



How to Deploy Certification Authorities and PKI Technology to
increase the security for transferring electronic documents
in the organizations of Thailand : A Case study of
Ministry of Interior

By

Mr. Teerachai Vatcharayoo

Submitted in Partial Fulfillment of
the Requirements for the Degree of
Master of Science
in Technology Management
Assumption University

February 2002

St. Gabriel's Library, Au

**/How to Deploy Certification
Authorities and PM Technology to
increase the security for transferring
electronic documents in the
organizations of Thailand:
A Case study of Ministry of Interior**



Mr. Teerachai Vatcharayoo

**Submitted in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Technology
Management
Assumption University**

The Faculty of Science and Technology

Project Approval

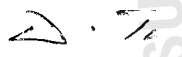
Project Title How to Deploy Certification Authorities and PKI Technology to increase the security for transferring electronic documents in the organizations of Thailand: A Case study of Ministry of Interior

By
Project Advisor Mr. Teerachai Vatcharayoo
 Dr. Wisanu Tuntawiroon

Academic Year 2/2001

The Department of Technology Management , Faculty of Science and Technology of Assumption University has approved this final report of the three credits course. **MT6500** Master Project, submitted in partial fulfillment of the requirements for the degree of Master of Science in Technology Management.


Approval Committee:




(Dr. Wisanu Tuntawiroon)
Advisor & Program Director



(Asst.Prof.Dr. Thotsapon Sortrakul)
Committee Member

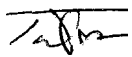


(A. Tanawat Ruangteprat)
Committee Member




(Dr. Soonthorn Pibulcharoensit)
Committee Member

Faculty Approval:



(Dr. Wisanu Tuntawiroon)
Program Director



(Asst.Prof.Dr. Pratit Santiprabhob)
Dean

February / 2002

ACKNOWLEDGEMENTS

I , the writer, would like to thank many people who help and paid attention with this development of this project.

I would like to thank GENIA Solution Co.,Ltd that gave a chance for me to develop this project in the real situation that makes me more clear and understand about all concepts and processes on PKI development.

And also thank many institutes that give a chance for me to develop this project, including Assumption University, Ministry of Interior, College of Management Mahidol University, Thammasat University, etc.



ABSTRACT

A worldwide Public Key Infrastructure (PKI) that supports international, government, and state policies/regulations will not be available until the turn of the century. In the meantime, corporations can utilize this security technology to satisfy current business needs. Corporate PKI addresses areas such as secure web application development and messaging. Many companies are choosing to manage their own Certificate Authority (CA) instead of outsourcing this function to a third party (i.e., Verisign, GTE CyberTrust). To benefit fully from the public key technology in a corporate environment, a thorough understanding of the current and future PKI technology and uses is required. The security requirements for each PKI component are detailed, as well as, their interaction with other components. In addition, a brief analysis of the PKI problem space is presented using a design framework graph.



TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1
1.1 OVERVIEW OF PM TECHNOLOGY	1
1.2 PROBLEM STATEMENT OF MINISTRY OF INTERIOR (MOI)	1
1.3 OBJECTIVES	2
1.4 LIMITATION OF THIS PROJECT	2
1.5 SAMPLE SIZE OF THE RESEARCH	2
1.6 TERMS AND DEFINITION	3
CHAPTER 2 SELECTIVE LITERATURE REVIEW	5
2.1 AVAILABLE SECURITY SERVICES AND TECHNOLOGIES	5
2.1.1 SECURITY SERVICES	5
2.1.2 NON-CRYPTOGRAPHIC SECURITY MECHANISMS	5
2.1.3 CRYPTOGRAPHIC SECURITY MECHANISMS	9
2.1.4 SECURITY INFRASTRUCTURES	15
2.1.5 PUBLIC KEY INFRASTRUCTURE	16
2.1.6 PM COMPONENTS	17
2.1.7 PM ARCHITECTURES	22
2.1.8 PM DATA STRUCTURES	28
2.1.9 ADDITIONAL PM SERVICES	36
CHAPTER 3 RESEARCH METHODOLOGY	38
3.1 DISCOVER OF THE DILEMMA ON THE EXISTING SYSTEM OF MOI ELECTRONIC DOCUMENT TRANSFERRED SYSTEM	38
3.2 DOING THE RESEARCH ON THE AVAILABLE TECHNOLOGY USAGES	38
3.3 DATA COLLECTION FROM MOI SYSTEM	39
3.4 THE SCOPE OF RESPONDENT	40
3.5 DEVELOPMENT OF GUIDELINE FOR MOI	40
CHAPTER 4 CASE STUDY ON IMPLEMENTING OF PM TECHNOLOGY	41
4.1 ANALYZE DATA AND APPLICATIONS FOR MOI	44
4.2 COLLECT SAMPLE POLICIES AND BASE STANDARDS	46
4.3 DRAFT CERTIFICATE POLICY(S)	46

4.4 SELECT PM PRODUCT OR SERVICE PROVIDER	51
4.5 DEVELOP CPS (CERTIFICATION PRACTICE STATEMENT)	53
4.6 DO A PILOT	53
4.7 NETWORK DIAGRAM OF MOI AFTER DEPLOYING PM	54
CHAPTER 5 ANALYSIS OF PM TECHNOLOGY BEFORE DEPLOYING	56
5.1 EXTERNAL ENVIRONMENT CRITERIA	56
5.2 INTERNAL ENVIRONMENT CRITERIA	57
5.3 COST/BENEFIT	59
CHAPTER 6 DEVELOPMENT PLAN	62
6.1 DEPLOYING PM	62
6.2 ANALYZE DATA AND APPLICATIONS FOR YOUR ORGANIZATION	62
6.3 COLLECT SAMPLE POLICIES AND BASE STANDARDS	63
6.4 DRAFT CERTIFICATE POLICY(S)	63
6.5 SELECT PM PRODUCT OR SERVICE PROVIDER	65
6.6 DEVELOP CPS (CERTIFICATION PRACTICE STATEMENT)	66
6.7 DO A PILOT	66
CHAPTER 7 CONCLUSION	68
BIBLIOGRAPHY	70
APPENDIX A	71
APPENDIX B	73
APPENDIX C	83

CHAPTER 1 INTRODUCTION

1.1 Overview of PM Technology

Computer networks are no longer closed systems in which a user's mere presence on the network can serve as proof of identity. In this age of information interconnection, an organization's network may consist of intranets, Internet sites, and extranets--all of which are potentially susceptible to access by unauthorized individuals who intend to maliciously view or alter an organization's digital information assets.

There are many potential opportunities for unauthorized access to information on networks. A person can attempt to monitor or alter information streams such as e-mail, electronic commerce transactions, and file transfers. Your organization may work with partners on projects of limited scope and duration, with employees whom you know nothing about, but who, nonetheless, must be given access to some of your information resources. If your users have a multitude of passwords to remember for accessing different secure systems, they may choose weak or common passwords to more easily remember them. This not only provides a hacker with a password that is easy to crack, but also one that will provide access to multiple secure systems and stored data.

How can a system administrator be sure of the identity of a person accessing information and, given that identity, control which information that person has access to? Additionally, how can a system administrator easily and securely distribute and manage identification credentials across an organization? These are issues that can be addressed with a well-planned public key infrastructure.

1.2 Problem Statement of Ministry of Interior (MOI)

Now, the existing system of transferring federal documents inside MOI is changed from paper based system to become paperless system that are based on computerized via network exchanged system. This system quite makes the operations inside MOI to be run smoothly and faster. But from the management point of view, this system still has the weakness in term of these points:

- Lacking of the security system that can track for the original messages are already altered or not.
- Lacking of the identification tools for ensuring the validity and integrity of the messages from the sender is generated from the sender or not.
- MOI wants to find the solution and guideline how to implement that system to reduce and protect the cause of those problems.
- MOI is wondering that it is possible for PKI is one of the solutions that can be the best choice to solve these problems or not.

1.3 Objectives

- To assist organization and management to make decision in determining if a PKI is appropriate to implement in the organization in Thailand environment
- To suggest how PM service can be deployed most effectively within the organization
- To provide an overview of PKI functions and their applications and fully analyze costs and benefits of PKI systems for the organization use
- To develop plans for the implementation PKI

1.4 Limitation of this project

This project has the limitation of the type of organization. For this project is based on Ministry of Interior case study that are already implemented, so the organizations that are willing to use this guideline for development for their own implementation maybe have to change some criteria according to their organization, such as existing policy of users is also different from MOI.

1.5 Sample Size of the Research

For the sample size of this research is for 750 officers of MOI will be the pilot for this implementation for PKI system. This will increase up to the whole organization within 1 – 2 years after the pilot training is successfully implemented.

1.6 Terms and Definitions

1.6.1 *What is Public Key Cryptography?*

Conventional cryptography consists of a single mathematical key used for both encryption and decryption of data. If you want to send a secure message to an addressee, you encrypt the message using a key known only to the sender and the recipient and then you pass both the key and encrypted message to the recipient so that the message can only be decrypted by the intended recipient. Public Key Cryptography uses two keys. One key is kept private and the other key is made public. If the Public Key is used to encrypt a message, the Private Key can decrypt the message. In other words, if you want to send an addressee a message, you encrypt the message with the addressee's Public Key and pass the message to the addressee. The addressee can then use the Private Key to decrypt it.

1.6.2 *What is a Digital Signature?*

With the invention of Public Key Cryptography, another process known as a digital signature is possible. A digital signature is much like a hand signature in that it provides proof that you are the originator of the message (Authentication). If you want to sign the message which you sent to an addressee, you pass the message through a mathematical function (known as a hash function) which provides a summary (hash code) of the message. This summary is unique for every message and is much like a fingerprint. You then encrypt this hash code with your Private Key and attach the code to the end of your message. This attached code is known as a digital signature. The addressee can then verify that the message was sent by you by decrypting the digital signature, using your public key, to get the hash code. The addressee then passes the received message through the same hash function. If the two hash codes are the same, then the message was sent from you (Non-repudiation) and was not altered (Integrity). All this sounds complicated but, in practice, selecting an icon on your computer screen is all that it takes to make it happen.

1.6.3 *What is a Public Key Infrastructure?*

A Public Key Infrastructure is a Cryptographic key and Certificate delivery system which makes possible secure financial electronic transactions and exchanges of sensitive information between relative strangers. A PKI will provide Privacy, Access control, Integrity, Authentication, and Non-repudiation support to information technology applications and electronic commerce transactions. A PKI will: manage the generation and distribution of Public/Private Key pairs; and publish the Public Keys with the user's identification as "certificates" in open bulletin boards (i.e., X.500 Directory Services). A PKI provides a high degree of confidence that: Private Keys are kept secure; specific Public Keys are truly linked to specific Private Keys; and the party holding a Public/Private Key pair is who the party purports to be.

Public Key Infrastructures (PKIs) can speed up and simplify delivery of products and services by providing electronic approaches to processes that historically have been paper based. These electronic solutions depend on data integrity and authenticity. Both can be accomplished by binding a unique digital signature to an individual and ensuring that the digital signature cannot be forged. The individual can then digitally sign the data and the recipient can verify the originator of the data and that the data has not been modified without the originator's knowledge. In addition, the PKI can provide encryption capabilities to ensure privacy. As with all aspects of information technology, introducing a PKI into an organization requires careful planning and a thorough understanding of its relationship to other automated systems.

CHAPTER 2 SELECTIVE LITERATURE REVIEW

2.1 Available Security Services and Technologies

This section is intended to describe the security services that may be achieved, and provide a comparison for the various techniques that may be used.

2.1.1 SECURITY SERVICES [7]

There are four basic security services: integrity, confidentiality, identification and authentication, and non-repudiation. This section describes the four services and why they may be necessary in a particular application.

Data integrity services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.

Confidentiality services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals or processes.

Identification and authentication services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin

Non-repudiation services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

2.1.2 NON-CRYPTOGRAPHIC SECURITY MECHANISMS

Some of the security services described above can be achieved without the use of cryptography. Where illustrations may be useful, we will use Nanako, Toshi, and

Yoshiki. Nanako and Toshi want to communicate in a secure manner. Yoshiki would like to interfere with the security services that Nanako and Toshi would like to obtain.

2.1.2.1 Parity Bits and Cyclic Redundancy Checks

The simplest security mechanisms were designed to ensure the integrity of data transmitted between devices (e.g., computers and terminals). When devices communicate over a noisy channel, such as a phone line, there was a possibility that data might be altered. To guard against this, systems would transmit an extra bit, the parity bit, for each byte of data. The value of the extra bit was chosen to ensure that the number of 1s in the nine bits were odd (odd parity) or even (even parity). If the parity was wrong, data had been altered, and should be rejected. This mechanism is frequently used with modem connections.

Parity bits are a relatively expensive form of integrity protection. They increase the size of the message by at least 12.5%. Worse, they may not detect multiple errors in the same byte. While this mechanism can be extended to detect such errors by using additional parity bits, the cost is increased yet again.

Cyclic redundancy checks, or CRCs, perform the same function for larger streams of data with less overhead. CRCs are calculated by the sender using a mathematical function applied to the data to be transmitted to create a fixed size output. The CRC is appended to the transmitted data. The receiver calculates the CRC from the data stream and matches it against the CRC provided by the sender. If the two match, the data has not changed accidentally. This technique is commonly used in network protocols, such as Ethernet.

Parity bits and CRCs protect against accidental modification of data, but do not protect against an attacker. If Nanako sends a message to Toshi, he can use these techniques as protection against a noisy channel, but a knowledgeable attacker could replace or modify the message without detection.

2.1.2.2 Digitized Signatures

In the paper world, the traditional mechanism for non-repudiation is the handwritten signature. This signature indicates that the signer has written, approved, or acknowledged the contents of the paper document. A digitized signature is sometimes used as a substitute for written signatures when applications are computerized.

A digitized signature is created by scanning in a handwritten signature. When someone wishes to sign an electronic document, they simply insert the image of their signature where appropriate. When the receiver views an electronic document or message, they immediately recognize the meaning of the digitized signature.

Digitized signatures are one of the easiest mechanisms to use. If Toshi knows Nanako's signature, he will recognize it right away. However, they are also one of the easiest to subvert. Yoshiki can easily cut Nanako's digitized signature from one document and insert it into another.

Digitized signatures should not be relied upon for any security services. Digitized signatures are generally used in conjunction with a stronger mechanism to add usability.

2.1.2.3 PINs and Passwords

The traditional method for authenticating users has been to provide them with a personal identification number or secret password, which they must use when requesting access to a particular system. Password systems can be effective if managed properly, but they seldom are. Authentication that relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons. If users are allowed to make up their own passwords, they tend to choose ones that are easy to remember and therefore easy to guess. If passwords are generated from a random combination of characters, users often write them down because they are difficult to remember. Where password-only authentication is not adequate for an application, it is often used in combination with other security mechanisms.

