Taiwan-CA Inc. CYBER Certification Authority Certification Practices Statement (TWCA CYBER CA CPS)

(Version 1.1)

Effective Date: 2024/02/29

Revision Record

Version	Effective	Released by	Description
1.0	2023/06/30	TWCA PMA	First release.
1.1	2024/02/29	TWCA PMA	Modify 7.1.2.2, 7.1.2.3 and 7.1.4.3.1.

Executive Summary

The major items of the Certification Practices Statement (CPS) for CYBER Certification Authority (CYBER CA) of TAIWAN-CA INC. (TWCA) are as follows:

1. Certificates to Issue
    - TWCA CYBER CA (this CA) issues certificates, including SSL certificates and EVSSL certificates to the Internet hosts of subscribers for Internet host validation. Unless specified, the “Subscriber Certificate” referred to in this CPS include the above two types of certificates.
    - Types of certificates and Applicability

Certificate Types	Applicability
EVSSL Certificate	It is used to protect online communication security and reduce the risk of malicious interception or tampering. It is suitable for network environments that require a very high level of security, such as financial transaction websites in the Internet environment.
SSL Certificate [note 1]	It is used to protect online communication security and reduce the risk of malicious interception or tampering. It is suitable for network environments that require a high level of security, such as e-commerce websites in the Internet environment.

[note 1]: There are four levels of TLS/SSL certificates defined internationally: from high to low are EV (Extended-Validation), OV (Organization-Validated), DV (Domain-Validated), IV (Individual-Validated). The SSL certificates issued by this CA are OV-Level certificates, the EVSSL certificates are EV-Level certificates. This CA does not issue DV-Level certificates and IV-Level certificates.

- Level of Assurance
  This CA operates according to Assurance Level 4 specified in the TWCA PKI CP and issues Level 3 certificates specified in the CP to certificate subscribers.

The subscriber certificates issued by this CA pursuant to this CPS are designed for organizations (subscribers) that have been approved in the “Organization Authentication procedures” and “Hostname Validation Procedures” by this CA to validate their organization and possession of the corresponding hostname. The certificate can be used to verify the mutual trust relationship between this CA and the Internet host when verifying the certificate of an Internet host with the pubic key of this CA. By verifying the authenticity of the digital signature can validate if the certificate of that Internet host is issued by this CA, and the identity information specified in the certificate is valid and has been approved by the initial identity validation procedure of the RA of this CA.

2. Legal Liabilities and Important Matters
   - When a subscriber needs to revoke a certificate under any of the circumstances of revocation specified in this CPS (e.g. private key information leakage or private key loss), the subscriber should notify this CA immediately and apply for certificate revocation. However, the subscriber shall be liable to the risks and responsibilities as a result of using such certificate prior to the publication of CRLs.
   - This CA assumes no responsibility for indemnifying any damages, if any, arising from or in connection with the processing of registration data and certificate issuance of subscribers; except for failure to follow this CPS or violation of relevant laws and regulations or intention or negligence attributed to this CA.
   - This CA also assumes no responsible for indemnifying any damages, if any, arising from or in connection with damage or loss caused to subscribers as a result of an act of God (e.g. earthquake) and/or events out of the reasonable control of this CA (e.g. war).
   - This CA shall be liable to indemnify the damages, if any, arising from or in connection with the damage caused to a third party from the leakage, marauding, interpolation or unintended use of the registration and/or certificate data of subscribers as a result of the failure to keep such data in custody with due faith and due care of this CA.

- After receiving a request of certificate revocation, this CA should investigate and preliminarily respond to the subscriber within 24 hours. In any case of requiring revocation, the timeframe from notice to revocation shall not exceed that stated in Section 4.9.1.1. After finish revoking the requested certificate, this CA should issue and complete publishing the CRL to the repository within 24 hours from revocation. Prior to the publication of the status of certificate revocation, subscribers shall take actions appropriate to minimize the effect on the relying parties of their certificates, and shall be fully liable for the consequences of the use of such certificates. See Section 4.9 for revocation practices.
- When damages arising from or connection with the issuance or use of certificates occurs between this CA and subscribers, both parties shall indemnify such damages, provided that the amount must not exceed the upper limit specified in the relevant laws and regulations or the agreement.
- When accepting the use of the certificates issued by this CA, the relying party is considered as accepting the legal terms of this CA and shall trust such certificates within the scope specified in this CPS.

3. Other Important Matters
    - When subscribers lost or have security doubts (e.g. being cracked) of their private keys, or when there is a change of relevant information, subscribers shall immediately report to this CA.
    - Subscribers shall properly generate, retain and use their private keys, and shall follow the limitations of certificate usage.
    - When applying for a certificate, subscribers shall provide full and accurate information. When receiving the certificate issued by this CA, subscribers shall check the correctness of information contained in the certificate, and the public key and private key are a key pair.
    - When verifying a certificate, the relying party shall verify the digital signature of the certificate of this UCA perform with the self-signed certificate of the root certification authority (RCA) and verify if the digital signature of the subscriber certificate is issued by the private key of this CA with the certificate of this UCA. The relying party shall also verify if the certificate has been revoked from the CRL.
    - When using the CRL issued by this CA, the relying party shall first verify the digital signature to ascertain if the CRL is valid.
    - This CA shall conduct internal audits at least once a quarter and external audits at least once a year. Please refer to “8. Compliance Audit and Other Assessments” for details concerning the operating specifications of these audits.

1. Introduction

1.1 Overview

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

The TWCA CYBER Certification Authority Certification Practices Statement (this CPS) is established in accordance with the TWCA PKI Certification Policy (CP). The aim of this CPS is to specify how the CYBER Certification Authority (this CA) issues and manages certificates by following the CP.

Except for national laws, this CA complies with Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (BR) and the Guidelines for the Issuance and Management of Extended Validation Certificates (EVG) formulated by CA/Browser Forum which published at http://www.cabforum.org.

In order to build a secure and reliable network environment where no fabrication, alteration and/or theft of data during network transfer is assured, and to reliably validate the name of Internet hosts and the identity of organizations possessing these hosts for the relying party to identify, TWCA has established the TWCA Public Key Infrastructure (TWCA PKI) and implemented the Root Certification Authority (RCA) as the trust anchor to issue certificates to the User Certification Authority (UCA) which further issues certificates to subscribers.

1.2 Document Name and Identification

The name of this document is “Taiwan-CA Inc. CYBER Certification Authority Certification Practices Statement”. Please refer to Section 7.1.6 for the types of certificates and their corresponding object identifier values.

1.2.1 Revisions

This CPS complies with the current version of BR and EVG. TWCA regularly reviews these requirements and revises this CPS at least once a year. If there is a discrepancy between this CPS and these requirements or the laws and regulations of this country, TWCA will revise and notify the CA/Browser Forum of the relevant information. For the previous version change records, please refer to the Section “Revision Record” of this CPS.

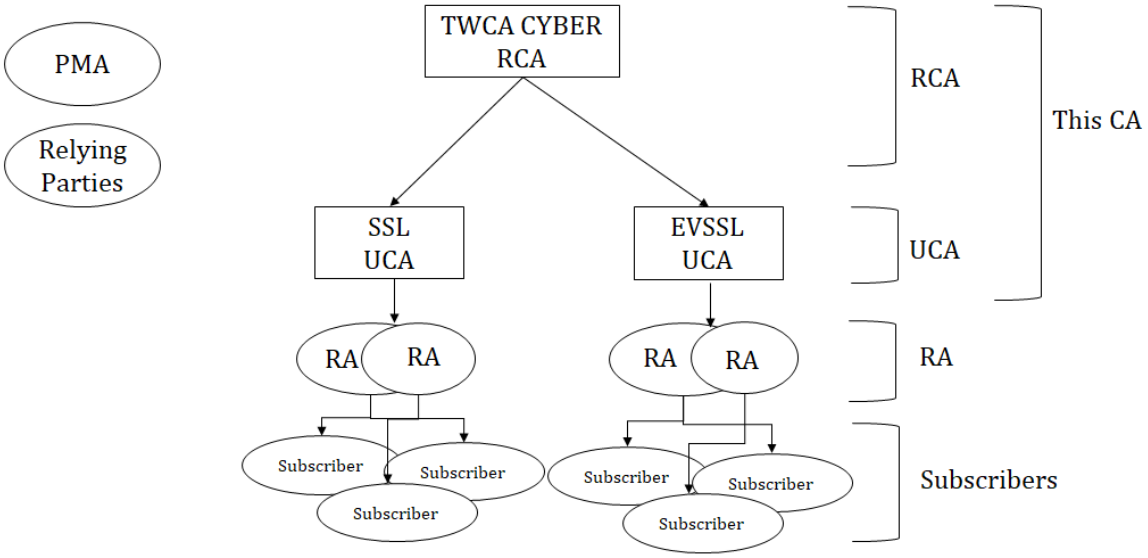
1.3 PKI Participants and Applicability

This CA includes the following members:

1. Certification Authority (CA);
2. Registration Authority (RA);
3. Subscriber;
4. Relying Party; and

5. and Policy Management Authority (PMA).

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



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

1.3.1 Certification Authority (CA)

1.3.1.1 Root Certification Authority (RCA)

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

1. to issue and manage the certificates issued to UCA, prohibited to issue subscriber certificates;
2. to manage and publish certificates and Certificates Revocation Lists (CRLs) in the repository;
3. to provide Online Certificate Status Protocol (OCSP) repository;
4. to maintain the stability and operations of the repository; and
5. to build an independent, safely controlled operating environment, the operation of generating public key, issuing certificates for UCA shall be performed by two or more authorized personnel. When the self-signed certificate of the RCA is generated or updated, it must be delivered to the user by the fastest and appropriate channel or notified to the RCA for request.

