Test Certificate Policy for the CHT V2X Public Key Infrastructure

Version 1.0.1

Executive Organization: ChungHwa Telecom Co., Ltd.
Jan 17, 2024

Version Revision Log

Version	Effective Date	Description of Revised Content
1.0	2023/12/25	first release
1.0.1	2024/01/17	delete typo at 6.1.7

CONTENTS

1. Introduction

In order to create a V2X infrastructure environment for testing, Chunghwa Telecom Co., Ltd. (hereinafter referred to as "CHT") had established the CHT V2X Public Key Infrastructure for testing (hereinafter referred to as "V2X-PKI") pursuant to IEEE 1609.2 standards. The V2X-PKI was mainly composed of trust anchor: Root Certification Authority (hereinafter referred to as the "RCA") and Subordinate Certification Authority.

In order to provide a common specification for the management of V2X-PKI certificates for testing, CHT had enacted the "Test Certificate Policy for the CHT V2X Public Key Infrastructure" (hereinafter referred to as the "Certificate Policy").

This Certificate Policy is for testing purposes only. CHT disclaims any liability that may arise from the use of this Certificate Policy.

1.1 Overview

This Certificate Policy pertains to certificates issued for testing and evaluation ONLY.

1.1.1 Certificate Policy

The Certificate Policy was enacted pursuant to the IEEE 1609.2 standards to serve as a basis for each Certification Authority to enact Certification Practice Statement. In order to ensure interoperability of the public key certificates, all of the Certificate Authorities joined the V2X-PKI shall comply with the Certificate Policy.

1.1.2 Relationship Between Certificate Policy and Certification Practice Statement

Certification Authority shall expressively state the means of compliance with the Certificate Policy in the Certification Practice Statement.

1.1.3 Certificate Policy Object Identifier Used by Certification Authority

Not applicable

1.2 Document Name and Identification

(1) Name: Test Certificate Policy for the CHT V2X Public Key Infrastructure

(2) Version: 1.0.1

(3) Announcement date: Jan 17, 2024

1.3 Primary Members

1.3.1 Certification Authority

1.3.1.1 Root Certification Authority

The Root Certification Authority is the V2X-PKI Root Certification Authority. Its main duties are described as follows:

(1) The issuance and management of self-signed certificates, self-issued certificates, cross-certificates and subordinate CA certificates.

(2) The publication of issued certificate and Certification Authority Revocation List in the repository and ensuring normal operation of the repository.

1.3.1.2 Subordinate Certification Authority

The tasks of the subordinate Certification Authority are described as follows:

(1) Intermediate Certification Authority: responsible for issuing and managing certificates for the lowest level certificate authorities.

(2) Lowest level Certification Authority: responsible for issuing and managing certificates for the subscribers.

1.3.2 Registration Authority

(1) Registration Authority is responsible for the collection and verification of subscriber identity and accuracy of related information.

(2) The Root Certification Authority shall assuming the role of a Registration Authority; subordinate Certification Authority may set up independent Registration Authority.

(3) Certification Authority shall describe the Registration Authority's operational approach in the Certification Practice Statement.

1.3.3 Subscribers

(1) Referred to the entities identified by the subject identifiers, which have possession of the certificate's public key and its corresponding private key.

(2) The Certification Authority identified by subject identifiers shall be called Subject Certification Authority instead of a subscriber.

1.3.4 Relying Party

Referred to the entity who/which trusting the subject identifier and its binding relationship with the public key and private key.

1.3.5 Other Related Members

Other organizations (such as Elector, CRL signer, MA, DC, etc.) may assist in the processing of certificate-related operations.

1.4 Certificate Usage

The relying party shall carefully evaluate various risks to choose the applicable certificate.

1.4.1 Applicability of the Certificate

Certificates issued under this certificate policy should be used for testing purposes ONLY.

1.4.2 Use Constraints on the Certificate

The relying party shall check validity of the certificate by using the certificate verification methods defined by the related international standards (such as: IEEE 1609.2, etc.).

1.4.3 Prohibited Uses of the Certificate

This Certificate Policy does not guarantee any particular level of assurance. These certificates should not be used to implement security for real-world applications.

The certificates issued by V2X-PKI Certification Authority are not permitted to be used for the following purposes:

(1) Crime;

(2) Military command and situation, and the control of nuclear, biological and chemical weapons;

(3) Other: subject to be specified by each subordinate Certification Authority.

1.5 Contact Details

1.5.1 Establishment and Administration Body of the Certificate Policy

The establishment and administration body of this Certificate Policy is Chunghwa Telecom.

1.5.2 Contact Information

E-mail address：tsaihg@cht.com.tw

1.5.3 Certification Practice Statement Review

No stipulation.

1.5.4 Procedures for the Change of Certificate Policy and Certification Practice Statement

No stipulation.

1.6 Definitions and Abbreviations

See Appendix 1 “Term Definitions”.

2 Information Publication and Repository's Responsibility

2.1 Repository

Refer to the Certification Practice Statement of each certification authority.

2.2 Publication of Certificate Information

Certification Authority shall publish the following contents in the repository:

(1) Certificate Policy and Certification Practice Statement;

(2) Certification Authority Revocation List or Certificate Revocation List;

(3) Certification Authority's certificates;

2.3 Publication Frequency or Time

Refer to the Certification Practice Statement of each certification authority.

2.4 Access Control

Certification Authority shall protection repository's information to prevent unauthorized modification.

3 Identification and Authentication

3.1 Naming

The naming of V2X-PKI certificates shall include the subject identifier.

3.1.1 Type of Names

The certificate subject identifier should comply with IEEE 1609.2. It may include the following types:

(1) LinkageData

(2) Hostname

(3) BinaryId

(4) none(NULL)

3.1.2 Need for Names to be Meaningful

No stipulation.

3.1.3 Anonymous or Fake-Name Subscribers

Certification Authority may, based on its needs, decide whether or not a subscriber can be allowed to use anonymous or fake name without stipulating the provision in the Certificate Policy.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

No stipulation.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Name Dispute Resolution Procedures

No stipulation.

3.2 Initial Registration

3.2.1 Method of Proving the Possession of Private Key

Processed according to the IEEE 1609.2.1 standard.

3.2.2 Authentication of Organization Identity

No stipulation.

3.2.3 Authentication of Individual Identity

No stipulation.

3.2.4 Unverified Subscriber Information

No stipulation.

3.2.5 Confirmation of Rights and Responsibilities

No stipulation.

3.2.6 Interoperability Standard

No stipulation.

3.2.7 Authentication of ICT Equipment or Server Application Software

No stipulation.

3.3 Identification and Authentication for Re-key Request

No stipulation.

