Research on Digital Signature Based on Digital Certificate
Yong Huang, Fugui Chen, Peixin Qu
School of Information Engineering, Henan Institute of Science and Technology, Xinxiang, 453003, China
451800@163.com

Abstract: The important significance of digital signature on internet transaction security is analyzed. The theory and technology base of digital signature is PKI, and the principle of digital signature is introduced. The defaults of the technique of digital signature based on public key and private key pairs, and the approach of digital signature based on digital certificate is presented, and its rationality, effectivity and feasibility are discussed. The process of design and implementation of digital signature system based on digital certificate are introduced, and the important source codes and running interfaces of prototype system are shown.

Keywords: digital signature; digital certificate; PKI (Public Key Infrastructure)

1 Introduction
The rapid development of Internet e-commerce has a new model of business activities. How to open network (Internet) transmission line to protect the legitimacy of the data, the only, non-repudiation to prevent illegal tampering and trading each other's identity, has become a serious problem. Stamp-based digital signature technology is proposed in this context, and become the field of information security research in the field of computer applications and a hot and difficult. Although e-commerce on-line transmission of data security have had a strong demand, however, to meet the security needs of the digital signature seals the theory and technology have not been very good solution. Ensure data integrity and non-repudiation of transactions each other is based on the seal of the digital signature system must address the core issue is the digital signature system seal the foundation.

In response to these problems, this paper through a digital signature technology, domestic and foreign technology in the current analysis, a digital signature based on the seal system model and analysis system used in key technology: one-way hash function digital signatures.

E-commerce may include the use of electronic data interchange, electronic money exchange, Internet advertising, websites, online databases, computer networks, and point-of-sale computer systems. So, the security problem becomes very important in e-commerce. Both buyers and sellers on the Internet must ensure that all financial transactions are real and reliable operation, and make customers, merchants and other parties have absolute confidence. Therefore, e-commerce must ensure that the system has a very reliable security technology, that is to say, the network must ensure the four major safety elements, and they are confidentiality, authentication, integrity, availability and non-repudiation of information.

2 PKI (Public Key Infrastructure)
PKI (Public Key Infrastructure) is a system, which offers services of public key encryption and digital signature, based on public key encryption technologies. It is composed of CA, numeric certificate library, secret key backup and restore system, numeric certificate withdraw system and API.

PKI, which is based largely on cryptographic theory and provides mainly the services of authentication and confidentiality and integrality and non-repudiation, turns into the very important secure platform of authentication and authorization in network application and guarantees the information security of the network activity to people.

CA is the kernel part of PKI, and it provides functions of awarding, updating, withdrawing and validating the numeric certificate. PKI technology has already been comprehensively used in many fields. For computer system and net. The key to PKI system is numeric certificate management (generate, distribute, validate, remove etc).

3 Digital Certificates
509 digital certificates based PKI system has offered the good trust mechanism in the network computing environment, and can offer the security services in common use such as confidentiality, integrality, no repudiation and so on.
Digital certificate is an electronic identification card similar to the role of the real-life an identification card. It is issued by an authority organization, people can use it to contact each other to identify the identity.

Signing in a written document means to confirm it, and its role are two points: first, because it is difficult to deny their own signature, which confirms the fact that documents have been signed; Second, because the signature difficult to counterfeit, it ensures this document is really.

The role of digital signature and signed a written document is similar. Digital signature can confirm the following two points: first, the message is sent by the signer; Second, the information received has not any changes. Therefore, digital signature can be used to prevent electronic information being modified easily, or sending a message by fraudulent use of other people's name. Or sent (received) a letter and then deny to happen, and so on.

Usually, the digital signatures are in three major ways, they are: RSA signature, DSS signature and the signature Hash. The three algorithms can be used alone, or combined use.

4 Design and Realization of Digital Signature

![Diagram of the process of signature and verification with certificate](image)

Figure 1. The process of signature and verification with certificate

5. The Core Resource Code

The code as follow:

1). Store
   Certificate Certificates { get; }
   void Open(CAPICOM_STORE_LOCATION StoreLocation, string StoreName, CAPICOM_STORE_OPEN_MODE OpenMode)
2). Signer
   Certificate Certificate { get; set; }
   void Load(string FileName, string Password)
3). Certificate
   PrivateKey PrivateKey { get; set; }
   void Load(string FileName, string Password, CAPICOM_KEY_STORAGE_FLAG KeyStorageFlag, CAPICOM_KEY_LOCATION KeyLocation)
void Display()

