TAIWAN-CA INC. CYBER Certification Authority Certificate Policy and Certification Practice Statement (TWCA CYBER CA CP/CPS)

(Version 2.2)

Effective Date: 2026/06/08

Document History

Version	Revision Date	Revision Description
1.0	October 30, 2022	Initial version.
1.1	February 29, 2024	Adjusted Sections 7.1.2.2, 7.1.2.3, and 7.1.4.3.1.
2.0	April 9, 2025	Revised in accordance with the "Required Items for Digital Signature Certification Practice Statements" promulgated under the new Electronic Signatures Act.
2.0.1	November 15, 2025	3.2.2: Added description of validation record validity period. 3.2.2.4: Added/removed domain validation methods and added MPIC requirements. 3.2.2.4: Added DNSSEC requirements. 3.2.2.5: Added MPIC requirements. 3.2.2.8: Added MPIC and DNSSEC requirements. 3.2.2.9: Added MPIC requirements. 3.3.1, 6.3.2: Added certificate validity period restrictions. 5.7.1.2: Added description of mass certificate revocation plan. 7.1.4.3.1: Tabulated certificate names.
2.2	June 8, 2026	Merged CP/CPS. Added international compliance declarations. 3.2.2: Removed unused validation methods, added long-lived validation methods, and tabulated them for readability. 4.1, 4.3, 4.7, 4.9: Added ACME automation operations. 5.2: Added developer role. 6.7: Added vulnerability response and remediation timelines. 3.2.2.8, 4.2.4: Added RFC 8657 CAA parameter (`accounturi` , `validationmethods`) processing disclosure pursuant to CA/Browser Forum Ballot SC-098v2.

Summary

The key items of the TAIWAN-CA INC. CYBER Certification Authority Certificate Policy and Certification Practice Statement are described as follows:

Certificates Issued

Certificates issued by the TAIWAN-CA INC. CYBER Certification Authority (hereinafter referred to as "this Certification Center") are issued to Subscribers' domain hosts, enabling Relying Parties to identify the host name and the managing organization, serving as certificates for domain host identity authentication. Certificate types include "SSL Certificates" and "EV SSL Certificates." Unless otherwise specified, "Subscriber certificates" in this document refers to both types of certificates.

Certificate Types and Applicable Scope

Certificate Type	Applicable Scope
SSL Certificate	Used to protect online communication security and reduce the risk of information being maliciously intercepted or tampered with. Through organization validation and domain validation, it provides website host identity authentication (Server Authentication), ensuring that users connect to genuine and legitimate servers. It is applicable to network environments requiring high security, such as e-commerce websites on the Internet.
EV SSL Certificate	Used to protect online communication security and reduce the risk of information being maliciously intercepted or tampered with. Through enhanced organization validation and domain validation, it provides website host identity authentication (Server Authentication), ensuring that users connect to genuine and legitimate servers. It is applicable to network environments requiring very high security, such as financial transaction websites on the Internet.

Note:

Internationally, SSL certificates are defined at four different levels: from highest to lowest, they are EV (Extended Validation), OV (Organization-Validated), DV (Domain-Validated), and IV (Individual-Validated). The "SSL Certificates" issued by this Certification Center are OV-level certificates, while "EV SSL Certificates" are EV-level certificates. This Certification Center does not issue DV or IV level certificates.

The EKU (extended key usage) extension field of Subscriber certificates issued by this Certification Center contains only the following usages:

- id-kp-serverAuth and id-kp-clientAuth; or
- id-kp-serverAuth

Subscriber certificates issued by this Certification Center in accordance with this CP/CPS require applicants to pass the "Organization Authentication Procedure" and the "Domain Authentication Procedure" ("Domain Host Name Authentication Procedure" or "IP Address Verification") prescribed by this Certification Center, to confirm the applicant's identity and ownership of the host name. Verifying a domain host's certificate using the Public Key of this Certification Center can be used to verify the mutual trust relationship between this Certification Center and the domain host. If the digital signature on the certificate is verified as correct, it can be confirmed that the domain host's certificate was indeed issued by

this Certification Center, and the name identification information recorded in the certificate is valid, having passed the initial verification procedure of this Certification Center's Registration Authority.

Important Legal Liability Matters

If a Subscriber encounters grounds for certificate revocation (such as Private Key compromise or loss), the Subscriber shall immediately notify this Certification Center and carry out certificate revocation procedures. However, the Subscriber shall bear the risks and liabilities arising from the use of the certificate before the revocation status is published.

This Certification Center shall not be liable for damages in processing Subscriber registration data and certificate issuance operations, unless this Certification Center has failed to follow the provisions of this CP/CPS, violated relevant laws and regulations, or the damage is attributable to the intentional act or negligence of this Certification Center.

This Certification Center shall not be liable for damages to Subscribers caused by force majeure events (e.g., earthquakes) or other causes not attributable to this Certification Center (e.g., war).

This Certification Center shall be liable for damages if it fails to properly safeguard Subscriber registration and certificate-related data, resulting in information leakage, unauthorized use, tampering, or arbitrary use causing damage to third parties.

Upon receiving a certificate revocation request, this Certification Center shall investigate and provide a preliminary response within 24 hours, and the time from receiving the request to completing the revocation shall not exceed the time frame specified in Section 4.9.1.1. After the certificate revocation operation is completed, the Certificate Revocation List shall be issued and published in the Repository at the frequency specified in Section 4.9.7. Before the certificate revocation status is published, the Subscriber shall take appropriate actions to reduce the impact on Relying Parties and shall bear all liabilities arising from the use of the certificate. For detailed revocation operation specifications, please refer to Section 4.9.

In the event of a damage compensation incident between this Certification Center and the Subscriber arising from certificate issuance or usage, the liability of both parties shall be limited to the scope prescribed by relevant laws and regulations and the contract.

By accepting and using certificates issued by this Certification Center, Relying Parties acknowledge and agree to the terms regarding this Certification Center's legal liability and shall rely on such certificates within the scope specified in this CP/CPS.

Other Important Matters

- When there are concerns that the Subscriber's Private Key has been lost or compromised, or when Subscriber-related information has changed, the Subscriber must notify this Certification Center in accordance with the relevant operating procedures.
- Subscribers shall properly generate, safeguard, and use Private Keys, and comply with the restrictions on the use of keys and certificates.

- When applying for certificates, Subscribers must provide accurate and correct information. When accepting certificates issued by this Certification Center, Subscribers must verify the correctness of the certificate content and confirm that the Public Key and Private Key are a matching key pair.
- When verifying certificates, Relying Parties shall use the self-signed certificate of the Root Certification Authority to verify the digital signature of the Subordinate Certification Authority certificate, and use the Subordinate Certification Authority certificate to verify whether the digital signature of the Subscriber certificate was signed by the Subordinate Certification Authority's Private Key, and verify through the Certificate Revocation List or OCSP whether the certificate status has been revoked.
- When using the Certificate Revocation List issued by this Certification Center, Relying Parties shall first verify the digital signature to confirm whether the Certificate Revocation List is valid.
- The Company obtained the ISO 27001 Information Security Management System certificate in September 2007, has maintained its validity continuously, and completed the transition to ISO 27001:2022 in June 2024.
- The Company obtained the BS 10012 Personal Information Management System certificate in November 2013. The transition to BS 10012:2017 was completed in July 2018, and the ISO 27701 Privacy Information Management System certificate was simultaneously obtained, maintaining validity to the present.
- The Company obtained the ISO 20000-1 IT Service Management System certificate in December 2020, maintaining validity to the present.
- The Company obtained the ISO 22301 Business Continuity Management System certificate in November 2021, maintaining validity to the present.
- This Certification Center conducts internal audits at least once per quarter and commissions an accounting firm to conduct at least one external audit per year to ensure that its operations comply with the Certification Practice Statement and Certificate Policy. For detailed audit operation specifications, please refer to Chapter 8.

1. Introduction

1.1 Overview

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

The TAIWAN-CA INC. CYBER Certification Authority Certificate Policy and Certification Practice Statement (TWCA CYBER Certification Authority Certificate Policy and Certification Practice Statement; hereinafter referred to as "this CP/CPS") is established in accordance with the "Required Items for Digital Signature Certification Practice Statements" promulgated by the competent authority of this country. It

primarily describes how the TAIWAN-CA INC. CYBER Certification Authority (hereinafter referred to as "this Certification Center") conducts certificate issuance and management operations.

In addition to domestic laws and regulations, this Certification Center, to ensure the global trustworthiness of issued certificates and to maintain Internet communication security and user trust, expressly declares compliance with the following international standards and the latest requirements of browser root certificate policies:

- **CA/Browser Forum**: The latest versions of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (hereinafter referred to as "BR") and the Guidelines for the Issuance and Management of Extended Validation Certificates (hereinafter referred to as "EVG"), published at http://www.cabforum.org.
- **Browser Policies**: Including but not limited to the Chrome Root Program Policy, Mozilla Root Store Policy, Apple Root Program, and Microsoft Trusted Root Program.
- **CCADB Policy**: Compliance with the Common CA Database (CCADB) policy requirements jointly maintained by multiple browser vendors.

To establish a secure and trustworthy online transaction environment, ensuring that information is not easily forged, tampered with, or stolen during network transmission, and to reliably authenticate domain host names and their associated legal entities or organizations for identification by Relying Parties, TWCA has established a Public Key Infrastructure (TWCA Public Key Infrastructure; TWCA PKI, hereinafter referred to as "this Infrastructure") and has set up a Trust Anchor Root Certification Authority (Root Certification Authority; RCA), which issues certificates to Subordinate Certification Authorities, which in turn issue certificates to Subscribers.

1.2 Document Name and Identification

The name of this CP/CPS is "TAIWAN-CA INC. CYBER Certification Authority Certificate Policy and Certification Practice Statement." For the certificate policy identifiers used by this Certification Center, please refer to Section 7.1.6.

1.2.1 Version Change History

This CP/CPS complies with and conforms to the BR and EVG. The Company periodically reviews these standards and revises this CP/CPS at least once per year. Additionally, if any inconsistencies between this CP/CPS and these standards or domestic laws are identified, the Company will make revisions or, as appropriate, raise objections with the CA/Browser Forum. The history of version changes can be found in the "Document History" section of this CP/CPS.

1.3 Members and Applicable Scope

This Certification Center includes the following members:

- Certification Authority (CA)
- Registration Authority (RA)

- Subscriber
- Relying Party
- Policy Management Authority (PMA)

The Certification Authority is divided by hierarchy and purpose into the "Root Certification Authority" (Root CA, abbreviated as RCA) and the "Subordinate Certification Authority" (User CA, abbreviated as UCA), collectively referred to as "this Certification Center." The member relationship diagram is as follows:

[Member Relationship Diagram]

This CP/CPS will describe in Chapter 3 and Chapter 4 how this Certification Center conducts Subscriber certificate issuance and management operations, and how Subscribers and Relying Parties apply for and use certificates; Chapter 5 describes the management guidelines for the Root Certification Authority and the Subordinate Certification Authority.

1.3.1 Certification Authority

1.3.1.1 Root Certification Authority

The Root Certification Authority is the top-level certification management organization and serves as the Trust Anchor of this Infrastructure. It is operated and managed by the Company and is primarily responsible for the following:

- Issuance and management of Subordinate Certification Authority certificates; it shall not issue Subscriber certificates.
- Management and publication of Subordinate Certification Authority certificates and Certificate Revocation Lists (CRL) in the Repository.
- Provision of Online Certificate Status Protocol (OCSP) services.
- Maintaining the stability and operation of the Repository.
- It is deployed in an independent, security-controlled operating environment, where two or more authorized personnel perform the generation, deployment, and issuance of Subordinate Certification Authority certificates using Public Keys. The RCA certificate is a self-signed certificate. When a new certificate is generated or renewed, it must be delivered to users or users must be notified to obtain it from the Root Certification Authority through the most expedient and appropriate channels.

1.3.1.2 Subordinate Certification Authority

The Subordinate Certification Authority is operated and managed by the Company and is primarily responsible for the following:

- Issuance and management of Subscriber certificates.
- Management and publication of Subscriber certificates and Subscriber Certificate Revocation Lists (CRL) in the Repository.

- Provision of Online Certificate Status Protocol (OCSP) services.
- Maintaining the stability and operation of the Repository.

1.3.1.3 Policy Management Authority

The TAIWAN-CA INC. Policy Management Authority (PMA) is an organization established within the Company and is responsible for formulating the following:

- Certificate Policy and Certification Practice Statement (CP/CPS).
- Operational standards.

1.3.2 Registration Authority

The Registration Authority (RA) is primarily responsible for verifying the identity of applicants (Subscribers) and the related information required for certificate issuance, to serve as the basis for this Certification Center to issue Subscriber certificates.

This Certification Center establishes its own Registration Authority and does not delegate it to a third party.

1.3.3 Subscriber

A Subscriber is the entity recorded in the certificate Subject name, who holds the Private Key corresponding to the Public Key in the certificate.

The Subscribers of this Certification Center are legal entities or organizations that apply for certificates.

1.3.4 Relying Party

A Relying Party is an entity that uses the Public Key in the certificate issued by this Certification Center to verify the validity of the digital signature messages of Subscriber certificates issued by this Certification Center.

Relying Parties use the identity information recorded in Subscriber certificates to identify the domain host name and the information of its associated legal entity or organization.

Relying Parties shall use the information recorded in the certificates issued by this Certification Center to determine whether to rely on the certificate or whether it can be used for a specific purpose.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued by this Certification Center to Subscribers are primarily used for website authentication, ensuring the authenticity of domain host identity and establishing a secure encrypted

transmission channel with the connecting party. Certificate types and applicable scope are as follows:

Certificate Type	Applicable Scope
SSL Certificate	Used to protect online communication security and reduce the risk of information being maliciously intercepted or tampered with. Through organization validation and domain validation, it provides website host identity authentication (Server Authentication), ensuring that users connect to genuine and legitimate servers. It is applicable to network environments requiring high security, such as e-commerce websites on the Internet.
EV SSL Certificate	Used to protect online communication security and reduce the risk of information being maliciously intercepted or tampered with. Through enhanced organization validation and domain validation, it provides website host identity authentication (Server Authentication), ensuring that users connect to genuine and legitimate servers. It is applicable to network environments requiring very high security, such as financial transaction websites on the Internet.

Note:

Internationally, SSL certificates are defined at four different levels: from highest to lowest, they are EV (Extended Validation), OV (Organization-Validated), DV (Domain-Validated), and IV (Individual-Validated). The "SSL Certificates" issued by this Certification Center are OV-level certificates, while "EV SSL Certificates" are EV-level certificates. This Certification Center does not issue DV or IV level certificates.

The EKU (extended key usage) extension field of Subscriber certificates issued by this Certification Center contains only the following usages:

- id-kp-serverAuth and id-kp-clientAuth; or
- id-kp-serverAuth

Subscriber certificates are issued by this Certification Center in accordance with this CP/CPS. Applicants must pass the "Organization Authentication Procedure" and the "Domain Authentication Procedure" prescribed by this Certification Center to confirm the applicant's identity and ownership of the host name. The authentication procedures are as follows:

Organization Authentication Procedure

When authenticating the identity of a legal entity or organization, the identity of its representative shall first be authenticated, and documents sufficient to prove the registration or existence of the legal entity or organization shall be verified.

Application documents may be submitted via the Internet, in person, by mail, or by fax. The information provided in the application documents is verified against third-party public information or other supporting information to confirm that the content of the application documents is consistent with the verified content. For details, please refer to Section 3.2.2.1.

Domain Authentication Procedure

- Domain host name authentication procedure: Must pass at least one of the validation methods defined in Section 3.2.2.4.
- IP address verification: Must pass at least one of the validation methods defined in Section 3.2.2.5.

Natural Person Authentication Procedure

Applications from natural persons are not accepted.

1.4.2 Prohibited Certificate Uses

Certificates issued by this Certification Center, other than for the uses specified in Section 1.4.1, are prohibited from being used for the following purposes:

- Eavesdropping on or intercepting third-party communications.
- Uses that cause bodily harm, death, or psychological injury.
- Applications or businesses that pose significant harm to social order and public interest.
- Applications or businesses explicitly prohibited or excluded by the Electronic Signatures Act, other relevant laws and regulations, or the competent authorities of the respective industries.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The authority for the formulation, revision, and publication of this CP/CPS rests with the PMA.

1.5.2 Contact Person

For any questions regarding this CP/CPS, or for related security incident reports (such as concerns about key compromise or certificate mis-issuance), please provide detailed information and contact details through the following contact:

Item	Details
Company Name	TAIWAN-CA INC. (TWCA)
Contact Person	Customer Service Center
Address	10th Floor, 85, Yen-Ping South Road, Zhongzheng District (100), Taipei, Taiwan, R.O.C.
Telephone	886-2-23708886
Fax	886-2-23700728
Email	ca@twca.com.tw

1.5.3 Certification Practice Statement Approval

The Certification Practice Statement established by this Certification Center is approved by the PMA.

1.5.4 Certification Practice Statement Approval Procedures

In accordance with the Electronic Signatures Act, the Certification Practice Statement established by this Certification Center must be approved by the competent authority before this CP/CPS may be publicly published and certificate issuance services may be provided.