1.3.1.2 User Certification Authority (UCA)

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

1. to issue and manage subscriber certificates;
2. to manage and publish subscriber certificates and CRLs of subscriber certificates in the repository;
3. provide OCSP repository; and
4. to maintain the stability and operations of the repository.

1.3.1.3 Policy Management Authority (PMA)

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

1. CP;
2. CPS; and
3. SOP.

1.3.2 Registration Authority (RA)

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

This CA sets up the RA by itself and not delegate to a third party as RA.

1.3.3 Subscribers

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

A subscriber of this CA shall be an organization applying for certificates.

1.3.4 Relying Parties

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

Based on the identify information specified in the subscriber certificate, the relying party identifies the name of the Internet host and the information of its corresponding organization (subscriber).

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

1.3.5 Other Participants

Not specified.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The assurance level of certificates issued by this CA is Level 3. They are used for website authentication and information security control. The types of certificates and their applicability are as follows:

Certificate Types	Applicability
EVSSL Certificate	It is used to protect online communication security and reduce the risk of malicious interception or tampering. It is suitable for network environments that require a very high level of security, such as financial transaction websites in the Internet environment.
SSL Certificate [note 1]	It is used to protect online communication security and reduce the risk of malicious interception or tampering. It is suitable for network environments that require a high level of security, such as e-commerce websites in the Internet environment.

[note 1]: There are four levels of TLS/SSL certificates defined internationally: from high to low are EV (Extended-Validation), OV (Organization-Validated), DV (Domain-Validated), IV (Individual-Validated). The SSL certificates issued by this CA are OV-Level certificates, the EVSSL certificates are EV-Level certificates. This CA does not issue DV-Level certificates and IV-Level certificates. [note 2]: Intermediate level of assurance, providing advanced identification, high confidence in the subscriber’s identity. It is suitable for use in a more dangerous network environment where malicious users may intercept or tamper with information.

The certificates issued by this CA pursuant to this CPS are designed for organizations (subscribers) that have been approved in the “Organization Authentication Procedure” and “Hostname Validation Procedure” by this CA to validate their organization and possession of the corresponding hostname.

The procedures are as follows:

1. Organization Authentication Procedure

   When authenticating the identity of an organization, documents issued by the competent authorities or other documents proven the existence of such organization shall be verified. Also, the identity of its statutory representative shall be authenticated.

   Application documents can be delivered either over the counter or by mail. And use the application documents submitted by the applicant to query the third-party public information or other certified information to confirm that the content of the application documents is consistent with the certified content. See Section 3.2.2.1 for details.

2. Hostname Validation Procedure

    - Domain Validation: Must pass at least one validation method defined in “Section 3.2.2.4: Validation of Domain Authorization or Control”.
    - IP Address Authentication: Must pass at least one validation method defined in “Section 3.2.2.5: Authentication for an IP Address”.
3. Procedure for Authenticating Individuals (natural persons)

   Not applicable to natural person.

1.4.2 Prohibited Certificate Uses

Except for the scope specified in Section 1.4.1, the certificates issued by this CA are prohibited from being used for the following purposes:

1. eavesdropping or intercepting third-party communications;
2. may cause physical or mental injuries to human beings;
3. may cause severe damage to social and public interest; or
4. in applications and/or business prohibited or eliminated in the Electronic Signatures Act or other relevant laws and regulations or by the competent authorities of respective business.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

1.5.2 Contact Person

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

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

1.5.3 Person Determining CPS Suitability for the Policy

PMA approves the suitability of this CPS established by this CA.

1.5.4 CPS Approval Procedures

The CPS established by this CA shall be approved by PMA prior to publication and issuing certificates.

1.6 Definitions and Acronyms

Defined in Appendix 2.

2. Publication and Repository

2.1 Repositories

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

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

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

2.2 Publication of Information

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

1. CPS;
2. CA certificate and related information;
3. Certificates issued;
4. CRLs;
5. OCSP; and
6. Test web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. Locations are published in the repository.

2.3 Time of Frequency of Publication

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

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

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

2.4 Access Controls on Repositories

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

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The Subject DN and the Issuer DN of certificates used and issued by this CA are in line with the X.500 Distinguished Name (DN) naming method. Also, CN (Common Name) and SANs (Subject Alternative Names) in certificates cannot contain internal names or reserved IP addresses. The attributes and values of the names follow the relevant provisions of RFC 5280, BR and EVG.

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

This CPS does not allow subscribers to use anonymity, pseudonyms, or aliases, etc. It is acceptable to use Punycode to encode Internationalized Domain Names (IDNs).

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Name

This CA will review the uniqueness of the Chinese and English names, Internet hostname and the organization name of subscribers. The same Internet hostname must not be used by different organizations; however, the same organization may apply for different certificates for the same Internet hostname.

3.1.6 Name Claim Dispute Resolution Procedures

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

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

3.1.7 Recognition, Verification and Role of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization and Domain Identity

Before issuing certificates, this CA MUST complete “Organization Authentication” and “Hostname Validation” (Domain Validation or IP Address Authentication) to confirm whether the applicant is a legal entity and whether it has the ownership of the domain to be applied for. During the authentication process, the contact information of the domain will be queried through WHOIS as the source of the contact channel.

The validation record of this CA is valid for 398 days. If there is no valid validation record, the initial identity validation procedures will be re-executed in accordance with the provisions of this section.

In addition, this CA will check the CAA records to confirm whether the applicant allows TWCA to perform certificate issuance operations. For details, refer to Section 3.2.2.8.

3.2.2.1 Organization Authentication Procedure

When authenticating the identity of an organization, documents issued by the competent authorities or other documents proven the existence of such organization shall be verified. Also, the identity of its statutory representative shall be authenticated. Application documents can be delivered either via internet, over the counter or by mail.

For the application documents provided by subscribers, this CA should query the incorporating agencies/registration agencies or other certified information disclosed by third party to confirm applicant's legal existence, its identity information is consistent with the certified content (such as registration name, tradename, country, etc.), and meets the identity authentication requirements of BR or EVG.

Before issuing EVSSL certificates, the following authentication procedures must be completed (The registration agency mentioned in the following procedure refers to the organization registration authority, not the certificate registration authority):

1. The organization name must include the full legal name for the subscribing organization as listed in official records.
2. This CA must verify the Applicant’s legal existence and identity directly with the incorporating agency or registration agency, and the business category field must contain one of the following: “Private Organization”, “Government Entity”, “Business Entity”, or “Non-Commercial Entity”.
3. Jurisdiction of incorporation/registration fields must not contain information that is not relevant to the level of the incorporating agency or registration agency.
4. Subject Registration Number: if the jurisdiction of incorporation or registration does not provide a registration number, then the date of incorporation or registration is entered in this field.
5. Subject physical address of place of business must contain the address of the physical location of the business.
6. Wildcard certificates are not allowed.
7. Assumed names must be verified with an appropriate government agency or a QIIS (Qualified Independent Information Source) that has verified the assumed name with the appropriate government agency.
8. Must verify that the applicant has the ability to engage in business with EVG Section 11.6.
9. The roles of certificate requestor, certificate approver, and contract signer are required for the issuance of EVSSL certificates.

3.2.2.2 DBA/Tradename

In accordance with Section 3.2.2.1.

3.2.2.3 Verification of Country

In accordance with Section 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

This CA validates the applicant's right to use or control each domain name that will be listed in the CN/SAN field of a certificate by using at least one of the following procedures:

1. Email, Fax, SMS, or Postal Mail to the Domain Contact by sending a unique Random Value (valid for no more than 30 days from its creation) to the Domain Contact and receiving confirmation by their use of the Random Value. The domain contacts are the registered information of the registrant contact, technical contact or administrative contact in the WHOIS record. This method follows BR section 3.2.2.4.2.
2. Constructed Email to Domain Contact establishing the Applicant’s control over the FQDN by sending an email created by using “admin”, “administrator”, “webmaster”, “hostmaster” or “postmaster” as the local part followed by the (“@”) sign, followed by an Authorization Domain Name, including a Random Value (valid for no more than 30 days from its creation) in the email, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4.
3. Domain Name Service (DNS) Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7.
4. IP Address - by confirming the Applicant’s control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8. This method is not suitable for validating Wildcard Domain Names.
5. Confirming the Applicant’s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 Section 3, performed in accordance with BR Section 3.2.2.4.13.
6. Confirming the Applicant’s control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.14.

7. Confirming the Applicant’s control over the FQDN by calling the Domain Contact’s phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.15.
8. Confirming the Applicant’s control over the FQDN by calling the DNS TXT Record Phone Contact’s phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.16.
9. Confirm the Applicant’s control over the FQDN by calling the DNS CAA Phone Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3, performed in accordance with BR Section 3.2.2.4.17.
10. Confirming the Applicant’s control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file on the website. The HTTP status code of the response must be success (2xx). If it is a forwarding address, only the HTTP layer forwarding address (MUST be the result of a 301, 302, or 307 HTTP status code) is required. After 1 December 2021, this method must not be used for validating Wildcard Domain Names. The URL to be forwarded must be an authorized Port using the HTTP/HTTPS protocol, performed in accordance with BR Section 3.2.2.4.18. This method is not suitable for validating Wildcard Domain Names.
11. Confirming the Applicant’s control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555, performed in accordance with BR Section 3.2.2.4.19. This method is not suitable for validating Wildcard Domain Names.

