

# 國立交通大學

電機資訊學院 資訊學程

## 碩士論文

以二維碼實現 PKI 之實體應用

Physical PKI Application with 2D Barcode



研究生：賴國旺

指導教授：葉義雄 教授

中華民國九十三年七月

以二維碼實現 PKI 之實體應用  
Physical PKI Application with 2D Barcode

研 究 生：賴國旺

Student : Kuo-Wang Lai

指 導 教 授：葉義雄

Advisor : Yi-Shiung Yeh

國 立 交 通 大 學  
電 機 資 訊 學 院 資 訊 學 程  
碩 士 論 文



A Thesis  
Submitted to Degree Program of Electrical Engineering Computer  
Science

College of Electrical Engineering and Computer Science  
National Chiao Tung University  
in Partial Fulfillment of the Requirements

for the Degree of  
Master of Science

In  
Computer Science

July 2004

Hsinchu, Taiwan, Republic of China

中華民國九十三年七月

## 以二維碼實現PKI之實體應用

學生：賴國旺

指導教授：葉義雄

國立交通大學電機資訊學院 資訊學程（研究所）碩士班

### 摘 要

目前PKI機制是捍衛電子商務交易安全的最佳方案，它提供虛擬網路世界一個信任的安全機制，對於電子商務的健全發展具有重大意義。然而在電子商務中，所有的資訊都是數位化、無紙化的虛擬物件，唯有透過數位化設備才能夠存取，不同於人們所習慣的實體生活。在人們習慣的實體生活中，許多交易都是以實體的物件為依據，像是電影票、統一發票、ATM轉帳的存根聯等票證，這些實體的票證，也很容易被人們所接受，通行無礙。而電子商務的應用中，實體化的需求也依然持續存在，為進一步推動PKI在實體化應用的發展，我們將嘗試把PKI機制由數位化轉為實體化，將PKI機制帶入實體的交易世界。在本篇論文中，我們會探討PKI實體應用的需求，並且提出一套實體化應用的方案，將PKI應用資訊實體化輸出，以提供實體化應用的需求。

**關鍵字：**公開金鑰架構，數位憑證，電子憑證，二維條碼，數位簽章

# Physical Application of PKI with 2D Barcode

Student: Kuo-Wang Lai

Advisor: Prof. Yi-Shiung Yeh

Degree Program College of Electrical Engineering and Computer  
Science  
National Chiao Tung University

## Abstract

Currently, PKI is considered as the optimal solution to safeguard e-commerce. PKI provides a reliable security mechanism for the virtual world and as well as plays a critical for the development of e-commerce. But all information in e-commerce contains virtual digitalized objects, which are not recorded on paper. Users retrieve information by digital devices, which are different from the real world life. In physical world, most transactions are conducted by means of physical objects, such as movie tickets, uniform invoices, ATM receipts, which are acceptable to the general public. Physical objects are required in e-commerce, too. In an effort to accelerate the physical application of PKI, this thesis attempts to transform digitalized PKI mechanism from digitalized objects into physical objects so as to incorporate PKI mechanism into physical world. This thesis relates to the requirements for PKI physical application and contains the study on physical applications so as to apply PKI digitalized information to physical objects for use in the physical world.

**Keywords:** Public Key Infrastructure (PKI), 2D Barcode, Electronic certificate, Digital signature

# Acknowledgement

First of all, I would like to express my heartfelt gratitude to my advisor, Professor Yi-Shiung Yeh, for his guidance for the past 2 years. Professor Yeh helped me to develop the most accurate research methods and learning attitude. Thanks to Professor Yeh, for my thesis was completed. And I also want to thank my supervisors and coworkers-- Clark Hor, Seth Chen-- for their encouragement and support. That's how I could spend my spare time and have thus completed my thesis.

My special thanks to my classmates -- Chen-Yu Lee, Alex Wang, Johnny Chiang, Athena Huang -- for their untiring support and encouragement for the past 2 years. Their friendship remains vivid in my mind and will not fade away for the rest of my life. Thanks also to the teachers on National Chiao Tung University for their valuable comments and suggestions.

I am particularly grateful to my wife Chin-Chia. Thank you for your tolerance and support. You inspired whenever I felt helpless. You comforted me whenever I was out of mind. Thank you so much for staying with me throughout my school life.

Last but not least, I want to thank my parents for giving me an opportunity for education. Thanks to my brothers and sisters. I won't be able to accomplish anything without you. Thank you again.

I humbly present my thesis to all those who ever care about me and have helped me during the past years. Please accept my most profound gratitude. Thank you.

Kuo-Wang Lai

College of Electrical Engineering and computer Science,  
National Chiao Tung University  
August 2004

# Contents

中文摘要 .....	i
ABSTRACT.....	ii
Acknowledgement.....	iii
Contents.....	iv
List of Tables .....	vi
List of Figures .....	vi
Chapter 1 Introduction .....	1
1.1 Research Motives .....	1
1.2 Goals.....	2
1.3 Cryptosystem.....	3
1.3.1 Secret Key Cryptosystem.....	3
1.3.2 Public Key Cryptosystem [14].....	4
1.3.3 One-way Hash function [14].....	8
1.4 Framework of thesis .....	10
Chapter 2 Background Research.....	11
2.1 Public Key Infrastructure .....	11
2.1.1 Digital Signature.....	12
2.1.2 X.509 Certificates.....	13
2.1.3 Certificate Revocation List.....	17
2.1.4 Overview of public key infrastructure .....	19
2.1.5 PKI application message standards and specifications .....	21
2.2 Two dimensional Barcode .....	31
2.2.1 About Two Dimensional Barcode [15].....	31
2.2.2 Types of 2D Bar Code [18] .....	31
2.2.3 Features of 2D Bar Code [17][18].....	32

2.2.4 PDF417 Barcode [18].....	33
Chapter 3 Requirements and Issues Related to PKI Physical Application .....	36
3.1 PKI implementation and application in Taiwan.....	36
3.2 Demands for e-document .....	39
3.3 Demands for e-uniform invoice .....	41
3.4 Research highlights on PKI physical application .....	43
Chapter 4 Proposed PKI Physical Techniques .....	44
4.1 Estimated Goals.....	44
4.2 Technical Issues To Be Overcome .....	44
4.3 Recommended PKI Application Proposal.....	46
4.3.1 The framework of encoding and output .....	47
4.3.2 Encoding technique for PKI information and 2D bar codes .....	47
4.3.3 Visualized template design and the Digital Mark .....	49
4.3.4 Reading and automatic validation process of Digital Mark.....	50
4.3.5 Decoding of Digital Mark .....	51
4.3.6 Validation module of PKI digital signature.....	52
4.4 Comparison and analysis of PKI application information carriers .....	53
Chapter 5 Implementation of Experimental System.....	55
5.1 Physical Environment .....	55
5.2 Experimental System Architecture.....	56
5.3 Experimental system process .....	59
5.4 User Interfaces and Message Verification Test .....	59
5.5 Evaluation of Experimental System Issues .....	66
Chapter 6 Conclusions .....	67
6.1 Conclusion.....	67
6.2 Future research directions .....	67
References .....	69

# List of Tables

Table 1: Comparison and analysis of PKI application information carriers.....54

# List of Figures

Figure 1 Secret key cryptosystem.....3

Figure 2 Public key cryptosystem.....7

Figure 3 One way hash function.....10

Figure 4 Digital signature.....13

Figure 5 recursive structure of PKCS#7.....24

Figure 6 1D Barcode versus 2D Barcode.....31

Figure 7 framework of PKI in Taiwan.....36

Figure 8 framework of PKI in government sector.....38

Figure 9 certification authorities approved by ministry of Economy affairs.....39

Figure 10 G2G e-document exchanges.....40

Figure 11 framework of e-uniform Invoice.....42

Figure 12 the architecture of proposed PKI physical application.....46

Figure 13 the framework of encoding and output of PKI information.....47

Figure 14 packaging and barcode encoding process of PKI information.....49

Figure 15 visualized template and of Digital Mark.....50

Figure 16 reading and automatic validation process of Digital Mark.....51

Figure 17 decoding of Digital Thumb.....52

Figure 18 validation modules of PKI digital signature.....53



Figure 19 the architecture of experimental system.....56  
Figure 20 the output sample in Postscript.....58  
Figure 21 the processes of experimental system.....59  
Figure 22 the user interface : 0 Selection of key pairs.....60  
Figure 23 the user interface : 1.1 Digital signature.....61  
Figure 24 the user interface : 1.2 Digital Thumb.....62  
Figure 25 the user interface : 1.3 Physical output.....63  
Figure 26 Sample of physically outputted document.....64  
Figure 27 the user interface : 2 Document verification.....65



# Chapter 1

## Introduction

### 1.1 Research Motives

Public Key Infrastructure (PKI) provides a secure environment to facilitate transactions in the virtual world. PKI helps users to acquire perfect solutions regarding the authentication of identity, security of document, data encryption, and even the non-repudiation of transactions. As a result, PKI has minimized the insecurity and risks of transactions via the Internet, and has thus accelerated the development of e-commerce.

PKI is designed for the virtual world created by Internet that calls for electronic devices, digital data, and printing devices as basic equipment. All data and information are recorded and transmitted electronically and digitally. PKI mechanism allows users to sign and encrypt important e-mails before the e-mails are sent. Recipients need the e-mail software to decrypt e-mails and verify the digital signature before they read the information on the screen. In this way E-mails are saved electronically, too. The content and digital signatures of the e-mails are enveloped and saved electronically. In other words, recipients are allowed to print the content of e-mails, but they cannot print out the signature and they will lose the security of PKI. Apparently, it is not what we want at all. Let's take another example about the official e-Document of TAIWAN government. The TAIWAN government is promoting e-Taiwan plan progressively in recent years. Now, government agencies exchange official e-Documents via PKI mechanism. The recipient print out the e-Document and assigns serial numbers to incoming

e-documents for further application after the documents are received. However, the digital signature is lost when the e-documents are printed. Apparently, there is no way to verify the source and content of the printed documents any more. Without sender's signature, verification is an impossible task. These may be a risk for the application of the printed e-document. Despite its overwhelming popularity in the digital world, PKI remains need to be improved, especially its application to the physical world. Is there any solution to solve these problems? This thesis attempts to find a technical solution with emphasis on physical application so as to solve the problems related to PKI application to physical world.

## 1.2 Goals

Paperless is considered a major benefit created by e-commerce. But the demand for paper still increased and the e-commerce grew more and more popular at the same time. The e-commerce stresses on fast, time reducing, and efficiency. As a result, the demand for papers decreased to a certain extent, but the overall demand for paper increased due to the rapid development of information technologies. Users still rely on papers to save critical information. As far as PKI application is concerned, proper techniques are needed to output digital certificates and digital signature. Physical output alone is not sufficient. Users need the automation capability regarding digital techniques so as to process information for automatic input, output, and verification. Papers are most popular carrier for information and are available all over. Users are eager to find out how to apply PKI-related techniques to papers. Therefore, this thesis concentrates on the following topics:

1. Requirements for PKI technologies and applications,
2. How to use PKI technologies non-electronically, and

### 3. Recommendations for PKI physical application.

## 1.3 Cryptosystem

### 1.3.1 Secret Key Cryptosystem

Secret key cryptosystem, also known as Single key cryptosystem, is a conventional encryption technology. Users are required to use the same secret key and algorithm for encryption/decryption. DES, triple-DES, AES, Blowfish, and RC5 are well-known secret key cryptosystems. Secret key cryptosystem's encryption/decryption process is shown as Fig. 1.

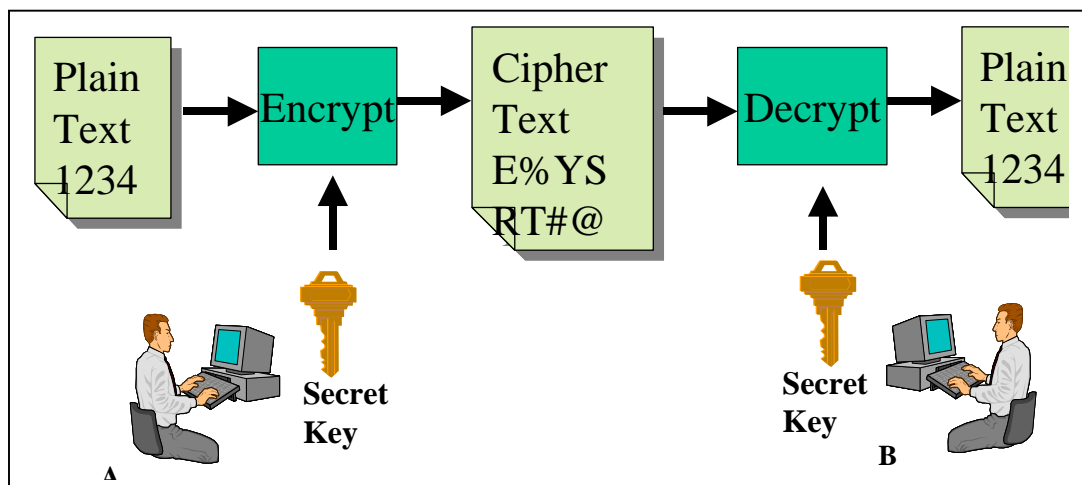


Fig. 1 Secret key cryptosystem

Secret key cryptosystem's features are explained as follows together with its advantages and disadvantages:

1. Features: use the same key for encryption and decryption. Users A and B obtain secret key in advance. Or users A and B use their common secret to develop a secret key via secret key algorithm. Alternatively, either A or B may create a secret key and deliver the key to the other party through secure channel for decryption. It is, however, difficult to establish a secure channel on Internet. Also, both parties have to keep

the secret key securely. Therefore, all parties have to discuss how to create secret key and how to exchange secret key securely before multiple parties communicate with one another. Apparently, secret key administration is not an easy task.

2. Advantage: as compared to public key cryptosystem, secret key allows users to encrypt and decrypt data swiftly, thereby facilitating the encryption/decryption process.
3. Disadvantages include:
  - (1) Secret key has to be shared among various parties and is, therefore, insecure.
  - (2) The distribution process of secret key is somewhat complicated.
  - (3) The number of secret key increases as the number of parties engaged in communication increases, which makes administration a difficult task.
  - (4) Non-repudiation is unreachable for both parties involved in communication.

### **1.3.2 Public Key Cryptosystem [14]**

Public key cryptosystem is also known as public-key encryption. Diffie and Hellman presented the concept of public key cryptosystem in 1976. However, they didn't implement any public key cryptosystem. Then, Ron Rivest, Adi Shamir, and Len Adleman disclosed the public key cryptosystem in 1978, which was known as RSA Public-Key Encryption Algorithm. In RSA Algorithm, encryption and decryption keys are paired. In other words, a pair of key includes a public key and a private key. RSA Public-Key Encryption Algorithm is described as follows:

Take plain text  $M$  and encrypted text  $C$  for example, encryption and

decryption process is shown as follows:

$$C = M^e \text{ mod } n$$

$$M = C^d \text{ mod } n = (M^e)^d \text{ mod } n = M^{ed} \text{ mod } n$$

Where  $\{e, n\}$  denotes public key and  $\{d, n\}$  denotes private key

The equation has to be consistent with public key algorithm and satisfy following requirements:

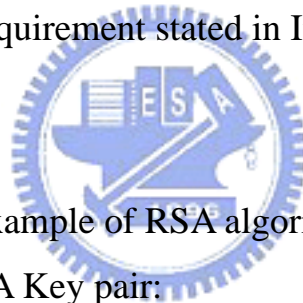
1. Suitable  $e, d,$  and  $n$  are selected. For all  $M < n$ ,

$$M^{ed} = M \text{ mod } n \text{ is essential.}$$

2. For all  $M < n$ ,  $M^e$  and  $C$  can be found out easily.

3. If  $e$  and  $n$  are known,  $d$  has to remain unknown.

4. To satisfy the requirement stated in Item 3,  $e$  and  $n$  have to be extremely large.



Following is an example of RSA algorithm:

1. Creation of RSA Key pair:

(1) Determine the values for prime numbers  $P$  and  $Q$ . For example,  $P =$

$$7, Q = 17$$

(2) Let modulus  $n = P * Q$ ,

$$\text{where } n = 7 * 17 = 119$$

(3) Let  $\phi(n) = (P - 1) * (Q - 1)$ , where  $\phi(1)(n) = 96$

(4) select a any number  $e < \phi(n)$ , wherein  $e$  and  $\phi(n)$  are prime numbers to each other; for example: let  $e = 5$

(5) select a any number  $d$  and  $d = e^{-1} \text{ mod } \phi(n)$  that satisfies

$$d * e = 1 \text{ mod } \phi(n), \text{ and then find out } d = 77$$

(6) Then, the public key  $\{e, n\} = \{5, 119\}$ ,

and the private key  $\{d, n\} = \{77, 119\}$

If  $p$  and  $q$  are unknown, it is hardly to estimate  $d$  based upon  $e$ . Therefore,  $e$  is public, and  $d$  is private.