1.6 Definitions and Abbreviations

Please refer to Appendix I and Appendix II.

2. Publication and Repository

2.1 Repository

The Repository of this Certification Center provides querying or downloading of certificates, Certificate Revocation Lists (CRL), Certificate Policy and Certification Practice Statement, and other certificate operation-related information. It also provides Online Certificate Status Protocol (OCSP) services.

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

The Repository addresses for CRL and OCSP are specified in certificate extension fields. For detailed information, please refer to Chapter 7.

2.2 Publication of Certificate Information

The information published by this Certification Center includes the following:

- Historical Certificate Policies and Certification Practice Statements.
- Certificates and related information of this Certification Center.
- Issued certificates.
- CRL.
- OCSP services.
- Certificate test websites, including test websites for valid certificates, expired certificates, and revoked certificates, the locations of which are published on CCADB.
- Historical audit reports.
- List of organizational Registration Authorities (see Section 3.2.2.7).

2.3 Time or Frequency of Publication

This CP/CPS, upon completion of revisions and approval by the Policy Management Authority (PMA), will be submitted to the competent authority for approval. The Company shall publish it in the Repository within 7 business days of receiving the approval document.

Certificates of this Certification Center, once issued, together with the certificate chain and related certificate information, shall be published in the Repository within 7 business days for querying by

Subscribers or Relying Parties. The CRL issuance frequency is in accordance with the provisions of Section 4.9.7.

This Certification Center periodically reviews this CP/CPS and revises this CP/CPS at least once per year.

2.4 Access Controls on Repositories

The Repository is made publicly available in read-only mode for querying by Subscribers or Relying Parties. However, to prevent malicious attacks or tampering, access controls are enforced when updating Repository information or when traffic is abnormal.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The certificates issued by this Certification Center and Subscribers use Subject Distinguished Names (Subject DN) and Issuer Distinguished Names (Issuer DN) that comply with the X.500 Distinguished Name (DN) naming convention. The Common Name (CN) or Subject Alternative Name (SAN) shall not use internal names or reserved IP addresses. The attributes and content of such names comply with the relevant provisions of RFC 5280, BR, and EVG.

3.1.2 Need for Names to Be Meaningful

The Subject Distinguished Name recorded in the Subscriber certificate shall comply with the naming requirements of applicable laws and regulations. It must be sufficient to identify a specific legal entity or organizational unit and Domain Name, and must be identifiable by Relying Parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

This CP/CPS does not allow Subscribers to use anonymous names, pseudonyms, aliases, or pen names. However, the use of Punycode encoding for Internationalized Domain Names (IDNs) is accepted.

3.1.4 Rules for Interpreting Various Name Forms

The interpretation rules for names recorded in certificates are defined in accordance with ITU-T X.520 name attribute definitions.

3.1.5 Uniqueness of Names

This Certification Center shall verify the uniqueness of Subscriber Chinese and English names, Domain Names, and legal entity or organization identification names. The same Domain Name may not be used by

different legal entities or organizations; however, multiple certificates for the same Domain Name may be issued to the same legal entity or organization.

When Subscriber certificates have identical unique distinguished names, this Certification Center gives priority to the Subscriber who first registered and passed the organization identity and domain validation. If a later applicant completes identity verification before the earlier applicant, the later applicant may be given priority.

In the event of a dispute regarding the use of a distinguished name, if a competent authority/institution confirms through legitimate documentation that the name belongs to another applicant, this Certification Center shall revoke the registered Subscriber's right to use the unique distinguished name, revoke the issued certificate, and the Subscriber shall bear the relevant legal liability.

3.1.6 Recognition, Authentication, and Role of Trademarks

This Certification Center respects the registered trademarks of Subscriber Chinese and English names. After verification, Subscribers are allowed to use such Chinese and English names; however, this Certification Center does not guarantee the recognition, verification, or uniqueness of the Subscriber's registered trademark. In the event of a trademark dispute, the Subscriber shall resolve the matter through legal channels.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Public Key in the certificate and the corresponding Private Key shall be generated by the Subscriber. The Subscriber shall submit a certificate request file in PKCS#10 format to this Certification Center as proof of possession of the Private Key. This Certification Center shall use the Subscriber's Public Key to verify the signature value within the request file, confirming that the Subscriber is the owner of the Private Key and that the Public Key and Private Key form a key pair.

3.2.2 Authentication of Organization and Domain Identity

Prior to issuing a Subscriber certificate, an "Organization Validation Procedure" and a "Domain Validation Procedure" ("Domain Name Validation Procedure" or "IP Address Verification") must be performed to confirm whether the applicant is a legitimate legal entity or organization, and to confirm whether the applicant possesses ownership and control of the domain being applied for.

The maximum validity periods for Validation Records of the "Organization Validation Procedure" and "Domain Validation Procedure" of this Certification Center are as follows. If no valid Validation Record is found, the initial validation procedure shall be re-performed in accordance with the provisions of this section.

The maximum validity periods for Validation Records shall be progressively shortened in accordance with BR Section 4.2.1 as follows:

Organization Validation Procedure — Validation Record Validity Period

Certificate NTB >=	Certificate NTB <	Maximum Validation Record Validity
—	March 15, 2026	825 days
March 15, 2026	—	398 days

Domain Validation Procedure — Validation Record Validity Period

Certificate NTB >=	Certificate NTB <	Maximum Validation Record Validity
—	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029	—	10 days

3.2.2.1 Organization Validation Procedure

This procedure applies to the validation of legal entities or organizations. For purposes of this section, the unified term "organization" is used. When performing identity validation of an organization, verification shall be conducted against certification documents issued by the competent authority or other documents that can prove the existence of the organization. The identity of the representative must also be verified. Application documents may be submitted via the Internet, in person at the counter, by mail, or by fax.

For application documents provided by Subscribers, third-party publicly available organization registration agencies or other evidentiary information shall be queried to verify the applicant's legal existence and identification information, and to confirm that the content of the application documents matches the verified content, such as the organization's registered name, trade name, and country, to satisfy the identity validation requirements of BR or EVG.

If the certificate type to be issued is an EV SSL Certificate, the following additional validation procedures must be completed for the applying organization before issuance (the "registration agency" referred to in the following procedures means the organization registration agency, not the certificate Registration Authority):

1. The organization name must be the full legal name. Organizational prefixes or suffixes may be abbreviated, e.g., "Company Name Incorporated" may be abbreviated to "Company Name, Inc."
2. The organization type must be confirmed as one of the following: Private Organization, Government Entity, Business Entity, or Non-Commercial Entity.
3. Data recorded in the certificate fields relating to the jurisdiction of incorporation (e.g., Jurisdiction of Incorporation Locality Name) shall not contain information not recorded by the registration agency.
4. If the registration agency's records do not contain an organization registration number (Unified Business Number), the organization's date of formation or registration shall be entered in the

organization registration number field of the certificate.

5. The business address recorded in the certificate fields must be the organization's physical business address.
6. If the applicant is a Business Entity representing an individual, the identity of the person in charge must be verified through an in-person, face-to-face process at the counter.
7. Organization registration data and company status shall be verified through trusted third-party registration agency channels, such as the Ministry of Economic Affairs business status inquiry and the Fiscal Information Agency of the Ministry of Finance. Such channels must be from the "Organization Registration Agency List." The "Organization Registration Agency List" used by this Certification Center is published in the Repository on the official website homepage, and all sources are official repositories of government agencies.
8. In accordance with EVG Section 11.6, it shall be confirmed whether the organization represented by the applicant genuinely exists.
9. When applying for an EV SSL Certificate, the Certificate Requestor, Certificate Approver, and Contract Signer information must be provided.

3.2.2.2 Trade Name Validation Procedure

In accordance with the provisions of Section 3.2.2.1.

3.2.2.3 Country Name Identification

In accordance with the provisions of Section 3.2.2.1.

3.2.2.4 Domain Name Validation Procedure

This Certification Center (hereinafter referred to as "this Center") shall perform ownership verification on the Common Name (CN) and Subject Alternative Name (SAN) of the certificate being applied for by the applicant, using at least one of the following "Domain Name Validation Procedures":

Validation Method Name (Applicable BR Section)	Description
Email Validation (BR 3.2.2.4.4)	This Center sends an email containing a unique random value with a 30-day validity period to the designated recipient. This Center then verifies the random value. The recipient email address is limited to: admin, administrator, webmaster, hostmaster, or postmaster, followed by "@" and the domain name to be validated. **Restrictions and requirements:** This Center will not use this validation method after March 15, 2028.
DNS Change Validation (BR 3.2.2.4.7)	The applicant creates a CNAME, TXT, or CAA resource record in the DNS service of the domain to be validated, naming it with the domain name to be validated or a label prefixed with an underscore character placed before the domain name to be validated, and places a unique Request Token value therein. This Center then verifies the record. **Restrictions and**

Validation Method Name (Applicable BR Section)	Description
	requirements: This Center will implement Multi-Perspective Issuance Corroboration (MPIC) for this validation method.
Website Change Validation (BR 3.2.2.4.18)	The applicant places a unique Request Token value designated by this Center in the specified website directory of the domain to be validated: "/.well-known/pki-validation". This Center then initiates an HTTP request to verify. The HTTP response status code must indicate success (2xx). If redirected, only HTTP-layer redirects are permitted (HTTP response status codes limited to: 301, 302, 307, or 308), and the redirected URL must use the HTTP/HTTPS protocol on an authorized port. **Restrictions and requirements:** This Center will implement Multi-Perspective Issuance Corroboration (MPIC) for this validation method. Wildcard Domain certificates shall not use this method for verification.
Website Change Validation (ACME) (BR 3.2.2.4.19)	The applicant uses the HTTP challenge method in the ACME protocol (defined in RFC 8555 to prove domain control, which is then verified by this Center. **Restrictions and requirements:** This Center will implement Multi-Perspective Issuance Corroboration (MPIC) for this validation method. Wildcard Domain certificates shall not use this method for verification.
Long-Lived DNS Validation (BR 3.2.2.4.22)	The applicant uses the "persistent DNS TXT record" domain validation method (corresponding to the ACME `dns-persist-01` challenge type) by adding a TXT record in a specific format under the _validation-persist label in DNS. The record must contain account identification information (accounturi) recognized by this Center. If a validity period (persistUntil) is set, the verification must occur within that period. After completion of this validation method, the validation data is valid for a maximum of 10 days. For this Center's Issuer Domain Names, please refer to Section 4.2.1. **Restrictions and requirements:** The Issuer Domain Name of this Certification Center is twca.com.tw. This Center will implement Multi-Perspective Issuance Corroboration (MPIC) for this validation method.

For the Long-Lived DNS Validation method (BR 3.2.2.4.22), the `accounturi` value carried in the persistent DNS TXT record shall be the URL of the requesting ACME account, in the format `https://ssl2.twca.com.tw/acme_m2/acct/{accountID}`, where `{accountID}` is the account identifier assigned by this Certification Center at the time of ACME account registration. The same format applies to the `accounturi` parameter as it appears in CAA records; see Section 4.2.4.

All Validation Records of this Certification Center include the applied Fully Qualified Domain Name (FQDN), the validation method used, the Authorization Domain Name for which verification was completed, and the BR version followed. Among the above validation methods, all methods except method (4) use Public Suffix List information, which is applied to Domain Name verification.

When performing the "Domain Name Validation Procedure," this Certification Center's Primary Network Perspective DNS resolver used for querying DNS records must establish a validation chain to the IANA DNSSEC root trust anchor and perform DNSSEC validation.

3.2.2.5 IP Address Verification

This Certification Center (hereinafter referred to as "this Center") shall perform ownership verification on all IP addresses to be included in the certificate applied for by the applicant, using at least one of the following "IP Address Verification Procedures":

Validation Method Name (Applicable BR Section)	Description
Website Change Validation (BR 3.2.2.5.1)	The applicant places a unique Request Token value designated by this Center in the specified website directory of the IP to be validated: "/.well-known/pki-validation". This Center then initiates an HTTP request to verify. **Restrictions and requirements:** This Center will implement Multi-Perspective Issuance Corroboration (MPIC) for this validation method.
Reverse IP Lookup Validation (BR 3.2.2.5.3)	A reverse-IP lookup is performed on the IP address to obtain the associated domain name. The FQDN is then validated for control using a domain validation method permitted under Section 3.2.2.4, thereby confirming the applicant's control over the IP address. **Restrictions and requirements:** This Center will implement Multi-Perspective Issuance Corroboration (MPIC) for this validation method. This Center will not use this validation method after March 15, 2027.
Website Change Validation (ACME) (BR 3.2.2.5.6)	Verification is performed using the http-01 method of the ACME protocol (defined in RFC 8555. **Restrictions and requirements:** This Center will implement Multi-Perspective Issuance Corroboration (MPIC) for this validation method.

3.2.2.6 Wildcard Domain Validation

After removing the "*." from the applied domain, the remaining domain name must not appear on the Public Suffix list. Related requirements comply with the requirements of BR Section 3.2.2.6. Other provisions follow Section 3.2.2.4.

3.2.2.7 Data Source Accuracy

The "Organization Registration Agency List" used by this Certification Center for the Organization Validation Procedure is published in the Repository on the official website homepage, and is regularly reviewed and updated.

The "Organization Registration Agency List" used by this Certification Center is sourced from official repositories of government agencies or other information channels generally accepted within the industry.

3.2.2.8 CAA Record Verification

When verifying the Certification Authority Authorization (CAA) records for the applicant's domain, this Certification Center checks, in accordance with RFC 8659 (or its subsequent updates), via the Domain

Name System (DNS) whether the domain has authorized issuance. If the CAA record authorizes this Certification Center, the certificate application may be approved; otherwise, it shall be rejected. During the verification process, the DNS resolver used by the Primary Network Perspective must establish a complete validation chain from the IANA DNSSEC root trust anchor and perform DNSSEC validation to ensure the integrity and security of the query. In addition, this Certification Center processes the `accounturi` and `validationmethods` parameters defined in RFC 8657; the supported parameter formats and matching practices are described in Section 4.2.4. The verification method follows BR Section 3.2.2.8, with detailed provisions in Section 4.2.1(7).

3.2.2.9 Multi-Perspective Issuance Corroboration (MPIC)

For "domain ownership" verification and "CAA record" verification, this Center will implement Multi-Perspective Issuance Corroboration (MPIC). Related requirements and provisions follow BR Section 3.2.2.9.

Minimum number of remote perspectives required:

Effective Date	Minimum Number of Remote Perspectives
September 15, 2025	2
March 15, 2026	3
June 15, 2026	4
December 15, 2026	5

Allowed number of inconsistencies for remote perspectives:

Number of Remote Perspectives	Allowed Number of Inconsistencies
2–5	1
6 or more	2

3.2.3 Authentication of Individual Identity

Applications from natural persons are not accepted.

3.2.4 Non-Verified Subscriber Information

All Subscriber information recorded in certificates issued by this Certification Center has been verified.

3.2.5 Validation of Authority

This Certification Center obtains reliable communication methods through the Organization Validation Procedure described in Section 3.2.2.1 to verify the identity of the legal entity or organization and its representative(s) and agent(s) (hereinafter referred to as "such persons"), including the authenticity of the names, titles, personal signatures, or company seals on the certificate application. When necessary, this

Certification Center shall contact the legal entity or organization to confirm that such persons are authorized to apply for the certificate.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

As the duration of key usage increases, the risk of loss or compromise also increases. Subscribers should regularly re-key to ensure key security. The maximum validity period of Subscriber certificates issued by this Certification Center is 200 days (the Private Key validity period is the same as the certificate validity period). The maximum validity period of Subscriber certificates will be progressively shortened in accordance with Section 6.3.2.

Re-keying a certificate means generating a new Public Key and Private Key pair before the certificate expires, and applying to this Certification Center for certificate issuance. This Certification Center will check whether a valid Validation Record exists. If no valid Validation Record is found, this Certification Center must re-perform the initial validation procedure in accordance with Section 3.2.

3.3.2 Identification and Authentication for Re-Key After Revocation

After a Subscriber's certificate is revoked, the Subscriber must undergo the initial validation procedure specified in Section 3.2 and re-apply for a new certificate.

3.4 Identification and Authentication for Revocation Request

When a revocation event described in Section 4.9.1 occurs, the person authorized to request revocation (as described in Section 4.9.2) shall submit a revocation request to this Certification Center. This Center adopts the following identification and authentication procedures for different business processes:

Business Process	Description
Manual Process	This Certification Center or Registration Authority shall verify the identity of the applicant (e.g., the original applicant, the legal representative, or an authorized agent). In addition to identity verification, the authenticity of the request data shall be verified in accordance with Section 3.2. When necessary, the legal entity or organization shall be contacted to confirm the specific facts for certificate revocation. If processed through an agent, the authorization requirements of Section 3.2.5 must be satisfied.
Self-Service Process	The applicant must log in using the originally established Self-Service issuance platform account. Upon login, the applicant must use a smart card issued by this Certification Center to

Business Process	Description
	perform a digital signature. After the signature is verified by the system, identity authentication is deemed passed. The system will verify whether the account has the authority to manage the certificate in question.
ACME Automated Process	The revocation request must comply with the RFC 8555 specification. The ACME Client must sign the revocation request message using the ACME account Private Key corresponding to the certificate. Upon receiving the request, this Certification Center will verify the digital signature using the ACME account Public Key bound in the database. The system verifies that the ACME account is the legitimate account that originally applied for the certificate; only after successful verification will the transaction request be accepted.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

This Certification Center operates under different business processes: "Manual Certificate Issuance," "Self-Service Certificate Issuance," and "ACME Automated Certificate Issuance."

