Taiwan-CA Inc.

Global Certification Authority

Certification Practices Statement (CPS)

(Version1.8)

臺灣網路認證股份有限公司
TAIWAN-CA INC.

Effective Date：2023/6/30

Revision Record

Version	Effective	Released by	Description
1.0	2013/01/22	TWCA PMA	First release.
1.1	2014/07/02	TWCA PMA	Add Device Certificates Practice Statement.
1.2	2016/08/23	TWCA PMA	Delete 2 subject names of SSL UCA.
1.3	2017/09/26	TWCA PMA	Add domain name and CAA records verification requirement.
1.5	2020/01/30	TWCA PMA	(1) Modified to compliance with CABF Baseline Requirement V1.6.4. (2) Add CA/Browser Forum Policy OID. (3) Add AATL certificate. (4) Add CAA records CA Domain requirements.
1.6	2021/12/21	TWCA PMA	(1) 1.2 section: Change the TLS/SSL certificate OID. (2) 1.4.1, 3.2.2 section: Renew the identity authentication methods for the TLS/SSL certificate and Device certificate. (3) 3.2.2, 4.2.1 section: Renew the CAA reference document(RFC 8659). (4) 3.2.2 section: Add domain and IP verification methods. Indicates that the verification method is unavailable. (5) 3.3.1, 6.3.2 section: Change the maximum TLS/SSL certificate validity period to 398 days. (6) 6.3.2 section: Change the maximum CA key pairs validity period to 20 years. (7) 4.9.12 section: Add the method to prove that the key is suspected of being compromised. (8) Add TSA Certificate. (9) 3.1.1：Modify AATL certificate’s naming. (10) 3.2.2：Modified to compliance with CABF Baseline Requirement V1.7.5. (11) 3.2.2：Public Suffix List is required for all domain verification.

1.7	2022/5/30	TWCA PMA	(1) Merge Device Certificates to TLS/SSL Certificates. (2) 2.2、3.2.2：Adjust the applicable certificate types of BR. (3) 3.2.2：Add Requirements compliant to BR 1.7.8. (4) 3.1.1、7.1.4：Add requirements compliant to BR 1.7.9. (5) 8.4：Update version of audit schemes.
1.8	2023/6/30	TWCA PMA	(1) Remove related content of TLS/SSL Certificates and EC SECURITY Certificates. (2) Rename InfoSec UCA Certificate to InfoSec Certificate. (3) Add AATL, S/MIME related content. (4) Add OCSP related content. (5) Add Sections of 1.6, 5.6.1, 5.6.2, and 8.7. (6) Revised Sections 1.4, 3.1.1, 3.2, 4.3.1, 5.2.4, 5.4.2, 5.4.5, 6.1.5, 6.1.6, 6.3.2, 6.5.2, 6.8, 7.1.3, 8.2, 8.6, 9.2.1, and 9.2.2.

Table of Contents

Executive Summary

This document is the Taiwan Global CA Certification Practice Statement (CPS). The important issues of this CPS are as follows:

1. Competent Authority Approval

This CPS is edited and complied with according to the "Regulations on the Required Information for Certification Practices Statements" announced by the competent authorities, and has been approved by the competent authorities with the following document:

2. Certificates to Issue

The type, level of assurance, and scope of use of the global certificates issued by this CA in accordance with this CPS are as follow:

	Types of Certificates	Level of Assurance	Applicability
1	InfoSec Certificate	Class 3	Financial transactions, securities transactions, e-commerce applications, online identity authentication, online tax declaration, e-invoice, e-voting, online patent/trademark applications, issue and transaction of short-term bills and securities, code signing
		Class 2	e-Commerce applications, online identify authentication, email applications
		Class 1	e-Commerce applications, online identity authentication
2	AATL Certificate	Class 3	PDF document signing, e-Commerce applications, online identify authentication, email applications
		Class 2	PDF document signing, e-Commerce applications, online identify authentication, email applications
3	TSA Certificate	Class 3	Evidence of the signing time of the electronic document or message
Note: Please refer to "1.4 Certificate Usage for details" of the assurance level and usage of certificates.			

3. Legal Liabilities and Important Matters

(1) When a subscriber needs to revoke a certificate under any of the circumstances of revocation specified in this CPS (e.g. private key information leakage or private key loss), the subscriber must notify this CA immediately and apply for certificate revocation. However, the subscriber must be liable to the risks and responsibilities as a result of using such certificate prior to the publication of CRLs.

(2) This CA assumes no responsibility for indemnifying any damages, if any, arising from or in connection with the processing of registration data and certificate issuance of subscribers; except for failure to follow this CPS or violation of relevant laws and regulations or intention or negligence attributed to this CA.

(3) This CA also assumes no responsible for indemnifying any damages, if any, arising from or in connection with damage or loss caused to subscribers as a result of an act of God (e.g. earthquake) and/or events out of the reasonable control of this CA (e.g. war).

(4) This CA must be liable to indemnify the damages, if any, arising from or in connection with the damage caused to a third party from the leakage, marauding, interpolation or unintended use of the registration and/or certificate data of subscribers as a result of the failure to keep such data in custody with due faith and due care of this CA.

(5) After receiving a request of certificate revocation, this CA must finish revoking the requested certificate within the time limit defined in Section 4.9.1 and issue and complete publishing the CRL to the repository according to frequency defined in Section 4.9.7. Prior to the publication of the status of certificate revocation or suspension, subscribers must take actions appropriate to minimize the effect on the relying parties of their certificates, and be fully liable to the consequences of the use of such certificates.

(6) When damages arising from or connection with the issuance or use of certificates occurs between this CA and subscribers, both parties must indemnify such damages, provided that the amount must not exceed the upper limit specified in the relevant laws and regulations or the agreement.

(7) When accepting the use of the certificates issued by this CA, the relying party is considered as accepting the legal terms of this CA and trust such certificates within the scope specified in this CPS.

4. Other Important Matters

(1) When subscribers lost or have security doubts (e.g. being cracked) of their private keys, or when there is a change of relevant information, subscribers must immediately report to this CA.

(2) Subscribers must properly generate, retain and use their private keys, and follow the limitations of certificate usage.

(3) When applying for a certificate, subscribers must provide full and accurate information. When receiving the certificate issued by this CA, subscribers must check the correctness of information contained in the certificate, and the public key and private key are a key pair.

(4) When verifying a certificate, the relying party must verify the digital signature of the certificate of this UCA perform with the self-signed certificate of the root certification authority (RCA) and verify if the digital signature of the subscriber certificate is issued by the private key of this CA with the certificate of this UCA. The relying party must also verify if the certificate has been revoked from the CRL.

(5) When using the CRL issued by this CA, the relying party must first verify the digital signature to ascertain if the CRL is valid.

(6) This CA must conduct internal audits at least once six months and external audits at least once a year. Please refer to “8. Compliance Audit and Other Assessments” for details concerning the operating specifications of these audits.

1. Introduction

1.1 Overview

Taiwan-CA Inc. (TWCA) is a joint venture formed by Taiwan Stock Exchange Corporation (TWSE), Taiwan Depository & Clearing Corporation (TDCC), Financial Information Service Corporation (FISC), and HiTRUST.COM Incorporated (HiTRUST).

The TWCA Global Certification Authority Certification Practice Statement (CPS) is established in accordance with the TWCA PKI Certification Policy (CP) and the Regulations on the Required Information for Certification Practices Statements announced by the competent authorities according to the Electronic Signatures Act. The aim of this CPS is to specify how the TWCA GLOBAL Certification Authority (this CA) issues and manages certificates by following the CP.

In order to build a secured and reliable network environment where no fabrication, alteration and/or theft of data during network transfer is assured, TWCA thus plans and implements the online certification system. It is a certification-related security mechanism using the public-key cryptography with security mechanisms conforming to the e-Banking Security Control Standards for Financial Institutions published by the Financial Supervisory Commission (FSC) and equipped with non-repudiation of network transaction messages, user identity authentication, message integrity verification, message encryption and other forms of security controls that are applicable to various e-commerce application systems, such as e-banking, online ordering, online tax declaration, online insurance, online securities and bills, enterprise enquiries and quotations, online purchase and online payment transactions.

1.2 Document Name and Identification

This document is the “Taiwan-CA Inc. Global CA Certification Practice Statement”.

This CPS is established in accordance with the CP. The types of certificates and their corresponding object identifier values are as follows:

Types of Certificates	Object Identifier
InfoSec Certificate	2.16.158.3.1.8.5 1.3.6.1.4.1.40869.1.1.23
AATL Certificate	1.3.6.1.4.1.40869.1.1.26
TSA Certificate	1.3.6.1.4.1.40869.1.1.27

1.21 Revisions

For the previous version change records, please refer to the Section “Revision Record” of this CPS.

1.3 PKI Participants

This CA includes the following members:

(1) Certification Authority (CA);

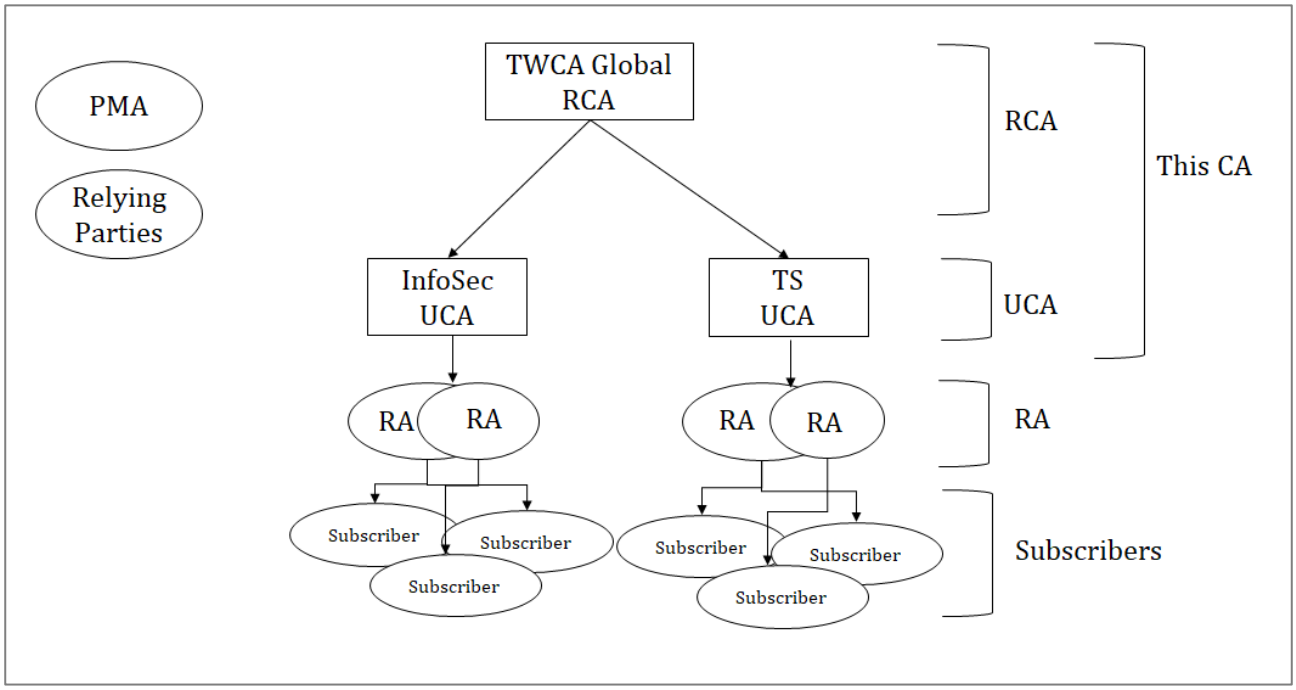
(2) Registration Authority (RA);

(3) Subscriber;

(4) Relying Party; and

(5) and Policy Management Authority (PMA).

The Certification Authorities is divided into RCA and UCA according to the level and purpose, collectively referred to as “this CA”. The membership diagram is as follows:



This CPS specifies how this CA performs the issuance and management of subscriber certificates, and how subscribers and relying parties apply for and use certificates in Chapters 3 and 4; the guidelines of RCA and UCA are specified in Chapter 5.

1.3.1 Certification Authority (CA)

1.3.1.1 Root Certification Authority (RCA)

As the trust anchor of the TWCA PKI, the RCA is the highest-level certification authority operated and managed by TWCA. Its functions and duties include:

(1) to issue and manage the certificates issued to UCA, prohibited to issue subscriber certificates;

(2) to manage and publish certificates and Certificates Revocation Lists (CRLs) in the repository;

(3) to provide Online Certificate Status Protocol (OCSP) repository;

(4) to maintain the stability and operations of the repository; and

(5) to build an independent, safely controlled operating environment, the operation of generating public key, issuing certificates for UCA must be performed by two or more authorized personnel. When the self-signed certificate of the RCA is generated or updated, it must be delivered to the user by the fastest and appropriate channel or notified to the RCA for request.

1.3.1.2 User Certification Authority (UCA)

The functions and duties of this UCA operated and managed by TWCA include:

(1) to issue and manage subscriber certificates;

(2) to manage and publish subscriber certificates and CRLs of subscriber certificates in the repository;

(3) provide OCSP repository; and

(4) to maintain the stability and operations of the repository.

1.3.1.3 Policy Management Authority (PMA)

The TWCA Policy Management Authority (PMA) is a TWCA organization responsible for establishing the following documents:

(1) CP;

(2) CPS; and

(3) SOP.

1.3.2 Registration Authority (RA)

A Registration Authority is an entity that performs identification and authentication of certificate applicants for this CA to issue certificates.