The all validation records include the Fully-Qualified Domain Name (FQDN) applied for, the method used, the domain (Authorization Domain Name) passed the validation, and the BR version to follow. All of the above methods for validation, except IP Address (BR Section 3.2.2.4.8) may be used for domain name validation along with current best practice of consulting a Public Suffix List.

3.2.2.5 Authentication for an IP Address

This CA validates the applicant's right to use or control each IP Address that will be listed in the CN/SAN field of a certificate by using at least one of the following procedures:

1. Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the “/.well-known/pki-validation” directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1.
2. Confirming the Applicant’s control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2.
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3.
4. Confirming the Applicant’s control over the IP Address by calling the IP Address Contact’s phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the Applicant’s request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5.
5. Confirming the Applicant’s control over the IP Address by performing the procedure documented for an “http-01” challenge in draft 04 of “ACME IP Identifier Validation Extension”, performed in accordance with BR Section 3.2.2.5.6.

3.2.2.6 Wildcard Domain Validation

The domain name after removing “*.” from the applied domain cannot appear in the Public Suffix List, other specifications are in accordance with Section 3.2.2.4.

3.2.2.7 Data Source Accuracy

The “Organization Registration Agency List” and “WHOIS Lookup List” used by this CA for the Organization Authentication Procedure are disclosed in the repository on the homepage of the official website. This CA conducts regular source confirmation and list updates.

The source of the “Organization Registration Agency List” used by this CA is the official repository of government units or other information channels generally accepted in the industry.

3.2.2.8 CAA Records

Examines the Certification Authority Authorization (CAA) DNS Resource Records as specified by RFC 8659 and, if such CAA Records are present and do not obviously grant TWCA authority to issue the certificate, triggers a more careful examination of the domain name, subject name and Applicant. For details, please refer to Section 4.2.1 (7).

3.2.3 Authentication of Individual Identity

Not applicable to natural person.

3.2.4 Non-verified Subscriber Information

This CA verifies all subscriber information.

3.2.5 Validation of Authority

This CA obtains reliable communication ways according to the Organization Authentication Procedure defined in Section 3.2.2.1 to verify the identity of the representative or agent of the organization, including the authenticity of their names, positions, personal signatures or company seals on the certificate application form.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication of Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The risk of loss and compromise of keys increases as the time of use extends. Therefore, subscribers should update their keys (re-key) from time to time to ascertain key security. The maximum validity period of the subscriber certificate issued by this CA is 398 days (the validity period of the private key is the same as the validity period of the certificate).

Certificate re-key refers to the generation of a new public and private key pair prior to the expiration of the corresponding key and re-application for certifiacate issuanceto this CA. This CA will check whether there is a valid validation record. If there is no valid validation record, this CA must perform the initial identity validation procedures again in accordance with the provisions of Section 3.2.

3.3.2 Identification and Authentication for Re-Key after Revocation

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

3.4 Identification and Authentication for Revocation Request

When subscribers make a revocation request, subscribers can contact this CA by email, phone or physical document. This CA will verify such requests according to the contact information of organizations registered in the initial identity validation.

4. Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

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

4.1.2 Enrollment Process and Responsibilities

Certificate applicants should read the Subscriber Agreement in the Certificate Application Form in advance to understand their rights and obligations. If they agree to the agreement terms, they should complete and sign the Certificate Application Form and deliver it to this CA to apply for a certificate.

Applicants must generate the key pair for the certificate applied by generating the PKCS#10 certificate request file and delivering the file via a secure channel provided by this CA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The procedure of subscriber certificate application is as follows:

1. The statutory representative of organizations should apply for certificates for the organization he/she represents either in person or through an agent he/she assigns.
2. Certificate Applicants should hand over the application form and the self-generated PKCS#10 certificate request file. The personal seal of the statutory representative and seal of the organization should affix to the application form, and these seals should be the same as the seals that are used in the business establishment registration to the competent authorities.
3. This CA will perform initial identity validation procedures according to Section 3.2. If there is no valid validation record, this CA must perform procedures in accordance with Section 3.2.

4. The public key of the PKCS#10 certificate request file must not be a weak key (e.g. Debian Weak Key), and CN/SANs cannot be included in the high-risk list (e.g. phishing website).
5. CN/SANs in certificates must not contain internal names or reserved IP addresses.
6. If applying for EVSSL certificates, CN/SANs in certificates must not contain Wildcard Domain Names.
7. This CA will check the DNS for the existence of a CAA record for each FQDN in the certificates to be issued according to the procedure in RFC 8659. This CA processes the “issue” and “issuewild” property tags and may not dispatch reports of issuance requests to the contact(s) listed in an “iodef” property tag. The Certification Authority CAA identifying domains for this CAs are “twca.com.tw” and any domain containing those identifying domains as suffixes (e.g. www.twca.com.tw).
8. After verifying the documents and data submitted, this CA will determine to accept the application, request supplementary information, or reject the application.
9. After accepting the application, the certificate issuance procedure will proceed.

4.2.2 Approval and Rejection of Certificate Applications

After completing the identification and authentication procedures specified in Section 4.2.1, the applicants of approved applications will become the subscribers of this CA; and applicants that cannot be identified or authenticated will be rejected.

4.2.3 Time to Process Certificate Applications

Not specified.

4.3 Certificate Issuance

4.3.1 CA Actions for Certificate Issuance

This CA will issue certificates according to the following procedure:

1. First-time applicants should prepare the “Certificate Application Form” which must include a seal with the company name (such as an invoice seal) and the applicant's signature, and mail the original of the application form to RA for processing.
2. For certificate renewal or additional purchase, a certificate application form should be prepared, and its content must include the signature of the applicant unit and the applicant's signature or two signatures from the department. Fax or email to RA for processing.
3. The applicant must produce the certificate request file in PKCS#10 format and deliver it to this CA together with the form number in the certificate application form through a secure channel.

4. This CA checks the certificate request file delivered by the applicant, and confirms the integrity and non-repudiation of the certificate request file by verifying the digital signature to prove that the applicant does have the corresponding private key; this will include the compliance of the certificate subject DN contained in the request file with the subject DN and extension fields in the application form, and CN/SANs must not contain internal names or reserved IP addresses.
5. The reviewers of this CA log in to the certificate management website through two-factor authentication to perform the Organization Authentication and Hostname Validation defined in Section 3.2, and another reviewer will conduct the review process to confirm that the information is correct, then certificate can be issued.
6. This CA will use a third-party tool (e.g. ZLint) to check the certificate format before issuing the certificate to ensure that the certificate format does not violate the relevant requirements of RFC 5280, BR or EVG. If the check fails, it will not be issued.
7. This CA will upload the Precertificate to CT (Certificate Transparency) record server before issuing, and issue the certificate after obtaining sufficient SCT (Signed Certificate Timestamp) information.
8. The start date of the certificate in the subscriber certificate issued by this CA does not go back to the past time; that is, the start date of the certificate will not be earlier than the current time when the certificate is issued.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

This CA will notify subscribers by either phone or email after certificate issuance.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

1. To verify the consistency of certificate contents with the application form, and that the subscriber information is correct.
2. To check if the public key of the certificate is the same as that of the PKCS#10 certificate request file.
3. To verify the certificate chain of the certificate, check the correctness, integrity and validity of each certificate, whether the certificate has been revoked, whether the validity period of the certificate has expired, and whether it is indeed issued by this CA.
4. To immediately notify this CA to revoke the certificate and repeat the Certificate Issuance procedure in Section 4.3 when subscribers are unable to complete the said procedure.

5. After receiving the certificate, subscribers should confirm they have fully understood and agreed to the rights and obligations of certificate usage. Disagreement to the rights and obligations of certificate usage will be considered as a rejection of certificate acceptance, and this CA shall revoke the certificate.

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

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not specified.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

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

4.5.2 Relying Party Public Key and Certificate Usage

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

1. To obtain the RCA self-signed certificate of this CA via proper and secure channels.
2. To check if the RCA self-signed certificate, the UCA certificate, and the subscriber certificate are expired.
3. To verify if the digital signature of the UCA certificate is valid with the public key of the RCA self-signed certificate and not revoked.
4. To verify if the digital signature of the subscriber certificate is valid with the public key of the UCA certificate.
5. To check if the subscriber certificate is not revoked by this UCA.

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

4.6 Certificate Renewal

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

This CA does NOT provide certificate renewal service.

4.7 Certificate Re-key

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

4.7.1 Circumstances for Certificate Key Re-key

Subject to Section 3.3.1.

4.7.2 Who May Request Re-key

Subscribers are entitled to re-key their certificates.

4.7.3 Processing Certificate Key Re-key Requests

1. Identity identification and authentication subject to Section 3.3.
2. Issuance of certificate subject to Section 4.3.

4.7.4 Notification of New Certificate/Key Issuance to Subscriber

Subject to Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-key Certificate/Key

Subject to Section 4.4.

4.7.6 Publication of the Re-key Certificate/Key by the CA

Subject to Section 4.4.2.

4.7.7 Notification of Re-key Certificate/Key Issuance by the CA to Other Entities

Subject to Section 4.4.3.

4.8 Certificate Modification

Certificate modification refers to the issuance of a certificate with new serial number after modifying the subscriber’s identify information without changing the public key.