4.1.1 Who Can Submit a Certificate Application

The representative or agent of a legal entity or organization wishing to apply for a certificate serves as the certificate applicant.

4.1.2 Enrollment Process and Responsibilities

Certificate applicants shall read the Subscriber agreement in advance and fully understand the rights and obligations associated with using the certificate. The applicant may complete identity verification through the online registration system and confirm agreement to the relevant terms, or prepare and sign a certificate application form in writing and submit it to this Certification Center for processing of the certificate application.

Certificate applicants must generate the certificate key pair and the corresponding PKCS#10 certificate request file (hereinafter referred to as CSR) themselves, and submit it through a secure channel provided by this Certification Center.

4.2 Certificate Application Processing

This Certification Center operates under different business processes: "Manual Issuance Process," "Self-Service Issuance Process," and "ACME Automated Issuance Process."

4.2.1 Performing Identification and Authentication Functions

The identification and authentication procedures for Subscriber certificate applications are as follows:

The representative of the legal entity or organization, or an agent designated by the representative, serves as the certificate applicant.

Overview of identification and authentication procedures for each business process:

Business Process	Description
Manual Process	The applicant does not need to establish an account in advance. For first-time applications, the applicant shall prepare the original certificate application form, affixed with the organization's official seal (e.g., company seal, invoice seal) and the applicant's signature, and mail it to this Certification Center for processing. This Certification Center manually verifies the authenticity of the application materials. The applicant shall prepare the certificate application form, affixed with the applying unit's departmental seal and the applicant's signature (or signatures of two persons from the unit), and submit it to the Registration Authority via fax, mail, or email. The applicant must generate the CSR and deliver it along with the application form number to this Certification Center through a secure channel.
Self-Service Process	The applicant must establish a Self-Service issuance platform account. The applicant must sign a contract with this Certification Center in advance, specifying the domain names in the contract. After review and approval by this Certification Center, a platform account is established and bound to the domain name whitelist. The applicant must use a smart card issued by this Certification Center as login credentials; upon login, a digital signature is performed, and certificate operations may proceed only after successful signature verification. For certificate renewal, the applicant logs into the issuance platform independently to perform the operation; for additional domain purchases, a separate contract must be signed with this Certification Center. The applicant must generate the CSR and log into the issuance platform to complete the certificate application request via file upload.
ACME Automated Process	The applicant must establish an automated issuance platform account. Before the first application, a contract must be signed specifying the domain names. The applicant must provide organization registration documentation, register an automated account on the online platform, and upon review and approval by this Certification Center, the account is established and bound to the domain name whitelist. The applicant must install an ACME Client in advance and obtain an External Account Binding (EAB) key to complete account association. This Certification Center binds the Subscriber identity with the ACME account Public Key. When executing ACME transactions, the ACME account Private Key must be used to sign the transaction messages; this Certification Center will accept the transaction request only after successful signature verification. For certificate renewal, within the contract validity period, the applicant may use the ACME Client to obtain a new certificate directly from this Certification Center; for additional domain purchases, a separate contract must be signed with this Certification Center. The ACME Client automatically generates the key pair and CSR, and transmits the certificate request information to this Certification Center via the ACME protocol.

The certificate applicant submits the certificate application form and a self-generated PKCS#10 format certificate request file. The certificate application form shall be affixed with the seal of the legal entity or organization, and the seal shall match the seal registered with the competent authority.

General Verification Requirements

Verification Requirement	Description
Validation Record validity check	This Certification Center performs validation in accordance with Section 3.2. If no valid "Organization Validation Record" or "Domain Validation Record" is found, the complete validation procedure must be re-executed. Validation Record validity periods are referenced in Section 3.2.2.
Key compliance	This Certification Center will check the Public Key in the CSR by querying the badkeys database (https://badkeys.info/) to ensure it is not a known weak key (e.g., Debian Weak Key) and does not duplicate any existing certificate key in this Certification Center's database. If the check fails, the certificate will not be issued.
Subject name restriction	This Certification Center will verify that the certificate Subject Name (CN) or Subject Alternative Name (SAN) does not contain an Internal Name or reserved IP address and is not listed on the Google Safe Browsing malware list.
EV SSL Certificate restriction	When applying for an Extended Validation (EV) certificate, the CN or SAN dNSName shall not contain a Wildcard Domain.

Review Result

After verifying the application materials, this CA determines whether to accept the application, request supplementary materials, or reject the application based on the verification results. Upon decision to accept, the process proceeds to the issuance phase.

4.2.2 Approval or Rejection of Certificate Applications

Applications that successfully complete the "Identification and Authentication Procedures" described in Section 4.2.1 are deemed to have passed the review, and the applicant obtains the status of a Subscriber of this Certification Center. If the applicant fails to pass the above procedures, this Center shall reject the certificate application.

To comply with international security standards, this Certification Center strictly prohibits the issuance of certificates containing the following attributes:

1. **Internal Names:** The Subject Name (CN) or Subject Alternative Name (SAN) of the certificate shall not use internal names. Specifically, the domain suffix must be listed in the IANA Root Zone Database (https://www.iana.org/domains/root/db); if the domain ending is not on that list, it is considered a non-publicly resolvable internal name.
2. **Reserved IP Addresses:** The CN or SAN of the certificate shall not contain reserved IP addresses. The definition follows the IANA IPv4 Special-Purpose Address Registry and IANA

IPv6 Special-Purpose Address Registry (https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml and https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml).

4.2.3 Time to Process Certificate Applications

No stipulation.

4.2.4 CAA Record Parameter Processing

When processing CAA records for an applicant's domain, this Certification Center processes the `accounturi` and `validationmethods` parameters defined in RFC 8657 when present, in addition to the issuer domain match performed under RFC 8659. Full processing of these parameters across all issuance processes (Manual, Self-Service, and ACME Automated) shall be in place no later than March 15, 2027, in accordance with the effective date specified in BR Section 4.2.2.1.

`accounturi` Parameter

The only `accounturi` value accepted by this Certification Center is the URL of the requesting ACME account, in the following form:

```
https://ssl2.twca.com.tw/acme_m2/acct/{accountID}
```

where `{accountID}` is the account identifier assigned by this Certification Center at the time of ACME account registration. Matching is performed by byte-for-byte case-sensitive comparison against the ACME account URL of the account submitting the certificate request.

For certificate applications submitted through the Manual or Self-Service processes, the `accounturi` parameter cannot be matched, since these processes do not utilize ACME accounts. Accordingly, if every CAA `issue` (or `issuewild`, for wildcard certificates) record authorizing this Certification Center for the relevant domain includes a non-empty `accounturi` parameter, the certificate application shall be rejected.

`validationmethods` Parameter

The `validationmethods` parameter is processed in accordance with RFC 8657 and BR Section 4.2.2.1. The labels recognized by this Certification Center, mapped to the validation methods listed in Section 3.2.2.4, are:

Label	Validation Method	Reference
`ca-tbr-4`	Email Validation (sunset March 15, 2028; see Section 3.2.2.4)	BR 3.2.2.4.4
`ca-tbr-7`	DNS Change Validation	BR 3.2.2.4.7
`dns-01`	DNS Change Validation via ACME `dns-01` Challenge (RFC 8555 §8.4)	BR 3.2.2.4.7

Label	Validation Method	Reference
`ca-tbr-18`	Website Change Validation	BR 3.2.2.4.18
`ca-tbr-19` / `http-01`	Website Change Validation (ACME)	BR 3.2.2.4.19
`ca-tbr-22` / `dns-persist-01`	Long-Lived DNS Validation	BR 3.2.2.4.22

Label matching is performed case-sensitively. A `validationmethods` parameter shall be deemed unsatisfied if none of its labels corresponds to the validation method actually used to validate domain control.

4.3 Certificate Issuance

This Certification Center operates under different business processes: "Manual Process," "Self-Service Process," and "ACME Automated Process."

4.3.1 CA Actions During Certificate Issuance

This Certification Center executes certificate issuance according to the following processes:

Overview of certificate issuance for each business process:

Business Process	Description
Manual Process	The system automatically checks the digital signature of the CSR to confirm integrity and proof of Private Key ownership; simultaneously, it verifies that the Subject Distinguished Name (DN) and extension fields are consistent with the application form and do not contain internal names or reserved IP addresses. The reviewing personnel log into the management console through two-factor authentication and perform the organization and domain validation defined in Section 3.2. A "dual-review system" is employed, where another personnel member confirms accuracy before issuance. This process shall not use domain validation methods 3.2.2.4.19 and 3.2.2.4.21.
Self-Service Process	The Subscriber logs into the Self-Service issuance platform account, generates the CSR, and initiates the certificate application request. The system automatically determines whether the organization and domain Validation Records are still valid. If the records are valid, the certificate is issued immediately; if invalid, the process is terminated and transferred to this Certification Center's personnel for manual review and validation. This process shall not use domain validation methods 3.2.2.4.19 and 3.2.2.4.21.
ACME Automated Process	The ACME Client automatically generates the key pair and CSR, transmitted through a TLS channel compliant with RFC 8555. The ACME Server automatically verifies the signature, Private Key ownership, and domain whitelist compliance. If verification passes, the certificate is automatically issued; if it fails, the automated process is terminated and transferred to this

Business Process	Description
	Certification Center's personnel for manual account configuration. This process is limited to domain validation methods 3.2.2.4.19, 3.2.2.4.21, or 3.2.2.4.22.

Pre-Issuance General Verification Requirements

Verification Requirement	Description
Certificate lint check	This Certification Center uses third-party tools (Zlint and pkilint) for verification to ensure the certificate complies with RFC 5280, CABF BR, and EVG specifications. If the check fails, the certificate will not be issued.
CAA record check	The Issuer Domain Name of this Certification Center is twca.com.tw. This Certification Center performs a CAA record check before certificate issuance. If the check fails, the certificate will not be issued. Refer to Section 3.2.2.8 for the specifications.

Certificate Transparency

This Certification Center uploads a Precertificate to CT (Certificate Transparency) log servers before issuing the final certificate. The certificate is issued only after obtaining a sufficient number of SCT (Signed Certificate Timestamp) entries. After issuance, the final certificate is also uploaded to the CT log servers.

Certificate Validity Period Restriction

The certificate start date (notBefore) in Subscriber certificates issued by this Certification Center is not backdated. That is, the certificate start date will not be earlier than the actual time of certificate issuance.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

This Certification Center notifies the Subscriber by telephone or email upon completion of certificate issuance. Subscribers using ACME automated certificate issuance will not be separately notified.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon receiving a certificate issued by this Certification Center, the Subscriber shall perform the following procedures:

1. Confirm that the certificate content is consistent with the information provided at the time of application and that it contains the Subscriber's correct information.
2. Verify that the Public Key in the certificate matches the Public Key information in the PKCS#10 certificate request file.

3. The Subscriber must validate the certificate chain, checking the correctness, integrity, and validity of each certificate in the chain, whether the certificate has been revoked, whether the certificate validity period has expired, and whether it was indeed issued by this Certification Center.
4. If the above procedures cannot be completed, the Subscriber shall immediately notify this Certification Center to revoke the certificate and may re-initiate the certificate issuance procedure described in Section 4.3.

The Subscriber, upon receiving the applied-for certificate, must confirm full understanding of and agreement to the rights and obligations associated with certificate use. If the Subscriber disagrees, the certificate is deemed rejected, and this Certification Center shall revoke the certificate.

This Certification Center only accepts certificate modification requests from Subscribers within 7 days after certificate issuance.

4.4.2 Publication of the Certificate by the CA

Upon completion of the certificate issuance procedure, this Certification Center publishes the Subscriber certificate in the Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The purpose, applicable scope, and restrictions of Subscriber certificates are in accordance with Section 1.4.

Subscribers shall properly protect their Private Keys. In the event of suspected misuse, exposure, loss, or other security concerns, Subscribers must report to this Certification Center.

4.5.2 Relying Party Public Key and Certificate Usage

Before relying on a Subscriber certificate issued by this Certification Center, Relying Parties shall at a minimum perform the following procedures to determine whether to trust the certificate:

1. Obtain the self-signed certificate of this Certification Center's Root Certification Authority (RCA) through an appropriate and secure channel.
2. Verify that the RCA self-signed certificate, the User Certification Authority (UCA) certificate, and the Subscriber certificate have not expired.
3. Using the Public Key of the RCA self-signed certificate, verify that the digital signature on the UCA certificate is valid and has not been revoked.

4. Using the Public Key of the UCA certificate, verify that the digital signature on the Subscriber certificate is valid.
5. Verify that the Subscriber certificate has not been revoked by the UCA.

If the above verifications cannot be passed, it indicates that the Subscriber certificate obtained by the Relying Party was not issued by this Certification Center, or the certificate is no longer valid, and the Relying Party should not trust the Subscriber certificate.

4.6 Certificate Renewal

Certificate renewal refers to re-issuing a certificate with the same key, a different serial number, and an extended validity period, while the Subscriber identification information remains unchanged.

This Certification Center does not provide certificate renewal service.

4.7 Certificate Re-Key

Certificate re-key refers to generating a new Public Key and Private Key pair and applying to the Certification Authority for certificate issuance using the original registration information. The following describes each business process:

Business Process	Description
Manual Process	The applicant shall prepare the certificate application form, affixed with the applying unit's departmental seal and the applicant's signature (or signatures of two persons from the unit), and submit it to the Registration Authority via fax or email. The applicant must generate the CSR and deliver it along with the application form number to this Certification Center through a secure channel. The reviewing personnel log into the management console through two-factor authentication and perform the organization and domain validation defined in Section 3.2. A "dual-review system" is employed, where another personnel member confirms accuracy before issuance.
Self-Service Process	The applicant completes the certificate re-key process through the Self-Service issuance platform account. The applicant must use a smart card issued by this Certification Center as login credentials; upon login, a digital signature is performed, and certificate re-key operations may proceed only after successful signature verification. The applicant must generate the CSR and complete the process by uploading the file on the platform. The system automatically determines whether the organization and domain Validation Records are still valid. If the records are valid, the certificate is issued immediately; if invalid, the process is terminated and transferred to this Certification Center's personnel for manual review and validation.
ACME Automated Process	The ACME Client automatically generates the key pair and CSR, transmitted through a TLS channel compliant with RFC 8555. The ACME Server automatically verifies the signature, Private Key ownership, and domain whitelist compliance. If verification passes, the certificate is

Business Process	Description
	automatically issued; if it fails, the automated process is terminated and transferred to this Certification Center's personnel for manual account configuration.

4.7.1 Circumstance for Certificate Re-Key

In accordance with the provisions of Section 3.3.1.

4.7.2 Who May Request Certification of a New Public Key

Subscribers are authorized to re-key certificates.

4.7.3 Processing Certificate Re-Key Requests

1. Identification and authentication of the Subscriber is performed in accordance with Section 3.3.
2. Certificate issuance is performed in accordance with Section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

In accordance with the provisions of Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

In accordance with the provisions of Section 4.4.

4.7.6 Publication of the Re-Keyed Certificate by the CA

In accordance with the provisions of Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

In accordance with the provisions of Section 4.4.3.

4.8 Certificate Modification

Certificate modification refers to re-issuing a certificate (generating a new certificate serial number) to the Subscriber when the Public Key remains unchanged but the Subscriber identification information recorded in the certificate needs to be modified.

This Certification Center only accepts certificate modification requests from Subscribers within 7 days after certificate issuance. If more than 7 days have passed and the Subscriber's identification information or other information recorded in the certificate needs to be modified, the certificate shall be revoked in accordance with Section 4.9, and a new certificate shall be re-applied for in accordance with Sections 4.1, 4.2, 4.3, and 4.4.

4.9 Certificate Revocation and Suspension

When a revocation situation occurs, the relevant certificate shall be revoked and added to the CRL/OCSP. Revoked certificates must be included in all subsequently published CRL/OCSP records until the certificate expires.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

This Certification Center shall revoke the certificate within 24 hours when any of the following circumstances occur:

1. The Subscriber requests in writing to terminate the use of the certificate.
2. The Subscriber informs that the original certificate application was not authorized.
3. The Private Key associated with the Subscriber's certificate is proven or suspected to have been compromised.
4. The key pair used by the Subscriber is a weak key (e.g., Debian Weak Key).
5. The validation data for the Subscriber's Domain Name or IP address is unreliable.

