# Design and Realization of RSA Digital Signature System Based on Digital Certificate

Yanna Wei, Yongtao Jin, Jianwei Zhou

North China Institute of Aerospace Engineering, China

*weiyanna_2005@163.com

**Keywords:** digital signature; digital certificate; digital digest; RSA

**Abstract.** Digital signature plays a more and more important role in e-commerce. The basic methods of digital signature are introduced and a digital signature scheme based on digital certificate is proposed in this paper. Digital certificate is generated after personal information is written. The effective data, RSA parameters and signature results are included in digital certificate. The related RSA parameters of private key certificate are encrypted by private key password. The digital digest is gotten through hash algorithm in this scheme. Digital signature is operated by using RSA parameters in private key certificate and the signature is verified by RSA parameters in public key certificate by verifier.

## 1 Introduction

Digital certificate is a credential issued by certificate authority center, which is the most important application field of digital signature technology [1][2]. In general, the certificate contains a public key, name of key's owner, signature of certificate authority center, valid time of key, license issuing authority, serial number of certificate and other information [3][4]. A digital certificate is a series of data that marking identity information of communicator in network communication. From the perspective of key management, the delivery of public key is completed by digital certificate. Considering realistic feasibility and legal effect, only the scheme of digital signature based on digital certificate has practical significance.

With the rapid development of information technology, the enterprises are inseparable from the network to survive and develop in the new information era [5]. The network also brings hidden danger in communication between enterprises. In 1988, network identification function is provided by ISO framework, which is called *X*.509 protocol. The most important part of this protocol is public key certificate. In this paper, a digital signature scheme based on digital certificate is used to ensure integrity of online trading data, non-repudiation of transmitting information and certainty of traders.

## 2 The Principle of RSA Algorithm

Two large prime numbers $p$ and $q$ are selected randomly, and $n$ is calculated to meet $n=p\times q$. The random number $e$ is selected to meet $1<e<\varphi(n)$ and $gcd(e, \varphi(n))=1$, so public key is $(e, n)$. $d$ is calculated to meet $ed=1 \bmod \varphi(n)$, so private key is $(d, n)$. $p$, $q$ and $\varphi(n)$ is destroyed finally. $\varphi$ is Euler function, in which $\varphi(n)=(p-1)\times(q-1)$. Plaintext and ciphertext spaces in RSA algorithm are integer values between 0 and $(n-1)$.

Message $m$ is divided into group $m_i$ in encryption process of RSA, and the length of $m_i$ just is less than $n$ bits. Each group of $m_i$ is encrypted using the function of $c_i = m_i^e \bmod n$, in which ciphertext $c$ is connected by $c_i$. Ciphertext $c$ is decomposed into $c_i$ in decryption process of RSA, and the length of $c_i$ just is less than $n$ bits. Each group of $c_i$ is decomposed using the function of $m_i = c_i^d \bmod n$, in which plaintext m is connected by $m_i$.

In RSA algorithm, $n$ is defined by $p\times q$, where $p$ and $q$ are prime number, the difference between $p$ and $q$ is larger, the greatest common factor of $(p-1)$ and $(q-1)$ is smaller, $p$ and $q$ are big enough.

In general, $e$ is not too small and order $i$ must reach value of $(p\text{-}1)\times(q\text{-}1)/2$ and $e^i = 1 \bmod \varphi(n)$.

After e is selected, Euclid algorithm is used to calculate $d$ in polynomial time. $d$ is demanded to be greater than $n^{1/4}$. If $d$ is smaller, the speed of signing and decryption is faster, but its safety is not strong.

## 3 The Digital Signature Based on Digital Certificate

**3.1 The Principle of Digital Signature.** A typical digital signature system must contain two important components of signature and authentication.

**The Processes of Signature.** The messages of sender are calculated by MD5 to generate message digest of 128 bits before signature firstly. MD5 function is a one-way hash function, by which messages of arbitrary length can be compressed into message digest of 128 bits. MD5 function is not based on any hypothesis and password system, but structured directly. Because the execution speed is very fast, MD5 is widely accepted to be one-way hash algorithm. Unidirectionality and crashworthiness of MD5 is applied to realize completeness of messages. Public key cryptography is used in sender, and message digest is encrypted by private key. After the processes above, encrypted character string is digital signature.

