; only the recipient can use the private key for decryption. On the contrary, the user is also able to use their private key to process data. In other words, the direction for keys can be optional. This provides the basis for the "digital signature", if a user uses his own private key to process data and others could use his public key to process data. Since only the owner himself knows the private key, this message processed has formed a kind of electronic signature.

Digital message

The digital signature produces message MSG composed by message M of any length and at least N-21-byte long. The calculation process of the signature S is as follows.

(1) Calculate the HASH value H of 20 bytes of message M= Hash [MSG].

(2) Split MSG into two parts MSG=(E||DE), where E is composed by N-22 bytes, at the extreme left (MSB) of MSG, DE is composed by the remaining L-N + 22 bytes (LSB) of MSG.

(3) Define a byte B: = '6A'.

(4) Define a byte C: = 'BC'.

(5) Define the block M_1 of L_1-byte to the connection of block B, E, H and C, accordingly,

X : =(B || E || H || C)

(6) The digital signature S is defined as the L_1-byte digital

(7) S : =Sign(S_K)[X]

Digital envelope

A symmetric key will be encrypted with the public key of the other party, to form a digital envelope. Only the recipient can use their private key to decrypt and obtain the symmetric key. As a real envelope that says the address and name of the recipient, who is the only person to dismantle this envelope. In this way, the advantages of the symmetric key are fully made use of. The public key on plaintext, digital signatures and certificates is encrypted for obtaining cipher text E. Encrypt the key using the public key of the other party with asymmetric algorithm to obtain DE, so the key will not be transmitted over the network and lost. Then transfer E+DE to the other party, by the opposite process of decryption, you can get the correct plaintext. Digital envelope ensures that only recipient can see the message content. The process is shown in Figure 5:

Driver and application program communication

Under the Window operating system, the information transmission from application program to driver can be realized by sending control codes to the drive, the underlying driver needs to communicate with the application program actively, and however, this way is not supported by the system. This problem is resolved in the way of event kernel object, namely, creating an event kernel object and initializing the object into the non-fiduciary status. Open in the application program to monitor, when the driver needs to communicate with the application, the event kernel object will be set to the status of the fiduciary status. When the application program monitors this change, it will send its control code of receiving information, in the same time, the driver will response to this request, put the data to be communicated into the data buffer area, when the request returns, the application will obtain the data to be communicated by driver. In this way, the two-way communication between the driver and the application program will be realized.

Accordingly, before using U Shield, normally it is necessary to install the driver, so that U shield can work properly. Besides, the digital certificate should be installed for authentication. When users need to submit an order to bank for transaction, the identity of the user should be verified, the system prompts the user to insert U shield, and enter the password of the U Shield, the system will verify in the background, meanwhile the user can not see the process, once proven, the user can continue to enter the online payment password and verification code. When all authentications approve correctness, transaction is complete.