This Certification Center shall revoke the certificate within 5 days when any of the following circumstances occur:

6. The key used by the Subscriber violates the provisions of Sections 6.1.5 and 6.1.6.
7. The Subscriber's certificate has been misused.
8. The Subscriber has violated the competent authority's laws, the certificate policy, this CP/CPS, or the Subscriber agreement.
9. The Subscriber is no longer permitted to legally use the Domain Name or IP address recorded in the certificate.
10. A Wildcard Domain certificate has been used for a fraudulent domain.
11. The information recorded in the certificate has changed.
12. The certificate was not issued in accordance with the procedures specified in the certificate policy or this CP/CPS.
13. The information recorded in the certificate is inaccurate.
14. This Certification Center's authority to issue certificates has expired, been revoked, or been suspended — unless arrangements have been made to continue maintaining CRL and OCSP services.
15. Items that the certificate policy requires to be revoked.
16. A method is known to exist that can compromise the Subscriber's key, or the key generation method has known weaknesses.
17. The Private Key associated with the Subscriber's certificate has been lost or damaged.
18. Or circumstances for certificate modification as described in Section 4.8.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Root Certification Authority (RCA) shall revoke the certificate within 7 days when any of the following circumstances occur:

1. The Subordinate CA requests revocation in writing.
2. The Subordinate CA informs that the original certificate application was not authorized.
3. The key used by the Subordinate CA violates the provisions of Sections 6.1.5 and 6.1.6.
4. The Subordinate CA's certificate has been misused.
5. The Subordinate CA's certificate was not issued in accordance with the procedures specified in the certificate policy or this CP/CPS.
6. The information recorded in the certificate is inaccurate.
7. The RCA or the Subordinate CA ceases operations and no other Certification Authority has been arranged to take over to provide certificate revocation services.
8. The authority of the RCA or the Subordinate CA to issue certificates has expired, been revoked, or been suspended — unless arrangements have been made to continue maintaining CRL and OCSP services.
9. Items that the certificate policy requires to be revoked.

4.9.2 Who Can Request Revocation

1. The Subscriber.
2. This Certification Center.
3. The competent authority or a court.
4. Persons other than those listed above who suspect that a certificate key has been compromised or have other security concerns may also notify this Certification Center. This Certification Center will proceed with the certificate revocation procedure after confirming the report is valid. For contact information, please refer to Section 1.5.2.

4.9.3 Procedure for Revocation Request

This Certification Center accepts certificate revocation requests 7 x 24. Applicants submit certificate revocation requests in accordance with Section 3.4. The certificate revocation procedure is described below for each business process:

Business Process	Description
Manual Process	Persons authorized to request certificate revocation as defined in Section 4.9.2 submit the certificate revocation request. If the revocation request is submitted by the certificate Subscriber, identification is performed in accordance with Section 3.4. Other certificate revocation requests are investigated based on the revocation reasons defined in Section 4.9.1. After this Certification Center completes identification, the revocation operation is completed within the time limits specified in Section 4.9.1.
Self-Service Process	The Subscriber logs into the Self-Service issuance platform account and submits a certificate revocation request, including the certificate information to be revoked and optionally selecting a Reason Code. The system immediately executes the certificate revocation operation.
ACME Automated Process	The ACME account owner (i.e., the Subscriber) may perform automated certificate revocation through the ACME Client. The request must comply with the RFC 8555 specification, including the certificate information to be revoked and optionally selecting a Reason Code. The ACME Client must send a revocation request message signed by the ACME account Private Key to this Certification Center to ensure the legitimacy and non-repudiation of the request source. Upon receiving the request, this Certification Center will immediately verify the digital signature using the ACME account Public Key. If the authorization is verified, the system will immediately execute the certificate revocation operation.

4.9.4 Revocation Request Grace Period

After the occurrence of a certificate revocation event, the Subscriber shall submit a certificate revocation request within a reasonable period consistent with general business practice. This CP/CPS does not mandate a specific grace period. If key compromise is suspected or confirmed, or other security matters require certificate revocation, the Subscriber shall submit the request within 24 hours.

4.9.5 Time Within Which CA Must Process the Revocation Request

Upon receiving a certificate revocation request from a Subscriber, this Certification Center shall investigate and provide an initial response within 24 hours. In cases requiring revocation, the time from receipt of the request to completion of revocation shall not exceed the time limits specified in Section 4.9.1.1.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties shall, based on their risk, liability, and potential consequences, independently decide whether to check certificate status through CRL or OCSP and determine the query frequency.

If a Relying Party checks certificate status through a CRL issued by this Certification Center, the Relying Party shall verify before use that the CRL was issued by this Certification Center, including verifying the correctness and validity of the CRL's digital signature. Other verification considerations must satisfy the relevant requirements of RFC 5280.

If a Relying Party checks certificate status through OCSP messages provided by this Certification Center, the Relying Party shall verify before use that the OCSP message was issued by this Certification Center's OCSP Responder, including verifying the correctness and validity of the OCSP message's digital signature. Other verification considerations must satisfy the relevant requirements of RFC 6960.

4.9.7 CRL Issuance Frequency

This Certification Center updates and issues a CRL every 24 hours.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

This Certification Center provides OCSP services, supporting OCSP queries via HTTP GET or POST methods. The response messages comply with the specifications of RFC 6960 and include a digital signature on the message.

This Certification Center updates the certificate status information provided by the OCSP service at least every 2 days, with a maximum validity of 4 days. For other related details, please refer to Section 7.3.

4.9.10 On-Line Revocation Checking Requirements

Relying Parties must check the certificate status before deciding to rely on a certificate issued by this Certification Center. If the Relying Party does not use a CRL issued by this Certification Center to check certificate status, the Relying Party must check certificate status through the OCSP service in the manner specified in Section 4.9.9.

For Precertificates that have been uploaded to CT (Certificate Transparency) log servers, if the transaction times out and the certificate is not issued to the Subscriber, this Certification Center shall revoke the Precertificate and add it to the CRL/OCSP. For the update frequency of CRL and OCSP services and other related details, please refer to Sections 4.9.7, 4.9.9, 7.2, and 7.3.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

If key compromise is suspected, the reporter may submit evidentiary information through legitimate channels (refer to Section 1.5.2) to contact the appropriate contact of this Certification Center. This Certification Center accepts the following method to prove suspected key compromise:

- Submit a CSR signed with the suspected compromised key (in standard PKCS#10 format) as proof. The CN of the CSR must be "Proof of Key Compromise for TWCA" for this Certification

Center to verify its authenticity.

When this Certification Center's signing key is compromised, the following procedures shall be followed:

1. Generate a new signing key pair and the corresponding new certificate.
2. Revoke all issued certificates. Use the new signing key to issue a CRL that includes all issued unexpired certificate information (including previously revoked certificates issued before the key compromise).
3. Notify Subscribers.
4. Provide the certificate corresponding to this Certification Center's new signing key.
5. Use the new signing key to issue certificates to Subscribers.

If a Subscriber's key is suspected or confirmed to have been compromised, the Subscriber shall notify this Certification Center to revoke the certificate within 24 hours of learning of the fact.

4.9.13 Circumstances for Suspension

As this Certification Center does not provide certificate suspension services, the following provisions regarding who may request certificate suspension, certificate suspension procedures, and certificate suspension period limitations are not applicable.

If key compromise occurs, the certificate suspension procedure shall not be used; the matter shall be handled in accordance with Section 4.9.12.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Subscribers may check certificate status through the CRL and OCSP services provided by this Certification Center.

The download location of the Certificate Revocation List (CRL) is noted in the cRLDistributionPoints extension field of the certificate.

The revocation information for a revoked certificate is removed from the CRL and OCSP services only after the certificate's validity period has expired.

4.10.2 Service Availability

This Certification Center provides 24x7 certificate status services for Relying Parties to query the status of all unexpired certificates.

Under normal network conditions, the response time for CRL and OCSP services provided by this Certification Center is typically within 10 seconds. For CRL issuance frequency, refer to Section 4.9.7.

This Certification Center provides a 24x7 contact mechanism for reporting significant certificate issues (e.g., certificates applied for fraudulently or issued erroneously). Upon confirmation, the problematic certificates will be revoked, and any illegal incidents will be referred to law enforcement agencies. For the contact window of this Certification Center, refer to Section 1.5.2.

4.10.3 Optional Features

Refer to the provisions of Sections 4.9.9 and 4.9.11.

4.11 End of Subscription

When a certificate issued by this Certification Center expires, is revoked, or this Certification Center ceases operations, the issued certificate becomes invalid.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The Private Key of this Certification Center is not permitted to be escrowed. The Private Key of Subscribers is not prohibited from being escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management and Operational Controls

In addition to complying with the Certificate Policy, the security controls of this Certification Center also comply with the "Network and Certificate System Security Requirements" established by the CA/Browser Forum.

5.1 Physical Controls

5.1.1 Site Location and Construction

The server room of this Certification Center is located within the Company's premises. It meets the facility standards for storing highly important and sensitive information, and incorporates physical security mechanisms including access control, security guards, intrusion detection, and video surveillance to prevent unauthorized access to the equipment of this Certification Center.

5.1.2 Physical Access

The physical access control measures for the server room of this Certification Center are as follows:

- Three levels of identity verification access control (using Smart Cards or fingerprint recognition), of which at least two levels require simultaneous identity authentication of two or more persons before entry is permitted. The facility is equipped with 24-hour CCTV motion-detection surveillance and infrared intrusion alarm systems to record access to the server room and prevent unauthorized entry.
- Backup data related to the Private Keys used in the operations of this Certification Center are securely stored in safes protected by surveillance camera systems. Operational personnel involved in certificate management system operations must have at least two persons present to perform certificate management operations, all under the monitoring of surveillance equipment.
- Equipment such as hardware, software, and Hardware Security Modules (HSMs) are all placed in environments protected by surveillance camera systems, and at least two persons must be present to perform key management-related operations.

5.1.3 Power and Air Conditioning

The server room of this Certification Center is equipped with diesel generators and an Uninterruptible Power Supply (UPS). When the regular power supply system fails, it automatically switches to diesel generator power, with the UPS providing stable power during the switchover process.

The facility has an independent air conditioning system to ensure stable system operation and provide an optimal working environment, with regular maintenance and testing performed.

5.1.4 Water Exposure

The server room of this Certification Center is a sealed building. Apart from internally accessible entry doors, the exterior is entirely a concrete structure, and the floor is fitted with raised flooring, eliminating concerns about water ingress.

5.1.5 Fire Prevention

The server room of this Certification Center is constructed with fire-resistant materials and equipped with fire suppression equipment with a central monitoring system that can automatically activate fire

suppression upon detection of a fire.

5.1.6 Media Storage

The media storage environment of this Certification Center is designed to prevent accidental media damage. It includes equipment and an environment with anti-magnetic and anti-static interference protection for magnetic media. Important data backup media are stored in fire-resistant safes, with one copy of the backup media stored at an Off-site Backup / Disaster Recovery Site with security control measures.

5.1.7 Waste Disposal

When hardware equipment, disk drives, and cryptographic devices used by this Certification Center are decommissioned, any commercially sensitive and confidential information stored therein must undergo secure erasure and destruction, verified by the audit unit, with verification documents retained.

Documents and media containing commercially sensitive and confidential information must undergo secure erasure and destruction during disposal so that the information cannot be recovered or accessed, verified by the audit unit, with verification documents retained.

5.1.8 Off-site Backup

This Certification Center maintains an Off-site Backup / Disaster Recovery Site with backup equipment. When the equipment used in daily operations cannot function normally due to external factors, the backup equipment can provide continuous operational capability for this Certification Center.

Media information and documents required for the operation of this Certification Center are backed up and stored at a highly secure Off-site Backup environment with temperature and humidity controls, anti-magnetic and anti-static interference protection, surveillance camera monitoring, and personnel access requiring authorization.

Backup log files of this Certification Center are all stored at the highly secure Off-site Backup / Disaster Recovery Site.

5.2 Procedural Controls

5.2.1 Trusted Roles

Under the Public Key Infrastructure (PKI) framework, the certificate management operations of this Certification Center must be conducted under rigorous and secure operational procedures. To ensure proper separation of duties and responsibilities, and to ensure that backup arrangements for positions do not jeopardize the overall system security and operational integrity, the Trusted Roles and their division of duties at this Certification Center are as follows:

- **System Administrator** — Responsible for system installation, management operations, and environment parameter configuration.

- **Certificate Officer** — Responsible for certificate issuance and certificate revocation.
- **Auditor** — Responsible for conducting internal audits, reviewing, and maintaining Audit Logs.
- **Operator** — Responsible for routine maintenance operations such as backup, restoration, and website data maintenance.
- **Developer** — Responsible for system design and development.

5.2.2 Number of Persons Required per Task

The personnel requirements for each Trusted Role are as follows:

- System Administrator — at least 2 persons.
- Certificate Officer — at least 2 persons.
- Auditor — at least 1 person.
- Operator — at least 2 persons.
- Developer — at least 1 person.

Before completed code is submitted for integration into the production environment, at least two authorized trusted persons must review and confirm it, ensuring the code meets business logic and security requirements before approval for release.

Before issuing a Subscriber certificate, at least 2 Trusted Role personnel must confirm before Subscriber certificate issuance can be executed.

5.2.3 Identification and Authentication for Each Role

System Administrators, Certificate Officers, Auditors, and Operators who perform certificate management operations at this Certification Center are assigned duties separated by business function and use unique identification codes, Smart Cards, and associated identity verification passwords to achieve identification and authentication of Trusted Roles.

Developers of this Certification Center access source code exclusively through a code version control management platform, integrated with Active Directory (AD) account privilege control mechanisms, with project access privileges assigned according to development tasks.

All operations performed by relevant operational personnel according to business requirements are recorded in detail to ensure auditability of system resource usage and to enable assessment of system security threats and risks.

5.2.4 Roles Requiring Separation of Duties

Role	Certificate Officer	System Administrator	Auditor	Operator	Developer
Certificate Officer	○	X	X	X	X
System Administrator	X	○	X	○	X
Auditor	X	X	○	X	X

Role	Certificate Officer	System Administrator	Auditor	Operator	Developer
Operator	X	○	X	○	X
Developer	X	X	X	X	○

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Operational personnel of this Certification Center must be loyal, trustworthy, and enthusiastic about their work. They shall not hold other concurrent positions that affect certificate operations and shall have no records of legal violations or poor credit.

- Certificate Officers must have at least practical experience in certificate operations, or have passed examinations after receiving certificate-related operational training.
- System Administrators must have at least practical experience in certificate operations and experience in computer system planning and operations management.
- Auditors must have at least professional knowledge in information security or system auditing and experience in independently reviewing operational processes.
- Operators must have at least received training in certificate lifecycle management and system management.
- Developers must have at least the capability of secure code writing and system development.

5.3.2 Background Check Procedures

Working personnel of this Certification Center must undergo an identity background security check by the human resources management department in accordance with background check regulations, followed by a practical experience review by the relevant operations department, before they may assume their positions. Annual reviews of practical experience must be conducted based on the characteristics of each position, serving as the basis for determining the person's suitability for the role or for making job adjustments.

5.3.3 Training Requirements

Operational personnel of this Certification Center receive training appropriate to their duties, covering the hardware and software functions required for system operation, operational procedures, certificate issuance review procedures, security control procedures, Disaster Recovery operation specifications, key management operations, the Certificate Policy and this CP/CPS, and other information security-related operational specifications. When there are changes to the certificate system or new systems are added, appropriate training is also provided.

For hardware, software, application systems, and security management systems related to the certificate management system, this Certification Center has established comprehensive training specifications.

Training on relevant skills is conducted when new personnel are hired or when systems at this Certification Center are changed. Detailed records of training outcomes are maintained and serve as a reference for work delegation of relevant operational personnel.

5.3.4 Retraining Frequency and Requirements

For personnel involved in the operation of the certificate management system, this Certification Center reviews their relevant knowledge and skills for operating the certificate management system at least once per year and provides appropriate training. Training is provided to operational personnel whenever certificate management system functions are updated, new systems are added, or there are advances and updates in Public Key Infrastructure-related knowledge and technology.

5.3.5 Job Rotation Frequency and Sequence

- A System Administrator must have left the original position for at least 1 year before being eligible to transfer to the role of Certificate Officer or Auditor.
- A Certificate Officer must have left the original position for at least 1 year before being eligible to transfer to the role of System Administrator or Auditor.
- An Auditor must have left the original position for at least 1 year before being eligible to transfer to the role of System Administrator or Certificate Officer.
- An Operator must have served for at least 2 years and must have completed relevant training and passed the review before being eligible to transfer to the role of System Administrator, Certificate Officer, or Auditor.
- A Developer must have left the original position for at least 1 year before being eligible to transfer to the role of System Administrator, Certificate Officer, or Auditor.

5.3.6 Sanctions for Unauthorized Actions

If operational personnel involved in the operation of the certificate management system of this Certification Center intentionally or negligently perform operations outside the scope of their duties, regardless of whether it causes security issues for the certificate management system, the matter shall be immediately reported to the supervisory manager and handled in accordance with relevant operational regulations.

5.3.7 Independent Contractor Requirements

If this Certification Center engages outsourced personnel to serve as Operators due to insufficient human resources, this Certification Center must conduct background checks in accordance with the procedures specified in Section 5.3.2, followed by training on job-related knowledge and skills as specified in Section 5.3.3. In addition to signing confidentiality agreements related to the scope of work, such outsourced personnel must comply with relevant operational regulations and legal requirements. The rights and obligations of such outsourced personnel are the same as those of the internal Operators of this Certification Center.