2. Encryption/decryption algorithm: let  $M$  ( $M= 19$ ) be a plain text and  $C$  denotes an RSA-encrypted text. RSA encryption/decryption process is shown as follows:

$$\text{Encryption: } C = M^e \bmod n \rightarrow C = 19^5 \bmod 119 = 66$$

$$\text{Decryption: } M = C^d \bmod n \rightarrow M = 66^{77} \bmod 119 = 19$$

3. RSA Algorithm's encryption process allows users to encrypt and decrypt texts into plain text. With RSA Algorithm's digital signature process, users can decrypt and encrypt into plain text. Apparently, RSA Algorithm is interchangeable.

4. RSA Algorithm's digital signature:

$$\text{Digital signature: } S = M^d \bmod n \rightarrow S = 19^{77} \bmod 119 = 66$$

$$\text{Verification signature: } M' = S^e \bmod n \rightarrow M' = 66^5 \bmod 119 = 19 = M$$

5. Selection of the number  $e$ : the Public Key Cryptographic Standard (PKCS #1) presented by RSA Security Lab suggests that  $e$  is 3 or  $65537(2^{16} + 1)$ , wherein  $e = 3$  was found insecure. Therefore, for the popular PKI application,  $e = 65537$ .

6. Dissolving  $n$  factor is the most difficult part of RSA. If  $n$  is large enough, it takes a long time to dissolve  $n$  factor. If  $n$  is long enough, RSA Algorithm is incapable of dissolving factors.

Public key cryptosystem process is shown as Fig. 2.

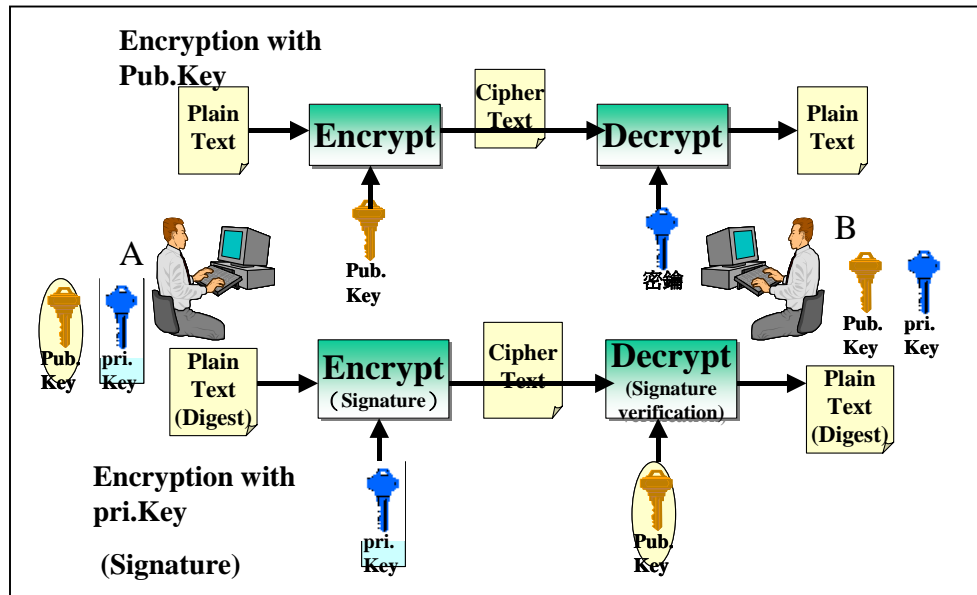


Fig. 2 Public key cryptosystem

Public key cryptosystem is known for the following features:

1. Each key pair comprises with a public key and a private key. Any two different key pairs do not use the same public key or private key.
2. The private key decrypts the data encrypted by the corresponding public key. The public key decrypts the data encrypted by the corresponding private key.
3. Public key corresponds to private key mathematically. However, the creation process of key pair is irreversible. In other words, it is unlikely to find out the corresponding private key based upon the public key due to the complicated mathematic relationship.
4. A public key and a private key make up a key pair. Public key can verify the data encrypted by the corresponding private key.
5. Digital signature is non-repudiation.

Advantages of public key cryptography system:



1. The security of RSA Algorithm is determined according to the level of difficulty associated with prime number dissolution. It is extremely difficult to dissolve  $n$  factors into  $P$ , to be multiplied by  $Q$ .
2. Key distribution and administration can be simplified.
3. Non-repudiation for Digital signature.

Disadvantages of public key cryptography system: the public key cryptography system's encryption/decryption algorithm is complicated and time-consuming.

Public key cryptographic system requires different keys for encryption and decryption via the public key cryptographic algorithm and Public key and private key are paired when they are created. In the public key cryptography system, "public key" encrypts the data and "private key" decrypts the encrypted data. If "private key" produces the digital signature, the "public key" is required to verify the digital signature. For securing the public key cryptographic system, the public key with adequate length are required and the private key has to be kept securely.

### **1.3.3 One-way Hash function [14]**

One-way hash function is also known as hash function. Hash function produces "fingerprint" for the files, messages or other types of data. Following characteristics are required for a perfect hash function  $H$ .

1.  $H$  is capable of processing the data of whatever length.
2. The results outputted by  $H$  algorithm contain data of fixed length.
3.  $H(x)$  can be processed easily, regardless whatever  $x$  is.

4. Regardless whatever  $h$  is, it is difficult to find out  $x$ , which makes  $H(x) = h$ .
5. Regardless whatever  $x$  is, it is difficult to find out  $y$ , which makes  $y \neq x$  and  $H(y) = H(x)$ .
6. It is difficult to find out an  $(x, y)$ , which makes  $H(y) = H(x)$ .

Hash function is primarily designed for message authentication and one-way irreversible algorithm. Only when the foregoing 6 requirements are satisfied, hash function is protected from attacks

As far as PKI application technique is concerned, hash function is recognized as the foundation for digital signature and digital envelopment and is, therefore, extremely important for PKI application. MD5 and SHA-1 Algorithm are hash functions. Ron Rivest developed MD5 (RFC 1321) that accommodates the inputted message of all lengths and outputs the authenticated message of 128 bits. This process is known as digest. However, a hash function comprising 128 bits is questionable in consideration of the fast CPU speed. Safety Hash Algorithm (SHA) was developed by NIST and was listed as FIPS 180 specification in 1993, and then revised to FIPS PUB 180-1 in 1995, also known as SHA-1. SHA-1 accommodates digest with 160-bit length converted from message less than  $2^{64}$ -bits, which is the most common hash function used for X509 certificates. The process of Hash function is shown as Fig. 3.

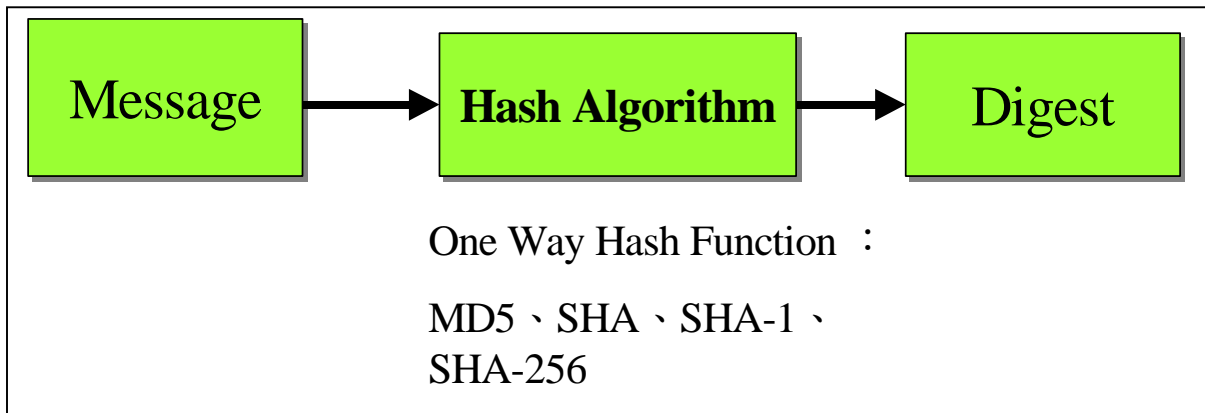


Fig. 3 The process of Hash function

## 1.4 Framework of thesis

This thesis is divided into six chapters. Chapter 1 contains general description and outlines of the thesis. Chapter 2 describes the techniques used in PKI application and 2D bar code. Chapter 3 relates to the analysis and description of PKI physical application regarding requirements and related issues. Chapter 4 contains the proposed PKI physical techniques and system framework. Chapter 5 relates to the experimental results. Chapter 6 contains conclusions together with recommendation for future research.

# Chapter 2

## Background Research

### 2.1 Public Key Infrastructure

Public Key Infrastructure (PKI) is developed along with asymmetric cryptography as foundation. Thus, a framework regarding the security of information services was created. The framework of PKI places emphasis on the security of asymmetric key and concentrates on how to ensure the accuracy of key distributions via digital certificates and key management policy. With the repository, PKI allows users to acquire public key certificates effortlessly, and thus verify the accuracy and hierarchical relationship of public key through verification process. With these features, PKI techniques are perfectly suitable for the applications of Internet. As the security of networks and information systems becomes more and more important, PKI grows more popular than ever. Both government and private sectors are progressively developing PKI mechanism and application framework so as to enhance security for their network environment.

The technical specifications and standards of PKI are becoming increasingly important at the time that PKI becomes more popular than ever. Technical standards have been developed rapidly in the last few years. International Telecommunications Unions (ITU) presented X.509 standard. The United States' RSA Security Corporation presented Public Key Cryptographic Standards (PKCSs). The PKI and X.509 working group (PKIX) of Internet Engineering Task Force (IETF) has also presented a series of PKI technical standards. These standards contributed to the rapid development of PKI techniques. To cope with Web Service's rapid development, W3C and IETF have progressively updated PKI technical specifications for XML technique, including XKMS, XML Signature,

and XML Encryption technical standards, which serve as the technical framework for the security of Web Service.

This thesis attempts to find the physical requirements for PKI application and, therefore, concentrates on PKI-related technical standards as the core technique. PKI-related technical standards will be described in following sections.

### **2.1.1 Digital Signature**

Digital signature is one kind of electronic signatures. Because the encryption and decryption via Public key cryptosystem are slowly. Messages are condensed into a message digest of fixed length via hash function, instead of encrypting the whole message, in the digital signature production process. Then, the message digest is encrypted via sender's private key. The encrypted message of digest serves as the digital signature for the original message. Recipient verifies the digital signature via the public key provided by the sender. Thus, the message-authentication and e-mails verification technique are developed to verify sender's identity and the integrity of the content.

If more than one party sign on the same document, all parties' digital signatures are different from one another, because their private keys are different. If one party signs on several documents, the message digests generated by hash function are different from one another, because the documents are different. As far as public key encryption technique is concerned, public key is considered public information and is accessible to the general public via digital certificate. Therefore, a third party can verify digital signature easily.

Following are unique features for digital signature's verification mechanism:

- 1.To verify sender's identification.
- 2.Non-repudiation for senders.
- 3.Integrity of plain text.

As a part of the message authentication technique, digital signature is not a data encryption mechanism. As such, the plain text is accessible to the general public and, therefore, encryption technique or digital envelopment technique is required to protect the private data. Digital signature's technical framework is shown as Fig. 4.

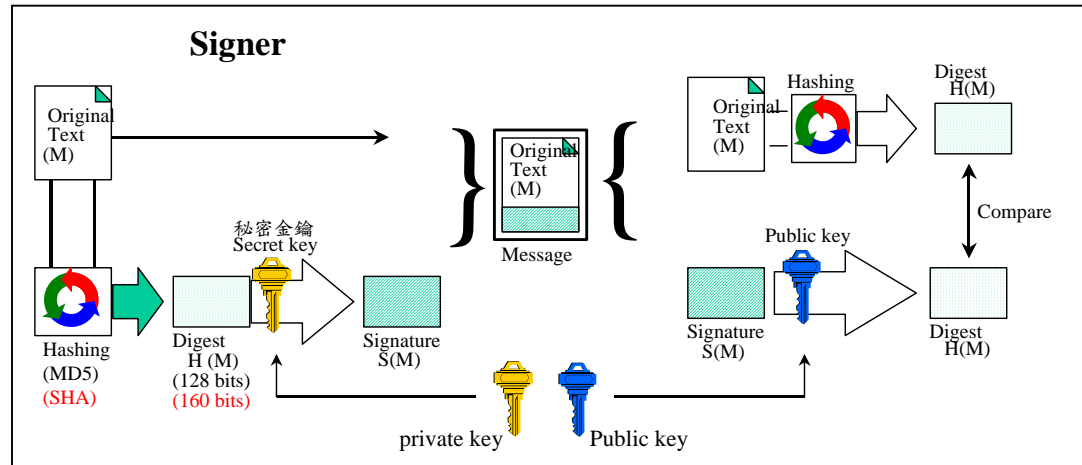


Fig 4 Digital Signature

### 2.1.2 X.509 Certificates

The basic problem with public key cryptography is determining who holds the corresponding private key. To answer this question, a PKI relies upon the concept of a public key certificate, or simply certificate. Each certificate contains a public key and identifies the user with the corresponding private key, which are also known as public key certificate. To cope with digital environment and electronic message processing, a public key certificate is a purely digital object. Therefore, public key certificate is also known as digital certificate. In this thesis, “digital certificate” refers to public key certificate. [1]

To make sure that digital certificate provides the public key and owners' information, the digital certificate has to serve following purposes:

1. It would be a purely digital object, and thus can be used on Internet.

2. It has to contain the information of private key owner and the owner's contact information.
3. It would be easily to determine the time of the certificate issued.
4. It would be issued by a trusted party, not by the private key owner.
5. It would be easily to determine the identity of private key owner, with no confusion at all.
6. It would be easily to determine if the certificate is genuine or forged.
7. It has to be temper-proof from changing data without approval.
8. It has to be determined the proper uses.

The foregoing properties reveal the expected digital certificate structure. Therefore, digital certificate means the public key certificate issued by the certification authority. Digital certificate also contains the information including validity and authority of issuance, the information of public key owner, public key details, and issuer's signature. In addition to the information regarding digital certificate, an open and standard certification process is also needed so as to verify the accuracy and effectiveness of digital certificate, thereby allowing users to trust the public key and to find out who the public key owner is.