1.3.3 Subscribers

A subscriber is an entity specified in the certificate subject and holds the private key corresponding to the certificate public key.

Subscribers are organizations (juristic person) and individuals (natural person) owned the certificates issued by this CA.

1.3.4 Relying Parties

A relying party is an entity verifying the validity of the digital signature in the subscriber certificate issued by this CA with the public key of the certificate of this CA.

Relying parties identify the network host name and its relying subscriber information based on the identity information recorded in the subscriber certificate.

A relying party must determine if the certificate is reliable or can be used for other purposes based on the information contained in the certificate issued by this CA.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Certificates Level of Assurance

This CA distinguishes different certificate assurance levels according to the strength of the identification method used by the subscriber during the registration stage. The meaning of each certificate assurance level is as follows:

Level of Assurance	Guaranteed Meaning
Testing Certificates	Testing certificates are intended for testing purpose and neither this CA nor the RA will implement subscriber identity authentication in any form. Therefore, they cannot be used in any applications or businesses

	other than testing.
Class 1	This CA and the RA only guarantee the uniqueness of the subscriber identity information in the database of this CA. The relevant information of subscribers is only subjected to limited verification.
Class 2	This CA and the RA only guarantee the uniqueness of the subscriber identity information in the database of this CA. For the subscriber-related information, only the verification is provided instead of the guarantee that it is absolutely correct.
Class 3	In addition to ensuring the uniqueness of the subscriber identity information in the database of this CA, this CA and the RA provide an identity guarantee similar to the strength of face-to-face authentication through multiple rigorous procedures.
Class 4	In addition to ensuring the uniqueness of the subscriber identity information in the database of this CA, this CA and the RA provide an identity guarantee equal to the strength of face-to-face authentication through multiple rigorous procedures.

For different assurance levels, the requirements for identification methods in the registration stage will also be different, as described in Section 3.2.

1.4.2 Scope of Applicability and Liability

I. Scope of Applicability

The code of InfoSec certificate, AATL Certificate, TSA Certificate is a four-part code as shown below:

Part 1・Part 2・Part 3・Part 4

Meanings of each part of the code:

Part 1 [Level of Assurance]	Part 2 [Usage]	Part 3 [Subscriber Status]	Part 4 [Business Category]
1. Class 1 2. Class 2 3. Class 3 0. Testing Certificate	1. Single Usage 2. Multi-usage in limited category	1. Organization (juristic person) 2. Individual (natural person)	1. Financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities 2. Securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting

			3. e-commerce applications, online identity authentication, online tax declaration, e-invoice, e-voting, online patent/trademark application , email applications, code signing, PDF document signing, evidence of the signing time of the electronic document or message(Time-Stamp)

Part 1・Part 2 ・Part 3・Part 4

Meanings of each part of the code:

(1) Part 1: Level of Assurance

There are four classes of certificates: (1) Class 1, (2) Class 2, (3) Class 3, and (0) testing certificates. The security level of certificates is classified by the method of identify authentication in subscriber registration. Please refer to "1.4.1 Certificates Level of Assurance" for details.

(2) Part 2: Usage

The usage of certificates includes (1) single usage and (2) multi-usage within a limited category (e.g. within a financial holding business) as described below:

- Single Usage: It refers to certificates designated for a specific usage or a specific transaction target, such as property declaration, online ordering or network banking. Also, the specific usage or specific transaction target of certificates is specified in the Terse Statement field of the certificate issuer in the Certificate Policy of the certificate.
- Multi-Usage in Limited Category: If the usage code is specified in the Terse Statement field of the certificate issuer in the Certificate Policy of the certificate, the category of multi-usage is subject to the usage specified by the code. If no code is specified, the usage is subject to the contract signed by TWCA or the announcement posted on the TWCA website.

(3) Part 3: Subscriber Type

Subscriber status includes (1) organization (juristic person) and (2) individual (natural person).

(4) Part 4: Business Category

There are three business categories: (1) financial transactions, e-commerce

applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities; (2) securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting; (3) e-commerce applications, online identity authentication, online tax declaration, e-invoice, e-voting, online patent/trademark application, email applications, code signing, PDF document signing, evidence of the signing time of the electronic document or message. Certificates for use in financial transactions can also be used in categories complying with the usage limitations or in securities transactions, e-commerce applications and online identity authentication with the consent of TWCA.

Example: The class code of current organization certificate for network banking is 3.1.1.1, representing:

3: Class 3 Assurance Level • 1: Single Usage • 1: Organization • 1: For use in financial transactions.

II. Limits on Transaction Amount and Liability of Certificates

The limits on transaction amount and limits on liability amount of InfoSec certificate, AATL Certificate, TSA Certificate are as follows:

(1) Limits on Transaction Amount: Different limits on transaction amount are set according to the level of assurance, usage, subscriber status, and business category of certificates. When a transaction proceeds, the transaction limit must not exceed the corresponding limit on transaction amount of that class code.

(2) Limits on Liability Amount: Different limits on liability amount are set according to the level of assurance, usage, and subscriber status of certificates. This limit refers to the maximum amount of liability for a single certificate of subscribers. Regardless of the counts of transaction, the cumulative amount of liability of a single certificate must not exceed the liability amount limit.

(3) When a subscriber and TWCA have signed a contract where scope of use, limits on transaction amount, and limits on liability amount are specified individually, such held by this subscriber must be subject to the contract terms.

(4) Multi-Usage in Limited Category: The scope of use of a subscriber certificate must be subject to the contract signed between the subscriber and TWCA or the relevant SOP established by TWCA and posted on the TWCA website.

The scope of use and liability of certificates are tabulated below:

(Table 1) Currency: NTD

Class	Level of Assurance	Usage	Subscriber Status	Business Category	Transaction Amount Limit	Liability Amount Limit
1.1.1.3	Class 1	Single Usage	Organization	e-Commerce applications, online identity authentication	3,000	3,000
1.1.2.3	Class 1	Single Usage	Individual	e-Commerce applications, online identity authentication	3,000	3,000
2.1.1.3	Class 2	Single Usage	Organization	e-Commerce applications, online identify authentication, email applications, PDF document signing	900,000	300,000
2.1.2.3	Class 2	Single Usage	Individual	e-Commerce applications, online identify authentication, email applications, PDF document signing	300,000	100,000
3.1.1.1	Class 3	Single Usage	Organization	Financial transactions	Unlimited	2,000,000
3.2.1.1	Class 3	Multi-usage in limited category	Organization	Financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities	Unlimited	2,000,000
3.1.2.1	Class 3	Single Usage	Individual	Financial transactions	Unlimited	300,000
3.2.2.1	Class 3	Multi-usage in limited category	Individual	Financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities	Unlimited	300,000
3.1.1.2	Class 3	Single Usage	Organization	Securities transactions	100,000,000	2,000,000
3.2.1.2	Class 3	Multi-usage in limited category	Organization	Securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting	100,000,000	2,000,000
3.1.2.2	Class 3	Single Usage	Individual	Securities transactions	15,000,000	300,000
3.2.2.2	Class 3	Multi-usage in limited category	Individual	Securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting	15,000,000	300,000
3.1.1.3	Class 3	Single Usage	Organization	e-Commerce applications, online identity authentication, online patent/trademark application, code signing, PDF document signing, evidence of the signing time of the electronic document or message	20,000,000	2,000,000
3.2.1.3	Class 3	Multi-usage in limited category	Organization	e-Commerce applications, online identity authentication, online tax declaration, e-invoice, e-voting, PDF document signing	20,000,000	2,000,000

3.1.2.3	Class 3	Single Usage	Individual	e-Commerce applications, online identity authentication, online patent/trademark application, code signing, PDF document signing	2,000,000	300,000
3.2.2.3	Class 3	Multi-usage in limited category	Individual	e-Commerce applications, online identity authentication, online tax declaration, e-voting, PDF document signing,	2,000,000	300,000
Note1: If the code representing the scope of use specified in the certificate is not found in the above table, this certificate cannot be use in any applications or businesses, except for testing. Also, TWCA assumes no liability for certificates of such kind. Note2: The code representing the scope of use is specified in the Terse Statement field of the certificate issuer in the Certificate Policy of the certificate.						

1.4.3 Prohibited Certificate Uses

Certificates issued by this CA cannot be used in applications and/or business that may eavesdrop or intercept third-party communications, cause physical or mental injuries to human beings, or cause severe damage to social order and public interest; except for the intended use specified in this CPS. These certificates also cannot be used in applications and/or business prohibited or eliminated in the Electronic Signatures Act or other relevant laws and regulations or by the competent authorities of respective business.

1.5 Policy Administration

1.5.1 Organization Administering the Document

PMA is responsible for the establishment, amendment and publication of this CPS.

1.5.2 Contact Person

Should you have any suggestions for modifying this CPS or related security concerns (such as key leakage or mis-sending of certificates, etc.), please email or mail your suggestions, supporting details and contact information to the following contact person:

Company Name	TAIWAN-CA INC. (TWCA)
Contact Person	Customer Service Center
Address	10th Floor, 85 Yen-Ping South Road, Taipei, Taiwan, ROC
Phone	886-2-23708886
Fax	886-2-23700728

Email	ca@twca.com.tw

1.5.3 Person Determining CPS Suitability for the Policy

The PMA must approve the suitability of this CPS established by this CA.

1.5.4 CPS Approval Procedures

Pursuant to the Electronic Signatures Act, the CPS established by this CA must be approved by the competent authorities prior to publication and issuing certificates.

1.6 Definitions and Acronyms

Defined in Appendix 2.

2. Publication and Repository

2.1 Repositories

The repository of this CA provides the following services: enquiry and download of certificates, CRLs, CP and CPS. This CA also provides Online Certificate Status Protocol (OCSP) repository for certificate revocation status checking.

The URL of the repository is https://www.twca.com.tw/repository

The CRL and OCSP repository addresses are specified in the certificate extension field, see Chapter 7 for details.

2.2 Publication of Information

The following information is published in the repository of this CA:

(1) CPS;

(2) CA certificate and related information;

(3) Certificates issued;

(4) CRLs; and

(5) OCSP.

2.3 Time of Frequency of Publication

CPS will be published at the repository after it is approved by the competent authorities.

Refer to Section 4.9.7 for the frequency of publication of CRLs.

This CA regularly reviews this CPS and revises this CPS at least once a year.

2.4 Access Controls on Repositories

This CPS and repository information is open for public access. To prevent malicious attacks or interpolations, access control is applied during repository update or flow anomalies.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The X.509 certificates used and issued by this CA contain X.501 Distinguished Names (DNs).

I. The Distinguished Names of subscriber certificates issued by this CA consist of the components specified in the following tables.

(1) InfoSec Certificate

Distinguished Name	Description	Example of DN Contents	REQUIRED
Country(C)	indicate the country attribute of certificate subject	TW	○
Organization(O)	indicate policy information of CA or information about the organization of the certificate applicant	Information	○
OrganizationUnit(OU)	indicate information of CA (issuing unit) or information about the organization unit of the certificate applicant (1)	TaiCA Information User CA	X
OrganizationUnit(OU)	indicate English identification names of RA or information about the organization unit of the certificate applicant (2)	12345678-RA-Trade	X
OrganizationUnit(OU)	indicate application/service names of RA or information about the organization unit of the certificate applicant (3)	Trade	X
Common Name (CN)	indicate the identification name of the certificate applicant, such as the business number or other identifiable names	12345678-01-000	○
Note1: If the InfoSec certificate has S/MIME function, the certificate must include the *id-kp-emailProtection* extended key usage, the Subject Alternative Name field must record the email information, and the component Organization(O) field is optional. Note2: The InfoSec certificate with S/MIME function is abbreviated as "S/MIME certificate" in this CPS.			

(2) AATL Certificate

Distinguished Name	Description	Example of DN Contents	REQUIRED
Country(C)	indicate the country attribute of certificate subject	TW	○

Organization(O)	indicate policy information of CA or information about the organization of the certificate applicant	TAIWAN-CA Inc.	○
OrganizationUnit(OU)	indicate information of CA (issuing unit) or information about the organization unit of the certificate applicant (1)	TWCA InfoSec User CA	X
OrganizationUnit(OU)	indicate English identification names of RA or information about the organization unit of the certificate applicant (2)	70759028-RA-AATL	X
OrganizationUnit(OU)	indicate application/service names of RA or information about the organization unit of the certificate applicant (3)	Information Security	X
CommonName(CN)	indicate the identification name or other identifiable names or other confirmed information of the certificate applicant	70759028-AATL	○

(3) TSA Certificate

Distinguished Name	Description	Example of DN Contents	REQUIRED
Country(C)	indicate the country attribute of CA	C = TW	○
Organization (O)	indicate the organization information of CA	O = TAIWAN-CA Inc.	○
CommonName(CN)	indicate the common name attribute of time stamp certificate	CN = 70759028-01-TSA	○

II. The DNs of this UCA

(1) InfoSec UCA

Distinguished Name	Description
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA Inc.
OrganizationUnit(OU)	OU=User CA
CommonName(CN)	CN=TWCA InfoSec User CA

(2) TS UCA

Distinguished Name	Description
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA Inc.

