Document History

Version	Effective Date	Issuer	Remarks
1.0	2001/04/01	TaiCA PMA	Initial CP Publication.
1.1	2002/01/01	TaiCA PMA	Revised to integrate with TaiCA CA PKI system documents (CPS, CP, etc.) and Trade-Van EDI Pan-Asian E-Commerce Alliance (PAA CP).
1.2	2002/04/01	TaiCA PMA	Revised in compliance with the regulations set by the Department of Commerce, MOEA, regarding the required content of Certification Practice Statements and the Regulations Governing Certification Authorities.
1.3	2008/08/13	TWCA PMA	Approved and updated by PMA.
1.4	2009/03/30	TWCA PMA	Supplemented Assurance Level OIDs and revised public key validity periods.
1.5	2009/08/04	TWCA PMA	Revised Section 6.3.2 based on PMA meeting resolutions on 2009/07/29.
1.6	2012/08/22	TWCA PMA	Revised Section 1.2 based on PMA meeting resolutions on 2012/08/22; added OID for "Business EC Certificate".
2.0	2012/11/23	TWCA PMA	Revised Section 1.2 based on PMA meeting resolutions on 2012/11/23; added company OID applied from IANA, and adjusted OIDs for each CA.
2.1	2013/12/26	TWCA PMA	Revised Section 1.2 based on PMA meeting resolutions on 2013/12/26; added OID for Device Certificates.
2.2	2019/5/15	TWCA PMA	Revised in accordance with CABF Baseline Requirements V1.6.4. Added CA/Browser Forum CP OID. Revised to comply with Adobe AATL trust root program. Removed regulations related to Internet NB certificates.
2.3	2021/8/4	TWCA PMA	Removed RSA 1024-bit keys and added maximum key validity periods for ECC P-256 and P-384. Added OID for Time-Stamping Certificates.
2.4	2022/5/5	TWCA PMA	Device Certificates merged into TLS/SSL Certificates. Removed unused OIDs for TLS/SSL and EV SSL Certificates. Added description of certificate types applicable to BR. Unified names for TLS/SSL and EV SSL Certificates.
2.5	2022/10/30	TWCA PMA	Removed CP OID for Device Certificates. Adjusted Section 1.2 Entity OIDs. Adjusted Section 1.4 Certificate Usage. Adjusted Section 3.2.2 Organization Identity Authentication. Adjusted Section 3.2.3 Individual

Version	Effective Date	Issuer	Remarks
			Identity Authentication. Adjusted Section 5.5.2 Archive Retention Period. Adjusted Section 7.1.3 OIDs. Renamed "InfoSec UCA Certificate" to "InfoSec Certificate". Renamed "TLS/SSL Certificate" to "SSL Certificate". Unified CABF terminology. Added Sections 1.6 and 8.7.
2.6	2023/7/20	TWCA PMA	Defined S/MIME certificate types and added descriptions regarding S/MIME BR compliance.
2.6.1	2024/7/1	TWCA PMA	Annual review with no changes; updated version number.
2.6.2	2025/6/30	TWCA PMA	Annual review with no changes; updated version number.
2.6.3	2025/11/15	TWCA PMA	1.2.1 Removed unused OIDs. 3.1.2 Adjusted description of Distinguished Name meaning. 3.1.3 Adjusted regulations for pseudonyms and anonymity. 3.2.1 Updated RFC documents. 6.5.2 Updated computer system security level requirements. 6.1.5, 6.3.2, 7.1.3 Added PQC-related algorithms.
2.8	2026/6/8	TWCA PMA	Certificate Policies for SSL Certificates and EV SSL Certificates merged into "TWCA CYBER CA CP/CPS"; original contents removed.

1 Introduction

TAIWAN-CA INC. (hereinafter referred to as "the Company" or "TWCA") was established through a joint investment by the Taiwan Stock Exchange, Taiwan Depository & Clearing Corporation, Financial Information Service Co., Ltd., and HiTRUST.COM Inc.

To establish a secure and reliable online transaction environment, ensuring that information transmitted over the network is resistant to forgery, tampering, or theft, and to authenticate the identities of transacting parties while preventing non-repudiation of completed transactions, TWCA has established a Public Key Infrastructure (TWCA PKI, hereinafter referred to as "this PKI"). TWCA serves as the Root Certification Authority (RCA), acting as the Trust Anchor, while simultaneously constructing Subordinate Certification Authorities (Subordinate CAs). This infrastructure provides subscribers with online identity verification and transaction authentication services, thereby building users' confidence in e-commerce transactions and protecting the rights and interests of all participating parties.

To provide the certificate services urgently needed by subscribers engaging in Internet transactions, the Company has built an Internet authentication service system equipped with security mechanisms related to certification. This system utilizes state-of-the-art public key cryptography. Its security standards comply with the "Security Control Guidelines for Electronic Banking Businesses Conducted by Financial Institutions" issued by the Ministry of Finance. The system provides the essential security controls required for secure online transactions, including non-repudiation, subscriber authentication, message

integrity verification, message encryption, and other security control mechanisms. It is applicable to Internet electronic banking and online trading systems, as well as e-commerce systems for insurance, bonds, corporate quoting, procurement, and payment transactions.

1.1 Overview

The Certificate Policy of the TAIWAN-CA INC. Public Key Infrastructure (hereinafter referred to as "this Policy" or "TWCA PKI CP") is a technical policy document formulated in accordance with the Electronic Signatures Act and relevant international standards (such as IETF RFC 3647). It serves as the basis for various Certification Authorities (CAs) within this PKI to draft their respective Certification Practice Statements (CPS).

To accommodate the specific security control requirements of various industries for e-commerce, this PKI comprises different types of CAs. The operational procedures, certificate applicability, rights and responsibilities, and the operational mechanisms of certificate management for each CA must comply with the provisions set forth in this Policy.

The following matters were specifically considered during the formulation of this Policy:

- Whether a Relying Party can identify the correlation between the certificate holder (individual subscriber, corporate subscriber, or subscriber of relevant hardware/software and application systems) stated in the certificate and the Public Key listed therein.
- Whether a Relying Party can confirm that the certificate holder possesses the corresponding Private Key.
- Whether subscribers and Relying Parties can trust the CAs within this PKI, as well as the security of their systems, keys, and procedures.
- Compliance with the regulations of the Electronic Signatures Act.

1.2 Document Name and Identification

1.2.1 Object Identifiers (OIDs) of this Policy

This Policy defines different Object Identifiers (OIDs) corresponding to the issued certificate content, certificate types, and applicability.

The OIDs of this Policy are as follows:

- `{ joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) CP(5) id-TWCA-PKI-CP-policy(5) } (2.16.158.3.1.5.5)`
- `{ ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) } (1.3.6.1.4.1.40869.1.1)`

The CP OIDs according to different certificate types are as follows:

Certificate Type	OID 1	OID 2
Business XML Certificate	{ joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) XML(8) id-CP-policy(5) } (2.16.158.3.1.8.5)	{ ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA (40869) certificates(1) policies(1) XML(12) } (1.3.6.1.4.1.40869.1.1.12)
Business EC Certificate	{ joint-iso-itu-t(2) country(16) Taiwan(886) TWCA(3) CA(1) EC+(3) id-CP-policy(1) } (2.16.886.3.1.3.1)	{ ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) EC(11) } (1.3.6.1.4.1.40869.1.1.11)
Customs Clearance Certificate	{ joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) FXML(5) id-CP-policy(5) } (2.16.158.3.1.5.5)	
InfoSec Certificate	{ joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) InfoSec(8) id-CP-policy(5) } (2.16.158.3.1.8.5)	{ ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) InfoSec(23) } (1.3.6.1.4.1.40869.1.1.23)
AATL Certificate	{ ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) AATLCert(26) } (1.3.6.1.4.1.40869.1.1.26)	
Time-Stamping Certificate	{ ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) TSACert(27) } (1.3.6.1.4.1.40869.1.1.27)	
S/MIME Certificate	{ ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) SMIMECert(28) } (1.3.6.1.4.1.40869.1.1.28)	

1.2.2 Other Policy OIDs

CA/Browser Forum (CABF) Certificate Policy OIDs are as follows:

Policy	OID
CA/Browser Forum (CABF)	`{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1)} (2.23.140.1)`

The corresponding CABF OIDs according to different certificate types are as follows:

S/MIME BR Type	Legacy	Multipurpose	Strict
Mailbox-validated	`(2.23.140.1.5.1.1)`	`(2.23.140.1.5.1.2)`	`(2.23.140.1.5.1.3)`
Organization-validated	`(2.23.140.1.5.2.1)`	`(2.23.140.1.5.2.2)`	`(2.23.140.1.5.2.3)`
Sponsor-validated	`(2.23.140.1.5.3.1)`	`(2.23.140.1.5.3.2)`	`(2.23.140.1.5.3.3)`
Individual-validated	`(2.23.140.1.5.4.1)`	`(2.23.140.1.5.4.2)`	`(2.23.140.1.5.4.3)`

All CAs within this PKI shall specify the referenced OIDs of this Policy in their Certification Practice Statements (CPS); if new OIDs need to be added due to new certificate applicability to ensure identification, they must be expanded under the respective CP OIDs defined in this Policy.

1.3 PKI Participants and Applicability

All entities referencing this Policy are participants of this PKI.

