# Taiwan-CA Inc.

# Global Certification Authority

# Certification Practices Statement (CPS)

(Version1.6)

臺灣網路認證股份有限公司

TAIWAN-CA INC.

Effective Date：2021/12/21

# Revision Record:

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

| | | | |
|---|---|---|---|
| | | | 8. Add TSA Certificate.<br>9. 3.1.1：Modify AATL certificate's naming.<br>10. 3.2.2：Modified to compliance with CABF Baseline Requirement V1.7.5.<br>11. 3.2.2：Public Suffix List is required for all domain verification. |

# Table of Contents

**Executive Summary ..... 15**

**1. Introduction ..... 19**

**1.1 Overview ..... 19**

**1.2 Document Name and Identification ..... 19**

**1.3 PKI Participants ..... 21**

1.3.1 Certification Authority (CA) ..... 21

1.3.1.1 Root Certification Authority (RCA) ..... 21

1.3.1.2 This CA ..... 21

1.3.1.3 Policy Management Authority (PMA) ..... 21

1.3.2 Registration Authority (RA) ..... 22

1.3.3 Subscribers ..... 22

1.3.4 Replying Parties ..... 22

1.3.5 Other Participants ..... 22

**1.4 Certificate Usage ..... 22**

1.4.1 Certificates Level of Assurance ..... 22

1.4.2 Scope of Applicability and Liability ..... 27

1.4.3 Prohibited Certificate Uses ..... 31

**1.5 Policy Administration ..... 32**

1.5.1 Organization Administering the Document ..... 32

1.5.2 Contact Person ..... 32

1.5.3 Person Determining CPS Suitability for the Policy ..... 32

1.5.4 CPS Approval Procedures ..... 32

**2. Publication and Repository ..... 33**

**2.1 Repositories** ..... **33**

**2.2 Publication of Certification Information** ..... **33**

**2.3 Time of Frequency of Publication** ..... **33**

**2.4 Access Controls on Repositories** ..... **34**

**3. Identification and Authentication** ..... **34**

**3.1 Naming** ..... **34**

3.1.1 Types of Names ..... 34

3.1.2 Need for Names to be Meaningful ..... 39

3.1.3 Anonymity or Pseudonymity of Subscribers ..... 39

3.1.4 Rules for Interpreting Various Name Forms ..... 39

3.1.5 Uniqueness of Name ..... 39

3.1.6 Name Claim Dispute Resolution Procedures ..... 39

3.1.7 Recognition, Verification and Role of Trademarks ..... 40

**3.2 Initial Identity Validation** ..... **40**

3.2.1 Method to Prove Possession of Private Key ..... 40

3.2.2 Authentication of Organization Identity ..... 40

3.2.3 Authentication of Individual Identity ..... 44

3.2.4 Non-verified Subscriber Information ..... 45

3.2.5 Validation of Authority ..... 45

3.2.6 Criteria for Interoperation ..... 45

**3.3 Identification and Authentication of Re-key Requests** ..... **45**

3.3.1 Identification and Authentication for Routine Re-Key ..... 45

3.3.2 Identification and Authentication for Re-Key after Revocation ..... 46

**3.4 Identification and Authentication for Revocation Request** ..... **47**

**4. Certificate Life-Cycle Operational Requirements** ..... **48**

**4.1 Certificate Application ..... 48**
4.1.1 Who Can Submit a Certificate Application ..... 48
4.1.2 Enrollment Process and Responsibilities ..... 48
**4.2 Certificate Application Processing ..... 49**
4.2.1 Performing Identification and Authentication Functions ..... 49
4.2.2 Approval and Rejection of Certificate Applications ..... 49
4.2.3 Time to Process Certificate Applications ..... 49
**4.3 Certificate Issuance ..... 49**
4.3.1 CA Actions for Certificate Issuance ..... 49
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate ..... 51
**4.4 Certificate Acceptance ..... 51**
4.4.1 Conduct Constituting Certificate Acceptance ..... 51