OrganizationUnit(OU)	OU=Timestamping Sub-CA
Common Name (CN)	CN=TWCA Timestamping Certification Authority

III. The DNs of this RCA

Distinguished Name	Description
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA Root Certification Authority

or

Distinguished Name	Description
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA Global Root CA

or

Distinguished Name	Description
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA Global Root CA G2

3.1.2 Need for Names to be Meaningful

The distinguished names of certificate subjects must comply with the naming rules in the relevant laws, regulations and specifications. Also, these names must be readily identifiable of the organization unit and individual, and must be identified by relying parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

This CPS does not allow subscribers to use anonymity, pseudonyms, or aliases, etc.

3.1.4 Rules for Interpreting Various Name Forms

DNs and their component Relative Distinguished Names (RDNs) are to be interpreted as defined in the applicable certificate profile according to the ITU-T X.520 naming elements.

3.1.5 Uniqueness of Name

This CA will review the uniqueness of the Chinese and English names and the organization name of subscribers.

3.1.6 Name Claim Dispute Resolution Procedures

When more than one subscriber uses the same unique DN, this CA must grant the priority of use of this DN to the first subscriber applying for registration of this DN and passing the identity clearance. Users who apply for registration later will have priority if they pass their identity clearance first.

When a name claim dispute arises and the legal documents issued by the competent authorities prove that the claimed DN is possessed by another applicant, this CA must cancel the right of use of this registered unique DN and revoked the issued certificate. Also, that subscriber must be responsible for the relevant liabilities.

3.1.7 Recognition, Verification and Role of Trademarks

This CA respects the registered trademarks of the Chinese and English names of subscribers and accept their use of such names. However, this CA assumes no guarantee for the recognition, verification and uniqueness of the subscriber's registered trademarks. Subscribers must apply for legal resolution of disputes arising from or in connection with the recognition, verification and role of trademarks.

3.2 Initial Identity Validation

The purpose of initial validation is to prevent fraudulent applications, and the authenticity of the identity information provided by the applicant has been confirmed. To this end, RA must adhere to the following principles when performing identity validation:

(1) Complete the verification, validation, and linkage with the applicant for the collected identity information, and the strength of authentications must match the certificate assurance level.

(2) If the applicant entrusts an agent, a verifiable authorization mechanism must be in place to complete the identity and authorization verification of the agent.

(3) The last registered identity information must be confirmed by the applicant to ensure that the information to be registered is the same as that submitted by the applicant and is the correct information of the applicant.

3.2.1 Method to Prove Possession of Private Key

Subscribers must generate the private key and its corresponding public key used in the certificate on their own and also submit the public key to this CA via sending the PKCS#10 certificate request file signed by subscriber's private key as a proof of private key possession. This CA will verify the digital signature in the PCKS#10 certificate request file submitted with the public key of the subscriber, to validate the subscriber's possession of the private key, and the integrity of the subscriber identity information.

3.2.2 Authentication of Organization Identity

The authentication method of organization identity varies according to the certificate assurance level (defined in Section 1.4.1) applied for. The specific authentication methods are described as follows:

Assurance Level	Authentication Method of Organization
Test Certificates	Do not require authentication, see 1.4.1 for instructions.
Class1	1. Organizations register with self-claimed identity information. 2. RA must verify the uniqueness of the information and conduct limited verification.
Class2	1. Must satisfy the above-mentioned Class1 relevant inspection. 2. Organizations must submit evidence to prove their identity information. 3. RA must check the existence and validity of the evidence.
Class3	1. Must satisfy the above-mentioned Class2 relevant inspection. 2. The representative or the agent holding the authorization document must provide the supporting documents sufficient to organization identity. 3. RA must conduct the authentication similar to the strength of face-to-face, and inquire information through trusted third-party (such as Commerce Industrial Inquiry Services), and check the identity information claimed by the organization or the information only known to the organization.
Class4	1. Must satisfy the above-mentioned Class3 relevant inspection. 2. RA must conduct face-to-face authentication.

If applying for S/MIME certificates, the organization authentication and email validation must be performed to confirm whether the applicant is a legal organization, and to confirm that the applicant has the ownership or control of mail boxes.

The following describes the Email Validation:

- Email validation: This CA uses at least one of the following validation methods to verify the right to use or ownership of the email address that the applicant wants to apply for in the certificate:

  (1) This CA sends a random value with 24 hours validity to the designated recipient, where the recipient's email address is the email address specified in the Subject Alternative Name of the S/MIME certificate issued in the future, and this CA verifies that random value.

  (2) This CA uses the domain name to check and confirm the ownership of the email address. The domain name is defined as the email's local part followed by the ("@") sign. The validation method can be any of the defined methods in "Domain validation".

- Domain validation: This CA validates the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the following procedures from section 3.2.2.4 of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (hereinafter referred to as SSL BR) published by CA/Browser Forum:

  (1) Email, Fax, SMS, or Postal Mail to the Domain Contact by sending a unique Random Value (valid for no more than 30 days from its creation) through email, fax, SMS, or postal mail, to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with SSL BR Section 3.2.2.4.2.

  (2) Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an email created by using "admin", "administrator", "webmaster", "hostmaster" or "postmaster" as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the email, and receiving a response using the Random Value, performed in accordance with SSL BR Section 3.2.2.4.4.

  (3) Domain Name Service (DNS) Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance SSL BR Section 3.2.2.4.7.

  (4) Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 Section 3, performed in accordance with SSL BR Section 3.2.2.4.13.

(5) Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with SSL BR Section 3.2.2.4.14.

(6) Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with SSL BR Section 3.2.2.4.15.

(7) Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with SSL BR Section 3.2.2.4.16.

(8) Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3, performed in accordance with SSL BR Section 3.2.2.4.17.

All the above methods for validation must be used for domain name validation along with current best practice of consulting a public suffix list.

3.2.3 Authentication of Individual Identity

The authentication method of individual identity varies according to the certificate assurance level (defined in Section 1.4.1) applied for. The specific authentication methods are described as follows:

Assurance Level	Authentication Method of Organization
Test Certificates	Do not require authentication, see 1.4.1 for instructions.

Class1	1. Individuals register with self-claimed identity information. 2. RA must verify the uniqueness of the information and conduct limited verification.
Class2	1. Must satisfy the above-mentioned Class1 relevant inspection. 2. Individuals must submit evidence to prove their identity information. 3. RA must check the existence and validity of the evidence.
Class3	1. Must satisfy the above-mentioned Class3 relevant inspection. 2. The individual or the agent holding the authorization document must provide the supporting documents sufficient to individual identity. 3. RA must conduct the authentication similar to the strength of face-to-face, and inquire information through trusted third-party (such as MOICA Individual Inquiry Services), and check the identity information claimed by the individual or the information only known to the individual.
Class4	Not applicable.

If applying for S/MIME certificates, the email validation must be performed to confirm whether the applicant is legal, and to confirm that the applicant has the ownership or control of mail boxes. The validation method is the same as “Section 3.2.2 Email Validation”.

3.2.4 Non-verified Subscriber Information

This CA verifies all subscriber information.

3.2.5 Validation of Authority

The certifications or documents of identity of the organization representative, organization agent or organization must be officially issued by the government. An RA must verify the authenticity of the power of attorney of agents.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication of Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The risk of loss and compromise of keys increases as the time of use extends. Therefore,

subscribers must re-key (update) their keys from time to time to assure the key security.

When the validity of a subscriber key (certificate) is set to one year, this key must be rekeyed upon expiration in one year. That is, the validity period of the user certificate is one year, within the certificate rekey period (e.g. one month before expiry), the subscriber must re-generate a public and private key pair and apply to this CA and RA for the issuance of a new certificate. This process is known as the "rekey" of certificate and private key.

The maximum validity of InfoSec certificate and AATL certificate is 39 months (the validity period of the private key is the same as the certificate validity period). However, the validity period of the S/MIME certificate is limited to 825 days.

Prior to certificate expiration, subscribers of InfoSec certificate and AATL certificate must sign the certificate application with the valid private key before delivering it to the RA to apply for the issuance of a new certificate.

When rekeying of the certificate and private key after the expiration of InfoSec certificate and AATL certificate, subscribers must apply to the RA for certificate rekey over the identity validation specified in Section 3.2. After obtaining the identity information for certificate rekey from the RA, subscribers must apply for the issuance of a new certificate to this CA or RA with the certificate application and identity information containing signature signed by the new private key. After receiving the certificate application from subscribers, apart from verifying the legitimacy of private key possession, RA must verify the legitimacy and integrity the subscriber's certificate application.

The maximum validity period of the TSA private key is 15 months, and the maximum validity period of the TSA certificate is 135 months.

Subscribers must apply for a new certificate before the expiration of their TSA certificates.

3.3.2 Identification and Authentication for Re-Key after Revocation

After revoking a certificate, subscribers must re-apply for a new certificate with initial identity validation or other forms of identity certification to this CA according to Section 3.2.

3.4 Identification and Authentication for Revocation Request

When subscribers make a revocation request, this CA must authenticate such request according to Section 4.9.3.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Organizations applying for certificates must make the application in the name of their statutory representatives or agents.

Individuals (natural persons) are also as the certificate applicant.

4.1.2 Enrollment Process and Responsibilities

Subscribers must apply for the issuance of certificates to the RA and complete the application for subscriber registration to the RA prior to certificate application.

(1) RA must explain in detail to subscribers the representations and warranties specified in certification application form and Subscriber Agreement, the operating procedure of the operation of relevant businesses and the provision of the user's guide and operation documents must be approved and confirmed by subscribers.

(2) Subscribers must fill correct and detailed information in the relevant application forms and submit the relevant supporting documents. After verifying the identity and supporting documents according to the SOP for identity authentication of different levels of assurance, RA must set the personal identification number (PIN) and protection password of subscribers to complete the subscriber registration.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The identity authentication procedure for different levels of assurance is specified in Section 1.4.1. The identification and authentication methods are specified in Section 3.2.

4.2.2 Approval and Rejection of Certificate Applications

After completing the identification and authentication procedures specified in Section 4.2.1, the applicant is approved. By contrast, applicants who cannot pass the identification and authentication will be rejected.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions for Certificate Issuance

The certificate issuance procedures for InfoSec certificate, AATL certificate, and TSA certificate are as follows:

(1) Subscribers must pass at least the PIN and password check and verification. After logging on to RA, subscribers must sign the certificate application information with the subscriber private key before delivering it to RA.

(2) After verifying the PIN and password of subscribers and checking the integrity of the certificate application information, RA must sign the certificate application information of subscribers with the RA private key if no error is found before delivering such information to this CA after encryption.

(3) The reviewers of this CA log in to the certificate management website through two-factor authentication to perform the authentication and/or the validation defined in Section 3.2, and another reviewer will conduct the review process to confirm that the information is correct, then certificate can be issued and delivered to RA.

(4) After examining the legitimacy and integrity of the reply information of subscriber certificates from this CA, RA must deliver the subscriber certificate to the applicant if no error is found.

(5) The start date of the certificate in the subscriber certificate issued by this CA does not go back to the past time; that is, the start date of the certificate will not be earlier than the current time when the certificate is issued.

For the consideration of security control measures, RA or this CA may deliver the software generated by the certificate application and the private key to the subscriber in a reliable and secure manner, and the software must be passed appropriate security assessments by RA or this CA.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

For subscribers applying for certificates on-line, this CA may notify them of the results of issuance immediately after the certificate is issued.

For subscribers applying for certificates not on-line, this CA may notify them of the results of issuance by phone or by email.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

After receiving the certificate issued by this CA, subscribers must proceed with the following procedure:

(1) To verify the consistency of certificate contents with the application form, and that the subscriber information is correct.

(2) To check if the public key of the certificate is the same as that of the PKCS#10 certificate request file.

(3) To verify the certificate chain of the certificate, check the correctness, integrity and validity of each certificate, whether the certificate has been revoked, whether the validity period of the certificate has expired, and whether it is indeed issued by this CA.

(4) If the procedures are unfulfilled, subscribers must immediately inform RA to revoke the certificate and re-initiate the certificate issuance procedure in Section 4.3.

(5) After receiving the certificate they apply for, subscribers must confirm that they have fully understood and agreed the representations and warranties regarding certificate uses. If they decline such representations and warranties, this will mean a rejection of the certificate, and they must inform RA to revoke the certificate.

This CA only accepts subscribers to request a re-issuance of certificates to this CA within 7 days after the certificate is issued.

4.4.2 Publication of the Certificate by the CA

After completing the certificate issuance procedure, this CA will publish the subscriber certificates issued in the repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The usage, applicability and limitation of subscriber certificates are specified in Section 1.4.

Subscribers must keep their private keys secure. When there are doubts about certificate security, such as key fraud, key exposure or key loss, subscribers must report to the RA.

4.5.2 Relying Party Public Key and Certificate Usage

Prior to accepting the certificates issued by this CA, relying parties must at least run the following procedure to determine if such certificates are reliable:

(1) To obtain the RCA self-signed certificate of this CA via proper and secure channels.

(2) To check if the RCA self-signed certificate, the UCA certificate and subscriber certificate are expired.

(3) To verify if the digital signature of the UCA certificate is valid with the public key of the RCA self-signed certificate and not revoked.

(4) To verify if the digital signature of the subscriber certificate is valid with the public key of the UCA certificate.

(5) To check if the subscriber certificate is not revoked by this UCA.

If the certificate fails to pass the above verifications, this suggests that the certificate obtained by the relying party is not issued by this CA or has expired. In this case, relying parties must not accept these subscriber certificates.

4.6 Certificate Renewal

Certificate renewal refers to issuances of a new certificate with the same key as the original certificate but a different serial number and extended validity without changing the subscriber identity information.

This CA does NOT provide certificate renewal service.

4.7 Certificate Re-key

Certificate re-key refers to the re-generation of a public key and private key pair to apply for certificate issuance to CA with the original registration data.