When the public key certificates of natural persons or legal entities governed by this Policy are used in application transaction systems, they can provide identity verification of the transaction initiator and receiver, message integrity verification, message confidentiality protection, applicability of non-repudiation mechanisms, rights and obligations, and operational guidelines to be followed when using the certificates.

1.3.1 Certification Authorities (CA)

Certification Authorities are primarily responsible for the issuance and management of certificates, and are categorized into Root Certification Authorities and Subordinate Certification Authorities based on their operational characteristics.

All CAs within this PKI must comply with the relevant provisions of this Policy and establish a contact window. If a CA serves as a Subordinate CA for another Public Key Infrastructure, its superior CA is not subject to the regulations of this Policy.

The Root Certification Authority serves as the Trust Anchor of this PKI and must maintain the highest level of public credibility. Its operations shall adhere to the highest level of security requirements defined in this Policy.

Subordinate Certification Authorities are the second-tier or third-tier CAs within this PKI. Certificates of second-tier CAs are issued by the Root CA, while certificates of third-tier CAs are issued by second-tier CAs.

The TWCA Root Certification Authority, managed and operated by the Company, is the highest-level CA of this PKI and is primarily responsible for the following tasks:

- Issuance and management of certificates for Subordinate CAs.
- Managing and publishing the certificates and Certificate Revocation Lists (CRLs) of Subordinate CAs in the repository.
- Maintaining the stability and operation of the repository.

Subordinate Certification Authorities are primarily responsible for the following tasks:

- Issuance and management of Subscriber certificates.
- Issuance and management of Registration Authority (RA) certificates.
- Managing and publishing Subscriber certificates and CRLs in the repository.
- Maintaining the stability and operation of the repository.

If a Subordinate CA issues certificates to its own subordinate CAs, it must also be responsible for the following tasks:

- Issuance and management of certificates for its subordinate CAs.
- Managing and publishing the certificates and certificate revocation information of its subordinate CAs in the repository.

1.3.2 Registration Authorities (RA)

Registration Authorities (RAs) are primarily responsible for verifying the identity of Subscribers and the relevant information required for certificates, enabling the CA to issue Subscriber certificates.

Each CA within this PKI shall specify the regulations for acting as an RA in its CPS.

When issuing certificates to Subordinate CAs, each CA within this PKI shall act as its own RA and execute RA tasks in accordance with the provisions of its CPS.

1.3.3 Subscribers

A Subscriber is the end entity named in the Certificate Subject of the certificate and holds the Private Key corresponding to the Public Key in the certificate. The applicability of the Subscriber's certificate shall be stated in the "Certification Practice Statement". Because application systems are not legally defined entities with behavioral capacity, if a certificate is issued to an application system for identification purposes, the Subscriber of that certificate is the natural person or legal entity who applied for it.

1.3.4 Relying Parties

A Relying Party accepts another person's (Subscriber's) certificate to verify the validity of a signed message or uses the Subscriber's certificate to encrypt a message before transmitting it to the Subscriber,

thereby achieving message confidentiality between the communicating parties.

Relying Parties should decide whether a certificate is trustworthy or whether it can be used for a specific purpose based on the information stated within the certificate.

1.3.5 Other Participants

If any new members wish to join this PKI, they must be approved by the Policy Management Authority (PMA) of "TAIWAN-CA INC."; for example, when CAs need to cross-certify with CAs outside of this PKI.

1.4 Certificate Usage

The certificate assurance levels and applicability defined in this Policy are summarized as follows:

Assurance Level	Description
Test Level	An assurance level provided for testing purposes by Subscribers or Relying Parties. It is strictly for testing and cannot be used for any non-testing purposes.
Class 1	A basic assurance level providing minimal confidence in the Subscriber's identity. It is suitable for identifying data integrity in network environments where the threat of malicious tampering is very low.
Class 2	An initial assurance level providing basic identity authentication with a certain degree of confidence in the Subscriber's identity. It is suitable for network environments where information might be tampered with, but the risk of malicious tampering is low.
Class 3	A medium assurance level providing advanced identity authentication with high confidence in the Subscriber's identity. It is suitable for higher-risk network environments where malicious users may intercept or tamper with information.
Class 4	A high assurance level providing the highest degree of identity authentication with extremely high confidence in the Subscriber's identity. It is suitable for network environments with high potential threats or where the cost of recovering tampered information is very high. This is exclusively for CA application use.

The applicable assurance levels for different certificate types are as follows:

Assurance Level	Certificate Type
Test Level	Business XML Certificate, Business EC Certificate, InfoSec Certificate
Class 1	Business XML Certificate, Business EC Certificate, InfoSec Certificate
Class 2	Business XML Certificate, Business EC Certificate, InfoSec Certificate, AATL Certificate

Assurance Level	Certificate Type
Class 3	Business XML Certificate, Business EC Certificate, InfoSec Certificate, AATL Certificate, Time-Stamping Certificate, S/MIME Certificate
Class 4	Exclusively for CA application use.

Each CA shall document in its CPS the assurance levels referenced from this Policy for issued certificates, as well as the usage limitations for each assurance level. Subscribers and Relying Parties must select appropriate certificates according to the assurance levels and applicability documented in the CPS.

1.4.1 Appropriate Certificate Uses

Subject to the provisions of each CA's Certification Practice Statement.

1.4.2 Prohibited Certificate Uses

Subject to the provisions of each CA's Certification Practice Statement.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Policy Management Authority (PMA) of "TAIWAN-CA INC." is the responsible entity for the formulation, updating, and publication of this Policy.

1.5.2 Contact Person

If Subscribers have any modification suggestions for the Certificate Policy, please email or mail detailed suggestions, explanatory documents, and contact information to the following contact window:

- **Company Name:** TAIWAN-CA INC. (TWCA)
- **Contact Person:** Policy Management Authority (PMA)
- **Address:** 10TH Floor, 85, Yen-Ping South Road, Taipei, Taiwan, R.O.C
- **Phone:** 886-2-23708886
- **Fax:** 886-2-23700728
- **Email:** ca@twca.com.tw

1.5.3 Person Determining CPS Suitability for the Policy

The Certification Practice Statements (CPS) established by each CA within this PKI shall be approved by the PMA.

1.5.4 CPS Approval Procedures

Each CA shall formulate a Certification Practice Statement (CPS) and ensure its compliance with this Policy; if the certificate usage falls within the scope of the national Electronic Signatures Act, the CPS formulated by the CA must be approved by the competent authority before the CA can provide public certificate issuance services.

1.6 Definitions and Acronyms

Refer to Appendix II.

2 Publication and Repository Responsibilities

2.1 Repositories

Repositories provide for the querying or downloading of certificate-related information, such as certificates, Certificate Revocation Lists (CRLs), certificate status, Certificate Policies, and Certification Practice Statements. Each Certification Authority (CA) within this PKI must have at least one publicly accessible repository. The URL of the repository must be stated in the Certification Practice Statement (CPS), and the CA must ensure the repository's availability, access controls, and data integrity.

2.2 Publication of Certification Information

The CA shall publish information essential for Subscribers and Relying Parties to use certificates, including but not limited to the Certification Practice Statement and Certificate Revocation Lists. Other CA information required to be published is subject to the provisions of each CA's CPS.

If a CA issues S/MIME certificates, its CPS must comply with the provisions of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" (hereinafter referred to as S/MIME BR) established by the CA/Browser Forum.

2.3 Time or Frequency of Publication

The publication frequency of CA information is subject to the provisions of each CA's CPS.

The publication frequency of Certificate Revocation Lists (CRLs) must be regulated in the CPS.

If a CA issues publicly trusted certificates, the CA must develop, implement, execute, and revise its CP/CPS to detail the latest status of these requirements.

If a CA issues S/MIME certificates, it must review or revise its Certificate Policy and Certification Practice Statement annually and demonstrate how it complies with the provisions of the S/MIME BR.

2.4 Access Controls on Repositories

The CA shall establish regulations for repository access control within its CPS.

3 Identification and Authentication

Each Certification Authority (CA) within this PKI must stipulate the operational procedures for Subscriber identity identification and authentication in its Certification Practice Statement (CPS) and Registration Authority (RA) operational guidelines.

3.1 Naming

3.1.1 Types of Names

Each CA must be capable of issuing X.509 certificates with a unique X.500 Distinguished Name (DN) as the Subject name. CAs shall specify the types of names in their respective CPS.

CAs may use the Subject Alternative Name extension as needed, but the Subject Alternative Name cannot be used alone while leaving the Subject name blank. Furthermore, the Subject Alternative Name must also comply with the X.500 standard naming conventions.

3.1.2 Need for Names to be Meaningful

The Subject Distinguished Name stated in the certificate must be sufficient to identify a specific organization, individual, or specific entity, and must be recognizable by the Relying Party.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CPS of each CA shall specify the relevant regulations regarding the use of anonymity, pseudonymity, aliases, or pen names by Subscribers.

3.1.4 Rules for Interpreting Various Name Forms

The rules for interpreting Subscriber names shall follow the regulations set by respective competent authorities. For example, Internet account distinguished names shall follow the bank codes and bank account regulations formulated by the Financial Data Center, Taxation Agency, Ministry of Finance; personal ID numbers shall follow the regulations of the Ministry of the Interior; corporate Unified Business Numbers (Tax ID Numbers) shall follow the regulations of the Ministry of Economic Affairs. The interpretation rules for other Subscriber distinguished names shall be handled according to each CA's CPS.