According to ITU-T X.509 [2] specification, digital certificate has developed X.509 certificate versions 1 to version 4. Nowadays, the X.509 certificate of version 3 still is the most widely distributed over the Internet.

Following is the basic syntax for X.509 certificate v3: Certificate is encoded in accordance with ASN.1[X.208].

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate ,
    signatureAlgorithm  AlgorithmIdentifier ,
    signatureValue      BIT STRING  }
```

```

TBSCertificate ::= SEQUENCE {
    version          [0] EXPLICIT Version DEFAULT v1 ,
    serialNumber     CertificateSerialNumber ,
    signature        AlgorithmIdentifier ,
    issuer           Name ,
    validity         Validity ,
    subject          Name ,
    subjectPublicKeyInfo SubjectPublicKeyInfo ,
    issuerUniqueID  [1] IMPLICIT UniqueIdentifier OPTIONAL ,
                    -- If present , version shall be v2 or v3
    subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL ,
                    -- If present , version shall be v2 or v3
    extensions      [3] EXPLICIT Extensions OPTIONAL
                    -- If present , version shall be v3
}

```

```

Version ::= INTEGER { v1(0) , v2(1) , v3(2) }

```

```

CertificateSerialNumber ::= INTEGER

```

```

Validity ::= SEQUENCE {
    notBefore      Time ,
    notAfter       Time }

```

```

Time ::= CHOICE {
    utcTime        UTCTime ,
    generalTime    GeneralizedTime }

```

```

UniqueIdentifier ::= BIT STRING

```

```

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm          AlgorithmIdentifier ,
    subjectPublicKey   BIT STRING }

```

```

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

```

```

Extension ::= SEQUENCE {
    extnID            OBJECT IDENTIFIER ,

```



```
critical          BOOLEAN DEFAULT FALSE ,
extnValue        OCTET STRING  }
```

Basic X.509 certificate content:

X.509 standard defines the information and the information format to be contained in the certificate. All fields are described as follows:

- 1.version: X.509 Version of the certificate, which determines the type and format of information contained in certificate.
2. serialNumber: the serial number is an integer number assigned by the certification issuer to each certificate. The serial number must be unique for each certificate generated by a particular issuer. The combination of the issuer name and serial number uniquely identifies any certificate.
3. Signature: the signature field is an algorithm identifier ( the OID of the digital signature algorithm).
4. Issuer: the issuer field contains the X.500 distinguished name of certificate issuer (CA).
5. Validity: the validity field has two components, including the dates on which the certificate becomes valid (notBefore) and the date on which the certificate expires (notAfter).
6. Subject: the subject field contains the distinguished name of public key owner.
7. subjectPublicKeyInfo: th subject public key information field contains the subject's public key and algorithm identifier (such as PKCS #1 = "1.2.840.113549.1.1.4").
8. issuerUniqueID: this is an optional field containing the unique identifier of the issuer (CA). This indicates if an issuer's name has been used repeatedly after a certain period of time. PKIX requires that the name must not be used repeatedly by other agency. This field has to be excluded from the Internet

certificate compatible with PKIX. [3]

9. **subjectUniqueID**: this is an optional field containing the unique identifier of the user that indicates if a user's name has been used repeatedly after a certain period of time. PKIX requires that the name must not be used repeatedly by other agency. This field has to be excluded from the Internet certificate compatible with PKIX. [3]
10. **Extensions**: X.509v3 certificate supports extended fields, including **id\_ce\_keyUsage**, **id\_ce\_basicConstraints**, **id\_ce\_subjectAlternativeName**, and **id\_ce\_certificatePolicies**. [3] Extensions accommodate additional characteristics, such as users or public key data related to communication. X.509v3 permits individual development regarding the additional information for users.
11. **signatureAlgorithm**: indicates the digital signature algorithm in use. (such as MD5WithRSAEncryption="1.2.840.113549.1.1.4")
12. **signatureValue**: the signature value field contains issuer's digital signature of the TBSCertificate. Digital signature is created after all fields of certificate, except signature, are entered. Digital signature's value is signed by the CA's private key.

### **2.1.3 Certificate Revocation List**

Certificate Revocation List (CRL) stores the information of revoked certificates. When a certificate needs to be revoked, the certification authority puts the certificate serial number on a hot list. Then the hot list is called a certificate revocation list (CRL). CRL helps users to find out if the certificate received from other party is valid or not. CRLv2 is the most recent version of CRL and is defined under X.509. [2]

## 1.CRLv2 ASN.1 grammar:

```
CertificateList ::= SEQUENCE {
  tbsCertList TBSCertList,
  signatureAlgorithm AlgorithmIdentifier,
  signatureValue BIT STRING
}
TBSCertList ::= SEQUENCE {
  version Version OPTIONAL,
  -- if present, shall be v2
  signature AlgorithmIdentifier,
  issuer Name,
  thisUpdate Time,
  nextUpdate Time OPTIONAL,
  revokedCertificates SEQUENCE OF SEQUENCE {
  userCertificate CertificateSerialNumber,
  revocationDate Time,
  Extensions OPTIONAL
  -- if present, shall be v2
  } OPTIONAL,
  crlExtensions [0] EXPLICIT Extensions OPTIONAL
  -- if present, shall be v2
}
```

## 2.Basic CRLv2 Contents

- (1) Version: The optional version field describes the syntax of the CRL.  
X509v2 CRL is the most recent version.
- (2) Signature: Object Identifier of the digital signature algorithm is in use,  
sha1WithRSAEncryption (1.3.14.3.2.29) of ISO standard containing 11

bytes – 0x30 0x09 0x06 0x05 0x2b 0x0e 0x03 0x02 0x1d 0x05 0x00 – is in use now.

- (3) Issuer: the X.500 distinguished name of CRL issuer.
- (4) thisUpdate: the this-update field indicates the issue date of this CRL will be issued. For example, 980909063324Z stands for September 9, 1998, 06:33:24
- (5) nextUpdate: the next update field indicates the issue date of next CRL will be issued.
- (6) revokedCertificates: the revoked certificates field contains the certificate serial number, revocation date, and extension data fields of the revoked certificates.
- (7) crlExtensions: extension fields of this CRL.
- (8) signatureAlgorithm: signature algorithm identifier of the digital signature algorithm.
- (9) signature value: digital signature value, CA's digital signature in relation to TBSCertList and consistent with PKCS #1 standard. [3]

CRL contains the data related to the revoked certificate together with CA's signature, and thus allows users to find out if the certificate is valid or not. CA produces CRL and place CRL in repository, to be downloaded by users, or in the LDAP Server defined by X.500, to be retrieved by those who need CRL.

### **2.1.4 Overview of public key infrastructure**

Public Key Infrastructure (PKI) is designed to issue, distribute, and administer the digital certificates. In other words, PKI makes use of public key cryptography to enhance privacy, consistency, identification verification, and non-repudiation via the issuance and administration mechanism of digital certificate, thereby

ensuring security for users and maintaining information security for commercial activities and communication.

PKI is a comprehensive structure, not just a technique or standard, and is made up of various techniques and service providers. According to RFC 2459 PKI recommended specification [3], PKI structure comprises clients (or end entity), certification authority (CA), registration authority (RA), and repository.

1. Clients (or end entity, EE): EE stands for certificate user or application system. Users administer their private keys and request public key certificates from certificate authority, and then distribute public key to other users via public key certificate or download other users' certificates or CRL data via CA's repository.
2. Certification authority (CA): CA is the core part of PKI. CA issues and revokes certificates. Once verified by RA, legitimate users receive public key certificate signed by the CA and the public key certificate is stored in repository. If users miss their private key or they intend to suspend their certificates, they have to notify CA. Then, CA revokes certificates accordingly and includes the revoked certificates in blacklist upon users' request, and announces the CRL periodically.
3. Registration authority (RA): RA records and verifies users' identification. RA safeguards CA. RA verifies and records users' identifications according to the certification policy initiated by CA. Users transmit certificate request to CA via RA, and then acquire public key certificates issued by CA.
4. Repository: repository stores and provides information regarding public key certificates and CRL. Normally, repository supports HTTP or LDAP communication protocols, thereby allowing users to find out certificate information or updated CRL data swiftly.

## 2.1.5 PKI application message standards and specifications

The Public Key Cryptographic Standards (PKCS) announced by RSA Security and XML Security standards of the W3C are major standards for PKI applications. Presently, XML Signature and XML Encryption are considered W3C recommended standards and are described as follows:

1. PKCS [4]: PKCS stands for Public Key Cryptography Standards announced by RSA Security Laboratories. In short, PKCS defines various message exchange specifications and message structures related to public key cryptosystem. PKCS series standards contain 10 PKCS message standards, including PKCS#1 RSA Encryption Standard, PKCS#3 Diffie-Hellman Key Agreement Standard, PKCS # 5 Password-Based Cryptography Standard, PKCS#6 Extended-Certificate Syntax Standard, PKCS#7 Cryptographic Message Syntax Standard, PKCS#8 Private-Key Information Syntax Standard, PKCS#9 Selected Attribute Types, PKCS#10 Certification Request Syntax Standard, PKCS#11 Cryptographic Token Interface Standard, PKCS#12 Personal Information Exchange Syntax, PKCS#13 Elliptic Curve Cryptography Standard, and PKCS#15 Cryptographic Token Information Format Standard. PKCS message standards comprise key storage format, encrypted message format, certificate format, encryption and signature message specification, secure key storage format, certificate request form, token specification, etc. In other words, specification is defined precisely for the critical messages of PKI system and serves as the critical standard for PKI industry. This thesis concentrates on PKI physical application and, therefore, PKCS#1 and PKCS#7 standards are among the foremost concerns for author. PKCS#1 and PKCS#7 are described as follows:

(1) PKCS #1 RSA Encryption Standard [5]

PKCS #1 is the encryption standard of RSA.

Shown in ASN.1:

```
RSAPublicKey ::= SEQUENCE {
    modulus INTEGER, -- n
    publicExponent INTEGER -- e
}
RSAPrivateKey ::= SEQUENCE {
    Version Version,
    modulus INTEGER, -- n
    publicExponent INTEGER, -- e
    privateExponent INTEGER, -- d
    prime1 INTEGER, -- p
    prime2 INTEGER, -- q
    exponent1 INTEGER, -- d mod (p-1)
    exponent2 INTEGER, -- d mod (q-1)
    coefficient INTEGER -- (inverse of q) mod p
}
Version ::= INTEGER
```

Except Version, n, e, and d, no other data exists in the physical products created by private key. Other data is kept for the purpose of accelerating decryption and signature process. Whether the physical products support the accelerated algorithm, however, is not listed in the standard as a criterion.

(2) PKCS #7 Cryptographic Message Syntax Standard [6]

PKCS#7 defines the level of confidentiality for documents, and

comprises 6 levels of confidentiality, to wit:

- Data
- Signed data
- Enveloped data
- Signed and enveloped data
- Digested data
- Encrypted data

In PKCS#7 standard, the data are expressed via ASN.1 syntax, shown as follows:

```
ContentInfo ::= SEQUENCE {  
    contentType ContentType,  
    content  
        [0] EXPLICIT ANY DEFINED BY contentType  
        OPTIONAL }
```

```
ContentType ::= OBJECT IDENTIFIER
```

ContentType indicates the type of content and is denoted as OID. ContentType is defined under the standard, and includes data, signed Data, enveloped Data, signed and enveloped Data, digested Data, and encrypted Data.

Content: the content of document, and one of 6 types of documents as stated in ContentType.

In PKCS#7, the syntax is recursive as shown by Fig. 5.



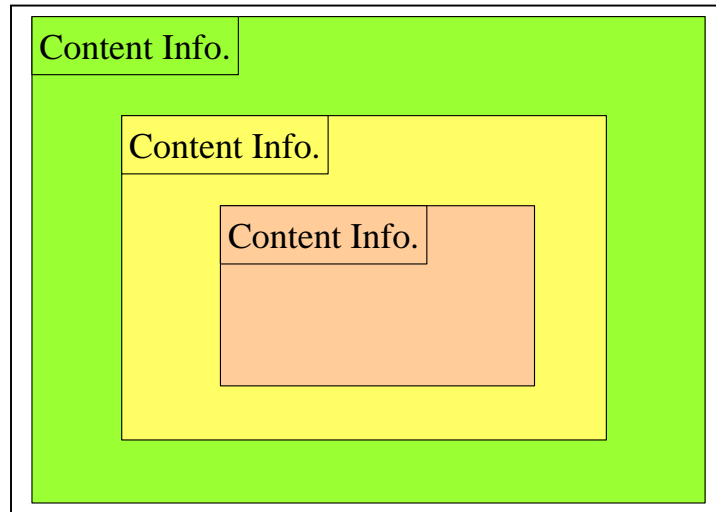


Fig. 5 Recursive structure of PKCS#7

As stated in previous chapters, PKCS#7 defines the level of confidentiality for documents. The level of confidentiality is determined according to OID (Object Identifier) of ContentType. 6 levels of confidentiality are described as follows:

Data	OBJECT IDENTIFIER ::= { pkcs-71 }
SignedData	OBJECT IDENTIFIER ::= { pkcs-72 }
EnvelopedData	OBJECT IDENTIFIER ::= { pkcs-73 }
SignedAndEnvelopedData	OBJECT IDENTIFIER ::= { pkcs-74 }
DigestedData	OBJECT IDENTIFIER ::= { pkcs-75 }
EncryptedData	OBJECT IDENTIFIER ::= { pkcs-76 }

All documents' syntax are defined as follows:

(1) Data

Data ::= OCTET STRING

(2) Signed Data

SignedData ::= SEQUENCE {  
 version Version,  
 digestAlgorithms DigestAlgorithmIdentifiers,

contentInfo ContentInfo,  
 certificates  
     [0] IMPLICIT ExtendedCertificatesAndCertificates  
         OPTIONAL,  
 crls  
     [1] IMPLICIT CertificateRevocationLists OPTIONAL,  
 signerInfos SignerInfos }  
 DigestAlgorithmIdentifiers ::=  
     SET OF DigestAlgorithmIdentifier  
 SignerInfos ::= SET OF SignerInfo

(3) Enveloped Data

EnvelopdData ::= SEQUENCE {  
     version Version,  
     recipientInfos RecipientInfos,  
     encryptedContentInfo EncryptedContentInfo }

RecipientInfos ::= SET OF RecipientInfo

EncryptedContentInfo ::= SEQUENCE {  
     contentType ContentType,  
     contentEncryptionAlgorithm  
         ContentEncryptionAlgorithmIdentifier,  
     encryptedContent  
         [0] IMPLICIT EncryptedContent OPTIONAL }

EncryptedContent ::= OCTET STRING

(4) Signed and enveloped data

```

SignedAndEnvelopdData ::= SEQUENCE {
    version Version,
    recipientInfos RecipientInfos,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encryptedContentInfo EncryptedContentInfo,
    certificates
        [0] IMPLICIT ExtendedCertificatesAndCertificates
OPTIONAL,
    crls
        [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos }

```

(5) Digested data

```

DigestedData ::= SEQUENCE {
    version Version,
    digestAlgorithm DigestAlgorithmIdentifier,
    contentInfo ContentInfo,
    digest Digest }

```

Digest ::= OCTET STRING

(6) Encrypted data