4.7.1 Circumstances for Certificate Re-key

Subject to Section 3.3.1.

4.7.2 Who May Request a New Public Re-key

Subscribers are entitled to re-key their certificates.

4.7.3 Processing Certificate Re-keying Requests

(1) Identity identification and authentication subject to Section 3.3.

(2) Issuance of certificate subject to Section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

Subject to Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of Re-keyed Certificate

Subject to Section 4.4.

4.7.6 Publication of the Re-keyed Certificate by the CA

Subject to Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Subject to Section 4.4.3.

4.8 Certificate Modification

Certificate modification refers to the issuance of a certificate after modifying the subscriber's identify information without changing the public key.

This CA does not accept the request of certificate modification. If the subscriber's identify information or other information recorded in the certificate needs to be changed, the certificate must be revoked in accordance with the provisions of Section 4.9 and re-apply for certificate issuance in accordance with the provisions of Sections 4.1, 4.2, 4.3 and 4.4 .

4.9 Certificate Revocation and Suspension

When revocation occurs, the relevant certificates must be revoked and added to the CRL/OCSP, and the revoked certificates must be included in the CRL/OCSP published thereafter until they

expire.

4.9.1 Circumstances for Revocation

Subscribers must revoke a certificate during its validity under any of the following circumstances:

(1) Subscribers

- Subscribers revoke a certificate for security consideration, e.g. after the termination of employment or transfer of an employee, or when they do not use the certificate anymore.
- Subscribers revoke a certificate when the contents and subscriber registration information in the certificate have been changed, such as updating the organization's registered name or related registration information after a restructuring or merger or for any special reasons.
- Subscribers revoke a certificate when the private key is damaged, lost, exposed or interpolated, or when there is a doubt of third-party theft.

(2) This CA may revoke a subscriber certificate without prior notice

- This CA may revoke a subscriber certificate when the certification system key is modified, invalid, or due to the need for system integration.
- This CA may revoke a subscriber certificate when this CA terminates operations and refers its business to another CA.
- This CA may revoke a subscriber certificate when RA (this CA) announces that its subscriber has failed to perform its representations specified in the contract or code of operations, such as paying the relevant fees, or the subscriber breaks the law, the relevant regulations, or the scope of certificate use as a result of an illegal use of the certificate.
- This CA may revoke a subscriber certificate when the subscriber information in the certificate does not comply with the CP, this CPS or the scope of certificate use; such as discrepancies between the certificate contents and registration information, discrepancies due to negligence in data input, or unofficial authority of the certificate.

(3) Responsible Units

- The competent authorities or a court of law may request certificate revocation according to the official and legal operating procedure due to business needs.

For S/MIME certificates, the certificate must be revoked under any of the following circumstances:

(1) The subscriber indicates that the original certificate request was not authorized and does not retroactively grant authorization.

(2) This CA obtains reasonable evidence that the subscriber's private key (corresponding to the public key of the certificate) has been compromised or is suspected of compromise.

(3) This CA obtains reasonable evidence that the certificate has been used for a purpose outside of that indicated in the certificate or in the CA operator's subscriber agreement.

(4) This CA receives notice or otherwise becomes aware that a subscriber has violated one or more of its material obligations under the subscriber agreement.

(5) This CA receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted.

(6) This CA receives notice or otherwise becomes aware of a material change in the information contained in the certificate.

(7) A determination that the certificate was not issued in accordance with the CP or CPS of this CA.

(8) This CA determines that any of the information appearing in the certificate is not accurate.

(9) This CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the certificate.

(10) The private key of this CA used in issuing the certificate is suspected to have been compromised.

(11) Additional revocation events published in CP.

(12) The certificate was issued in violation of the regulations of this CPS or MRSP (Mozilla Root Store Policy).

4.9.2 Who can Request Revocation

RA or this CA related to subscribers, the competent authorities or a legally authorized third party, and subscribers are entitled to request certificate revocation.

(1) Subscribers

- Subscribers may request certificate revocation as needed in accordance with the RA's SOP.

(2) RA (this CA)

- When requesting certificate revocation, RA (this CA) must follow "Section 4.9.3 Circumstances for Revocation", contract signed with the subscriber, and the relevant SOPs.

(3) Authorized Third Parties

- The authorized person of an organization may request certificate revocation with legal authorization from the organization.
- When a legal legacy successor of a subscriber requests certificate revocation, RA must verify the death status and the identity of the legal successor according to the relevant SOPs.
- A court of law may request certificate revocation from RA for litigation and arbitration reasons according to the relevant TWCA SOPs.
- The competent authorities may request certificate revocation in accordance with the relevant laws, regulations, and SOPs.

4.9.3 Procedure for Certificate Revocation

I. Personal Revocation Requests

After subscribers make a revocation request, this CA will check their identity. If no error is detected, operators of this CA will revoke the requested certificates.

II. Online Revocation Requests

After subscriber log on to the RA certification system website, RA will check their identity. If no error is detected, the certification system of this CA will revoke the requested certificates.

After receiving the certificate revocation reply from this CA, RA will check the legitimacy and integrity of the reply and reply to the subscriber requesting revocation if no error is found.

The competent authorities, a court of law and an arbitration institution, or other authorized parties must make an official certificate revocation request to RA in writing.

4.9.4 Revocation Request Grace Period

When the circumstances for revocation are detected, subscribers must make a revocation request within a reasonable grace period according to general commercial practices, and no

specific grace period is defined in this CPS. When there is an alleged or proven compromise or security concerns of the certificate key, subscribers must make a revocation request within 24 hours.

This CA provides online 24 x 7 acceptance of certificate revocation and reports of improper use of certificates. The processing procedure after case acceptance is shown in Section 4.9.5.

4.9.5 Time Within Which CA Must Process the Revocation Request

After receiving a request of certificate revocation or report of improper certificate use from subscribers, RA (or this CA) must process the request or report immediately during operating or office hours, and must complete processing the request or report within at least one workday.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties must check the certificate status through CRLs or OCSP Responder based their risk, responsibilities and potential consequences, and determine the query frequency.

If relying parties check the certificate status through the CRL issued by this CA, they must verify the CRL is issued by this CA, including verifying the correctness and validity of the digital signature of the CRL. Other precautions for verification must meet the RFC 5280 related requirements.

If relying parties check the certificate status through the OCSP Responder provided by this CA, they must verify whether the OCSP response is issued by the OCSP Responder of this CA before using it, including verifying the correctness and validity of the digital signature of the OCSP response. Other precautions for verification must meet the RFC 6960 related requirements.

4.9.7 CRL Issuance Frequency

This CA updates and issues CRLs every 24 hours.

4.9.8 Maximum Latency for CRLs

Not specified.

4.9.9 On-line Revocation/Status Checking Availability

This CA only provides OCSP Responder for S/MIME certificates and supports querying certificate status by HTTP GET or POST. And its response message conforms to the specification of RFC 6960 and includes the digital signature of the message.

This CA updates the certificate status information provided by the OCSP Responder every 24

hours, and the validity period is up to 4 days. For other details, please refer to Section 7.3.

4.9.10 On-line Revocation Checking Requirements

Prior to trusting the certificates issued by this CA, relying parties must check the status of certificates using CRLs issued by this CA.

If relying parties of S/MIME certificates do not use the CRL issued by this CA to check the certificate status, relying parties must check the certificate status through the OCSP Responder specified in Section 4.9.9.

4.9.11 Other Forms of Revocation Advertisements Available

Not specified.

4.9.12 Special Requirements for Key Compromise

If the key is suspected of being compromised, the informant can contact the appropriate window of this CA through legal channels with the certification information. This CA accepts the following methods to prove that the key is suspected of being compromised:

Provide a CSR (using the PKCS#10 format) issued with a key that is suspected of being compromised. The common name of the CSR must be “Proof of Key Compromise for TWCA” for the CA to verify its authenticity.

When the signing key of this CA is compromised, this CA must proceed the following procedure:

(1) To generate a new key pair for signing and the corresponding new certificate.

(2) Revoke all issued certificates and issue CRLs with the new signing key, this CRL must include all issued but still valid certificates (including certificates revoked prior to the key compromise).

(3) To notify subscribers.

(4) To securely deliver the new certificate to subscribers.

(5) To issue new certificates to subscribers with the new signing key.

When the subscriber key is alleged or proven to be compromised, subscribers must notify this CA to revoke the corresponding certificates within 24 hours.

4.9.13 Circumstances for Suspension

I. InfoSec Certificate

The suspension of subscriber certificates must be operated in accordance with the business requirements and SOP of this CA and RA. When it is necessary to suspend a certificate during its validity, subscribers must request certificate suspension in any of the following circumstances:

(1) Subscribers

- When there are doubts about private key loss and exposure, subscribers may request certificate suspension without revoking them in order to reserve the right of certificate use.
- Subscribers may request certificate suspension when they do not wish to use them for a period of time.

(2) RA/This CA

- RA or this CA may suspend a certificate after announcing that its subscriber has failed to perform its representations, such as paying the relevant fees, or the subscriber has improperly used the certificate which may break the law, the relevant regulations, this CPS or the scope of certificate use.

(3) Responsible Units

- The competent authorities or a court of law may request certification suspension according to the relevant SOP due to business needs.

II. AATL Certificate

Suspension of AATL certificate is currently unavailable.

III. TSA Certificate

Suspension of TSA certificate is currently unavailable.

4.9.14 Who Can Request Suspension

I. InfoSec Certificate

RA or this CA related to subscribers, the competent authorities or a legally authorized third party, and subscribers are entitled to request certificate suspension.

(1) Subscribers

- Subscribers may request certificate suspension as needed in accordance with the RA's SOP.

(2) RA (this CA)

- When requesting certificate suspension, RA (this CA) must follow "Section 4.9.15 Circumstances for Suspension", contract signed with the subscriber, and the relevant SOPs.

(3) Authorized Third Parties

- The authorized person of an organization may request certificate suspension with legal authorization from the organization.
- A court of law may request certificate suspension from RA for litigation and arbitration reasons according to the relevant SOPs of this CA.
- The competent authorities may request certificate suspension in accordance with the relevant laws, regulations, and SOPs.

II. AATL Certificate

Suspension is not applicable to AATL certificates.

III. TSA Certificate

Suspension of TSA certificate is currently unavailable.

4.9.15 Procedure for Suspension Request

I. InfoSec Certificate

(1) Personal Revocation Requests:

After subscribers make a suspension request, this CA will check their identity. If no error is detected, operators of this CA will suspend the requested certificates.

(2) Online Revocation Requests:

After subscriber log on to the RA certification system website, RA will check their identity. If no error is detected, the certification system of this CA will suspend the requested certificates.

After receiving the certificate suspension reply from this CA, RA will check the legitimacy and integrity of the reply and reply to the subscriber requesting revocation if no error is found.

The competent authorities, a court of law and an arbitration institution, or other authorized parties must make an official certificate revocation request to RA in writing.

If subscribers wish to continue to use the suspended certificate after the reasons for suspension are relieved, and the certificate is still valid, they may request cancelation of suspension to RA to revalidate and use the certificate.

II. AATL Certificate

Suspension of AATL certificate is currently unavailable.

III. TSA Certificate

Suspension of TSA certificate is currently unavailable.

4.9.16 Limits on Suspension Period

I. InfoSec Certificate

After suspending a certificate, the certificate is always listed in the CRL before its expiration if subscribers do not cancel the suspension. In this case, this certificate is invalid.

The limits on suspension period refer to the period from the completion of suspension and listing in the CRL of certificates until subscribers cancel suspension and certificates are delisted from the CRL. If subscribers do not cancel suspension before certificate expiration, this certificate is considered as overdue (cannot be use any longer as a revoked certificate).

The maximum suspension period is the expiration of the subscriber certificates issued by this CA.

II. AATL Certificate

Suspension of AATL certificate is currently unavailable.

III. TSA Certificate

Suspension of TSA certificate is currently unavailable.

4.10 Certificate Status Service

4.10.1 Operational Characteristics

Certificate status information is available via CRLs and OCSP responder. Revocation entries on a CRL/OSCP will not be removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

This CA maintains an online 24x7 Repository that the relying party can use to check the current status of all unexpired certificates.

Certificate status of all certificates issued by this CA can be queried through CRLs, S/SMIME

certificates can also be queried via OCSP Responder.

The response time of the CRL and OCSP Responder provided by this CA is generally no longer than 10 seconds under normal network operating conditions.

This CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint. Please refer to Section 1.5.2 for the contact window of this CA.

4.10.3 Operational Features

Please refer to Sections 4.9.9 and 4.9.11.

4.11 End of Subscription

When certificates issued by this CA expire, are revoked, or when this CA discontinues its operations, all certificates issued are ineffective.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No key escrow is allowed for the keys of this CA and subscribers.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not specified.

5. Facility, Management and Operational Controls

In addition to the CP, the security control of this CA also follows the "NETWORK AND CERTIFCATE SYSTEM SECURITY REQUIREMENTS" specification set by the CA/Browser Forum.

5.1 Physical Controls

5.1.1 Site Location and Construction

The computer room of this CA is located at TWCA. The location and construction of the facility housing CA equipment is consistent with the facilities used to house high value, sensitive information. The site location and construction, combined with other physical security protection mechanisms, such as gated control, guards and intrusion sensors and CCTV system, provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

The access controls to the computer room of this CA include:

(1) Identity authentication with three gated facilities (smart card or fingerprint recognition). Access into the computer room requires 2-person access after identity authentication. Twenty-four-hour CCTV system is provided to ascertain taped surveillance. IrDA sensors are equipped in the intrusion detection system. All these facilities are designed to maintain the status of access to the CA computer room and to prevent unauthorized access to the CA computer room.