3.3.1 Identification and Authentication for Routine Re-key

No stipulation.

3.3.2 Identification and Authentication of Re-key After Certificate Revocation

No stipulation.

3.3.3 Re-key After Certificate Renewal

Not Applicable.

3.4 Identification and Authentication of Certificate Revocation Application

No stipulation.

4 Operational Requirements in a Certificate Lifespan

4.1 Certificate Application

4.1.1 Certificate Applicant

Certificate applicants include all V2X-PKI partitipants who require certificates.

4.1.2 Registration Procedures and Responsibility

No stipulation.

4.2 Certificate Application Procedures

(1) Subordinate Certification Authority's certificate application shall be approved by its superior Certification Authority.

(2) Subscribers must follow the interface of the certificate application to the certificate authority in accordance with the IEEE 1609.2.1 standard or relevant testing protocols.

4.2.1 Performance of Identification and Authentication Functions

No stipulation.

4.2.2 Approval or Refusal of Certificate Application

Proceed in accordance with the Certificate Authority's Certification Practice Statement.

4.2.3 Processing Time for Certificate Application

No stipulation.

4.3 Certificate Issuance Procedures

4.3.1 Operation of Certification Authority

Certification Authority's issuance of certificate shall be performed by adequate role, and the Certification Authority or Registration Authority shall notify the applicant via appropriate means.

4.3.2 Certification Authority's Notification to the Certificate Applicant

Certification Authority shall specify the following particulars in the Certification Practice Statement:

(1) The means of notifying the applicant when it agrees to issue the certificate.

(2) The means of notifying the applicant when it refuses to issue the certificate.

4.4 Certificate Acceptance Procedures

4.4.1 Elements of Certificate Acceptance

No stipulation.

4.4.2 Certificate Published by Certification Authority

Certification Authority may commission Registration Authority or other organizations to transmit the certificate to its subscriber.

4.4.3 Certification Authority's Certificate Issuance Notification to Other Entities

No stipulation.

4.5 Usage of the Key Pair and Certificate

4.5.1 Subscriber's Use of Private Key and Certificate

(1) Private key shall not be used on certificate issuance.

(2) Private key shall be protected against unauthorized use or disclosure by others.

4.5.2 Relying Party's Use of Public Key and Certificate

(1) Relying party shall comply with the Certification Practice Statement provisions of each Certification Authority when using the certificate.

(2) The certificate shall be proven validity before applying in the following operations:

- To verify the integrity of electronic document's digital signature.
- To verify identity of the signatory of the document.
- To establish secure communication channel with the subscribers.

(3) Each Certification Authority shall, in the Certification Practice Statement, specify the means to verify the certificate.

4.6 Certificate Renewal

No stipulation.

4.7 Certificate's Re-key

No stipulation.

4.8 Certificate Modification

No stipulation.

4.9 Temporary Suspension and Revocation of the Certificate

(1) This V2X-PKI may provide revocation and temporary suspension service for the certificate.

(2) The revoked certificates shall be listed on the Certification Authority Revocation List or Certificate Revocation List before the next scheduled publication of the Certification Authority Revocation List or Certificate Revocation List and announced in the repository until the certificates are expired; the certificate status announcement shall include the revoked certificates.

4.9.1 Causes of Certificate Revocation

No stipulation.

4.9.2 Certificate Revocation Applicant

Certificate revocation applicant include at least the following:

(1) Certification Authority;

(2) "Subscribers" defined in Section 1.3.3.

4.9.3 Certificate Revocation Procedures

If the Certification Authority's key is proven compromised, the Certification Authority's certificate and its issued certificate shall be revoked immediately.

4.9.4 Grace Period for the Certificate Revocation Application

No stipulation.

4.9.5 Certification Authority's Processing Period for the Certificate Revocation Application

No stipulation.

4.9.6 Requirement for the Relying Party to Check the Revoked Certificate

Relying party using certificate shall, prior to the use of the certificate, enquire current Certification Authority Revocation List and Certificate Revocation List.

Relying party shall, take into consideration the risks, responsibility and affect and upon its own discretion, determine the time to obtain the certificate revocation information.

Certification Authority shall, in the Certification Practice Statement, specify the relying party's request to check the Certification Authority Revocation List or the Certificate Revocation List.

4.9.7 Frequency of Issuance of Certification Authority Revocation List and Certificate Revocation List

No stipulation.

4.9.8 Maximum Latency in the Publication of the Certification Authority Revocation list and Certificate Revocation List

No stipulation.

4.9.9 Online Certificate Revocation and Status-Checking Services

Not applicable.

4.9.10 Provisions Regarding Double-Checking the Revoked Certificate Online

Not applicable.

4.9.11 Other Forms of Revocation Announcement

No stipulation.

4.9.12 Other Special Provisions on Compromised Key

No stipulation.

4.9.13 Causes of Temporary Suspension and Reuse of a Certificate

No stipulation.

4.9.14 Applicant of Temporary Suspension and recovery of a certificate

No stipulation.

4.9.15 Procedures of Temporary Suspension and Reuse of a Certificate

No stipulation.

4.9.16 Constraints During Temporary Suspension of the Certificate

No stipulation.

4.10 Certificate Status Services

4.10.1 Service Features

Certification Authority shall provide Certification Authority Revocation List or Certificate Revocation List.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 Termination of Services

No stipulation.

4.12 Escrow and Recovery of Private Key

4.12.1 Policy and Practices for Key Escrow and Recovery

Not applicable.

4.12.2 Key Encapsulation and Recovery Policy and Practices for Communication

Not applicable.

5 Infrastructures, Security Management and Operation Procedures Controls

The purpose of this Certificate Policy is to provide a testing-oriented V2X-PKI certificate management specification. To ensure the normal operation of V2X-PKI, in addition to referencing the infrastructure, security management, and operational procedures control in this chapter, the most appropriate method can also be chosen based on actual testing requirements.

5.1 Physical Control

5.1.1 Physical Location and Structure

The physical location and structure of the machine room shall prevent unauthorized access by a combination of physical security mechanisms such as access control, security, intrusion detection, surveillance video, etc.

5.1.2 Physical Access

(1)

The certificate authorities, whose physical security mechanisms are as follows:

- Shall prevent unauthorized intrusion.
- The storage media and documents with sensitive information shall be stored in secure premises.
- Shall maintain and review access log periodically.
-

5.1.3 Electrical Power and Air Conditioning

Certification Authority shall be equipped with adequate electrical power, air conditioning and UPS with at least 6hrs of backup power.

5.1.4 Flood Prevention and Protection

Selection of Certification Authority's setup site shall take into consideration of possible flood to avoid flood damage.