3.1.5 Uniqueness of Names

Each CA shall ensure the uniqueness of the certificate names it issues, and shall stipulate the naming principles and how to ensure their uniqueness within its CPS.

3.1.6 Resolution of Disputes Regarding Naming

When registered distinguished names are identical, the CA shall prioritize the first applicant. However, if other applicants present relevant evidentiary documents issued by competent authorities/organizations, the CA shall initiate the naming dispute resolution process.

Each CA shall stipulate the procedures for handling naming disputes within its CPS.

3.1.7 Recognition, Authentication, and Role of Trademarks

Subject to the provisions of each CA's Certification Practice Statement.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

If the Public Key in the certificate and its corresponding Private Key are generated by the Subscriber, the CA must require the Subscriber to provide proof of possession of the Private Key. This can be done, for example, by verifying a signed message to confirm the Subscriber is the owner of the Private Key (e.g., using methods from RFC 2986, RFC 4210, RFC 4211 standards).

If the Private Key is generated by the RA, the CA, or another authorized third party on behalf of the Subscriber, there is no need to verify whether the Subscriber possesses the Private Key. However, the security control measures for delivering the Private Key to the Subscriber must be stipulated in the CPS.

3.2.2 Authentication of Organization Identity

When authenticating the identity of an organization, the organization must provide evidentiary documents issued by the competent authority or other documents proving its existence, and the identity of the representative must be verified, along with whether they are authorized by the organization. If handled by an authorized agent of the organization, the agent's relevant identity documents must be verified, submitted in writing, or handled by the agent using a method equivalent to the strength of an in-person application.

The CA must stipulate the organizational Subscriber identity authentication procedures in its CPS. The RA shall follow the CPS to publish an organizational Subscriber identity authentication policy and execute the authentication based on this published policy.

The requirements for organizational identity authentication procedures across different assurance levels are as follows:

Assurance Level	Requirements
Test Level	If a CA issues Test Level certificates for organizations, the CA shall regulate this in its CPS.
Class 1	Organizational Subscribers register using self-asserted identity information. The RA shall verify the uniqueness of this information and conduct limited verification.
Class 2	Must meet the verification requirements of Class 1. Organizational Subscribers must submit evidence proving their organizational identity information. The RA shall verify the existence and validity of this evidence.
Class 3	Must meet the verification requirements of Class 2. The representative or an agent holding an authorization document must provide proof of identity sufficient to identify the organization. The RA shall process this using a method similar to in-person authentication strength and consult trusted third-party authoritative sources to verify the identity information claimed by the organization or information known only to the organization.
Class 4	Must meet the verification requirements of Class 3. The RA shall conduct authentication in person.

For the initial validation of information or communication hardware/software equipment (such as routers, firewalls, servers, etc.) owned by an organization, the equipment administrator must additionally provide the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., domain name).
- Equipment Public Key.
- Equipment authorized usage and attributes (only required if these must be included in the certificate).
- Administrator contact information for communication by the RA or CA.

The CA shall verify the registration data using methods commensurate with the requested certificate's assurance level. Verification methods include, but are not limited to, the methods defined in this section, authenticating the Subscriber's identity, or doing so via the Subscriber's digital signature (the signing certificate must have been issued in compliance with this Policy).

For S/MIME certificates, the CA shall follow the S/MIME BR specifications to perform ownership verification operations on the Email domain and Email mailbox provided by the applicant. The verification methods used by the CA must be documented in the CPS.

Applicants may be required to provide more information or undergo additional verification procedures to meet equivalent trust requirements.

3.2.3 Authentication of Individual Identity

The CA must stipulate the individual Subscriber identity authentication procedures in its CPS. The RA shall follow the CPS to publish an individual Subscriber identity authentication policy and execute the authentication based on this published policy.

The requirements for individual identity authentication procedures across different assurance levels are as follows:

Assurance Level	Requirements
Test Level	If a CA issues Test Level certificates for individuals, the CA shall regulate this in its CPS.
Class 1	Individual Subscribers register using self-asserted identity information. The RA shall verify the uniqueness of this information and conduct limited verification.
Class 2	Must meet the verification requirements of Class 1. Individual Subscribers must submit evidence proving their individual identity information. The RA shall verify the existence and validity of this evidence.
Class 3	Must meet the verification requirements of Class 2. The individual or an agent holding an authorization document must provide proof of identity sufficient to identify the individual. The RA shall process this using a method similar to in-person authentication strength and consult trusted third-party authoritative sources to verify the identity information claimed by the individual or information known only to the individual.
Class 4	Not applicable.

For information or communication hardware/software equipment owned by an individual, the individual is considered the equipment administrator and shall proceed according to the provisions in Section 3.2.2.

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

The identity documents of individuals, organizational representatives, agents, and organizations (hereinafter referred to as "such persons") shall be official documents issued by the government (hereinafter referred to as "the documents"). The RA must verify the authenticity of the agent's authorization documents, and such persons must attest under declaration that the documents are genuine.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Subscribers of each CA shall perform identity identification and authentication for key update operations based on the following identity authentication requirements:

Assurance Level	Requirements
Test Level	No stipulation.
Class 1	No stipulation.
Class 2	May use agreed-upon account passwords or the current signing key for identity authentication.
Class 3	May use the current signing key for identity authentication.
Class 4	Initial validation must be performed for every key update.

3.3.1 Identification and Authentication for Routine Re-key

As the usage time of a key increases, the risk of it being lost or compromised also increases. Therefore, Subscribers should regularly replace their keys to ensure key security. Key replacement (re-key) refers to generating a new Public Key and Private Key pair and applying to the CA for certificate issuance using the original registration information. The new certificate after the key update has the same characteristics and assurance level as the old certificate.

The CA shall stipulate the Subscriber identity identification and authentication requirements for routine key updates in its CPS.

3.3.2 Identification and Authentication for Re-key After Revocation

After a Subscriber's certificate is revoked, the initial validation methods specified in Section 3.2 must be re-executed to re-apply for a new certificate.

3.4 Identification and Authentication for Revocation Request

The CA shall authenticate certificate revocation requests. Authentication of a certificate revocation request can be performed by verifying the signature generated by the Private Key corresponding to the certificate, regardless of whether the Private Key has been compromised.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

When the certificate user is a natural person, the person themselves is the certificate applicant. When the certificate user is a legal entity, the representative of the legal entity or its authorized agent is the

certificate applicant.

4.1.2 Enrollment Process and Responsibilities

The certificate applicant shall read the certificate subscriber agreement in advance. After agreeing to the terms, they shall fill out the certificate application form and submit it to the Registration Authority (RA).

The CA must stipulate the method for transmitting the Public Key to the certificate issuer in its Certification Practice Statement (CPS).

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

When a certificate applicant applies for a certificate, the RA shall follow these regulations:

1. Obtain the applicant's certificate application-related data in accordance with Section 3.2.
2. Verify and record the applicant's identification data in accordance with Section 3.2.
3. Obtain the applicant's Public Key and verify its linkage with the Private Key in accordance with Section 3.2.
4. Confirm whether the information to be recorded in the certificate is correct.

The detailed steps for implementing the above regulations shall be formulated by each CA and stated in the CPS; the above-regulated items must be completed before the certificate is issued.

4.2.2 Approval or Rejection of Certificate Applications

Upon completion of the identification and authentication procedures in Section 4.2.1, the certificate application is considered approved. If the identification and authentication procedures cannot be completed, the certificate application shall be rejected.

If the CA and RA issue S/MIME certificates, they must comply with industry standards (such as S/MIME BR) when approving certificate applications and issuing certificates, and this shall be documented in the CPS.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

All communications between the RA and the CA shall undergo identity authentication. Communication methods can be online or offline, and the integrity and confidentiality of the information must be protected

during communication.

When the certificate applicant's Public Key is transmitted to the CA, the CA must confirm that the application data is correctly linked to the Public Key without error. The CA may use cryptographic methods to ensure this linkage, or use non-cryptographic physical or procedural methods, including but not limited to using floppy disks (or other storage media) sent via registered mail or courier.

Upon receiving a certificate issuance request, the CA shall:

1. Verify the sender's identity.
2. Check the integrity of the transmitted data.
3. Confirm that the content of the certificate issuance request meets the requirements for issuing certificate content before generating and issuing the certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

After issuing the certificate, the CA shall notify the Subscriber of the issuance and deliver the certificate in an appropriate manner. If the CA refuses to issue the certificate, it shall notify the Subscriber in an appropriate manner and explicitly state the reasons for refusal. The aforementioned notification and delivery may also be executed through the RA.

In addition to reasons related to the failure to pass the verification of the certificate issuance request, the CA may refuse to issue a certificate for other reasons.

4.4 Certificate Acceptance

The CA's CPS shall regulate:

- The Subscriber certificate acceptance procedure.
- Ensuring the certificate applicant clearly understands the responsibilities and obligations of using the certificate before accepting it.
- How to inform the certificate applicant of the contents of the issued certificate.

If the certificate applicant refuses to accept the issued certificate after reviewing its contents, the RA shall notify the CA to revoke the certificate.