(2) The backup copy and relevant data of the private key for CA operations are stored properly in a vault with taped CCTV surveillance. Personnel managing and operating CA management and operation systems must run the administration with at least two employees at a time. All operations are under taped surveillance.

(3) Software, hardware, and hardware cryptographic modules are installed in environments protected by taped surveillance system, and two-factor authentication is required by authorized employees for running key management.

5.1.3 Power and Air Conditioning

The computer room of this CA is equipped with the diesel generation set and uninterrupted power supply (UPS) system. When general power supply fails, the system will automatically switch to the diesel generation set, with the UPS providing temporary power supply during the transit.

Independent air conditioning system is equipped in the computer room to ascertain the stability and optimal work environment for system operations. Periodic maintenance and tests are conducted at planned intervals.

5.1.4 Water Exposure

The computer room of this CA is sealed construction. Apart from the internal access, the exterior is a RC building with elevated floors such that it is not in danger of exposure to water.

5.1.5 Fire Prevention and Protection

The computer center of this CA is built with fire-retardant materials and equipped with fire protection and suppression facilities over a central monitoring system. When a fire is detected, the system can automatically activate the fire extinguishing function.

5.1.6 Media Storage

The media storage environment of this CA is built to protect media against damage, with facilities and environments to protect magnetic media against EMI and ESD. The media for storing the backup copies of important data are stored in a vault with fire protection and suppression functions. One of the backup copies of these data is stored in an off-site location with security controls.

5.1.7 Waste Disposal

Prior to scrap, the business sensitive data and confidential information stored in hardware equipment, disk drives and cryptographic modules used by this CA must be securely expunged and destroyed and verified by the audit unit. Records are maintained for future reference.

Documents and media containing business sensitive and confidential data must be expunged and destroyed to ascertain that no information can be recovered or accessed for reuse. Also, data destruction must be verified by the audit unit, and records must be maintained.

5.1.8 Off-site Backup

This CA is equipped with an off-site backup computer room with backup equipment. When equipment for daily operations fails due to external factors, the backup equipment allows this CA to maintain business continuity

The information and documents of the relevant media required for CA operations are backed up in an off-site backup environment with temperature and humidity control, EMI protection, ESD protection, taped CCTV surveillance, and high personnel access control.

The backup log of this CA is stored in an off-site backup computer room with high security control.

5.2 Procedural Control

5.2.1 Trusted Roles

Under the PKI architecture, this CA must perform certificate management with a tight and secure operating procedure. To ensure that one-person acting alone cannot circumvent safeguards, CA responsibilities and authority are divided between multiple roles and individuals. The trust roles and their division of labor of this CA are as follows:

(1) Administrator: To take charge of system installation, system management and environment parameter setup.

(2) Officer: To take charge of the issuance and revocation of certificates.

(3) Auditor: To conduct internal audit, review and maintenance of audit records.

(4) Operator: To run routine maintenance, such as backup, recovery and website data maintenance.

5.2.2 Number of Persons Required Per Task

The number of persons required per task:

(1) Administrator: At least two.

(2) Officer: At least two.

(3) Auditor: At least one.

(4) Operator: At least two.

5.2.3 Identification and Authentication for Each Role

System resources are assigned to administrators, officers, auditors and operators according to their scope of business. The unique ID, smartcard, and relevant PIN are applied for identifying and authenticating the trusted roles.

Detailed records of the operations and functions implemented by operators are maintained to ensure the auditability of system resources and facilitate the threat and risk assessment of system security.

5.2.4 Roles Requiring Separation of Duty

Role	Officer	Administrator	Auditor	Operator
Officer	○	X	X	X
Administrator	X	○	X	○
Auditor	X	X	○	X
Operator	X	○	X	○

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

(1) Operators of this CA must be loyal, reliable and enthusiastic about work. They must not engage in any sideline job affecting certification work, nor should they have any criminal and dishonorable records.

(2) Officers must equip with practical certification experience, or receive relevant training and pass the relevant tests.

(3) Administrators must at least be equipped with practical certification experience and with experience in the planning, operations and administration of computing systems.

5.3.2 Background Check Procedures

The personnel related departments must run a background check on CA employees for security purposes according to the background check and review specifications. Other relevant business departments must review the practice and experience. Employees must pass the background check and relevant reviews prior to employment. A practice and experience review must be performed every year according to the characteristics of duties of individual operators as the reference for job assignment or work adjustment.

5.3.3 Training Requirements

Based on the duties and functions of operators, this CA arranges their training on the ability for operating the CA hardware and software, the operating procedures, certificate issuance and validation procedures, security control procedures, disaster recovery operating standards, key management and certification policies, this CPS, and other operating procedures concerning information security. Appropriate training will also be arranged when there is a change or addition of certification systems.

This CA has established complete education and training specifications for the hardware and

software, application and security management systems of the Certificate management system. When there are newcomers or changes of the Certificate management system, education and training on the relevant skills will be arranged. Also, a record on the training results will be maintained for the reference of the appointment of relevant operators.

5.3.4 Retraining Frequency and Requirements

This CA will review the knowledge and skills required for operating the Certificate management system of relevant personnel at least once a year and arrange appropriate education and training for them. Education and training will also be arranged for them after a Certificate management system update, an addition of new systems, or progress or update of PKI-related knowledge and technologies.

5.3.5 Job Rotation Frequency and Sequence

(1) An administrator will only be assigned as an officer or auditor one full year after being transferred away from his/her original position.

(2) An officer will only be assigned as an administrator or auditor one full year after being transferred away from his/her original position.

(3) An auditor will only be assigned as an administrator or officer one full year after being transferred away from his/her original position.

(4) An operator must work as an operator for two full years, complete the relevant education and training, and pass the review before he/she is qualified for transferring to an administrator, officer or auditor post.

5.3.6 Sanctions for Unauthorized Actions

Out of either intention or negligence, operators of this CA executing operations with unspecified duties or functions must be reported immediately to the supervisor and handled according to the relevant codes, whether these operations have caused security threats to the Certificate management system.

5.3.7 Independent Contractor Requirements

When tasks are outsourced to external operators due the human resource shortage, this CA must run the background check on these independent contractors according to Section 5.3.2 and provide them with education and training on the knowledge and skills specified in Section 5.3.3 required for finishing such tasks. In addition to singing the non-disclosure agreement for the work contents, these independent contractors must follow the relevant operating procedure, codes and legal requirements. Also, the rights and obligations of these independent

contractors will be the same as the internal operators of this CA.

5.3.8 Documentation Supplied to Personnel

To ensure the normal operation of the Certificate management system, this CA must provide to personnel documentation needed for operating the system. The documentation must at least include the following:

(1) documents for operating the hardware and software platforms, documents related to the network system and website, and documents for operating the hardware cryptographic module;

(2) documents relating to operating the Certificate management system of this CA;

(3) this CPS, CP and relevant operating standards and SOPs;

(4) internal operation documents of the Certificate management system of this CA, such as system backup and recovery operating procedure, off-site DR operating procedure, and routine operating procedure.

5.4 Audit Logging Procedure

5.4.1 Types of Events Recorded

At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

(1) Type of entry;

(2) The date and time the event occurred;

(3) A success or failure indicator when executing the CA's signing process;

(4) Identity of the entity and/or operator that caused the event; and

(5) Event Description.

This CA logs the following types of entry:

(1) Security Audit

- Changes of any important audit parameters, such as audit event type, contents of new and old parameters.
- Any attempt to delete or modify an audit log.

(2) Management, identification and authentication of personnel and trusted roles

- New role setup, regardless of success or failure.
- The maximum limit of identity authentication attempts.
- The maximum failure limit of identity authentication attempts of users at system logon.
- Administrator unlocks a locked account.
- Administrator changes the identity authentication mechanism of the system; such as from password into biometrics.

(3) Key Operating Procedure

- Key generation.
- Key destruction.

(4) Private Key Loading and Storage

- Loading a private key to the system component.

(5) Addition, Deletion and Storage of Trusted Public Keys

- Modifications of trusted public keys, including addition, deletion and storage.

(6) Private Key Output

- Output of private keys (not including keys for single use or one-time key)

(7) Certificate Registration/Signing

- The process of registration request of certificates.
- Certificate issuance.

(8) Certificate Revocation

- The process of revocation request of certificates.
- The process of CRL production.
- The signature record of OCSP Response.

(9) Approval of Certificate Status Change

- Approval or rejection of request of certificate status change.

(10) Configuration

- Changes of security-related configurations.

(11) Account Management

- Addition or deletion of roles and users.
- Modification of user account or role access authority.

(12) Certificate Profile Management

- Change of certificate profiles.

(13) CRL Profile Management

- Change of CRL profiles.

(14) Important Events in System Installation and Operations

- Installation of operating systems.
- Installation of certificate management system.
- Installation of hardware cryptographic modules.
- Removal of hardware cryptographic modules.
- Destruction of hardware cryptographic modules.
- System activation.
- Attempt to log on to the certificate management system.
- Hardware or software receiving.
- Attempt to set passwords.
- Attempt to modify passwords.
- Backup of the internal data of this CA.
- Recovery of the internal data of this CA.
- File operations (e.g. generation, rename or move).
- Sending information to the repository.
- Access to the internal database of this CA.
- Key compromise.
- Key replacement of this CA.

(15) Change of the Server Settings of this CA

- Hardware.
- Software.
- OS.
- Patches.
- Security Profiles.

(16) Physical Access and Location Security

- Personnel access the computer room of this CA.
- Access to the server of this CA.
- Acknowledged or suspected violation of physical security regulations.

(17) Abnormal Events

- Software errors.
- Failures of software integrity check.
- Receiving of messages in wrong formats.
- Abnormal routing of message.
- Network attack (suspected or confirmed)
- Equipment failures.
- Power supply anomalies.
- UPS failures.
- Significant and critical network service or access failures.
- Violation of this CPS.
- System clock reset.

5.4.2 Frequency of Processing Log

This CA reviews the audit log once a month to trace and investigate events that occurred. The review includes verification of the audit log for alteration; viewing all items in the log and checking for warnings or anomalies; and explanation of the causes of such events and proposition of preventive actions. Document the results of audit log reviews.

5.4.3 Retention Period for Audit Log

The relevant audit log reports and media data must be retained at least 7 years and must not less than 2 years after the relevant key is destroyed, the certificate expires, and the revocation.

5.4.4 Protection of Audit Log

(1) Ensure that only authorized persons can read and back up audit logs.

(2) Digital signatures or encryption technologies must be applied to retain current and archived electronic audit logs stored in non-rewritable discs or other media where audit log modification is disabled.

(3) The key for protecting event logs must not be used for other purposes.

(4) Paper or physical audit logs must be stored in a secure and safe location.

5.4.5 Audit Log Backup Procedures

Electronic audit logs are backed up at least once a month and stored in the offsite backup location outside of this CA.

5.4.6 Audit Collection System

The audit system is built inside the certificate management system of this CA. The audit procedure is activated when the certificate management system starts up and stops only when the certificate management system is shut down.

If the automatic audit system does not work properly to protect system data integrity, and system data security is exposed to high risk, this CA will suspend the certificate issuance service until problems have been resolved.

5.4.7 Notification to Event-Causing Subject

When an event occurred and is recorded in the audit system, the audit system does not need to notify the event-causing subject of the logging of such event.

5.7.8 Vulnerability Assessment

The following risk assessments must be performed once a year:

(1) Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

(2) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

(3) Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5 Records Archival

5.5.1 Types of Records Archived

The records archived by this CA include:

(1) CA accreditation data;

(2) Certification Practices Statement;

(3) Subscriber agreement;

(4) System and equipment configuration;

(5) Modifications and updates to system or configuration;

(6) Certificate requests;

(7) Revocation requests;

(8) Documentation of receipt and acceptance of certificates;

(9) All certificates issued or published;

(10) Record of rekey;

(11) All CRLs issued and/or published;

(12) All audit logs;

(13) Other data or applications to verify archive contents;

(14) Documentation required by compliance auditors; and

(15) Subscriber Identity Authentication data.

5.5.2 Retention Period for Archive

All archived data of this CA must be retained at least 7 years and must not less than 2 years after the relevant key is destroyed, the certificate expires, and the revocation.

5.5.3 Protection of Archive

No archived data can be written, modified and/or deleted. Individually archived data of subscribers can be released by corresponding subscribers or other legally approved organizations.

One copy of the archived data must be stored at a site off this CA and protected with proper security controls and media damage preventive measures.

5.5.4 Archive Backup Procedures

According to the backup and disaster recovery operating procedures, key, certificate and transaction data must be archived and backed up daily, weekly and monthly. One backup copy must be stored at the TWCA in an environment protected with security controls. Also, another backup copy must be stored in an offsite location equipped with security controls. When the certification system is abnormal and unable to start up, the certification system recovery must be initiated with the stored backup data according to the System Backup and Recovery Operating Manual.

5.5.5 Requirements for Time-Stamping of Records

Archived electronic records (e.g. certificates, CRLs, and audit records) are automatically time-stamped as they are created and are protected appropriately with the digital signature or cryptographic algorithm. These policies are applied to ensure that alteration of such records can be detected from the time stamp. However, as the data contained in the time stamp of these records are not the electronic time stamp provided by a third party, but the date and time of the computer operating system.