5.3.8 Documentation Supplied to Personnel

To ensure the normal operation of the certificate management system, this Certification Center must provide relevant operational personnel with the following operational documents for system operation, including at minimum:

- Operating documents for hardware, software operating platforms, network systems and website-related operations, and cryptographic system operations.
- Operating documents related to the certificate management system of this Certification Center.
- This CP/CPS, Certificate Policy, and related operational specification documents.
- Internal operational documents of the certificate management system of this Certification Center, such as: system backup and recovery operational documents, off-site Disaster Recovery backup and recovery operational documents, and routine work operational documents.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Each Audit Log entry of this Certification Center, whether recorded automatically or manually, includes the following items:

- Event type.
- Date and time of the event.
- Result of the event (success or failure).
- The entity or person that triggered the event.
- Description of the event content.

The following are the types of audit events recorded by this Certification Center:

Security Audit

- Any changes to important audit parameters, such as audit event types, old and new parameter values, etc.
- Any attempts to delete or modify Audit Log files.

Personnel and Trusted Role Management, Identification and Authentication

- Setup of new roles, whether successful or failed.
- Changes to the maximum tolerance for authentication attempts.
- Maximum number of failed authentication attempts when a user logs into the system.
- Administrator unlocking a locked account.
- Administrator changing the system's authentication mechanism, e.g., from password to biometric.

Key Operation Procedures

- Key generation.
- Key destruction.

Private Key Loading and Storage

- Loading Private Keys into system components.

Addition, Deletion, and Storage of Trusted Public Keys

- Changes to trusted Public Keys, including addition, deletion, and storage.

Private Key Export

- Export of Private Keys (excluding keys intended for single-use or one-time use only).

Certificate Registration

- Certificate registration application process.

Certificate Revocation

- Certificate revocation application process.
- CRL generation records.
- OCSP service signing records.

Approval of Certificate Status Changes

- Approval or rejection of applications for certificate status changes.

Configuration Settings

- Changes to security configuration-related settings.

Account Management

- Adding or removing roles and users.
- Modifying access permissions of user accounts or roles.

Certificate Profile Management

- Changes to certificate profiles.

CRL Profile Management

- Changes to CRL profiles.

System Installation and Significant Operational Events

- Installing the operating system.
- Installing the certificate management system.
- Installing the Hardware Security Module (HSM).
- Removing the Hardware Security Module (HSM).
- Destroying the Hardware Security Module (HSM).
- Starting the system.
- Attempting to log into the certificate management system.

- Receipt of hardware and software.
- Attempting to set a password.
- Attempting to change a password.
- Internal data backup of this Certification Center.
- Internal data restoration of this Certification Center.
- File operations (e.g., creation, renaming, moving, etc.).
- Transmitting any information to the repository.
- Accessing the internal database of this Certification Center.
- Key Compromise.
- Key changeover of this Certification Center.

Changes to This Certification Center's Server Configuration

- Hardware.
- Software.
- Operating system.
- Patches.
- Security profiles.

Physical Access and Site Security

- Personnel entering and exiting the server room of this Certification Center.
- Accessing the servers of this Certification Center.
- Known or suspected violations of physical security regulations.

Anomalous Events

- Software errors.
- Software integrity check failures.
- Receipt of malformed messages.
- Messages routed through non-standard paths.
- Network attacks (suspected or confirmed).
- Equipment failures.
- Power irregularities.
- UPS failures.
- Significant network service or access failures.
- Violations of this CP/CPS.
- System clock resets.

5.4.2 Frequency of Processing Log

This Certification Center reviews the Audit Logs once per month, investigating events that have occurred. The review includes verifying that the Audit Logs have not been tampered with, reviewing all log entries,

and examining any alerts or anomalies, with explanations provided and preventive measures proposed. The results of the Audit Log review are documented.

5.4.3 Retention Period for Audit Log

The relevant Audit Log reports and media data of this Certification Center are retained for at least 7 years and no earlier than 2 years after the related key destruction, certificate expiration, or revocation.

5.4.4 Protection of Audit Log

- Only authorized personnel may read the Audit Logs, and only authorized personnel may back up the Audit Logs.
- Signature or encryption technology is used to preserve current and archived electronic Audit Logs, which are stored on write-once optical discs or other media that cannot alter the Audit Log records.
- Keys used to protect event logs shall not be used for any other purpose.
- Paper and physical Audit Logs are stored in a secure location.

5.4.5 Audit Log Backup Procedures

Electronic Audit Logs are backed up once per month and stored at a backup location outside of this Certification Center.

5.4.6 Audit Collection System

The audit system is built into the certificate management system of this Certification Center. The audit process is activated when the certificate management system starts and is only stopped when the certificate management system is shut down.

If the automated audit system cannot operate normally and the security mechanisms protecting system data integrity and confidentiality are in a high-risk state, this Certification Center will suspend certificate issuance services until the issue is resolved.

5.4.7 Notification to Event-Causing Subject

If an event is recorded by the audit system, the audit system is not required to notify the individual who caused the event that the event has been recorded by the system.

5.4.8 Vulnerability Assessment

The following Vulnerability Assessments are conducted once per year:

- Identify foreseeable internal and external threats that may result in unauthorized access, information disclosure, information misuse, data tampering, or destruction of any certificate data or certificate management processes.

- Assess the likelihood of threats occurring and the potential damage to certificate data and certificate management processes if they occur.
- Assess whether the current applicable information security policies, management procedures, information technology, and other protective measures of this Certification Center are sufficient to defend against threats.

5.5 Records Archival

5.5.1 Types of Records Archived

The Archive Records of this Certification Center include the following types:

- Accreditation-verified data.
- Certificate Practice Statement.
- Subscriber agreements.
- System and equipment configuration settings.
- Content of system or configuration modifications and updates.
- Certificate application data.
- Revocation application data.
- Certificate acceptance confirmation documents.
- Issued or published certificates.
- Records of key changeover.
- Issued or published CRLs.
- Audit Logs.
- Other explanatory materials or applications used to verify and corroborate archived content.
- Documents required by independent auditors.
- Subscriber identification and authentication data.

5.5.2 Retention Period for Archive

The archived data of this Certification Center is retained for at least 7 years and no earlier than 2 years after the related key destruction, certificate expiration, or revocation.

5.5.3 Protection of Archive

Archived data shall not be written to, modified, or deleted. Individual archived data belonging to a Subscriber may be released to that Subscriber or to other institutions permitted by law.

Archived data must have one copy stored at an Off-site Backup / Disaster Recovery Site outside the location of this Certification Center, with security control measures and damage prevention measures for storage media.

5.5.4 Archive Backup Procedures

Key, certificate, transaction data, and other related data are organized, archived, and backed up on a daily, weekly, and monthly basis in accordance with backup and disaster recovery procedures. One copy is stored in a secure environment within the Company, and another copy is stored at a secure Off-site Backup environment. When the certificate system cannot be opened due to an anomaly, the certificate system recovery operation is performed using the preserved backup data in accordance with the system backup and recovery operation manual.

5.5.5 Requirements for Time-Stamping of Records

Archived electronic records (e.g., certificates, CRLs, and Audit Logs) include date and time information, and these records are protected by appropriate digital signatures or cryptographic algorithms that can be used to detect whether the date and time information in the records has been tampered with. However, the date and time information in these electronic records is not electronic timestamp data provided by a neutral third party, but rather the date and time of the computer operating system.

All computer systems of this Certification Center undergo regular time synchronization to ensure the accuracy and reliability of the date and time information in electronic records.

Archived paper records also include date information, and time information when necessary. The date and time records in paper documents shall not be arbitrarily altered; if alteration is necessary, it must be confirmed with the signature of an Auditor.

5.5.6 Archive Collection System

The archived record information related to the operations of this Certification Center is maintained by internal operational personnel of the Company, generated under resource accountability independence and secure control measures. The information preserved by the Audit Log collection system is also generated by internal control systems. Archived records of documents related to the operation of the certificate management system are collected and managed by personnel with the relevant business authority.

5.5.7 Procedures to Obtain and Verify Archive Information

A written application with formal authorization must be obtained before archived data can be accessed. The Auditor is responsible for verifying archived data; paper documents must be verified for the authenticity of the document issuer and date, while electronic files are verified through the digital signature of the archived data or by cryptographic means.

5.6 Key Changeover

To reduce the risk of the signing key of this Certification Center being compromised, the signing key must be renewed periodically.

When the User Certification Authority (UCA) performs key changeover, a new Key Pair is generated and submitted to the Root Certification Authority (RCA) for certificate issuance, then made available for download by Relying Parties in accordance with the provisions of Section 6.1.4.

The key validity period for Subscribers should take into account key length, protection methods, control methods, and other various factors, and must not violate the provisions of Section 6.1.5.

5.6.1 Subscriber Key Changeover

The User Certification Authority (UCA) sets the lifecycle for Subscriber keys to be the same as the lifecycle of certificates issued by the UCA to Subscribers; that is, once the validity period of the Subscriber certificate ends, the Subscriber key immediately becomes invalid and cannot be used.

Before the Subscriber key validity period expires, the Subscriber may generate a new Key Pair and apply to the User Certification Authority (UCA) or Registration Authority for the issuance of a new certificate. Relevant operations are governed by the provisions of Section 3.3.1.

When an old key has security concerns and its validity period has not yet expired, the Subscriber must first apply to the User Certification Authority (UCA) or Registration Authority to revoke the old certificate before generating a new Key Pair and applying for the issuance of a new certificate in accordance with the Registration Authority's operational specifications. Certificate revocation operations are governed by the provisions of Section 4.9.

5.6.2 User Certification Authority (UCA) Key Changeover

The key used by the User Certification Authority (UCA) to issue Subscriber certificates has a validity period equal to the lifecycle of the corresponding certificate, not to exceed 10 years.

When the User Certification Authority (UCA) performs key changeover, a new Key Pair is generated and submitted to the Root Certification Authority (RCA) for certificate issuance, then made available for download by Relying Parties in accordance with the provisions of Section 6.1.4.

When the UCA key validity period expires, a new Key Pair may be generated and submitted to the Root Certification Authority (RCA) for the issuance of a new certificate, with the Registration Authority immediately notified. Upon completion, the new Private Key is used to issue Subscriber certificates, while the old key continues to sign CRLs until the end of the old key's lifecycle.

When the old key of the User Certification Authority (UCA) has security concerns and its validity period has not yet expired, revocation of the old certificate must first be requested from the Root Certification Authority (RCA) before a new Key Pair can be generated and a new certificate issued. Upon completion, the new Private Key is used to issue Subscriber certificates and CRLs, and Subscribers and the Registration Authority are immediately notified. All Subscriber certificates and CRLs previously signed using the old Private Key of the UCA become invalid, and Subscribers must regenerate new Key Pairs and apply to the User Certification Authority (UCA) for the issuance of new certificates.

5.6.3 Root Certification Authority (RCA) Key Changeover

The key used by the Root Certification Authority (RCA) to issue subordinate certificates has a validity period equal to the lifecycle of the corresponding certificate, not to exceed 25 years.

Before the key validity period of the Root Certification Authority (RCA) expires, a new Key Pair and self-signed certificate are generated, and the new self-signed certificate is immediately published, with subordinate Certification Authorities immediately notified. The old key continues to sign CRLs until the end of the old key's lifecycle.

When the Root Certification Authority (RCA) has security concerns about a key whose certificate validity period has not yet expired, the certificate must first be revoked before a new Key Pair and self-signed certificate can be generated, with subordinate Certification Authorities immediately notified. At this point, all subordinate Certification Authority certificates become invalid, and they must regenerate new Key Pairs and apply to the Root Certification Authority (RCA) for the issuance of new certificates.

When the Private Key of the Root Certification Authority (RCA) is compromised, all subordinate Certification Authority certificates shall be revoked, and the subordinate Certification Authorities shall be notified to proceed with revoking all Subscriber certificates and to notify business application systems to cease using certificates issued by the subordinate Certification Authorities.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

5.7.1.1 Incident Response and Disaster Recovery Plan

If the User Certification Authority (UCA) key is compromised or lost (even if it has not yet been confirmed whether compromise is possible), the following procedures must be carried out:

- All Subscribers and the Root Certification Authority (RCA) must be notified as soon as possible via secure email or in writing.
- A new Key Pair is generated in accordance with Section 6.1 and submitted to the Root Certification Authority (RCA) for the issuance of a new certificate.
- All issued certificates are revoked. The new signing key is used to sign the CRL, which includes information on all issued unexpired certificates (including revoked certificates issued before the Key Compromise).
- New certificates are issued to each Subscriber in accordance with the procedures of Section 4.3.
- Incident information is reported and disclosed to Relying Parties and the trust list maintenance organizations of each Root CA.

If the Root Certification Authority (RCA) key is compromised or lost, the following procedures must be carried out:

- All subordinate Certification Authorities must be notified as soon as possible via secure email or in writing to proceed with revoking all Subscriber certificates.

- All issued certificates are revoked.
- A new Key Pair and self-signed certificate are generated in accordance with Section 6.1.
- New certificates are issued to subordinate Certification Authorities.
- Incident information is reported and disclosed to Relying Parties and the trust list maintenance organizations of each Root CA.

This Certification Center must investigate and report to the PMA on the cause of the Key Compromise or loss, and the measures taken to prevent the same situation from recurring.

This Certification Center has established incident response handling procedures and a Disaster Recovery plan, documenting business continuity plans and Disaster Recovery procedures in writing. The content includes notification procedures for software vendors (e.g., browser vendors), Subscribers, and Relying Parties when disasters, security compromises, and operational interruption events occur. These procedures are reviewed or revised annually by this Certification Center.

If this Certification Center issues certificates erroneously or not in accordance with this CP/CPS, the incident will also be disclosed on Bugzilla.

5.7.1.2 Mass Certificate Revocation Plan

This Certification Center has established a mass certificate revocation plan that details the procedures for handling mass certificate revocation events. The content includes "Source Confirmation," "Impact Scope Confirmation," "Internal Notification and Incident Response Team Organization," "Response Actions and Procedures," "Plan Training, Testing, and Continuous Improvement," and "Third-Party Assessment." Annual simulation exercises are conducted, and experiences gained from exercises or actual incidents are incorporated into the plan for continuous improvement and enhancement of response capabilities.

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

This Certification Center has established recovery procedures for computer resources, software, and data that have been damaged, and conducts exercises annually.

If the computer equipment of this Certification Center is damaged or inoperable but the signing key has not been compromised, priority is given to restoring the repository, followed by the rapid rebuilding of certificate issuance, revocation, and management capabilities.

5.7.3 Entity Private Key Compromise Procedures

When a Subscriber's key is suspected of being compromised, the procedures specified in Section 4.9.3 shall be followed.

When a Certification Authority's key is suspected of being compromised, the procedures specified in Section 5.7.1 shall be followed.

5.7.4 Business Continuity Capabilities After a Disaster

In the event of a natural disaster or other disaster where certificate status services cannot be restored within 24 hours, the Off-site Backup / Disaster Recovery Site facilities will be activated, and certificate status services will be restored within 24 hours after activation.

5.8 CA or RA Termination

When this Certification Center terminates its services, it shall comply with the relevant provisions of the Electronic Signatures Act.

When this Certification Center ceases system operations for any reason, the impact on system operations must be minimized, and the relevant certificate operations must be securely transferred to another Certification Authority for continued operation.

Upon normal business termination, or contract termination, or corporate reorganization without security concerns:

- The competent authority shall be notified 30 days before the service termination date.
- Subscribers shall be notified and the repository shall be updated 3 months before the service termination date regarding the service termination and the assumption of related business by another Certification Authority.
- Under an operationally secure environment, the relevant Private Keys and certificates of this Certification Center being terminated shall be transferred to the assuming Certification Authority.
- The Certificate Policy, Certificate Practice Statement, related Certification Authority operational manuals, Subscriber agreements and registration data, Audit Logs, Archive Records, certificate status data, and other documents necessary for business succession shall be transferred to the assuming Certification Authority.
- All relevant Private Keys of this Certification Center shall be completely erased, and a formal announcement shall be made to Subscribers that certificate operations have been transferred to the assuming Certification Authority for continued operation.
- Upon abnormal business termination (court-declared bankruptcy or illegality), this Certification Center must notify Subscribers of the facts as soon as possible and must execute the procedures for normal business termination to minimize the impact.
- When this Certification Center ceases business, the relevant rights and obligations shall also be handled in accordance with the Subscriber agreements.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Certification Center Key Pair:

- This Certification Center develops a key generation script and generates the Key Pair in accordance with the script.
- In accordance with Section 6.2.1, this Certification Center uses a Hardware Security Module (HSM) that meets at least CNS 15135, ISO 19790, FIPS 140-2 Level 3, or FIPS 140-3 Level 3 to generate the Key Pair. The Private Key is generated within the HSM and remains stored therein without being disclosed.
- The key generation process is conducted in the presence of a third-party witness. The entire key generation procedure is recorded on video. After key generation, the witness signs a key generation witness certificate to ensure public trust.

Subscriber Key Pair:

- The Key Pair is generated securely by the Subscriber.
- This Certification Center checks whether the Public Key uploaded by the Subscriber is a duplicate, whether it is a weak key, and whether the key quality has defects. If the key fails the checks, a certificate will not be issued.

