Taiwan-CA Inc.
EV SSL Certification Authority
Certification Practices Statement (CPS)

(Version 1.5)

臺灣網路認證股份有限公司
TAIWAN-CA INC.

Effective Date 30 Jan 2020

Revision Record

Version	Effective Date	Released by	Remarks
1.0	6 May 2011	TWCA PMA	First release
1.1	23 Oct 2012	TWCA PMA	Add Online Certificate Status Protocol (OCSP) service description.
1.2	23 AUG 2016	TWCA PMA	1. Add OID. 2. Modify Need for Names.
1.3	26 SEP 2017	TWCA PMA	Add CAA records checking requirement.
1.5	15 MAY 2019	TWCA PMA	1. Modified to compliance with CABF Baseline Requirement V1.6.4. 2. Add CA / Browser Forum Policy OID 3. Add CAA records CA domain requirements.

Table of Contents

Executive Summary **9**
1. Introduction **12**
1.1 Overview **12**
1.2 Document Name and Identification **12**
1.3 PKI Participants and Applicability 13
1.3.1 Certification Authority (CA) 13
1.3.1.1 Root Certification Authority (RCA) 13
1.3.1.2 EV SSL CA 13
1.3.1.3 Policy Management Authority (PMA) 13
1.3.2 Registration Authority (RA) 13
1.3.3 Subscribers 14
1.3.4 Replying Parties 14
1.3.5 Other Participants 14
1.4 Certificate Usage 14
1.4.1 Appropriate Certificate Uses 14
1.4.2 Prohibited Certificate Uses 15
1.5 Policy Administration 15
1.5.1 Organization Administering the Document 15
1.5.2 Contact Person 15
1.5.3 Person Determining CPS Suitability for the Policy 15
1.5.4 CPS Approval Procedures 16
2. Publication and Repository **17**
2.1 Repositories 17
2.2 Publication of Certification Information 17
2.3 Time of Frequency of Publication 17
2.4 Access Controls on Repositories 17
3. Identification and Authentication **18**
3.1 Naming **18**
3.1.2 Need for Names to be Meaningful 18
3.1.3 Anonymity or Pseudonymity of Subscribers 18
3.1.4 Rules for Interpreting Various Name Forms 19
3.1.5 Uniqueness of Name 19
3.1.6 Name Claim Dispute Resolution Procedures 19
3.1.7 Recognition, Verification and Role of Trademarks 19
3.2 Initial Identity Validation **19**
3.2.1 Method to Prove Possession of Private Key 19
3.2.2 Authentication of Organization Identity 20
3.2.2.1 Organization Authentication Procedure 20
3.2.2.2 Internet Host Authentication Procedure 20
3.2.2.3 CAA Records 23
3.2.3 Authentication of Individual Identity 23
3.2.4 Non-verified Subscriber Information 23
3.2.5 Validation of Authority 23
3.2.6 Criteria for Interoperation 23
3.3 Identification and Authentication of Re-Key Requests **23**
3.3.1 Identification and Authentication for Routine Re-Key 23
3.3.2 Identification and Authentication for Re-Key after Revocation 23
3.4 Identification and Authentication for Revocation Request **23**
4. Certificate Life Cycle Operational Requirements **25**

4.1 Certificate Application **25**
4.1.1 Who Can Submit a Certificate Application 25
4.1.2 Enrollment Process and Responsibilities 25
4.2 Certificate Application Processing **25**
4.2.1 Performing Identification and Authentication Functions 25
4.2.2 Approval and Rejection of Certificate Applications 26
4.2.3 Time to Process Certificate Applications 26
4.3 Certificate Issuance **26**
4.3.1 CA Actions for Certificate Issuance 26
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate 26
4.4 Certificate Acceptance **26**
4.4.1 Conduct Constituting Certificate Acceptance 26
4.4.2 Publication of the Certificate by the CA 27
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 27
4.5 Key Pair and Certificate Usage **27**
4.5.1 Subscriber Private Key and Certificate Usage 27
4.5.2 Relying Party Public Key and Certificate Usage 27
4.6 Certificate Renewal **28**
4.6.1 Circumstances for Certificate Renewal 28
4.6.2 Who May Request Renewal 28
4.6.3 Processing Certificate Renewal Requests 28
4.6.4 Notification of New Certificate Issuance to Subscriber 28
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 28
4.6.6 Publication of the Renewal Certificate by the CA 28
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 28
4.7 Certificate Re-key **28**
4.7.1 Circumstances for Certificate Key Re-key 29
4.7.2 Who May Request Re-key 29
4.7.3 Processing Certificate Key Re-key Requests 29
4.7.4 Notification of New Certificate/Key Issuance to Subscriber 29
4.7.5 Conduct Constituting Acceptance of a Re-key Certificate/Key 29
4.7.6 Publication of the Re-key Certificate/Key by the CA 29
4.7.7 Notification of Re-key Certificate/Key Issuance by the CA to Other Entities 29
4.8 Certificate Modification **29**
4.8.1 Circumstances for Certificate Modification 29
4.8.2 Who May Request a New Public Modification 29
4.8.3 Processing Certificate Modification Requests 30
4.8.4 Notification of New Certificate Issuance to Subscriber 30
4.8.5 Conduct Constituting Acceptance of a Modification Certificate 30
4.8.6 Publication of the Modification Certificate by the CA 30
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 30
4.9 Certificate Revocation and Suspension **30**
4.9.1 Circumstances for Revocation 30
4.9.2 Who May Request Revocation 30
4.9.3 Certificate Revocation Procedure 31
4.9.4 Revocation Request Grace Period 31
4.9.5 Time Within Which CA Must Process the Revocation Request 31
4.9.6 Revocation Checking Requirements for Relying Parties 31
4.9.7 CRL Issuance Frequency 31
4.9.8 Maximum Latency for CRLs 32
4.9.9 On-line Revocation/Status Checking Availability 32
4.9.10 On-line Revocation Checking Requirements 32