```

EncryptedData ::= SEQUENCE {
    version Version,
    encryptedContentInfo EncryptedContentInfo }

```

## **2.Web Service Security [10][11]**

Ever since W3C announced XML 1.0 in 1998, computer industry has been changed dramatically. XML was developed from SGML and HTML, and was designed to facilitate reading and, at the same time, to allow computer programs to identify language format and grammars. XML has changed the thinking structure, description, and information exchange process. With its rapid growth, XML is an irreversible trend for computer technology.

The e-commerce techniques in the early days, such as EDI, web EDI, content Server, application Server, EAI (Enterprise Application Integration), and the solutions designed for portal web site and individual e-commerce application, cannot catch up with the rapid development of e-commerce. Therefore, an XML-based Web service was developed to provide e-commerce solutions under a brand new technical structure. Web services envelope messages, behaviors, data, and commerce process uniformly for all systems and equipment. Web services allow enterprises to integrate e-commerce in a manner that was considered impossible before. As such, the core competence can be shared among various enterprises regarding inter-enterprise e-commerce, and thus a commercial Web was created.

Shortly after Web Service was created, the security requirement of Web Service was discussed extensively. Therefore, W3C developed WA-Security standard to serve as a protection mechanism for Web Service. WA-Security enhances the protection for SOAP via the integrity and confidentiality of messages together with message verification. Web Services Security specification (WS-Security) serves as a security mechanism to facilitate SOAP message exchange for Web Service developers. WS-Security stresses the enforcement of SOAP message transmission, thereby creating various

protection levels for SOAP message applications with emphasis on integrity, confidentiality, and verification of messages. The basic mechanisms can be connected through various methods for the security models that incorporate various encryption techniques. Also, WS-Security provides a universal mechanism that connects security certificate to messages. To accommodate extension (such as supporting multi-security certificate) in connection with certification and authorization mechanisms, WS-Security falls behind the requirements for the format of security certificate. For example, requestors are likely to provide identification document and signature announcement, such as business certification, that allows Web Service to determine the level of trust for the announcement. Also, WS-Security describes how to edit decimal security certificates and how to add the edited decimal security certificates to SOAP messages. WS-Security incorporates extension mechanism to describe the certificate information contained in the messages.


In WS Security standards, the integrity of messages is assured with XML Signature and digital certificate and makes sure certain that the messages are transmitted from the desirable sender and the messages have not been changed in the transmission process. Similarly, XML Encryption and security certificate assure that the full SOAP messages are processed confidentially.

XML Signature is a digital signature standard developed by W3C in cooperation with IETF, and has become an official standard recommended by W3C. XML signature has defined a <signature> element including all information needed by digital signature. XML signature sample [8] is shown as follows:

(? Denotes none or only one; + denotes at least one; \*denotes none or several)

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
      (<Transforms>)?
      <DigestMethod>
      <DigestValue>
    </Reference>)+
  </SignedInfo>
  <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
</Signature>
```