**The Processes of Authentication.** Digital signature is decrypted by public key of sender in receiver, and the result should be message digest of 128 bits. Original message is recalculated by using MD5 to get message digest of own. These two message digests are compared, if both of them are same, then verification is successful, which can confirm message integrity and signature really belong to sender. Otherwise, the authentication fails, which can confirm signature has been tampered and pretended. This digital signature system is suitable for information processing of large files.

The processes of signature and authentication in digital signature system are shown in Fig. 1.

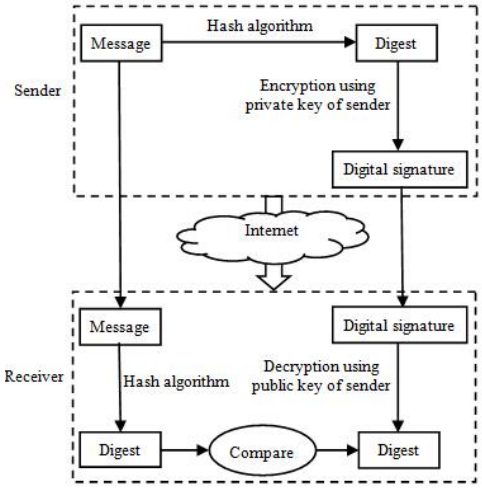


Figure 1. The processes of signature and authentication in digital signature system

**The identification process of *X*.509.** Identification process of *X*.509 is divided into three types, which are simple identification, two-way identification and strong identification. The private key signature of sender is needed and public key is known by both sides in the entire identification process. The identification process of *X*.509 is shown in Fig. 2.

**Simple identification.** The process of simple identification is shown in Fig. 2(a). The signature information of *A* is transmitted to *B*. $t_A$ is timestamp of *A*, $r_A$ is random number, *sgnData* is signature with private key of *A*, and $Ek_{uB}[K_{ab}]$ is used to encrypt with public key of *B*. Identity of *A* only is verified, because private key of *A* is used to sign in this process.

**Two-way identification.** The process of two-way identification is shown in Fig. 2(b). The first step is same with simple identification. In the second step, $t_B$ is timestamp of *B*, $r_B$ is random number and it is generated by *B*, *sgnData* is signature with private key of *B*, and $Ek_{uA}[K_{ba}]$ is used to encrypt with public key of *A*. Identity of *A* and *B* are verified in this process.

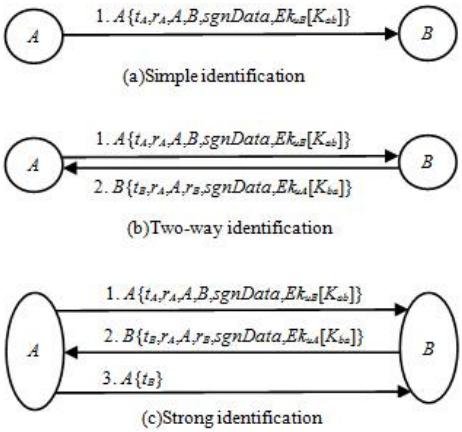


Figure 2. The identification process of *X*.509

**Strong identification.** The process of strong identification is shown in Fig. 2(c). The former two steps are same with two-way identification. In the third step, $r_B$ is contained in message of *A* to *B*, which is used to deal with replay threat without checking timestamp.

**Module Design.** Digital signature system based on digital certificate mainly includes certificate generation module, digest processing module, signature module and authentication module.