PINs and passwords do not provide non-repudiation, confidentiality, or integrity. If Nanako wishes to authenticate to Toshi using a password, Toshi must also know it.

Since both Nanako and Toshi know the password, it is difficult to prove which of them performed a particular operation.

2.1.2.4 Biometrics

Biometric authentication relies on a unique physical characteristic to verify the identity of system users. Common biometric identifiers include fingerprints, written signatures, voice patterns, typing patterns, retinal scans, and hand geometry. The unique pattern that identifies a user is formed during an enrollment process, producing a template for that user.

When a user wishes to authenticate to the system, a physical measurement is made to obtain a current biometric pattern for the user. This pattern can then be compared against the enrollment template in order to verify the user's identity. Biometric authentication devices tend to cost more than password or token-based systems, because the hardware required capturing and analyzing biometric patterns is more complicated. However, biometrics provides a very high level of security because the authentication is directly related to a unique physical characteristic of the user which is more difficult to counterfeit. Recent technological advances have also helped to reduce the cost of biometric authentication systems.

2.1.2.5 Summary for Non-Cryptographic Security Mechanisms

Non-cryptographic mechanisms may be used to authenticate the identity of a user or verify the integrity of data that has been transmitted over a communications line. None of these mechanisms provide confidentiality or non-repudiation. In general, cryptographic security mechanisms are required to achieve confidentiality or non-repudiation.

Mechanism	Data integrity	Confidentiality	Identification and authentication	Non-repudiation
Parity bits and CRCs	Yes	No	No	No
Digitized signatures	No	No	No	No
PINs and passwords	No	No	Yes	No
Biometrics	No	No	Yes	No

Table 1. Summary for Non-Cryptographic Security Mechanisms

2.1.3 CRYPTOGRAPHIC SECURITY MECHANISMS

Cryptography is a branch of applied mathematics concerned with transformations of data for security. In cryptography, a sender transforms unprotected information (plaintext) into coded text (ciphertext). A receiver uses cryptography to either (a) transform the ciphertext back into plaintext, (b) verify the sender's identity, (c) verify the data's integrity, or some combination.

In many cases, the sender and receiver will use keys as an additional input to the cryptographic algorithm. With some algorithms, it is critical that the keys remain a secret. If Yoshiaki is able to obtain secret keys, he can pretend to be Nanako or Toshi, or read their private messages. One of the principal problems associated with cryptography is getting secret keys to authorized users without disclosing them to an attacker. This is known as secret key distribution.

2.1.3.1 Symmetric Key

Symmetric key cryptography is a class of algorithms where Nanako and Toshi share a secret key. These algorithms are primarily used to achieve confidentiality, but may also be used for authentication, integrity and limited non-repudiation.

Symmetric algorithms are ideally suited for confidentiality. Modern symmetric algorithms, such as AES, are very fast and very strong. To use a symmetric algorithm for confidentiality, Nanako transforms a plaintext message to ciphertext using a symmetric algorithm and a key. Nanako transmits the ciphertext to Toshi. Toshi uses the same key to transform the ciphertext back into the plaintext.

Symmetric algorithms can also be used to authenticate the integrity and origin of data. Nanako uses her key to generate ciphertext for the entire plaintext, as above. She sends the plaintext and a portion of the ciphertext to Toshi. This portion of the ciphertext is known as a message authentication code, or MAC. Toshi uses his copy of the key to generate the ciphertext, selects the same portion of the ciphertext and compares it to the MAC he received. If they match, Toshi knows that Nanako sent him the message. This does not provide non-repudiation, though. Nanako can deny sending the message, since Toshi could have generated it himself.

Nanako and Toshi need to share a symmetric key before Nanako encrypts or generates a MAC for a message. Establishing that shared key is called key management, and it is a difficult problem. Key management can be performed with symmetric key cryptography, but it is a classic "chicken vs. egg" problem. To use symmetric cryptography, Nanako and Toshi need to share a secret. Once Nanako and Toshi share a symmetric encryption key, the algorithm can be used to establish additional shared secrets.

In general, that first shared key must be established through "out-of-band" mechanisms. This is acceptable if Nanako communicates only with Toshi. If she communicates with a larger community, the burden of establishing each relationship becomes a serious impediment to obtaining security services.

However, this problem can become manageable through the introduction of a trusted third party (TTP). If Nanako and the party she wishes to communicate with trust the same TTP, they can get a new key for this purpose from the TTP. Each party must establish a secret out of band with the TTP as a starting point. However, Nanako will not need to repeat this process for each new party with which she communicates.

2.1.3.2 Secure Hash

2260

The secure hash function takes a stream of data and reduces it to a fixed size through a oneway mathematical function. The result is called a message digest and can be thought of as a fingerprint of the data. The message digest can be reproduced by any party with the same stream of data, but it is virtually impossible to create a different stream of data that produces the same message digest.

A message digest can be used to provide integrity. If Nanako sends a message and its digest to Toshi, he can recompute the message digest to protect against accidental changes in the data. However, this does not protect Toshi from an attacker. Yoshiki can intercept Nanako's message and replace it with a new message and the digest of the new message.

A secure hash can be used to create a hash-based message authentication code, or HMAC, if Nanako and Toshi share a secret key. If Nanako sends a message and its HMAC to Toshi, he can recompute the HMAC to protect against changes in the data from any source. Yoshiki can intercept Nanako's message and replace it with a new message, but he cannot compute an acceptable HMAC without knowing the secret key. If Toshi trusts Nanako, he may accept an HMAC as authenticating Nanako's identity. However, the services of confidentiality and nonrepudiation are not provided. The current standard for a secure hash algorithm is SHA-1. An Internet Engineering Task Force document describes an open specification for HMAC use on the internet. The RFC 2104 HMAC can be used in combination with any iterated cryptographic hash, such as MD5 and SHA-1. It also provides for use of a secret key to calculate and verify the message authentication values.

2.1.3.3 Asymmetric (public key) Cryptography

Asymmetric key cryptography, also known as public key cryptography, uses a class of algorithms in which Nanako has a private key, and Toshi (and others) have her public key. The public and private keys are generated at the same time, and data encrypted with one key can be decrypted with the other key. That is, a party can encrypt a message using Nanako's public key, then only Nanako, the owner of the matching private key, can decrypt the message. Asymmetric algorithms are poorly suited for

encrypting large messages because they are relatively slow. Instead, these algorithms are used to achieve authentication, integrity and nonrepudiation, and support confidentiality through key management. Asymmetric algorithms are used to perform three operations explained below: digital signatures, key transport, and key agreement.

Digital Signatures: Nanako can generate a digital signature for a message using a message digest and her private key. To authenticate Nanako as the sender, Toshi generates the message digest as well and uses Nanako's public key to validate the signature. If a different private key was used to generate the signature, the validation will fail.

In contrast to handwritten signatures, a digital signature also verifies the integrity of the data. If the data has been changed since the signature was applied, a different digest would be produced. This would result in a different signature. Therefore, if the data does not have integrity, the validation will fail.

In some circumstances, the digital signature can be used to establish non-repudiation. If Toshi can demonstrate that only Nanako holds the private key, Nanako cannot deny generating the signature. In general, Toshi will need to rely on a third party to attest that Nanako had the private key.

Digital signatures are also used for authentication to systems or applications. A system can authenticate Nanako's identity through a challenge-response protocol. The system generates a random challenge and Nanako signs it. If the signature is verified with Nanako's public key, it must have been signed by Nanako. This type of authentication is useful for remote access to information on a server, protecting network management from masqueraders, or for gaining physical access to a restricted area.

Key Transport: Some asymmetric algorithms can be used to encrypt and decrypt data. In practice these algorithms are never used to encrypt large amounts of data, because they are much slower than symmetric key algorithms. However, these algorithms are perfectly suited to encrypting small amounts of data – such as a symmetric key. This

operation is called key transport or key exchange, and is used in many protocols. The following example might describe an electronic mail message from Nanako to Toshi:

- Nanako generates an AES key, and encrypts the message. She encrypts the AES key using Toshi's public key, and sends both the encrypted key and encrypted message to Toshi.
- Toshi uses his private key to recover Nanako's AES key; he then uses the AES key to obtain the plaintext message.

In this case, Nanako uses asymmetric cryptography to achieve confidentiality for key distribution. This procedure does not provide any additional security services; since Nanako used Toshi's public key, anyone could have generated the message.

Key Agreement: Other asymmetric algorithms may be used for key agreement. Assume Toshi and Nanako each generated a pair of Diffie-Hellman keys. Nanako has her private key and Toshi's public key. Toshi has his private key and Nanako's public key. Through a mathematical algorithm, Nanako and Toshi both generate the same secret value. Yoshiki may have both public keys, but he cannot calculate the secret value. Nanako and Toshi can use the secret value that they independently calculated as the AES key and protect their messages.

There are forms of key agreement that provide implicit authentication as well. If Toshi can retrieve the plaintext, he knows it was encrypted by Nanako. She is the only one that could have generated the same secret value.

2.1.3.4 Summary – Cryptographic Mechanisms

Cryptographic mechanisms need to be used in concert to provide a complete suite of security services. Each class of algorithms has strengths and weaknesses.

Symmetric cryptographic algorithms, such as AES, are needed to achieve confidentiality. These algorithms can provide some degree of integrity and authentication as well, but they are poorly suited to achieve non-repudiation. The Achilles heel for symmetric algorithms, however, is key distribution.

The secure hash algorithm and the HMAC provide the basis for data integrity in electronic communications. They do not provide confidentiality, and are a weak tool for authentication or non-repudiation. The secure hash and HMAC cannot be used for key distribution, either.

Symmetric cryptographic algorithms are highly effective for integrity, authentication, and key distribution. Digital signature algorithms, such as RSA or DSA, leverage secure hash algorithms for efficiency. When leveraging a trusted third party, digital signatures can be used to provide non-repudiation. Key transport algorithms (e.g., RSA) and key agreement algorithms (e.g., Diffie-Hellman) can be used to efficiently and securely distribute symmetric keys. Once again, leveraging a trusted third party to establish the identity of the private key holder simplifies the problem.

Many applications will use these three classes of cryptographic mechanisms in concert to achieve the complete suite of security services.

Mechanism		Data integrity	Confidentiality	Identification and authentication	Non-repudiation	Key Distribution
Symmetric key cryptography	Encryption	No	Yes	No	No	No
	Message authentication :000s	yes	No	Yes	No	No
	Key transport	No	No	No	No	Yes-requires out-of-band initialization step or a TTP
Secure hash Functions	Message digest	Yes	No	No	No	No
	HMAC	Yes	No	Yes	No	No
Asymmetric cryptography	Digital signatures	Yes	No	Yes	Yes (with a TTP)	No
	Key transport	No	No	No	No	yes
	Key Agreement	No	No	Yes	No	Yes

Table 2. Summary – Cryptographic Mechanisms**2.1.4 SECURITY INFRASTRUCTURES**

To achieve the broad range of security services, Nanako and Toshi will need to use several classes of cryptographic security mechanisms in concert. In particular, to achieve confidentiality they will need to distribute symmetric encryption keys.

Distributing symmetric keys can be performed in three ways: (1) directly between the parties using symmetric encryption; (2) using symmetric encryption and a trusted third party (TTP); or (3) using public key based key management with a TTP.

The first mechanism is sufficient for small closed communities. If Nanako communicates with just three or four people, she can perform an out-of-band initialization with each party. As communities grow, this solution fails to scale, though. What if Nanako communicates with dozens of people? Now she needs a TTP to eliminate the out-of-band initialization step. The second mechanism is clearly more scalable, but it provides only limited support for authentication and does not support non-repudiation.

The third mechanism is also scalable, and it also provides a comprehensive solution. If a TTP binds the public key to a user or system – that is, attests to the identity of the party holding the corresponding private key - the complete range of security services may be obtained. The user may obtain integrity, authentication, and non-repudiation through digital signatures. Symmetric keys can be distributed using either key transport or key agreement. Those symmetric keys can be used to achieve confidentiality.

Of course, a single TTP will only scale so far. To achieve security services across organizational boundaries, many inter-linked TTPs will be required. This set of interlinked TTPs forms a security infrastructure that users can rely upon to obtain security services. When this security infrastructure is designed to distribute public keys, it is known as a public key infrastructure (PKI).

2.1.5 PUBLIC KEY INFRASTRUCTURE [6]

A public key infrastructure (PKI) binds public keys to entities, enables other entities to verify public key bindings, and provides the services needed for ongoing management of keys in a distributed system. The overall goals of modern security architectures are to protect and distribute information that is needed in a widely distributed environment, where the users, resources and stake-holders may all be in different places at different times. The emerging approach to address these security needs makes use of the scalable and distributed characteristics of public key infrastructure (“PKI”). PKI allows you to conduct business electronically with the confidence that:

- The person or process identified as sending the transaction is actually the originator.
- The person or process receiving the transaction is the intended recipient.
- Data integrity has not been compromised.

In conventional business transactions, customers and merchants rely on credit cards (e.g., VISA or MasterCard) to complete the financial aspects of transactions. The merchant may authenticate the customer through signature comparison or by checking identification, such as a driver's license. The merchant relies on the information on the credit card and status information obtained from the credit card issuer to ensure that payment will be received. Similarly, the customer performs the transaction knowing they can reject the bill if the merchant fails to provide the goods or services. The credit card issuer is the trusted third party in this type of transaction.

The same model is often applied in electronic commerce, even though the customer and issuer may never meet. The merchant cannot check the signature or request identification information. At best, the merchant can verify the customer's address against the credit card issuer's database. Again, the customer knows that they can reject the bill if the merchant fails to provide the goods or services. The credit card issuer is the trusted third party that makes consumer-to-business e-commerce possible.

With electronic commerce, customer and merchant may be separated by hundreds of miles. Other forms of authentication are needed, and the customer's credit card and financial information must be protected for transmission over the internet. Customers

who do business with a merchant over the internet must use encryption methods that enable them to protect the information they transmit to the merchant, and the merchant must protect the information it transmits back to customers. Both customer and merchant must be able to obtain encryption keys and ensure that the other party is legitimate. The PKI provides the mechanisms to accomplish these tasks.

Two parties who wish to transact business securely may be separated geographically, and may not have ever met. To use public key cryptography to achieve their security services, they must be able to obtain each other's public keys and authenticate the other party's identity. This may be performed out-of-band if only two parties need to conduct business. If they will conduct business with a variety of parties, or cannot use out-of-band means, they must rely on a trusted third party to distribute the public keys and authenticate the identity of the party associated with the corresponding key pair.