6.1.2 Private Key Delivery to Subscriber

The Private Key is generated and securely maintained by the Subscriber; therefore, delivery is not required.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber's Public Key is transmitted to this Certification Center via a PKCS#10 certificate request file. The transmission method shall use a securely protected channel. Verification of possession of the Private Key is completed in the manner described in Section 3.2.1.

6.1.4 CA Public Key Delivery to Relying Parties

This Certification Center shall publish the certificates it issues to the repository for Subscribers and Relying Parties to query and download.

6.1.5 Key Sizes

The RSA Public Key length of this Certification Center is at least 2048 bits, and the bit length must be divisible by 8; the ECC Public Key uses a curve with a security strength of at least P-256.

The RSA Public Key length for Subscribers is at least 2048 bits, and the bit length must be divisible by 8; the ECC Public Key uses a curve with a security strength of at least P-256.

6.1.6 Public Key Parameters Generation and Quality Checking

RSA: This Certification Center uses the RSA algorithm. The prime number generator uses the ANSI X9.31 algorithm to generate the prime numbers required by the RSA algorithm, which ensures that the primes are strong primes. The exponent shall have the following characteristics: an odd number greater than or equal to 3 and between 2^16 + 1 and 2^256 - 1. The modulus shall have the following characteristics: odd, not a prime power, and having no factors smaller than 752.

ECC: This Certification Center uses the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine to ensure the validity of all keys.

This Certification Center performs weak key checks (e.g., Debian Weak Key) on keys generated by itself or by Subscribers. If the key fails the check, it is not permitted for use as a certificate key.

6.1.7 Key Usage Purposes

For certificates issued by this Certification Center, key usage purposes refer to the Key Usage and Extended Key Usage extensions described in Section 7.1.2.

6.1.8 Subscriber Key Generation Equipment

The Key Pair generation device for Subscribers is typically the built-in key generation device of the web server or network equipment.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

This Certification Center uses a Hardware Security Module (HSM) that meets at least CNS 15135, ISO 19790, FIPS 140-2 Level 3, or FIPS 140-3 Level 3 as the protection device for Private Keys, with Multi-person (m-of-n) Control capability.

6.2.2 Private Key (m-of-n) Multi-person Control

The Private Key activation data of this Certification Center is managed through Multi-person (m-of-n) Control using a Secret Sharing method, which is a Perfect Secret form of Secret Sharing that can be used for secure activation, backup, and recovery of Private Keys.

Smart Cards and personal passwords protecting Private Key-related information are managed by personnel with separate independent duties and stored in a secure environment with appropriate security controls.

6.2.3 Private Key Escrow

The Private Keys of this Certification Center are not permitted to be escrowed, nor does this Certification Center provide Private Key escrow services for Subscribers.

6.2.4 Private Key Backup

- The Private Key of this Certification Center is stored in the Hardware Security Module (HSM) and is backed up using the Multi-person (m-of-n) Control method described in Section 6.2.2, with the Private Key encrypted before backup. The encryption key secret sharing information is stored on high-security Smart Cards.
- Smart Cards storing encryption key secret sharing information are kept in a dual-controlled secure environment, sealed and maintained by security control personnel.
- At least 2 copies of the encryption key secret sharing information are retained: one stored at a secure location within this Certification Center, and another stored at a secure Off-site Backup / Disaster Recovery Site.

6.2.5 Private Key Archival

The Private Keys of this Certification Center are not archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The Private Key of this Certification Center is generated and stored within the Hardware Security Module (HSM). Only during key backup recovery can the Private Key be imported into another HSM. Export from the Cryptographic Module is handled in accordance with Section 6.2.4.

6.2.7 Private Key Storage on Cryptographic Module

The Private Key of this Certification Center is stored in encrypted form in a Hardware Security Module (HSM) that meets at least CNS 15135, ISO 19790, FIPS 140-2 Level 3, or FIPS 140-3 Level 3, with Multi-person (m-of-n) Control capability.

6.2.8 Method of Activating Private Key

The Private Key stored in the Cryptographic Module must be activated by 2 or more authorized Certificate Officers after identity authentication. Activation is performed through Smart Card-based authentication of Certificate Officer identity, and the activation procedure controls must comply with the provisions of Section 5.2.

6.2.9 Method of Deactivating Private Key

After the Private Key is activated, it is deactivated by either manually shutting down the Cryptographic Module after identity authentication or by automatically logging out after a specified period of inactivity, to prevent unauthorized use of the Private Key.

6.2.10 Method of Destroying Private Key

When the Private Key usage period of this Certification Center expires, the key is destroyed in the following year in the presence of a third-party witness. The memory locations storing the old Private Key in the Hardware Security Module (HSM) are zeroized to destroy the old Private Key in the HSM.

In addition to destroying the old Private Key in the HSM, backup copies of the old Private Key (three generations retained) are also physically destroyed when the backup expires. However, if the key backup copies must be used for restoration and the restored keys include expired keys, those expired keys are immediately deleted.

6.2.11 Cryptographic Module Rating

The Hardware Security Module (HSM) used by this Certification Center must meet at least CNS 15135, ISO 19790, FIPS 140-2 Level 3, or FIPS 140-3 Level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

When certificates issued by this Certification Center reach the end of their lifecycle, the certificates are archived and the Public Keys are archived simultaneously.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity periods of Public Keys and Private Keys listed below are identical.

- The Key Pair validity period for the Root Certification Authority (RCA) has a maximum of 25 years.
- The Key Pair validity period for the User Certification Authority (UCA) has a maximum of 10 years.
- The Key Pair validity period for Subscribers has a maximum of 200 days. Per BR Section 6.3.2, the maximum Subscriber certificate validity period will be progressively shortened as follows:

Certificate Not Before >=	Certificate Not Before <	Maximum Subscriber Certificate Validity
-	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days

Certificate Not Before >=	Certificate Not Before <	Maximum Subscriber Certificate Validity
March 15, 2027	March 15, 2029	100 days
March 15, 2029	-	47 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data for the signing Private Key is generated individually by multiple Smart Cards, using a Multi-person (m-of-n) Control duty separation mechanism. The activation data in the Smart Cards is accessed by a card reader, and the Personal Identification Number (hereinafter referred to as PIN) of the Smart Card is used for identity authentication to access the activation data.

6.4.2 Activation Data Protection

The activation data is protected by the controlling Smart Card set. The PIN of the Smart Card is maintained by the custodian and shall not be recorded on any media. If the number of failed login attempts exceeds 3, the Smart Card is locked. When a Smart Card is transferred, the new custodian must reset the PIN.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

This Certification Center and related auxiliary systems provide the following security control functions through the operating system, or through a combination of operating system, software, and physical protection measures:

- Identity authentication and multi-factor login.
- Self-defined access control.
- Security audit capabilities.
- Access control restrictions for various certificate services and Trusted Roles.
- Identification and authentication of Trusted Roles and identities.
- Ensuring the security of communications and databases.
- Secure and trusted channels for Trusted Roles and related identity identification.
- Process integrity and security control protection.

6.5.2 Computer Security Rating

The computer system security of the systems used in the operations of this Certification Center shall have passed Common Criteria (CC, ISO/IEC 15408) GPOSPP (General Purpose Operating Systems Protection Profile) validation, or EAL4+ validation, or be approved for use through an internal security assessment.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development of this Certification Center complies with the ISO 27001 standards.

The hardware and software of this Certification Center use only components that comply with the security policy. Hardware devices, network connections, or software components unrelated to operations are not installed. Each use includes a check for malicious code.

6.6.2 Security Management Controls

This Certification Center operates in compliance with the ISO 27001 and WebTrust for CA (AICPA/CICA) standards.

When the software of this Certification Center is installed or updated, it is confirmed that the correct version has been provided by the developer and has not been modified. After system installation, the integrity of the software is verified at each startup.

This Certification Center records and controls changes to system configuration and functionality.

6.6.3 Life Cycle Security Controls

This Certification Center annually reviews whether the current algorithms or keys are at risk of being compromised.

6.7 Network Security Controls

The Root Certification Authority (RCA) certificate system is an off-line, standalone management system that can only be operated manually by authorized operational personnel with the relevant business authority.

The certificate management system of this Certification Center requires authorization before operational personnel with the relevant business authority may perform management operations. When performing management operations, the certificate management system authenticates the identity of the operational personnel, and operations are permitted only after successful authentication.

To prevent network intrusion and sabotage, the hosts of this Certification Center are installed and configured with firewalls, intrusion prevention systems, and antivirus systems to enhance network security, with regular system patch updates and system vulnerability scans performed to strengthen

protection. This Certification Center conducts risk assessments on identified vulnerabilities and ensures that responses and remediation are completed within the timeframes specified in the following table:

Vulnerability Risk Level	Review and Response Deadline	Remediation/Fix Deadline
High	Within 5 business days	Within 30 calendar days
Medium	Within 10 business days	Within 90 calendar days

The hosts and internal databases of this Certification Center are connected only to the internal network and isolated by firewalls. Only internal host connections are permitted, and identity authentication is required to confirm that the person or system accessing the resources is authorized.

The repository is connected to the Internet, providing uninterrupted certificate, CRL, and OCSP query services (except for necessary maintenance or backup situations).

6.8 Time-Stamping

This Certification Center regularly synchronizes time through a trusted time source to ensure the accuracy of the time values for various operations of this Certification Center, including but not limited to the following time values:

- Certificate issuance time.
- Certificate revocation time.
- CRL issuance time.
- OCSP issuance time.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificate serial numbers used by this Certification Center are encoded in a non-sequential, greater-than-zero custom format, containing at least 64 bits of randomness generated by a Cryptographically Secure Pseudorandom Number Generator (CSPRNG).

7.1.1 Version

The certificates of this Certification Center and the certificates issued to Subscribers are X.509 v3, with the following fields (field definitions comply with the RFC 5280 standard):

Field	Description
Version	Fixed as v3
Serial Number	Certificate serial number

Field	Description
Signature Hash Algorithm	The signature hash algorithm used for issuing certificates. This Certification Center supports: sha256WithRSAEncryption, sha384WithRSAEncryption, ECDSAWithSHA256, ECDSAWithSHA384
Signature Value	Signature value generated by the issuer's signing
Issuer	Subject information of the CA corresponding to this certificate
Validity Not Before	Certificate start date
Validity Not After	Certificate end date
Subject	Certificate subject information; see Sections 7.1.4.2 and 7.1.4.3
Public Key	Public Key corresponding to the certificate
Extensions	See Section 7.1.2

7.1.2 Certificate Extensions

The Extensions used by this Certification Center comply with the RFC 5280 standard and the requirements of BR Section 7.1.2.

7.1.2.1 Subscriber Certificates

The Extension settings for Subscriber certificates issued by the User Certification Authority (UCA) are as follows:

Certificate Extension	Used	Description
Authority Key Identifier	○	Uses SHA-1 algorithm
Subject Key Identifier	○	Uses SHA-1 or SHA-256 algorithm
CRL Distribution Points	○	Contains CRL download location
Subject Alternative Name	○	Contains at least one subject information entry (see Section 7.1.4.2.1)
Authority Information Access	○*	Contains CA Issuers (accessMethod=1.3.6.1.5.5.7.48.2) (required), Online Certificate Status Protocol (accessMethod=1.3.6.1.5.5.7.48.1) (optional)

Certificate Extension	Used	Description
Certificate Policies	○	Contains certificatePolicies:policyIdentifier, certificatePolicies:policyQualifiers:policyQualifierId, certificatePolicies:policyQualifiers:qualifier:cPSuri
Basic Constraints	○	cA=false, pathLenConstraint=None
Key Usage	○	digitalSignature (required), keyEncipherment (optional)
Extended Key Usage	○	serverAuth (1.3.6.1.5.5.7.3.1) (required), clientAuth (1.3.6.1.5.5.7.3.2) (optional)
SCT List	○	One or more Signed Certificate Timestamp signature values

* Authority Information Access: Starting from March 15, 2024, the Online Certificate Status Protocol is no longer required information.

7.1.2.2 All Certificates

All other Extensions must comply with the RFC 5280 standard and the requirements of BR Section 7.1.2.11.

7.1.2.3 Application of RFC 5280

Precertificates are not considered certificates that need to comply with RFC 5280.

7.1.3 Algorithm Object Identifiers

7.1.3.1 Key Algorithms

The key identifiers used by this Certification Center when issuing certificates are as follows:

Key Algorithm	Object Identifier (OID)
rsaEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)} (1.2.840.113549.1.1.1)
ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) ecPublicKey(1)} (1.2.840.10045.2.1)

7.1.3.2 Signature Algorithms

The signature algorithm object identifiers used by this Certification Center when issuing certificates are as follows:

Signature Algorithm	Object Identifier (OID)
sha256WithRSAEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} (1.2.840.113549.1.1.11)
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)} (1.2.840.113549.1.1.12)
ECDSAWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} (1.2.840.10045.4.3.2)
ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)} (1.2.840.10045.4.3.3)

7.1.4 Distinguished Name Format

7.1.4.1 Name Encoding

The certificate Subject Distinguished Name and Issuer Distinguished Name of this Certification Center and Subscribers comply with the X.500 Distinguished Name (DN) naming convention. The attribute types of these names comply with the relevant provisions of RFC 5280.

For Subscriber certificates issued by this Certification Center, the Issuer Distinguished Name (Issuer DN) must be encoded identically to the Subject Distinguished Name (Subject DN) of the Issuer's certificate. All CA certificates that have the same Subject DN according to the RFC 5280 DN comparison algorithm must be encoded identically.

7.1.4.2 Subject Information of Subscriber Certificates

For Subscriber certificates issued by this Certification Center, the verification procedures for subject information are conducted in accordance with the requirements of Section 3.2.2 of this CP/CPS, ensuring that all verification procedures are correct prior to issuance.

For Subscriber certificates issued by this Certification Center, each attribute in the subject shall not use incomplete, inapplicable, or default values. Except for the CN attribute in the subject information, no other attributes may contain domain names or IP addresses.

7.1.4.2.1 Subject Alternative Name (SAN)

Subscriber certificates issued by this Certification Center must contain a Subject Alternative Name (SAN) Extension. Its value must be in dNSName or iPAddress form, and shall not use internal names or reserved IPs, and must contain at least one value matching the subject information CN. Per the requirements of RFC 5280, the dNSName content shall not contain underscores ("_").

7.1.4.2.2 Subject Distinguished Name Fields

The Distinguished Name (DN) attributes of Subscriber certificates issued by this Certification Center are shown in the table below. It should also be noted that the SAN of certificates issued by this Certification

Center must contain a value matching the subject information CN; the content of that value is described in Section 7.1.4.2.1.

Subject Name Attribute	Description	SSL Certificate (Used)	EV SSL Certificate (Used)
Common Name (CN)	Domain host identifier name	○	○
Organization (O)	Organization registered name	○	○
GivenName/Surname	Natural person's name	X	X
Street Address	Organization business address	X	○
Locality (L)	City name	○	○
State or Province (S)	State or province name	○	○
Postal Code	Organization postal code	X	○
Country (C)	Country	○	○
Organizational Unit (OU)	Organizational unit name	X	X
Business Category	Organization type	X	○
Jurisdiction of Incorporation Locality Name	City name of the jurisdiction of incorporation	X	○
Jurisdiction of Incorporation State or ProvinceName	State or province name of the jurisdiction of incorporation	X	○
Jurisdiction of Incorporation Country Name	Country name of the jurisdiction of incorporation	X	○
Serial Number	Organization registration number	X	○
Other Subject Attributes	Other subject attributes	X	X

7.1.4.3 Subject Information of CA Certificates

The self-signed certificates issued by the Root Certification Authority (RCA) and the certificates of the User Certification Authority (UCA) are issued in accordance with the certificate policy, ensuring that all subject information is correct prior to issuance.

7.1.4.3.1 Subject Distinguished Name Fields

The Distinguished Names of the User Certification Authority (UCA) certificates are:

SSL UCA

Distinguished Name (DN)
C=TW, O=TAIWAN-CA, OU=Global SSL Sub-CA, CN=TWCA Global SSL Certification Authority
C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority
C=TW, O=TAIWAN-CA, OU=SSL Sub-CA, CN=TWCA SSL Certification Authority
C=TW, O=TAIWAN-CA, CN=TWCA Secure SSL Certification Authority
C=TW, O=TAIWAN-CA, CN=TWCA SSL Certification Authority

EV SSL UCA

Distinguished Name (DN)
C=TW, O=TAIWAN-CA, OU=Global EVSSL Sub-CA, CN=TWCA Global EVSSL Certification Authority
C=TW, O=TAIWAN-CA, OU=EVSSL Sub-CA, CN=TWCA EVSSL Certification Authority
C=TW, O=TAIWAN-CA, CN=TWCA EVSSL Certification Authority

The Distinguished Names of the Root Certification Authority (RCA) certificates are:

Distinguished Name (DN)
C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Root Certification Authority
C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Global Root CA
C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA CYBER Root CA

7.1.5 Name Constraints

The certificates of this Certification Center and the certificates it issues do not use the "Name Constraint" Extension.