4.4.2 Publication of the Certificate by the CA ..... 52
4.4.3 Notification of Certificate Issuance by the CA to Other Entities ..... 52
**4.5 Key Pair and Certificate Usage ..... 53**
4.5.1 Subscriber Private Key and Certificate Usage ..... 53
4.5.2 Relying Party Public Key and Certificate Usage ..... 53
**4.6 Certificate Renewal ..... 53**
4.6.1 Circumstances for Certificate Renewal ..... 54
4.6.2 Who May Request Renewal ..... 54
4.6.3 Processing Certificate Renewal Requests ..... 54
4.6.4 Notification of New Certificate Issuance to Subscriber ..... 54
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate ..... 54
4.6.6 Publication of the Renewal Certificate by the CA ..... 54
4.6.7 Notification of Certificate Issuance by the CA to Other Entities ..... 54
**4.7 Certificate Re-key ..... 55**
4.7.1 Circumstances for Certificate Re-key ..... 55

4.7.2 Who May Request a New Public Re-key .....55
4.7.3 Processing Certificate Re-keying Requests .....55
4.7.4 Notification of New Certificate Issuance to Subscriber .....55
4.7.5 Conduct Constituting Acceptance of Re-keyed Certificate .....55
4.7.6 Publication of the Re-keyed Certificate by the CA .....55
4.7.7 Notification of Certificate Issuance by the CA to Other Entities .....56
**4.8 Certificate Modification .....56**
4.8.1 Circumstances for Certificate Modification .....56
4.8.2 Who May Request Certificate Modification .....56
4.8.3 Processing Certificate Modification Requests .....56
4.8.4 Notification of New Certificate Issuance to Subscriber .....56
4.8.5 Conduct Constituting Acceptance of Modified Certificate .....57
4.8.6 Publication of the Modified Certificate by the CA .....57
4.8.7 Notification of Certificate Issuance by the CA to Other Entities .....57
**4.9 Certificate Revocation and Suspension .....57**
4.9.1 Circumstances for Revocation .....57
4.9.2 Who can Request Revocation .....58
4.9.3 Procedure for Certificate Revocation .....59
4.9.4 Revocation Request Grace Period .....60
4.9.5 Time Within Which CA Must Process the Revocation Request .....60
4.9.6 Revocation Checking Requirements for Relying Parties .....60
4.9.7 CRL Issuance Frequency .....61
4.9.8 Maximum Latency for CRLs .....61
4.9.9 On-line Revocation/Status Checking Availability .....61
4.9.10 On-line Revocation Checking Requirements .....61
4.9.11 Other Forms of Revocation Advertisements Available .....61
4.9.12 Special Requirements for Key Compromise .....62

4.9.13 Circumstances for Suspension .....62
4.9.14 Who Can Request Suspension .....63
4.9.15 Procedure for Suspension Request .....65
4.9.16 Limits on Suspension Period .....66
**4.10 Certificate Status Service .....67**
4.10.1 Operational Characteristics .....67
4.10.2 Service Availability .....67
4.10.3 Operational Features .....67
**4.11 End of Subscription .....67**
**4.12 Key Escrow and Recovery .....68**
4.12.1 Key Escrow and Recovery Policy and Practices .....68
4.12.2 Session Key Encapsulation and Recovery Policy and Practices .....68

**5. Facility, Management and Operational Controls .....69**

**5.1 Physical Controls .....69**
5.1.1 Site Location and Construction .....69
5.1.2 Physical Access .....69
5.1.3 Power and Air Conditioning .....70
5.1.4 Water Exposure .....70
5.1.5 Fire Prevention and Protection .....70
5.1.6 Media Storage .....70
5.1.7 Waste Disposal .....70
5.1.8 Off-site Backup .....71
**5.2 Procedural Control .....71**
5.2.1 Trusted Roles .....71
5.2.2 Number of Persons Required Per Task .....72
5.2.3 Identification and Authentication for Each Role .....72