4.9.11 Other Forms of Revocation Advertisements Available 32
4.9.12 Special Requirements Re/Key Compromise 32
4.9.13 Circumstances for Suspension 32
4.9.14 Who Can Request Suspension 33
4.9.15 Procedure for Suspension Request 33
4.9.16 Limits on Suspension Period 33
4.10 Certificate Status Service 33
4.10.1 Operational Characteristics 33
4.10.2 Service Availability 33
4.10.3 Operational Features 33
4.11 End of Subscription 33
4.12 Key Escrow and Recovery 33
4.12.1 Key Escrow and Recovery Policy and Practices 33
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 34
5. Facility, Management and Operational Controls 35
5.1 Physical Controls 35
5.1.1 Site Location and Construction 35
5.1.2 Physical Access 35
5.1.3 Power and Air Conditioning 35
5.1.4 Water Exposure 36
5.1.5 Fire Prevention and Protection 36
5.1.6 Media Storage 36
5.1.7 Waste Disposal 36
5.1.8 Off-site Backup 36
5.2 Procedural Control 37
5.2.1 Trusted Roles 37
5.2.2 Number of Persons Required Per Task 37
5.2.3 Identification and Authentication for Each Role 37
5.2.4 Roles Requiring Separation of Duty 37
5.3 Personnel Controls 38
5.3.1 Qualifications, Experience, and Clearance Requirements 38
5.3.2 Background Check Procedures 38
5.3.3 Training Requirements 38
5.3.4 Retraining Frequency and Requirements 39
5.3.5 Job Rotation Frequency and Sequence 39
5.3.6 Sanctions for Unauthorized Actions 39
5.3.7 Independent Contractor Requirements 39
5.3.8 Documentation Supplied to Personnel 39
5.4 Audit Logging Procedure 40
5.4.1 Types of Events Recorded 40
5.4.2 Frequency of Processing Log 43
5.4.3 Retention Period for Audit Log 43
5.4.4 Protection of Audit Log 43
5.4.5 Audit Log Backup Procedures 43
5.4.6 Audit Collection System 43
5.4.7 Notification to Event-Causing Subject 43
5.4.8 Vulnerability Assessment 44
5.5 Records Archival 44
5.5.1 Types of Records Archived 44
5.5.2 Retention Period for Archive 44
5.5.3 Protection of Archive 44
5.5.4 Archive Backup Procedures 45

5.5.5 Requirements for Time-Stamping of Records 45
5.5.6 Archive Collection System 45
5.5.7 Procedures to Obtain and Verify Archive Information 45
5.6 Key Changeover 46
5.7 Compromise and Disaster Recovery 46
5.7.1 Incident and Compromise Handling Procedures 46
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 47
5.7.3 Entity Private Key Compromise Procedures 47
5.7.4 Business Continuity Capabilities after a Disaster 47
5.8 CA or RA Termination 47
6. Technical Security Controls 49
6.1 Key Pair Generation and Installation 49
6.1.1 Key Pair Generation 49
6.1.2 Private Key Delivery to Subscriber 49
6.1.3 Public Key Delivery to Certificate Issuer 49
6.1.4 CA Public Key Delivery to Relying Parties 49
6.1.5 Key Sizes 49
6.1.6 Public Key Parameters Generation and Quality Checking 49
6.1.7 Key Usage Purposes 50
6.1.8 Subscriber Key Generation Equipment 50
6.2 Private Key Protection and Cryptographic Module Engineering Control 50
6.2.1 Cryptographic Module Standards and Controls 50
6.2.2 Private Key (m-out-of-n) Multi-Person Control 50
6.2.3 Private Key Escrow 50
6.2.4 Private Key Backup 50
6.2.5 Private Key Archival 51
6.2.6 Private Key Transfer Into or From a Cryptographic Module 51
6.2.7 Private Key Storage on Cryptographic Module 51
6.2.8 Method of Activating Private Key 51
6.2.9 Method of Deactivating Private Key 51
6.2.10 Method of Destroying Private Key 51
6.2.11 Cryptographic Module Rating 51
6.3 Other Aspects of Key Pair Management 51
6.3.1 Public Key Archival 51
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 52
6.4 Activation Data 52
6.4.1 Activation Data Generation and Installation 52
6.4.2 Activation Data Protection 52
6.4.3 Other Aspects of Activation Data 52
6.5 Computer Security Controls 52
6.5.1 Specific Computer Security Technical Requirements 52
6.5.2 Computer Security Rating 53
6.6 Life Cycle Technical Controls 53
6.6.1 System Development Controls 53
6.6.2 Security Management Controls 53
6.6.3 Life Cycle Security Controls 53
6.7 Network Security Controls 53
6.8 Time Stamping 54
7. Certificate, CRL, and OCSP Profiles 55
7.1 Certificate Profile 55
7.1.1 Version Number(s) 55