7.1.6 Certificate Policy Object Identifier

For certificates issued by this Certification Center, the "Certificate Policy" Extension within the certificate uses the Certificate Policy Object Identifier defined by the certificate policy.

7.1.6.1 Reserved Certificate Policy Object Identifiers

The following are Certificate Policy Object Identifiers reserved by CABF BR:

Object Identifier	Usage
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)	Not used (this Certification Center does not issue DV certificates)

Object Identifier	Usage
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)	Used for SSL CA certificates and SSL Certificates
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)	Not used (this Certification Center does not issue IV certificates)
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1)	Used for EV SSL CA certificates and EV SSL Certificates

7.1.6.2 Root Certification Authority Certificates

The certificates of the Root Certification Authority (RCA) do not contain the Certificate Policy Extension.

7.1.6.3 User Certification Authority Certificates

The certificates of the User Certification Authority (UCA) contain the Certificate Policy Extension and use the following Certificate Policy Object Identifiers:

Certificate Type	Object Identifier
SSL CA Certificate	{ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) SSL(21)} (1.3.6.1.4.1.40869.1.1.21); {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)
EV SSL CA Certificate	{ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) EV(22) class3(3)} (1.3.6.1.4.1.40869.1.1.22.3); {joint-iso-itu-t(2) international-organization(23) ca-browser-forum(140) certificate-policies(1) extended-validation(1)} (2.23.140.1.1)

7.1.6.4 Subscriber Certificates

Subscriber certificates issued by the User Certification Authority (UCA) contain the Certificate Policy Extension and use the following Certificate Policy Object Identifiers:

Certificate Type	Object Identifier
SSL Certificate	{ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) SSL(21)} (1.3.6.1.4.1.40869.1.1.21); {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

Certificate Type	Object Identifier
EV SSL Certificate	{ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) EV(22) class3(3)} (1.3.6.1.4.1.40869.1.1.22.3); {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) extended-validation(1)} (2.23.140.1.1)

7.1.7 Usage of Policy Constraints Extension

Certificates issued by this Certification Center may include the "Policy Constraint" Extension as needed.

7.1.8 Policy Qualifier Syntax and Semantics

Certificates issued by this Certification Center may include "Policy Qualifier" syntax as needed.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

The service URL can be obtained from the CRL Distribution Points Extension in the Subscriber certificate. The frequency at which this Certification Center issues CRLs is specified in Section 4.9.7.

7.2.1 Version

This Certification Center issues CRLs in X.509 v2 format, compliant with RFC 5280, with the following fields:

Field	Description
Version Number	Fixed as v2
Issuer	Subject DN of the issuing CA
Effective Date	CRL issuance time
Next Update	Next issuance time
Signature Hash Algorithm	The signature hash algorithm used for issuing the CRL. This Certification Center supports: sha256WithRSAEncryption, sha384WithRSAEncryption, ECDSAWithSHA256, ECDSAWithSHA384
Revoked Certificates List	List of revoked certificates, including certificate serial number and revocation time
Signature Value	Signature value generated by the issuer's signing

7.2.2 CRL and CRL Entry Extensions

The CRLs issued by this Certification Center contain the following Extensions:

Extension	Description
CRL Number	An incrementing sequential number identifying each generation of CRL
Authority Key Identifier	Identifies the issuing CA
Reason Code	Identifies the reason for certificate revocation (see description below)

The permitted revocation reasons for Subscriber certificates are: Key Compromised, Affiliation Changed, Superseded, Cessation of Operation, Privilege Withdrawn, and Unspecified.

The usage scenarios for each Reason Code are described below:

Reason Code	Description
Key Compromised (1)	The CA obtains evidence that the Private Key has been compromised. The CA is made aware of a demonstrated or proven method that can compromise the Private Key. There is clear evidence that the method of generating the Private Key was flawed. The CA is made aware of a demonstrated or proven method to compute the Private Key from the Public Key (e.g., Debian Weak Key). When anyone (not limited to the Subscriber) requests certificate revocation and can prove current possession of the Private Key (per the proof method specified in the CA's CPS), the CA must revoke all certificates with the same Public Key, not limited to the requesting Subscriber's certificates. When a Subscriber requests certificate revocation but does not prove current possession of the Private Key, the CA may revoke that Subscriber's certificate, but shall not treat this as evidence that the Private Key has been compromised; the CA may choose to block further issuance of certificates with this Public Key.
Affiliation Changed (3)	The Subscriber requests certificate revocation for this reason. The CA reissues a certificate due to a change in subject identity information, and there is no other reason for revocation.
Superseded (4)	The Subscriber requests certificate revocation for this reason. The CA revokes the certificate due to domain validation or compliance issues, and the issue is unrelated to key compromise or privilege withdrawal.
Cessation of Operation (5)	The applicant no longer owns or is no longer authorized to use all domain names in the certificate. The website using the certificate is no longer in operation. The CA is made aware that the domain name or IP in the certificate can no longer be legally used, such as by court order.
Privilege Withdrawn (9)	The CA obtains evidence that the certificate has been misused. The CA is made aware that the Subscriber has violated the Subscriber agreement or terms of use. The CA is made aware that a wildcard certificate has been used for a misleading or fraudulent subdomain. The CA is made aware that information in the certificate has changed. The CA determines or is made aware that information in the certificate is incorrect. The CA is made aware that the certificate application was not authorized.

Reason Code	Description
Unspecified (0)	The reason for revocation does not fall under any of the above circumstances.

The Issuer Distinguished Name (Subject DN) in the CRL's Issuer certificate must be encoded identically to the Issuer DN of the CRL issuer.

7.3 OCSP Profile

The service URL can be obtained from the Authority Information Access Extension of the Subscriber certificate. The OCSP service provided by this Certification Center has the following characteristics:

- The signing certificate used for response messages is prohibited from using the SHA-1 algorithm and must be issued by this Certification Center.
- The signature value of response messages is prohibited from using the SHA-1 algorithm.
- The certificate statuses supported in response messages are: good, revoked, and unknown.
- When a status query request is received for a certificate not issued by this Certification Center, a response with certificate status unknown will be returned.
- For other details, refer to Section 4.9.9.

7.3.1 Version

The Online Certificate Status Protocol (OCSP) version of this Certification Center is 1.0, compliant with RFC 6960. The OCSP response messages issued by this Certification Center contain the following fields:

Field	Description
Version	Fixed as v1
Responder ID	Contains the SHA-1 hash value of the responder certificate's Public Key (SubjectPublicKeyInfo)
Produced At	OCSP response signing time
Certificate Status	This Certification Center supports the following certificate statuses: good, revoked, unknown
Validity Period	The validity period of the OCSP response, including ThisUpdate and NextUpdate times
Signature Hash Algorithm	The signature hash algorithm used for issuing the OCSP response. This Certification Center supports: sha256WithRSAEncryption, sha384WithRSAEncryption, ECDSAWithSHA256, ECDSAWithSHA384
Signature Value	Signature value generated by the OCSP responder signing the OCSP response
Signer Certificate	Certificate of the OCSP responder

7.3.2 OCSP Extensions

The Extensions used in the Online Certificate Status Protocol (OCSP) of this Certification Center comply with the RFC 6960 specification.

8 Compliance Audit

8.1 Frequency or Circumstances of Assessment

This Certification Center conducts external audits at least once per year and internal audits at least once per quarter.

8.2 Identity/Qualifications of Assessor

The audit personnel conducting internal and external audits for this Certification Center must possess at least knowledge of certification authority and information system security auditing, have more than 2 years of audit-related experience or certificate operations experience, and must be familiar with the operational specifications of this CP/CPS, as well as have knowledge and experience in application systems and computer hardware/software systems. If the competent authority has relevant regulations regarding the qualification of audit personnel, those regulations shall prevail.

When conducting external audits, the commissioned audit firm must comply with the requirements of BR Section 8.2 and CCADB Policy Section 5.2 and possess nationally recognized formal audit qualifications or internationally recognized audit credentials to provide fair and objective audit services. When conducting audits, this Certification Center will first verify the qualifications of the audit personnel, and after the audit is completed, the audit report will also list the audit credentials and certifications held by the audit personnel.

8.3 Assessor's Relationship to Assessed Entity

The internal audit personnel conducting audits for this Certification Center have independent and separate responsibilities from the audited units, with no conflicts of interest that could affect the objectivity of the audit, and they perform assessments with an independent, fair, and objective attitude.

External audits of this Certification Center are conducted by commissioned audit firms to audit the operations of this Certification Center.

8.4 Topics Covered by Assessment

The audit covers the following items:

- Whether a Certification Practice Statement and related operational specifications have been established and published, including operational specifications established in accordance with

the Certification Practice Statement.

- Whether certificate management and related operations are performed in accordance with the Certification Practice Statement and related operational specifications, to meet the integrity requirements of certificate services and the security controls of this Certification Center's environment.
- Whether the Certification Practice Statement complies with the requirements of the Certificate Policy.

This Certification Center's audit standards comply with the following:

- WebTrust Principles and Criteria for Certification Authorities -- Version 2.2.2 or later.
- WebTrust Principles and Criteria for Certification Authorities -- Extended Validation TLS -- Version 2.0.1 or later.
- WebTrust Principles and Criteria for Certification Authorities -- TLS Baseline -- Version 2.10 or later.
- WebTrust Principles and Criteria for Certification Authorities -- Network Security -- Version 2.0.5 or later.

8.5 Actions Taken as a Result of Deficiency

After a thorough audit assessment of this Certification Center's operations, if any non-compliance with the Certification Practice Statement is found, the auditor shall itemize the findings according to deficiency severity levels and notify this Certification Center. Upon receiving the incident details, this Certification Center will proactively disclose significant deficiencies on Bugzilla.

This Certification Center must propose corrective and preventive measures for the deficiencies and track subsequent improvement progress.

8.6 Communication of Results

This Certification Center will publish historical WebTrust audit reports in the Repository. The company also displays international certification marks on its official website, and clicking on the mark icon allows viewing of the WebTrust audit report.

8.7 Self-Audits

This Certification Center monitors its compliance with the Certificate Policy and Certification Practice Statement and conducts internal audits at least once per quarter to strictly control service quality, including random sampling of at least 3% of certificates issued during the audit period for internal audit.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance and Renewal Fees

This Certification Center issues certificates to Subscribers and collects certificate fees from the Subscribers. Certificate fees are specified in the certificate application form, certificate quotation, Subscriber agreement, or published on this Certification Center's website.

9.1.2 Certificate Access Fees

No charge.

9.1.3 Revocation or Status Information Access Fees

No charge.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

If a Subscriber applies for a refund after completing the certificate application but before the certificate has been issued, a processing fee of NTD 3,000 will be deducted, and the remainder will be refunded without interest. If the Subscriber applies for a refund after the certificate has been issued, the fees for the months used will be deducted proportionally, and then a processing fee of NTD 3,000 will be deducted, with the remainder refunded without interest.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Regarding risk management related to certification management operations, in addition to earthquake and fire insurance already obtained for buildings and hardware facilities, to diversify business operational risks, a general liability insurance policy of USD 2 million and a professional liability insurance policy of USD 5 million have been obtained.

9.2.2 Other Assets

The financial operations audit related to the certificate business conducted by this Certification Center is regularly performed annually by a fair and objective third-party organization.

9.2.3 Indemnification for Subscribers and Relying Parties

- The verification service items and content provided by this Certification Center are all specified in Section 1.4.1 of this CP/CPS. Content not specified in this CP/CPS is excluded from indemnification liability.
- In processing Subscriber registration data and certificate issuance operations, this Certification Center shall not be liable for damages unless the loss was caused by failure to follow this CP/CPS, the Certificate Policy, and related operational specifications, and is attributable to the negligence of this Certification Center.
- This Certification Center shall not be liable for damages caused to Subscribers due to force majeure events (e.g., earthquakes) or other causes not attributable to this Certification Center (e.g., war).
- If operational personnel of this Certification Center intentionally or negligently fail to follow this CP/CPS, the Certificate Policy, and related operational specifications in performing registration, certificate issuance and revocation operations, or violate relevant legal regulations resulting in damage to Subscribers, this Certification Center shall compensate the Subscriber for damages in accordance with regulations, with the maximum compensation limited as specified in Section 9.8 on limitation of liability.
- During the period after a request to revoke a Subscriber's certificate is submitted by this Certification Center or other authorized parties, until this Certification Center actually publishes the revocation of that Subscriber's certificate (recorded in the CRL), if legal disputes arise from the use of that Subscriber's certificate, this Certification Center shall not be liable for damages if it has performed processing operations in accordance with this CP/CPS and related operational specifications.
- This Certification Center shall not be liable for damages caused by the use of illegally forged or erroneous certificates by Subscribers.
- The limitation period for Subscribers' damage claims shall be governed by relevant laws and regulations.

9.3 Confidential Information

9.3.1 Scope of Confidential Information

Confidential Information includes:

- Private Keys and passwords used for the operations of this Certification Center.
- Key share data controlling the Private Keys of this Certification Center.
- Personal data of the certificate applicant representatives and agents when Subscribers apply for certificates.
- Auditable and traceable records generated or maintained by this Certification Center.
- Audit records and documents generated by audit personnel during the audit process.

- Operations-related documents classified as confidential.

9.3.2 Types of Non-Confidential Information

The Certificate Policy, this CP/CPS, certificates issued by this Certification Center, CRLs issued by this Certification Center, and external audit results are all publicly available information.

9.3.3 Responsibility to Protect Confidential Information

Unless one of the following conditions is met, the Subscriber's basic registration data and identity verification-related data shall never be disclosed to management authorities or any other person:

- As required by laws and regulations and authorized by the management authority through legal procedures.
- When a court or arbitration institution with lawful jurisdiction processes disputes or arbitration arising from certificates and requests through legal procedures.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

This Certification Center operates in accordance with the "Personal Data Protection Act and related regulations" and other relevant government regulations. Specific personal data and privacy management are specified in the certificate application form.

The company obtained the BS 10012 Personal Information Management System certificate in November 2013. The transition to BS 10012:2017 was conducted in July 2018, and the ISO 27701 Privacy Information Management System was simultaneously obtained, which has been continuously maintained as valid to date.

9.4.2 Types of Personal Information Considered Private

As specified in Section 9.4.1.

9.4.3 Types of Information Not Considered Private

No stipulation.

9.4.4 Responsibility to Protect Personal Information

Handled in accordance with relevant laws and regulations.

9.4.5 Notice and Consent to Use Personal Information

Handled in accordance with relevant laws and regulations.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

As specified in Section 9.3.3.

9.4.7 Other Information Disclosure Circumstances

As specified in Section 9.3.3.

9.5 Intellectual Property Rights

- The key pairs and key shares produced by this Certification Center are the intellectual property of the company.
- The certificates and CRLs issued by this Certification Center are the intellectual property of the company.
- The key pairs of Subscribers are the intellectual property of the Subscribers; however, when the Public Key is issued as a certificate by this Certification Center, that certificate is the intellectual property of the company.
- This Certification Center will ensure the accuracy of Subscriber names but does not guarantee the ownership of Intellectual Property Rights recorded in the Subject Distinguished Name of Subscriber certificates.
- The intellectual property of documents written by this Certification Center in the course of performing certificate management operations is owned by the company.
- The Intellectual Property Rights of this CP/CPS are owned by the company.
- This CP/CPS may be freely downloaded from the Repository of this Certification Center.
- This Certification Center shall not bear any legal liability for any consequences arising from improper use of this CP/CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

- This Certification Center must fulfill its responsibility to properly safeguard Subscriber registration data, certificate data, and related certificate operation information, and to prevent Confidential Information from being leaked, misused, tampered with, or used without authorization.
- This Certification Center shall accept Subscriber certificate applications, certificate renewals, and certificate revocation requests in accordance with the Certificate Policy and Certification Practice Statement, verify the correctness and completeness of relevant information sent by Subscribers to this Certification Center, perform certificate issuance and certificate revocation operations, and deliver relevant response messages to Subscribers.

- When issuing Subscriber certificates, this Certification Center must verify the correctness and legality of application documents and Subscriber identity.
- When there are security concerns regarding the Private Key of the User Certification Authority (UCA), the UCA must notify Subscribers and the Root Certification Authority (RCA). When there are security concerns regarding the Private Key of the RCA, the RCA must notify all UCAs.
- When issuing certificates, this Certification Center shall securely deliver the issued certificates to the Repository in accordance with this CP/CPS.
- When revoking Subscriber certificates, this Certification Center shall generate CRLs in accordance with this CP/CPS and securely deliver them to the Repository.
- This Certification Center shall provide certificate application procedures and a Subscriber agreement prior to the Subscriber's certificate application, detailing the operational specifications for certificate application, renewal, revocation, and usage, as well as the relevant rights and obligations.
- The Private Keys used by this Certification Center for issuing certificates and CRLs must be used independently and shall not be shared with other functions. If there are other requirements for message signing and encryption, different Private Keys must be used.
- This Certification Center reviews and warrants the following:
    - Right to use domain or IP address: See Section 3.2.2.
    - Authorization for certificate application: See Section 3.2.2.
    - Accuracy of information: See Section 3.2.2.
    - No misleading information: See Section 3.2.2.
    - Applicant identity: See Section 3.2.2.