5.1.5 Fire Prevention and Protection

Certification Authority shall be equipped with automatic fire detection and activate fire extinguish functions.

5.1.6 Media Storage

Certification Authority shall protect relevant storage media from accidental damage.

5.1.7 Waste Disposal

Certification Authority may specify its own waste disposal methods. The

Certificate Policy will not specify in this regard.

5.1.8 Remote Backup

Not specified.

5.2 Procedural Controls

5.2.1 Trusted Roles

Certification Authority shall, take into consideration the security and validity of the certificates, provide trusted roles to perform related tasks and adequately separate various tasks with at least 2 persons deployed on the same task.

Certification Authority shall, in the Certification Practice Statement, specify the definition of the trusted roles.

5.2.2 Number of People Required for an Individual Task

The performance of an individual task shall not be completed by a single staff. Certification Authority shall, in the Certification Practice Statement, specify the task of the trusted roles and number of people deployed to each task.

5.2.3 Identification and Authentication of Each Role

The trusted roles shall undergo identity identification and authentication operations before performing tasks.

5.2.4 Division of the Authority and Responsibility of Each Role

Certification Authority shall, in the Certification Practice Statement, specify the division of authority and responsibility of the trusted roles.

5.3 Personnel Controls

Certification Authority shall possess control over its certificate operations related personnel.

5.3.1 Background, Qualifications, Experiences and Security Cearance Requirements

Certification Authority shall undergo the identification operation on its operation related personnel and specify the qualifications, selection, supervision and auditing methods of personnel in the Certification Practice Statement.

5.3.2 Background Check Procedures

Certification Authority shall, in the Certification Practice Statement, specify the operational personnel background check procedures.

5.3.3 Training Requirements

CA personnel shall be subject to related trainings, which include at least the following contents:

(1) Certification Authority’s security certification mechanism;

(2) Software and hardware used in the Certification Authority's system;

(3) Job assignments;

(4) Post-disaster recovery and business continuity plan.

5.3.4 Personnel Retraining Requirements and Frequency

Certification Authority shall undergo personnel retraining when there are major changes such as changes in laws and regulations, software and hardware upgrades or changes in work procedures and specify the requirements and frequency in the Certification Practice Statement.

5.3.5 Job Rotation Frequency and Sequence

Certification Authority may define job rotation frequency and sequence pursuant to the Statement. The Certificate Policy will not specify in this regard.

5.3.6 Sanctions for Unauthorized Actions

Certification Authority shall, in the Certification Practice Statement, specify the means of sanctions upon personnel's violation of the provisions.

5.3.7 Provisions on Contract Personnel

Certification Authority shall, in the Certification Practice Statement, specify the provisions on hiring personnel to serve at relevant function of the Certification Authority.

5.3.8 Documentation Provided to Personnel

Certification Authority shall, in the Certification Practice Statement, specify the provision of documentations required for the relevant CA personnel to perform their business.

5.4 Procedures on Logging of Audit Trail

The certification authority should possess appropriate audit logging functions, and the audit logginging procedures should be specified in the Certification Practice Statement.

5.4.1 Type of Log

Certification Authority shall record at least the following audit trail particulars:

Certification Authority shall record at least the following audit trail particulars:

(1) Type of event;

(2) Event-causing entity or event manipulator;

(3) Event occurance site or location;

(4) Event occurance date and time;

(5) Records of successful (or unsuccessful) certificate issuance or revocation operations.

(1) Type of event;

(2) Event-causing entity or event manipulator;

(3) Event occurance site or location;

(4) Event occurance date and time;

(5) Records of successful (or unsuccessful) certificate issuance or revocation operations.

5.4.2 Frequency of Log Processing

Certification Authority shall, in the Certification Practice Statement, specify the frequency of log processing.

5.4.3 Audit Log Retention Period

CA audit log shall be kept in-situ for at least 2 months and processes pursuant to Section 5.4.4, 5.4.5, 5.4.6 and 5.5 provisions.

The audit logs shall, upon expiration of the retention period, be removed by auditor instead of any other personnel.

5.4.4 Audit Log Protection

Certification Authority shall take adequate mechanism to protect the audit logs in order to avoid unauthorized access.

Certification Authority shall, in the Certification Practice Statement, specify audit log protection method.

5.4.5 Audit Log Backup Procedures

Certification Authority shall, in the Certification Practice Statement, specify audit log backup practice.

5.4.6 Audit Log Compaction System

The audit system shall continue operation since the activation of certificate system until the certificate management system is turned off.

5.4.7 Informing the Person Who Caused the Event

The audit system does not need to inform the entity causing the event.

5.4.8 Vulnerability Assessment

Certification Authority shall, in the Certification Practice Statement, specify dically perform vulnerability assessment.

5.5 Log Archiving Methods

5.5.1 Type of Archived Logs

Certification Authority shall determine the types of archival records it wishes to use, and this certificate policy does not further specify in this regard.

Schedule 5-4 Archiving Records

5.5.2 Retention Period of Archived Logs

The retention period of archived logs shall, except for the test level, not be less than the issued duration.

Certification Authority shall, in the Certification Practice Statement, specify the method of processing the archived logs upon the expiration of retention period of archives.

5.5.3 Protection of Archived Logs

(1) The archived logs shall not be changed or deleted;

(2) The archived logs shall be stored at the location equipped with security control measures and harmless to the storage media.

(3) The archived logs may be provided to other individual or organization upon the subscriber's authorization and consent.

5.5.4 Backup Procedures for Archived Logs

Certification Authority may, at its own discretion, determine backup procedures for the archived logs based on its needs. The Certificate Policy will not specify in this regard.

5.5.5 Time-Stamping Requirements for the Archived Logs

Certification Authority may, at its own discretion, determine the time-stamping requirements for the archived logs based on its needs. The Certificate Policy will not specify in this regard.

5.5.6 Compaction System for the Archived Logs

Certification Authority may, at its own discretion, determine the compaction system for the archived logs based on its needs. The Certificate Policy will not specify in this regard.

5.5.7 Procedures on Obtaining and Verifying the Archived Logs

Certification Authority shall, in the Certification Practice Statement, specify the procedures on obtaining and verifying the archived logs.

5.6 Re-key

5.6.1 CA Re-key

(1) Certification Authority shall, pursuant to Section 6.3.2 "Usage Period of the

Subscriber's Public Key and Private Key" provisions, replacement private key periodically and make announcement.

(2) Old private key shall still be used to issue response message of the Certification Authority Revocation List, Certificate Revocation List or Online Certificate Status Protocol and maintained until all of the subscriber's certificate issued by old private key are expired.