4.4.1 Conduct Constituting Certificate Acceptance

Upon receiving the certificate, the Subscriber shall confirm whether the information recorded in the certificate is correct and thoroughly understand the terms of the certificate subscriber agreement before commencing the use of the certificate.

4.4.2 Publication of the Certificate by the CA

After issuing the certificate, each CA may publish the certificate in the repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

After issuing the certificate, in addition to delivering it to the Subscriber, each CA may also deliver the certificate to the RA.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

A Subscriber is the entity that holds the Private Key corresponding to the Public Key within the certificate. The certificate's applicability determines the permitted uses of the Subscriber's Private Key. The applicability of Subscriber certificates issued by each CA shall be stated in the CPS.

If there are any concerns that the Subscriber's Private Key has been compromised, exposed, or lost, the Subscriber must report to the RA or CA in accordance with the provisions of the CA's CPS.

The scope and limitations of the use of the Subscriber certificate and its corresponding Private Key must comply with the regulations of this Policy and the CA's CPS.

4.5.2 Relying Party Public Key and Certificate Usage

This Policy does not specify the verification steps that Relying Parties must perform when deciding to trust a certificate. When verifying a certificate, a Relying Party shall still follow the relevant regulations of the respective CA's CPS to establish a certificate trust path and verify the certificate, serving as a reference for whether to trust the certificate. A Relying Party may only use the certificate to verify the correctness of a digital signature on an electronic document and authenticate the signer's identity after the certificate has been trusted.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Certificate renewal refers to the issuance of a new certificate with the same key, a different serial number, and an extended validity period, under the condition that the Subscriber's identification information remains unchanged.

Each CA within this PKI may determine independently whether to accept certificate renewals.

4.6.2 Who May Request Renewal

The Subscriber has the right to request certificate renewal.

4.6.3 Processing Certificate Renewal Requests

Before the certificate's validity period expires, the Subscriber shall apply to the RA/CA for the issuance of a new certificate using the original Subscriber registration data and Public Key.

When a Subscriber performs a certificate renewal, the CA shall confirm the accuracy of the registration data and the Public Key.

Certificates are issued in accordance with the provisions of Section 4.3.

4.6.4 Notification of New Certificate Issuance to Subscriber

Subject to the provisions of Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Subject to the provisions of Section 4.4.

4.6.6 Publication of the Renewal Certificate by the CA

Subject to the provisions of Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Subject to the provisions of Section 4.4.3.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

Replacing a key for a certificate refers to generating a new pair of Public and Private Keys and applying to the CA for certificate issuance using the original registration information.

Each CA within this PKI shall independently regulate the procedures for certificate and Private Key updates.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber has the right to request a certificate re-key.

4.7.3 Processing Certificate Re-keying Requests

Perform Subscriber identity identification and authentication in accordance with the provisions of Section 3.3.

Certificates are issued in accordance with the provisions of Section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

Subject to the provisions of Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Subject to the provisions of Section 4.4.

4.7.6 Publication of the Re-keyed Certificate by the CA

Subject to the provisions of Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Subject to the provisions of Section 4.4.3.

4.8 Certificate Modification

Certificate modification refers to reissuing a certificate to a Subscriber when the Public Key remains unchanged, but the recorded Subscriber identification information needs to be altered.

4.8.1 Circumstance for Certificate Modification

Subject to the provisions of each CA's CPS.

4.8.2 Who May Request Certificate Modification

Subject to the provisions of each CA's CPS.

4.8.3 Processing Certificate Modification Requests

Subject to the provisions of each CA's CPS.

4.8.4 Notification of New Certificate Issuance to Subscriber

Subject to the provisions of each CA's CPS.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Subject to the provisions of each CA's CPS.

4.8.6 Publication of the Modified Certificate by the CA

Subject to the provisions of each CA's CPS.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Subject to the provisions of each CA's CPS.

4.9 Certificate Revocation and Suspension

If a CA issues S/MIME certificates, its certificate revocation operational guidelines must comply with the provisions of the S/MIME BR and be documented in the CPS.

4.9.1 Circumstances for Revocation

- The Subscriber wishes to terminate the use of the certificate, or the certificate-related Subscriber agreement is terminated.
- Within the validity period of the certificate, changes occur to the Subscriber-related information within the certificate.
- The Private Key associated with the certificate is confirmed or suspected to be compromised, corrupted, lost, exposed, or tampered with.
- The Subscriber violates the Certificate Policy, Certification Practice Statement, or Subscriber agreement.
- The CA's signing key is confirmed or suspected to be compromised.

When the above situations occur, the relevant certificate shall be revoked and added to the Certificate Revocation List (CRL). The revoked certificate must be included in subsequently published CRLs until the certificate expires.

4.9.2 Who Can Request Revocation

Each CA shall stipulate the regulations concerning who has the right to request a certificate revocation in its CPS.

4.9.3 Procedure for Revocation Request

A certificate revocation request must specify the certificate to be revoked and state the reason for revocation. Each CA shall specify the procedures for revoking a certificate in its CPS.

4.9.4 Revocation Request Grace Period

Each CA shall stipulate the deadline for Subscribers to submit a certificate revocation request in its CPS.

4.9.5 Time within which CA Must Process the Revocation Request

Each CA shall stipulate the time limit for processing a certificate revocation request in its CPS.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties shall independently determine the interval for querying (or downloading) revocation data (Certificate Revocation Lists) based on their risk, responsibilities, and potential consequences. When a Relying Party uses a Subscriber certificate to verify a Subscriber's digital signature, it shall check whether the Subscriber's certificate is in a revoked status.

The CA shall state the requirements for Relying Parties to check the CRL in its CPS.

4.9.7 CRL Issuance Frequency

In principle, a CA shall regularly generate a Certificate Revocation List (CRL). Processed certificate revocation information shall be updated within the time specified in the "Next Update" field of the CRL, and the revocation information shall be added during the next CRL update for Relying Parties to query. The CA must also execute the CRL issuance process even if no Subscriber has applied to revoke a certificate within the interval of the CRL generation frequency.

The frequency for a CA to generate a CRL is fundamentally once every 24 hours, but this may vary according to the practical needs of individual CAs.

Each CA shall stipulate the frequency of issuing CRLs in its CPS.

4.9.8 Maximum Latency for CRLs

The maximum latency for CRLs refers to the time difference between the generation of the CRL and its actual publication in the repository.

No stipulation in this Policy.

4.9.9 On-line Revocation/Status Checking Availability

Each CA may provide an Online Certificate Status Protocol (OCSP) service as needed. Because not all application software on the Relying Party's end can perform real-time querying, each CA must provide at least a CRL download service, and state whether an online certificate status querying service is provided in its CPS.

4.9.10 On-line Revocation Checking Requirements

Regulated by each CA in its CPS.

4.9.11 Other Forms of Revocation Advertisements Equivalent to CRLs

If a CA provides certificate status query functions in other forms, it must regulate its operational methods in the CPS, and the data protection method should be at least equivalent to the implementation of a CRL.

4.9.12 Special Requirements Related to Key Compromise

When a CA's signing key is compromised, the following principles shall be followed:

1. Revoke the valid certificates that have been issued.
2. Update the certificate status information in the CRL or the online certificate status query service.
3. Generate a new signing key pair and corresponding new certificate.
4. Notify Subordinate CAs that the key has been compromised.
5. If a Subordinate CA's key is compromised, it shall notify its superior CA within 24 hours.
6. Reissue certificates using the new signing key in accordance with the provisions of Sections 4.2 and 4.3.
7. Deliver the new certificates according to the provisions of Section 6.1.4.

Each CA shall document the procedures for handling key compromises in its CPS.

4.9.13 Circumstances for Suspension

Subject to the provisions of each CA's CPS.

4.9.14 Who Can Request Suspension

Subject to the provisions of each CA's CPS.

4.9.15 Procedure for Suspension Request

No entity other than the CA that issued the Subscriber certificate may provide certificate suspension services.

If the CA that issued the Subscriber certificate provides Subscriber certificate suspension services, it shall document the certificate suspension procedure in its CPS.

4.9.16 Limits on Suspension Period

Subject to the provisions of each CA's CPS.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Refer to the provisions in Sections 4.9.9, 4.9.11, and 4.9.13.

The CA may only remove the certificate revocation information from the certificate status service after the validity period of the revoked Subscriber certificate has expired.

4.10.2 Service Availability

Refer to the provisions in Sections 4.9.9, 4.9.11, and 4.9.13.

If the CA issues S/MIME certificates, the availability of the certificate status service must comply with the provisions of the S/MIME BR and be documented in the CPS.

4.10.3 Optional Features

Refer to the provisions in Sections 4.9.9, 4.9.11, and 4.9.13.

4.11 End of Subscription

Certificates issued by each CA become invalid upon certificate revocation, expiration of validity, or when the CA terminates operations.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Refer to Section 6.2.3.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The buildings where each Certification Authority's (CA's) equipment is located shall meet the facility standards for storing highly critical and sensitive information. These facilities must integrate physical security mechanisms such as access control, security guards, intrusion detection, and video surveillance to prevent unauthorized access to CA-related equipment.

5.1.2 Physical Access

Each CA's physical access control must meet at least the following requirements:

- Prevent unauthorized access to hardware equipment.