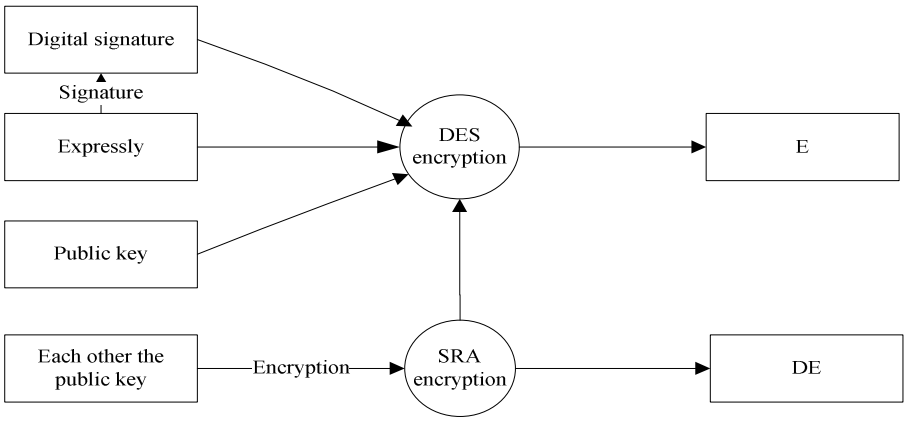

Figure 5 : Digital envelope encryption process

CONCLUSIONS

By introducing the physical structure of U shield, PKI-based identity authentication methods, digital certificates used by this authentication method as authentication credentials, and combining with the asymmetric encryption and symmetric encryption technology, it is illustrated safety and efficiency in the certification process. By means of digital signature technology, mutual communication is enhanced, at the same time, by using the USB Key; users can protect even more their private information, which ensures the confidentiality of online transactions, authenticity, integrity, and non repudiation. With U-shield protection, online transactions are guaranteed in security, on basis of low-cost, high efficiency, convenience, and fastnesses, prompting online banking system of major banks flourish (hereinafter referred to as online banking).

ACKNOWLEDGE

The research work is supported by National Natural Science Foundation (61304061).

REFERENCES

[1] B.Vimala, A.Hossein, S.H.Lau, K.K.Teoh; A secure remote user authentication system - Digital certificates, IBIMA, **(2009)**.

[2] B.Danny; Digital certificates: Worth the paper they're written on?, Computer Fraud and Security, **10 (2012)**.

[3] L.Hehua, W.Chuning; Study on the application of digital certificates in the protection of network information security and data integrity, Journal of Networks, **8(11)**, 2592-2598 **(2013)**.

[4] A.Mohammed, Z.Qingwei, B.Azzedine, R.Yonglin; An efficient k-Means authentication scheme for digital certificates revocation validation in vehicular ad hoc networks, Wireless Communications and Mobile Computing, **14(16)**, 1546-1563 **(2014)**.

[5] H.Jeff; Weaponised malware: How criminals use digital certificates to cripple your organisation, Network Security, June, **6(12-14)**, **(2011)**

[6] Z.Yunsheng; Secure digital certificate design based on the RSA algorithm, Journal of Digital Information Management, December, **11(6)**, 423-429 **(2013)**.

[7] X.Yingying; Research and design of a PKI-based authentication system, China Electric Power Education, Research Summary and Technology Forum Special Issue, **(2006)**.

[8] Q.Yunhui, B.Xinguo; Principle and application of digital signature technology, Fujian Computer, **05 (2010)**.

[9] Z.Rigui, L.Wei, H.Tiantian; Quantum identity authentication and digital signature through quantum digital certificate, Journal of Computational Information Systems, May 15, **10(10)**, 4425-4432 **(2014)**.

[10] J.Qingxuan, G.Panpan, G.Xin, W.Xin, Z.Bing, C.Baojiang; A digital certificate-based lightweight authenticated protocol with key agreement for wireless, Journal of Computational Information Systems, May 15, **9(10)**, 3817-3825 **(2013)**.

[11] O.Maria, S.Sergio; University authentication system based on java card and digital X.509 certificate, International Journal of Computer Science Issues, July, **9(44-3)**, 23-29 **(2012)**.
[12] Q.Zhang; Secure digital certificate design based on the public key cryptography algorithm, Telkomnika - Indonesian Journal of Electrical Engineering, December, **11(12)**, 7366-7372 **(2013)**.
[13] H.Lein, R.Jian; Generalized digital certificate for user authentication and key establishment for secure communications, IEEE Transactions on Wireless Communications, July, **10(7)**, 2372-2379 **(2011)**.
[14] S.Liujie, Z.Leihong, L.Zhen, Z.Songlin; A technology of printing forgery prevention for certificates based on fingerprint information, Advanced Materials Research, **174**, 112-117 **(2011)**.
[15] R.B.Steven, S.Stephen; Trust darknet: Control and compromise in the internet's certificate authority model, IEEE Internet Computing, **17(3)**, 18-25 **(2013)**.