(3) Certification Authority shall, if its own certificate is revoked, suspend its private key and replace the key pair.

(4) The Root Certification Authority shall, before the self-signed certificate expires, replace the key pair used for the issuance of subordinate CA's certificate, issue 1 new self-signed certificate, and use new / old private key to issue 1 self-issued certificate to each other. The new certificate issuance procedures are subject to Section 4.3 "Certificate Issuance Procedures" provisions.

(5) Subordinate Certification Authority shall, before the certificate expires, replace the key pair used for the issuance of certificate. The subordinate Certification Authority shall, after replaced the key pair, apply for new certificate pursuant to Section 4.2 "Certificate Application Procedures" provisions.

5.6.2 Subscriber's Re-key

(1) Subscriber's private key shall be replaced periodically pursuant to Section 6.3.2 "Usage Periods of the Public Key and Private Key" provisions.

(2) The subscriber shall, upon certificate revocation, suspend the use of its private key. If new certificate application is required, it shall be processed pursuant to Section 4.2 "Certificate Application Procedures" provisions.

(3) Certification Authority shall, in the Certification Practice Statement, specify the subscriber's re-key provisions.

5.7 Recovery Procedures When the Key is Compromised or Following A Disaster

Certification Authority's post-disaster recovery job shall be performed by recovering the repository first in order to provide certificate status information as usual.

5.7.1 Processing Procedures for Emergency and Compromised System

Certification Authority shall, in the Certification Practice Statement, specify the notifications, processing, and recovery procedures, which shall carry out exercise operation every year, for an emergency or when the system is compromised.

5.7.2 Recovery Procedures for Compromised Computer Resources, Software or Data

Certification Authority shall, in the Certification Practice Statement, specify the

recovery procedures for compromised computer resources, software or information.

5.7.3 Recovery Procedures for Compromised CA Signing Key

Certification Authority shall, in the Certification Practice Statement, specify the recovery procedures for compromised CA signing key.

5.7.4 Certification Authority's Post-Disaster On-Going Operation

Certification Authority shall, in the Certification Practice Statement, specify Certification Authority's post-disaster on-going operation.

5.7.5 Recovery Procedures for Certification Authority's Revoked Signing-Key Certificate

Certification Authority shall, in the Certification Practice Statement, specify the recovery procedures for Certification Authority's revoked signing-key certificate.

5.8 Termination of CA or RA Services

Termination of CA or RA services shall be handled pursuant to the relevant provisions of the Electronic Signatures Act.

6 Technical Security Control

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

(1) The generated private key shall be protected against access by non-authorized personnel or under unrecorded circumstances.

(2) Certification Authority shall take adequate measures to ensure the uniqueness of the subscriber's public key.

(3) The entity that generated signing private key on behalf of the subscribers shall not retention backup of that key.

(4)

6.1.2 Secure Delivery of Private Keys to Subscribers

(1) The key-generating entity shall, in addition to the generation of private key and the storage of private key in subscriber's cryptographic module, deliver the private key to the Subject via secure and auditable means.

(2) Certification Authority shall, in the Certification Practice Statement, specify the means of secure delivery of private key to the subscriber and the subscriber's means of confirming the acceptance of the private key.

6.1.3 Secure Delivery of Public Keys to the CA

Certification Authority shall, in the Certification Practice Statement, specify the means of secure delivery of public key to the Certification Authority.

6.1.4 Secure Delivery of CA Public Keys to Relying Parties

Certification Authority shall, in the Certification Practice Statement, specify the means of secure delivery of CA public key to the relying party.

6.1.5 Key Sizes

The certificate shall use NIST P-256 or other type of key with an equivalent or higher security strength.

6.1.6 Generation and Quality Check of the Public Key Parameters

Not specified.

6.1.7 Usage Purposes of Key

Not specified.

6.2 Private Key Protection and Security Control Measures for the Cryptographic Module

6.2.1 Standards and Control of Cryptographic Module

Not specified.

6.2.2 Multi-Person Control Over the Key

Not specified.

6.2.3 Escrow of Private Key

Not specified.

6.2.4 Private Key Backup

6.2.4.1 Backup of the Certification Authority's Signing Private Key

Not specified.

6.2.4.2 Backup of the Subscriber's Signing Private Key

Not specified.

6.2.5 Archive of Private Key

The signing private key shall not be archived.

6.2.6 Transmission Between Private Key and Cryptographic Module

(1) Key generation is subject to Section 6.1.1 "Key Pair Generation" provisions.

(2) Certification Authority shall, except for backup-key recovery, re-key and cryptographic module replacement, not carry out transmiission between the private key and the cryptographic module.

(3) Transmission between Certification Authority's private key and the cryptographic module can be carry out by encryption or multi-person control method; it shall not exist outside the cryptographic module in plain text form. The private key shall be input into the cryptographic module pursuant to Section 6.2.2 "Multi-Person Control Over the Key" provisions.

(4) Certification Authority shall, upon the completion of private key input, completely destroy the parameters generated during the process.

6.2.7 Storage of Private Key in Cryptographic Module

Not applicable.

6.2.8 Method of Activating Private Key

Not specified.

6.2.9 Method of Deactivating Private Key

Not specified.

6.2.10 Method of Destroying Private Key

(1)

Not specified.

6.2.11 Cryptographic Module Rating

Not specified.

6.3 Other Provisions on Key Pair Management

Not specified.

6.4 Protection for the Activation Data

6.4.1 Generation of Activation Data

(1) For the Certification Authority operates with AL 1 to AL 3 level of assurance and its subscribers, its activation data may be chosen at the subscriber's own discretion.

(2) Certification Authority operates with AL 4 level of assurance and its subscribers shall adopt security mechanisms such as subscriber's biometric value or cryptographic module.

(3) Certification Authority shall, if password is used as the activation data, comply with the information security management guidelines and related information security requirements of the Executive Yuan and its affiliates.

6.4.2 Protection for the Activation Data

Certification Authority may, at its own discretion, define the mechanism for protecting activation data based on its needs. The Certificate Policy will not specify in this regard.

6.4.3 Other Provisions for the Activation Data

Certification Authority may, at its own discretion, define other provisions for the activation data. The Certificate Policy will not specify in this regard.

6.5 Security Control Measures for the Computer Software and Hardware

6.5.1 Technical Requirements for the Security of Specific Computers

(1) Specific computer: referred to the private key storage equipment.

(2) The specific computer equipment shall be set on operating plaform that has passed the security assessment, its technical requirements for the security of specific computers are as follows:

- Login via identity authentication;
- Shall define access control method;

- ■
- ■ Ensuring the security upon every communication;
- ■ Being equipped with integrity and security control protection over the procedures.