All computer systems of this CA will run system clock synchronization at planned intervals to ensure the accuracy and reliability of the date and time in the electronic time stamp.

Date information will also be included in the paper archive records, and time information can be added where necessary. Neither the date nor the time of a written record can be altered without prior permission. Date and time alterations must be signed by auditors for confirmation.

5.5.6 Archive Collection System

The archival information of records of this CA is generated by internal operators of TWCA with independent resources, authority and security controls. The storage information of audit record collection is also generated by the internal control system. The archival records of documentation related to the operations of the certificate management system are collected

and managed by responsible persons.

5.5.7 Procedures to Obtain and Verify Archive Information

Archive information is obtainable only with an authentic written authorization. Auditors are responsible for verifying archive information, and the authenticity of issuer and date of written documents must be verified. The digital signature or cryptographic verification must be applied to verify the archive information in electronic files.

5.6 Key Changeover

To minimize the risk of compromise, CA signing keys must be changed over from time to time.

When changing over a key, this UCA will generate a new key pair. After handing over the key pair to the RCA to issue the certificate, this UCA will notify the relying parties to download this key according to Section 6.1.4.

The validity of subscriber keys must consider the key size, protection, controls and other factors; and no violation of Section 6.1.5 is allowed.

5.6.1 Key Changeover of UCA

The validity period of the key of this UCA for issuing subscriber certificates is equal to the life cycle of the corresponding certificate and must not exceed 10 years.

When the UCA performs key update, a new pair of key pairs will be produced. After the certificate is issued by the RCA, it will be available for relying parties to query and download in accordance with Section 6.1.4.

When the validity period of this UCA's key is about to expire, a new key pair can be generated to apply to this RCA for the issuance of a new certificate. After completion, this UCA must immediately notify the RA and issue subscriber certificates with new private key. CRLs will continue to be issued until the end of the lifetime of the old key.

When there are doubts about the security of this UCA's old key, this UCA must apply to the RCA for revocation of the old certificate before generating a new key pair and issuing a new certificate. After key changeover, the subscriber certificates and CRLs will be issued with the new private key and immediately notify the subscribers and the RA that subscriber certificates and CRLs previously issued with the old private key of this UCA are invalid, subscribers must generate a new key pair to apply to this UCA for a new issuance of certificate.

5.6.2 Key Changeover of RCA

The validity period of the key of this RCA for issuing UCA certificate is equal to the life cycle of the corresponding certificate and must not exceed 25 years.

This RCA will produce a pair of new key pair and self-signed certificate before the expiration of the key usage period. After completion, this RCA must immediately announce the new self-signed certificate and notify subordinate CAs. The old key continues to issue CRLs until the life cycle of the old key ends.

When there are doubts about the security of this RCA's key whose validity period has not expired, the certificate must be revoked before generating a new key pair and self-signed certificate. After key changeover, the subordinate CAs will be notified immediately. At this time, the certificates of subordinate CAs are all invalid, and a new key pair must be regenerated to apply for the issuance of new certificate to this RCA.

When the private key of this RCA is compromised, the certificates of all subordinate CAs must be revoked, and subordinate CAs must be notified to revoke the certificates of all subscribers, and notify the business application system to stop using the certificates issued by the subordinate CA.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The following procedures must be implemented when the UCA's key is compromised or lost (either detected or suspected):

(1) Notify all subscribers and RCA by email or in writing as quickly as possible.

(2) Generate a new key pair and hand it over to RCA to issue a new certificate according to Section 6.1.

(3) Revoke all issued certificates and issue CRLs with the new signing key, this CRL must include all issued but still valid certificates (including certificates revoked prior to the key compromise).

(4) Issue new certificates to all subscribers according to Section 4.3.

(5) Report and disclose the accident information to relying parties and Root CA Programs.

The following procedures must be implemented when the RCA's key is compromised or lost:

(1) All subordinate CAs must be notified as soon as possible through email or in writing, and certificates of all subscribers must be revoked.

(2) Revoke all issued certificates.

(3) Generate a new key pair and self-signed certificate according to Section 6.1.

(4) Issue new certificates to all subordinate CAs.

(5) Report and disclose the accident information to relying parties and Root CA Programs.

This CA must investigate and report to the PMA on the causes of the key compromise or loss, and must propose actions taken to prevent the recurrence of the incident.

This CA establishes Incident Response Plans and Disaster Recovery Plans, and records Business Continuity Plans and Disaster Recovery Procedures in writing. The content includes notification procedures to software vendors (such as browser manufacturers), subscribers, and relying parties in the event of disasters, security breaches, and business interruptions. The above plans and procedures will be regularly revised by this CA every year.

If this CA mistakenly issues or fails to issue S/MIME certificates in accordance with this CPS, the accident will also be disclosed in Bugzilla.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

This CA has established and exercises every year the recovery procedures for computer resource, software and/or data corruption.

When the operations of this CA are interrupted as a result of computer equipment corruption or failure and the signing key remains unaffected, repository operation recovery must be prioritized to quickly restore the certificate issuance, revocation and management functions.

5.7.3 Entity Private Key Compromise Procedures

When a suspected compromise of subscriber keys is detected, proceed with Section 4.9.3.

5.7.4 Business Continuity Capabilities after a Disaster

When the CRL/OCSP repository is unable to recover within 24 hours from the occurrence of a natural disaster or other accident, the facilities in the off-site computer room will be activated, and the CRL/OCSP repository must be recovered within 24 hours from activation.

5.8 CA or RA Termination

When this CA terminates its service, the termination will be proceeded with according to the Electronic Signatures Act.

When this CA terminates system operations due to some reasons, it must minimize the impact on system operations by securely transferring relevant certification business to other CAs to ensure business continuity.

When business terminates under normal circumstances, the contract terminates, or there is an organization restructure without security consideration, the CA must:

(1) Inform the competent authorities 30 days prior to the day of service termination;

(2) Notify subscribers of the fact of service termination and transfer of the relevant business to other CAs and publish such fact on the repository three months prior to the day of service termination;

(3) Transfer the relevant private keys and certificates of this CA to the undertaking CAs in an environment free from security threat;

(4) Transfer to the undertaking CAs the CP, CPS, CA operating manuals and documentation, subscriber agreements and registration data, audit records, archive information, certificate status data and other relevant documents required for business undertaking;

(5) Expunge the relevant private keys of this CA and officially announce to subscribers that the certification business has been transferred to the undertaking CAs.

When the business is terminated under abnormal circumstances (being pronounced bankruptcy or illegal operations by a court of law), this CA must notify subscribers of the truth as quickly as possible and run the operating procedures for business termination under normal circumstances, in order to minimize the impact from business termination.

When this CA terminates its business, the relevant rights and obligations must be subject to the subscriber agreement.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

For generation key pairs this CA must:

(1) Prepare and follow a Key Generation Script;

(2) Use a hardware cryptographic module that at least complies with CNS 15135, ISO 19790, FIPS 140-2 Level 3 or FIPS 140-3 Level 3 to produce key pairs in accordance with the provisions of Section 6.2.1. The private key is stored in the hardware cryptographic module without any leakage after generation; and

(3) Have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process.

For generation key pairs subscribers must:

(1) If the subscriber applies for an AATL certificate, the key storage device must be a hardware device, and the relevant hardware specifications must meet the "Adobe Approved Trust List Technical Requirements".

6.1.2 Private Key Delivery to Subscriber

Private keys are generated by subscribers and thus need no delivery.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber public key is delivered to this CA with the PKCS#10 certificate request file via secured and protected channels. Also, the possession of private key generated is proved with methods specified in Section 3.2.1.

6.1.4 CA Public Key Delivery to Relying Parties

This CA must publish in the repository the certificates it has issued for subscribers and relying parties to check and download.

6.1.5 Key Sizes

The length of the RSA public key of this CA is at least 2048 bits, and the bit length must be

divisible by 8; the security strength of the curve used by the ECC public key is at least P-256.

The length of the subscriber's RSA public key is at least 2048 bits, and the bit length must be divisible by 8; the security strength of the curve used by the ECC public key is at least P-256.

6.1.6 Public Key Parameters Generation and Quality Checking

RSA: This CA adopts the prime number generator uses the ANSI X9.31 Algorithm to generate the prime number required by the RSA Algorithm. This method can ensure that the prime number is Strong Prime. Additionally, the public exponent must contain the following properties: an odd number greater than or equal to 3 and between 2^16 + 1 and 2^256 - 1; the modulus must contain the following properties: an odd number, not a prime power, and not a factor less than 752.

ECC: This CA confirms the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

6.1.7 Key Usage Purposes

Subscribers must use the certificates issued by this CA for electronic signature, encryption, and other purposes with reference to the level of assurance of certificates in accordance with the CPS and the specifications of business application systems. Also, subscribers must follow the instructions specified in the “Key Usage” field in the standard extension of X.509 v3 certificates when using them in the relevant business systems.

Apart from electronic signature and encryption, subscribers requesting certificates for other purposes must apply to this CA for the key and certificate that meet their intended use.

6.2 Private Key Protection and Cryptographic Module Engineering Control

6.2.1 Cryptographic Module Standards and Controls

This CA uses a hardware cryptographic module that must be at least compliant with CNS 15135, ISO 19790, FIPS 140-2 Level 3 or FIPS 140-3 Level 3 as the protection device for private keys, and equipped with multi-person control.

According to the requirements of “Adobe Approved Trust List Technical Requirements”, the private key of AATL certificates must be generated and stored in at least FIPS 140-2 Level 2 or FIPS 140-3 Level 2 or above or equivalent security level Hardware cryptographic modules.

6.2.2 Private Key (m-out-of-n) Multi-Person Control

The private key activation data of this CA is protected by the m-out-of-n multi-person control. It is a perfectly secret way of secret sharing to ensure the secured activation, backup and recovery of private keys.

The smartcard and password for protecting the relevant private key information are controlled by administrators of individual duties and stored in an environment with security controls.

6.2.3 Private Key Escrow

No escrow is allowed for the private key of this CA, nor does this CA provide private key escrow service for certificate subscribers.

6.2.4 Private Key Backup

(1) The private key of this CA is stored in the hardware cryptographic module. It is encrypted before backup with multi-person control according to Section 6.2.2. The information of the private key under multi-person control is stored in the highly secured smartcard.

(2) The smartcard containing the encrypted private key information under multi-person control is stored in a secured environment with dual control and keep in custody by security controllers after sealing.

(3) At least two copies of multi-person control information of the encrypted key must be maintained, with one copy stored at the secured location inside this CA and another copy in the off-site backup site with security control.

6.2.5 Private Key Archival

No private key of this CA will be archived.

6.2.6 Private Key Transfer into or From a Cryptographic Module

The private key of this CA is generated and stored in the hardware cryptographic module. The private key can only be input in another hardware cryptographic module in key backup recovery. When outputting from the cryptographic module, the private key backup procedure specified in Section 6.2.4 must be proceeded.

6.2.7 Private Key Storage on Cryptographic Module

The private key of this CA is stored in the cryptographic module after encryption.

6.2.8 Method of Activating Private Key

The private key stored in the cryptographic module must be activate by at least two authorized officers after identify authentication. The activation is achieved by means of identity authentication with the smartcard. Also, the procedural control of activation must comply with Section 5.2.

6.2.9 Method of Deactivating Private Key

After use, the CA cryptographic module is deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity, to prevent the unauthorized use of the private key.

6.2.10 Method of Destroying Private Key

When the archival period of a private key expires, this CA will run "zeroization" on the memory address where the old private key is stored in the hardware cryptographic module to destroy the old private key in the cryptographic module.

In addition to destroying the old private key in the hardware cryptographic module, the backup copy of the old private key (reserved for three generations) will also be physically destroyed when the backup expires. However, when the backup copy of the key must be used to restore, it will be deleted immediately if there is an expired key in the restored key.

6.2.11 Cryptographic Module Rating

The hardware cryptographic modules used by this CA must at least comply with CNS 15135, ISO 19790 or FIPS 140-2 Level 3, or FIPS 140-3 Level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

This CA will archive certificates issued when their life-cycle expires, including the corresponding public key.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Maximum validity period of certificates:

Type	Private Key Usage	Certificate Term/ Public Key Usage
RCA Certificate	25 years	25 years
UCA Certificate	10 years	10 years

InfoSec Certificate	39 months	39 months
AATL Certificate	39 months	39 months
S/MIME certificate	825 days	825 days
TSA Certificate	15 months	135 months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data for activating the signature private key are generated individually by multiple smartcards and protected by multi-person control in duty separation. The activation data stored in the smartcard is read by the card reader and accessed after identity authentication with the personal identification number (PIN) of the smartcard.

6.4.2 Activation Data Protection

The activation data are protected by a set of smartcards, and the smartcard PIN is kept by the card custodian without recording in any medium. When users fail to log into the system with the smartcard after three attempts, the smartcard will be locked. When handing over the smartcard, the new custodian must change the PIN.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

This CA and relevant supporting systems provide the following security controls with operating systems, or by integrating with operating systems, software and physical protection:

(1) System login with identification authentication and multi-factor.

(2) User-defined access control.

(3) Security audit ability.

(4) Restrictions on various certificate services and the access control of trusted roles.

(5) Identification and authentication of trusted roles and identity.

(6) Assurance of communication and database security.

(7) Secured and reliable channels for the identification of trusted roles and relevant identity.

(8) Protection for procedural integrity and security controls.

6.5.2 Computer Security Rating

The security rating of the computer operating systems used by this CA must at least comply with EAL3 [ISO/IEC 15408 Common Criteria] or C2 [TCSEC] or E2 [ITSEC].