Public key infrastructure is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks. PKI integrates digital certificates, public key cryptography, and certification authorities into a complete enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

The term public key infrastructure is derived from public key cryptography, the technology on which PKI is based. Public key cryptography is the technology behind modern digital signature techniques. It has unique features that make it invaluable as a basis for security functions in distributed systems. This section provides additional background on the underlying mechanisms of a public key system.

2.1.6 PKI COMPONENTS

Functional elements of a public key infrastructure include certification authorities, registration authorities, repositories, and archives. The users of the PKI come in two flavors: certificate holders and relying parties. An attribute authority is an optional component.

A certification authority (CA) is similar to a notary. The CA confirms the identities of parties sending and receiving electronic payments or other communications.

Authentication is a necessary element of many formal communications between parties, including payment transactions. In most check-cashing transactions, a driver's license with a picture is sufficient authentication. A personal identification number (PIN) provides electronic authentication for transactions at a bank automated teller machine (ATM).

A registration authority (RA) is an entity that is trusted by the CA to register or vouch for the identity of users to a CA.

A repository is a database of active digital certificates for a CA system. The main business of the repository is to provide data that allows users to confirm the status of digital certificates for individuals and businesses that receive digitally signed messages. These message recipients are called relying parties. CAs post certificates and CRLs to repositories.

An archive is a database of information to be used in settling future disputes. The business of the archive is to store and protect sufficient information to determine if a digital signature on an "old" document should be trusted.

The CA issues a public key certificate for each identity, confirming that the identity has the appropriate credentials. A digital certificate typically includes the public key, information about the identity of the party holding the corresponding private key, the operational period for the certificate, and the CA's own digital signature. In addition, the certificate may contain other information about the signing party or information about the recommended uses for the public key. A subscriber is an individual or business entity that has contracted with a CA to receive a digital certificate verifying an identity for digitally signing electronic messages.

CAs must also issue and process certificate revocation lists (CRLs), which are lists of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates may be revoked, for example, if the owner's private key has been lost; the owner leaves the company or organization; or the owner's name changes. CRLs also document the historical revocation status of certificates. That is, a

dated signature may be presumed to be valid if the signature date was within the validity period of the certificate, and the current CRL of the issuing CA at that date did not show the certificate to be revoked.

PKI users are organizations or individuals that use the PKI, but do not issue certificates. They rely on the other components of the PKI to obtain certificates, and to verify the certificates of other entities that they do business with. End entities include the relying party, who relies on the certificate to know, with certainty, the public key of another entity; and the certificate holder, that is issued a certificate and can sign digital documents. Note that an individual or organization may be both a relying party and a certificate holder for various applications.

2.1.6.1 Certification Authorities

The certification authority, or CA, is the basic building block of the PKI. The CA is a collection of computer hardware, software, and the people who operate it. The CA is known by two attributes: its name and its public key. The CA performs four basic PKI functions: issues certificates (i.e., creates and signs them); maintains certificate status information and issues CRLs; publishes its current (e.g., unexpired) certificates and CRLs, so users can obtain the information they need to implement security services; and maintains archives of status information about the expired certificates that it issued. These requirements may be difficult to satisfy simultaneously. To fulfill these requirements, the CA may delegate certain functions to the other components of the infrastructure.

A CA may issue certificates to users, to other CAs, or both. When a CA issues a certificate, it is asserting that the subject (the entity named in the certificate) has the private key that corresponds to the public key contained in the certificate. If the CA includes additional information in the certificate, the CA is asserting the information corresponds to the subject as well. This additional information might be contact information (e.g., an electronic mail address), or policy information (e.g., the types of applications that can be performed with this public key.) When the subject of the certificate is another CA, the issuer is asserting that the certificates issued by the other CA are trustworthy.

The CA inserts its name in every certificate (and CRL) it generates, and signs them with its private key. Once users establish that they trust a CA (directly, or through a certification path) they can trust certificates issued by that CA. Users can easily identify certificates issued by that CA by comparing its name. To ensure the certificate is genuine, they verify the signature using the CA's public key. As a result, it is important that the CA provides adequate protection for its own private key.

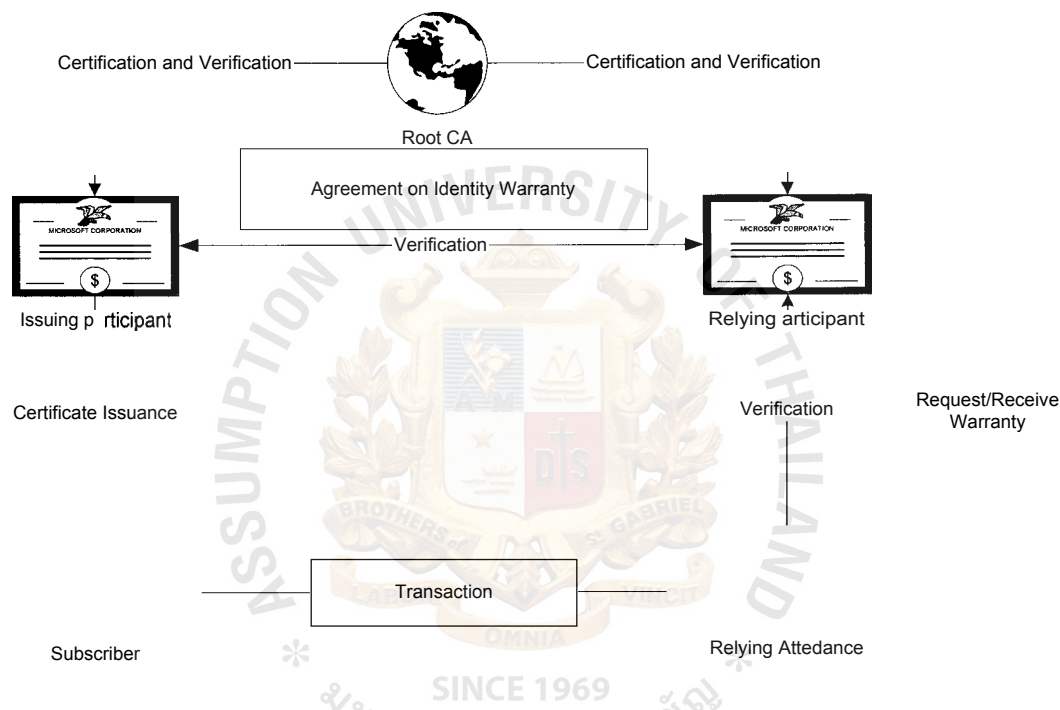


Figure 1. How CA works diagram

2.1.6.2 Registration Authorities

An RA is designed to verify certificate contents for the CA. Certificate contents may reflect information presented by the entity requesting the certificate, such as a drivers license or recent pay stub. They may also reflect information provided by a third party. For example, the credit limit assigned to a credit card reflects information obtained from credit bureaus. A certificate may reflect data from the company's Human Resources department, or a letter from a designated company official. For example,

Toshi's certificate could indicate that he has signature authority for small contracts. The RA aggregates these inputs and provides this information to the CA.

Like the CA, the RA is a collection of computer hardware, software, and the person or people who operate it. Unlike a CA, an RA will often be operated by a single person. Each CA will maintain a list of accredited RAs; that is a list of RAs determined to be trustworthy. An RA is known to the CA by a name and a public key. By verifying the RA's signature on a message, the CA can be sure an accredited RA provided the information, and it can be trusted. As a result, it is important that the RA provide adequate protection for its own private key.

2.1.6.3 PM Repositories

PKI applications are heavily dependent on an underlying directory service for the distribution of certificates and certificate status information. The directory provides a means of storing and distributing certificates, and managing updates to certificates. Directory servers are typically implementations of the X.500 standard or subset of this standard.

X.500 consists of a series of recommendations and the specification itself references several ISO standards. It was designed for directory services that could work across system, corporate, and international boundaries. A suite of protocols is specified for operations such as chaining, shadowing, and referral for server-to-server communication, and the Directory Access Protocol (DAP) for client to server communication. The Lightweight Directory Access Protocol (LDAP) was later developed as an alternative to DAP. Most directory servers and clients support LDAP, though not all support DAP.

To be useful for the PKI applications, directory servers need to be interoperable; without such interoperability, a relying party will not be able to retrieve the needed certificates and CRLs from remote sites for signature verifications. To promote interoperability among organization directories and thus PKI deployments, the PKI Technical Working Group is developing a PKI Directory Profile to assist organizations interested in participating in the demonstration effort. It is recommended that

organizations refer to this document for the minimum interoperability requirements before standing up their organization directories.

2.1.6.4 Archives

An archive accepts the responsibility for long term storage of archival information on behalf of the CA. An archive asserts that the information was good at the time it was received, and has not been modified while in the archive. The information provided by the CA to the archive must be sufficient to determine if a certificate was actually issued by the CA as specified in the certificate, and valid at that time. The archive protects that information through technical mechanisms and appropriate procedures while in its care. If a dispute arises at a later date, the information can be used to verify that the private key associated with the certificate was used to sign a document. This permits the verification of signatures on old documents (such as wills) at a later date.

2.1.6.5 PM users

PKI Users are organizations or individuals that use the PKI, but do not issue certificates. They rely on the other components of the PKI to obtain certificates, and to verify the certificates of other entities that they do business with. End entities include the relying party, who relies on the certificate to know, with certainty, the public key of another entity; and the certificate holder, that is issued a certificate and can sign digital documents. Note that an individual or organization may be both a relying party and a certificate holder for various applications.

2.1.7 PM ARCHITECTURES

Certificate holders will obtain their certificates from different CAs, depending upon the organization or community in which they are a member. A PKI is typically composed of many CAs linked by trust paths. A trust path links a relying party with one or more trusted third parties, such that the relying party can have confidence in the validity of the certificate in use.

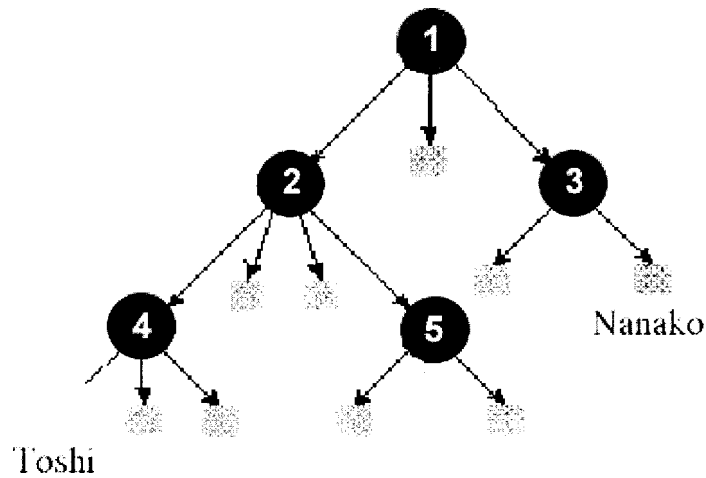
Recipients of a signed message who have no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate.

The initial challenge is deploying a PKI that can be used throughout an enterprise (e.g., a company or government organization). There are two traditional PKI architectures to support this goal, hierarchical and mesh enterprise architectures. More recently, enterprises are seeking to link their own PKIs to those of their business partners. A third approach, bridge CA architecture, has been developed to address this problem. These three architectures are described below.

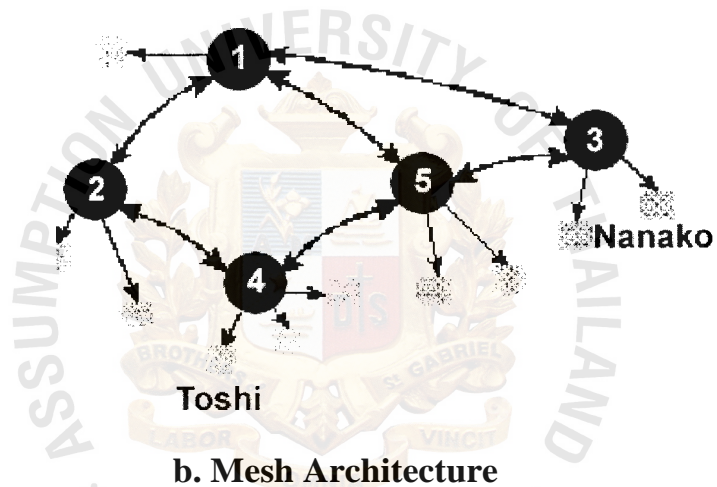
2.1.7.1 Enterprise PM Architectures

CAs may be linked in a number of ways. Most enterprises that deploy a PKI will choose either a "mesh" or a "hierarchical" architecture:

- *Hierarchical*: Authorities are arranged hierarchically under a "root" CA that issues certificates to subordinate CAs. These CAs may issue certificates to CAs below them in the hierarchy, or to users. In a hierarchical PKI, every relying party knows the public key of the root CA. Any certificate may be verified by verifying the certification path of certificates from the root CA. Nanako verifies Toshi's certificate, issued by CA 4, then CA 4's certificate, issued by CA 2, and then CA 2's certificate issued by CA 1, the root, whose public key she knows.
- *Mesh*: Independent CA's cross certify each other (that is issue certificates to each other), resulting in a general mesh of trust relationships between peer CAs. Figure 2 (b) illustrates a mesh of authorities. A relying party knows the public key of a CA "near" himself, generally the one that issued his certificate. The relying party verifies certificate by verifying a certification path of certificates that leads from that trusted CA. CAs cross certify with each other, that is they issue certificates to each other, and combine the two in a cross Certificate Pair. So, for example, Nanako knows the public key of CA 3, while Toshi knows the public key of CA 4. There are several certification paths that lead from Toshi to Nanako. The shortest requires Nanako to verify Toshi's certificate, issued by CA 4, then CA 4's certificate issued by CA 5 and finally CA 5's certificate, issued by CA 3. CA 3 is Nanako's CA and she trusts CA 3 and knows its public key.



a. Hierarchical Structure



b. Mesh Architecture

Figure 2 Traditional PM Architectures

2.1.7.2 Bridge PM Architecture

The Bridge CA architecture was designed to connect enterprise PKIs regardless of the architecture. This is accomplished by introducing a new CA, called a Bridge CA, whose sole purpose is to establish relationships with enterprise PKIs.

Unlike a mesh CA, the Bridge CA does not issue certificates directly to users. Unlike a root CA in a hierarchy, the Bridge CA is not intended for use as a trust point. All PKI users consider the Bridge CA an intermediary. The Bridge CA establishes peer-to-peer

relationships with different enterprise PKIs. These relationships can be combined to form a bridge of trust connecting the users from the different PKIs.