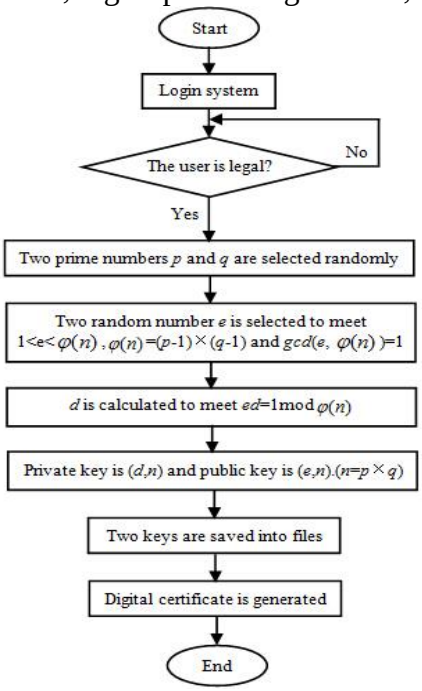


Figure 3. The system flowchart of certificate generation module

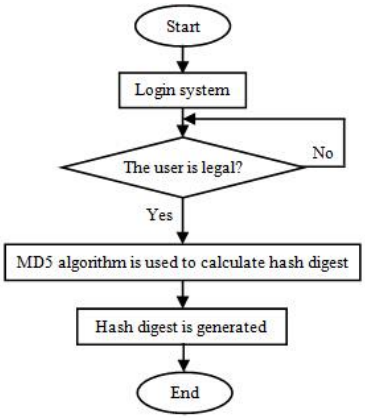


Figure 4. The system flowchart of digest processing module

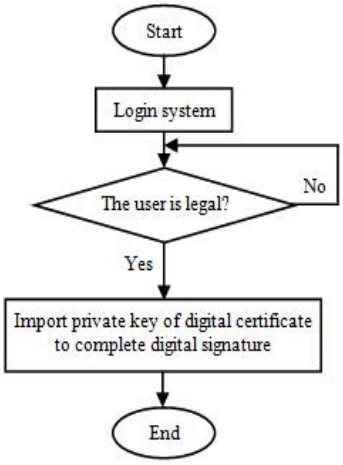


Figure5. The system flowchart of signature module

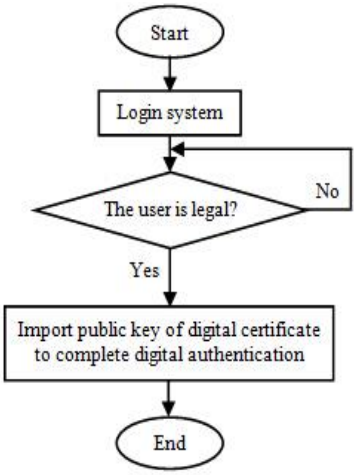


Figure 6. The system flowchart of authentication module

Public key and private key are provided for signature in certificate generation module, two files are used to save these keys. The system flowchart of certificate generation module is shown in Fig. 3.

Hash digest of 128 bits is generated in digest processing module, MD5 algorithm is used in this module. The system flowchart of digest processing module is shown in Fig. 4.

Document digest is signed using RSA algorithm and the signature result is saved in signature module. The system flowchart of signature module is shown in Fig. 5.

Signature result is authenticated using RSA algorithm and authentication result is returned in authentication module. The system flowchart of authentication module is shown in Fig. 6.

**System implementation.** According to module design, three classes are defined. There are MD5 algorithm class, hash class and RSA algorithm class. Main functions in system are shown as follows:

Encrypt (char * OutFile, char * InFile, char * RsaKeyStr, char * RsaModStr) //according to digest to generate signature

Decrypt (char * InFile, char * RsaKeyStr, char * RsaModStr) // according to signature to restore digest

OnMD5Hash () // MD5 algorithm is processed on selected file

**Safety analysis.** The key used in RSA algorithm comes from certificate. Relevant information is filled in by applicant, after which tow files are generated. One file is used to store private key, and another file is used to store public key. Private key is encrypted with password to ensure the safety. Public key is signed to ensure the integrity. The management of keys is more convenient.

## 4 Conclusions

Digital signature based on digital certificate has the same legal effect with the traditional handwriting signature. Digital certificate is introduced to preserve the relevant key information in digital signature system, which solves management issues of key and satisfies the basic requirement of security. Digital certificate is generated to effectively prevent from files are damaged and tampered in the process of file transmission.

## Acknowledgment

This work is supported by Hebei province science and technology support project (No.13210707), all support is gratefully acknowledged.

## References

[1] M. Abdalla, J.H. An, M. Bellare and C. Namprempre. 2008. From identification to signatures via the Fiat-Shamir transform: Necessary and sufficient conditions for security and forward security, IEEE Transactios on Information Theory, 54(8): 3631-3646.

[2] J.H. An, Y. Dodis and T. Rabin. 2002. On the security of joint signature and encryption, In Advances in Cryptology-Eurocrypt 2002, 2332: 83-107.

[3] B. Barak and M. Mahmoody-Ghidary. 2007. Lower bounds of signatures from symmetric primitives, In 48th Annal Symposium on Foundations of Computer Science, 290(1-2): 680-688.

[4] M. Bellare and S. Shoup. 2008. Two-tier signatures from the Fiat-Shamir transform with applications to strongly unforgeable and one-time signatures, IET Proc.Information Security, 2(2): 47-63.

[5] D. Boneh. 2008. Short signatures without random oracles and the SDH assumption in bilinear groups, Journal of cryptology, 21(2): 149-177.