Following is a simple XML signature sample [8]:



```
[s01] <Signature Id="MyFirstSignature"
xmlns="http://www.w3.org/2000/09/xmldsig#">
  [s02]   <SignedInfo>
  [s03]   <CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
  [s04]   <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
  [s05]   <Reference
URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
  [s06]     <Transforms>
  [s07]     <Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

[s08] </Transforms>  
[s09] <DigestMethod  
Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>  
[s10]  
<DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>  
[s11] </Reference>  
[s12] </SignedInfo>  
[s13] <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>  
[s14] <KeyInfo>  
[s15a] <KeyValue>  
[s15b] <DSAKeyValue>  
[s15c] <P>...</P><Q>...</Q><G>...</G><Y>...</Y>  
[s15d] </DSAKeyValue>  
[s15e] </KeyValue>  
[s16] </KeyInfo>  
[s17] </Signature>



## 2.2 Two dimensional Barcode

### 2.2.1 About Two Dimensional Barcode [15]

Two dimensional barcode (2D Bar Code) stores up to 1,000 bytes, or 500 Chinese words, which are different from one dimensional barcode (1D Bar Code) storing up to 28 bytes. In addition, 2D Bar Code allows users to store list and tables, texts, images, and condensed data in bar codes, thereby allowing recipients to enter data into computers automatically via scanners. 2D Bar Code is highly resistible to diskettes and, therefore, users need not worry about virus, damages, and insufficient capacity.



Fig. 6 1D Bar Code versus 2D Bar Code [15]

### 2.2.2 Types of 2D Bar Code [18]

Based upon graphics combination/structure, 2D Bar Code is divided into two categories, including stacked bar code comprising the overlapped or multiple bar codes made up of digit strings. CODE 49, CODE 16K, Codeblock, Supercode, Softstrip, and PDF417 are well-known 2D Bar Codes. Stacked bar code was developed from 1D bar code and is, therefore, incapable of correcting errors. PDF417 is the only stacked bar code capable of correcting errors. The other bar code is made up of matrix code and dot code. Digits are edited in 2D format and are, therefore, known as matrix bar code. Matrix bar code allows users to read data



from all angles. Therefore, scanners can be erected in a wide range of positions. Maxicode, Minicode, Philips Dot Code, and Vericode are well-known matrix bar codes.

Stacked bar code edits data into 1D bar code with narrowed height. 1D bar codes are stacked into several rows to facilitate code design, inspection, and identification. However, stacked bar code differs from 1D bar code with respect to the number of rows, verification, decoding algorithm, and software [17].

Matrix bar code uses dot to denote “1” and nullity to denote “0” as in binary system. The combination of dots determines the significance of matrix. The dots can be square, round, or any other shape. Matrix incorporates computer graphics-processing technique together with combined editing method for automatic identification of symbols, and is, therefore, no longer a mere “bar code”. [17]



### **2.2.3 Features of 2D Bar Code [17][18]**

Following are the features of 2D Bar Code:

1. Huge storage capacity:

2D Bar Code stores up to 1000 – 2000 words, much more than 1D Bar Code (such as EAN8, EAN13, UPC8...) does.

2. Highly resistible to damages:

2D Bar Code incorporates error-correcting code that is capable of reading the data contained in the damaged bar code and maintaining information in sound conditions through photocopy and facsimile.

3. Traceability (portability):

2D Bar Code allows all data to be stored in barcodes, which means data is portable and easy to trace.


#### 4. Security:

Cryptography can be added to the editing process and decoding process. Therefore, 2D Bar Code is known as “secure barcode”.

#### 5. Increasing popularity of reading devices:

With the joint efforts of government and private sector, 2D Bar Code is becoming more and more popular, especially in the logistics and express delivery service industry. The Ministry of Finance has applied 2D Bar Code to tax filing procedure in recent years, and has thus accelerated the filing process. With the increasing popularity of 2D Bar Code, the prices of reading-devices have been reduced significantly. Most bar code-reading devices support 2D Bar Code regarding verification and reading, thereby simplifying the requirements for application.

### **2.2.4 PDF417 Barcode [18]**



United States' Symbol Technologies, Inc. invented PDF417 in 1989. Dr. Yin-jin Wang was the inventor. PDF stands for Portable Data File. 417 means that each code word is made up of 17 modules and each code word contains 4 black bars relevant to multiple width codes. Symbol Technologies Inc. was the designer of PDF 417. The overlapped code contains row-end identification symbol and scanning software to acquire digits from other portions of labels. Complete digits are entered right after all rows are scanned. The digits are highly reliable. Even if 50% of labels are damaged, all digits are still readable.

PDF 417 is a portable digital document with high density and high message capacity and is, therefore, a highly reliable saving tool with maximum capacity and can be read by machine. PDF 417 bar code is known for following features:

1. Large capacity of messages: each square inch stores up to 250 – 1,100

words. PDF 417 bar code stores 1,848 alphabets or 2,729 numerical symbols, approximately 500 Chinese words, in an area recognized by international standard (same as 2/3 size of postcard, approximately 76mm\*25mm), which is ten times more than the capacity of regular bar code.

2. Extensive application for editing: PDF 417 allows users to edit all digitalized messages, including photos, fingerprints, palm prints, signature, voice, and texts.
3. Confidentiality and anti-counterfeit performance: PDF 417 is provided with multiple anti-counterfeit features, such as cryptography, software encryption. PDF 417 permits anti-counterfeit treatment via the messages contained in the bar code, such as fingerprints and photos. Therefore, PDF 417 is a perfect tool to enhance confidentiality and anti-counterfeit.
4. Highly reliable for decoding: the average decoding error is approximately 2 millionth for regular bar codes. In the case of PDF 417, however, the decoding error is less than 1 ten millionth. Apparently, decoding results are reliable.
5. Highly capable of correcting errors: PDF 417 incorporates the most advanced error-correcting mechanism. If the damaged area is less than 50% of total area, the messages contained in the damaged bar codes still can be recovered.
6. Easy production and low cost: PDF 417 2D bar codes can be easily printed on papers, cards, PVC, even metal via the matrix, LaserJet, ink, heat-sensor/heat-printing, and card-production devices. In other words, ink is the only additional cost for users. Therefore, PDF 417 is also known as “zero-cost” technique.
7. Adjustable shape of bar code: PDF 417 bar codes allow self-adjustment in

accordance with the surface of carriers.



# Chapter 3

## Requirements and Issues Related to PKI Physical Application

### 3.1 PKI implementation and application in Taiwan

PKI is known for the unique features of integrity, confidentiality, authentication, and non-repudiation. With these features, PKI is specifically suitable for the virtual world created by Internet. PKI helps the digital objects of virtual world to be converted into physical objects of the real world. PKI enhances security for various applications on Internet, and thus enhances users' confidence in e-commerce. More and more countries have passed laws regarding electronic signatures. The digital signature of PKI mechanism is now under the protection of laws.

PKI develops rapidly in Taiwan. PKI structure is shown as Fig. 7:

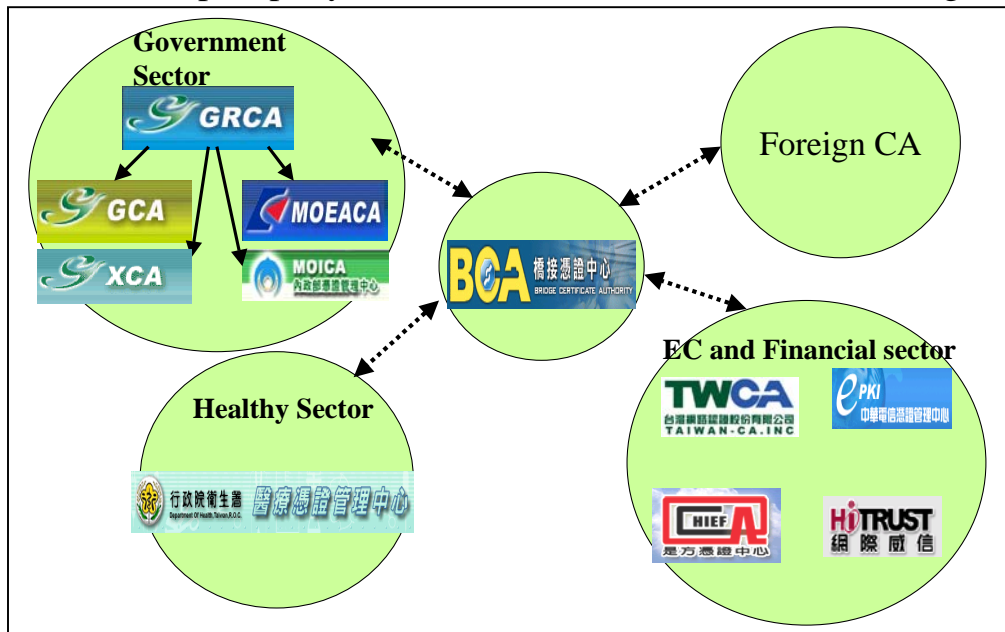


Fig. 7 Framework of PKI in Taiwan

The government has inaugurated GPKI plan [20]. The Research, Development, and Evaluation Commission, Executive Yuan, has established the Government Root Certification Authority (GRCA) and all government agencies have established certification authorities affiliated to GRCA, including Government Certification Authority (GCA), Certification Authority of MOEA (MOEA CA), Certification Authority of MOI (MOICA), and Mixed Organization Certification Authority (XCA) as shown by Fig. 8. GPKI oversees government's certification services, certificate issuance, Server software certificate issuance and administration [21]. MOICA issues IC Cards for ROC citizens over 18 years old and public key certificates [23]. MOEACA supervises certificates issued by enterprises [22]. XCA oversees the certificates issued by schools (incl. public & private schools), for-profit entities, not-for-profit entities, administration agencies, professional firms, and other entities [24]. Thus, GPKI has implemented a secure structure for e-government to provide online services to the general public, including e-document, online vehicle registration, online income tax filing, e-taxation, online land administration services, online corporate filing, online labor & farmer insurance services, online household registration services, etc. – a wide range of G2G, G2B, and G2C services.

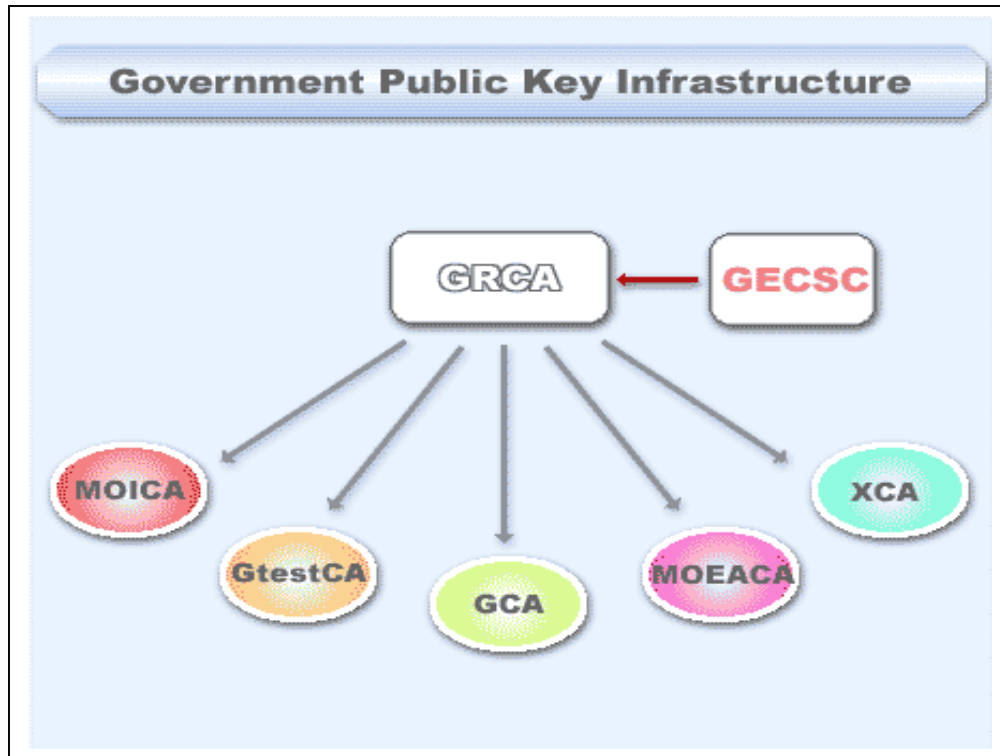


Fig. 8 Framework of PKI in Government sector

Financial sector, medical sector, and e-commerce sector have established PKI structures, including Secure Electronic Transaction (SET) certification Authority, TAIWAN Financial Certification Authority, Non-SET Business Certification Authority, EC Certification Authority, Financial XML Certification Authority, Hitrust Certification Authority, Chief Certification Authority, Chunghwa Telecom Certification Authority, and the Certification Authority under the Department of Health, Executive Yuan. [25] Private sector's PKI implementation has successfully triggered electronic application and e-commerce, such as network banking, network securities trading, online procurement, online shareholders' meeting, etc. The certification institutions approved by the Ministry of Economic Affairs are shown as Fig. 9.



Fig. 9 Certification authorities approved by Ministry of Economic Affairs