If the trust domain is implemented as a hierarchical PKI, the Bridge CA will establish a relationship with the root CA. If the domain is implemented as a mesh PKI, the bridge will establish a relationship with only one of its CAs. In either case, the CA that enters into a trust relationship with the Bridge is termed a principal CA.

In Figure 3, the Bridge CA has established relationships with three enterprise PKIs. The first is Toshi's and Nanako's CA, the second is Carol's hierarchical PKI, and the third is Doug's mesh PKI. None of the users trusts the Bridge CA directly. Nanako and Toshi trust the CA that issued their certificates; they trust the Bridge CA because the Fox CA issued a certificate to it. Carol's trust point is the root CA of her hierarchy; she trusts the Bridge CA because the root CA issued a certificate to it. Doug trusts the CA in the mesh that issued his certificate; he trusts the Bridge CA because there is a valid certification path from the CA that issued him a certificate to the Bridge CA. Nanako (or Toshi) can use the bridge of trust that exists through the Bridge CA to establish relationships with Carol and Doug.

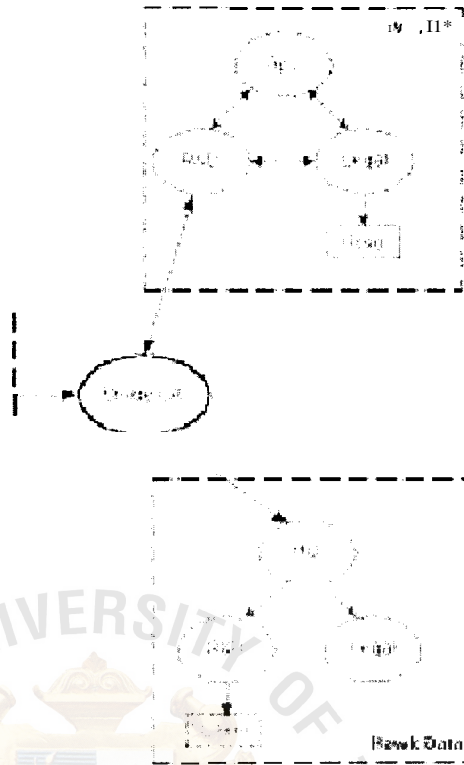


Figure 3 Bridge CA and EnterprisePKIs

2.1.7.3 Physical Architecture

There are numerous ways in which a PKI can be designed physically. It is highly recommended that the major PKI components be implemented on separate systems, that is, the CA on one system, the RA on a different system, and directory servers on other systems. Because the systems contain sensitive data, they should be located behind an organization's Internet firewall. The CA system is especially important because a compromise to that system could potentially disrupt the entire operations of the PKI and necessitate starting over with new certificates. Consequently, placing the CA system behind an additional organizational firewall is recommended so that it is protected both from the Internet and from systems in the organization itself. Of course, the organizational firewall would permit communications between the CA and the RA as well as other appropriate systems.

If distinct organizations wish to access certificates from each other, their directories will need to be made available to each other and possibly to other organizations on the Internet. However, some organizations will use the directory server for much more than simply a repository for certificates. The directory server may contain other data considered sensitive to the organization and thus the directory may be too sensitive to be made publicly available. A typical solution would be to create a directory that contains only the public keys or certificates and to locate this directory at the border of the organization - this directory is referred to as a **border directory**. A likely location for the directory would be outside the organization's firewall or perhaps on a protected DMZ segment of its network so that it is still available to the public but better protected from attack. Figure 4 illustrates a typical arrangement of PKI-related systems.

The main directory server located within the organization's protected network would periodically refresh the border directory with new certificates or updates to the existing certificates. Users within the organization would use the main directory server, whereas other systems and organizations would access only the border directory. When a user in organization A wishes to send encrypted e-mail to a user in organization B, user A would then retrieve user B's certificate from organization B's border directory, and then use the public key in that certificate to encrypt the e-mail.

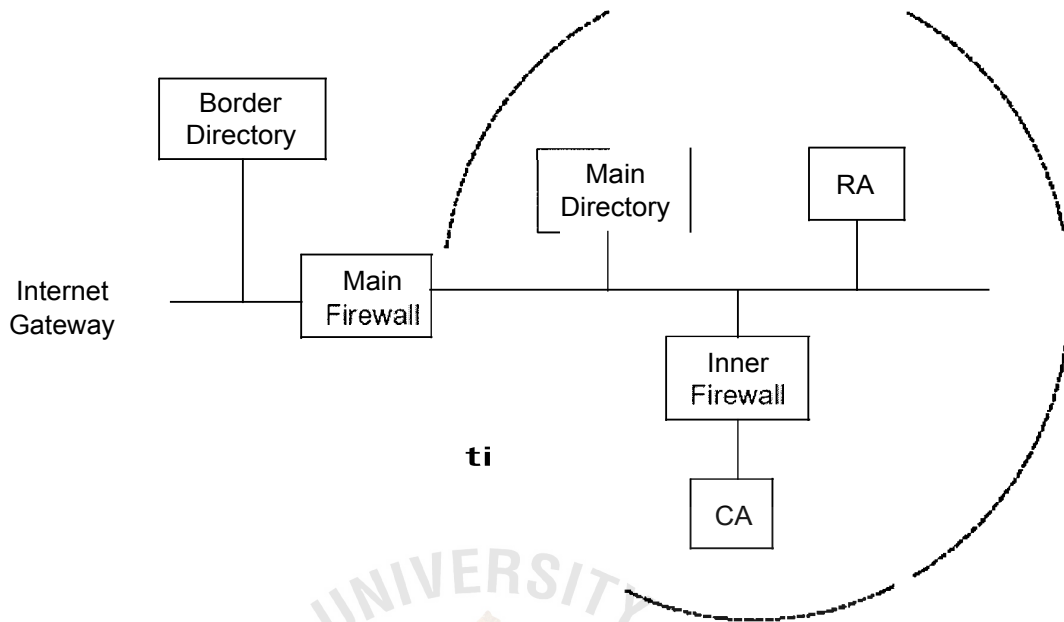


Figure 4 PM Physical Topology

2.1.8 PM DATA STRUCTURES

Two basic data structures are used in PKIs. These are the public key certificate and the certificate revocation lists. A third data structure, the attribute certificate, may be used as an addendum

2.1.8.1 X.509 Public Key Certificates

The X.509 public key certificate format has evolved into a flexible and powerful mechanism. It may be used to convey a wide variety of information. Much of that information is optional, and the contents of mandatory fields may vary as well. It is important for PKI implementers to understand the choices they face, and their consequences. Unwise choices may hinder interoperability or prevent support for critical applications.

The X.509 public key certificate is protected by a digital signature of the issuer. Certificate users know the contents have not been tampered with since the signature was generated if the signature can be verified. Certificates contain a set of common fields, and may also include an optional set of extensions.

There are ten common fields: six mandatory and four optional. The mandatory fields are: the serial number, the certificate signature algorithm identifier, the certificate issuer name, the certificate validity period, the public key, and the subject name. The subject is the party that controls the corresponding private key. There are four optional fields: the version number, two unique identifiers, and the extensions. These optional fields appear only in version 2 and 3 certificates.

Version: The version field describes the syntax of the certificate. When the version field is omitted, the certificate is encoded in the original, version 1, syntax. Version 1 certificates do not include the unique identifiers or extensions. When the certificate includes unique identifiers but not extensions, the version field indicates version 2. When the certificate includes extensions, as almost all modern certificates do, the version field indicates version 3.

Serial number: The serial number is an integer assigned by the certificate 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.

Signature: The signature field indicates which digital signature algorithm (e.g., DSA with SHA-1 or RSA with MD5) was used to protect the certificate.

Issuer: The issuer field contains the X.500 distinguished name of the TTP that generated the certificate.

Validity: The validity field indicates the dates on which the certificate becomes valid and the date on which the certificate expires.

Subject: The subject field contains the distinguished name of the holder of the private key corresponding to the public key in this certificate. The subject may be a CA, a RA, or an end entity. End entities can be human users, hardware devices, or anything else that might make use of the private key.

Subject public key information: The subject public key information field contains the subject's public key, optional parameters, and algorithm identifier. The public key in this field, along with the optional algorithm parameters, is used to verify digital signatures or perform key management. If the certificate subject is a CA, then the public key is used to verify the digital signature on a certificate.

Issuer unique ID and subject unique ID: These fields contain identifiers, and only appear in version 2 or version 3 certificates. The subject and issuer unique identifiers are intended to handle the reuse of subject names or issuer names over time. However, this mechanism has proven to be an unsatisfactory solution. The Internet Certificate and CRL profile does not recommend inclusion of these fields.

Extensions: This optional field only appears in version 3 certificates. If present, this field contains one or more certificate extensions. Each extension includes an extension identifier, a criticality flag, and an extension value. Common certificate extensions have been defined by ISO and ANSI to answer questions that are not satisfied by the common fields.

Subject type: This field indicates whether a subject is a CA or an end entity.

Names and identity information: This field aids in resolving questions about a user's identity, e.g., are “Nanako@geniasolution.com” and “c=TH; o=Assumption University; ou=Technology Management; cn=Nanako Matsushima” the same person?

Key attributes: This field specifies relevant attributes of public keys, e.g., whether it can be used for key transport, or be used to verify a digital signature.

Policy information: This field helps users determine if another user's certificate can be trusted, whether it is appropriate for large transactions, and other conditions that vary with organizational policies.

Certificate extensions allow the CA to include information not supported by the basic certificate content. Any organization may define a private extension to meet its particular business requirements. However, most requirements can be satisfied using standard extensions. Standard extensions are widely supported by commercial products. Standard extensions offer improved interoperability, and they are more cost effective than private extensions.

Extensions have three components: extension identifier, a criticality flag, and extension value. The extension identifier indicates the format and semantics of the extension value. The criticality flag indicates the importance of the extension. When the criticality flag is set, the information is essential to certificate use. Therefore, if an unrecognized critical extension is encountered, the certificate must not be used. Alternatively, unrecognized non-critical extension may be ignored.

The subject of a certificate could be an end user or another CA. The basic certificate fields do not differentiate between these types of users. The basic constraints extension appears in CA certificates, indicating this certificate may be used to build certification paths.

The key usage extension indicates the types of security services that this public key can be used to implement. These may be generic services (e.g., non-repudiation or data encryption) or PKI specific services (e.g., verifying signatures on certificates or CRLs). The subject field contains a directory name, but that may not be the type of name that is used by a particular application. The subject alternative name extension is used to provide other name forms for the owner of the private key, such as DNS names or email addresses. For example, the email address Nanako@geniasolution.com could appear in this field.

CAs may have multiple key pairs. The authority key identifier extension helps users select the right public key to verify the signature on this certificate.

Users may also have multiple key pairs, or multiple certificates for the same key. The subject key identifier extension is used to identify the appropriate public key.

Organizations may support a broad range of applications using PKI. Some certificates may be more trustworthy than others, based on the procedures used to issue them or the type of user cryptographic module. The certificate policies extension contains a globally unique identifier that specifies the certificate policy that applies to this certificate.

Different organizations will use different certificate policies. Users will not recognize policies from other organizations. The policy mappings extension converts policy information from other organizations into locally useful policies. This extension appears only in CA certificates.

The CRL distribution points extension contains a pointer to the X.509 CRL where status information for this certificate may be found. (X.509 CRLs are described in the following section.)

When a CA issues a certificate to another CA, it is asserting that the other CA's certificates are trustworthy. Sometimes, the issuer would like to assert that a subset of the certificates should be trusted. There are three basic ways to specify that a subset of certificates should be trusted:

The basic constraints extension (described above) has a second role, indicating whether this CA is trusted to issue CA certificates, or just user certificates.

The name constraints extension can be used to describe a subset of certificates based on the names in either the subject or subject alternative name fields. This extension can be used to define the set of acceptable names, or the set of unacceptable names.

The policy constraints extension can be used to describe a subset of certificates based on the contents of the policy extension. If policy constraints are implemented, users

will reject certificates without a policy extension, or where the specified policies are unrecognized.

2.1.8.2 Certificate Revocation Lists (CRLs)

Certificates contain an expiration date. Unfortunately, the data in a certificate may become unreliable before the expiration date arrives. Certificate issuers need a mechanism to provide a status update for the certificates they have issued. One mechanism is the X.509 certification revocation list (CRL).

CRLs are the PKI analog of the credit card hot list that store clerks review before accepting large credit card transactions. The CRL is protected by a digital signature of the CRL issuer. If the signature can be verified, CRL users know the contents have not been tampered with since the signature was generated. CRLs contain a set of common fields, and may also include an optional set of extensions. The CRL contains the following fields:

Version: The optional version field describes the syntax of the CRL. (In general, the version will be two.)

Signature: The signature field contains the algorithm identifier for the digital signature algorithm used by the CRL issuer to sign the CRL.

Issuer: The issuer field contains the X.500 distinguished name of the CRL issuer.

This update: The this-update field indicates the issue date of this CRL.

Next update: The next-update field indicates the date by which the next CRL will be issued.

Revoked certificates: The revoked certificates structure lists the revoked certificates. The entry for each revoked certificate contains the certificate serial number, time of revocation, and optional CRL entry extensions. The CRL entry extensions field is used

to provide additional information about this particular revoked certificate. This field may only appear if the version is v2.

CRL Extensions: The CRL extensions field is used to provide additional information about the whole CRL. Again, this field may only appear if the version is v2.

ITU-T and ANSI X9 have defined several CRL extensions for X.509 v2 CRLs. They are specified in [X509 97] and [X955]. Each extension in a CRL may be designated as critical or non-critical. A CRL validation fails if an unrecognized critical extension is encountered. However, unrecognized non-critical extensions may be ignored. The X.509 v2 CRL format allows communities to define private extensions to carry information unique to those communities. Communities are encouraged to define non-critical private extensions so that their CRLs can be readily validated by all implementations.

The most commonly used CRL extensions include the following:

The CRL number extension is essentially a counter. In general, this extension is provided so that users are informed if an emergency CRL was issued.

As noted in the previous section, CAs may have multiple key pairs. When appearing in a CRL, the authority key identifier extension helps users select the right public key to verify the signature on this CRL.

The issuer field contains a directory name, but that may not be the type of name that is used by a particular application. The issuer alternative name extension is used to provide other name forms for the owner of the private key, such as DNS names or email addresses. For example, the email address `genia@geniasolution.com` could appear in this field.

The issuing distribution points extension is used in conjunction with the CRL distribution points extension in certificates. This extension is used to confirm that this particular CRL is the one described by the CRL distribution points extension and contains status information for certificate in question. This extension is required when

the CRL does not cover all certificates issued by a CA, since the CRL may be distributed on an insecure network.