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

This CA follows the ISO 27001 specifications in system development.

Both hardware and software of this CA used only are components complying with the security policy , and no irrelevant hardware devices, network connection or software components are installed. Also, programs are scanned for malicious codes every time before use.

6.6.2 Security Management Controls

Prior to software installation, this CA validates the correct version is provided by developers, and the software is unmodified. After software installation, this CA verifies its integrity when running it.

This CA records and controls the configuration and functional changes of systems.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The Certificate Management System of this RCA is an Off-Line, independent operation management system, and only business-related operators can perform operations manually after authorization.

Only authorized personnel of the relevant business can implement management work with the certificate management system of this CA. These personnel must pass the identity authentication by accessing to the certificate management system over the network before they are allowed to access the system.

To prevent network intrusion and damage, each host of this CA is equipped with firewalls, intrusion prevention and anti-virus systems to enhance network security, and regularly performs system patch updates and system vulnerability scans to strengthen protection.

The hosts and internal databases of this CA are connected only to the intranet and segregated from outside by means of a firewall. Connections with the internal hosts must pass the identity authentication, and only authorized personnel or systems can access to the internal host.

Repositories are connected to the Internet to provide uninterrupted certificate and CRL/OSCP enquiry service (except for necessary maintenance and backup).

6.8 Time Stamping

The CA regularly calibrates the time through the trusted time source to ensure the accuracy of the time values of each operation of the Certificate Management Center, including but not limited to the following time values:

(1) Time of certificate issuance;

(2) Time of certificate revocation;

(3) Time of CRL issuance; and

(4) Time of OCSP issuance.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

This CA uses and issues to subscribers X.509 version 3 certificates.

7.1.2 Certificate Extensions

RFC 5280-compliant certificate extensions are included in certificates issued by this CA. These extensions are detailed in the certificate profile and CRL profile of this CA.

The S/MIME certificate issued by this CA complies with the following:

(1) contain a Mailbox Address of the Subject via rfc822Name or otherName value of type id-on-SmtpUTF8Mailbox in the Subject Alternative Name (SAN) extension;

(2) the value *id-kp-emailProtection* must be present in the *extKeyUsage* extension; and

(3) the OCSP service URL can be obtained in the extension field of *authorityInfoAccess*.

7.1.3 Algorithm Object Identifiers

The following algorithm object identifiers are used in certificates issued by this CA.

Type	Algorithm	Object Identifier
Key	rsaEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
Key	ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) ecPublicKey(1)}
Signature	sha256WithRSAEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
Signature	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}

Signature	ECDSAWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
Signature	ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

7.1.4 Name Forms

The subject and issuer DN fields of the certificates and subscriber certificates of this CA comply with the uniqueness of X.500 distinguished name (DN) and the RFC 5280 rules.

7.1.5 Name Constraints

This CA issues certificates with no *nameConstraints* extension field.

7.1.6 Certificate Policy Object Identifier

The CP object identifier defined in the CP is used in the *certificatePolicies* extension of the certificates issued by this CA.

7.1.7 Usage of Policy Constraints Extension

The *policyConstraints* extension is added to the certificates issued by this CA where appropriate.

7.1.8 Policy Qualifiers Syntax and Semantics

The *policyQualifier* syntax and semantics are added to the certificates issued by this CA where appropriate.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

The service URL can be obtained in the *cRLDistributionPoints* extension field of subscriber certificates. The frequency of CRL Issuance by this CA is as specified in Section 4.9.7.

7.2.1 Version Number(s)

This CA issues X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The extensions are detailed in the certificate and CRL profiles of this CA.

7.3 OCSP Profile

The service URL can be obtained in the *authorityInfoAccess* extension field of subscriber certificates. The OCSP Responder provided by this CA complies with the following:

(1) The SHA-1 algorithm is prohibited for the signing certificate used in response, and this certificate must be issued by this CA;

(2) The signature value of the response is prohibited from using the SHA-1 algorithm;

(3) Reponses for certificate status support: good, revoked, and unknown;

(4) When receiving a status query request for a certificate not issued by this CA, it will reply with a message that the certificate status is unknown; and

(5) Refer to Section 4.9.9 for other content.

7.3.1 Version Number(s)

Version 1 of OCSP specification as defined by RFC 6960 is supported.

7.3.2 OCSP Extensions

The extensions of the OCSP comply with the RFC 6960 specification.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

This CA must conduct external audits at least once a year and internal audits at least once six months.

The RA to which this CA belongs can audit itself, except being audited only by the external RAs authorized to issue certificates for specific groups. All other RAs must be audited by this CA or an external auditor assigned by this CA.

8.2 Identity/Qualifications of Assessors

Auditors implementing internal and external audits must be equipped with the knowledge in CA and IT system security audit, have at least 2 years of practical audit experience or certificate practice experience, must be familiar with the operation rules of the CPS, and possess knowledge and experience related to the operations of application system and computer hardware and software systems. When competent authorities have set the requirements for the qualifications of auditors, these requirements must prevail.

External audits must be conducted by qualified professional audit firms complied with the requirements of MRSP (Mozilla Root Store Policy). Auditors carrying out the external audit must hold the national auditor qualification or internationally recognized auditor qualification to provide objective and unbiased audit service. This CA must identify the identity of auditors prior to the audit. After the audit is completed, the audit report will also list the audit qualifications and audit certificates of the auditors.

8.3 Assessor's Relationship to Assessed Entity

Internal auditors of this CA carrying out an audit must be independent from the units audited and have no conflict of interest with the audited units to ensure the objectivity of audit. Auditors should perform the audit and assessment with an independent, impartial and objective attitude.

This CA will assign audit organizations to perform the external audit.

8.4 Topics Covered by Assessment

Audits should be carried out to verify if:

(1) the CPS and relevant codes of operations are established and published, including the operating specifications of the CPS;

(2) if certificate management is carried out according to the CPS and the relevant codes of operations to meet the requirements for certificate service integrity and CA environment security controls; and the relevant operations are carried out according to the CPS and the relevant codes of operations to meet the requirements for certificate service integrity and CA environment security controls;

(3) CPS is complied with the CP regulations.

The audit schemes of this CA are:

- WebTrust for CAs v2.2.1 or newer;
- WebTrust for CAs SSL Baseline with Network Security v2.5 or newer.

8.5 Actions Taken as a Result of Deficiency

When nonconformities to the CPS are detected in the detailed assessment, auditors must list the defects detected in detail by severity and notify this CA. This CA must propose corrective and preventive actions, and follow up on the improvement.

If the S/MIME certificate operation accident is found in the audit, this CA will take the initiative to reveal the major defects to Bugzilla.

8.6 Communication of Results

This CA will publish the latest and previous WebTrust audit reports in the repository. At the same time, TWCA will reveal the obtained International Seals on the official website, click the seal icon for the WebTrust audit reports.

8.7 Self-Audits

This CA monitors adherence to its CP, CPS and strictly control its service quality by performing self-audits at least once six months.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

This CA will charge subscribers for certificate issuance. The fee will be specified in the application form or published on the website of this CA.

9.1.2 Certificate Access Fees

Free of charge.

9.1.3 Revocation or Status Information Access Fees

Free of charge.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

When subscribers apply for a refund after completing the certificate request but prior to certificate issuance, this CA will return the certificate issuance fee to subscribers without interest after deducting a handling fee of NT$3,000. When the request of refund is made after certificate issuance, this CA will return the certificate issuance fee to subscribers without interest after deducting the monthly fee of certificate use plus a handling fee of NT$3,000.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

(1) This CA assumes no responsibility for indemnifying any damages arising from or in connection with the processing of subscriber registration data and certificate issuance; except for losses caused by this CA's failure to follow this CPS, the CP and/or the relevant codes of operations as a result of negligence attributable to this CA.

(2) This CA assumes no responsibility for indemnifying any damages arising from or in connection with losses as a result of an act of God or natural disasters (e.g. earthquakes) and/or events (e.g. wars) beyond the reasonable control of this CA.

(3) This CA must indemnify the direct damages caused to subscribers according to relevant regulations as a result of the intention or negligence of operators; failure to register, issue and revoke subscriber certificates according to this CPS, the CP and/or the relevant codes of operations; or violation of the relevant laws and regulations.

(4) This CA assumes no responsibility for indemnifying any damages arising from or in connection with legal disputes over the use of a subscriber certificate from receiving a revocation request made by this CA or persons who can make a revocation request until the publication of certificate revocation listed in CRLs, provided that this CA processes the revocation request according to this CPS and the relevant codes of operations.

(5) This CA assumes no responsibility for indemnifying any damages arising from or in connection with the use of illegal, fabricated or erroneous certificates.

(6) The statue of repose of the subscriber's claim for damages is subject to the relevant laws and regulations.

9.2.2 Other Assets

In financial audit, this CA assigns impartial and objective third party to audit our financial operations every year.

In risk management, this CA has applied for earthquake and fire insurance for the building and the hardware facilities inside. Also, this CA has applied for liability insurance at US$2 million and professional liability insurance at US$5 million to disperse operational risk

9.2.3 Insurance or Warranty Coverage for End-Entities

Subject to Section 9.2.1.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Confidential information includes:

(1) The private key and password for operating this CA.

(2) The multi-person control data for controlling the private key of this CA.

(3) The personal data of the representative and agent applying for certificates.

(4) Records valid for audit and traceability generated and/or held in custody by this CA.

(5) Audit records and documents generated by auditors during the audit.

(6) Classified operation-related documents.

9.3.2 Information Not Within the Scope of Confidential Information

The CP, this CPS, certificates issued by this CA, CRLs issued by this CA, and results of external audits are not within the scope of confidential information.

9.3.3 Responsibility to Protect Confidential Information

No subscriber's personal information and identity verification data be disclosed to the competent authorities or any person, except under any of the following circumstances:

(1) Disclosure made by the law with the authorization of the competent authorization given according to the regulatory procedures.

(2) Disclosure requested according to the regulatory procedure by an arbitration organization within the jurisdiction of the Company Act for handling disputes arising from or in connection with certificates.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

This CA protects personal information according to the Personal Information Protection Act and the relevant government regulations.

9.4.2 Information Treated as Private

Subject to Section 9.4.1.

9.4.3 Information Not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

Subject to the relevant laws and regulations.

9.4.5 Notice and Consent to Use Private Information

Subject to the relevant laws and regulations.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Subject of Section 9.3.3.

9.4.7 Other Information Disclosure Circumstances

Subject of Section 9.3.3.

9.5 Intellectual Property Rights

(1) The outcomes of the key pairs and key shadow generated by this CA are the intellectual property of TWCA.

(2) The certificates and CRLs issued by this CA are the intellectual property of TWCA.

(3) Subscriber key pairs are treated as the intellectual property of their subscribers. However, when their public keys are issued as certificates by this CA, such certificates are the intellectual property of TWCA.

(4) This CA must ensure the correctness of subscriber names, without guaranteeing the ownership of the intellectual property right of the subject DN in the subscriber certificate.

(5) The intellectual property right of documents written by this CA for CA operations is owned by TWCA.

(6) The intellectual property right of this CPS is owned by TWCA.

(7) This CPS is available for free download from the repository of this CA or distributable according to the relevant regulations in the Copyright Act after being authorized by TWCA.

(8) No one can charge for the distribution of this CPS.

(9) This CA assumes no responsibility for the consequences as a result of improper use or distribution of this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

(1) To establish, publish and manage the CPS and CP for certificate issuance and the SOPs related to certification.

(2) To confirm the representations and warranties between this CA and RA, and RA must practice in accordance with this CPS, the CP, and related SOPs.

(3) To confirm the selection of certification system personnel (including independent contractors) and ensure that system operation conforms to the CPS.

(4) Operators must take good care of the registration and certificate data and related information of subscribers to prevent leakage, marauding, interpolation and/or unintended use of such data and information.

(5) To accept the request of certificate, certificate rekey, certificate suspension, certificate revocation, and certificate status check made by subscribers (RA) and the related information of registration request; to confirm the accuracy and integrity of the related transaction information delivered to this CA by RA and subscribers; to issue certificates; and to accurately and securely deliver related replies to subscribers in accordance with the CPS.

(6) To accurately and securely deliver TWCA certificates and CRLs to the repository in accordance with the CPS.

(7) To explain the detailed operating procedure of the request of certificate, certificate rekey, certificate suspension, certificate revocation, certificate registration and use, and the related representations and warranties in the contract or related documents for subscribers.

(8) The private key of this CA can only be used to issue and revoke subscriber certificates. If information encryption or another signing task is required, this CA must use a different and independent private key.

This CA Warranties the following:

- Right to Use Domain Name or IP Address: as described in section 3.2.2
- Authorization for Certificate: as described in section 3.2.2 and 3.2.3.
- Accuracy of Information: as described in section 3.2.2 and 3.2.3.
- No Misleading Information: as described in section 3.2.2 and 3.2.3.
- Identity of Applicant: as described in section 3.2.2 and 3.2.3.

9.6.2 RA Representations and Warranties

(1) To confirm the representations and warranties between RA and subscribers; and to verify the legitimacy and integrity of the request information when implementing the identity authentication in subscriber registration and certificate request, rekey request, suspension request, and renovation request in accordance with this CPS, the CP and RA SOP.

(2) To confirm the selection of RA certification system personnel (including independent contractors) and ensure that system operation conforms to the CPS and RA SOP.