6.5.2 Computer Security Rating

Certification Authority may, based on its needs, define the minimum standard of its computer secure rating. The Certificate Policy will not specify in this regard.

6.6 Lifespan Technical Control Measures

6.6.1 System Development Control Measures

Certification Authority may, based on its needs, define the system development control measures. The Certificate Policy will not specify in this regard.

6.6.2 Security Management Control Measures

(1) Shall record and control related system configuration and system revision history;
(2) Shall be equipped with mechanism capable of detecting unauthorized revision on CA software or configuration;
(3) Shall confirm if the software is the untempered correct version when installing the software.

6.6.3 Lifespan Security Control Measures

Certification Authority may, at its own discretion, determine the lifespan security control measures based on its needs. The Certificate Policy will not specify in this regard.

6.7 Network Security Control Measures

Certification Authority shall, in the Certification Practice Statement, specify network security control measures.

6.8 Time Stamps

Certification Authority may, at its own discretion, determine the related provisions for time-stamping based on its needs. The Certificate Policy will not specify in this regard.

6.9 Security Control Measures for the Cryptographic Module

Not specified.

7 Certificate, Certificate Revocation List and Online Certificate Status Protocol Profiles

7.1 Certificate Profile

The Certificate Profile issued by the V2X-PKI Root Certification Authority follows the IEEE 1609.2 standard. Detailed certificate fields and content will be defined in the Certificate Practice Statement.

7.1.1 Version Number Field

Certification Authority shall issuance IEEE Std 1609.2-2020 certificates.

7.1.2 Certificate Type Field

This field determines whether this certificate type is an explicit certificate or an implicit certificate, and must comply with the specifications outlined in the certificate profile.

7.1.3 Certificate Issuer Field

This field represents either the self-signed certificate or the HashedId8 value of the Certification Authority certificate that issued this certificate. It must comply with the specifications outlined in the certificate profile.7.1.4 ToBeSigned Field

The ToBeSigned field contains numerous subfields and must adhere to the IEEE 1609.2 standard. However, the subfields vary depending on the certificate type and must comply with the specifications outlined in the certificate profile.

7.1.5 Signature Field

This field represents the signature generated by the Certification Authority for the content of the certificate to be signed. If the certificate type is explicit, this signature value field must be included; otherwise, it can be omitted.

Certificate shall not include “policy qualifier”.

7.1.9 Semantic Processing for Critical Certificate Policy Extension Fields

The semantic processing for critical Certificate Policy extension fields shall comply with “Government Public Key Infrastructure Certificate and Certificate Revocation List Profile” provisions.

7.2 Certification Authority Revocation List and Certificate Revocation List Profile

The Certification Authority Revocation List and Certificate Revocation List Profile issued by the V2X-PKI Root Certification Authority follows the IEEE 1609.2 standard. Detailed certificate revocation list fields and content will be defined in the Certificate Practice Statement.

7.3 Online Certificate Status Protocol profile

Certification Authority shall, if it provides the Online Certificate Status Protocol enquiry service, specify in the Certification Practice Statement regarding the service version number and the standard used on the extension fields; the response message shall add digital signature.

The Certification Authority only provides the Certification Authority Revocation List and Certificate Revocation List Profile and does not offer the Online Certificate Status Protocol enquiry service.

7.3.1 Version Number

Not applicable.

7.3.2 Extension Fields of the Online Certificate Status Protocol

Not applicable.

8 Audit Methods

The purpose of this Certificate Policy is to provide a testing V2X-PKI certificate management specification. To ensure the compliance of the Certification Authority's operations, the Certification Authority will conduct regular self-audits. In addition to referring to the audit methods provided in this chapter, the certificate authority may also choose the most appropriate audit method based on actual testing requirements.

8.1 Audit Frequency or Assessment Particulars

Certification Authority shall be subject to periodic audit to ensure its capability for effective security certificate management.

Certification Authority shall conduct audit on its subordinate Certification Authority and the Registration Authority on a regular basis and as-needed basis to ensure its compliance with the operation of the Certification Practice Statement.

8.2 Identity and Qualifications of the Audit Personnel

The auditors shall be independent of the audited Certification Authority, who can be served by the following entities:

(1) A just third-party;

(2) Another independent entity that is different from the audited Certification Authority In terms of organizational division.

The auditors shall provide just and independent assessment. Its qualifications shall be approved by the Certification Authority’s competent authority, and it shall be familiar with provisions relating to the Certification Authority’s certificate issuance and management. Certification Authority shall perform identity identification on the auditors before the audit.

8.3 Relationship Between the Audit Personnel and the Audited Party

In addition to the provision where the auditors shall be independent of the audited Certification Authority, its qualifications shall be pursuant to Section 8.2 “Identity and Qualifications of the Audit Personnel” provisions.

8.4 Scope of Audit

The scope of audit is prescribed as follows:

(1) Check if the Certification Authority comply with the operation of the Certification Practice Statement;

(2) Check if the Certification Authority’s Certification Practice Statement comply with

regulations of the Certificate Policy.

The auditors shall carry out audit on the operation maintenance units such as the Registration Authority of the Certification Authority. If the Certification Authority entered into Cross-Certification Agreement with its subordinate Certification Authority, the scope of audit shall cover that subordinate Certification Authority to see whether it complies with the provisions of the Cross-Certification Agreement.

8.5 Ways to Cope with Audit Results

The auditors shall, if the Certification Authority's setup and operation maintenance are found non-conforming with the Certificate Policy or provisions of the Cross-Certification Agreement, take the following actions:

(1) The auditors shall record non-conforming circumstances;

(2) The auditors shall notify the occurance of non-conforming circumstances to the Certification Authority's competent authority.

The Certification Authority having non-conforming circumstances shall perform correction based on the audit report, Certificate Policy or provisions of the Cross-Certification Agreement.

For the Certification Authority non-conforming with the audit standard requirements, the Certification Authority's competent authority may require it to show improvement within a certain period of time or take other necessary measures.

8.6 Scope of Disclosure of Audit Results

The certificate information trusted by the relying party shall be publicly available unless such information may lead to system security risks or subject to Section 9.3 "Confidentiality of Business Information" provisions.

Certification Authority shall publish the latest audit results.

9 Other Business and Legal Particulars

9.1 Fees

Certification Authority may, based on its business needs, determine whether or not it shall charge fees on certificate related operation. The Certificate Policy will not specify in this regard.

9.1.1 Certificate Issuance and Renewal Fees

Certification Authority may, at its own discretion, determine the certificate issuance and certificate renewal fees. The Certificate Policy will not specify in this regard.