This CA only accepts the modification request of subscriber certificate within 7 days after the certificate is issued; if it exceeds 7 days, when the subscriber's identify information or other information recorded in the certificate needs to be changed, the certificate shall be revoked in accordance with Section 4.9. Afterwards, re-apply for certificate issuance in accordance with Sections 4.1, 4.2, 4.3, and 4.4.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

This CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The subscriber requests in writing that this CA revoke the certificate;
2. The subscriber notifies this CA the original certificate request was not authorized and does not retroactively grant authorization;
3. This CA obtains evidence that the subscriber's private key corresponding to the public key of the certificate suffered a key compromise;
4. This CA is made aware of a demonstrated or proven method that can easily compute the subscriber's private key based on the public key of the certificate; or
5. This CA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the Certificate should not be relied upon.

This CA SHOULD revoke a certificate within 24 hours and MUST revoke a certificate within 5 days if one or more of the following occurs:

1. The subscriber certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
2. This CA obtains evidence that the subscriber certificate was misused;
3. This CA is made aware that a subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. This CA is made aware of any circumstance indicating that use of a FQDN or IP address in the certificate is no longer legally permitted;
5. This CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6. This CA is made aware of a material change in the information contained in the certificate;
7. This CA is made aware that the certificate was not issued in accordance with this CA's CP/CPS;

8. This CA determines or is made aware that any of the information appearing in the certificate is inaccurate;
9. This CA's right to issue certificates expires or is revoked or terminated, unless this CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by this CA's CP/CPS;
11. This CA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise or if there is clear evidence that the specific method used to generate the private key was flawed;
12. When the private key related to the subscriber certificate is lost or destroyed; or
13. the reason for certificate modification in Section 4.8.

4.9.1.2 Reasons for Revoking a UCA Certificate

This RCA SHALL revoke a UCA Certificate within 7 days if one or more of the following occurs:

1. This UCA requests revocation in writing;
2. This UCA notifies this RCA that the original certificate request was not authorized and does not retroactively grant authorization;
3. This RCA obtains evidence that this UCA's private key corresponding to the public key of the certificate suffered a key compromise or no longer complies with Section 6.1.5 and Section 6.1.6;
4. This RCA obtains evidence that the certificate was misused;
5. This RCA is made aware that the certificate was not issued in accordance with or that this UCA has not complied with this CA's CP/CPS;
6. This RCA determines that any of the information appearing in the certificate is inaccurate or misleading;
7. This RCA or UCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
8. This RCA's or UCA's right to issue certificates expires or is revoked or terminated, unless they have made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by this CA's CP/CPS.

4.9.2 Who May Request Revocation

1. Subscriber;
2. This CA; and
3. Competent authorities or a court of law.

If anyone other than the above-mentioned persons suspect that the certificate key has been compromised or other security matters, they can also notify this CA. This CA will perform the certificate revocation procedure after confirmation. For contact information, please refer to

Section 1.5.2.

4.9.3 Certificate Revocation Procedure

Subscribers may apply for a certificate revocation according to the following procedure:

1. Those who have the right to request a certificate revocation as defined in Section 4.9.2 shall apply for the revocation of the certificate.
2. If an application for certificate revocation is submitted by a subscriber, it shall be authenticated in accordance with Section 3.4, and other applications for certificate revocation shall be verified according to the reasons defined in Section 4.9.1.
3. After authenticating the request, this CA will revoke the relevant certificate within the time limit specified in Section 4.9.1.

4.9.4 Revocation Request Grace Period

When the circumstances for revocation are detected, subscribers should make a revocation request within a reasonable grace period according to general commercial practices, and no specific grace period is defined in this CPS. When there is an alleged or proven compromise or security concerns of the certificate key, subscribers should make a revocation request within 24 hours.

4.9.5 Time Within Which CA Must Process the Revocation Request

After receiving a revocation request from subscribers, this CA shall investigate and provide preliminary reports to the subscriber within 24 hours. In any case requiring revocation, the timeframe from notice to revocation shall not exceed that stated in Section 4.9.1.1.

4.9.6 Revocation Checking Requirements for Relying Parties

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

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

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

4.9.7 CRL Issuance Frequency

This CA updates and issues CRLs every 24 hours.

4.9.8 Maximum Latency for CRLs

Not specified.

4.9.9 On-line Revocation/Status Checking Availability

This CA provides Online Certificate Status Protocol (OCSP) Responder to support querying certificate status by HTTP GET or POST. And its response message conforms to the specification of RFC 6960 and includes the digital signature of the message.

This CA updates the certificate status information provided by the OCSP Responder every 2 days, and the validity period is up to 4 days. For other details, please refer to Section 7.3.

4.9.10 On-line Revocation Checking Requirements

Prior to trusting the certificates issued by this CA, relying parties must check the certificate status. If relying parties do not check the certificate status using CRLs issued by this CA, relying parties must check the certificate status through the OCSP Responder specified in Section 4.9.9.

For the Precertificate uploaded to CT record server, if the transaction is overdue and the certificate is not issued to the subscriber, this CA will revoke the Precertificate and add it to CRL/OCSP. Please refer to Sections 4.9.7, 4.9.9, 7.2, and 7.3 for the updating frequency of CRL/OCSP and other related content.

4.9.11 Other Forms of Revocation Advertisements Available

Not specified.

4.9.12 Special Requirements Re/Key Compromise

If the key is suspected of being compromised, the informant can contact the appropriate window of this CA through legal channels (See Section 1.5.2) with the certification information. This CA accepts the following methods to prove that the key is suspected of being compromised:

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

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

1. To generate a new key pair for signing and the corresponding new certificate.
2. To revoke all issued certificates and issue CRLs with the new signing key. This CRL should include the information of all signed but still valid certificates (including the revoked certificates signed prior to key compromise).
3. To notify subscribers.
4. To securely deliver the new certificate to subscribers.
5. To issue new certificates to subscribers with the new signing key.

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

4.9.13 Circumstances for Suspension

The following sections, including Who Can Request Suspension, Procedure for Suspension Request, and Limits on Suspension Period, will be not applicable as this CA does NOT provide certification suspension service.

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 Service

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

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

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

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

contact window of this CA.

4.10.3 Operational Features

Please refer to Sections 4.9.9 and 4.9.11.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not specified.

5. Facility, Management and Operational Controls

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

5.1 Physical Controls

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

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

2. The backup copy and relevant data of the private key for CA operations are stored properly in a vault with taped CCTV surveillance. Personnel managing and operating CA management and operation systems must run the administration with at least two employees at a time. All operations are under taped surveillance.
3. Software, hardware, and hardware cryptographic modules are installed in environments protected by taped surveillance system, and two-factor authentication is required by authorized employees for running key management.

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposure

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

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

5.1.8 Off-site Backup

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

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

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

5.2 Procedural Control

5.2.1 Trusted Roles

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

1. Administrator: To take charge of system installation, system management and environment parameter setup.
2. Officer: To take charge of the issuance and revocation of certificates.
3. Auditor: To conduct internal audit, review and maintenance of audit records.
4. Operator: To run routine maintenance, such as backup, recovery and website data maintenance.

5.2.2 Number of Persons Required Per Task

The number of persons required per task:

1. Administrator: At least two.
2. Officer: At least two.
3. Auditor: At least one.
4. Operator: At least two.

Before issuing a subscriber certificate, at least 2 trusted persons must confirm that the certificate can be issued.

5.2.3 Identification and Authentication for Each Role

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

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

5.2.4 Roles Requiring Separation of Duty

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

1. Operators of this CA must be loyal, reliable and enthusiastic about work. They should not engage in any sideline job affecting certification work, nor should they have any criminal and dishonorable records.
2. Officers should equip with practical certification experience, or receive relevant training and pass the relevant tests.
3. Administrators should at least be equipped with practical certification experience and with experience in the planning, operations and administration of computing systems.

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

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

This CA has established complete education and training specifications for the hardware and software, application and security management systems of the Certificate Management System. When there are newcomers or changes of the Certificate Management System, education and training on the relevant skills will be arranged. Also, a record on the training results will be maintained for the reference of the appointment of relevant operators.

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

1. An administrator will only be assigned as an officer or auditor one full year after being transferred away from his/her original position.
2. An officer will only be assigned as an administrator or auditor one full year after being transferred away from his/her original position.
3. An auditor will only be assigned as an administrator or officer one full year after being transferred away from his/her original position.
4. An operator must work as an operator for two full years, complete the relevant education and training, and pass the review before he/she is qualified for transferring to an administrator, officer or auditor post.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

1. documents for operating the hardware and software platforms, documents related to the network system and website, and documents for operating the hardware cryptographic module;
2. documents relating to operating the Certificate Management System of this CA;
3. this CPS, CP and relevant operating standards and SOPs;
4. internal operation documents of the Certificate Management System of this CA, such as system backup and recovery operating procedure, off-site DR operating procedure, and routine operating procedure.

5.4 Audit Logging Procedure

5.4.1 Types of Events Recorded

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

1. Type of entry;
2. The date and time the event occurred;
3. A success or failure indicator when executing the CA’s signing process;
4. Identity of the entity and/or operator that caused the event; and
5. Event description.