5.2.4 Roles Requiring Separation of Duty....72
**5.3 Personnel Controls....73**
5.3.1 Qualifications, Experience, and Clearance Requirements....73
5.3.2 Background Check Procedures....73
5.3.3 Training Requirements....73
5.3.4 Retraining Frequency and Requirements....74
5.3.5 Job Rotation Frequency and Sequence....74
5.3.6 Sanctions for Unauthorized Actions....74
5.3.7 Independent Contractor Requirements....74
5.3.8 Documentation Supplied to Personnel....75
**5.4 Audit Logging Procedure....75**
5.4.1 Types of Events Recorded....75
5.4.2 Frequency of Processing Log....79
5.4.3 Retention Period for Audit Log....79
5.4.4 Protection of Audit Log....79
5.4.5 Audit Log Backup Procedures....80
5.4.6 Audit Collection System....80
5.4.7 Notification to Event-Causing Subject....80
5.4.8 Vulnerability Assessment....80
**5.5 Records Archival....81**
5.5.1 Types of Records Archived....81
5.5.2 Retention Period for Archive....81
5.5.3 Protection of Archive....82
5.5.4 Archive Backup Procedures....82
5.5.5 Requirements for Time-Stamping of Records....82
5.5.6 Archive Collection System....83
5.5.7 Procedures to Obtain and Verify Archive Information....83

**5.6 Key Changeover.....83**

**5.7 Compromise and Disaster Recovery.....84**

5.7.1 Incident and Compromise Handling Procedures.....84

5.7.2 Computing Resources, Software, and/or Data Are Corrupted.....84

5.7.3 Entity Private Key Compromise Procedures.....85

5.7.4 Business Continuity Capabilities after a Disaster.....85

**5.8 CA or RA Termination.....85**

**6. Technical Security Controls.....87**

**6.1 Key Pair Generation and Installation.....87**

6.1.1 Key Pair Generation.....87

6.1.2 Private Key Delivery to Subscriber.....87

6.1.3 Public Key Delivery to Certificate Issuer.....87

6.1.4 CA Public Key Delivery to Relying Parties.....87

6.1.5 Key Sizes.....88

6.1.6 Public Key Parameters Generation and Quality Checking.....88

6.1.7 Key Usage Purposes.....88

**6.2 Private Key Protection and Cryptographic Module Engineering Control.....89**

6.2.1 Cryptographic Module Standards and Controls.....89

6.2.2 Private Key (m-out-of-n) Multi-Person Control.....89

6.2.3 Private Key Escrow.....89

6.2.4 Private Key Backup.....89

6.2.5 Private Key Archival.....90

6.2.6 Private Key Transfer Into or From a Cryptographic Module.....90

6.2.7 Private Key Storage on Cryptographic Module.....90

6.2.8 Method of Activating Private Key.....90

6.2.9 Method of Deactivating Private Key.....90

6.2.10 Method of Destroying Private Key .....91
6.2.11 Cryptographic Module Rating .....91
**6.3 Other Aspects of Key Pair Management .....91**
6.3.1 Public Key Archival .....91
6.3.2 Certificate Operational Periods and Key Pair Usage Periods .....91
**6.4 Activation Data .....92**
6.4.1 Activation Data Generation and Installation .....92
6.4.2 Activation Data Protection .....92
6.4.3 Other Aspects of Activation Data .....92
**6.5 Computer Security Controls .....92**
6.5.1 Specific Computer Security Technical Requirements .....92
6.5.2 Computer Security Rating .....93
**6.6 Life Cycle Technical Controls .....93**
6.6.1 System Development Controls .....93
6.6.2 Security Management Controls .....93
6.6.3 Life Cycle Security Controls .....94
**6.7 Network Security Controls .....94**
**6.8 Time Stamping .....94**

**7. Certificate, CRL, and OCSP Profiles .....95**

**7.1 Certificate Profile .....95**
7.1.1 Version Number(s) .....95
7.1.2 Certificate Extensions .....95
7.1.3 Algorithm Object Identifiers .....95
7.1.4 Name Forms .....96
7.1.5 Name Constraints .....96
7.1.6 Certificate Policy Object Identifier .....96