- Ensure all removable media or paper documents containing sensitive information are stored in a secure location.
- Monitor and record unauthorized access manually or automatically 24 hours a day, 7 days a week.
- Regularly review access logs and ensure their availability.

The server room housing the CA's certificate issuance equipment must have access control measures requiring at least two persons for entry and access.

5.1.3 Power and Air Conditioning

Each CA must have adequate backup power and air conditioning equipment to maintain normal operations or safely shut down equipment when affected by external factors. Additionally, a backup power system must be provided, supplying at least 6 hours of backup power for repository backup data.

5.1.4 Water Exposures

Each CA's equipment shall be installed in a location protected from floods and water damage.

5.1.5 Fire Prevention and Protection

Each CA's server room shall be equipped with automatic fire extinguishing equipment that activates automatically upon detecting a fire. Manual switches shall also be installed at main entrances for on-site personnel to operate manually in emergency situations.

5.1.6 Media Storage

The media storage environment of each CA shall prevent accidental damage to the media. Critical data backup media must be stored at a location other than the CA's primary site.

5.1.7 Waste Disposal

Each CA must formulate secure clearing and destruction procedures for sensitive information, which shall be documented in the Certification Practice Statement (CPS).

5.1.8 Off-Site Backup

Each CA shall maintain off-site backup facilities and document the off-site backup mechanisms in its CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Each CA's certificate management operations must be conducted under strict and secure operational procedures. To ensure the separation of duties and responsibilities, and to guarantee that role backup does

not compromise overall system security and operational integrity, each CA shall stipulate trusted roles and their division of labor in its CPS.

This Policy defines four trusted roles and their general division of labor as follows:

- **Administrator:** Responsible for system installation, management operations, and environmental parameter configuration.
- **Officer:** Responsible for generating certificate application request files, and executing certificate revocation and issuance.
- **Auditor:** Responsible for conducting internal audits, as well as reviewing and maintaining audit logs.
- **Operator:** Responsible for routine maintenance operations, such as backup, restoration, and website data maintenance.

5.2.2 Number of Persons Required per Task

Each CA shall stipulate the required number of operational personnel in its CPS, which must comply with the provisions of Section 5.2.1.

5.2.3 Identification and Authentication for Each Role

Operational personnel must undergo identity identification and authentication before executing the tasks associated with their roles.

5.2.4 Roles Requiring Separation of Duties

Each CA shall separate roles according to the following principles:

- Ensure the four trusted roles described in Section 5.2.1 are in place.
- The Officer and Administrator roles cannot be held by the same person.
- The Officer and Auditor roles cannot be held by the same person.
- The Administrator and Auditor roles cannot be held by the same person.
- The Operator and Officer roles cannot be held by the same person.
- The Operator and Auditor roles cannot be held by the same person.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Each CA must establish qualification requirements for personnel executing certificate management operations. These individuals must at least possess the characteristics of loyalty and trustworthiness, and have no criminal records or poor credit history. The CPS shall also establish qualification requirements for operational personnel. If there is a need to hire independent contractors (outsourced personnel), their qualification requirements must also be established.

5.3.2 Background Check Procedures

Each CA must formulate regulations for reviewing the identity background and job execution of personnel responsible for the certificate management system, complying with the requirements of Section 5.3.1.

5.3.3 Training Requirements

Each CA's operational personnel shall receive training corresponding to their duties. This training shall cover software/hardware functions, operational procedures, security control procedures, the CP, the CPS, and other relevant technical and operational specifications necessary for the operation of the certificate management system.

5.3.4 Retraining Frequency and Requirements

When there are changes to the operational environment or security management mechanisms, each CA must provide appropriate retraining to its personnel. The training plans and frequency shall be stipulated in the CPS.

5.3.5 Job Rotation Frequency and Sequence

Each CA may establish operational regulations for job rotation, which shall be documented in the CPS.

5.3.6 Sanctions for Unauthorized Actions

Each CA shall document disciplinary procedures for unauthorized actions in its CPS.

5.3.7 Independent Contractor Requirements

Each CA shall document control procedures for independent contractors (outsourced personnel) in its CPS.

5.3.8 Documentation Supplied to Personnel

The operational documents of each CA must at least satisfy the needs of personnel in various roles executing maintenance operations. The CA shall document the operational document requirements in its CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Each CA's audit logs, whether manual or automated, must at least include the following items:

- Event type.
- Date and time of the event occurrence.

- Location or position of the event occurrence.
- Success or failure results when executing certificate issuance or revocation operations.
- The entity or individual that triggered the event.

When events occur, the CA may determine whether to record the audit logs electronically or physically. The types of audit events to be recorded by the CA are as follows:

- Security audit management operations.
- Personnel and trusted role management, identification, and authentication.
- Creation, modification, and deletion of Subscriber information.
- CA key generation.
- Changes to Private Keys and trusted Public Keys.
- Certificate application, issuance, revocation, and status changes.
- Certificate management system configuration settings and changes.
- System and application startup or shutdown.
- Personnel login and logout from systems and applications.
- Installation, removal, and destruction of cryptographic modules.
- Access control and physical environment access.
- Hardware and software system updates.
- Data backup and recovery.
- Unauthorized file system access.
- Abnormal network system access.
- Key compromise, system anomalies, and hazards.
- Violations of the CP and CPS.

5.4.2 Frequency of Processing Log

Each CA shall review audit logs at least once a month. During the review, the integrity of the audit logs shall be checked to ensure they have not been tampered with, and all log entries shall be examined. Any abnormalities or warning signs shall be carefully investigated. The response plan based on the review results must be documented.

5.4.3 Retention Period for Audit Log

Relevant audit log reports and media data shall be retained at the CA's location for at least 2 months. Except for video surveillance media records, relevant audit logs shall be archived before being removed.

5.4.4 Protection of Audit Log

Each CA must prevent unauthorized personnel from reading audit logs and performing audit log backups, and prevent the audit logs from being tampered with.

5.4.5 Audit Log Backup Procedures

Each CA must stipulate audit log backup procedures in its CPS, backing up audit logs at least once a month, and storing one backup copy at a backup site outside the CA's primary location.

5.4.6 Audit Collection System

The collection of audit logs may be conducted externally or internally to the CA's certificate management system. Automated audit procedures shall be initiated by the certificate management system and must continue until the system is shut down. The collection of audit logs can be recorded via the operating system, certificate management system, and certificate management operational personnel, either automatically by computer or manually by personnel.

5.4.7 Notification to Event-Causing Subject

When an occurring event is recorded by the audit system, there is no need to notify the relevant personnel who generated the event. The reporting procedures for abnormal event logs shall be regulated in each CA's CPS.

5.4.8 Vulnerability Assessments

Each CA shall conduct regular vulnerability assessments of its security controls.

5.5 Records Archival

5.5.1 Types of Records Archived

Each CA's archived records shall include at least the following types:

- Data from external evaluations accepted by the CA
- Certification Practice Statement (CPS)
- Contracts related to CA operations
- System environment setup and configuration files
- System change records
- Certificate application files
- All issued and published certificates
- Key replacement records
- Audit data files
- Revocation request records
- Subscriber registration data
- Subscriber agreements
- Revoked certificate data files

- Data and tools used to verify archived records
- Documents requested by auditors

If the CA escrows Subscriber encryption keys, they shall also be archived together.

5.5.2 Retention Period for Archive

Each CA's archived data retention period shall be a minimum of 7 years and shall not be earlier than 2 years after the relevant key is destroyed, or the certificate expires or is revoked. The CA shall regulate the retention period of archived data in its CPS.

5.5.3 Protection of Archive

Archived data cannot be written to, modified, or deleted. Individual archived data belonging to a Subscriber may be provided to that Subscriber, personnel authorized by that Subscriber, and organizations permitted by law. Archived data must be preserved in a copy at another location with secure control measures that is harmless to the storage media.

5.5.4 Archive Backup Procedures

Independently regulated by each CA in its CPS.

5.5.5 Requirements for Time-Stamping of Records

Independently regulated by each CA in its CPS.

5.5.6 Archive Collection System

Independently regulated by each CA in its CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Independently regulated by each CA in its CPS.

5.6 Key Changeover

To reduce the risk of the CA's signing key being compromised, the CA's keys must undergo periodic Key Changeover. Upon completion of the changeover, the original key can no longer be used to issue certificates.

When selecting key validity periods, each CA shall consider key length, protection methods, control methods, and various other factors, and must not exceed the provisions of Section 6.1.5 of this Policy.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Each CA shall establish emergency response procedures and disaster recovery plans.

Each CA shall document business continuity plans and disaster recovery procedures in writing, including notification procedures to software vendors (e.g., browser vendors), Subscribers, and Relying Parties in the event of a disaster, security compromise, or operational interruption.

If a CA issues S/MIME certificates, its key compromise and emergency response procedures shall comply with the provisions of the S/MIME BR and be documented in the CPS.

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

When the equipment used by a CA is abnormally damaged, it must be rebuilt as quickly as possible, prioritizing the ability to generate certificate status information. Each CA shall stipulate its recovery procedures in the CPS and conduct a recovery drill for computing resources, software, and data corruption at least once a year.

5.7.3 Entity Private Key Compromise Procedures

Each CA shall document the procedures for handling the compromise of signing keys for each member of this PKI in its CPS or relevant documents.