7.1.2 Certificate Extensions 55
7.1.3 Algorithm Object Identifiers 55
7.1.4 Name Forms 55
7.1.5 Name Constraints 55
7.1.6 Certificate Policy Object Identifier 55
7.1.7 Usage of Policy Constraints Extension 56
7.1.8 Policy Qualifiers Syntax and Semantics 56
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 56
7.2 CRL Profile 56
7.2.1 Version Number(s) 56
7.2.2 CRL and CRL Entry Extensions 56
7.3 OCSP Profile 56
7.3.1 Version Number(s) 56
7.3.2 OCSP Extensions 56
8. Compliance Audit and Other Assessments 57
8.1 Frequency and Circumstances of Assessment 57
8.2 Identity/Qualifications of Assessors 57
8.3 Assessor's Relationship to Assessed Entity 57
8.4 Topics Covered by Assessment 57
8.5 Actions Taken as a Result of Deficiency 58
8.6 Communication of Results 58
9. Other Business and Legal Matters 59
9.1 Fees 59
9.2 Financial Responsibility 59
9.2.2 Other Assets 60
9.2.3 Insurance or Warranty Coverage for End-Entities 60
9.3 Confidentiality of Business Information 60
9.3.1 Scope of Confidential Information 60
9.3.2 Information Not Within the Scope of Confidential Information 61
9.3.3 Responsibility to Protect Confidential Information 61
9.4 Privacy of Personal Information 61
9.4.1 Privacy Plan 61
9.4.2 Information Treated as Private 61
9.4.4 Responsibility to Protect Private Information 61
9.4.5 Notice and Consent to Use Private Information 61
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 61
9.4.7 Other Information Disclosure Circumstances 62
9.5 Intellectual Property Rights 62
9.6 Representations and Warranties 62
9.6.1 CA Representations and Warranties 62
9.6.2 RA Representations and Warranties 63
9.6.3 Subscriber Representations and Warranties 63
9.6.4 Relying Party Representations and Warranties 64
9.6.5 Representations and Warranties of Other Participants 65
9.7 Disclaimers of Warranties 65
9.8 Limitation of Liability 65
9.9 Indemnities 66
9.10 Term and Termination 66
9.10.1 Term 66
9.10.2 Termination 66
9.10.3 Effect of Termination and Survival 66

9.11 Individual Notices and Communications with Participants 66
9.12 Amendments 66
9.12.1 Procedure for Amendment 66
9.12.2 Notification Mechanism and Period 66
9.12.3 Circumstances Under Which OID Must Be Changed 67
9.13 Dispute Resolution Provisions 67
9.14 Governing Law 67
9.15 Compliance with Applicable Law 68
9.16 Miscellaneous Provisions 68
9.16.1 Entire Agreement 68
9.16.2 Assignment 68
9.16.3 Severability 68
9.16.4 Enforcement 68
9.16.5 Act of God 68
9.17 Other Provisions 68
Appendix 1 Glossary 69
Appendix 2 Acronyms and Abbreviations) 72

Executive Summary

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

1. Competent Authority Approval

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

Letter Jing-Shang-Zi 10902002050, Ministry of Economic Affairs, dated 30 Jan 2020.

2. Certificates to Issue

(1) Types of certificates: TWCA EV SSL CA (this CA) issues certificates to the Internet hosts of subscribers for Internet host authentication.

(2) Level of Assurance

This CA operates according to Assurance Level 4 specified in the TWCA PKI CP and issues Class 3 certificates specified in the CP to EV SSL certificate subscribers

The following elaborates the Class 3 assurance

Class 3: Medium assurance level suitable for use in network environments exposing to the risk of interception and/or interpolation of information by malicious users; such as e-commerce websites or financial transaction websites in the Internet environment.