The extensions described above apply to the entire CRL. There are also extensions that apply to a particular revoked certificate.

Certificates may be revoked for a number of different reasons. The user's crypto module may have been stolen, for example, or the module may simply have been broken. The reason code extension describes why a particular certificate was revoked. The relying party may use this information to decide if a previously generated signature may be accepted. Sometimes a CA does not wish to issue its own CRLs. It may delegate this task to another CA.

The CA that issues a CRL may include the status of certificates issued by a number of different CAs in the same CRL. The certificate issuer extension is used to specify which CA issued a particular certificate, or set of certificates, on a CRL.

2.1.8.3 Attribute Certificates

The public key certificates are focused on the binding between the subject and the public key. The relationship between the subject and public key is expected to be a long-lived relationship. Most end entity certificates include a validity period of a year or two years.

Organizations seek improved access control. Public key certificates can be used to authenticate the identity of a user, and this identity can be used as an input to access control decision functions. However, in many contexts, the identity is not the criterion used for access control decisions. The access control decision may depend upon role, security clearance, group membership, or ability to pay.

Authorization information, such as membership in a group, often has a shorter lifetime than the binding of the identity and the public key. Authorization information could be placed in a public key certificate extension. However, this is not a good strategy for two reasons. First, the certificate is likely to be revoked because the authorization

information needs to be updated. Revoking and reissuing the public key certificate with updated authorization information is quite expensive. Second, the CA that issues public key certificates is not likely to be authoritative for the authorization information. This results in additional steps for the CA to contact the authoritative authorization information source.

The X.509 attribute certificate (AC) binds attributes to an AC holder. This definition is being profiled for use in Internet applications. Since the AC does not contain a public key, the AC is used in conjunction with a public key certificate. An access control function may make use of the attributes in an AC, but it is not a replacement for authentication. The public key certificate must first be used to perform authentication, then the AC is used to associate attributes with the authenticated identity.

ACs may also be used in the context of a data origin authentication service and a non-repudiation service. In these contexts, the attributes contained in the AC provide additional information about the signing entity. This information can be used to make sure that the entity is authorized to sign the data. This kind of checking depends either on the context in which the data is exchanged or on the data that has been digitally signed.

An X.509 AC resembles the X.509 public key certificate. The AC is an ASN.1 DER encoded object, and is signed by the issuer. An AC contains nine fields: version, holder, issuer, signature algorithm identifier, serial number, validity period, attributes, issuer unique identifier, and extensions. The AC holder is similar to the public key certificate subject, but the holder may be specified with a name, the issuer and serial number of a public key certificate, or the one-way hash of a certificate or public key. The attributes describe the authorization information associated with the AC holder. The extensions describe additional information about the certificate and how it may be used.

2.1.9 ADDITIONAL PM SERVICES

In addition to the security services described previously (non-repudiation, identification and authentication, confidentiality and integrity), PKIs can also offer

other services. Two important services that may be offered by a PKI are key recovery and authorization. These services are described below.

Key Recovery: If a user's key is lost, organizations and businesses must still be able to recover data that the employee had encrypted, which can only be done by recovering the encryption key. Reasons for key recovery may include an employee forgetting a password to unlock an encrypted file, the death of an employee who has encrypted some information, or someone attempting to hide criminal activity from law enforcement officials. To ensure the ability to recover encrypted data, encryption keys must be backed up and stored securely.

Note, however, that signing keys, i.e., keys used for digital signatures, should not be backed up, since doing so prevents the PKI from ensuring non-repudiation. If anyone other than a particular user has a copy of a signing key, then that user can claim that someone else supplied the signature on a contested document. If a user loses a signing key, a new key and associated certificate can be easily generated. The PKI must keep track of the user's possession of a key, but not the key itself.

Privilege/Authorization: Certificates can be used to vouch for a user's identity and also specify privileges the user has been granted. Privileges might include authority to view classified information or permission to modify material on a Web server among other privileges.

CHAPTER 3 RESEARCH METHODOLOGY

To complete this project, it took many steps and processes for doing the research of this technology and implement into the real situation as follows:

3.1 Discover the dilemma on the existing system of MOI electronic document transferred system

From the experiment in the existing system on MOI technology infrastructures, everything is quite alright except they are lacking of the security system and tools to protect the integrity and validity of the electronic documents that are flowing inside MOI network. So the dilemma occurred in the mind as "How to increase the security level in term of protecting the integrity and validity of original messages and non-repudiation for the misuse and mistake from the originator?"

3.2 Doing the research on the available technology usages

So after we got the dilemma, we try to discuss with the expert in the security field to get the questions for further researches as follows:

- Are there any technologies or solutions that are able to reduce this cause of problems or not?
- How the technologies and solutions be able to implement in every type of business?
- Are there any examples of the organization that implement this system and the result of the implementation?
- What are the advantages and disadvantages of this solution?
- What are the costs of implementation?
- etc.

These are the questions that are used for further researches from many sources that are available in the world to clarify all of the questions. The most sources of information is the secondary data that I used for doing the research on technology, such as Internet,

library, because they have the tremendous amount of these data and information available for researchers.

And after doing the research, I found that the most appropriate solution for this case of problem should be Public Key Infrastructure (PKI) that can archive and cover the requirements and dilemma of MOI quite well. (For more detail on the research, you can review them on the literatures review part)

Then we know that PKI will be the selected technology for this case, the next thing that we need to do is getting the facts and real information from MOI to know what should be planned and developed for the next phases.

3.3 Data collection from MOI system

The first thing that we need to concern about the data and information need is the data about the existing system and the flow of operation of MOI. By knowing these kinds of data and information, we are able to define the plan for the new system that should be developed in which way, can integrate with the existing system or have to develop separately or not. To get this information, we have to go directly to the technical department to see how the existing system and operations of MOI flow by using the operation map that is available at this department. When we know that how the operation inside of MOI flow in which way, the next thing that we have to gather is the existing policies, rules and laws inside MOI. This will make us understand more on the current policy that are more strictly or loosely controlled over the officers or not. The thing that we also need to know is the information about the users, nature of the users, skills on computing and networking. This will be the information that reflects the level of the security level and training that we need to concern.

All of these information that we need can be found at the information technology and technical department of MOI by contacting directly to the head officer of the department, and we will get all of the information required from them because this department already keeps all information that currently flow inside MOI. And it is the main database that contain all attributes of officers in the organization and the technology processes flow and policy of the organization.

3.4 The Scope of Respondent

For the scope of respondent in this phase of implementation of PKI, the sample respondent will be focused on the 750 MOI officers that are responsible for dealing with the electronic documents transferring. This group of respondent consists of many levels of users, from operational to top management of the organization. This group of users have their own computer that are connected to MOI network and exchanging the information over this infrastructure.

3.5 Development of guideline for MOI

After we got all of information that we need to do for analysis and development of plan to implement PKI, the next thing that we have to do is developing the guidelines that are based on the information that are available from MOI and from the researches. This guideline will be developed for MOI as the proposal of MOI to implement the solution that can help the organization reduce the cause of problems from the dilemma. This guideline can be developed for other organization also, but it may be different from MOI because the culture and nature of the each organization is different and the criteria and factors for the success also different.

CHAPTER 4 CASE STUDY ON IMPLEMENTING OF PM TECHNOLOGY

Ministry of Interior (MOI) PM Case Study

The Ministry of Interior (MOI) has authorities and responsibilities concerned with "remedies for the sufferings and nourishment for the needy" promoting and developing politics, administration, precinct administration, local administration, public registration, promoting education and earning a living, community development, internal security-keeping, public disaster prevention, keeping the peace and order of the people, land affairs, public utilities and public services, public works, penitentiary works, town and country planning and rural development.

The current operations and procedures inside MOI is still based on the traditional way of working by using papers and documents as the media for containing and exchanging the information within and outside MOI. For each document, the processing time starting from creating the document, submission for the approval, waiting for many departments approval, until the document become effective quite take a longer time than it should be. So MOI decide to migrate from the paper based system to paperless system that can save more time and cost of operation quite better than the existing system.

After MOI implement the new paperless system instead of the traditional paper based system, the operation flowed quite well and faster. The examples of documents that are flow in this system are the documents of promoting the authorities level of the officers of MOI, the documents of distribution of budget inside MOI, the documents for introducing for the new policies of MOI, etc. All of these documents contain the significant information to the officers and people that are related to MOI. But there are some risks hidden inside this effective system also.

The risk that we can see is about the security on using the electronic documents for exchanging and distribution inside the organization. The first point is the authentication of the documents. The traditional electronic documents transferring cannot guarantee and ensure the identity of the originator and information. Any person that is able to use e-mail system can be the one who create the fake e-mail of others.

The next point is confidentiality and integrity. The electronic document exchange system right now cannot be able to protect any information from the interception of intrusion during the transmission that is easy for the incorrect information and incomplete information will be handed at the destination. And the last point is the electronic document exchange system cannot provide evidence the transaction occurred, that is lacking of Non-repudiation and this will make any person be able to do the illegal things by using this system easily.

When using only electronic document exchange system is not enough to achieve the full effective operations inside the organization, so MOI has to decide the solution to solve all of these problems that maybe occurred anytime and each problem will cost a very big damage to the organization on losing the correct information that are very important for the operations inside the organization.

PM and Digital Signature is the solution

Because of the characteristics of PKI that are:

Data integrity services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.

Confidentiality services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals or processes.

Identification and authentication services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin.

Non-repudiation services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

So at this time, the very possible solution for MOI to reduce the problems on using electronic document exchange system is PKI and Digital Signature. But before MOI will make the decision on this solution, we have the guideline to implement PKI solution to make this implementation get the most effective to the organization. So we suggest all of this guideline to MOI for implementation PKI that are the following:



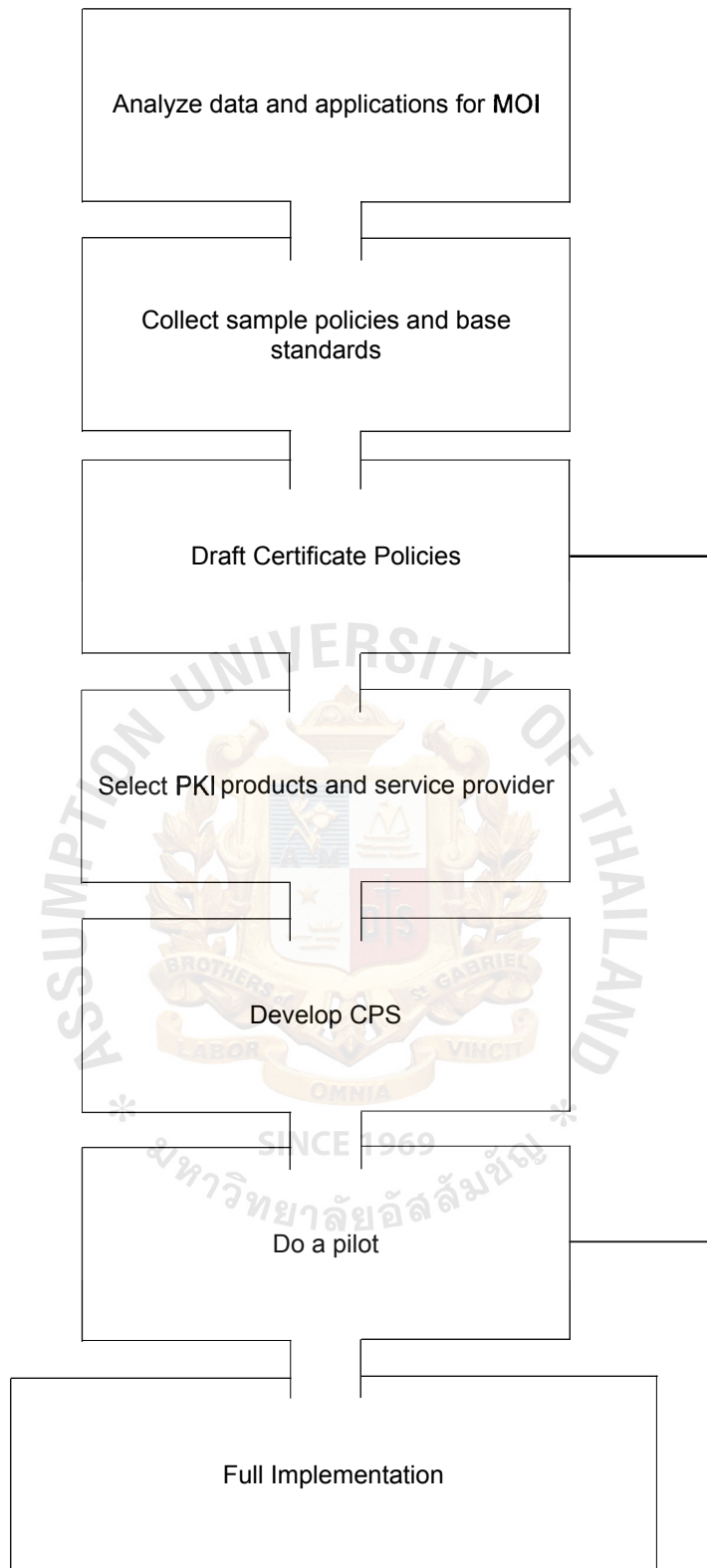


Figure 5. Process Diagram of deploying PM for MOI

4.1 ANALYZE DATA AND APPLICATIONS FOR MOI

4.1.1 The Benefit/Cost of Implementation of PM solution

This is the comparison between cost for implementation and the cost of the damage that can be occurred from the insecurity of the existing system

Infrastructure	Quantity	Cost
Root CA Server	1 unit	110,000
Backup Root CA Server	1 unit	110,000
* Subordinate CA Server	1 unit	52,500
* Backup Subordinate CA Server	1 unit	52,500
Windows 2000 Advance Server	1 unit	12,500
Training	1 time/ 150 officers	15,000
Server Room	1 unit	50,000
Administrators Salary	2 person / month	13,000*2
Maintenance / Update	1 time / year	15,000

Table 3. Cost of PM

* The number of server will depend on how many departments that organization design to be trusted under the same root policy

For the other network infrastructures that need to be used to operate PKI, we will use the existing infrastructures that are already implemented inside the organization. So we will not count it as the cost of implementing for new PKI

From the cost that occurred for implementing PKI, it costs at 402,500 for the security system that can solve the problems of the existing electronic document exchange system that take the risks of losing the significant information that can cost the organization more than 402,500 in the long term

4.1.2 Data and Applications to be protected

There are many things that we have to concern when we have to implement the new system. Data and applications is the thing that need to be considered very carefully because these things are the things that we must manage in the way that can improve the performance and effectiveness through the organization

Data: Data that we need to concern for MOI is any documents that are in the electronic format that contain the significant information for the organization. And another data that we need to concern is the historical data that are contained in the database of MOI. This data contain the huge amount of valuable resources of organization and people in Thailand, and others that are related to the transaction and operation to MOI. For example, information of citizen of Thailand also the valuable resources for business side also.