9.6.2 RA Representations and Warranties

As specified in Section 9.6.1.

9.6.3 Subscriber Obligations

Subscribers of this Certification Center are legal entities or organizations. Their obligations are as follows:

- When applying for a certificate from this Certification Center, the Subscriber must fully understand and agree to the rights and obligations in the application form and agreement, as well as the content of this CP/CPS and related specifications.
- When there are security concerns regarding the Subscriber's Private Key, such as loss or compromise, or when information related to the Subscriber's certificate has changed, the Subscriber must report to this Certification Center in accordance with the relevant operational procedures.
- When applying for a certificate, the Subscriber must provide truthful and accurate information. When accepting a Subscriber certificate issued by this Certification Center, the Subscriber must

verify the correctness of the certificate content and that the Public Key and Private Key are a matching key pair.

- The Subscriber shall properly generate, safeguard, and use the Private Key, and comply with usage restrictions on keys and certificates.
- If a reason for certificate revocation occurs (such as Private Key data being leaked or lost), the Subscriber shall immediately notify this Certification Center and process the certificate revocation. However, the Subscriber shall bear the risk and liability arising from the use of the certificate before the revocation status has been published.
- If this Certification Center is unable to operate normally due to unforeseen circumstances, the Subscriber shall promptly seek other means to complete legal acts with others, and shall not use the inability of this Certification Center to operate normally as a defense against others.
- Technical personnel or contracted entities installing Subscriber site certificates shall have the capability to replace certificates within 24 hours or 5 days to avoid site operation disruption due to certificate revocation.
- In accordance with Section 4.9.1, when circumstances meeting the grounds for certificate revocation occur, depending on the revocation reason classification, revocation shall be performed within 24 hours (e.g., key compromise) or 5 days (e.g., incorrect certificate content) after the event. Subscribers shall not request an extension of the revocation deadline. This Certification Center will proactively revoke the certificate when the revocation deadline expires without further notice.

9.6.4 Relying Party Obligations

- Relying Parties shall obtain the User Certification Authority (UCA) and the Root Certification Authority (RCA) self-signed certificates in accordance with this CP/CPS.
- Relying Parties shall use the UCA certificate and the RCA self-signed certificate to establish and verify the certificate chain, to determine whether to trust Subscriber certificates.
- When verifying certificates, Relying Parties shall use the RCA self-signed certificate to verify whether the digital signature of the UCA certificate was signed by the RCA's Private Key, and verify through the CRL whether the certificate has been revoked.
- When verifying Subscriber certificates, Relying Parties shall use the UCA certificate to verify whether the digital signature of the Subscriber certificate was signed by the UCA's Private Key, and verify through the CRL or OCSP service whether the certificate has been revoked.
- When using CRLs issued by this Certification Center, the Relying Party shall first verify the digital signature and check the Next Update time recorded in the CRL. If the Next Update time has passed, the latest CRL should be obtained. When using the OCSP service, the digital signature of the OCSP response should first be verified.
- Relying Parties shall select a secure computing environment and trustworthy applications. If user rights are compromised due to factors inherent in the computing environment or applications, the Relying Party shall bear the responsibility.

- If this Certification Center is unable to operate normally due to unforeseen circumstances, Relying Parties shall promptly seek other means to complete legal acts with others, and shall not use the inability of this Certification Center to operate normally as a defense against others.
- By accepting the use of certificates issued by this Certification Center, the Relying Party acknowledges understanding and agreement with the terms regarding the legal liability of this Certification Center, and shall rely on the certificate within the scope specified in this CP/CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

- In processing Subscriber registration data and certificate issuance operations, this Certification Center shall not be liable for damages unless it has failed to comply with this CP/CPS, violated relevant laws and regulations, or negligence is attributable to this Certification Center.
- This Certification Center shall not be liable for damages to Subscribers and Relying Parties caused by force majeure events (e.g., earthquakes) or other causes not attributable to this Certification Center (e.g., war).
- If this Certification Center fails to properly safeguard the Subscriber's registration and certificate-related Confidential Information, resulting in information being leaked, misused, tampered with, or used without authorization, causing damage to third parties, this Certification Center shall be liable for damages.
- After receiving a certificate revocation request, this Certification Center shall investigate and provide a preliminary response within 24 hours, and the time from receipt of the request to completion of revocation shall not exceed the timeframe specified in Section 4.9.1.1. After the certificate revocation operation is completed, the Certificate Revocation List (CRL) shall be issued and published in the Repository at the frequency specified in Section 4.9.7. Before the certificate revocation status is published, the Subscriber shall take appropriate action to minimize the impact on Relying Parties and bear all liability arising from the use of the certificate. For revocation operational specifications, please refer to Section 4.9.

9.8 Limitations of Liability

When Subscribers and Relying Parties suffer damage events arising from the issuance or use of certificates, the liability for damages that this Certification Center shall bear is limited to the scope defined by relevant laws and regulations, the Subscriber agreement, or the company's insurance liability limit.

9.9 Indemnities

As specified in Section 9.2.1.

9.10 Term and Termination

9.10.1 Term

This CP/CPS becomes effective upon approval by the competent authority in accordance with the Electronic Signatures Act and publication in the Repository of this Certification Center.

9.10.2 Termination

Upon approval and publication of a new version of this CP/CPS by the competent authority, the current version is terminated.

9.10.3 Effect of Termination and Survival

The effectiveness of this CP/CPS is maintained until the last certificate issued in compliance with this CP/CPS expires or is revoked.

9.11 Individual Notices and Communications with Participants

This Certification Center will establish communication channels with Subscribers by appropriate means, including but not limited to the following: telephone, fax, or email.

9.12 Amendments

9.12.1 Procedure for Amendment

- The responsible management unit for this CP/CPS is the Policy Management Authority (PMA), which updates this CP/CPS at least once per year. Revision methods include revisions through supplementary documents or direct revision of the content of this CP/CPS.
- If the Certificate Policy is revised or the object identifier is changed, this CP/CPS will be revised accordingly.
- If changes are required due to changes in legal regulations, updates to international standards (e.g., BR), or other factors, this CP/CPS will also be revised accordingly.
- After the revision of this CP/CPS is reviewed and approved by the competent authority, it will be published in the Repository as specified in Chapter 2.

9.12.2 Notification Mechanism and Period

- For suggestions to update this CP/CPS, please mail or email the detailed suggestion documents to the contact point in Section 1.5.2, to be reviewed by the PMA.
- After the revision of this CP/CPS is reviewed and approved by the competent authority, it will be published in the Repository of this Certification Center for download.

- Unless otherwise specified, this Certification Center uses the method specified in Section 9.11 as the amendment notification mechanism with Subscribers.

9.12.3 Circumstances Under Which OID Must Be Changed

The Certificate Policy Object Identifiers referenced in this CP/CPS will not be changed when the content of this CP/CPS is amended; only the version identification code of this CP/CPS will be incremented.

9.13 Dispute Resolution Procedures

If Subscribers have disputes regarding the services of this Certification Center or the use of certificates issued by it, the following provisions apply:

- The disputing parties shall, in good faith and through reasonable means, endeavor to resolve the dispute through negotiation.
- If the disputing parties are unable to reasonably resolve the dispute through negotiation within 30 days, they must appoint a competent and impartial third-party mediator to mediate and resolve the dispute.
- If the disputing parties are unable to agree on the mediator's negotiation and ruling within 60 days, both parties agree that the Taipei District Court shall be the court of first instance jurisdiction.
- The allocation of costs incurred during dispute negotiation and litigation proceedings shall be handled in accordance with the negotiation or relevant legal regulations.
- If a cross-border or cross-regional dispute cannot be resolved by the above methods, it must be handled in accordance with the relevant cross-border or cross-regional dispute arbitration regulations.

9.14 Governing Law

The content of this CP/CPS and the execution and interpretation of the related business of this Certification Center shall comply with the relevant laws and regulations of the competent authority and the relevant laws of this country.

9.15 Compliance with Applicable Law

- This CP/CPS and this Certification Center shall comply with the provisions of the Electronic Signatures Act and its enforcement rules of this country, and shall not conflict with the laws of this country.
- This Certification Center also complies with the latest versions of the BR and EVG requirements. If this CP/CPS is inconsistent with the requirements of the above specifications, the above specifications shall prevail. If the above specifications conflict with the laws of this

country, the laws of this country shall prevail, and this Certification Center shall raise an objection with the CA/Browser Forum.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If certain provisions of this CP/CPS are inapplicable and must be revised, the remaining provisions shall remain effective and unaffected by the inapplicable provision, until a new version of this CP/CPS is updated and published.

When the legal requirements of this country conflict with the BR or EVG, this Certification Center will adjust this CP/CPS to comply with the legal requirements of this country, list the relevant legal provisions in this section, and promptly notify the CA/Browser Forum.

Updates to this CP/CPS shall be handled in accordance with Section 9.12.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

This Certification Center shall not be liable for damages due to force majeure events (e.g., earthquakes) or other causes not attributable to this Certification Center (e.g., war).

9.17 Other Provisions

No stipulation.

Appendix I: Glossary

Internet Many different computer networks interconnected through standard communication protocols, enabling the exchange of information with each other.

(Electronic) Message Refers to text, sound, images, symbols, or other data produced in electronic, magnetic, or other forms that cannot be directly perceived by human senses, sufficient to represent the

intended meaning, for the purpose of electronic processing.

RSA Algorithm An asymmetric encryption algorithm proposed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. Its security strength is based on the difficulty of factoring large numbers into prime factors.

Elliptic Curve Cryptography (ECC) A public key encryption algorithm based on elliptic curve mathematics, proposed by Neal Koblitz and Victor Miller in 1985. Its security strength is based on the difficulty of solving the elliptic curve discrete logarithm problem.

ECC P-256 Curve An elliptic curve standard defined by NIST in FIPS 186-3, which defines the elliptic curve parameters p, a, b, G, n, h, where the x and y coordinates of the base point G are each 256 bits in length.

Electronic Signature Refers to data messages existing in electronic form, attached to electronic documents that can be used to identify and confirm the identity of the signer of electronic documents, and messages generated by the signer using digital, voice, fingerprint, or other biometric-optical technology characteristics. It is attached to electronic messages and has the same effect as a signature, which can be used to identify and confirm the identity of the signer of electronic documents and to verify the integrity of the signed message.

Encrypt/Encipher Refers to using mathematical algorithms or other methods to scramble electronic documents to ensure the security of data transmission.

Decrypt/Decipher Restoring messages that have been encrypted and rendered unrecognizable to a form that is recognizable and meaningful using relevant mathematical algorithms or other methods.

Digital Signature A type of electronic signature that uses an asymmetric cryptosystem and a hash function to compress a digital message of a certain length and then encrypt it with the signer's Private Key. The corresponding Public Key can verify this encrypted digital message, forming data that can identify the signer's identity and the authenticity of the electronic document.

Private Key Refers to a set of paired 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.

Public Key In the digital signature of an asymmetric cryptosystem, refers to a set of paired digital data used to create and verify digital signatures that is publicly disclosed. It can be used to verify the correctness of message data signed by the signer. When performing message confidentiality functions, it can encrypt transmitted messages.

Public Key Certificate or Certificate A digitally recorded entry issued by a certification authority using a computer as its 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 prove that they possess a matching pair of Public Key and Private Key.

Certification Authority (CA) An organization that provides digital signature creation and electronic authentication services. It is an entity that, from a fair and objective position, verifies the correctness of the

certificate applicant's identity information and the relevance and legality between the Public Key and Private Key to be verified, and issues Public Key certificates accordingly.

Certification Practice Statement (CPS) The operational specifications and application procedures published by a certification authority to its service recipients regarding certificate issuance, revocation, and inquiry management, including the Public Key architecture and security mechanisms for certificate operations, operational specifications and procedures, security mechanisms implemented in the certification authority's hardware and software, authority management, and related specifications.

Asymmetric Cryptosystem A mathematical algorithm using a computer as its medium 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 the signed messages. The Public Key can also be used to encrypt messages, and the corresponding Private Key is used to decrypt the encrypted messages.

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

Automated Certificate Management Environment (ACME) A communication protocol used to automate certificate-related management operations (e.g., certificate applications) between a Certification Authority (CA) and its client web servers, allowing users to automatically deploy public key infrastructure at extremely low cost. The protocol primarily transmits formatted JSON messages over HTTPS. The relevant standard is defined in RFC 8555.

Certificate Signing Request (CSR) An encoded file that allows certificate applicants to transmit Public Keys and certificate-related information (e.g., domain names) to a certification authority for certificate issuance through a standardized method. The file can concretely prove that the applicant is the owner of the Private Key.

Issue a Certificate Refers to the certification authority, in accordance with the Certification Practice Statement, verifying the identity qualifications and related documents of the Public Key certificate applicant, verifying the pairing relationship between the Public Key and Private Key, and then issuing a Public Key certificate or other certificates.

Public Suffix List (PSL) A public resource created by Mozilla, located at https://publicsuffix.org/. The list consists of two parts: one is the TLD (Top Level Domain) list provided by ICANN, and the other is the PRIVATE list provided by individuals or organizations.

Punycode A way of representing Unicode and ASCII with a limited character set. For example, the Chinese characters for "Taiwan" would be encoded as "xn--kpry57d". The purpose of Punycode is to enable multilingual domain names to be encoded as ASCII within the framework of internationalized domain name labels.

Bugzilla A web-based bug tracking management application maintained by Mozilla. When a CA has a significant deficiency, it must be reported here. Located at https://bugzilla.mozilla.org/home.

Internal Name Refers to a domain host name that cannot be resolved through the public Domain Name System (Public DNS).

Reserved IP In the Internet addressing structure, IP addresses reserved for special purposes by the IETF (Internet Engineering Task Force) and IANA (Internet Assigned Numbers Authority). They can be queried at the following URLs: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

Certificate Transparency (CT) Defined in RFC 6962, the purpose is to monitor certificates issued by CAs. By having CAs upload certificates to public servers (Log servers), Certificate Transparency allows website users and domain owners to identify improperly or maliciously issued certificates, and also to monitor improper CA operational behavior.

Precertificate Defined in RFC 6962, a special type of certificate in CT, used for auditing and verifying CA issuance records. This certificate must be issued in advance before the actual certificate is issued to the Subscriber, and uploaded to the CT log server to obtain SCTs (Signed Certificate Timestamps). The actual certificate issued to the Subscriber will contain these SCTs to prove that it has been successfully uploaded to the CT log server.

Certificate Authority Authorization (CAA) A DNS resource record that allows website owners to specify which CAs are authorized to issue TLS certificates for their domain. By setting CAA records, website administrators can restrict certificate issuance authority, effectively preventing unauthorized CAs from accidentally or maliciously issuing certificates for their domain, thereby enhancing domain certificate security.

Multi-Perspective Issuance Corroboration (MPIC) Multi-perspective issuance corroboration requires CAs, before issuing certificates, to cross-verify DNS records and domain validation results from multiple geographically distributed verification nodes to reduce the risk of erroneous validation caused by BGP hijacking, DNS poisoning, or regional network attacks. In the MPIC architecture, the verification process includes two types of perspectives:

- **Primary Perspective**: Executed by the CA's primary verification node, responsible for obtaining basic verification data such as DNS, CAA, HTTP-01, or TLS-ALPN-01, serving as a baseline for subsequent comparison. The primary perspective is mainly used to confirm whether the applicant has basic and normally observable verification configurations.
- **Remote Perspective**: Executed by nodes distributed in geographic regions different from the primary perspective, with different network paths. These nodes must be able to obtain verification information consistent with the primary perspective to confirm that the domain configuration is consistent globally, and to rule out routing or DNS spoofing that only occurs near the CA's primary perspective.

The CA may consider the domain validation valid and issue a certificate only when the primary perspective and all remote perspectives obtain consistent results. If any perspective observes an inconsistency, the validation is deemed to have failed.

Common CA Database (CCADB) A common CA database jointly maintained by major browser vendors such as Google, Apple, Microsoft, and Mozilla, used to centrally manage and track global CA audit

reports, policy documents, and root certificate information. It is a key management platform for ensuring that certificates can be trusted by major systems.

Appendix II: Acronyms and Abbreviations

Acronym	Full Name
ACME	Automated Certificate Management Environment
ANSI	American National Standard Institute
BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
CA	Certification Authority
CAA	Certificate Authority Authorization
CABF	CA/Browser Forum
CC	Common Criteria
CCADB	Common CA Database
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DNSSEC	Domain Name System Security Extensions
ECC	Elliptic Curve Cryptography
EVG	Guidelines for the Issuance and Management of Extended Validation Certificates
EVSSL	Extended Validation SSL
FIPS	Federal Information Processing Standard
IDNs	Internationalized Domain Names
ISO/IEC	The International Organization for Standardization/The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
MPIC	Multi-Perspective Issuance Corroboration

Acronym	Full Name
MRSP	Mozilla Root Store Policy
OCSP	Online Certificates Status Protocol
OID	Object Identifier
PMA	Policy Management Authority
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certification Authority
RSA	Rivest, Shamir, Adleman (Encryption Algorithm)
SAN	Subject Alternative Name
SSL	Secure Socket Layer
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location