(3) Applicability

- The EV SSL certificates issued by this CA aim at identifying the name of the Internet host of subscribers to facilitate the relying party to identify the name and administration unit of the corresponding host.
- The EV SSL certificates issued by this CA act as a security mechanism for identify

authentication.

- The EV SSL certificates issued by this CA pursuant to this CPS are designed for organizations (subscribers) that have been approved in the organization identity authentication and hostname authentication procedures by this CA to validate their organization and possession of the corresponding hostname. The EV SSL 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, such as verifying the authenticity of the digital signature, this can validate if the certificate of that Internet host is issued by this CA, and the name identification information specified in the certificate is valid and has been approved by the identity authentication procedure of the RA of this CA.

3. Legal Liabilities and Important Matters

(1) When a subscriber needs to revoke a certificate under any of the circumstances of revocation specified in this CPS (e.g. private key information leakage or private key loss), the subscriber 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 CRL.

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

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

(4) This CA 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.

(5) After receiving a request of certificate revocation, this CA shall finish revoking the requested certificate within one workday and issue and complete publishing the CRL to the repository within 24 hours from the 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.

(6) 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.

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

4. Other Important Matters

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

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

(3) 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.

(4) When verifying a certificate, the relying party shall verify the digital signature of the certificate of this CA 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 CA. The relying party shall also verify if the certificate has been revoked from the CRL.

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

(6) This CA shall conduct internal 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 Extended Validation SSL Certification Authority Certification Practices Statement (this CPS) is established in accordance with the TWCA PKI Certification Policy (CP), the **Guidelines for the Issuance and Management of Extended Validation Certificates** (**EV SSL Guidelines**) formulated by CA/Browser Forum, and the Regulations on the Required Information for Certification Practices Statements announced by the competent authorities according to the Electronic Signatures Act. The aim of this CPS is to specify how the EV SSL Certification Authority (this CA) issues and manages certificates by following the CP.

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 authenticate 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 this CA which further issues certificates to EV SSL certificate subscribers.

1.2 Document Name and Identification

The name of this document is Taiwan-CA Inc. Extended Validation Secure Sockets Layer Certification Authority Certification Practices Statement.

This CPS is established according to the CP, and its OID is

{joint-iso-itu-t (2) country (16) Taiwan (158) TWCA (3) CA (1) EV (6) id-CP-policy (5)}.

{ISO (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) TWCA (40869) certificates (1) policies (1) EV (22) class3 (3)}

{joint-iso-itu-t (2) international-organizations (23) ca-browser-forum (140) certificate-policies (1) extended-validation (1)} (In compliance with the Extended Validation Guidelines)

1.3 PKI Participants and Applicability

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 by this CA;

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

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

Please refer to the Taiwan-CA Inc. Root Certification Authority Certification Practices Statement for the details of RCA operations.

1.3.1.2 EV SSL CA

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

(1) to issue and manage subscriber certificates;

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

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

1.3.1.3 Policy Management Authority (PMA)

The PMA is a TWCA organization responsible for establishing the following documents:

(1) CP;

(2) CPS; and

(3) SOP.

1.3.2 Registration Authority (RA)

The duty of RA is to verify the identity of the subscribers applying for EV SSL certificates and the information required for certificate issuance for this CA to issue EV SSL certificates.

This CA is also a RA, and there is no need to establish a separate RA.

1.3.3 Subscribers

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

A subscriber of this CA shall be an organization applying for an EV SSL certificate.

1.3.4 Replying Parties

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

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

A replying 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

Certificates issued by this CA are primary a security mechanism for identity authentication.

The EV SSL certificates issued by this CA pursuant to this CPS are designed for organizations (subscribers) that have been approved in the organization identity authentication and hostname authentication procedures by this CA to validate their organization verity and possession of the corresponding hostname. The EV SSL 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, such as verifying the authenticity of the digital signature, this can validate if the certificate of that Internet host is issued by this CA, and the name identification information specified in the certificate is valid and has been approved by the identity

authentication procedure of the RA of this CA.

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

The TWCA Policy Management Authority (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 when there is an incident, please e-mail 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
E-mail	ca@twca.com.tw

1.5.3 Person Determining CPS Suitability for the Policy

The PMA shall determine the suitability of this CPS established by this CA.

1.5.4 CPS Approval Procedures

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

2. Publication and Repository

2.1 Repositories

The repository of this CA provides the following services: enquiry and download of certificates, CRL, CP and CPS.

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

TWCA also provides Online Certificate Status Protocol ("OCSP") services for EVSSL certificate revocation status checking.

2.2 Publication of Certification 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) Certificate revocation status (OCSP)

TWCA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

2.3 Time of Frequency of Publication

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

CRLs are published on a daily basis.