5.7.4 Business Continuity Capabilities After a Disaster

Each CA shall document in its CPS the procedures used to rescue its equipment and maintain business continuity in the event of a natural disaster or other catastrophe before a secure environment is re-established.

5.8 CA Termination

Each CA shall document in its CPS the procedures to be followed upon termination of operations, which shall comply with the regulations of the Electronic Signatures Act.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key generation process shall be documented in the Certification Practice Statement (CPS). The CA's key generation equipment shall at least use a hardware cryptographic module compliant with FIPS 140-2 Level 3 or FIPS 140-3 Level 3.

Each CA shall document the provisions for generating Subscriber key pairs in its CPS.

6.1.2 Private Key Delivery to Subscriber

If a CA provides a service to generate key pairs on behalf of Subscribers, it shall document the security control measures for delivering the Private Key in its CPS.

6.1.3 Public Key Delivery to Certificate Issuer

When a Subscriber's Public Key is transmitted to the CA, the authenticity of the data must be ensured. The method of delivering the Public Key may be via a digitally signed message, physical media (such as a floppy disk) sent by courier, delivered in person by the applicant, or other transmission methods.

The CPS of each CA shall establish the method by which the Subscriber's Public Key is transmitted to the CA.

6.1.4 CA Public Key Delivery to Relying Parties

When there is a need to deliver the CA's Public Key, the Public Key certificate must at least be protected for message integrity.

6.1.5 Key Sizes

For CA certificates:

- **RSA:** Key size must be at least 2048 bits.
- **ECC:** The curve used must have a security strength of at least P-256.
- **ML-DSA:** The parameters used must have a security strength of at least ML-DSA-44.
- **SLH-DSA:** The parameters used must have a security strength of at least SLH-DSA-SHA2-128s, SLH-DSA-SHA2-128f, SLH-DSA-SHAKE-128s, or SLH-DSA-SHAKE-128f.

For Subscriber certificates:

- **RSA:** Key size must be at least 2048 bits.
- **ECC:** The curve used must have a security strength of at least P-256.

- **ML-DSA:** The parameters used must have a security strength of at least ML-DSA-44.
- **SLH-DSA:** The parameters used must have a security strength of at least SLH-DSA-SHA2-128s, SLH-DSA-SHA2-128f, SLH-DSA-SHAKE-128s, or SLH-DSA-SHAKE-128f.
- **ML-KEM:** The parameters used must have a security strength of at least ML-KEM-512, ML-KEM-768, or ML-KEM-1024.

6.1.6 Public Key Parameters Generation and Quality Checking

The generation and selection of Public Key parameters for each CA must use prime parameters generated by a random number generator compliant with FIPS 186-4 or similar specifications, or the generation of random numbers for Public Key parameters must comply with FIPS 140-2 or FIPS 140-3 standards.

If a Subscriber uses a hardware cryptographic module (such as an IC card), it is recommended to use a hardware cryptographic module that is at least compliant with FIPS 140-2 Level 2, FIPS 140-3 Level 2, or equivalent security level standards.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

Restrictions on key usage purposes are recorded in the Key Usage extension field of the X.509 certificate.

CA certificates shall only have the `keyCertSign` and `cRLSign` bits set, which may only be used for certificate signing and Certificate Revocation List (CRL) signing.

Subscriber signature certificates shall have the `digitalSignature` and/or `nonRepudiation` bits set. Encryption certificates shall have the `keyEncipherment` and/or `dataEncipherment` bits set.

If a CA issues certificates for purposes other than signature and encryption, it must document the key usage purposes in its CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards

The CA's cryptographic modules must at least use hardware cryptographic modules validated to FIPS 140-2 Level 3, FIPS 140-3 Level 3, or equivalent security level standards.

When Registration Authorities (RAs) use hardware certificate tokens, it is recommended to use tokens validated to at least FIPS 140-2 Level 2, FIPS 140-3 Level 2, or equivalent security level standards.

When Subscribers use hardware certificate tokens, it is recommended to use tokens validated to at least FIPS 140-2 Level 2, FIPS 140-3 Level 2, or equivalent security level standards.

The security control measures of the cryptographic modules for each CA must possess multi-person control capabilities.

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

The CA's signing Private Key must comply with the multi-person control procedures detailed in Chapter 5.

6.2.3 Private Key Escrow, Recovery, and Preservation

The CA's signing Private Key shall not be escrowed.

If a CA provides escrow, recovery, and preservation services for Subscriber Private Keys, it must stipulate relevant operational guidelines in its CPS.

6.2.4 Private Key Backup

The CA's Private Key is stored within an encrypted hardware cryptographic module. During backup, it must be performed using multi-person control and stored at a backup site. The Private Key backup procedures shall be documented in the CPS.

This Policy does not regulate the backup and preservation of RA and Subscriber Private Keys.

6.2.5 Private Key Archival

The CA's signing Private Key shall not be archived.

The CA's encryption Private Key may be archived. The CA shall document the procedures for archiving encryption Private Keys in its CPS.

This Policy does not regulate the archival of RA and Subscriber Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The Private Key should be generated within a cryptographic module. If a Private Key must be transferred from one cryptographic module to another, the transfer must be executed by authorized personnel, and the Private Key must never exist in plaintext form outside of a cryptographic module. The encryption key used to encrypt the Private Key must be protected to prevent disclosure.

6.2.7 Private Key Storage on Cryptographic Module

Private Keys may be stored within the cryptographic module in plaintext or ciphertext format.

6.2.8 Method of Activating Private Key

Private Keys stored within the cryptographic module must be activated by authorized personnel after identity authentication. Methods of authentication include, but are not limited to, passwords, personal identification numbers (PINs), or biometric identification. Activation data must be protected upon entry to prevent disclosure.

6.2.9 Method of Deactivating Private Key

The deactivation of Private Keys must only be executed by authorized personnel.

The CA shall document the operational procedures for deactivating Private Keys in its CPS.

6.2.10 Method of Destroying Private Key

When a CA's signing Private Key is no longer used, or when the corresponding Public Key expires or is revoked, the Private Key within the cryptographic module must be cleared using a Zeroization overwrite method.

6.2.11 Cryptographic Module Rating

The cryptographic modules used by the CA must be hardware cryptographic modules validated to at least FIPS 140-2 Level 3, FIPS 140-3 Level 3, or equivalent security level standards.

The cryptographic modules used by Subscribers are regulated independently by each CA within its CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The Public Key is archived concurrently when the certificate is archived; therefore, separate archival of the Public Key is not performed.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity periods for Public Keys and Private Keys of participants in this PKI may be identical. Depending on the security strength (key size), the usage periods are as follows:

RSA Key Size (bits)	ECC Curve	ML-DSA	ML-KEM	SLH-DSA	Security Strength	Validity Period
2048	-	-	-	-	112 bits	Up to 10 years
3072	P-256	ML-DSA-44	ML-KEM-512	SLH-DSA-SHA2-128s SLH-DSA-SHA2-128f SLH-DSA-SHAKE-128s SLH-DSA-SHAKE-128f	128 bits	Up to 20 years
4096	P-384	ML-DSA-65	ML-KEM-768	SLH-DSA-SHA2-192s SLH-DSA-SHA2-192f SLH-DSA-SHAKE-192s SLH-DSA-SHAKE-192f	192 bits	Up to 25 years

RSA Key Size (bits)	ECC Curve	ML-DSA	ML-KEM	SLH-DSA	Security Strength	Validity Period
-	P-521	ML-DSA-87	ML-KEM-1024	SLH-DSA-SHA2-256s SLH-DSA-SHA2-256f SLH-DSA-SHAKE-256s SLH-DSA-SHAKE-256f	256 bits	Up to 30 years

The CA shall document the validity periods of key pairs for Subordinate CAs and Subscribers in its CPS or relevant operational guidelines.

6.4 Activation Data

The CA shall document the protection of activation data in its CPS, covering the entire life-cycle from generation and archival to destruction.

6.4.1 Activation Data Generation and Installation

The activation data used to unlock the CA's or Subscriber's Private Key, along with other related access control mechanisms, must have appropriate protection.

The CA's activation data may be chosen by the users themselves and must be implemented using multi-person control. The activation data must utilize biometric data or security mechanisms strengthened by cryptographic modules.

Subscriber activation data may be chosen by themselves. If activation data must be pre-generated and then transmitted, it must be delivered through appropriately secured channels.

6.4.2 Activation Data Protection

The activation data of each CA must be protected using cryptographic or physical access control methods.

6.4.3 Other Aspects of Activation Data

Each CA may establish operational guidelines for activation data within its CPS, based on the security requirements of the certificate's applicability.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Each CA shall provide the following security measures through its operating system, or a combination of operating system, software, and physical protection technologies:

- Login procedures requiring user identity identification and authentication.

- Customizable access controls.
- Security auditing capabilities.
- Access control restrictions for various certificate services and PKI trusted roles.
- Identification and authentication of PKI trusted roles and related identities.
- Assurance of communication and database security.
- Secure and reliable channels for identifying PKI trusted roles and related identities.
- Process integrity and security control protection.

If a CA issues publicly trusted certificates recognized by browsers or computer operating systems, the CA shall implement information security control measures compliant with the "NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS" published by the CA/Browser Forum.