This CA logs the following types of entry:

1. Security Audit
    - Changes of any important audit parameters, such as audit event type, contents of new and old parameters.
    - Any attempt to delete or modify an audit log.
2. Management, identification and authentication of personnel and trusted roles

    - New role setup, regardless of success or failure.
    - The maximum limit of identity authentication attempts.
    - The maximum failure limit of identity authentication attempts of users at system logon.
    - Administrator unlocks a locked account.
    - Administrator changes the identity authentication mechanism of the system; such as from password into biometrics.
3. Key Operating Procedure
    - Key generation.
    - Key destruction.
4. Private Key Loading and Storage
    - Loading a private key to the system component.
5. Addition, Deletion and Storage of Trusted Public Keys
    - Modifications of trusted public keys, including addition, deletion and storage.
6. Private Key Output
    - Output of private keys (including keys for single use or one-time key)
7. Certificate Registration
    - The process of registration request of certificates.
8. Certificate Revocation
    - The process of revocation request of certificates.
    - The process of CRL production.
    - The signature record of OCSP Response.
9. Approval of Certificate Status Change
    - Approval or rejection of request of certificate status change.
10. Configuration
    - Changes of security-related configurations.
11. Account Management
    - Addition or deletion of roles and users.
    - Modification of user account or role access authority.
12. Certificate Profile Management
    - Change of certificate profiles.
13. CRL Profile Management
    - Change of CRL profiles.
14. Important Events in System Installation and Operations
    - Installation of operating systems.
    - Installation of Certificate Management System.
    - Installation of hardware cryptographic modules.

    - Removal of hardware cryptographic modules.
    - Destruction of hardware cryptographic modules.
    - System activation.
    - Attempt to log on to the Certificate Management System.
    - Hardware or software receiving.
    - Attempt to set passwords.
    - Attempt to modify passwords.
    - Backup of the internal data of this CA.
    - Recovery of the internal data of this CA.
    - File operations (e.g. generation, rename or move).
    - Sending information to the repository.
    - Access to the internal database of this CA.
    - Key compromise.
    - Key replacement of this CA.
15. Change of the Server Settings of this CA
    - Hardware.
    - Software.
    - OS.
    - Patches.
    - Security Profiles.
16. Physical Access and Location Security
    - Personnel access the computer room of this CA.
    - Access to the server of this CA.
    - Acknowledged or suspected violation of physical security regulations.
17. Abnormal Events
    - Software errors.
    - Failures of software integrity check.
    - Receiving of messages in wrong formats.
    - Abnormal routing of message.
    - Network attack (suspected or confirmed)
    - Equipment failures.
    - Power supply anomalies.
    - UPS failures.
    - Significant and critical network service or access failures.
    - Violation of this CPS.
    - System clock reset.

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

1. Ensure that only authorized persons can read and back up audit logs.
2. Digital signatures or encryption technologies should be applied to retain current and archived electronic audit logs stored in non-rewritable discs or other media where audit log modification is disabled.
3. The key for protecting event logs must not be used for other purposes.
4. Paper or physical audit logs should be stored in a secure and safe location.

5.4.5 Audit Log Backup Procedures

Electronic audit logs should be backed up once a month and stored in an off-site location away from this CA.

5.4.6 Audit Collection System

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

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

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessment

The following risk assessments should be performed once a year:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5 Records Archival

5.5.1 Types of Records Archived

The records archived by this CA include:

1. CA accreditation data;
2. Certification Practices Statement;
3. Subscriber agreement;
4. System and equipment configuration;
5. Modifications and updates to system or configuration;
6. Certificate requests;
7. Revocation requests;
8. Documentation of receipt and acceptance of certificates;
9. All certificates issued or published;
10. Record of rekey;
11. All CRLs issued and/or published;
12. All audit logs;
13. Other data or applications to verify archive contents;
14. Documentation required by compliance auditors; and
15. Subscriber Identity Authentication data.

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

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

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

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

5.5.6 Archive Collection System

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

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

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

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

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

5.6.1 Key Changeover of UCA

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

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

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

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

5.6.2 Key Changeover of RCA

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

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

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

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

1. Notify all subscribers and RCA by email or in writing as quickly as possible.
2. Generate a new key pair and hand it over to RCA to issue a new certificate according to Section 6.1.
3. Revoke all issued certificates and issue CRLs with the new signing key, this CRL should include all issued but still valid certificates (including certificates revoked prior to the key compromise).
4. Issue new certificates to all subscribers according to Section 4.3.
5. Report and disclose the accident information to relying parties and Root CA Programs.

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

1. All subordinate CAs must be notified as soon as possible through email or in writing, and certificates of all subscribers must be revoked.
2. Revoke all issued certificates.
3. Generate a new key pair and self-signed certificate according to Section 6.1.
4. Issue new certificates to all subordinate CAs.
5. Report and disclose the accident information to relying parties and Root CA Programs.

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

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

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

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

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

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

5.7.3 Entity Private Key Compromise Procedures

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

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

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

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

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

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

2. Notify subscribers of the fact of service termination and transfer of the relevant business to other CAs and publish such fact on the repository three months prior to the day of service termination;
3. Transfer the relevant private keys and certificates of this CA to the undertaking CAs in an environment free from security threat;
4. Transfer to the undertaking CAs the CP, CPS, CA operating manuals and documentation, subscriber agreements and registration data, audit records, archive information, certificate status data and other relevant documents required for business undertaking;
5. Expunge the relevant private keys of this CA and officially announce to subscribers that the certification business has been transferred to the undertaking CAs.

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

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

For generation key pairs this CA SHALL:

1. Prepare and follow a Key Generation Script;
2. Use a hardware cryptographic module that at least complies with CNS 15135, ISO 19790, FIPS 140-2 Level 3 or FIPS 140-3 Level 3 to produce key pairs in accordance with the provisions of Section 6.2.1. The private key is stored in the hardware cryptographic module without any leakage after generation; and
3. Have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process.

For generation key pairs subscribers SHALL:

1. Use a safe method to generate the key. This CA will check whether the key uploaded by the subscriber is duplicated, whether it is a weak key, and whether the quality of the key is defective. If it does not pass the test, the certificate will not be issued.

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

This CA will check the weak key (e.g. Debian Weak Key) for the key produced by itself or the key produced by subscribers. If it fails the check, it is not allowed to be used as a certificate key.

6.1.7 Key Usage Purposes

The extension field of *keyUsage* and *extKeyUsage* in the certificate issued by this CA please refer to Section 7.1.2.

6.1.8 Subscriber Key Generation Equipment

The key pair generation device of subscribers usually refers to the key generation device built in the web server or network equipment.

6.2 Private Key Protection and Cryptographic Module Engineering Control

6.2.1 Cryptographic Module Standards and Controls

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

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

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

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

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

1. The private key of this CA is stored in the hardware cryptographic module. It is encrypted before backup with multi-person control according to Section 6.2.2. The information of the private key under multi-person control is stored in the highly secured smartcard.
2. The smartcard containing the encrypted private key information under multi-person control is stored in a secured environment with dual control and keep in custody by security controllers after sealing.
3. At least two copies of multi-person control information of the encrypted key should be maintained, with one copy stored at the secured location inside this CA and another copy in the off-site backup site with security control.

6.2.5 Private Key Archival

No private key of this CA will be archived.

6.2.6 Private Key Transfer into or From a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

The private key of this CA is encrypted and stored in a hardware cryptographic module that conforms to at least CNS 15135, ISO 19790, FIPS140-2 Level 3 or FIPS 140-3 Level 3, and equipped with multi-person control.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

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

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

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificates shall have a maximum validity period of:

Type	Private Key Usage	Certificate Term/ Public Key Usage
RCA Certificate	25 years	25 years
UCA Certificate	10 years	10 years
SSL Certificate	398 days	398 days
EVSSL Certificate	398 days	398 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

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

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

1. System login with identification authentication and multi-factor.
2. User-defined access control.
3. Security audit ability.
4. Restrictions on various certificate services and the access control of trusted roles.
5. Identification and authentication of trusted roles and identity.
6. Assurance of communication and database security.
7. Secured and reliable channels for the identification of trusted roles and relevant identity.
8. Protection for procedural integrity and security controls.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

This CA follows the ISO 27001 specifications in system development.

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

6.6.2 Security Management Controls

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

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

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

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

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

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

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

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

6.8 Time Stamping

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

1. Time of certificate issuance;
2. Time of certificate revocation;
3. Time of CRL issuance; and
4. Time of OCSP issuance.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

This CA generates non-sequential serial numbers greater than zero containing at least 64 bits of output from Cryptographically Secure Pseudorandom Number Generator (CSPRNG).

7.1.1 Version Number(s)

This CA uses and issues certificates in compliance with X.509 v3 and the fields in certificates meet the RFC 5280 standard as follows:

Fields	Description
Version	v3
Serial Number	certificate serial number
Signature Hash Algorithm	The signature hash algorithm used to issue certificates, this CA supports the following: sha256WithRSAEncryption, sha384WithRSAEncryption, ECDSAWithSHA256, and ECDSAWithSHA384
Signature	the signature value generated by the issuer
Issuer	the subject information of the signing CA
NotBefore	certificate start date
NotAfter	certificate end date
Subject	certificate subject information, see Sections 7.1.4.2 and 7.1.4.3
Subject Public Key Info	the public key corresponding to the certificate
Extensions	see Section 7.1.2

7.1.2 Certificate Extensions

The extension fields included in certificates issued by this CA conforms to the relevant requirements of RFC 5280 and BR 7.1.2.