This CA develops, implements, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

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 names of certificate subjects must be X.501 Distinguished Names (DN) using a set of the following X.509 naming elements:

Distinguished Name	Description	Required (Y/N)
Country(C):	Country name	Y
Organization(O)	Organization name	Y
Organization Unit(OU)	Unit or service DN	N
State or Province (S):	Name of state of province	Y
Locality (L) :	Name of city	Y
Common Name (CN) :	Internet host DN	Y
businessCategory:	Business type	Y
jurisdictionOfIncorporationLocalityName	Name of the city of the jurisdiction of incorporation	N
jurisdictionOfIncorporationStateOrProvinceName	Name of the state or province of the jurisdiction of incorporation	N
jurisdictionOfIncorporationCountryName	Name of the country of the jurisdiction of incorporation	Y
serialNumber	Organization serial number	Y
streetAddress	Organization address	N
postalCode	Postal code of organization location	N

DNs in the self-signed certificate of this CA:

Distinguished Name	Description
1. Country(C)	C=TW
2. Organization(O)	O=TAIWAN-CA
3. OrganizationUnit(OU)	OU=Global EVSSL Sub-CA
4. CommonName(CN)	CN=TWCA Global EVSSL Certification Authority

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 replying parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

Neither anonyms nor pseudonyms are allowed under this CPS.

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.

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

3.2.2 Authentication of Organization Identity

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 and identity documents can be delivered either over the counter or by mail.

In addition to verifying the documents submitted by subscribers, information shall be verified according to the identity identification and authentication requirements specified in the **EV SSL Guidelines**. At least the following actions shall be taken to verify the identity of an organization:

(1) Private organization: To check if the contents contained in the documents submitted by the organization match with the contents registered to the competent authorities with the open information provided by the competent authorities.

(2) Public organization: The legal reference for formation of public organizations shall be verified. Public organizations shall be requested to submit the application in an official document, and the name appeared in the official seal affixed to the document must be identical to the organization name indicated. The identification information provided for the application must match with the information published in the government organization database.

3.2.2.2 Internet Host Authentication Procedure

(1) Private organizations: To validate in the database of the administration unit of public Internet domain name that the domain name used by the Internet host name provided by a private organization in the initial registration is managed and used by that private organization.

(2) Public organizations: To validate the domain name of public organizations at the government’s public directory service and verify that the domain name used by the Internet host name provided in the initial registration exists, and the name of the user unit is identical to the public organization validated in 3.2.2.1. Domain validation:

TWCA validates the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the following procedures from section 3.2.2.4 of the Baseline Requirements:

1. This method (BR Section 3.2.2.4.1) is no longer used because it was

deprecated as of 1-August-2018;

2. Email, Fax, SMS, or Postal Mail to the Domain Contact by sending a unique Random Value (valid for no more than 30 days from its creation) through email, fax, SMS, or postal mail, to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with BR Section 3.2.2.4.2;
3. (BR Section 3.2.2.4.3) is no longer used because it was deprecated as of 31-May-2019;
4. Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an email created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the email, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4;
5. (BR Section 3.2.2.4.5) is no longer used because it was deprecated as of 1-August-2018;
6. An Agreed-Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Random Value in the "/.well-known/pki-validation" directory, performed in accordance with BR Section 3.2.2.4.6;
7. 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;
8. 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;
9. This method (BR Section 3.2.2.4.9) is no longer used;
10. This method (BR Section 3.2.2.4.10) is no longer used;
11. This method (BR Section 3.2.2.4.11) is no longer used;
12. TWCA is not compliant with this method (BR Section 3.2.2.4.12);
13. 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 6844 Section 4, as amended by Errata 5065 performed in accordance with BR Section 3.2.2.4.13;
14. 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;
15. 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; and

16. 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.

All of the above methods for validation, except IP Address (BR Section 3.2.2.4.8) may be used for Wildcard Certificate Domain Name validation along with current best practice of consulting a public suffix list.

(3) CAA Records: Examines the Certification Authority Authorization (CAA) DNS Resource Records as specified by RFC 6844 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.

(4) IP Address: For each IP Address listed in a Certificate, TWCA confirms that, as of the date the Certificate was issued, the Applicant controlled the IP Address by:

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. After July 31, 2019, TWCA will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;

5. 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;

3.2.2.3 CAA Records

Examines the Certification Authority Authorization (CAA) DNS Resource Records as specified by RFC 6844 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.

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

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

3.2.6 Criteria for Interoperation

This CA assumes no criteria for the interoperation among CAs, subscribers and certificate replying parties.

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 re-key (update) their keys from time to time to ascertain key security.

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 initial identity validation to this CA according to Section 3.2.

3.3.2 Identification and Authentication for Re-Key after Revocation

After revoking a certificate, subscribers must apply for a new certificate and 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, this CA shall authenticate such request through any of the following ways:

(1) Authentication of the revocation security code known only to the subscriber and this CA.