7.1.7 Usage of Policy Constraints Extension .....96
7.1.8 Policy Qualifiers Syntax and Semantics.....96
7.1.9 Processing Semantics for the Critical Certificate Policy Extension.....96
**7.2 CRL Profile .....97**
7.2.1 Version Number(s) .....97
7.2.2 CRL and CRL Entry Extensions.....97
**7.3 OCSP Profile .....97**
7.3.1 Version Number(s) .....97
7.3.2 OCSP Extensions.....97

**8. Compliance Audit and Other Assessments.....98**

**8.1 Frequency and Circumstances of Assessment.....98**
**8.2 Identity/Qualifications of Assessors .....98**
**8.3 Assessor's Relationship to Assessed Entity.....99**
**8.4 Topics Covered by Assessment.....99**
**8.5 Actions Taken As a Result of Deficiency .....99**
**8.6 Communication of Results.....100**

**9. Other Business and Legal Matters.....101**

**9.1 Fees .....101**
9.1.1 Certificate Issuance or Renewal Fees .....101
9.1.2 Certificate Access Fees.....101
9.1.3 Revocation or Status Information Access Fees .....101
9.1.4 Fees for Other Services.....101
9.1.5 Refund Policy .....101
**9.2 Financial Responsibility.....102**
9.2.1 Insurance Coverage .....102

9.2.2 Other Assets....103
9.2.3 Insurance or Warranty Coverage for End-Entities....103
**9.3 Confidentiality of Business Information....103**
9.3.1 Scope of Confidential Information....103
9.3.2 Information Not Within the Scope of Confidential Information....103
9.3.3 Responsibility to Protect Confidential Information....104
**9.4 Privacy of Personal Information....104**
9.4.1 Privacy Plan....104
9.4.2 Information Treated as Private....104
9.4.3 Information Not Deemed Private....104
9.4.4 Responsibility to Protect Private Information....104
9.4.5 Notice and Consent to Use Private Information....104
9.4.6 Disclosure Pursuant to Judicial or Administrative Process....105
9.4.7 Other Information Disclosure Circumstances....105
**9.5 Intellectual Property Rights....105**
**9.6 Representations and Warranties....106**
9.6.1 CA Representations and Warranties....106
9.6.2 RA Representations and Warranties....107
9.6.3 Subscriber Representations and Warranties....108
9.6.4 Relying Party Representations and Warranties....108
9.6.5 Representations and Warranties of Other Participants....109
**9.7 Disclaimers of Warranties....109**
**9.8 Limitation of Liability....110**
**9.9 Indemnities....110**
**9.10 Term and Termination....110**
9.10.1 Term....110
9.10.2 Termination....110

9.10.3 Effect of Termination and Survival .....111
**9.11 Individual Notices and Communications with Participants .....111**
**9.12 Amendments .....111**
9.12.1 Procedure for Amendment.....111
9.12.2 Notification Mechanism and Period.....111
9.12.3 Circumstances Under Which OID Must be Changed .....112
**9.13 Dispute Resolution Provisions .....112**
**9.14 Governing Law .....112**
**9.15 Compliance with Applicable Law .....113**
**9.16 Miscellaneous Provisions .....113**
9.16.1 Entire Agreement.....113
9.16.2 Assignment.....113
9.16.3 Severability.....113
9.16.4 Enforcement .....113
9.16.5 Force Majeure .....114
**9.17 Other Provisions .....114**