### 3.2 Demands for e-document

Traditionally, government agencies process official business via paper documents. Paper documents are prepared, reviewed, and approved. Thanks to the popularity of network, government agencies have computerized document flow via PC and network system, thereby upgrading the efficiency of document administration. In 1999, Executive Yuan established a task force to study document e-exchange plan. The Research, Development, and Evaluation Commission, Executive Yuan, completed the outsourcing service plan regarding document e-exchange for government agencies and school in 2001. Since then, all government agencies and schools started exchanging documents electronically. With the success of e-document exchange plan, Executive Yuan is now developing G2B and G2C based upon its successful experience of G2G so as to upgrade the efficiency for government, which is considered the major task for “e-government plan”.

E-document plan has successfully integrated information and communication



technologies, and has thus accomplished the goals of document computerization and process automation. Government agencies exchange e-documents via Internet and GPKI ensures the security of e-documents. GCA Server software certificates assure the security of documents transmitted via SSL Security Path. GCA signs the outgoing documents digitally. Recipients verify the incoming documents by the sender's GCA public key certificate, print out the documents, and then reply to senders. E-document's exchange structure is shown as Fig. 10.

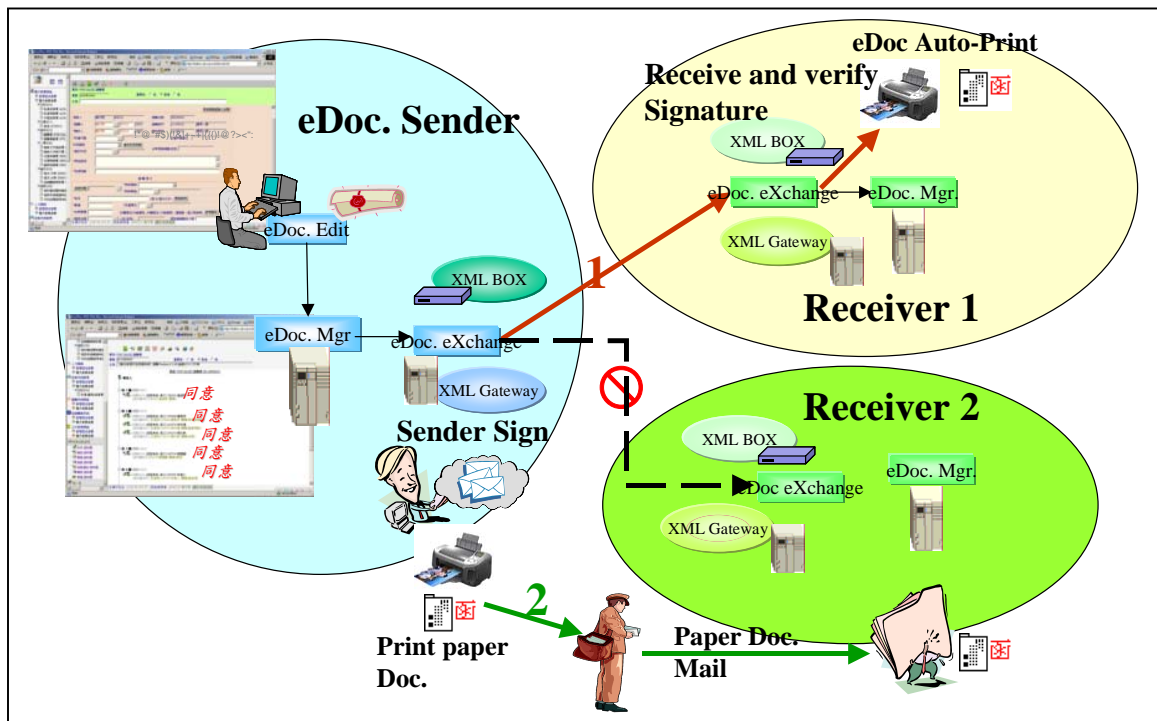


Fig. 10 G2G e-document exchange

Currently, senders are required to check if recipients accept e-documents before e-documents are transmitted. If recipients can accept e-documents, senders sign the documents by the technique of digital signature, and then transmit e-documents to the recipients. In Fig. 10, red arrow signs denote outgoing process 1. Upon receiving e-documents, recipients verify the digital signature shown on e-documents by sender's public key certificate. If the result of verification is true,

the document is printed out automatically and confirmation is delivered to sender. Then, the message is included into document management process. If senders find out that the recipients cannot accept online e-documents, paper documents are forwarded instead, as shown by green arrow signs 2 of Fig. 10.

According to the current e-document exchange specifications, recipients must print out the e-documents before send confirmations to senders. As we know, after the recipients verify the e-documents and print out the documents as papers, digital signatures of e-documents could not be printed correctly. Therefore, e-documents and digital signature are not kept at the same time and the digital signature is likely to be missing. Also, the printed documents do not bear the physical chop or digital signature imprinted by senders. Apparently, the validity of paper documents is questionable. A number of government agencies imprint watermarks on paper documents to replace the digital signature of sender. However, sender's digital signature is still missing and, as a result, the integrity and non-repudiation become questionable. Therefore, the foremost concern is whether PKI digital signature can be kept and imprinted on paper documents.

### **3.3 Demands for e-uniform invoice**

Uniform invoice is a unique feature of Taiwan's taxation system. Uniform invoice serves as a solid evidence for internal revenue service. However, using uniform invoice means costs and financial burden for businesses, such as paper costs, delivery, certified mail costs or personal delivery, warehouse administration and recordation, and manpower associated with issuing uniform invoice. With the popularity of Internet application, uniform invoice is possibly to be forwarded electronically, instead of postal delivery.

If uniform invoice is delivered via Internet, security is the foremost concern

and, in this connection, security control measures are essential and PKI is naturally the top choice so as to enhance the integrity, confidentiality, data source identification, and non-repudiation of e-uniform invoice. E-uniform invoice structure is shown as Fig. 11.

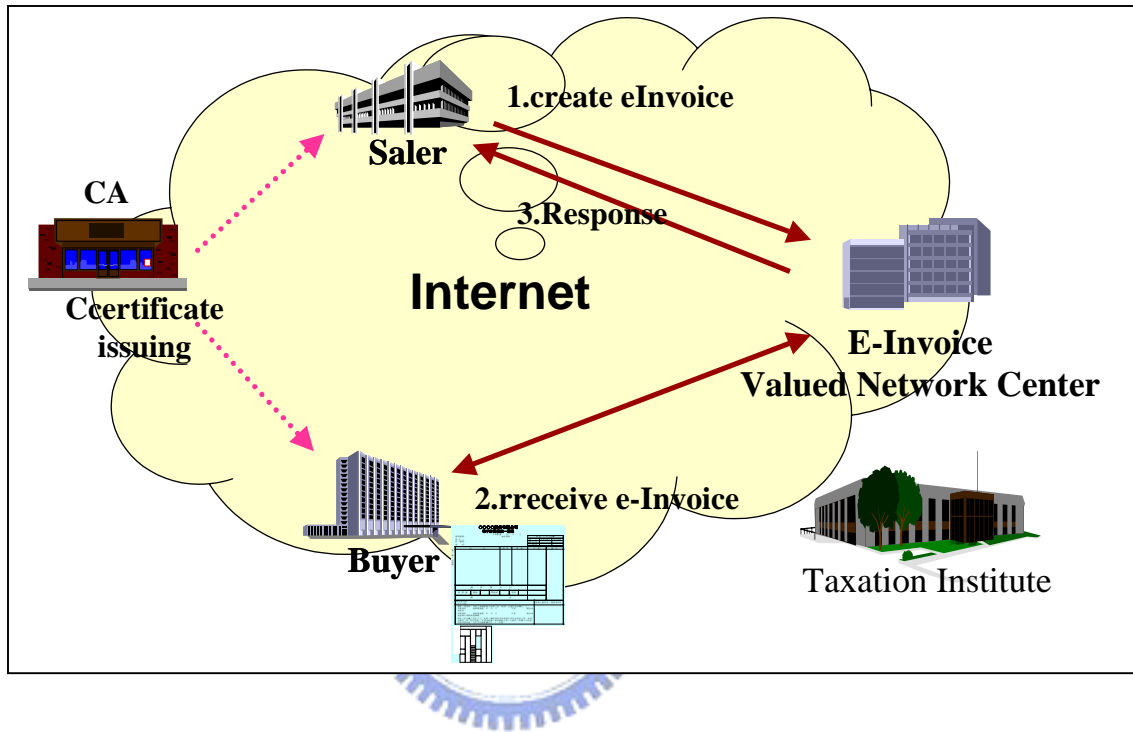


Fig. 11 Framework of E-uniform invoice

PKI allows e-uniform invoice system to be incorporated into Internet securely. The government stands behind the development of e-uniform invoice to protect the internal revenue system. Various government agencies have set forth rules governing the use of e-uniform invoice. Actually, a large number of businesses are ineligible to use e-uniform invoice. In this regard, how to include the ineligible businesses into e-uniform invoice system remains a critical challenge. Therefore, it is important to find out how to output the PKI security mechanism contained in e-uniform invoice to paper invoice so as to enhance security for e-uniform invoice.

## **3.4 Research highlights on PKI physical application**

As stated in section 3.2 and 3.3, PKI mechanism facilitates the applications and development of e-life and thus allows users to enjoy the convenience of digitalized life. Nevertheless, paper documents, paper certificates, and paper tickets remain indispensable for human being's life. Therefore, this thesis concentrates on how to output the secure digital information to paper carriers completely and securely.

As stated in the case studies contained in previous chapters, how to maintain the integrity of digital signature and the verification mechanism of physical information is the foremost challenge for outputting digital data. In this connection, researchers need to find out how to maintain digital signature completely on the physical information and how to develop a verification model in accordance with PKI mechanism.



# Chapter 4

## Proposed PKI Physical Techniques

### 4.1 Estimated Goals

According to the analysis on the demands for PKI application stated in Chapter 3, the demands and value of PKI physical application are obvious. It is, therefore, necessary to define the goals of physical application before solutions are presented. Based upon the analysis for the demands of PKI application, following goals are considered essential:

1. Visualization: data and signature have to be visualized; thereby allowing users to identify data and signature of original in visualized ways, and thus facilitates manual identification and data retrieval.
2. Automation: physical data and signature have to be consistent with machines' requirements to facilitate automatic reading and identification, thereby allowing the machines to read data, analyze and verify data, so as to verify the consistency of information and data source, and thus prevents counterfeit in accordance with the requirements of automation.
3. PKI standard: automatic verification mechanism has to be consistent with PKI validation requirements.
4. Usability: the outputted physical objects have to be consistent with the requirements of low costs, high usability, and portability.

### 4.2 Technical Issues To Be Overcome

When digital data is converted into physical objects, the foremost concern is whether digital data's properties remain unchanged and if the storage cost increases.

When users convert digital information into physical objects, following issues become apparent: the technique of encoding or packaging of digital information, types of physical outputs, outputted data carriers, output equipment requirements, how do outputted objects identify techniques, how to maintain the automation properties of digital information, how to convert back into digital information, requirements for restoration equipment, as well as the treatment and verification issues associated with restoration process. These challenges have to be overcome. In this regard, a solution will be presented so as to accomplish the PKI estimated goals stated in Section 4.1.

As far as PKI application is concerned, digital information comprises content data itself and digital signature data. The content data of digital information can be outputted correctly. The digital signature data comprises digital signature and public key certificates, which are usually written in binary code. Public key certificates data is affiliated to the digital signature. The data needs to be encoded. In the PKI standards, the PKCS#7 designed by RSA Security and the XML Signature standard of W3C serve as the main standards for the message encoding of digital signature. The encoding techniques and physical output process of PKI message are directly related to the encoding and packaging techniques associated with the output process, and are the first step of physical output. In the physical output process, the properties of output techniques determine the types of output, outputted data carrier, output equipment, outputted objects verification process, restoration equipment requirements, and restoration process. As to the selection of output techniques, outputted data carriers, output equipment, and reading device acquisition have to be included into consideration. As far as outputted objects are concerned, papers are most affordable and easiest carrier and are, therefore, consistent with the requirements stated in Chapter 3. As such, papers are probably the first choice for PKI physical application. To cope with the diversified PKI

application needs, however, PVC cards and other materials are probably the most suitable carriers for outputted data regarding physical application in the future.

### 4.3 Recommended PKI Application Proposal

How to convert digital data and digital signature into physical objects? This thesis suggests that the digital information be packaged and converted into physical objects via 2D Bar Code techniques. PKI physical application architecture and technical requirements are shown as Fig. 12.

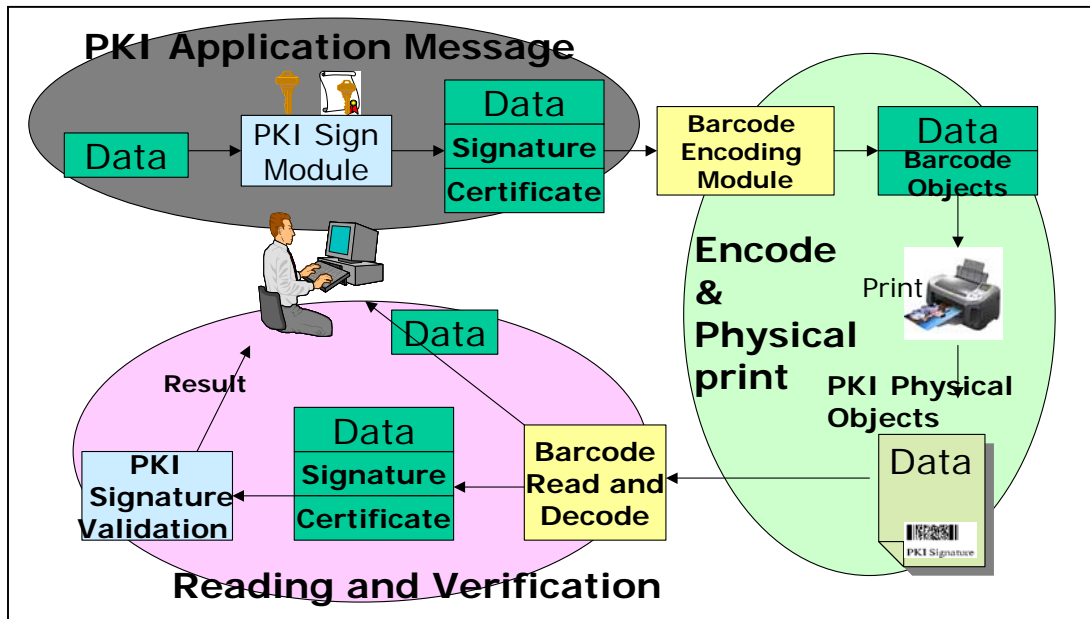


Fig. 12 The architecture of proposed PKI physical application

This chapter describes the technical description regarding PKI physical application with emphasis on physical output, follow-up reading and processing. Description is illustrated in 6 sections as follows:

### 4.3.1 The framework of encoding and output

The framework of encoding and output of PKI application information incorporates the data and signature into 2D Bar Code, and then converts PKI data into physical objects via output equipment, such as printer, barcode printer, and card printer. The carrier of outputted data varies, depending on the application purposes, such as regular papers, cards, and 3-coupon uniform invoice. The outputted objects contain visualized content, including data itself and 2D Bar Codes. The outputted 2D Bar Code is named “Digital Mark” in this thesis as opposed to the 2D Bar Code in the conventional sense. The PKI information encoding and outputting process are shown as Fig. 13.

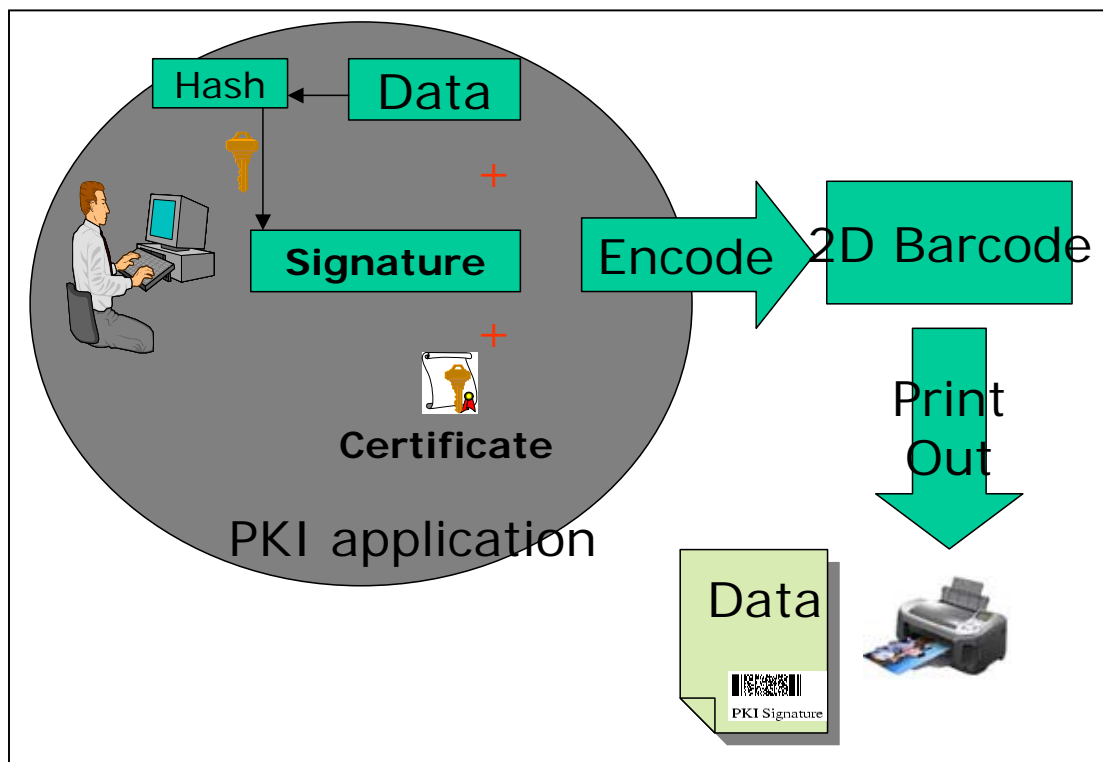


Fig. 13 the framework of encoding and output of PKI information