(2) When requests of revocation are made in writing, this CA will verity such requests according to the contact information of public 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 advance to understand their rights and obligations. If they agree to the agreement terms, they should complete the Certificate Application Form, prepare the origin or photocopy of the requested certifications of identity, and deliver them 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) Organizations should hand over an application form and the self-generated PKCS#10 application 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 the identity identification and authentication according to Section 3.2.

(4) This CA will check the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844. 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. example.twca.com.tw).

(5) After verifying the documents and data submitted, this CA will determine to accept the application, request supplementary information, or reject the application.

(6) 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) The self-generated PKCS#10 certificate application file will be delivered to this CA via a secure channel.

(2) This CA should confirm that the application file delivered by applicants is generated by applicants.

(3) The integrity of the PKCS#10 application file will be verified by means of digital signature verification. This will include the compliance of the certificate subject DN contained in the application file with the subject DN and application renewals contained in the application form.

(4) After checking every item and when no error is detected, this CA will issue a certificate to the applicant, and notify the subscriber either off-line or on-line to download the certificate from this CA.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

This CA will notify subscribers by either phone or e-mail 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 in the certificate is the same as that of the PKCS#10 certificate application file.

(3) To verify the effectiveness and legitimacy of the certificate with the CA certificate.

(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 that they have fully understood and agree 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 will revoke the certificate.

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 self-signed certificate of the RCA issuing the certificate of this CA via proper and secure channels.

(2) To check if the RCA self-signed certificate, the CA certificate and subscriber

certificate are expired.

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

(4) To verify the digital signature issued by this CA, including the digital signature used in the subscriber certificate, with the certificate and public key of this CA.

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

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 identification information.

4.6.1 Circumstances for Certificate Renewal

This CA does not provide certificate renewal service.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

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 may re-key the certificate key.

4.7.3 Processing Certificate Key Re-key Requests

- Identity identification and authentication subject to Section 3.3.
- 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 4.4.

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

Subject to 4.4.2.

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

Subject to 4.4.3.

4.8 Certificate Modification

Certificate modification refers to the issuance of a certificate after a change of the subscriber's name identification information without changing the public key.

4.8.1 Circumstances for Certificate Modification

This CA does not accept the request of certificate modification. Subscribers wishing to change their identification information or other information contained in the certificate should apply for certificate revocation in accordance with Section 4.9 and then for the issuance of a new certificate in accordance with Sections 4.1 to 4.4.

4.8.2 Who May Request a New Public Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of a Modification Certificate

Not applicable.

4.8.6 Publication of the Modification Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificates are revoked under any of the following circumstances:

(1) Subscribers wish to terminate certificate use.

(2) There are errors in a subscriber certificate or subscribers wish to change the information in the certificate during its validity.

(3) The relevant private keys of subscriber certificates are proven or alleged to be compromised, damaged, lost, exposed and/or altered.

This CA may revoke, without prior notice, the certificate of subscribers violating the laws and regulations proclaimed by the competent authorities, the CP, this CPA and/or the subscriber agreement.

When subscribers are in any of the said circumstances, the relevant certificates should be revoked and added to the CRL. The revoked certificates must be included in the CRLs published thereafter until they expire.

This CA will also revoke subscriber certificate if the reasons listed in chapter 4.9.1.1 of CA-Browser Forum Baseline Requirement occurs.

4.9.2 Who May Request Revocation

(1) Subscriber

(2) This CA.

(3) Competent authorities or a court of law.

4.9.3 Certificate Revocation Procedure

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

(1) The representative of subscribers may assign an agent to be the applicant to or directly apply for certificate revocation.

(2) The revocation request will be authenticated according to the procedure specified in Section 3.4.

(3) After authenticating the request, this CA will revoke the relevant certificates within one workday.

(4) When an emergency certificate revocation is requested out of an alleged or proven compromise or other security concerns of the certificate key, subscribers may notify this CA to revoke their certificates with the digital signature or other electronic information valid for authenticating their identity.

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 should complete certificate revocation within no later than one workday.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties should justify and check (or download) the revocation data (CRL) interval based their risk, responsibilities and potential consequences.

Relying parties should verify if the CRL is issued by this CA (verify the digital signature of the CRL) prior to using the CRL issued by this CA. Relying parties should also check if the certificate of this CA has been revoked.

4.9.7 CRL Issuance Frequency

This CA updates and issues the CRL once a day.

4.9.8 Maximum Latency for CRLs

Not specified.

4.9.9 On-line Revocation/Status Checking Availability

TWCA provides Online Certificate Status Protocol (“OCSP”) services for EVSSL certificate revocation status checking. The URL for OCSP server is: **http://evsslocsp.twca.com.tw/**

OCSP responses conform to RFC6960. OCSP responses will signed by the certificate whose is signed by this CA.