9.1.2 Certificate Enquiry Fee

Certification Authority may, at its own discretion, determine the certificate enquiry fee. The Certificate Policy will not specify in this regard.

9.1.3 Certificate Revocation and Status Enquiry Fees

Certification Authority may, at its own discretion, determine the certificate revocation and certificate status enquiry fees. The Certificate Policy will not specify in this regard.

9.1.4 Other Service Charges

Certification Authority may, at its own discretion, determine other service fees. The Certificate Policy will not specify in this regard.

9.1.5 Refund Request Procedures

Certification Authority may, at its own discretion, determine the refund application procedures. The Certificate Policy will not specify in this regard.

9.2 Financial Responsibility

Certification Authority may plan for its financial insurance responsibility based on its business concern. The Certificate Policy will not specify in this regard.

9.2.1 Scope of Insurance

Certification Authority may, at its own discretion, determine the scope of financial insurance for its certificate services. The Certificate Policy will not specify in this regard.

9.2.2 Other Assets

Certification Authority may, at its own discretion, determine the financial responsibility of other assets. The Certificate Policy will not specify in this regard.

9.2.3 Insurance or Warranty Responsibility to End Entity

Certification Authority may, at its own discretion, determine its insurance or warranty responsibility to the end entity. The Certificate Policy will not specify in this regard.

9.3 Confidentiality of Business Information

9.3.1 Scope of Sensitive Information

Certification Authority shall, in the Certification Practice Statement, specify the scope and type of sensitive information, which shall be handled pursuant to the relevant laws and regulations.

9.3.2 Scope of Non-Sensitive Information

Certification Authority shall, in the Certification Practice Statement, specify the scope and type of non-sensitive information.

9.3.3 Responsibility in the Protection of Sensitive Information

Certification Authority shall, in the Certification Practice Statement, specify the responsibility in the protection of sensitive information.

9.4 Privacy Nature of Personal Information

9.4.1 Privacy Protection Plan

Certification Authority shall, in the Certification Practice Statement, specify personal data protection and privacy statement.

9.4.2 Type of Private Information

Certification Authority shall, in the Certification Practice Statement or website, specify the type of private information.

9.4.3 Non-Private Information

Certification Authority shall, in the Certification Practice Statement, specify the type of non-private information.

9.4.4 Responsibility in the Protection of Private Information

Certification Authority shall, in the Certification Practice Statement, specify the responsibility in the protection of private information.

9.4.5 Announcement and Consent in the Use of Private Information

Certification Authority shall, in the Certification Practice Statement, specify the regulation regarding the use of private information.

9.4.6 Information Released Due to Judicial or Administrative Procedures

Certification Authority shall, in the Certification Practice Statement, specify the regulation relating to the provisions of private information to judicial personnel.

9.4.7 The Release of Other Information

Certification Authority shall, in the Certification Practice Statement, specify the regulation relating to the provisions of other information, which shall be handled pursuant to the relevant laws and regulations.

9.5 Intellectual Property Rights

The intellectual property rights of the Certificate Policy is owned by CHT. The related information can be downloaded from the Root Certification Authority's repository or be reproduced or distributed pursuant to the related provisions of the copyright law, provided that, the copy shall be complete and specify the copyright ownership. In addition, the reproduction or distribution of the Certificate Policy shall not involve fees charged on others and shall not refuse anybody's request in obtaining the Certificate Policy. CHT will not be bear any legal liability for any problem arising from the inproper use or distribution of the Certificate Policy.

9.6 Duties and Obligations

9.6.1 Certification Authority's Duties and Obligations

Certification Authority's duties and obligations shall include at least the following particulars:

(1) To comply with the Certificate Policy's provisions;

(2) To perform the identification and authentication on certificate application;

(3) To issue and publish certificates;

(4) To revoke certificates;

(5) To issuce and publish the Certification Authority Revocation List or the Certificate Revocation List;

(6) To issue and provide response message for the Online Certificate Status Protocol enquiry service;

(7) To securely generate CA private keys;

(8) To protect CA private keys;

(9) To publish the Certification Practice Statement and specify the subscriber's and relying party's responsibilities.

9.6.2 Registration Authority's Duties and Obligations

Registration Authority's duties and obligations shall include at least the following particulars:

(1) To provide certificate application service;

(2) To inform the subscriber's and relying party's regarding the obligations and responsibility of the Certification Authority and Registration Authority;

(3) To manage the Registration Authority's private keys;

(4) The Registration Authority shall not use the RA private key in the operation outside the scope registered in the certificate without its superior Certification Authority's consent.

9.6.3 Subscriber's Obligations

The subscriber's obligations shall include at least the following particulars:

(1) To provide accurate and complete information;

(2) To comply with relevant provisions of the Certificate Policy and the Certification Practice Statement;

(3) To safeguard and use the private key appropriately;

(4) To promptly notify the Certification Authority and suspend the certificate when the private key is used without its consent, compromised or lost;

(5) To securely generate its private key and avoid been compromised.

9.6.4 Relying Party's Obligations

The relying party's obligations shall include at least the following particulars:

(1) To use the certificate pursuant to the certificate and the certificate's assurance level and applicability;

(2) To ensure a secure environment for the use of the certificate and bear the responsibility not attributable to the Certification Authority;

(3) Relying party shall, when the Certification Authority cannot operate normally, seek other means to complete its legal acts with others at its earliest convenience and shall not use Certification Authority's failure to operate normally as the reason in dispute with others.

9.6.5 Other Participant's Obligations

Certification Authority may, at its own discretion, determine other participants' obligations. The Certificate Policy will not specify in this regard.

9.7 Disclaimer

Certification Authority shall, in the Certification Practice Statement, specify disclaimer and its constraints, provided that, the consequences attributable to its own negligence shall not be included in the disclaimer.

9.8 Responsibility and Constraints

Certification Authority shall, in the Certification Practice Statement, specify the responsibility and constraints. Certification Authority shall, if there is any issuance SSL certificate, comply with the requirements of the official version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" Published by CA/Browser

Forum.

9.9 Indemnity

Certification Authority shall, in the Certification Practice Statement, specify the indemnity responsibility to the subscribers and relying party, which shall be in compliance with the Electronic Signatures Act and the related laws and regulations.

9.10 Expiration Date and Termination

Certification Authority shall, in the Certification Practice Statement, specify the expiration date and termination.

9.10.1 Expiration Date

This Certificate Policy and its Appendix are effective upon announcement on the GPKI website and repository.

9.10.2 Termination

The termination of Certificate Policy becomes effective upon announcement on the website and repository.

9.10.3 Termination and Duration Effects

After the termination of this Certificate Policy, the validity of the certificate shall expire.