### 4.3.2 Encoding technique for PKI information and 2D bar codes

Digital signature and digital envelope are the primary types of PKI



information. This thesis concentrates on the application information together with digital signature. According to PKI standards, the PKCS#7 designed by RSA Security and XML Signature of W3C are the primary standards for digital signature. Apparently, PKCS#7 is the most popular message standard nowadays. XML Signature is consistent with Web Service requirements. Therefore, the XML Signature associated with Web Service will become more and more popular in the future.

Bar code is a popular technique for data encoding and requires least costs. The present printing technique allows bar code to be printed on all kinds of carriers. Barcode scanners read the encoded information automatically, and then convert the barcode data into digital information. There are many kinds of bar code techniques. PKI is required to process huge quantity of data and the 1D Bar Code technique falls behind expectation. For the needs of storage and fuzzy requirements, 2D Bar Code is an ideal tool for PKI regarding physical output. As stated in Section 2.4, there are a number of 2D Bar Code techniques, such as Maxicode, Data Matrix, Codeblock, PDF 417, etc. All 2D Bar Code techniques comply with the basic technical requirements of PKI application. This thesis adopts the open barcode technique in consideration of technique acquisition. Therefore, PDF 417 technical standard is used as PKI physical barcode encoding technique in this thesis. With its openness, popularity, data storage capacity, and error correcting capabilities, PDF 417 is likely to enhance the development of PKI application. PKI information packaging and barcode encoding process is shown as Fig. 14.

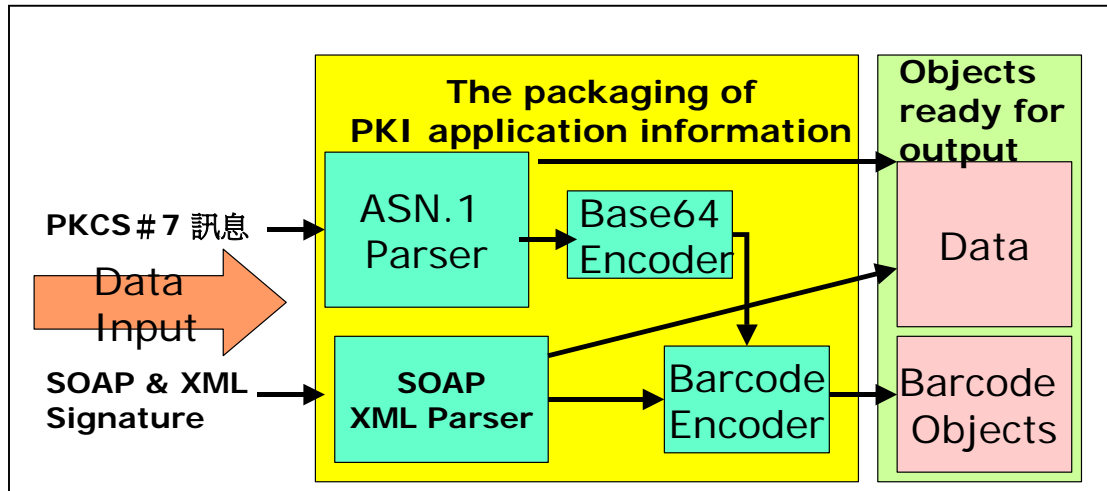


Fig. 14 packaging and barcode encoding process of PKI information

### 4.3.3 Visualized template design and the Digital Mark

Physical objects satisfy human being's reading habits and allow users to identify objects manually and are, therefore, acceptable to human beings. Apparently, physical objects are essential for PKI application. In this connection, this thesis intends to visualize the design and specifications of the physically outputted templates so as to satisfy reading habits in accordance with the traditional sense of value and judgment.

In the design template (Fig. 15), Digital Mark is an important symbol for physical output. Digital Mark comprises 2D Bar Code to be read by machines, instead of any messages to be verified visually. Therefore, this thesis intends to visualize Digital Mark and provide the information to be identified visually. The chop mark visualizes digital signature and facilitates verification process for digital certification authority, thereby enhancing users' confidence. The visualized template and Digital Mark are shown as Fig. 15.

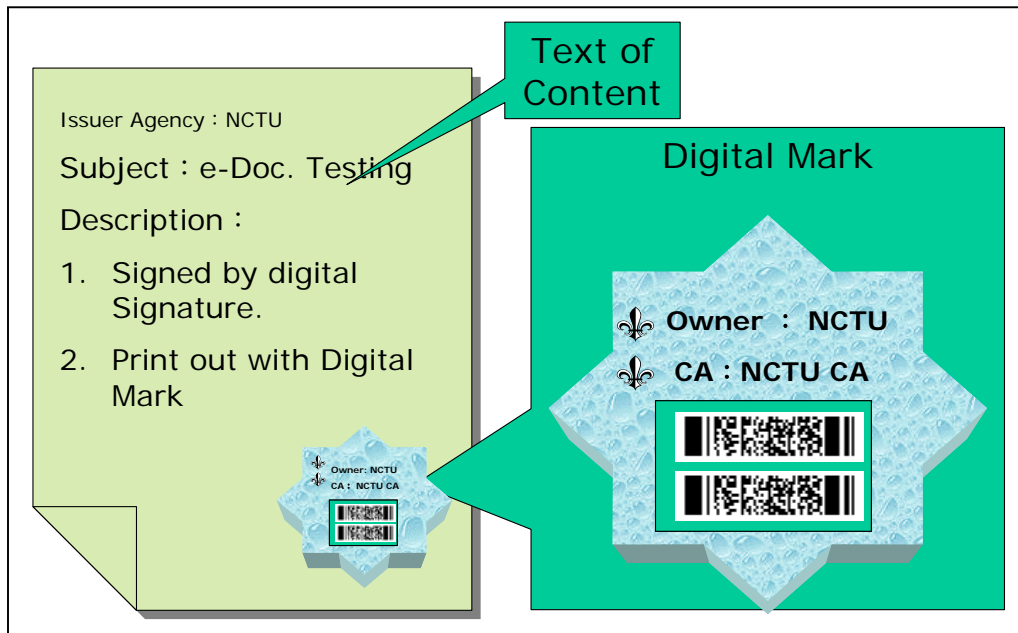


Fig. 15 Visualized template and Digital Mark

#### 4.3.4 Reading and automatic validation process of Digital Mark

Using 2D Bar Code symbols, the Digital Mark can be read into computer system via automatic 2D Bar Code scanners, and decoded messages via Digital Mark decoder. Digital Mark contains the data itself and digital signature. The data itself is outputted via computer monitor to be verified if the data is consistent with paper copy. Digital signature is verified via the PKI validation module provided in the computer system. The verification results are then displayed on computer monitor. Verifiers determine if the document is accurate and correct based upon the data verification and signature validation resulted generated by computer system. Physical information contained in barcodes is read and decoded, and then inputted into computer system again so as to restore the original digital information. Digital Mark reading and automatic validation process is shown as Fig. 16.

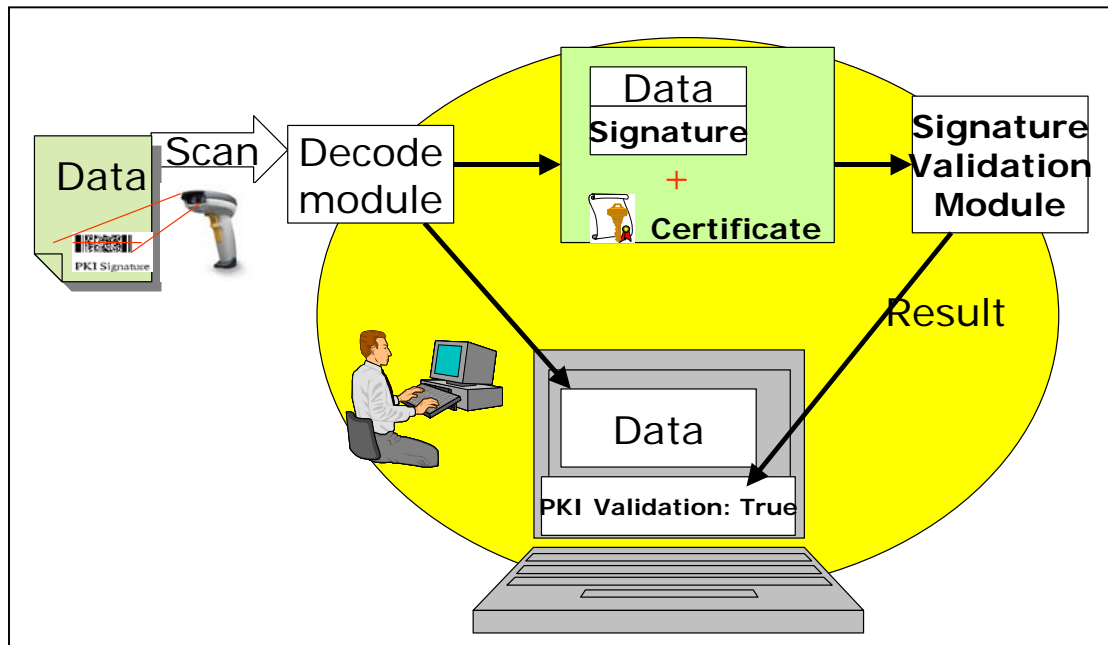


Fig. 16 Reading and automatic validation process of Digital Mark

#### 4.3.5 Decoding of Digital Mark

Digital Mark is converted into digital data after the Digital Mark is scanned by 2D Bar Code scanner. The Digital Mark has to be decoded and restored to the original PKI application data. The decoding module includes Base 64 Decoder, SOAP & SML Parser, and ASN.1 Parser modules. The PKCS#7 signature encoded by Base 64 is restored to Binary Code, analyzed by ASN.1 Parser to generate digital signature value and public key certificates. Alternatively, the data edited by SOAP and XML is analyzed to find out data and digital signature value together with public key certificates encoded by Base 64. The digital signature value and public key certificates are then analyzed via Base 64 decoder. The process is shown as Fig. 17.

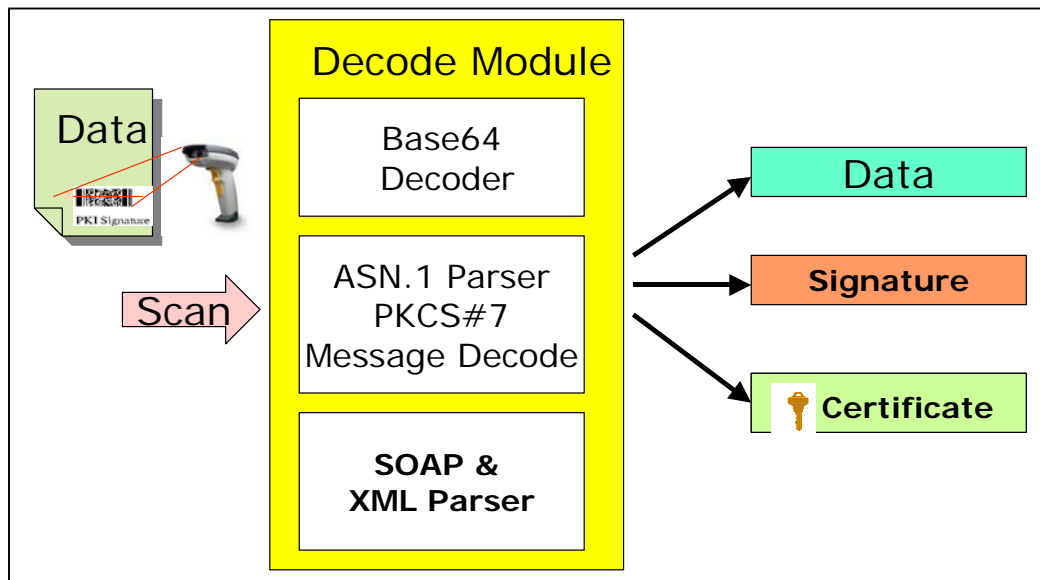


Fig. 17 Decoding of the Digital Mark

#### 4.3.6 Validation module of PKI digital signature

Physical PKI messages are encoded into the Digital Mark. The Digital Mark can be read with human eyes simply. As to the accuracy of data and the integrity message, standard PKI mechanism is needed so as to figure out the validation results precisely. Validation mechanism comprises the validation of public key certificate as well as the verification of the digital signature value. The decoded public key certificates stated in Section 4.3.5 has to pass the validation by the digital signature validation module regarding certificate path validation so as to find out if its the certification authority and Trust Anchor are trusty, if its Trust Anchor is consistent with the accuracy requirement of the certificate, if CRL repository is examined, and if the certificate is valid. The hash value of the text has to be re-calculated, and then compared to the decrypted signature hash value so as to determine if both values are the same.

Digital Mark is considered accurate only if the validation of the public key

certificates and digital signature are all truth. If that's the case, the validation of data sustains. If any validation shows false result, the data will be considered invalid. The architecture of digital signature validation module is shown as Fig. 18.

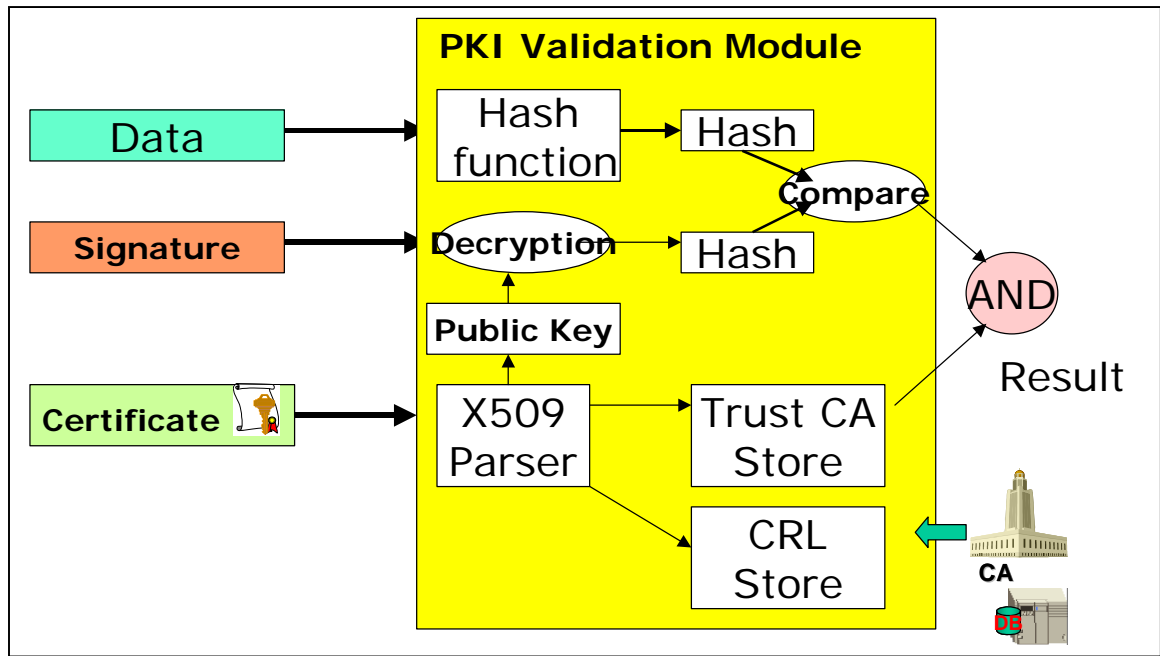


Fig. 18 Validation module of PKI digital signature

## 4.4 Comparison and analysis of PKI application information carriers

PKI application is significantly related to information security. The carriers have to be secure enough for the protection of user's private key. Smart card, key token, hard disk, and floppy disk are extensively used as carriers. Smart card and key token are the most secure carriers nowadays. Carriers are designed to store private keys. In reality, the information of PKI application is stored in hard disk or database as primary repository. And the information is stored in digital. All information has to be retrieved via electronic equipment, cannot be used physically.

The solutions stated in this thesis are designed to solve the issues related to paper carriers or similar carriers. PKI application information has nothing to do with the administration of user's private key and, therefore, security concerns do not exist. PKI carriers are compared and the results are shown as Table 1. Apparently, paper is highly competitive with respect to costs, size, and portability. Furthermore, paper provides visualized information, while other carriers do not.

Table 1: Comparison and analysis of PKI application information carriers

	Floppy disk	Hard disk	Smart card	Key Token	Paper
Cost	Small	High(High density)	Middle	Middle	Least (Low density)
Physical Size	Small	Large	Small	Small	Letter, A4...
Portable	Yes	No	Yes	Yes	Yes
I/O Device	Floppy Reader		Reader		Bar code scanner
Interface API	Propriety API	CAPI OPENSSL LIB	CAPI PKCS#11	CAPI PKCS#11	Barcode API
Visualization	No	No	No	No	Yes

# Chapter 5

## Implementation of Experimental System

This chapter describes the feasibility test and verification process for the PKI physical application proposal stated in Chapter 4 with emphasis on physical environment, experimental system architecture, experimental process, user interfaces, and experimental test.

### 5.1 Physical Environment

The experimental system is established in a test environment with single machine for system development and testing. Following are the system development environment and software/hardware resources required by this study.

#### 1. Hardware:

- (1) Host: Acer TrvelMate 360 Notebook Intel Pentium III 1.0GHz CPU , 512 MB RAM , 20GB HDD.
- (2) Output equipment (printer): HP LaserJet 4300
- (3) Input equipment (barcode scanner): HHP Image Team 4600 Scanner USB Interface.

#### 2. Software:

- (1) Operating system: Microsoft Windows 2000 Operating System together with Service Pack 4.
- (2) System development platform: Boland Jbuilder X Enterprise Edition



Trial Version ◦

- (3) Software development libraries (Libraries & APIs): Sun Java SDK 1.4.2 [28], Bouncy Castle Crypto APIs [25], 2D barcode PDF417 Library [26], GSView for Windows.

## 5.2 Experimental System Architecture

The experimental system is designed to generate digital content data in connection with PKI simulated application. The data is edited and processed, and forwarded to PKI application sample as a template for physical output. The PKI physical template is then inputted into system via automation equipment, and then digital information is restored and digital signature validation is completed. The core system modules include PKI certificate management and digital signature module, Digital Mark encoding module, barcode encoding & outputting module, barcode reading/decoding and PKI Validation module as shown by Fig. 19.

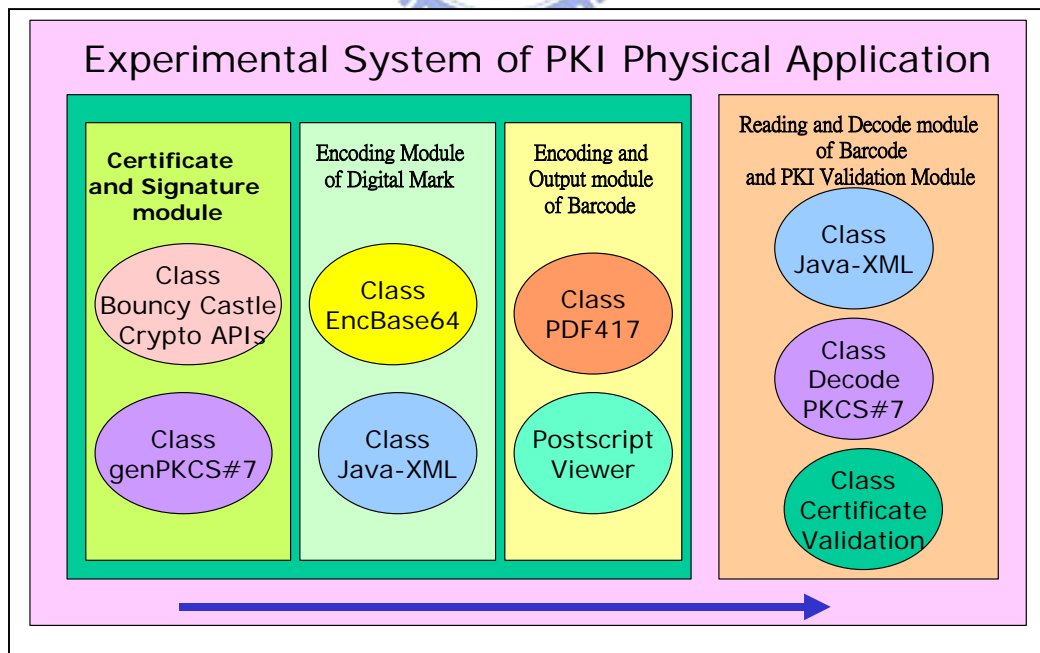


Fig. 19 the architecture of experimental system

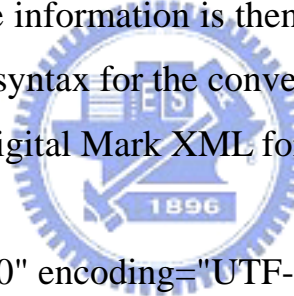
## 1. Certificate management and digital signature module

PKI certificate management and digital signature module are the primary data sources of the experimental system for the purpose of loading private key and public key certificates so as to produce PKI application messages required by the test and to envelope PKI application messages in the format consistent with PKCS#7 standard.

## 2. Encoding module of Digital Mark

Digital Mark includes the text and the visualized Digital Mark of digital signature. Prior to converting encoded messages into 2D barcode messages, PKI retrieves Digital Mark information to be displayed via Digital Mark encoding module. The information is then processed via the encoding method consistent with XML syntax for the convenience of subsequent treatment.

Following is the Digital Mark XML format contained in the experimental system:



```
<?xml version="1.0" encoding="UTF-8"?>
  <eDoc>
    <!-- Digital Mark sample of test -->
    <version>1.0</version>
    <docID>NCTU93060001</docID>
    <date>Fri Jun 25 00:54:59 CST 2004</date>
    <docIssuer>PKI test doc signer</docIssuer>
    <TrustCA>Test CA</TrustCA>
    <content>PKI Application on Physical Object Testing
    Program.....</content>
    <signature type="PKCS#7" method="BASE64"
  >MIIGGAYJKoZIhvcNAQcCoIIGCTCCBgUCAQExCzAJBgUrDgM
```

```

CGgUAMAsGCSqGSIb3DQEHAaCCBOgwggTkMIIDzKADAgECAi
ICHBH53tSNpDXwg8Js/DWK/.....
/.....AoGnp2lzVtWUusuXW/w==</signature>
</eDoc>

```

### 3. Encoding and output module of Barcode

The encoded PKI application messages are processed via Digital Mark encoding module and are prepared to convert into barcode data, ready for output. The PDF 417 libraries are used to transform those data into 2D barcode. However, graphic output format is still needed so as to produce 2D barcode, such as Postscript or PDF format. The experimental system uses Postscript format as the sample to be outputted by Digital Marks. The Postscript file outputted by Digital Marks is read via Postscript Viewer. In the experimental process, GS View for windows is used for preview and printing. The process is shown as Fig. 20.

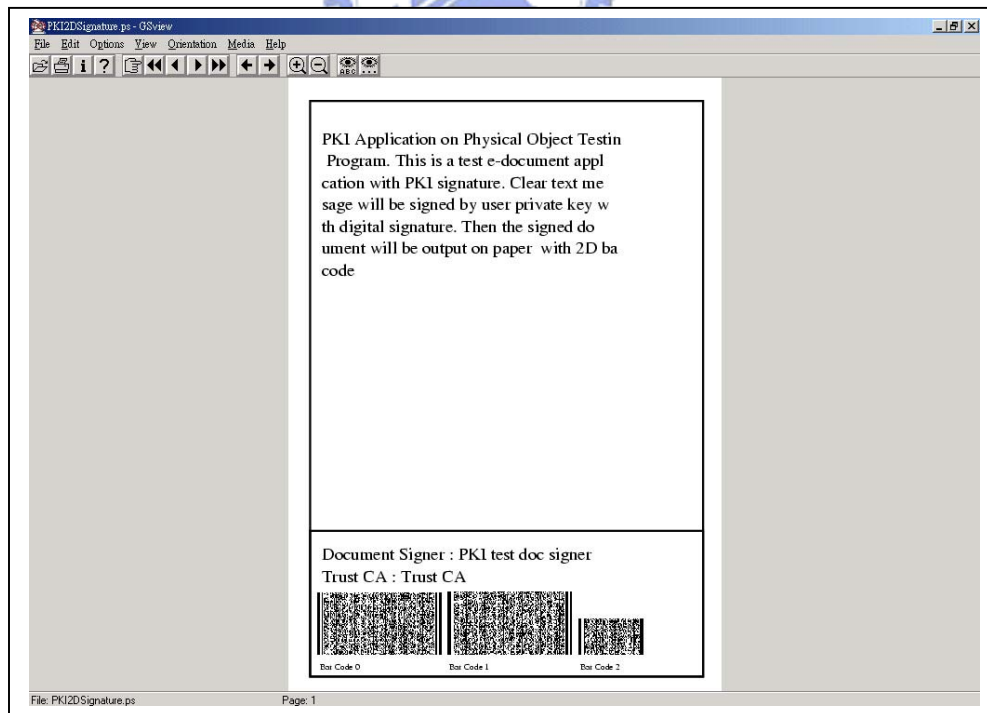


Fig. 20 Output sample in Postscript

### 4. Barcode reading/decoding and PKI validation module

Digital Marks are scanned via 2D barcode scanner and encoded by XML, and then inputted into the system. Then, XML Parser analyzes the data along with the signature data encoded in PKCS#7. The signed data decoded by Base 64 is analyzed by PKCS#7 so as to retrieve signature and public key certificates for verifications of digital signature and validation of certificates.

### 5.3 Experimental system process

The experimental system process is shown as Fig. 21.

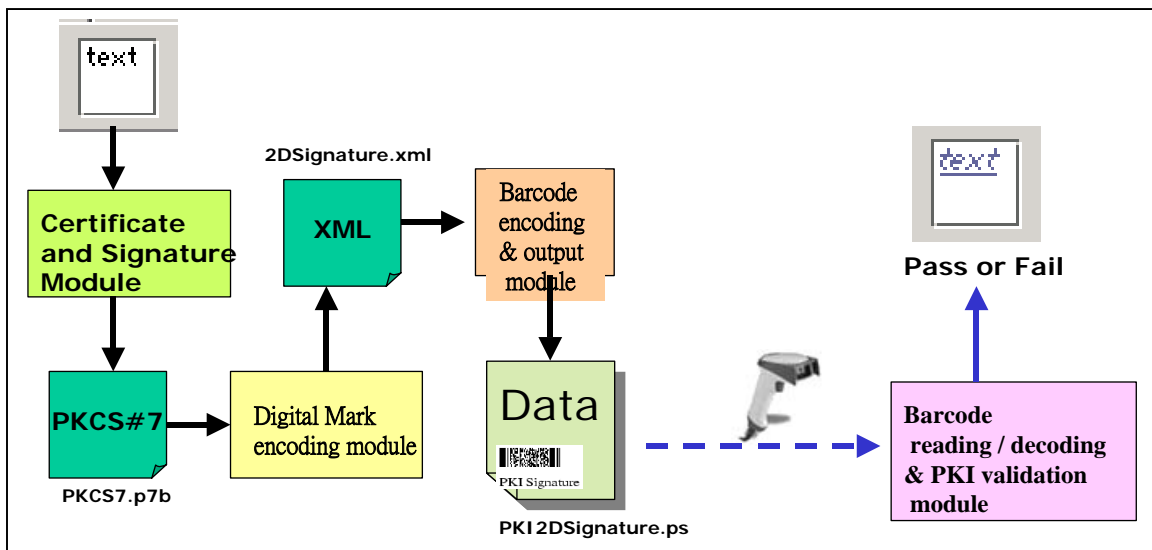


Fig. 21 the process of experimental system

### 5.4 User Interfaces and Message Verification Test

The experimental system developed by this study is presented as GUI, which is then divided into 5 UI according to the experimental system architecture. The experimental system comprises 2 parts – to generate PKI physically outputted objects and PKI physical object’s input & verification, respectively. The first part of experimental system comprises 4 modules – “0 selecting key pairs”, “1.1 digital

signature”, “1.2 Digital Mark”, and “1.3 physical object output”. “2 document verification” is classified as the test interface of part 2. The experimental system illustrates test examples as follows:

1. User interface: “0 selecting key pair”

Public key pair is the foundation for PKI application system. The experimental system is provided with Sun Java Key Store and PKCS#12 personal information exchange files as the sources of public key pairs. After selecting key source and entering source filename together with password, click “loading key” to load the information of private key and public key from keystore for the purpose of follow-up signature process. The user interface is shown as Fig. 22.



Fig. 22 the user interface: “0 Selecting key pair”

## 2. User interface: “1.1 digital signature”

Enter the content of test document to the plain text field and click “generate message signature file (PKCS7.p7b)” button. The experimental system signs digitally by the predetermined private key and certificate, and creates message signature file PKCS7.p7b, which is consistent with PKCS#7 standard, under the operation directory. The signature value field displays the digital signature text encoded by Base 64 and is shown as Fig. 23.



Fig. 23 the user interface: “1.1 Digital signature”

### 3. User interface: “1.2 Digital Mark”

Before the process of 2D barcode begins, the plain text and digital signature stated in picture 1.1 regarding digital signature are encoded via XML Digital Mark template. Thus, “2D signature.xml” file is created under the operation directory. The XML encoding results created by Digital Mark template are shown in the fields, which allow users to verify the progress of the test. The process is shown as Fig. 24.

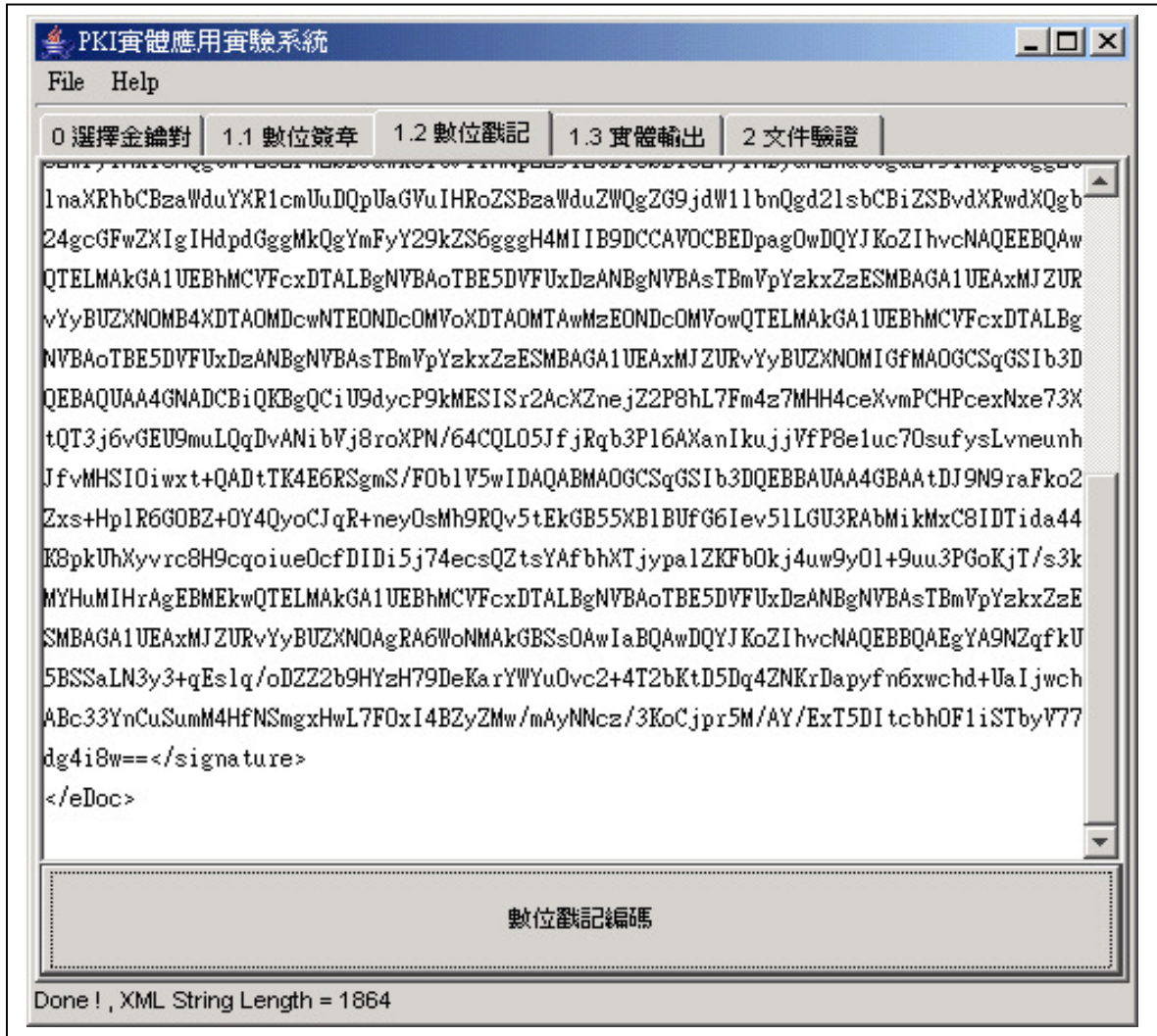


Fig. 24 the user interface: “1.2 Digital Mark”



#### 4. User interface: “1.3 physical output”

This feature converts the Digital Mark data encoded by XML into Postscript graphic output file, to be divided into 2D barcode with proper length. PDF 417 accommodates a limited amount of 2D barcode data. To make sure that the amount of data does not exceed the restriction of PDF 417, in this thesis we limit the stored data bytes of single barcode less than 1200 bytes. Then the Digital Mark would be constructed by several barcodes. A Postscript file named PK12Dsignature.ps is created. The process is shown as Fig. 25 and Fig. 26.

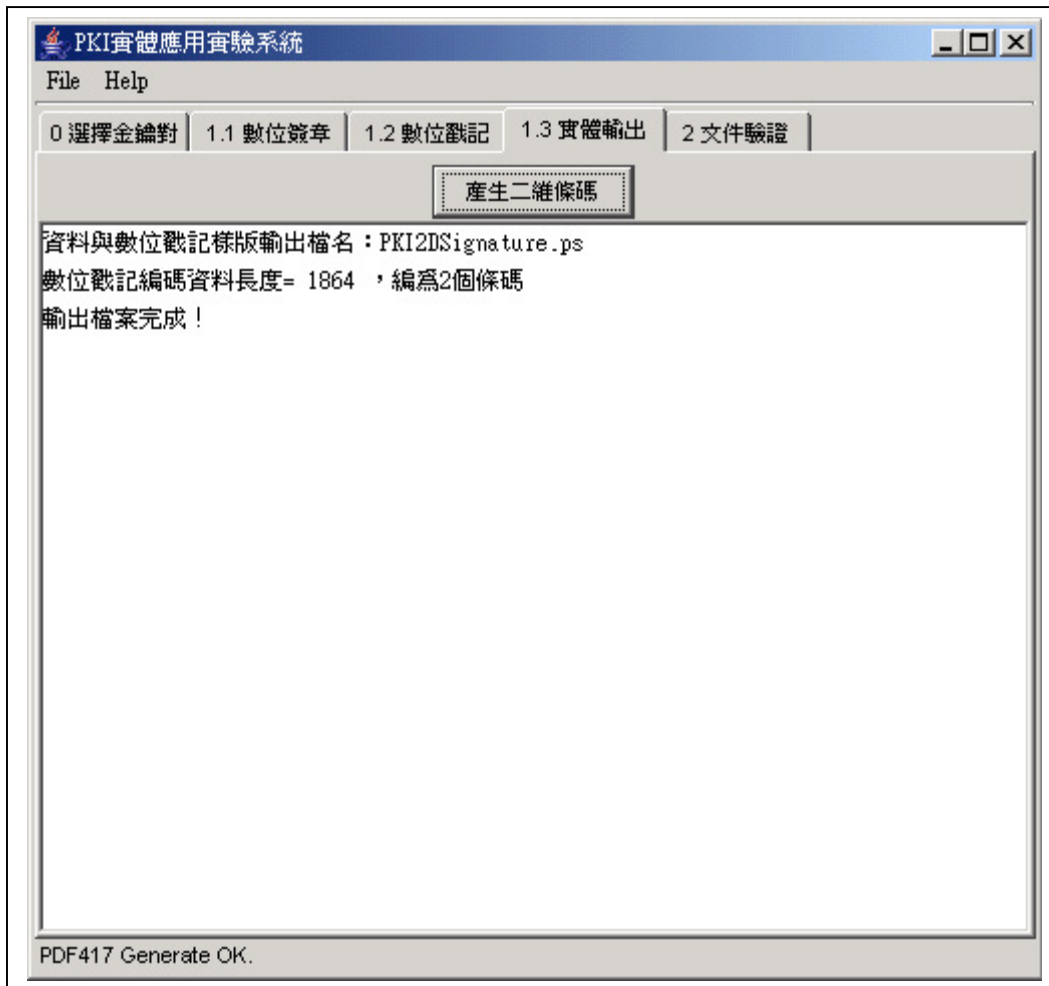


Fig. 25 the user interface: “1.3 Physical output”



## JKS 1024 Key Length Testing

### PKI Application on Physical Object Testing Program.

This is a test e-document application with PKI signature.

Clear text message will be signed by user private key with digital signature.

Then the signed document will be output on paper with 2D barcode.

Document Signer :

CN=eDoc Test, OU=eic91g, O=NCTU, C=TW

Trust CA :

CN=eDoc Test, OU=eic91g, O=NCTU, C=TW



Bar Code 0

Bar Code 1

Fig. 26 Sample of physically outputted document

## 5. User interface: “2 document certification”

PKI physically outputted sample is inputted and information is verified. The process is shown as Fig. 27. The physically outputted sample data is read via 2D barcode scanner and the decoded text of content is entered into the left window. Press “Digital Mark verification” button. The system will be activated to analyze XML encoding data and to retrieve PKCS#7 signature message. Release PKCS#7 encoding data. Verify the validation of public key certificate and verify the accuracy of signature data. Finally, the plain text and verification results appear in the right window.

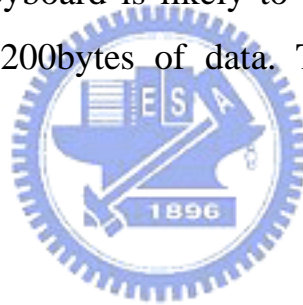


Fig. 27 the user interface: “2 Document verification”

## 5.5 Evaluation of Experimental System Issues

Following issues were found in the experimental system test process:

1. Huge amount of plain text requires several barcodes for encoding and the data has to be read in sequence. Every 1200 bytes of data requires a barcode. For 1MB data, 874 barcodes are needed, which makes the task difficult.
2. PDF 417 barcode is approximately 6cm wide and 3cm high, which appears to be large in an A4 paper. It is, therefore, reasonable to use smaller 2D barcode, such as Maxicode or another.
3. It takes a long time to input 2D barcode data into system. In other words, the speed is not fast enough. If data is inputted via 2D scanner through USB Keyboard interface, keyboard is likely to slow down. 35-40 seconds will be needed for entering 1200bytes of data. Therefore, further improvement is required.



# Chapter 6

## Conclusions

### 6.1 Conclusion

The rapid development of Internet has triggered the demands for information security and identity authentication. Also, PKI application is growing steadily. At the time more and more PKI application plans are implemented, the demand for physical application increases. As indicated by the experiment results, the PKI physical application proposal stated in this thesis has been recognized as a feasible solution for e-document or e-mail, thereby integrating paper with digital signature, and thus uses paper as an economic tool for verification so as to prevent counterfeit from happening.

The digital trading messages on the Internet could become a physical and portable service via the Digital Mark technique, which can be applied to the purchase of a ticket as well, and thus integrate PKI security mechanism into a physical life step by step.

### 6.2 Future research directions

This study attempts to find out a formula that allows PKI application to be accepted in the physical trading environment, thereby improving security and convenience for PKI. This thesis suggests that 2D barcode serves as the carrier for PKI objects so as to enhance user's confidence via Digital Mark. However, huge amount of data has to be divided and inputted into several barcodes, and then read in sequence. Apparently, the present situation is far from perfect. 2D barcode uses

binary system comprising black and white as basic elements. If 8bits-color editing technique becomes available one day, more portable data will be allowed. Digital watermark is probably a possible technique in the future to enhance the overall confidence.



# References

- [1] Russ Housely, Tim Polk, Planning for PKI, Best practices guide for deploying public key infrastructure, 2001.
- [2] INTERNATIONAL TELECOMMUNICATION UNION,  
ITU-T Recommendation X.509, Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, 2000/03.
- [3] RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, <http://www.ietf.org/rfc/rfc2459.txt>
- [4] <http://www.rsasecurity.com/>
- [5] RSA Laboratories [2001], PKCS #1: RSA Cryptography Standard, RSA Security.
- [6] RSA Laboratories [1993], PKCS #7: Cryptographic Message Syntax Standard, RSA Security.
- [7] <http://www.w3.org/2001/XKMS/>
- [8] <http://www.w3.org/TR/xmlldsig-core/>
- [9] <http://www.w3.org/TR/xmlldsig-requirements>
- [10] Steve Graham, et al., Building Web Services with Java : Making Sense of XML, SOAP, WSDL, and UDDI, Sams Publishing, 2002.
- [11] <http://www2.tw.ibm.com/developerWorks/>
- [12] Scott Oaks, Java Security, 2/e O'Reilly & Associates, Inc., 2002.
- [13] Jonathan Knudsen, JAVA Cryptography, O'Reilly & Associates, Inc., 1999.
- [14] William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Higher Education, September 2002.
- [15] <http://www.sunny.org.tw/tax/teach/teach15.htm>
- [16] <http://www.shyang.com.tw/2DCodeSkill/index.asp>

- [17] <http://www.vcollege.org.tw/>
- [18] <http://www.cgan.net/book/books/print/barcode/links/st1.htm>
- [19] The technology of Barcode, <http://www.barcodeusa.com/barcode.htm>
- [20] Public key infrastructure of government (GPKI), <http://grca.nat.gov.tw/>
- [21] Government certification authority, <http://www.pki.gov.tw/>
- [22] Certificate Authority of MOEA (MOEACA), <http://moeaca.nat.gov.tw/>
- [23] Certificate Authority of MOI (MOICA),  
<http://moica.nat.gov.tw/html/index.htm> ◦
- [24] Mixed Organization Certification Authority (XCA), <http://xca.nat.gov.tw/>
- [25] Electronic signatures act, <http://www.icct.com.tw/esign/default.asp> ◦
- [26] The website of the Research, Development and Evaluation Commission,  
Executive Yuan, <http://www.rdec.gov.tw/home/egov.htm>
- [27] Bouncy Castle Crypto APIs, <http://www.bouncycastle.org/>
- [28] Project: 2D barcode PDF417 library, <http://sourceforge.net/projects/pdf417lib/>
- [29] Borland Taiwan branch, Borland Jbuilder X technical book, Gotop Information Inc., February 2004.
- [30] Sun Java Home , <http://www.java.com/en/learn/developers.jsp> ◦
- [31] Brett McLaughlin, Java & XML, 2nd Edition: Solutions to Real-World Problems, September 2001
- [32] Hiroshi Maruyama, et al., XML and Java: Developing Web Applications, Second Edition, Addison-Wesley Professional, May 2002.
- [33] Adobe Systems Incorporated, Postscript language tutorial and cookbook, Addison-Wesley publishing company, Inc., 1985.
- [34] Kapil Raina, PKI Security Solution for the Enterprise: Solving HIPAA, E-paper Act, and Other Compliance Issues, Wiley Publishing Inc., 2003.
- [35] Tom Austia, PKI A Wiley Tech Brief, Wiley Publishing Inc., 2001.

- [36] Charlie Adams, Steve Lloyd, Understanding Public-Key Infrastructure Concepts, Standards, and Deployment Considerations, Macmillan Technical Publishing, 1999
- [37] Website of Taiwan BCA, <http://www.bca.org.tw>
- [38] Website of PKI Interoperability management and promotion program in Taiwan, <http://www.pki-pma.org.tw>
- [39] NIST PKI Program, <http://csrc.nist.gov/pki/twg/welcome.html>
- [40] Public-Key Infrastructure (X.509) (pkix),  
<http://www.ietf.org/html.charters/pkix-charter.html>