4.9.10 On-line Revocation Checking Requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a relying party does not check the status of a certificate using CRLs, he/she/it shall check the certificate status by requesting Certificate status using the OCSP responder which specified in section 4.9.9.

This CA will update information provided via an Online Certificate Status Protocol at least every four days.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder will respond with a "unknown" status.

4.9.11 Other Forms of Revocation Advertisements Available

Not specified.

4.9.12 Special Requirements Re/Key Compromise

When the signature key is compromised, this CA should respond according to the following procedure:

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

(2) To revoke all issued certificates and issue a CRL with the new signature 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 new certificates to subscribers.

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

When the 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 CRL and OCSP responder. Revocation entries on a CRL or OCSP Response 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.

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.

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

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.

The systems used to process and approve EV Certificate Requests must require actions by at least two trusted persons before creating an EV Certificate.

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
Officer	○	**X**	**X**
Administrator	**X**	○	**X**

Auditor	**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; and the operating 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 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):

- Type of entry;
- The date and time the event occurred;
- A success or failure indicator when executing the CA's signing process; and
- Identity of the entity and/or operator that caused the event;
- 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.

(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.

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;

(15) Subscriber Identity Authentication data;

5.5.2 Retention Period for Archive

All archived data of this CA should be retained for no less than seven years.

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. certificate, CRL 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 signature keys must be changed over from time to time. The validity of the signature key of this CA is equivalent to the life-cycle of its corresponding certificate. The life-cycle of a certificate must not exceed 30 years.

When changing over a key, this CA will generate a new key pair. After handing over the key pair to the RCA to issue the certificate, this CA 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.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

- Notify all subscribers and RCA by e-mail or in writing as quickly as possible.
- Generate a new key pair and hand it over to RCA to issue a new certificate according to Section 6.1.
- Revoke all issued certificates and issue a CRL with the new signature key, this CRL should include all issued but still valid certificates (including certificates revoked prior to the key compromise).
- Issue new certificates to all subscribers according to Section 4.3.

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

This CA have an Incident Response Plan and a Disaster Recovery Plan.

This CA maintains a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

This CA will annually test, review, and update these procedures.

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 is interrupted as a result of computer equipment corruption or failure and the signature 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 OCSP service 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 OCSP service 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

This CA Key Pairs generation will:

1. prepare and follow a Key Generation Script,

2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process.

According to Section 6.2.1, this CA generates the RSA key pair with CNS 15135, ISO 19790 or FIPS 140-2 Class 3 hardware cryptographic modules. The private key is stored in the hardware cryptographic module without any leakage after generation.

Keys are generated in witness by the Qualified Auditor, whose will sign in the Key Generation Testimonial after key generation as a sign of credibility.

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 replying parties to check and download.

6.1.5 Key Sizes

The size of the CA RSA key is at least be 2048 bits, ECC curve is at least be NIST P-256.

The size of the subscriber RSA key CA RSA key is at least be 2048 bits, ECC curve is at least be NIST P-256.

6.1.6 Public Key Parameters Generation and Quality Checking

RSA: The prime generator generates the RSA-required primes with the ANSI X9.31 algorithms to ensure the prime is a strong prime. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

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

6.1.7 Key Usage Purposes

In the certificates issued to subscribers by this CA, the key purpose bits in the bX.509v3 certificate key purpose extensions are digitalSignature, keyEncipherment, dataEncipherment and keyAgreement.

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 protects private keys with the CNS 15135, ISO 19790 or FIPS 140-2 Class 3 hardware cryptographic modules 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 stored in the cryptographic module after encryption.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

6.2.11 Cryptographic Module Rating

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

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

The validity of the public key and private key of this CA is the same.

Based on the sizes of keys, the validity of the public key and private key of this CA and subscribers varies as described below:

(1) The 2048 bits RSA or ECC P-256 key pairs of this CA are valid for a maximum term of 30 years.

The subscribers certificates are valid for a maximum term of 825 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.

(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.

The security controls of this CA is complied with CA-Browser Forum NETWORK AND CERTIFCATE SYSTEM SECURITY REQUIREMENTS.

6.5.2 Computer Security Rating

The security rating of the computer operating systems used by this CA complies with the TCSEC C2 or international security standards of equivalent level.

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 are dedicated, only components complying with the security policy are used, and no irrelevant hardware devices, network connection or software components are installed. Also, malicious program codes are scanned 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

Only authorized personnel of the relevant business can implement management work with the certificate management system of this CP. 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, firewall, intrusion defense system and antivirus system are installed and implemented to enhance network security.

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).

Patches update, system vulnerability scan, intrusion defense system and firewall system are applied to protect the repository of this CA against denial of service (DoS) and instructions.