9.11 Individual Notification and Communication with the Participants

Individual notification and communication with the participants shall be carried out by appropriate means.

9.12 Revision

Certification Authority may, at its own discretion, determine the minimum annual review frequency for Certificate Policies and the number of reviews for Certification Practice Statement. The Certificate Policy will not specify in this regard.

9.12.1 Revision Procedures

The Certificate Policy amendment is subject to the review before promulgation.

9.12.2 Notification Mechanism and Deadline

Certification Authority shall announce any modifications that may cause major impact on the subscribers in the repository. Certification Authority shall, in the Certification Practice Statement, specify the notification mechanism and announcement period for the modifications.

9.12.3 Causes for the Revision of Certificate Policy Object Identifier

Not applicable. This is due to the Certificate Policy Object Identifier not being

documented in the IEEE 1609.2 certificate format.

9.13 Dispute Processing Procedures

Certification Authority shall, in the Certification Practice Statement, specify the dispute processing procedures.

9.14 Governing Law

GPKI shall be subject to the laws of the Republic of China in performing its business.

9.15 Applicable Laws

GPKI shall perform its business pursuant to the relevant laws and regulations. Certification Authority shall, in the Certification Practice Statement, specify the applicable laws.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Certification Authority may, at its own discretion, determine the entire agreement with the contracting party of its Certification Practice Statement. The Certificate Policy will not specify in this regard.

9.16.2 Assignment

Certification Authority shall, in the Certification Practice Statement, specify the provisions regarding the assignment of primary member's right or responsibility.

9.16.3 Severability

The Certificate Policy shall remain valid even when any of its sections becomes not applicable and subject to amendment.

(1)

9.16.4 Contract Performance

Whereas the subscriber or the relying party violates the relevant provisions of the Certificate Policy, causing the CHT Root Certification Authority to suffer damages, if the responsibility is attributable to the subscriber or the relying party's intentional act or negligent, the CHT Root Certification Authority may, in addition to claiming for compensation, ask either of the attributable parties to pay for the attorney's fees associated with the dispute or litigation process.

The CHT Root Certification Authority's hold back on claiming its rights from the one who violated the Certificate Policy does not mean that the CHT Root Certification Authority waived the right to claim its rights in any subsequent or future violation against the Certificate Policy.

9.16.5 Force Majeure

The Certification Authority shall not be held liable for any damages caused by force majeure and other factors not attributable to the Certification Authority. The

Certificate Policy serves to regulate the testing certificates issued by the Certification Authority, and it is not attributable to any actions of the Certification Authority.

Certification Authority may, in the Certification Practice Statement, specify the exemption provisions, provided that, mistakes arising from its own negligence shall not be listed in the exemption provisions.

9.17Other Provisions

Certification Authority may, at its own discretion, define other provisions based on its needs. The Certificate Policy will not specify in this regard.

Appendix 1: Term Definitions

- **A**
  - **Activation Data:** Private data required besides keys to access cryptographic module (such as data used to activate private key for signatures or encryption).
  - **American Institute of Certified Public Accountants, AICPA:** The unit jointly enacted "The Trust Services Principles and Criteria for Secure, Availability, Processing Integrity, Confidentiality and Privacy" standards with Chartered Professional Accountants Canada, and the administrator of the marks of the WebTrust for CA, SSL Baseline Requirement & Network Secure.
  - **Applicant:** Subscriber who applies for certificate from a Certification Authority but have not yet completed the certification procedures.
  - **Archive:** A physically separate (from the storage site of primary information) storage site for long-term information, which can be used to support audit, usage and integrity services.
  - **Audit:** Assessment on whether system controls are adequate to ensure conformance with the existing policy and operation procedure, while being independent in reviewing and investigating the recommended necessary improvements on current controls, policies and procedures.
  - **Audit Log:** System activity logs sorted by time of occurrence, which can be used to reconstruct or investigate the time sequence or changes occurred in a certain event.
  - **Authenticate:** The process of verifying legitimacy of the identity of a certain entity.
  - **Authentication:**
    - The procedures used to establish the reliability of the identity of the administrator or information system.
    - The means to establish security measures used for information transmit, messages and sources, or the authority to to verify whether individuals have received certain types of information.
- **C**
  - **Certificate:**
    - Refers to the verification information carrying a digital signature used to verify the identity and qualifications of the signatory in electronic form.
    - Digital presentation of information, which includes the the contents:
      - ✓ Issuing Certification Authority;
      - ✓ Subscriber's name or identity;
      - ✓ Subscriber's public key;

- ✓ Certificate validity period;
- ✓ Certification Authority's digital signature.

- **Certificate Policy (CP):** An administrative policy with dedicated profile set for the electronic transactions performed through certificate administration. The Certificate Policy covers a variety of issues including the formation, generation, transmission, auditing, post-compromise recovery and administration of digital certificates. Certificate Policy and its related techniques can provide secure services required for specific application.
- **Certificate Revocation List (CRL):**
  - Certificate revocation list is digitally signed by Certification Authority available to be used by the relying party.
  - A list maintained by Certification Authority, which listed the certificates issued by the Certification Authority and revoked before their expiry dates.
- **Certification Authority (CA):**
  - The agency or natural person that issues certificates.
  - The competent body trusted by the subscribers. Its functions are to issue and administer X.509 format public key certificates, Certification Authority Revocation List and Certificate Revocation List.
- **Certification Authority Revocation List (CARL):** A signed and time stamped list. The list contains the serial numbers of revoked CA public key certificates (including cross-certificates of the subordinate Certification Authority).
- **Certificate Modification:** Refers to the provision of a new certificate in replacement of the original certificate to the same subject, provided that, the expiration date of the new certificate shall be the same as that of the old certificate. The original certificate shall be revoked after the modification.
- **Certification Practice Statement (CPS):**
  - External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work.
  - Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts).
- **Chartered Professional Accountants Canada (CPA):** The unit jointly enacted "The Trust Services Principles and Criteria for Secure, Availability, Processing Integrity,

Confidentiality and Privacy" standards with American Institute of Certified Public Accountants, and the administrator of the marks of the WebTrust for CA, SSL Baseline Requirement & Network Secure. Chartered Professional Accountants Canada, formerly named as "Canadian Institute of Chartered Accountants (CICA)".