Application: The applications that we need to concern on the security in MOI include e-mail application, web browser access, and information access between workstation-to-workstation, workstation-to-server, and server-to-server. All of these activities can make the losing and damaging valuable information during the transaction is processing.

4.2 COLLECT SAMPLE POLICIES AND BASE STANDARDS

The next step is we have to collect the existing policies of the system and adopt this current policies and generate the new policies that are quite suitable for MOI because if we develop the new policies that nobody get familiar with them, the problems of misunderstand and misuse will be occurred.

4.3 DRAFT CERTIFICATE POLICY(S)

After we get all of the existing policies and adopt them to be more effective in term of suitability for organization and committee acceptance, we can generate the draft of

Certificate Policies. This is the example of the draft that we develop for MOI approval for implementation that contains eight sections inside the draft.

4.3.1 Introduction

The certificates that are used for MOI use as the tool to identify and authenticate any transactions that occurred by the people inside the organization. This mean that every officer inside MOI will have certificate for each person to identify itself and have to use it when they try to access or making the transaction via electronic media over MOI network (both inside and outside). And the person who will take care of this certificate management will be the team of certificate administration in technical department of MOI.

4.3.2 General Provisions

For MOI PKI, there are many participants that include 1 CA, 1 RA and 750 subscribers inside MOI network.

For CA, hold a central role in the PKI by acting as the repository of trust from which digital certificates derive legitimacy. Digital certificates are created, managed, administrated, and revoked by the CA.

For RA, is the people, processes, and tools used to support the registration of users within the PKI and ongoing administration, most importantly the revocation of certificates. The designated RA is responsible and liable for accurately authenticating certificate authority users. The certificate authority relies on the RA for instruction as to whom it should grant a digital certificate.

For Subscribers, they are the officers who have responsibilities to deal with electronic documents that are assigned by the top management of each subdivision.

There are many laws and rules of using PKI for MOI. But the most important rule that everyone has to recognize is the rule of non-repudiation. Because each transaction after implementing PKI will be secured and have authentication by itself, if any information

is originated from which one, they have to respond for that thing even if it is good or bad. And the punishment will be based on the regulation of MOI. But one of the immediate punishments to those officers is that certificate will be revoked and the authorities to any information inside MOI of those officers will be limited.

For any subscribers of MOI PKI will have the authorities to access, view, execute, but can't modify directly to the whole information of the originator for the every certificate.

4.3.3 Identification and Authentication

This is the process of how to identify and authenticate for the request of certificates.

To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. The delimited information to be signed is termed the message in these Guidelines. Then a hash function in the signers software computes a hash result unique (for all practical purposes) to the message. The signer's software then transforms the hash result into a digital signature using the signer's private key. The resulting digital signature is thus unique to both the message and the private key used to create it. Typically, a digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. However, it may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital signature is unique to its message, it is useless if wholly disassociated from its message.

The next step is verification of a digital signature is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks: (1) whether the digital signature was created using the corresponding private key; and (2) whether the newly computed hash result matches the original hash result which was transformed into the digital signature during the signing process. The verification software will confirm the digital signature as verified if: (1) the signer's private key was used to digitally sign the message, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a digital signature created with the signer's private key; and (2) the

message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

4.3.4 Operational Requirements

For the operation processes linkage among CA, RA, Subscribers can be described into steps as follow;

- For any subscribers, they have to submit their information that are necessary to RA for RA processing for verifying subscribers' information are valid or not. Subscribers have to use the real identities of each person to show that they are the real owner of that certificate request, such as national ID, VISA, Passport.
- After RA verify all of information from subscribers, RA have to submit these information to CA for generating the certificates for each subscriber according to these information provide from RA.
- All of information from subscriber will be kept for both CA and RA for verification and identification of the owner of each certificate.
- After CA generate certificates for subscriber, certificates will be distributed to RA for further distribution to each subscriber in the later stages.
- If the subscribers have the problem about certificate, such as changing the first name, last name or other attributes of their identity, they have to contact to their RA to change these information and then RA will submit these information to CA for processing.
- In the case of subscribers breaking the rule of using certificate, this action will be reported to CA for terminating that certificate immediately.

4.3.5 Physical, Procedural, and Personnel Security Controls

For the location of CA and RA servers, they should be put in the room that are the most secure by having the security system protect to check the authorization of officer that have authority to enter this room or not, such system as finger print system, smartcard, etc. And there should be only one or two administrators that have the responsibilities of taking care of these servers and these administrators should be the technical team of MOI that are especially expert in PKI technology and be able to solve the unstructured problem quite well because there are many things that are unpredictable that administrator should handle them effectively.

4.3.6 Technical Security Control

For the PKI system technical security, the first thing that needs to be done at the very beginning is backing up every parameter and certificates that are stored in the operating CA server and RA servers to the backup servers and run it as parallel processing. This can be the method that can handle as the disaster recovery for the case that when there are the critical problems on the operating server, we can recover it as fast as possible. And another thing that we need to concern is intrusion detection system. We need the intrusion detection system put the gate of CA server and RA server before any transactions can go to these servers because it is very risk to let any transactions go directly to CA server. So firewall maybe the way that can be used for detecting the intrusion to CA server. And antivirus tools also be needed to integrate into the servers also for protecting the antivirus threats that can damage to the PKI system.

4.3.7 Certificate and CRL Profiles

For the algorithm that MOI use for signing certificate is SHA-1 that are based for windows users and the bit length of the key is 4096 bits that is the highest number of bit that can be generated for certificate right now. The name of certificate will be the name of MOI in the full format "Ministry of Interior" and the unit that are responsible for administrative on CA is "Certificate Service" and the period of expiring will be within 2 years after the first implementation. And the location of CRL profile has to be

online after implementation also, and the URL should be <http://www.moi.go.th/CertEnroll/MOI.crl>.

4.3.8 Specification Administration

For the administration processes, if there are any needs for modification in the attributes of any certificates in CA server, the CA administrators must carefully revise the information that are getting from RA for checking the validity of those subscriber information is correct or not before having any modification. If the modification is done, the administrators have to publish the modified CRL for anyone can verify it.

4.4 SELECT PKI PRODUCT OR SERVICE PROVIDER

This step is concerning to MOI for selecting PKI product and service that are the most appropriate to the organization. There are the major players for PKI products for the implementation, Windows Based PKI, and Unix Based PKI. To select which one to be implemented should be weighted on comparison all of these criteria;

- *Compatibilities and interpretabilities with other PKI products/services:* To accomplish this criterion, the most appropriate PKI product should be Windows Based PKI because the most provider using this kind of PKI solution. So if MOI wants to join with other PKI for interoperation outside the organization in the future, Windows Based PM should be the most appropriate solution.
- *Ease to adoption to open standard:* Both Unix and Windows Based PKI right now are quite acceptable to be open standard for PKI products and services. But to be more flexible in term of open source of product that we can adapt it to enhance it later, the most appropriate solution should be Unix Based PKI.
- *Minimum proprietary API dependency:* To accomplish this criteria, Unix Based PKI is more appropriate solution because it has no dependency to the

programming interface, so any programmer can configure it out to fix, enhance the feature by coding it in the way that organization needs to be.

- *Ease of supporting applications, such as virtual private networks, access control, secure e-commerce, smartcard management, smartcards and hardware, directories, secure messaging, secure forms, enterprise, and others:* For both Unix and Windows Based PKI are able to configure it to support all of these application quite effectively, but for the easiest solution is Windows Based PKI because Windows Based PKI already integrates with Windows Operating System that support many kinds of application above, so it may be more comfortable for the user to use Windows Based PKI to support these applications.
- *Ease of deployment:* Windows Based PKI is the easiest way to deploy PKI because organization just license for Windows 2000 Advance Server, it will have the function to configure it out.
- *Flexibility of administration:* If we compare in term of easier for the administrator to manage and more comfortable to view, issue, terminate certificate, Windows Based PKI is quite more flexible. But if we compare in term of flexibility of configuration of source code for other modification of PKI system, Unix Based PKI will give this flexible to the administration.
- *Scalability and portability of installation:* Both Windows and Unix Based PKI can give the best result on this criterion.

Right now, the existing system of MOI is based on Windows based application that has Windows NT as the main server that distribute the policy to all of the users in the organization. And the requirements of MOI base more on ease of supporting applications, such as virtual private networks, access control, secure e-commerce, smartcard management, smartcards and hardware, directories, secure messaging, secure forms, enterprise, and others, and also base on flexibility of administration and ease of deployment. So the most appropriate PKI solution for MOI should be Windows

Based PKI because it can accomplish these criteria quite well and it is easier to integrate with the existing system that is based on Windows also.

4.5 DEVELOP CPS (CERTIFICATION PRACTICE STATEMENT)

4.5.1 CPS for **MOI**

After MOI committee has agreed on the policy that are the most suitable for the organization, then MOI has to set up the CA server and RA server that are configured to use for PKI services only. Then committee has to assign whom to be the administrators of these servers to take care of these servers to be well organized structure. Then all of the officers that are the subscribers of the PKI system have to fill in the application and bring the evidence that identify themselves attach with the form, such National ID, for getting the digital certificates for each person and submit this form to RA for the first verification of these information. If this information is valid, then RA will submit this information to CA for issuing the certificates. Then CA will distribute certificates back to RA for later distribution to their subscribers later. The time that these processes will be taken place will occur within 2 weeks.

After subscribers get their digital certificates, they have to use them for any transactions that are related to transfer, access to electronic documents with other officers and related parties, such as sending e-mail, access to information and databases resided in other workstations and servers, publish electronic documents on servers, according to the policy that MOI committee has set it up. If there are any violence occurred from which subscribers that can be traced from the log file of the PKI server, CA can revoke and terminate those certificates immediately without exception. If that subscribers' certificate are terminated or revoked, they have to get the punishment from the rules and laws inside MOI and not authorized to access any information inside MOI again.

4.6 DO A PILOT

So we come to the step of testing run of PKI system. These are the things that we should exercise in the step;

- Set up test accounts (users) for all application that will use the PKI: the first phase is 750 accounts that are the higher level of officers that quite have to practice how to use this system first because these people will be the management level that have to make the decision and have to command their subordinates. So this group of users should be the first pilot group and should make them understand quite clearly about the system, and how to use it.
- Test all the administration operations to make sure they all work properly: MOI committee have to evaluate the performance and understanding of these administrators on the processes and the tasks that they have to deal with.
- Shut down the system, bring it back up, and check that everything works correctly: Try to make the situation for testing the uncertainty of the system in the way that the major system is crashed and how the MOI administrators can recover it back or not and how they perform well or not.
- etc.

After the pilot test, if we see any mistake in which part of the system that can be the hole that can be opened from the hacker to break into the system, we can improve the system from the experiences of pilot testing that we can close that hole to make this PKI system as the effective security system to protect organization.

4.7 NETWORK DIAGRAM OF MOI AFTER DEPLOYING PM

In Figure 6, it demonstrates the network diagram of MOI after PKI technology is deployed.

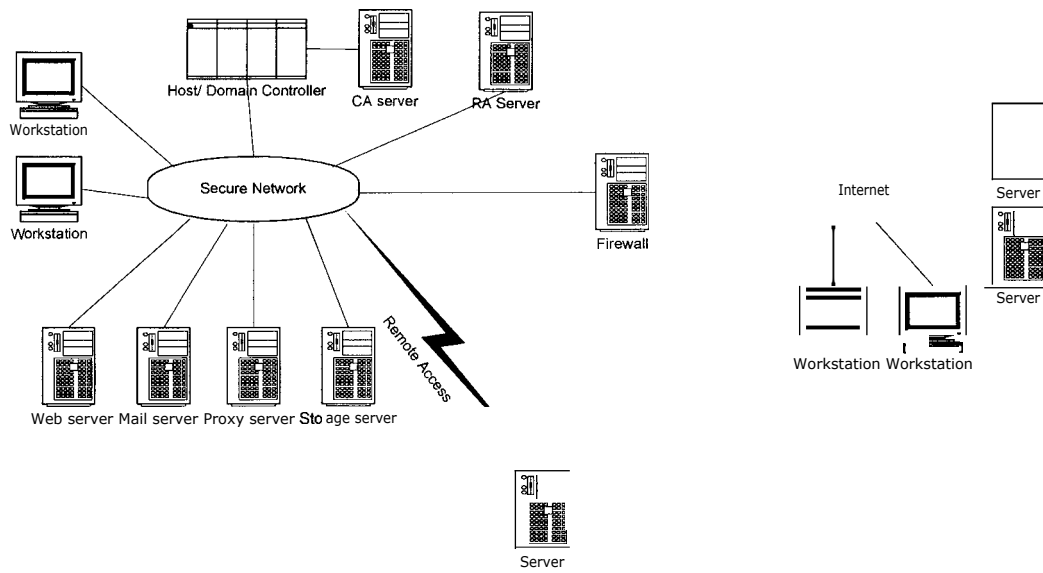


Figure 6. MOI Network Diagram with PM technology



CHAPTER 5 ANALYSIS OF PM TECHNOLOGY BEFORE DEPLOYING

5.1 External Environment Criteria

To deploy PKI in which organization, based on MOI case study, the organization should be carefully checking and evaluating that there are any criteria that the organization can take the advantages from the external environment or not, because external environment is one of the factors that influence in the success of implementation of PKI also. These are the external environment criteria that organization should be concerned.

5.1.1 *Law and regulation*

At this time, there are no any law and regulation that concern about the usage of PKI technology for the people to make people must use PKI technology attach with messages that are generated from the senders. So this can be the one weakness from the external environment that can make people ignore the usage of PKI technology and can make the violence on the usage of PKI that can be the cause of the problem that already occurred in the situation right now. So organization should be aware that the organization can not make them use PKI with 100 percents sincerity, but the organization should find the way to motivate them to use this solution and make people feel it is needed to be in their working and life. For example, the organization may set the policy that make the officer who uses PKI system for every transaction will get the reward of getting more authorized level or getting promoted in the line of control, etc.

Or the other way, if we can push the government to see the importance of PKI solution that every identity in the Internet community should have the validity, by submitting the issues about these security to the government for approval, the law and regulation of Thailand PKI maybe occur in the near future, but this solution should be widespread using in Thailand environment first and it should be successfully implemented and can show the significance over the electronic document transferring.