6.8 Time Stamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

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

7.1.3 Algorithm Object Identifiers

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

Algorithm Type	Algorithm	Object Identifiers
Key	rsaEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)1}
Key	ecPublicKey	{iso(1)member-body(2)us(840)ansi-X9-62(10045)keyType(2)ecPublicKey(1)}
Signature	sha256WithRSAEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)11}
Signature	ECDSAWithSHA256	{iso(1)member-body(2)us(840)ansi-X9-62(10045)signatures(4)ecdsa-with-SHA2(3)2}
Signature	ECDSAWithSHA384	{iso(1)member-body(2)us(840)ansi-X9-62(10045)signatures(4)ecdsa-with-SHA2(3)3}

7.1.4 Name Forms

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

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

The CP object identifier defined in the CP is used in the certificatePolicies

extension of the certificates issued by this CA.

7.1.7 Usage of Policy Constraints Extension

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

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

This CA issues X.509 v2 CRLs.

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC6960 is supported.

7.3.2 OCSP Extensions

The OCSP Extension usage is complying with the requirements of RFC6960.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

This CA should conduct internal and external audits at least once a year.

This CA monitors adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

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, 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. Auditors carrying out the external audit should hold the national auditor qualification or internationally recognized auditor qualification and with practical experience in relevant audit work to provide objective and unbiased audit service. This CA should identify the identity of auditors prior to the audit.

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 comply with the CP regulations.

The audit schemes of this CA are:

- WebTrust for CAs v2.0 or newer;
- WebTrust for CAs SSL Baseline with Network Security v2.2 or newer; and
- WebTrust for Certification Authorities - Extended Validation – SSL v1.6.2 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 must propose corrective and preventive actions, and follow up on the improvement.

8.6 Communication of Results

This CA will publish in the repository the results of the latest external audit, except the information causing security threats to this CA.

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) TWCA 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 direct damages caused to subscribers according to relevant regulations as a result of the intention or negligence of operators; failure

to register, issue and revoke subscriber certificates according to this CPA, the CP and/or the relevant codes of operations; or violation of the relevant laws and regulations.

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

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

(8) 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.

9.2.2 Other Assets

To protect the rights and benefits of subscribers, this CA appropriates NT$30 million as the financial bond for the liability risk from indemnification for carrying out the certification business.

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.

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 or distributable according to the relevant regulations in the Copyright Act.

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

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

(1) 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 is doubt about security of the CA private key, this CA must notify subscribers and RCA.

(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 the CRL and securely deliver the CRL 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.

By Baseline Requirements , 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 CRL.

(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 CA and RCA.

(2) Relying parties should establish and verify the certificate chain with the self-signed certificate provided by this CA and RCA to determine if the subscriber certificates are reliable.

(3) When verifying a certificate, relying parties should verify the certificate digital signature of this CA perform with the self-signed certificate of the RCA and if the certificate has been revoked with the CRL.

(4) When verifying a subscriber certificate with the certificate of this CA, relying parties should validate if the digital signature of the certificate is issued with the private key of this CA. Relying parties should also verify if the certificate has been revoked with the CRL.

(5) When using the CRL issued by this CA, relying parties should first verify the digital signature to ascertain if the CRL is valid. Replying parties should also check the next update time of the CRL. If the next update time has passed, obtain the latest CRL.

(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 agree 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 finish revoking the requested certificate within one workday and issue and complete publishing the CRL to the repository within one day from revocation. Prior to the publication of the status of certificate revocation, 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 the competent authorities according to the Electronic Signatures Act and published by this CA in the repository.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

(1) This CA is the responsible unit of this CPS. This CA should review 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 CPA will also be amended accordingly when there is a change in the legislative requirements and/or international standards.

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

9.12.2 Notification Mechanism and Period

(1) Suggestions for CPS amendments can be mailed or e-mailed to the contact person

specified in Section 1.5.2 to refer to the TWCA PMA for review.

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

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

9.12.3 Circumstances Under Which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

Subscribers 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. Also, both parties must agree to the mediations and decisions of the mediator.

(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 the Republic of China.

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.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

This CPS is amended according to Section 9.12.

9.16.4 Enforcement

No stipulation.

9.16.5 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) 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.

(4) Encrypt/Encipher

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

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) <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.

(10) 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.

(11) 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.

(12) 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.

(13) 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.

(14) 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.

Appendix 2 Acronyms and Abbreviations)

AICPA	American Institute of Certified Public Accountants, Inc.
ANS	American National Standard
CA	Certification Authority
CC	Common Criteria
CCITSE	Common Criteria for Information Technology Security Evaluation
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
FIPS	Federal Information Processing Standard
ISO/IEC	the International Organization for Standardization, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificates Status Protocol
OID	Object Identifier
OECD	Organization for Economic Co-operation and Development
PMA	Policy Management Authority
PIN	Personal Identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certification Authority
RSA	Rivest, Shamir, Adleman (encryption algorithm)
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location
SSL	Secure Socket Layer
EV SSL	Extended Validation SSL