6.5.2 Computer Security Rating

The computer operating system platforms used by each CA must have their computer system security evaluated and approved for use either through Common Criteria (CC, ISO/IEC 15408) General Purpose Operating Systems Protection Profile (GPOSPP) certification, EAL4+ certification, or via an internal security assessment.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The development controls for each CA's certificate management system shall meet the following requirements:

- Must have detailed documentation.
- The procurement of hardware and software for the certificate management system must involve procedures that reduce the risk of component tampering.
- Hardware and software developed specifically for the CA must be conducted in a controlled environment, and the development process must be defined and documented.

6.6.2 Security Management Controls

Configurations, modifications, or upgrades to each CA's certificate management system must be fully controlled with documented records. There should be detection mechanisms for unauthorized software modifications or setting changes.

Each CA shall have control measures to ensure the integrity of the certificate management system software.

Each CA shall have operational guidelines for the security control of the hardware and software equipment lifecycle used for the certificate management system. Equipment must undergo security protection checks upon receipt.

Hardware and software equipment used by each CA for the certificate management system may only install software and execute operations related to certificate tasks. Installing software or executing tasks unrelated to CA business is prohibited. The installation and updating of hardware and software must have relevant operational guidelines and be conducted in a securely controlled environment.

6.6.3 Life Cycle Security Rating

No stipulation.

6.7 Network Security Controls

The certificate management system of each CA must have an independent operational management system, and only authorized operational personnel may perform operations.

To ensure network anti-intrusion and anti-destruction security functions, the CA must install and construct firewalls, intrusion detection systems, and anti-virus management systems to enhance the security control measures of the network management system.

The certificate management system of the Root CA must be installed in an independent and securely controlled environment. It must be maintained in an Off-Line status when routine operations are not being performed, and can only be activated after authorization.

6.8 Time-Stamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The format of certificates issued by each Certification Authority (CA) shall be specified in its Certification Practice Statement (CPS) or related operational guidelines.

7.1.1 Version Number(s)

Each CA within this PKI shall issue X.509 version 3 (ITU-T X.509 06/1997, ISO 9594-8) certificates.

7.1.2 Certificate Extensions

The use of certificate extensions shall comply with the ITU-T X.509 or IETF RFC 5280 standards in principle.

7.1.3 Algorithm Object Identifiers

The cryptographic algorithm Object Identifiers (OIDs) used by the CA are as follows:

Algorithm Type	Algorithm	Object Identifier (OID)
Key/Encryption	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	sha1WithRSAEncryption	`{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)}`
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)}`
Key/Signature	ML-DSA-44	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-44(17)}`
Key/Signature	ML-DSA-65	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-65(18)}`
Key/Signature	ML-DSA-87	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-87(19)}`
Key/Signature	SLH-DSA-SHA2-128s	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 20}`
Key/Signature	SLH-DSA-SHA2-128f	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 21}`

Algorithm Type	Algorithm	Object Identifier (OID)
Key/Signature	SLH-DSA-SHA2-192s	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 22}`
Key/Signature	SLH-DSA-SHA2-192f	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 23}`
Key/Signature	SLH-DSA-SHA2-256s	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 24}`
Key/Signature	SLH-DSA-SHA2-256f	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 25}`
Key/Signature	SLH-DSA-SHAKE-128s	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 26}`
Key/Signature	SLH-DSA-SHAKE-128f	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 27}`
Key/Signature	SLH-DSA-SHAKE-192s	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 28}`
Key/Signature	SLH-DSA-SHAKE-192f	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 29}`
Key/Signature	SLH-DSA-SHAKE-256s	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 30}`
Key/Signature	SLH-DSA-SHAKE-256f	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) 31}`
Key/Encryption	ML-KEM-512	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) kems(4) 1}`
Key/Encryption	ML-KEM-768	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) kems(4) 2}`

Algorithm Type	Algorithm	Object Identifier (OID)
Key/Encryption	ML-KEM-1024	`{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) kems(4) 3}`

Each CA shall explicitly specify the algorithm Object Identifiers used in its Certification Practice Statement (CPS).

7.1.4 Name Forms

The Subject Distinguished Name format used in certificates issued by each CA must conform to the X.500 Distinguished Name (DN) naming convention.

7.1.5 Name Constraints

Certificates issued by each CA may use the Name Constraints extension as needed.

7.1.6 Certificate Policy Object Identifier

Certificates issued by each CA may include the Object Identifiers defined in this Certificate Policy as needed.

7.1.7 Usage of Policy Constraints Extension

Each CA may use the Policy Constraints extension as needed.

7.1.8 Policy Qualifiers Syntax and Semantics

Each CA may use Policy Qualifiers as needed.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

The detailed content of Certificate Revocation Lists (CRLs) issued by each CA shall be specified in its Certification Practice Statement (CPS) or related operational guidelines.

7.2.1 Version Number(s)

Each CA within this PKI shall issue X.509 version 2 (v2) CRLs.

7.2.2 CRL and CRL Entry Extensions

When a CA uses CRL extensions in its Certificate Revocation Lists, the format shall be specified in its Certification Practice Statement (CPS) or related operational guidelines.

7.3 OCSP Profile

If a CA provides Online Certificate Status Protocol (OCSP) services, the response messages must include a digital signature.

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The Root Certification Authority (RCA) must undergo an internal audit and an external audit at least once a year. Other Certification Authorities (CAs) must regulate their audit frequencies in their Certification Practice Statements (CPS).

8.2 Identity/Qualifications of Assessor

The auditor of each CA must at least be familiar with the CPS and this Policy, as well as the audit criteria for compliance audits.

8.3 Assessor's Relationship to Assessed Entity

The auditor of each CA must conduct the audit with an independent, impartial, and objective attitude toward the assessed entity.

8.4 Topics Covered by Assessment

The audit scope for each CA must at least include the following items:

- Whether the CPS complies with the regulations of this Certificate Policy.

- Whether the CA executes certificate management and related operations in accordance with the CPS.
- If the CA issues publicly trusted certificates recognized by browsers or computer operating systems, such as S/MIME certificates, it must disclose its audit plan in its CPS.

8.5 Actions Taken as a Result of Deficiency

After a detailed audit and assessment of each CA's operations, if there is any non-compliance with the CPS, the auditor shall list them in detail according to the severity of the deficiency, and notify the auditing department and the relevant audited departments. The audited department must propose and execute corrective and preventive measures based on the deficiencies, and track the subsequent improvement status.

8.6 Communication of Results

The audit results of each CA shall be submitted to the Policy Management Authority (PMA).

8.7 Internal Audit

If a CA issues S/MIME certificates, its CPS must comply with the relevant requirements of the S/MIME BR and specify the internal audit frequency and sample size to strictly control service quality.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Each CA shall regulate this in its CPS; this Policy does not stipulate this matter.

9.1.2 Certificate Access Fees

Each CA shall regulate this in its CPS; this Policy does not stipulate this matter.

9.1.3 Revocation or Status Information Access Fees

Each CA shall regulate this in its CPS; this Policy does not stipulate this matter.

9.1.4 Fees for Other Services

Each CA shall regulate this in its CPS; this Policy does not stipulate this matter.

9.1.5 Refund Policy

Each CA shall regulate this in its CPS; this Policy does not stipulate this matter.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Regulated by each CA in its CPS.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

Regulated by each CA in its CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Regulated by each CA in its CPS, and shall be handled in accordance with relevant laws and regulations.

9.3.2 Information Not Within the Scope of Confidential Information

Regulated by each CA in its CPS, and shall be handled in accordance with relevant laws and regulations.

9.3.3 Responsibility to Protect Confidential Information

Regulated by each CA in its CPS, and shall be handled in accordance with relevant laws and regulations.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Each CA shall operate in accordance with the "Personal Data Protection Act" or the relevant regulations of other government agencies; when engaging in cross-border cooperation, each CA must also comply with the OECD (Organization for Economic Co-operation and Development) "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data".

9.4.2 Information Treated as Private

Each CA must specify the types of personal privacy data to be kept confidential in its CPS or privacy protection policy.

9.4.3 Information Not Deemed Private

Each CA must regulate in its CPS the types of data that can be published, such as Subscriber certificates, certificate revocation and suspension information, and the CPS. If there is any other information that must be published due to operational requirements, it shall be specified in the CPS.

9.4.4 Responsibility to Protect Private Information

Regulated by each CA in its CPS, and shall be handled in accordance with relevant laws and regulations.

9.4.5 Notice and Consent to Use Private Information

Regulated by each CA in its CPS, and shall be handled in accordance with relevant laws and regulations.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Each CA shall regulate in its CPS the types of protected data that must be provided pursuant to administrative regulations and judicial requests.

9.4.7 Other Information Disclosure Circumstances

Each CA shall regulate in its CPS the types of protected data that can be provided upon Subscriber request, and shall handle them in accordance with relevant laws and regulations.

9.5 Intellectual Property Rights

The intellectual property rights of this Policy belong to TAIWAN-CA INC.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

- Formulate a Certification Practice Statement (CPS) in accordance with this Policy.
- Publish the CPS and ensure all operations and provided services comply with the regulations set forth in the CPS.
- Execute certificate issuance and publication, and retain appropriate proof information.
- Confirm that the Subscriber agreement terms comply with baseline requirements.