5.1.2 *Technology changes*

Today technology changes quite faster than previously, so the implementation right now may become obsolete in the next few months. So the organization has to consider that now the organization really has to invest in the PKI system or not or maybe use wait-and-see strategy to see that there are any other product that will substitute PKI or not. Maybe in the next few months, it may be possible that the new technology may become one-stop solution that can cover all of the problems that just only implement one solution. And maybe the new standard of security will be changed in the near future, so does the organization really need to cover that change or not, or just satisfy to protect only this problems.

5.2 Internal Environment Criteria

After we consider the external environment criteria, we also need to consider its own internal environment of the organization that is ready to serve the new system or not.

5.2.1 Officers

The officers are the most important factors that can identify that the implement of PKI successful or not because the human factors is the most difficult thing for pushing and introducing the new solution that they have never seen before to integrate into their daily lifestyle. It is like we have to make them understand more what we are trying to do for them and clarify the benefits that they will get from this system.

The officer criteria that are suitable for implementing PKI effectively must be;

- Having some computer and information technology background: because the PKI users must be able to create, view, modify, and other activities related to computerized activities quite a lot.
- Be able to handle with the changes quite well: because every officer has to change their working styles and processes according to the new policy that are published for every officer to operate it.

5.2.2 Data and information inside organization

There are many data and information that are flowing and stored inside the organization. If we compare the cost of investment of new PKI system to the cost of

operation and utilization of the existing system of the organization, in the case of MOI, we can see that the value of each message and information that are transferring inside MOI is quite worthwhile to implement PKI to protect this value of and integrity of these information.

For this criteria, if the organization does not have more information that has the big effect to the organization and these data and information are not significant enough to protect, such as, the transaction that are no longer related to the organization or the most of information that are flowing is in the format of personal use, that is no need for the organization to invest a lot of money for implementing the big solution when compared to the significance of information flow inside organization.

5.2.3 Existing infrastructure and policy

The existing infrastructure and policy can be one of the criteria that can identify the easiness and possibility of implementation of PKI system. If the existing infrastructure and policy, that is very familiar for every officers, can be able to integrate with the model of PKI solution quite well and has no need to change in the majority part of the system, it will be more beneficial to the organization because it can reduce the risk of resistance of changes to the new system from the users and easier to migrate every thing from the existing one to the new system effectively.

5.2.4 Type of Organization

For the type of organization that is suitable to implement PKI system should have these characteristics;

- Medium to large size of organization (50 officers up): because if the size of organization is quite small, the cost of investment may be not reasonable to the size of officers and the processes that are small
- Most of transactions and processes are based on paperless, client/server architecture: because PKI can support many activities that are concerned with the client/server network architecture. And PKI system will not be able to protect the integrity of information and validity of information if it is not in the electronic format.

- Data and information is more valuable: such as the financial budget information to distribute to overall organization or country, the significant information that are related to the life and job positioning of each officer, etc. If organization operations and processes are related to these information, PKI should be developed to secure these information.

5.3 Cost / Benefit

5.3.1 *What are the costs?*

When determining the total cost of implementing PKI organizations should look at several important concepts: when possible, leverage existing investments and keep the purchase of PKI in perspective. Examine the impact of costs for products, technologies, processes, people, plant (facilities) over a multiyear period. In addition businesses should scrutinize cost and investment in:

- The requirements to update and include in the overall cost the physical plant for secure computing facilities, physical security, and redundancy.
- PKI products and technologies with the inclusive maintenance and support for client software, client hardware, server software (certificate server, security server, directory services, and PKI server certificates).
- Maintenance and support for the hardware required for the PKI Server.
- The cost for implementation of key recovery for PKI and disaster planning.
- The number of people who will need to get involved in the process, and what costs are associated with those involved. Which applications will PKI be used for and who are the application owners.

5.3.2 *Applications of tangible and intangible enhancements*

Look for the right strategic fit and systems integration in business applications and processes. If PKI is used by the business can it increase revenues by:

- Improving collaboration with others, protect intellectual property, without compromise: In the arena of supply chain design and development PKI will enable strong authentication of users, private communications via encryption, and access to information at the source as well as the destination.

- Addressing customers concerns about privacy: Many corporations are looking at secure privacy for applications as a method to enhance customer base. What elements of privacy when added to legacy and new applications will address customer concerns thereby, making the customer more comfortable.
- PKI can meet the requirements of authenticity and integrity of online information, increasing the ability for employees, customers, partners and suppliers to access controlled/proprietary, copyrighted information: Distribution of copyrighted material to specific individuals can be ensured and the organizations can control the privacy of information, and protect intellectual property.
- Reducing the time it takes without reduction in integrity to process an application.
- Using strong authentication to eliminate help desk calls caused by password resets.

5.3.3 *Cost reductions*

What costs can be avoided through the use of PKI? How do organizations spend fewer dollars than before by the inclusion of PKI in existing and new processes? PKI can benefit savings and reduce cost by authentication of users, insuring the integrity and accessibility of information.

- Examine what applications a physical signature is required for and a organization can realize the direct cost saving advantages of PKI both internally and externally.
- Reductions in personnel can be realized if these benefits are applied to self-service organizations. For example, enablement of 24x7 access.
- Keep selected customers instantaneously informed about an ever-changing set of products and services specific to them and their contractual needs.
- A big return on a PKI investment can be gained through changes to help desk service. Examine the type of online customer service verses cost per transaction and ensure that the new application is as good and responsive as the legacy agent involved.

- Remote communications can realize benefits of site-to-site through secure VPN connections.
- Additionally, stronger authentication than with a user ID/password alone, easier management and administration of devices.
- Savings can be seen with a reduction in administrative staff, training costs, and improved customer service.



CHAPTER 6 DEVELOPMENT PLAN

6.1 DEPLOYING PM

PKIs will, in most cases, be developed in some degree of isolation. The PKI will be developed to meet internal requirements, where both the subscriber and the relying party are users within that organization. Adequate planning can ensure that an PKI is ready to join the broader PKI, providing access to security services with a growing community of users. This section recommends steps for setting up an PKI.

There are numerous impediments and challenges in creating an organization PKI that will interoperate with other PKI's. Some of the challenges an organization will face include the significant cost that can be associated with implementing a PKI, including the cost of creating and distributing certificates, purchasing or creating client software, and in maintaining and supporting users of the PKI. As well, different vendors may implement standards differently, and therefore interoperation of directories and other associated software between PKI's will be tricky.

6.2 ANALYZE DATA AND APPLICATIONS FOR YOUR ORGANIZATION

Installing a PKI can have a significant impact on the security model of an information technology operation. As with most security planning, the organization PKI must be designed using the familiar principles of Risk Management. Planning should begin with risk analysis. In addition to comparing the initial and operating costs of the PKI with anticipated cost-reductions, the cost-benefit analysis should attempt to identify larger risks from not implementing a PKI.

The next step is to identify the data and applications that need to be secured within the organization's computing system. Data may include data used during execution, stored data on magnetic media, printed data, archival data, update logs, audit records, and documentation.

Applications may include local/network communications, access controls, and Internet applications. The analysis should also determine the impact if security is compromised,

and the degree of risk will determine the appropriate level of assurance for the organization PKI. For example, the more limited the life of a certificate, the lower the risk exposure for the issuing CA. More than one policy may be required if there is a wide variation of risk associated with different applications.

6.3 COLLECT SAMPLE POLICIES AND BASE STANDARDS

It is efficient to begin the development of the PKI by collecting sample policies and using them as templates to develop the organization's own policy(s). Collections of standards are also required for writing your policy(s) because standards are the basis for achieving interoperability between organizations.

6.4 DRAFT CERTIFICATE POLICY(S)

The first requirement for an organization developing a PKI is to establish appropriate certificate policy(s) (CP). The policy(s) must reflect the types of applications that will be secured by the PKI. An effective strategy is to adapt and reuse existing policies to create policy(s) for the organization. Certificate policies should be at a sufficiently high level that the policies will not change too frequently.

The set of policies under which a CA issues certificates is termed its **trust domain** or **policy domain**. The organization needs to obtain an object identifier (OID) for each of the policies in its *trust domain*. These OIDs will be used to differentiate the appropriate set of applications for a particular certificate. An X.509 v3 certificate may state one or more certificate policies in the **Certificate Policy** extension. A **Certificate Policy** extension contains one or more **Policy Identifiers**. A **Policy Identifier** is a unique, registered OID that represents a certificate policy in a certificate. Applications may use these policies to decide whether or not to trust a certificate for a particular purpose. The registration process follows the procedures specified in ISO/IEC and ITU standards. The application that registers the OID also needs a textual specification of the certificate policy, for examination by certificate users and other applications. If an organization issues under a single policy, it should still obtain an OD for that policy.

6.4.1 Certificate Policies

Policies are generally written in standard format. RFC 2527, the Certificate Policy and Certification Practices Framework, defines the accepted standard CP format. RFC 2527 includes a standard outline with eight major sections and 185 second and third level subsections. Most CPs are written to this outline, since the standard format has a number of distinct advantages.

By adhering to a well-defined format, the CP writer is less likely to forget something important. It would be easy to overlook a few of the 185 topics identified in RFC 2527 if the author changed the outline. Adhering to the standard format will also simplify cross-certification with other CAs. The cross-certification process should always include a comparison of the other CA's certificate policies. This information is used to determine the contents of the policy mappings and policy constraints extensions to be included in the CA certificates. The eight major sections are summarized below;

- The **INTRODUCTION** explains how to identify certificates issued under this policy (i.e., the OID that will appear in the policy extension), defines the community for these certificates (e.g., employees, or financial managers,) and provides contact information for the people who administer the CA and maintain the policy.
- The **GENERAL PROVISIONS** captures broadly applicable legal and general practices information. For example, this section identifies the various participants in the PKI (e.g., CA, RAs, subscriber, and relying party) and their various obligations and liabilities. It identifies the applicable laws, fees, and auditing requirements. This section also describes what information (if any) will be considered confidential and the circumstances that would justify disclosure (e.g., a subpoena.).
- **IDENTIFICATION AND AUTHENTICATION** describes the procedures used to authenticate requests for certificates, or for certificate revocation.
- **OPERATIONAL REQUIREMENTS** describes the operations that must be performed by the CA, RAs, end entities, or other parties under this policy. Specific

actions are identified that must be performed when requesting or generating new certificates, revoking certificates, creating and protecting audit logs, archiving records, changing the CA's key, disaster recovery, and terminating the CA's operations.

- **PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS**

describes how the PKI uses physical security (e.g., guards, guns, and gates), procedures (e.g., separation of duty), and personnel requirements (e.g., background checks and procedures) to complement the technical security controls.

- **TECHNICAL SECURITY CONTROLS** describes the security measures used to protect cryptographic keys, protect critical security parameters (such as the list of trusted RAs), and provide quality assurance for the systems, and protect the CA from network-based attacks.

- **CERTIFICATE AND CRL PROFILES** specifies the certificate and CRL profile. This section specifies the cryptographic algorithms that will be used to sign the certificates, the length of the signing key, and the name forms that will appear in certificates. It describes the extensions that are included in certificates and CRLs.

- **SPECIFICATION ADMINISTRATION** is the final section, and it describes who the policy will be maintained. It describes the procedures that will be followed if the specification is changed, how those modifications will be published, and the approval procedures. CP authors should not develop their documents in a vacuum. CP authors should search the available CPs and identify CPs with similar scope and requirements. These CPs should be used as inputs to the CP development process.

6.5 SELECT PM PRODUCT OR SERVICE PROVIDER

The next step after planning is to select the appropriate PKI product or service provider. The organization needs to review the candidate products or service providers to determine which can implement the organization's policy(s). The following lists aspects to be considered for the selection.

- Compatibility and interoperability with other PKI products/service providers.

- Ease of adoption to open standards.
- Minimum proprietary API dependency.
- Ease of supporting applications such as virtual private networks, access control, secure e-commerce, smartcard management, smartcards and hardware, directories, secure messaging, secure forms, enterprise, and others.
- Ease of deployment.
- Flexibility of administration.
- Scalability and portability of installation.

6.6 DEVELOP CPS (CERTIFICATION PRACTICE STATEMENT)

After the selection of vendor product or service provider the organization needs to develop a highly specific document a CPS (Certification Practice Statements). A CPS is a statement of the practices that a particular CA employs in issuing certificates. A CPS describes the details of the system used and the practices employed by a CA to issue certificates, and it details the procedures used to implement the policies identified in the certificates issued by a CA, including the means used to identify certificate subjects. The CPS also states the means used to protect the private key of the CA, and the other operational practices followed by the CA to ensure security. Each CA will post its CPS in the BCA Repository, and also post the CPS in any repository associated with the CA.

6.7 DO A PILOT

PKIs are non-trivial. It is recommended that the organization starts by supporting a limited number of users and use it for internal applications first. During the pilot the following operations need to be exercised:

- Set up test accounts (users) for all application that will use the PKI.
- Test all the administration operations to make sure they all work properly.
- Shut down the system, bring it back up, and check that everything works correctly.
- Test all PKI functions of the applications locally and remotely (through network if applicable).

- Make sure that the organization has the physical security and personnel controls in place to support the PKI.
- Repeat to incorporate lessons learned.



CHAPTER 7 CONCLUSION

As organization operations are moved online, information technology security services based on cryptography become essential. Public key cryptography can play an important role in providing needed security services including confidentiality, integrity, authentication, and digital signatures. Public key cryptography uses two electronic keys: a public key and a private key.

The public key can be known by anyone while the private key is kept secret by its owner. Public key cryptography is straightforward to implement for a pair of users and a single application. This technology will scale easily to support a few applications or a small community of users. However, as the community grows, it becomes difficult to distribute the public keys and keep track of the user that owns the corresponding private key. To use public key cryptography on a broad scale, users need the support of a security infrastructure to manage public keys.

A public key infrastructure (PKI) allows public key cryptography to be employed on a broad scale. With a PKI, parties who have not met in person are able to engage in verifiable transactions. The identity of the originator of a message can be traced to the owner of the private key as long as there is strong binding between the owner and the owner's public key. A PKI provides the means to bind public keys to their owners and helps in the reliable distribution of public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable Certification Authority (CA).

A PKI is often composed of many CAs linked by trust paths. The CAs may be linked in several ways. They may be arranged hierarchically under a "root CA" that issues certificates to subordinate CAs. The CAs can also be arranged independently in a network. Recipients of a signed message with no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate.