**Appendix 1 Glossary .....115**

**Appendix 2 Acronyms and Abbreviations .....118**

# Executive Summary

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

## 1. Competent Authority Approval

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

**Letter Jing-Shang-Zi 11002441710, Ministry of Economic Affairs, dated 21 Dec 2021.**

## 2. Certificates to Issue

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

| | Types of Certificates | Level of Assurance | Applicability | Remarks |
|---|---|---|---|---|
| 1 | SSL Certificate | Class 3 | Website authentication and information security control. | |
| 2 | InfoSec Certificate | Class 3 | Financial transactions, securities transactions, e-commerce applications, online identity authentication, online tax declaration, e-invoice, e-voting, online patent/trademark applications, and issue, transaction and application of short-term bills, code signing. | |

| | | | | |
|---|---|---|---|---|
| | | Class 2 | e-Commerce applications, online identify authentication and e-mail applications | |
| | | Class 1 | e-Commerce applications and online identity authentication. | |
| 3 | EC SECURITY Certificate | Class 3 | Online order transactions, financial transactions, e-commerce applications, online tax declaration, e-invoice and e-voting. | |
| 4. | Device Certificate | Class 2 | | |
| 5. | AATL(Adobe Approved Trust List) Certificate | Class 3 | PDF document signing, e-Commerce applications, online identify authentication and e-mail applications | |
| 6. | TSA Certificate | Class 3 | Evidence of the signing time of the electronic document or message. | |
| Note: Please refer to “1.4 Certificate Usage for details” of the assurance level and usage of certificates. | | | | |

# 3. Legal Liabilities and Important Matters

(1) When a subscriber needs to revoke a certificate under any of the circumstances of revocation specified in this CPS (e.g. private key information leakage or private key loss), the subscriber 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 or suspension, this CA shall finish revoking or suspending the requested certificate no later than 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 or suspension, subscribers shall take actions appropriate to minimize the effect on the relying parties of their certificates, and shall be fully liable to the consequences of the use of such certificates.

(6) When damages arising from or connection with the issuance or use of certificates occurs between this CA and subscribers, both parties 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 Global Certification Authority Certification Practice Statement ('CPS') is established in accordance with the TWCA PKI Certification Policy (CP) and the Regulations on the Required Information for Certification Practices Statements announced by the competent authorities according to the Electronic Signatures Act. The aim of this CPS is to specify how the TWCA GLOBAL Certification Authority (this CA) issues and manages certificates by following the CP.

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

## 1.2 Document Name and Identification

This document is the Taiwan Global CA Certification Practice Statement (CPS).

This CPS is established in accordance with the CP. The types of certificates

and their corresponding object identifier values are as follows:

(1) TLS / SSL Certificate

OID=2.16.158.3.1.3.5

OID=1.3.6.1.4.1.40869.1.1.21

OID=2.23.140.1.2.2 (Compliant with Baseline Requirements – Organization identity asserted)

(2) InfoSec Certificate

OID=2.16.158.3.1.3.5

OID=1.3.6.1.4.1.40869.1.1.23

(3) EC SECURITY Certificate

OID=2.16.158.3.1.3.1

OID=1.3.6.1.4.1.40869.1.1.24

(4) Device Certificate

OID=1.3.6.1.4.1.40869.1.1.25

(5) AATL (Adobe Approved Trust List) Certificate

OID=1.3.6.1.4.1.40869.1.1.26

(6) TSA (Time Stamping Authority) Certificate

OID=1.3.6.1.4.1.40869.1.1.27

# 1.3 PKI Participants

## 1.3.1 Certification Authority (CA)

### 1.3.1.1 Root Certification Authority (RCA)

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

(1) to issue and manage the certificates issued to this CA;
(2) to manage and publish certificates and CRLs in the repository;
(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 This 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)

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

### 1.3.3 Subscribers

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

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

### 1.3.4 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.

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

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

No stipulation.

## 1.4 Certificate Usage

### 1.4.1 Certificates Level of Assurance

1. InfoSec Certificate, AATL Certificate, TSA Certificate and EC SECURITY

Certificate

When subscribers register to the TWCA certification service system, this CA will distinguish their security class and assurance level according to the following methods of identity authentication:

(1) Class 1

A. Method of Identity Authentication:

This CA or the RA conducts limited verification of the subscriber's name (e.g. the name of an individual or the registered name or universal resource location (URL) of an organization) and e-mail data with a simple procedure.