(3) When make a registration request, RA must ensure that subscribers really understand and agree to the representations and warranties specified in the application form and contract, and the contents of business-related SOPs. RA must also ask subscribers (or the legally authorized agent of corporations) to sign in the related documents, or ask subscribers to sign in the document according to the SOP of the level of assurance at which subscribers authenticate their identity.

(4) To accept the request of subscriber registration, certificate, certificate rekey, certificate suspension, certificate status check, and certificate revocation.

(5) To verify the legitimacy and accuracy of subscriber identity in a request of subscriber registration and a request of certificate; and to securely deliver to subscribers the correct reply sent from this CA after notifying this CA to issue certificates to subscribers.

(6) RA and RA operators must take good care of the registration and certificate data and related information of subscribers to prevent leakage, marauding, interpolation and/or unintended use of such data and information.

(7) To explain the detailed operating procedure of the request of certificate, certificate rekey, certificate suspension, certificate revocation, certificate status check, certificate registration and use, and the related representations and warranties in the contract or related documents for subscribers.

(8) When there are doubts regarding the marauding, exposure and/or loss of the corresponding private key of RA and certificates; or when there is a change in the related RA information in the certificate, RA must immediately report to this CA issuing that certificate for handling in accordance with the related SOPs.

(9) RA assumes the representations and warranties relating to subscriber registration. This CA assumes the representations and warranties relating to the issuance of certificate commissioned by RA. RA must provide the information regarding the above representations and warranties for subscribers and trustees.

9.6.3 Subscriber Representations and Warranties

(1) When registering to RA, subscribers must submit detailed and correct documents and data of identity.

(2) When registering to RA, subscribers must understand and agree to the representations and warranties in the application form and contract, and the contents of the SOPs relating

to the request of certificate, certificate rekey, certificate suspension, certificate revocation, certificate registration and use; and accept such prior to signing in the related documents.

(3) Subscribers must exactly and properly generate and protect their private key and private key protection password securely; and must not disclose or lend such to any third party.

(4) When accepting the subscriber certificates issued by TWCA, subscribers must verify the legitimacy of the identity of subscriber and this CA, and the integrity and validity of certificate information.

(5) Subscriber must understand and agree to the SOPs specified in the CPS; legally and correctly use the private key and certificate in the related business systems; and engage in any operation breaking the law and infringing the rights of a third party.

(6) When there are doubts regarding the marauding, exposure and/or loss of the corresponding private key of certificates; or when there is a change in the related subscriber information in the certificate, subscribers must immediately report to RA for handling in accordance with the related SOPs.

9.6.4 Relying Party Representations and Warranties

(1) When using certificates, relying parties must understand and agree to the CPS and the representations and warranties specified in the SOP of related business systems. Relying parties also use certificates in related business systems according to the business category specified in the certificate and this CPS without breaking the law and infringing the rights of a third party.

(2) When using certificates, relying parties must verify the accuracy and validity of certificates from the certificate chain via verifying the certificate status through CRL/OCSP in accordance with the CPS, the SOP of application business systems, and X.509 certificate standards. If relying parties query the S/MIME certificate through OCSP Responder, relying parties must first verify the digital signature of the OCSP response.

(3) When verifying the validity of transaction information, apart from verifying the validity and legitimacy of subscriber certificates, underlying parties must verify the transaction amount limit, liability amount limit, business category, and liability of certificates in accordance with the CPS and the SOP of related business systems.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

(1) This CA assumes no responsibility for indemnifying any damages arising from or in connection with the processing of subscriber registration data and certificate issuance; except for losses caused by this CA's failure to follow this CPS, the CP and/or the relevant codes of operations as a result of negligence attributable to this CA.

(2) This CA assumes no responsibility for indemnifying any damages arising from or in connection with losses caused to subscribers or relying parties as a result of an act of God or natural disasters (e.g. earthquakes) and/or events (e.g. wars) beyond the reasonable control of this CA.

(3) This CA is liable to indemnify the damages arising from or in connection with the damage caused to a third party from the leakage, marauding, interpolation or unintended use of the registration and/or certificate data of subscribers as a result of the failure to keep such data in custody with due faith and due care of this CA.

(4) After receiving a request of certificate revocation, this CA must finish revoking the requested certificate within the time limit defined in Section 4.9.1 and issue and complete publishing the CRL to the repository according to frequency defined in Section 4.9.7. Prior to CRL publication, subscribers must take actions appropriate to minimize the impact on trustees and assume all liabilities resulting from the related certificates.

9.8 Limitation of Liability

The liability of this CA for liability events arising from or in connection with the issuance or use of certificates occurred to subscribers or trustees is specified in Section 1.4.2.

9.9 Indemnities

Subject to Section 9.2.1.

9.10 Term and Termination

9.10.1 Term

This CPS is effective after being approved by the competent authorities according to the Electronic Signatures Act and published by this CA in the repository.

9.10.2 Termination

When the new version of this CPS is approved and published by the competent authorities, the existing version will be terminated.

9.10.3 Effect of Termination and Survival

The effect of this CPS remains valid until the expiration or revocation of the last certificate issued according to this CPS.

9.11 Individual Notices and Communications with Participants

This CA will establish contact channels with subscribers with appropriate methods. These will include, but are not limited to, telephone, fax and/or email.

9.12 Amendments

9.12.1 Procedure for Amendment

(1) This CA is the responsible unit of this CPS. This CA must revise this CPS at least once a year. Amendments include addenda or direct amendments of the CPS contents.

(2) This CPS will be amended accordingly when the CP is amended or OID is changed.

(3) This CPS will also be amended accordingly when there is a change in the legislative requirements and/or international standards.

(4) After being reviewed and approved by the competent authorities, this CPS will be published in the repository according to Chapter 2.

9.12.2 Notification Mechanism and Period

(1) Should there be suggestions for updating this CPS, please deliver them to the contact person specified in Section 1.5.2 by mail or email to forward them to the PMA of TWCA.

(2) After being reviewed and approved by the competent authorities, amendments of this CPS will be published in the repository for download.

(3) Unless otherwise specified, this CA will contact subscribers according to the methods specified in Section 9.11.

9.12.3 Circumstances Under Which OID Must Be Changed

The OID of the normative CP used in this CPS will remain unchanged when the contents of this CPS are amended. Only the version OID of CPS version will be added.

9.13 Dispute Resolution Provisions

Subscribers must seek resolutions for disputes over the services of this CA or the certificates it

issues according to the following rules:

(1) Both parties of the dispute must seek reasonable resolutions through negotiations with due faith.

(2) When both parties of the dispute are unable to seek reasonable resolutions within thirty days, a qualified third party must be assigned as the mediator of the dispute, in order to mediate and resolve the dispute.

(3) When both parties of the dispute are unable to agree to the mediations and decisions made by the mediator within sixty days, both parties agree that the Taipei District Court of Taiwan will be the jurisdiction court for the first instance.

(4) The sharing of the fees and charges arising from the negotiation and litigation of the disputes must be determined through negotiations or according to the relevant laws and regulations.

(5) When the dispute is a transnational or trans-regional dispute that cannot be resolved according to the said procedures, both parties must seek resolutions through international arbitration.

9.14 Governing Law

The interpretation of the contents of this CPS and the implementation of the relevant business of this CA are subject to the relevant regulations of the competent authorities and the law of this country.

9.15 Compliance with Applicable Law

This CPS and this CA must comply with the Electronic Signatures Act and the Enforcement Rule of the Electronic Signatures Act.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

When it is necessary to amend some sections of this CPS when they are obsolete, other sections remain valid and unaffected by those obsolete sections until the new version of this CPS is completed and published.

This CPS is amended according to Section 9.12.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

This CA assumes no responsibility for indemnifying the damages arising from or in connection with an act of Act or natural disasters (e.g. earthquakes) and/or events beyond the reasonable control of this CA (e.g. wars).

9.17 Other Provisions

No stipulation.

Appendix 1: Glossary

(1) Internet

It refers to the interconnection of various computer networks using a standard protocol for information interchange.

(2) (Electronic) Message

It refers to the record validity for expressing the intent of a text, voice, image, symbol or other data generated electronically, magnetically or with any means that cannot be directly perceived by the human senses but for electronic processing.

(3) RSA Algorithm

It refers to an asymmetric encryption algorithm proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. Its security strength is based on the difficulty of factoring the product of two large prime numbers, the “factoring problem”.

(4) Elliptic Curve Cryptography (ECC)

It refers to a public key encryption algorithm based on elliptic curve mathematics. It was proposed by Neal Koblitz and Victor Miller in 1985. Its security strength is based on the difficulty of solving elliptic curve discrete logarithm problems (ECDLP).

(5) ECC P-256 Curve

The elliptic curve standard formulated by NIST in FIPS 186-3, which defines the relevant parameters p, a, b, G, n, h of the elliptic curve where the length of the x and y coordinates of the base point G of the curve is 256 bits respectively .

(6) Electronic Signature

It refers to a data message presented in an electronic format attaching to an electronic document that can identify and validate the identity of the person signed the electronic document; and the message generated by the signed person with digital, voice, fingerprint or other biometrical or optical technology attaching to the electronic message containing the same effect of a signature for identifying and validating the identity of the signed person and identifying the integrity of the signed message.

(7) Encrypt/Encipher

It refers to use of mathematical algorithms or other means to encipher an electronic document, so as to ensure information security in transmission.

(8) Decrypt/Decipher

It refers to the reduction of an encrypted or enciphered message that is unable to identify or interpret by humans with relevant mathematical algorithms or other means into a message that can be identified and interpreted by humans.

(9) Digital Signature

A digital signature is a kind of electronic signature. It refers to a data message that can identify the authenticity of the signed person and his electronic document with corresponding public key can verify this encrypted digital message. A digital signature uses the asymmetric cryptosystem and hash function to compress a digital message of a particular size before encrypting with the private key of the signed person.

(10) Private Key

It refers to a set of matching digital data that kept by the signed person for generating and verifying a digital signature. Apart from generating the digital signature, these digital data can be used to decrypt electronic messages.

(11) Public Key

In the digital signature using asymmetric cryptosystem, it refers to a set of matching public digital data for generating and verifying a digital signature. It can be used to verify the correctness of data in messages signed by the signed person, and can encrypt delivery messages when running the message privacy function.

(12) <Public Key>Certification or Certificate

It refers to a computer-based digital record issued by the CA containing the registration identifier of the applicant, the public key, the validity of the public key, the registration identifier and signature of the CA, and other identifying information to validate the identity of the signed person and to prove his possession of the paired public and private keys.

(13) Certification Authority or Certificates Authority (CA)

It refers to the authority providing digital signature generation and electronic certification services; i.e. it is an authority examining the correctness of the identity data of the

applicant and his connection and legitimacy with the public and private keys to be verified in an unimpaired and objective position in order to issue the public key certificate.

(14) Certification Practice Statement (CPS)

It refers to the operating and application procedures for the CA to offer certificate issue, revocation and enquiry services to subscribers. The CPS includes the public key architecture and security mechanism and operating specifications and procedures of certification, the security mechanisms of CA hardware and software implementation, responsibility and authority management, and the relevant rules.

(15) Asymmetric Cryptosystem

It refers to a computer-based mathematical algorithm for generating and using an arithmetically correlated secure key pair. The private key generated can be used as the message signature, and the corresponding public key can verify the signed message. The public key can also encrypt a message, and the corresponding private key can decrypt the message encrypted with the public key.

(16) Hash Function

It is an algorithm that can concert a long message (containing many bytes) into a fixed size message. The output of the same message after compression function computing must be identical, and it is absolutely impossible to reduce the input message from the output message.

(17) Automated Certificate Management Environment (ACME)

A communication protocol for automating certificate-related automating interactions (such as certificate requests) between a certificate authority (CA) and its user's server, allowing users to automate the deployment of public key infrastructure at a very low cost. The protocol mainly transmits formatted JSON messages through HTTPS, and the relevant standards are defined in RFC 8555.

(18) Certificate Signing Request (CSR)

An encoded file that allows certificate applicants to pass the public key and identifying information (such as domain names) to the certificate authority for certificate issuance in a standardized way. This file also provides proof-of-possession of the private key.

(19) Issue a Certificate (Electronic Certification)

It refers to the public key certificate or other certificates issued by the certification center (CA) after reviewing the qualifications and relevant documents of the public key certificate applicant and verifying the matching relationship between the public and private keys according to the CPS.

(20) Public Suffix List (PSL)

A public resource created by Mozilla, the list is located at https://publicsuffix.org/, which consists of two parts: one is a list of TLDs (Top Level Domains) provided by ICANN, and one is a PRIVATE list provided by individuals or institutions.

(21) Bugzilla

It is a web-based general-purpose bug tracking system of browser issues maintained by Mozilla. CAs must report major failures to https://bugzilla.mozilla.org/home.

(22) Secure Multipurpose Internet Mail Extensions (S/MIME)

It is an Internet standard that expands the MIME protocol in terms of security, and can encapsulate MIME data (such as digital signatures and encrypted information) into secure objects, adding message authenticity, integrity and confidentiality to email applications.

Appendix 2: Acronyms and Abbreviations

ACME	Automated Certificate Management Environment
ANSI	American National Standard Institute
CA	Certification Authority
CC	Common Criteria
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing request
DN	Distinguished Name
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standard
ISO/IEC	the International Organization for Standardization, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
OCSP	Online Certificates Status Protocol
OID	Object Identifier
MRSP	Mozilla Root Store Policy
PMA	Policy Management Authority
PIN	Personal Identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure

RA	Registration Authority
RCA	Root Certification Authority
RSA	Rivest, Shamir, Adleman (encryption algorithm)
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location