- **Compromise:** Information disclosed to unauthorized persons or unauthorized intentional or unintentional disclosure, modification, destruction or loss of objects which constitutes a violation of information security policy.
- **Cross-Certificate:** A type of certificate that establishes a trust relationship between two root certification authorities and is regarded as a CA certificate, not a subscriber certificate.
- **Cross-Certification:** The act or procedures of a Certification Authority under a public key infrastructure issuing a public key certificate to another Certification Authority under a public key infrastructure.
- **Cross Certification Agreement (CCA):** The agreement containing the terms and individual liability and obligations that must be followed when the government root certification authority and subordinate certification authorities apply to join the V2X public key infrastructure.
- **Cryptographic Module:** A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including cryptoalgorithms) and included within the cryptographic boundaries of the module.

◆ **D**

- **Digital Signature:** An electronic signature generated by the use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key and capable of being verified by the public key.
- **Duration:** A certificate field made up on two subfields, "start time of the validity period" and "length of the validity period".

◆ **F**

- **Federal Information Processing Standard (FIPS):** The information process standard used by all government agencies and government contractors (excluding military agencies) formulated by the U.S. federal government, where the standard security clearance requirements of the cryptographic module are FIPS 140; FIPS 140-2 classifies cryptographic modules into 11 types of security requirements, and each security requirement is subdivided into 4 security levels.

◆ **I**

- **Internet Engineering Task Force (IETF):** responsible for the development and

promotion internet standard. Its mission is to impact human design, use and management of the internet via the generation of high-quality technical document to make the internet operates more smoothly. (official website: https: //www.ietf.org).

- **Issuing CA: Issuing CA**: in terms of the certificate, the Certification Authority that issued the certificate is certificate's Issuing CA.

◆ **K**

- **Key Escrow:** Storage of related information using the subscriber's private key and according to the regulations of the mandatory subscriber escrow agreement (or similar contract). The terms of this escrow agreement requires that one or more than one agencies have possession the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.
- **Key Pair:** Two mathematically linked keys possessing the following attributes:
  - One of the keys is used for encryption. This encrypted data may only be decrypted by the other key.
  - It is impossible to determine one key from another (from a mathematical calculation standpoint).

◆ **M**

- **Mutual Authentication:** When two parties authenticate one another during communication activities.

◆ **O**

- **Object Identifier (OID)**
  - Refers to a unique alphanumeric / numeric identifier registered under the International Standard Organization registration standard and which could be used to identify the uniquely corresponding certificate policy.
  - When a special form of code, object or object type is registered with the International Organization for Standardization, the unique code may be used as an identifier. For example, this code can be used in the public key infrastructure to indicate what certificate policy and cryptographic algorithms are used.
- **Online Certificate Status Protocol (OCSP):** An online certificate checking protocol allowing the relying party's application software to determine the status (such as revocation status, its validity, etc.) of a particular certificate.

◆ **P**

- **Private Key:** this key shall be kept confidential under the following two circumstances

- The key in the signature key pair used to generate digital signatures;
- The key in the encryption key pair used to decrypt secret information.

- **Public Key：** the key shall be made publicly available under the following two circumstances (usually in a digital certificate form).
  - The key in the signature key pair used to verify the validity of the digital signature.
  - The key in the encryption key pair used for encrypting confidential information.
- **Public Key Infrastructure (PKI)：** Develop and manage asymmetric cryptography and public key certificates on a vast scale covering laws, policies, regulations, personnel, equipment, facilities, technologies, processes, audits, and services.

◆ **R**

- **Registration Authority (RA)**
  A component of the Security Credential Management System (SCMS) that is the main point of contact for an end entity (EE), and is responsible for provisioning the EE with authorization and successor enrollment certificates.
- **Re-key a Certificate:** Re-key a Certificate refers to the issuance of a new certificate with the same characteristics and level of assurance as the old certificate, except that the new certificate has a brand new and distinct public key (corresponding to a new and different private key) and a different serial number, even a different expiration date.
- **Relying Party**
  - Recipient of a certificate who acts in reliance of that certificate or a digital signature to verify the public key listed in the certificate, or the counterparty to identity (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate.
  - The individual or agency which receives information which includes a certificate and digital signature (the public key listed on the certificate may be used to verify this digital signature) and may rely on this information.
- **Renew a Certificate:** The procedure for issuing a new certificate with new serial number to renew the old certificate bearing the same subject name, key and relevant information in order to extend the validity.
- **Repository**
  - A trustworthy system used to store and retrieve certificates or other information relevant to certifications.
  - The repository containing the certificate policy and certificate-related

information.

- **Revoke a Certificate:** Termination of a certificate prior to its expiry date.
- **Root Certification Authority (Root CA):** the highest-level Certification Authority in public key infrastructure. In addition to issuing subordinate CA certificates and self-signed certificates, its self-signed certificate shall be distributed by application software vendors.

◆ **S**

- **Self-Issued Certificate:** The self-issued certificate is issued by the Root Certification Authority when the replacement of key or Certificate Policy is needed. The two generations of Root Certification Authorities use their private keys to issue each other to establish the trust path between the old and new keys or between one Certificate Policy and another Certificate Policy.
- **Self-Signed Certificate:** A self-signed certificate is a type of certificate where the issuer name is the same as that of the subject. That is, using the same pair of private key to issue certificates for the public key and other information in the paired relationship. A self-signed certificate within the public key infrastructure can be used as the trust anchor of the certificate path. Its issuance subject is the Root Certification Authority itself, which contains the public key of the Root Certification Authority and bearing the same issuer name as that of the subject, to allow the relying party to verify the digital signature on the self-issued certificate, subordinate Certification Authority certificate, cross-certificate and Certification Authority Revocation List issued by the Root Certification Authority.
- **Subject Certification Authority:** For a CA certificate, the certificate authority referred to in the certificate subject of a certificate is the subject CA for that certificate.
- **Subordinate Certification Authority:** In the public key infrastructure hierarchy, certificates that are issued by another certificate authority and the activities of the certificate authority are restricted to this other certificate authority.
- **Subscriber**
  - Refers to a subject named or identified in the certificate that holds the private key that corresponds with the public key listed in the certificate.
  - An entity having the following attributes including (but not restricted to) individuals, organizations and network devices:
    - ✓ Entity listed on an issued certificate;
    - ✓ A private key that corresponds to the public key listed in the

certification;

- ✓ Other parties that do not issue certificates.

◆ **T**

- **Trust Anchor:** The starting certificate of the trust path, which is trusted by the relying party and is obtained via a secure and reliable transmission method.
- **Trustworthy System:** Computer hardware, software and programs which possess the following attributes:
  - Functions that protect again intrusion and misuse;
  - Provides reasonably accessible, reliable and accurate operations;
  - Appropriate implementation of preset function;
  - Security procedures uniformly accepted by the general public.

◆ **Z**

- **Zeroize:** Method to delete electronically stored information. Storage of changed information to prevent information recovery.