B. Level of Assurance:

This CA and RA assure only the uniqueness of the name and e-mail data of subscribers in the database of this CA, and all other information related to subscribers is considered as unverified.

C. Scope of Use:

Subscribers can only send electronic documents by e-mail or protect their own electronic documents with Class 1 certificates and cannot use such in business transactions requiring identity authentication.

(2) Class 2:

A. Method of Identity Authentication:

Apart from checking the name of an individual or the registered name or URL of an organization, and the general relevant information, subscribers shall provide legal and correct identity documents (e.g. the photocopy of the citizen identity card or the profit business registration of company) during the registration which can be applied for by an agent. This CA or RA will verify the identity of the applicant either by phone or through other means (e.g. a third-party database).

B. Level of Assurance:

This CA and RA assure only the uniqueness of the name and e-mail

data of subscribers in the database of this CA, as well as general verification of the relevant information of subscribers instead of assurance for absolutely correct subscriber information.

C. Scope of Use:

Subscribers are advised to use Class 2 certificates in enterprise intranets or non-financial or non-securities small amount e-commerce transactions or the encryption of such data for transmission.

(3) Class 3

A. Method of Identity Authentication:

Apart from checking the information of Class 2 certificates, subscribers shall personally apply for the registration. An organization (juristic person) may apply for registration through an agent holding valid authorization documents and documents that can identify his/her identity. When organizations can provide identity documents that can verify their organization status and such documents have been confirmed by the RA, they may apply for registration by e-mail, by fax, or by electronic document containing an electronic signature.

B. Level of Assurance:

Multiple and rigorous operating procedures are planned and implemented for the identity authentication of Class 2 or higher-class certificates to assure full verification and accuracy of relevant subscriber information.

C. Scope of Use:

Class 3 certificates are advised to use in financial or securities transactions.

(4) Testing Certificates:

A. Method of Identity Authentication:

Testing certificates are intended for testing purpose and neither this CA nor the RA will implement subscriber identity authentication in any form.

Therefore, they cannot be used in any applications or businesses.

B. Level of Assurance:

No assurance will be made by this CA or the RA

C. Scope of Use:

Test certificates are used by subscribers authorized by this CA for testing only. No use in any applications or businesses other than testing is allowed.

2. TLS / SSL Certificate

(1) The assurance level of TLS / SSL certificate is Level 3. They are used for website authentication and information security control.

(2) Methods for Identity Authentication

- 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. And use the application documents submitted by the applicant to query the third-party public information or other certification information to confirm that the content of the application documents is consistent with the verified content.

- Procedure for Identifying Server Hostname and IP Address

(A) Domain validation: Must pass at least one verification method defined by 「section 3.2.2 (2) Domain validation」.

(B) IP Address: Reference: Must pass at least one verification method defined by 「section 3.2.2 (4) IP Address」.

- Procedure for Identifying Individuals (natural persons).

Not applicable to natural person.

(3) Methods for Organization Unit Name Authentication:

After authenticating the identity of organizations according to (2), this CA confirms with the business contact person and technical contact person indicated in the subscriber application form to ensure the organization unit (OU) name. If abbreviations or acronyms are used, use general and easy to understand OU, such as MIS, IT, etc.

3. Device Certificate

(1) The assurance level of Device Certificate is Level 2.

(2) Methods for Identity Authentication

- 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. And use the application documents submitted by the applicant to query the third-party public information or other certification information to confirm that the content of the application documents is consistent with the verified content.

- Procedure for Identifying Server Hostname and IP Address

  (A) Domain validation: Must pass at least one verification method defined by 「section 3.2.2 (2) Domain validation」.

  (B) IP Address: Reference: Must pass at least one verification method defined by 「section 3.2.2 (4) IP Address」.

- Procedure for Identifying Individuals (natural persons).

  Not applicable to natural person.

(3) Methods for Organization Unit Name Authentication:

After authenticating the identity of organizations according to (2), this CA confirms with the business contact person and technical contact person indicated in the subscriber application form to ensure the organization unit (OU) name. If

abbreviations or acronyms are used, use general and easy to understand OU, such as MIS, IT, etc.