7.1.2.1 Root CA Certificate

The self-certificate extension fields of this RCA are set as follows:

Extension Fields	Used	Description
Authority Key Identifier	○	use SHA-1 algorithm
Subject Key Identifier	○	use SHA-1 algorithm
CRL Distribution Points	X	
Subject Alternative Name	X	
Authority Information Access	X	
Certificate Policies	X	
Basic Constraints	○	cA=true pathLenConstraint=None

Extension Fields	Used	Description
Key Usage	○	keyCertSign cRLSign
Extended Key Usage	X	
SCT List	X	

7.1.2.2 Subordinate CA Certificate

The certificate extension fields of this UCA are set as follows:

Extension Fields	Used	Description
Authority Key Identifier	○	use SHA-1 algorithm
Subject Key Identifier	○	use SHA-1 algorithm
CRL Distribution Points	○	including CRL download location
Subject Alternative Name	X	
Authority Information Access	○*	including accessMethod= 1.3.6.1.5.5.7.48.2 (MUST) accessMethod=1.3.6.1.5.5.7.48.1 (MAY)
Certificate Policies	○	including certificatePolicies:policyIdentifier certificatePolicies:policyQualifiers:policyQualifierId certificatePolicies:policyQualifiers:qualifier:cPSuri
Basic Constraints	○	cA=true pathLenConstraint=0
Key Usage	○	keyCertSign (MUST) cRLSign (MAY) digitalSignature (MAY)
Extended Key Usage	○*	serverAuth (1.3.6.1.5.5.7.3.1) (MUST) clientAuth (1.3.6.1.5.5.7.3.2) (MAY)
SCT List	X	

* Effective 2024-03-15, id-ad-ocsp (1.3.6.1.5.5.7.48.1) is non-essential information.
* Extended Key Usage must present in Subordinate CA’s certificate.

7.1.2.3 Subscriber Certificate

The certificate extension fields of subscribers are set as follows:

Extension Fields	Used	Description
Authority Key Identifier	○	use SHA-1 algorithm

Extension Fields	Used	Description
Subject Key Identifier	○	use SHA-1 algorithm
CRL Distribution Points	○	including CRL download location
Subject Alternative Name	○	at least contains CN (refer to Section 7.1.4.2.1)
Authority Information Access	○*	including accessMethod= 1.3.6.1.5.5.7.48.2 (MUST) accessMethod=1.3.6.1.5.5.7.48.1 (MAY)
Certificate Policies	○	including certificatePolicies:policyIdentifier certificatePolicies:policyQualifiers:policyQualifierId certificatePolicies:policyQualifiers:qualifier:cPSuri
Basic Constraints	○	cA=false pathLenConstraint=None
Key Usage	○	digitalSignature (MUST) keyEncipherment (MAY)
Extended Key Usage	○	serverAuth (1.3.6.1.5.5.7.3.1) (MUST) clientAuth(1.3.6.1.5.5.7.3.2) (MAY)
SCT List	○	one or more signed certificate timestamp signatures

* Effective 2024-03-15, id-ad-ocsp (1.3.6.1.5.5.7.48.1) is non-essential information.

7.1.2.4 Subscriber Certificate

All other extension fields comply with requirements of RFC 5280 and BR 7.1.2.4.

7.1.2.5 Subscriber Certificate

A Precertificate shall not be considered to be a “certificate” subject to the requirements of RFC 5280.

7.1.3 Algorithm Object Identifiers

7.1.3.1 Key Algorithm Identifier

This CA issues certificates with key algorithms indicated by the following OIDs:

Key Algorithm	Object Identifier
rsaEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)} (1.2.840.113549.1.1.1)

Key Algorithm	Object Identifier
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 Algorithm Identifier

This CA issues certificates with signature algorithms indicated by the following OIDs:

Signature Algorithm	Object Identifier
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 Name Forms

7.1.4.1 Name Encoding

The Subject DN field and Issuer DN field of certificates this CA used and issued comply with the uniqueness of X.500 distinguished name (DN) and the RFC 5280 rules.

For the subscriber certificate issued by this CA, the encoded content of the Issuer DN field is byte-for-byte identical with the encoded form of the Subject DN field of the Issuing CA certificate. For each CA Certificate in the Certification Path, the encoded content of the Subject DN field of a Certificate is byte-for-byte identical among all Certificates whose Subject DN can be compared as equal, and including expired and revoked Certificates.

7.1.4.2 Subject Information - Subscriber Certificates

For the subscriber certificate issued by this CA, the verification procedure of the subject information complies with the requirements of Section 3.2.2 of this CPS, and ensure that all verification procedures are correct before issuance.

For the subscriber certificate issued by this CA, Subject attributes do not contain only metadata such as “.”, “-”, and “ “ (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable. Except for the CN attribute in the subject information, other attributes cannot appear domain name or IP address.

7.1.4.2.1 Subject Alternative Name Extension

The subscriber certificate issued by this CA, the SAN extension MUST contain at least one entry with the value of CN. Each entry MUST be either a dNSName (FQDN) or an iPAddress of a server. This CA does not issue certificates with SANs or CN containing a Reserved IP Address or Internal Name. Entries in the dNSName MUST be in the “preferred name syntax”, as specified in RFC 5280, and thus MUST NOT contain underscore characters (“_”).

7.1.4.2.2 Subject Distinguished Name Fields

The Subject DN field of the subscriber certificate issued by this CA are shown in the following table. It should be noted that the certificate issued by this CA must contain a value of CN in its SANs. Refer to Section 7.1.4.2.1 for the content.

Attributes of Subject DN	Description	SSL	EVSSL
		Used or Not	Used or Not
Common Name(CN)	network host name	○	○
Organization(O)	organization registered name	○	○
GivenName/Surname	name of natural person	X	X
Street Address	the address of the organization's place of business	X	○
Locality(L)	locality name	○	○
State or Province(S)	state or province name	○	○
Postal Code	zip code	X	○
Country(C)	country code	○	○
Organizational Unit(OU)	organizational unit name	X	X
Business Category	business category	X	○
Jurisdiction of Incorporation Locality Name	jurisdiction of incorporation locality Name	X	○

Attributes of Subject DN	Description	SSL	EVSSL
Jurisdiction of Incorporation State or Province Name	jurisdiction of incorporation state or province name	X	○
Jurisdiction of Incorporation Country Name	jurisdiction of incorporation country name	X	○
Serial Number	organization registration number	X	○
Other Subject Attributes	other attributes	X	X

7.1.4.3 Subject Information - RCA Certificates and UCA Certificates

The self-signed certificate of this RCA and the certificate of this UCA are issued in accordance with the CP, and ensured that all subject information is correct before issuance.

7.1.4.3.1 Subject Distinguished Name Fields

1. The subject DNs of this UCA are:
    - SSL UCA

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA INC.
OrganizationUnit(OU)	OU= SSL Security Services
CommonName(CN)	CN=TWCA Secure Certification Authority

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Global SSL Sub-CA
CommonName(CN)	CN=TWCA Global SSL Certification Authority

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU= Secure SSL Sub-CA
CommonName(CN)	CN= TWCA Secure SSL Certification Authority

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=SSL Sub-CA
CommonName(CN)	CN=TWCA SSL Certification Authority

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
CommonName(CN)	CN= TWCA Secure SSL Certification Authority

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
CommonName(CN)	CN=TWCA SSL Certification Authority

- EVSSL UCA

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU= Global EVSSL Sub-CA

Attributes of Subject DN	Value
CommonName(CN)	CN=TWCA Global EVSSL Certification Authority

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=EVSSL Sub-CA
CommonName(CN)	CN=TWCA EVSSL Certification Authority

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
CommonName(CN)	CN=TWCA EVSSL Certification Authority

2. The subject DNs of this RCA are:

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA Root Certification Authority

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA Global Root CA

or

Attributes of Subject DN	Value
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA CYBER Root CA

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

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

7.1.6.1 Reserved Certificate Policy Identifiers

This CA issues certificates with the following policy identifiers reserved by BR:

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 CA does not issue DV certificate)
{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 by SSL CA certificate, SSL certificate
{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 CA does not issue IV certificate)
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1)	Used by EVSSL CA certificate, EVSSL certificate

7.1.6.2 RCA Certificates

There is no *certificatePolicies* extension field in RCA Certificates.

7.1.6.3 UCA Certificates

The certificates of this UCA contain the *certificatePolicies* extension field with the following policy identifier:

Certificate Types	Identifiers
SSL UCA 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)
EVSSL UCA 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

The subscriber certificates issued by this CA contain the *certificatePolicies* extension field with the following policy identifier:

Certificate Types	Identifiers
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 Types	Identifiers
EVSSL 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

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

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

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

7.2.1 Version Number(s)

This CA issues X.509 v2 CRLs contain the following fields per RFC 5280:

Fields	Description
Version	v2
Issuer Name	the Subject DN of the issuing CA
This Update	the issuance date of this CRL
Next Update	the date by which the next CRL will be issued
Hash Algorithm	The signature hash algorithm used to issue CRLs, this CA supports the following: sha256WithRSAEncryption, ECDSAWithSHA256, and ECDSAWithSHA384

Fields	Description
Revoked Certificates	list of revoked certificates, including their serial number and revocation time
Signature	the signature value generated by the issuer

7.2.2 CRL and CRL Entry Extensions

The CRL issued by this CA has the following extension fields:

Extension Fields	Description
CRL Number	incremental serial number to identify each generation of CRLs
Authority Key Identifier	AKI of the issuing CA
Reason Code	reasons for Certificate Revocation (Refer to the description below)

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

Scenarios for the use of each revocation reason are described below:

Reason	Description

Key Compromised (1)	• the CA operator obtains verifiable evidence that the certificate subscriber’s private key corresponding to the public key of the certificate suffered a key compromise; • the CA operator is made aware of a demonstrated or proven method that exposes the certificate subscriber’s private key to compromise; • there is clear evidence that the specific method used to generate the private key was flawed; • the CA operator is made aware of a demonstrated or proven method that can easily compute the certificate subscriber’s private key based on the public key of the certificate (e.g. Debian Weak Key); or • anyone (Not limited to subscribers) requesting revocation for keyCompromise has previously demonstrated or can currently demonstrate possession of the private key of the certificate (According to the proof method stipulated by CA CPS), then the CA operator MUST revoke all instances of that key across all subscribers; or • the certificate subscriber requests that the CA operator revoke the certificate for keyCompromise, and has not previously demonstrated and cannot currently demonstrate possession of the associated private key of that certificate, the CA operator MAY revoke all certificates associated with that subscriber that contain that public key. The CA operator MUST NOT assume that it has evidence of private key compromise for the purposes of revoking the certificates of other subscribers, but MAY block issuance of future certificates with that key.
Affiliation Changed (3)	• the certificate subscriber has requested that their certificate be revoked for this reason; or • the CA operator has replaced the certificate due to changes in the certificate’s subject information and the CA has not replaced the certificate for the other reasons: keyCompromise, superseded, cessationOfOperation, or privilegeWithdrawn.