The confidence that can be placed on the binding between a public key and its owner depends much on the confidence that can be placed on the CA that issued the certificate that binds them. Provisions in the X.509 standard enable the identification of policies that indicate the strength of mechanisms used and the do's and don'ts of certificate handling. The rules expressed by certificate policies are reflected in certification practice statements (CPSs) that detail the operational rules and system features of CAs and other PKI components. By examining the policies associated with a sender's certificate, the recipient of a signed or encrypted message can determine whether the binding between the sender and the sender's key is acceptable and thus accept or reject the message. By examining a CA's CPS, users can determine whether to obtain certificates from it, based on their security requirements. Other CAs can also use the CPS to determine if they want to cross-certify with that CA.



BIBLIOGRAPHY

- [1] Burr, W., D. Dodson, N. Nazario, W.T. Polk. *Minimum Interoperability Specification for PKI Components (MISPC), Version 1*. NIST SP 800-15. National Institute of Standards and Technology, January 1998.
- [2] Cooper, D.A. "A model of certificate revocation," Proceedings of the Fifteenth Annual Computer Security Applications Conference, pages 256-264, December 1999.
- [3] Diffie, W. M.E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, v. IT-22, n. 6, (Nov 1976), pp. 644-654.
- [4] Digital Signature Technology, *Secure Your E-Commerce Documents*.
<http://www.win2000mag.com/Articles/Index.cfm?ArticleID=4772&pg=1>,
<http://www.win2000mag.com/Articles/Index.cfm?ArticleID=4772&pg=2>
- [5] Entrust Technologies. "The PKI: Paving the Way for Secure Electronic Service Delivery," January, 2000.
- [6] Housley, R., and W.T. Polk. *Planning for PKI: Best practices for PKI Deployment*, Wiley & Sons, 2001.
- [7] Kennedy, Tim. Aligning PKI Technology and Business Goals. May 22, 2001. http://www.sans.org/infosecFAQ/encryption/PKI_tech.htm
- [8] Lee, A. *Guideline for Implementing Cryptography in the Federal Government*, NIST SP 800-21. National Institute of Standards and Technology, November, 1999.
- [9] Moses, T. "Trust Management in the Public Key Infrastructure," Entrust Technologies, January 14, 1999.
<http://www.entrust.com/resources/pdf/trustmodels.pdf>
- [10] Public-Key Infrastructure (X.509)
(pkix).<http://www.ietf.org/html.charters/pkix-charter.html>



APPENDIX A

ABBREVIATION

API - Application programming interface

ARL - Authority Revocation List

CA - Certification Authority

CP - Certificate Policy

CPS - Certification Practice Statement

CRL - Certificate Revocation List

CSOR - Computer Security Object Registry

DN - Distinguished Name

DSA - Digital Signature Algorithm

DSS - Digital Signature Standard

ECA - External certification authority

ERC - Enhanced Reliability Check

IETF - Internet Engineering Task Force

ISO - International Standards Organization

ITU - International Telecommunications Union

ITU-T - International Telecommunications Union – Telecommunications Sector

ITU-TSS - International Telecommunications Union – Telecommunications System Sector

MOA - Memorandum of Agreement

OID - Object Identifier

PIN - Personal Identification Number

PKI - Public Key Infrastructure

PKIX - Public Key Infrastructure X.509

RA - Registration Authority

RFC - Request For Comments

RSA - Rivest-Shamir-Adleman

SHA-1 - Secure Hash Algorithm, Version 1

SSL - Secure Sockets Layer

URL - Uniform Resource Locator

WWW - World Wide Web



APPENDIX B

GLOSSARY

Access - Ability to make use of any information system (IS) resource.

Access Control - Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

Accreditation - Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Activation Data - Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Applicant - The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.

Archive - Long-term, physically separate storage.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Data - Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.

Authenticate - To confirm the identity of an entity when that identity is presented.

Authentication - Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Backup - Copy of files and programs made to facilitate recovery if necessary.

Binding - Process of associating two related elements of information.

Biometric - A physical or behavioral characteristic of a human being.

Certificate - A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.

Certification Authority (CA) - An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.

Certification Authority Revocation List (CARL) - A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.

CA Facility - The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate Management Authority (CMA) - A Certification Authority or a Registration Authority.

Certification Authority Software - Key Management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CP) - A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS) - A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Certificate- Related Information - Information, such as a subscriber's postal address that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List (CRL) - A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.

Certificate Status Authority - A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Client (application) - A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Common Criteria - A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Compromise - Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Confidentiality Assurance that information is not disclosed to unauthorized entities or processes.

Cross-Certificate - A certificate used to establish a trust relationship between two Certification Authorities.

Cryptographic Module - The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Cryptoperiod - Time span during which each key setting remains in effect.

Data Integrity - Assurance that the data are unchanged from creation to reception.

Digital Signature - The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.

Dual Use Certificate - A certificate that is intended for use with both digital signature and data encryption services.

Duration - A field within a certificate that is composed of two subfields; "date of issue" and "date of next issue".

E-commerce - The use of network technology (especially the internet) to buy or sell goods and services.

Employee Any person employed by an Agency as defined above.

Encrypted Network - A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.

Encryption Certificate - A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

End Entity - Relying Parties and Subscribers.

Firewall Gateway that limits access between networks in accordance with local security policy.

High Assurance Guard (HAG) - An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

Information System Security Officer (ISSO) - Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal.

Inside threat - An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Integrity - Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property - Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intermediate CA - A CA that is subordinate to another CA, and has a CA subordinate to itself

Key Escrow - A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.

Key Exchange - The process of exchanging public keys in order to establish secure communications.

Key Generation Material - Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair - Two mathematically related keys having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Non-Repudiation - Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID) - A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.

Private Key (1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key (1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

Public Key Infrastructure (PM) - A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA) - An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate) - To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party - A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate) - The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository - A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

Responsible Individual - A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate - To prematurely end the operational period of a certificate effective at a specific date and time.

Root CA - In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Server - A system entity that provides a service in response to requests from clients.

Signature Certificate - A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA - In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscriber - A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device

Superior CA - In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

Trusted Certificate - A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trustworthy System - Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Update (a certificate) - The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate





Memorandum of Understanding

This Memorandum of Understanding ("MOU") is made and effective this the 31 August, 200 by and between Ministry of Interior (MOI) and (kmia Solution (Thailand) Co_ Ltd. ("Genia").

Genia agreed to provide free Technical Support for MOI in order to start a Certificate Authority to issues digital certificate for 750 Signees, used by Mt)1 for internal purposes.

NOW, THEREFORE, it is agreed as follows:

1. Purpose

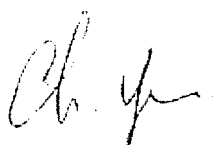
MOI and Genia agree to jointly develop in the area of IT infrastructure and I security as provided in this MOI. The purpose of the joint agreement shall be to develop a Certificate Authority for the Ministry of Interior. MOI and Genia agree to jointly develop the certificate authority and service in the area of CA infrastructure and CA security as provided in this MOU. Genia will act as the root Certificate Authority for this CA while the first party will provide the physical facilities in order to verify the identities of the signees. The CA will act as the authority to issue digital certificate for 750 signees of the Ministry of Interior. All the certificates issued by the joint party would be used for the purpose only.

Digital Certificate is an electronic tool equivalent to a sealed envelope or your signature attached to a document when you would like to submit information through the network. Certificate has a major feature in providing security and confidentiality to a message transmitted online. Business using certification service can have a confidence that they can trace the record and source or information.

MOI will provide the entire physical infrastructure and facilities in order to collect, maintain and verify all the track record of the subscribers including:

- Copy of Personal identification
- Copy of Job Identification
- Signed Certificate Subscriber Agreement (Attached Document)
- A web interface to GENIA Solution Certificate Authority server

Genia will provide all the relevant software for setting the entire infrastructure including:



A
M. J. S.

- Providing, CA key to approved individuals
- Providing, verification proof for e-commerce usage
- Providing complete integration solution for protecting all forms of critical communication including, email, electronic documents etc.
- Providing support and troubleshooting related to CA offered

2. General Duties

In connection with the joint developing of MOI's Services and Genia's Services, the parties agree to the following mutual duties

A. To include, where appropriate literature concerning the other party's services in individual direct mail or other direct marketing and online publication.

B. To provide, at the earliest practical date, information about consulting service development, or modification to existing Consulting Services jointly marketed pursuant to this Agreement.

C. To share information with respect to IT or CA business infrastructure.

D. To provide a reasonable number of samples, demonstration units or other publications of services to the other party.

E. To mention or include the other party's services in advertisements, brochures, promotion, website and press releases.

F. To share information with respect to trade shows, seminars and other events which may be beneficial to the other party.

G. To advise the other party about ideas or recommendations for new services to existing services which may be appropriate for the other party's services.

3. Specific Duties

In addition to the general duties set forth in Section 2 above, the parties agree to engage in the following specific IT infrastructure evaluation activities during the Initial Term of this Agreement:

A. Press Releases. Within thirty days of the date of this Agreement, the parties shall jointly prepare and issue a press release announcing the joint development program and generally promoting the Services. Any later press release, which refers to the other party or its services, must be approved by the other party prior to release.

B. Training. Each party agrees to provide one individual to attend a meeting of the other party for the purpose of demonstrating and training personnel with respect to the party's CA (each party) shall bear its own expenses for transportation and other out of pocket expenses for sending its representative to the other party's meeting.

Ty

4. Confidentiality

During this Agreement, each party may disclose to the other information that is confidential and proprietary to the disclosing party ("Confidential Information"). Confidential information may include, but is not limited to, business plans, marketing plans, financial statements, competitive analysis, Market research, product development plans, Computer Programs, Designs, and Models, Communicated Orally, in writing, or by electronic media. Confidential Information disclosed orally Or electronically shall be identified as such within live (5) days of disclosure. Confidential Information disclosed in writing shall be marked "Confidential". Each party agrees that it will maintain the Confidential Information of the other party in confidence and shall use such information only for the purposes of this Agreement. Confidential Information may be disclosed by a receiving party within its organization only to specific employees who have a need to know such information for the purposes of this Agreement and have agreed in writing not to disclose it. Upon expiration or termination of this Agreement or sooner if demanded by a party, the receiving Party shall return to a disclosing party any: of the disclosing party's Confidential Information all copies thereof. The obligations of each party in this section shall continue for a period of two years following the expiration or termination of this Agreement. The obligations of this section shall not apply to any Confidential Information that

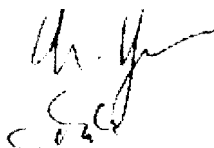
- A. Is or becomes public through no act of a receiving party,.
- B. Is or becomes fully received from a third party without obligations of confidentiality;
- C. Independently developed by a receiving party without reference to the other party's Confidential Information.

5. Payment

During the MOU period, Genia shall not incur all payment for the Technical Services rendered to it

6. Term and Termination

A. The initial term of this Agreement shall start on August 31, 2001 and shall end on August 31, 2003. At least sixty (60) days prior to the end of the Initial Term or any renewal term as provided herein, the parties shall each notify the other as to whether it desires to renew this Agreement. If either party notifies the other that it does not desire to continue this Agreement, then the Agreement shall end upon the expiration of the Initial Term or renewal term. If, however, both parties desire to renew the Agreement, then the parties shall meet to jointly determine the following:



(i) The specific duties for the renewal term in lieu of the specific duties set forth in Section 3 herein as applicable to the preceding Initial Term OF term;

(ii) The period for the renewal term; and

tin) Any other proposed amendments. If the parties agree on all of the foregoing items before end of the Initial Term or renewal term, then this Agreement shall expire ::1!; of the end of the Initial Term or the renew term. If the parties agree to all of the foregoing items, then the Agreement will continue with such specific duties and other amendments for the renewal term agreed upon.

B. his ment may be terminated at any time upon the occurrence of any f the following events:

By die reason of force majeure

Force majeure means any event the happening, or pernicious results if which could not be prevented even though it person against whom it happened or threatened to happen were to take such appropriate care :is might be expected from a person in his position and situation.

If either OF die parties shall default on any material obligation and such default is not cured within n fifteen days following notice from the other part :..

(iii) a part)... tiles a petition of bankruptcy, is insolvent, makes an assignment for benefit of creditors or trustee or receive° is appointed for a party, and 60 days.

7. Entire Agreement

This MOU supersedes any previous agreement or arrangements, whether oral or written between the parties. Only a further witting that is, duly executed by duly authorized representatives of each party may modify this Agreement

Severability

any term of this MOU held by a court of competent jurisdiction to be invalid or unenforceable, then this MOU, including 'all of the remaining, terms, will remain in full force and effect as if such invalid or unenforceable term had never been included.

9. Notice

Any notice required this MOU or given connection with it, shall be in writing and be given to the appropriate deliver\ m registered postage prepaid, or recognized overnight

If to First Party:

Ministry of Interior

Asdang Rd.

Pranakorn district, Bangk 0200

[Signature]

[Signature]

And if to Second Party:

Gema Solution (Thailand) Co., Ltd.

2330/1 Ramkhamheang 63, Hua Mark, Bang Kapi, Bangkok 10210

10. Governing Law and Language

A, This Agreement shall be governed by and construed in accordance with the laws of Kingdom of Thailand.

B. This MOU is made in the Thai language with an English translation

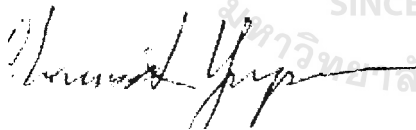
II. No Assignment

Neither Party shall assign this Agreement or any interest or obligation herein without the prior written consent of the other party.

IN WITNESS WHEREOF, this MOU has been executed by duly authorized representatives of the parties hereto on the day, month and year first above written the parties have executed this Agreement as of the date first above written.

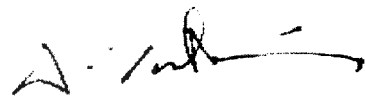
"This Agreement is made in two copies having the same contents and both parties have read and thoroughly understood the contents hereof and hereby affixed their respective signatures and seals (if any) before witnesses and each retains one copy.

MOI Signature



(Mr. Chanasak
Permanent Secretary of Interior

Gettial Signature



(l)l. Wisanu Tuntawirun)
Managing Partner

Witness



(Mr. Manoot Watanakornen)
Deputy Permanent Secretary of Interior

Witness



(Mr. Christoph Franke.)
Chief Operating Officer

Service Agreement for setting up Certificate Authority for Ministry of Interior

As the agreement for the implementation of Certificate Authority between GENIA Solution Co.,Ltd and Ministry of Interior, So GENIA Solution will assign **Mr.Teerachai Vatcharayoo**, the technical staff, as project leader to set up, and implement the PKI and Certificate Authority Solution for Ministry of Interior. This person will responsible as consultant and technical support role for this project until the end of project period. If there are any problems and questions about the solution, please contact to **Mr.Teerachai Vatcharayoo** directly.



— 

(Dr. Wisanu Tuntawiroon)
Managing Partner

St. Gabriel's Library, **Ai**