(4) Procedure for Identifying device serial number:

When identifying the serial number of the device, a verification inquiry should be made with the manufacturer of the device to confirm the correctness of the serial number of the device.

## 1.4.2 Scope of Applicability and Liability

1. Scope of Applicability

TLS / SSL certificate are designated for use in website authentication and information security control.

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

Part 1・Part 2 ・Part 3・Part 4

Meanings of each part of the code:

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

| | | | |
|---|---|---|---|
| | | | signing, e-commerce applications, online identity authentication, online tax declaration, e-invoice, e-voting, online patent/trademark application , e-mail applications, code signing |

(1) Part 1: Level of Assurance:

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

(2) Part 2: Usage:

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

(A) Single Usage: It refers to certificates designated for a specific usage or a specific transaction target, such as property declaration, online ordering or network banking. Also, the specific usage or specific transaction target of certificates is specified in the Terse Statement field of the certificate issuer in the Certificate Policy of the certificate.

(B) Multi-Usage in Limited Category: If the usage code is specified in the Terse Statement field of the certificate issuer in the Certificate Policy of the certificate, the category of multi-usage is subject to the usage specified by the code. If no code is specified, the usage is subject to the contract signed by TWCA or the announcement posted on the TWCA website.

(3) Part 3: Subscriber Type:

Subscriber status includes (1) organization (juristic person), (2)

individual (natural person), and (3) others.

(4) Part 4: Business Category:

There are three business categories: (1) financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities; (2) securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting; (3) e-commerce applications, online identity authentication, online tax declaration, e-invoice, e-voting, online patent/trademark application, e-mail applications, and code signing. Certificates for use in financial transactions can also be used in categories complying with the usage limitations or in securities transactions, e-commerce applications and online identity authentication with the consent of TWCA.

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

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

2. Limits on Transaction Amount and Liability of Certificates

The liabilities of TLS / SSL certificate are subject to the terms and conditions specified in the subscriber order or subscriber contract.

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

(1) Limits on Transaction Amount: Different limits on transaction amount are set according to the level of assurance, usage, subscriber status, and business category of certificates. When a transaction proceeds, the transaction limit shall not exceed the corresponding limit on transaction amount of that class code.
(2) Limits on Liability Amount: Different limits on liability amount are set according to the level of assurance, usage, and subscriber status of certificates. This limit refers to the maximum amount of liability for a single certificate of subscribers. That is to say, regardless of the counts of transaction, the cumulative amount of liability of a single certificate shall not exceed the liability amount limit.