- Revoke certificates of Subscribers who violate their obligations or for reasons specified in the baseline requirements.
- Execute the issuance and publication of Certificate Revocation Lists (CRLs).
- Provide repository services as described in Chapter 2.
- If a CA issues S/MIME certificates, according to S/MIME BR requirements, the CA shall verify the following:
    - The right to use the Email mailbox.
    - Authorization to apply for the certificate.
    - Accuracy of the information.
    - Absence of misleading information.
    - Identity of the applicant.

9.6.2 RA Representations and Warranties

- Execute Subscriber registration-related operations in accordance with this Policy and the CA's CPS.
- Operate securely in accordance with this Policy and the CA's CPS when executing Subscriber registration-related operations.
- Accept certificate application request information and retain proof data sufficient to verify the accuracy of the certificate application request information.
- Confirm that the Subscriber fully understands and agrees to the Subscriber's obligations upon registration application.

9.6.3 Subscriber Representations and Warranties

- Must provide detailed and accurate identity proof documents and information when registering with the RA.
- Securely and properly protect their Private Key in accordance with this Policy and the CA's CPS.
- Fully understand and agree to the regulations regarding certificate acceptance and usage in this Policy and the CA's CPS, and may only use the certificate after accepting it.
- If there is any concern that the Private Key corresponding to the certificate has been compromised, exposed, or lost, the Subscriber must report to the RA in accordance with the provisions of the CA's CPS.
- The scope and limitations of the use of the certificate and its corresponding Private Key must comply with the provisions of this Policy and the CA's CPS.

9.6.4 Relying Party Representations and Warranties

When verifying a certificate, a Relying Party shall follow the relevant regulations of each CA's CPS to establish a certificate trust path and verify the certificate, serving as a reference for whether to trust the

certificate.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Regulated by each CA in its CPS.

9.8 Limitations of Liability

Regulated by each CA in its CPS.

9.9 Indemnities

Each CA shall document the liability indemnification of the CA, RA, Subscribers, and Relying Parties in its CPS, which shall comply with the relevant provisions of the Electronic Signatures Act.

9.10 Term and Termination

9.10.1 Term

This Policy becomes effective upon approval by the PMA.

9.10.2 Termination

The termination of this Policy must be ruled by the PMA.

9.10.3 Effect of Termination and Survival

After this Policy is terminated, its validity shall survive until the last certificate issued in compliance with this Policy expires or is revoked.

9.11 Individual Notices and Communications with Participants

The PMA will establish communication channels with each CA within this PKI in an appropriate manner, including but not limited to the following methods: telephone, fax, or Email.

9.12 Amendments

9.12.1 Procedure for Amendment

The administering entity of this Certificate Policy is the PMA, which shall review this Policy at least once a year. CAs referencing this Policy shall review their CPS at least once a year. When this Policy needs to be amended due to factors such as changes in legal regulations or updates to international standards, the CA's CPS shall be amended accordingly. Amendments to this Policy must be approved by the PMA.

9.12.2 Notification Mechanism and Period

If there are update suggestions for this Policy, please mail or Email the suggestion documents to the contact window specified in Section 1.5.2 for PMA review.

9.12.3 Circumstances under which OID Must Be Changed

Changes to the Object Identifiers (OIDs) of this Policy must be approved by the PMA.

9.13 Dispute Resolution Provisions

For disputes arising from the use of certificates, both parties to the dispute shall adhere to the principle of good faith and strive to resolve it through negotiation in a reasonable manner. Each CA shall stipulate the procedures for handling certificate usage disputes in its CPS.

9.14 Governing Law

The content formulated in this Policy and the execution and interpretation of CA-related businesses are all based on the relevant laws of the competent authority, and are subject to the jurisdiction of the relevant laws of the Republic of China (R.O.C.).

9.15 Compliance with Applicable Law

Each CA shall specify its applicable laws in its CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If certain sections of this Certificate Policy become inapplicable and must be amended, the provisions of other sections remain valid and unaffected by the inapplicable provisions until a new version of the Certificate Policy is updated and published. Updates to the Certificate Policy shall be handled in accordance with the provisions of Section 9.12 of this Policy.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

If a CA causes losses to its issued certificates due to force majeure and other circumstances not attributable to the CA (such as wars or earthquakes), the CA may be exempted from liability for damages.

9.17 Other Provisions

No stipulation.

Appendix I: Glossary

(1) Internet Many different computer networks interconnected through standard communication protocols, enabling the mutual exchange of information.

(2) (Electronic) Message Refers to text, sound, images, symbols, or other data produced in electronic, magnetic, or other forms that cannot be directly perceived by humans, sufficient to represent the intended meaning of the record, and used for electronic processing purposes.

(3) Electronic Signature Refers to data in electronic form that is attached to an electronic document and can be used to identify and confirm the identity of the signer of the electronic document. The signer produces the message using digital, voice, fingerprint, or other biometric optical technology characteristics. It is attached to the electronic message and has the same effect as a handwritten signature, and can be used to identify and confirm the identity of the signer and to verify the integrity of the signed message.

(4) Encrypt/Encipher Refers to the use of mathematical algorithms or other methods to process an electronic document into garbled form to ensure the security of data transmission.

(5) Decrypt/Decipher The process of restoring an encrypted message that is unrecognizable to humans back into a recognizable message using relevant mathematical algorithms or other methods.

(6) Digital Signature A Digital Signature is a type of Electronic Signature that uses an Asymmetric Cryptosystem and a Hash Function to compress a fixed-length digital message and then encrypt it with the signer's Private Key. The corresponding Public Key can verify this encrypted digital message, forming a data message that can identify the signer's identity and verify the authenticity of the electronic document.

(7) Private Key Refers to one of a pair of mathematically related digital data used to create and verify digital signatures, held by the signer. In addition to being used for creating digital signatures, this digital data can also be used for decrypting electronic messages.

(8) Public Key In an asymmetric cryptographic algorithm for digital signatures, refers to the publicly disclosed one of a pair of mathematically related digital data used to create and verify digital signatures. It can be used to verify the correctness of messages signed by the signer, and when performing message confidentiality functions, it can be used to encrypt transmitted messages.

(9) (Public Key) Certificate or Electronic Certificate A digitally formatted record signed and issued by a Certification Authority using a computer as a medium, containing the applicant's registered Distinguished Name, Public Key, the validity period of the Public Key, the Certification Authority's registered Distinguished Name and signature, and other relevant identification information, used to confirm the identity of the signer and to prove that they possess the corresponding Public Key and Private Key pair.

(10) Certification Authority (CA) An organization that provides digital signature creation and electronic authentication services. It is an entity that maintains an objective and impartial position, verifies the correctness of certificate applicants' identity information, the association between and legitimacy of their Public Key and Private Key, and issues Public Key certificates accordingly.

(11) Certification Practice Statement (CPS) The operational guidelines published by a Certification Authority to its served entities regarding certificate issuance, revocation, inquiry, and other management operations and application procedures. It contains the Public Key Infrastructure and security mechanisms for certificate operations, operational guidelines and procedures, security mechanisms implemented in the CA's hardware and software, responsibility management, and related regulations.

(12) Asymmetric Cryptosystem A computer-based mathematical algorithm that can generate and use a pair of mathematically related security keys. The Private Key is used to sign messages, and the corresponding Public Key is used to verify signed messages. The Public Key can also be used to encrypt messages, and the corresponding Private Key is used to decrypt encrypted messages.

(13) Hash Function A mathematical algorithm that can convert a long string of bit messages into a fixed-length bit message. The same message input through the compression function will always produce the same output, and it is impossible to derive the input message from the output result.

(14) Issue a Certificate (Electronic Authentication) Refers to the process where a Certification Authority, in accordance with its Certification Practice Statement, reviews the identity qualifications and related documents of a Public Key certificate applicant, verifies the pairing relationship between their Public Key and Private Key, and then issues a Public Key certificate or other certificates.

(15) CABF (CA/Browser Forum) A non-profit organization composed of CAs and browser developers. The primary goal of this organization is to establish and promote industry standards for certificates, ensuring that certificates are trusted and widely accepted. Currently, the organization has defined relevant specifications for TLS certificates, CodeSign certificates, and S/MIME certificates. CAs issuing such certificates shall comply with the relevant specifications in order for their issued certificates to be publicly trusted (https://cabforum.org/).

Appendix II: Acronyms and Abbreviations

Acronym / Abbreviation	Description
CA	Certification Authority
CC	Common Criteria
CCITSE	Common Criteria for Information Technology Security Evaluation
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
EAL	Evaluation Assurance Level
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
LDAP	Lightweight Directory Access Protocol
ML-DSA	Module-Lattice-based Digital Signature Algorithm
ML-KEM	Module-Lattice-based Key-Encapsulation Mechanism
NB	Network Banking
OCSP	Online Certificate Status Protocol
OECD	Organization for Economic Co-operation and Development
OID	Object Identifier
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure

Acronym / Abbreviation	Description
PMA	Policy Management Authority
RA	Registration Authority
RCA	Root Certification Authority
RSA	Rivest, Shamir, Adleman (Encryption Algorithm)
S/MIME	Secure/Multipurpose Internet Mail Extensions
S/MIME BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
SLH-DSA	Stateless Hash-based Digital Signature Algorithm
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location