Superseded (4)	• the certificate subscriber has requested that their certificate be revoked for this reason; or • the CA operator has revoked the certificate due to domain authorization or compliance issues other than those related to keyCompromise or privilegeWithdrawn.
Cessation of Operation (5)	• the certificate subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate; • the certificate subscriber will no longer be using the certificate because they are discontinuing their website; or • the CA operator is made aware of any circumstance indicating that use of a fully-qualified domain name or IP address in the certificate is no longer legally permitted.
Privilege Withdrawn (9)	• the CA operator obtains evidence that the certificate was misused; • the CA operator is made aware that the certificate subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use; • the CA operator is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name; • the CA operator is made aware of a material change in the information contained in the certificate; • the CA operator determines or is made aware that any of the information appearing in the certificate is inaccurate; or • the CA operator is made aware that the original certificate request was not authorized and that the Subscriber does not retroactively grant authorization.
Unspecified (0)	When the reason for revocation does not belong to the above.

The encoding of the Issuer field in the CRL must be byte-for-byte equivalent with the encoding of the Issuer in the certificate.

7.3 OCSP Profile

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

1. The SHA-1 algorithm is prohibited for the signing certificate used in response, and this certificate must be issued by this CA;
2. The signature value of the response is prohibited from using the SHA-1 algorithm;
3. Reponses for certificate status support: good, revoked, and unknown;
4. When receiving a status query request for a certificate not issued by this CA, it will reply with a message that the certificate status is unknown; and
5. Refer to Section 4.9.9 for other content.

7.3.1 Version Number(s)

This CA issues v1.0 OCSP Responses contain the following fields per RFC 6960:

Fields	**Description**
Version	v1
Responder ID	SHA-1 hash of responder’s public key
Produced Time	the time at which this response was signed
Certificate Status	This CA supports the following certificate status: normal (good) revoked unknown
ThisUpdate/NextUpdate	The validity period of the OCSP response, including the current update time (ThisUpdate) and the next update time (NextUpdate)
Signature Algorithm	The signature hash algorithm used to issue the OCSP response, this CA supports the following: sha256WithRSAEncryption, sha384WithRSAEncryption, ECDSAWithSHA256, and ECDSAWithSHA384
Signature	signature value generated by the responder
Certificates	the OCSP Responder’s Certificate

7.3.2 OCSP Extensions

OCSP Extensions are complying with the requirements of RFC6960.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

This CA conducts an external audit at least once a year and an internal audit at least once a quarter.

8.2 Identity/Qualifications of Assessors

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

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

8.3 Assessor’s Relationship to Assessed Entity

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

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

8.4 Topics Covered by Assessment

Audits should be carried out to verify if:

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

2. if certificate management is carried out according to the CPS and the relevant codes of operations to meet the requirements for certificate service integrity and CA environment security controls; and the relevant operations are carried out according to the CPS and the relevant codes of operations to meet the requirements for certificate service integrity and CA environment security controls;
3. if the CPS complies with the CP regulations.

The audit schemes of this CA are:

- WebTrust for CAs v2.2.1 or newer;
- WebTrust for CAs SSL Baseline with Network Security v2.5 or newer; and
- WebTrust for Certification Authorities – Extended Validation – SSL v1.7.3 or newer.

8.5 Actions Taken as a Result of Deficiency

When nonconformities to the CPS are detected in the detailed assessment, auditors should list the defects detected in detail by severity and notify this CA. This CA will take the initiative to reveal the major defects in Bugzilla after obtaining the accident content.

This CA must propose corrective and preventive actions, and follow up on the improvement.

8.6 Communication of Results

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

8.7 Self-Audits

This CA monitors adherence to its CP, CPS and strictly control its service quality by performing self-audits at least once a quarter basis against randomly selected at least three percent of the Certificates issued by it during the auditing period.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

Free of charge.

9.1.3 Revocation or Status Information Access Fees

Free of charge.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

1. This CA assumes no responsibility for indemnifying any damages arising from or in connection with the processing of subscriber registration data and certificate issuance; except for losses caused by this CA's failure to follow this CPS, the CP and/or the relevant codes of operations as a result of negligence attributable to this CA.
2. This CA assumes no responsibility for indemnifying any damages arising from or in connection with losses as a result of an act of God or natural disasters (e.g. earthquakes) and/or events (e.g. wars) beyond the reasonable control of this CA.
3. This CA should indemnify the damages caused to subscribers according to relevant regulations as a result of the intention or negligence of operators; failure to register, issue and revoke subscriber certificates according to this CPS, the CP and/or the relevant codes of operations; or violation of the relevant laws and regulations. The upper limit of compensation is in accordance with the provisions of 9.8 Limitation of Liability.
4. This CA assumes no responsibility for indemnifying any damages arising from or in connection with legal disputes over the use of a subscriber certificate from receiving a revocation request made by this CA or persons who can make a revocation request until the publication of certificate revocation listed in CRLs, provided that this CA processes the revocation request according to this CPS and the relevant codes of operations.

5. This CA assumes no responsibility for indemnifying any damages arising from or in connection with the use of illegal, fabricated or erroneous certificates.
6. The statue of repose of the subscriber’s claim for damages is subject to the relevant laws and regulations.

9.2.2 Other Assets

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

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

9.2.3 Insurance or Warranty Coverage for End-Entities

Subject to Section 9.2.1.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Confidential information includes:

1. The private key and password for operating this CA.
2. The multi-person control data for controlling the private key of this CA.
3. The personal data of the representative and agent applying for certificates.
4. Records valid for audit and traceability generated and/or held in custody by this CA.
5. Audit records and documents generated by auditors during the audit.
6. Classified operation-related documents.

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

No subscriber basic data and identity verification data shall be disclosed to the competent authorities or any person, except under any of the following circumstances:

1. Disclosure made by the law with the authorization of the competent authorization given according to the regulatory procedures.
2. Disclosure requested according to the regulatory procedure by an arbitration organization within the jurisdiction of the Company Act for handling disputes arising from or in connection with certificates.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

This CA protects personal information according to the Personal Information Protection Act and the relevant government regulations. The specific personal information and privacy rights management are specified in the certificate application form.

9.4.2 Information Treated as Private

Subject to Section 9.4.1.

9.4.3 Information Not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

Subject to the relevant laws and regulations.

9.4.5 Notice and Consent to Use Private Information

Subject to the relevant laws and regulations.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Subject of Section 9.3.3.

9.4.7 Other Information Disclosure Circumstances

Subject of Section 9.3.3.

9.5 Intellectual Property Rights

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

2. The certificates and CRLs issued by this CA are the intellectual property of TWCA.
3. Subscriber key pairs are treated as the intellectual property of their subscribers. However, when their public keys are issued as certificates by this CA, such certificates are the intellectual property of TWCA.
4. This CA should ensure the correctness of subscriber names, without guaranteeing the ownership of the intellectual property right of the subject DN in the subscriber certificate.
5. The intellectual property right of documents written by this CA for CA operations is owned by TWCA.
6. The intellectual property right of this CPS is owned by TWCA.
7. This CPS is available for free download from the repository of this CA.
8. This CA assumes no responsibility for the consequences as a result of improper use of this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

1. This CA should keep with due care the registration data, certificate data and relevant information of subscribers to prevent leakage, marauding, alteration and/or unintended use of confidential information.
2. This CA should accept the certificate application, certificate rekey and certificate revocation information of subscribers; ensure the correctness and integrity of the relevant information delivered by subscribers to this CA; issue and revoke certificates; and send the results to subscribers according to the CP and this CPS.
3. When issuing subscriber certificates, this CP must verify the correctness and legitimacy of the application documents and subscriber identity.
4. When there are security concerns about the private key of this UCA, this UCA must notify subscribers and this RCA. When there are security concerns about the private key of this RCA, this RCA must notify all its UCAs.
5. When issuing certificates, this CA must follow this CPS to securely deliver certificates issued to the repository
6. When revoking certificates, this CA must follow this CPS to generate CRLs and securely deliver CRLs to the repository.
7. Before subscribers apply for certificates, this CA should provide the application procedure and subscriber agreement to subscribers and explain to them the code of operations concerning certificate application, certificate renewal, certificate revocation and certificate usage, as well as the relevant rights and obligations.