4). Certificates
   int Count { get; }
   Certificates
   Find(CAPICOM_CERTIFICATE_FIND_TYPE
      FindType, object varCriteria, bool
      bFindValidOnly)
   Certificates Select(string Title, string
      DisplayString, bool bMultiSelect)

5). HashedData
   string Value { get; }
   CAPICOM_HASH_ALGORITHM Algorithm
   { get; set; }
   void Hash(string newVal)

6). SignedData
   string Content { get; set; }
   Certificates Certificates { get; }
   string Sign(ISigner pSigner, bool bDetached,
      CAPICOM_HASH_ALGORITHM Algorithm,
      CAPICOM_ENCODING_TYPE EncodingType)
   void Verify(string SignedMessage, bool
      bDetached,
      CAPICOM_SIGNED_DATA_VERIFY_FLAG
      VerifyFlag)

7). public enum CAPICOM_STORE_LOCATION
   { CAPICOM_MEMORY_STORE = 0,
     CAPICOM_LOCAL_MACHINE_STORE = 1,
     CAPICOM_CURRENT_USER_STORE = 2,
     CAPICOM_ACTIVE_DIRECTORY_USER_STORE = 3,
     CAPICOM_SMART_CARD_USER_STORE = 4,
   }
   public enum CAPICOM_STORE_OPEN_MODE
   { CAPICOM_STORE_OPEN_READ_ONLY = 0,
     CAPICOM_STORE_OPEN_READ_WRITE = 1,
     CAPICOM_STORE_OPEN_MAXIMUM_ALLOWED
     = 2,
     CAPICOM_STORE_OPEN_EXISTING_ONLY = 128,
     CAPICOM_STORE_OPEN_INCLUDE_ARCHIVED
     = 256,
   }
   public enum CAPICOM_KEY_STORAGE_FLAG
   { CAPICOM_KEY_STORAGE_DEFAULT = 0,
     CAPICOM_KEY_STORAGE_EXPORTABLE = 1,
     CAPICOM_KEY_STORAGE_USER_PROTECTED
     = 2,
   }
   public enum CAPICOM_KEY_LOCATION
   { CAPICOM_CURRENT_USER_KEY = 0,
     CAPICOM_LOCAL_MACHINE_KEY = 1,
   }
   public enum CAPICOM_CERTIFICATE_FIND_TYPE
   { CAPICOM_CERTIFICATE_FIND_SHA1_HASH = 0,
     CAPICOM_CERTIFICATE_FIND_SUBJECT_NAME
     = 1,
     CAPICOM_CERTIFICATE_FIND_ISSUER_NAME = 2,
     CAPICOM_CERTIFICATE_FIND_ROOT_NAME = 3,
     CAPICOM_CERTIFICATE_FIND_TEMPLATE_NAME
     = 4,
     CAPICOM_CERTIFICATE_FIND_EXTENSION = 5,
     CAPICOM_CERTIFICATE_FIND_EXTENDED_PROPERTY
     = 6,
     CAPICOM_CERTIFICATE_FIND_APPLICATION_POLICY
     = 7,
     CAPICOM_CERTIFICATE_FIND_CERTIFICATE_POLICY
     = 8,
     CAPICOM_CERTIFICATE_FIND_TIME_VALID = 9,
     CAPICOM_CERTIFICATE_FIND_TIME_NOT_YET_VALID
     = 10,
     CAPICOM_CERTIFICATE_FIND_TIME_EXPIRED = 11,
     CAPICOM_CERTIFICATE_FIND_KEY_USAGE = 12,
   }
   public enum CAPICOM_HASH_ALGORITHM
   { CAPICOM_HASH_ALGORITHM_SHA1 = 0,
     CAPICOM_HASH_ALGORITHM_MD2 = 1,
     CAPICOM_HASH_ALGORITHM_MD4 = 2,
     CAPICOM_HASH_ALGORITHM_MD5 = 3,
   }
   public enum CAPICOM_ENCODING_TYPE
   { CAPICOM_ENCODE_ANY = -1,
     CAPICOM_ENCODE_BASE64 = 0,
     CAPICOM_ENCODE_BINARY = 1,
   }
   public enum CAPICOM_SIGNED_DATA_VERIFY_FLAG
   { CAPICOM_VERIFY_SIGNATURE_ONLY = 0,
     CAPICOM_VERIFY_SIGNATURE_AND_CERTIFICATE
     = 1,
   }

6. The Running Interface of Digital Signature System Based on Digital Certificate

The running interface of digital signature system based on digital stamp is based on the scientific research fund of Hunan provincial education department(08A009 and 08B015), as shown in Figure 2.

Figure 2. The running interface of digital signature system based on digital stamp (a)
References