8. The private keys for issuing certificates and CRLs must be used independently by this CA. These keys should not be used with other functions. When there are other needs for information signature or encryption, this CA must use separate private keys.

This CA warranties the following:

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

9.6.2 RA Representations and Warranties

Subject to Section 9.6.1.

9.6.3 Subscriber Representations and Warranties

When the subscriber is an organization, its obligations are as follows:

1. When applying for certificates to this CA, subscribers should fully understand and agree to the rights and obligations specified in the application form and agreement, and the relevant regulations specified in this CPS.
2. When there is doubt about a lost or compromised private key, or when there is a change of information in the subscriber certificate, subscribers should report to this CA according to the relevant regulations.
3. Subscribers should provide full and accurate information to apply for a certificate. When accepting a subscriber certificate issued by this CA, subscribers should conform to the correctness of certificate contents and the public and private key pair.
4. Subscribers should properly generate, keep and use their private keys and follow the limitations of key and certificate use.
5. When a subscriber needs to revoke a certificate under any of the circumstances for revocation specified in this CPS (e.g. private key information leakage or private key loss), the subscriber should notify this CA immediately and apply for certificate revocation. However, the subscriber is liable to the risks and responsibilities as a result of using such certificate prior to the publication of CRLs.
6. When this CA is unable to operate normally, subscribers should seek other ways to fulfill their legal responsibility for other parties as quickly as possible. Under no circumstances shall subscribers deny their legal responsibility for others as a result of the inability to normal operation of this CA.

9.6.4 Relying Party Representations and Warranties

1. Relying parties should follow the regulations of this CPS to obtain the self-signed certificate of this RCA and the certificate of this UCA.
2. Relying parties should establish and verify the certificate chain with the self-signed certificate provided by this RCA and the certificate of this UCA to determine if the subscriber certificate is reliable.
3. When verifying a certificate, relying parties should verify the certificate digital signature of this UCA perform with the self-signed certificate of this RCA and check if the certificate has been revoked with the CRL.
4. When verifying a subscriber certificate with the certificate of this UCA, relying parties should validate if the digital signature of the certificate is issued with the private key of this UCA. Relying parties should also verify if the certificate has been revoked with the CRL or OCSP.
5. When using the CRL issued by this CA, relying parties should first verify the digital signature to ascertain if the CRL is valid. Relying parties should also check the next update time of the CRL. If the next update time has passed, obtain the latest CRL. When using OCSP Responder, relying parties should first verify the digital signature of the OCSP response.
6. Relying parties should carefully select a secured computer environment and reliable application systems. Relying parties are fully liable for the damage caused to the rights and benefits of users as a result of computer environment and/or application system problems.
7. When this CA is unable to operate normally, relying parties should seek other ways to fulfill their legal responsibility for other parties as quickly as possible. Under no circumstances shall relying parties deny their legal responsibility for others as a result of the inability to normal operation of this CA
8. When accepting the certificates issued by this CA, relying parties have understood and agreed to all the liability terms of this CA and to trust these certificates according to the scope specified in this CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

2. This CA assumes no responsibility for indemnifying any damages arising from or in connection with losses caused to subscribers or relying parties as a result of an act of God or natural disasters (e.g. earthquakes) and/or events (e.g. wars) beyond the reasonable control of this CA.
3. This CA is liable to indemnify the damages arising from or in connection with the damage caused to a third party from the leakage, marauding, interpolation or unintended use of the registration and/or certificate data of subscribers as a result of the failure to keep such data in custody with due faith and due care of this CA.
4. After receiving a request of certificate revocation, this CA should investigate and preliminarily respond to the subscriber within 24 hours. In any case of requiring revocation, the timeframe from notice to revocation shall not exceed that stated in Section 4.9.1.1. After finish revoking the requested certificate, this CA should issue and complete publishing the CRL to the repository within 24 hours from revocation. Prior to the publication of the status of revoked certificates, subscribers should take actions appropriate to minimize the effect on the relying parties of their certificates, and should be fully liable to the consequences of the use of such certificates.

9.8 Limitation of Liability

When damages arising from or connection with the issuance or use of certificates occurs to subscribers and relying parties, this CA should indemnify such damages, provided that the amount must not exceed the upper limit specified in the relevant laws and regulations or the agreement

9.9 Indemnities

Subject to Section 9.2.1.

9.10 Term and Termination

9.10.1 Term

This CPS shall be effective after being approved by PMA.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

1. PMA is the responsible unit of this CPS. This CA should revise this CPS at least once a year. Amendments include addenda or direct amendments of the CPS contents.
2. This CPS will be amended accordingly when the CP is amended or OID is changed.
3. This CPS will also be amended accordingly when there is a change in the legislative requirements and/or international standards (e.g. BR).
4. After being reviewed and approved by PMA, this CPS will be published in the repository according to Chapter 2.

9.12.2 Notification Mechanism and Period

1. Should there be suggestions for updating this CPS, please deliver them to the contact person specified in Section 1.5.2 by mail or email to forward them to the PMA of TWCA.
2. After being reviewed and approved by PMA, amendments of this CPS will be published in the repository for download.
3. Unless otherwise specified, this CA will contact subscribers according to the methods specified in Section 9.11.

9.12.3 Circumstances Under Which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

Subscribers should seek resolutions for disputes over the services of this CA or the certificates it issues according to the following rules:

1. Both parties of the dispute should seek reasonable resolutions through negotiations with due faith.
2. When both parties of the dispute are unable to seek reasonable resolutions within thirty days, a qualified third party must be assigned as the mediator of the dispute, in order to mediate and resolve the dispute.

3. When both parties of the dispute are unable to agree to the mediations and decisions made by the mediator within sixty days, both parties agree that the Taipei District Court of Taiwan will be the jurisdiction court for the first instance.
4. The sharing of the fees and charges arising from the negotiation and litigation of the disputes should be determined through negotiations or according to the relevant laws and regulations.
5. When the dispute is a transnational or trans-regional dispute that cannot be resolved according to the said procedures, both parties should seek resolutions through international arbitration.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

This CPS and this CA should comply with the Electronic Signatures Act and the Enforcement Rule of the Electronic Signatures Act, and must not violate laws and regulations of this country.

This CA conforms to the current version of BR and EVG. In the event of any inconsistency between this CPS and those Requirements, those Requirements take precedence over this CPS. The laws of the country should prevail if the above specification conflicts with the laws of this country, and this CA will raise an objection to 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

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

In the event of a conflict between the law of our country and BR or EVG, this CA will adjust this CPS to comply with the law of our country, list it in this section, and notify the CA/Browser Forum immediately.

This CPS is amended according to Section 9.12.

9.16.4 Enforcement

No stipulation.

9.16.5 Act of God

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

9.17 Other Provisions

No stipulation.

Appendix 1: Glossary

1. Internet

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

2. (Electronic) Message

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

3. RSA Algorithm

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

4. Elliptic Curve Cryptography (ECC)

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

5. ECC P-256 Curve

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

6. Electronic Signature

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

of the signed person and identifying the integrity of the signed message.

7. Encrypt/Encipher

   It refers to the enciphering of electronic documents using mathematical algorithms or other means to ensure data transmission security.

8. Decrypt/Decipher

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

9. Digital Signature

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

10. Private Key

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

11. Public Key

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

12. <Public Key>Certification or Certificate

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

13. Certification Authority or Certificates Authority (CA)

    It refers to the authority providing digital signature generation and electronic certification services; i.e. it is an authority examining the correctness of the identity data of the applicant and his connection and legitimacy with the public and private keys to be verified in an unimpaired and objective position in order to issue the public key certificate.

14. Certification Practice Statement (CPS)

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

15. Asymmetric Cryptosystem

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

16. Hash Function

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

17. Automated Certificate Management Environment (ACME)

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

18. Certificate Signing Request (CSR)

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

19. Issue a Certificate (Electronic Certification)

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

20. Public Suffix List (PSL)

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

21. Punycode

    Punycode is a representation of Unicode with the limited ASCII character subset used for Internet hostnames (e.g. "台灣" will be encoded as "xn--kpry57d"). The purpose of Punycode is to enable these multilingual domain names to be encoded as ASCII within the framework of

internationalized domain name labels.

22. Bugzilla

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

23. Internal Name

    A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate cannot be resolved through the public domain name service (Public DNS).

24. Reserved IP

    In the Internet addressing structure, IETF (Internet Engineering Task Force, Internet Engineering Group) and IANA (Internet Assigned Numbers Authority, Internet Assigned Numbers Authority) reserved Internet Protocol addresses (IP) for special purposes. Inquiries can be made at the following URL:
    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

25. Certificate Transparency (CT)

    It is an open framework for monitoring and auditing the issuance of digital certificates defined in RFC 6962. With certificate transparency, newly-issued certificates are uploaded to the public server (Log Server) through each certificate authorities (CAs), allowing efficient identification of mistakenly or maliciously issued certificates.

26. Precertificate

    It is a special certificate for auditing and verifying issuance records of CA by uploading it to CT log server defined in RFC 6962. The certificate must be pre-issued before it is actually issued to the subscriber, uploaded to CT log server to obtain SCT (Signed Certificate Timestamp), and the content of the certificate actually issued to the subscriber will include these SCTs to prove that it has been successfully uploaded to the CT log server.

Appendix 2: Acronyms and Abbreviations

ACME Automated Certificate Management Environment

ANSI American National Standard Institute

BR Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

CA Certification Authority

CC Common Criteria

CN Common Name

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSR Certificate Signing request

DN Distinguished Name

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

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