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

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

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

(Table 1) Currency: NTD

| Class | Level of Assurance | Usage | Subscriber Status | Business Category | Transaction Amount Limit | Liability Amount Limit |
|---|---|---|---|---|---|---|
| 1.1.1.3 | Class 1 | Single Usage | Organization | e-Commerce applications, online identity authentication | 3,000 | 3,000 |
| 1.1.2.3 | Class 1 | Single Usage | Individual | e-Commerce applications, online identity authentication | 3,000 | 3,000 |
| 1.1.3.3 | Class 1 | Single Usage | Others | e-Commerce applications, online identity authentication | 3,000 | 3,000 |
| 2.1.1.3 | Class 2 | Single Usage | Organization | e-Commerce applications, online identify authentication and e-mail applications | 900,000 | 300,000 |
| 2.1.2.3 | Class 2 | Single Usage | Individual | e-Commerce applications, online identify authentication and e-mail applications | 300,000 | 100,000 |
| 2.1.3.3 | Class 2 | Single Usage | Others | e-Commerce applications, online identify authentication and e-mail applications | 900,000 | 300,000 |
| 3.1.1.1 | Class 3 | Single Usage | Organization | Financial transactions | Unlimited | 2,000,000 |
| 3.2.1.1 | Class 3 | Multi-usage in limited category | Organization | Financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities | Unlimited | 2,000,000 |
| 3.1.2.1 | Class 3 | Single Usage | Individual | Financial transactions | Unlimited | 300,000 |
| 3.2.2.1 | Class 3 | Multi-usage in limited category | Individual | Financial transactions, e-commerce applications, online tax declaration, e-invoice, e-voting, issue and transaction of short-term bills and securities | Unlimited | 300,000 |
| 3.1.1.2 | Class 3 | Single Usage | Organization | Securities transactions | 100,000,000 | 2,000,000 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3.2.1.2 | Class 3 | Multi-usage in limited category | Organization | Securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting | 100,000,000 | 2,000,000 |
| 3.1.2.2 | Class 3 | Single Usage | Individual | Securities transactions | 15,000,000 | 300,000 |
| 3.2.2.2 | Class 3 | Multi-usage in limited category | Individual | Securities transactions, e-commerce applications, online tax declaration, e-invoice, e-voting | 15,000,000 | 300,000 |
| 3.1.1.3 | Class 3 | Single Usage | Organization | PDF document signing, e-Commerce applications, online identity authentication, online patent/trademark application, code signing | 20,000,000 | 2,000,000 |
| 3.2.1.3 | Class 3 | Multi-usage in limited category | Organization | PDF document signing, e-Commerce applications, online identity authentication, online tax declaration, e-invoice, e-voting | 20,000,000 | 2,000,000 |
| 3.1.2.3 | Class 3 | Single Usage | Individual | PDF document signing, e-Commerce applications, online identity authentication, online patent/trademark application, code signing | 2,000,000 | 300,000 |
| 3.2.2.3 | Class 3 | Multi-usage in limited category | Individual | PDF document signing, e-Commerce applications, online identity authentication, online tax declaration, e-voting | 2,000,000 | 300,000 |

Note: If the code representing the scope of use specified in the certificate is not found in the above table, this certificate cannot be use in any applications or businesses, except for testing. Also, TWCA assumes no liability for certificates of such kind.

The code representing the scope of use is specified in the Terse Statement field of the certificate issuer in the Certificate Policy of the certificate.

## 1.4.3 Prohibited Certificate Uses

Certificates issued by this CA cannot be used in applications and/or business that may 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, R.O.C |
| 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

https://www.twca.com.tw

This CA provides the online certificate status protocol (OCSP) service for status checking of TLS / SSL certificates.

## 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) 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 X.509 certificates issued by TWCA contain a X.501 Distinguished Names (DN).

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

(1) TLS / SSL Certificate

| Distinguished Name | Description | Example of DN Contents |
|---|---|---|
| 1.Country(C) | Indicates the country of the certificate applicant. | C = TW |
| 2.State(S) | Indicates the state of the certificate applicant. | S = TAIWAN |
| 3.Locality(L) | Indicates the locality of the certificate applicant | L = TAIPEI |
| 4. Organization(O) | Indicates the organization attribute of the subscriber. | O = TAIWAN-CA Inc. |
| 5. OrganizationUnit(OU) | Indicates the organization unit attribute (name or category of service) of the certificate applicant. | OU = IT |
| 6. Common Name (CN) | Indicates the common name of the certificate applicant, e.g. URL. | CN = www.twca.com.tw |

(2) InfoSec Certificate

- General Certificate

| Distinguished Name | Description | Example of DN Contents |
|---|---|---|
| 1.Country(C) | Indicates the country of the certificate issuer. | C = TW |
| 2. Organization(O) | Indicates the organizational policy of the CA. | O = Information |
| 3. OrganizationUnit(OU) | Indicates the organization unit (issuing unit) attribute of the CA. | OU = TaiCA Information User CA |
| 4. OrganizationUnit(OU) | Indicates the organization unit attribute (English name) of the RA. | OU = 12345678-RA-Trade |
| 5. OrganizationUnit(OU) | Indicates the application or service attribute of the RA. | OU = Trade |
| 6. Common Name (CN) | Indicates the common name of the subscriber, e.g. the profit business tax code. | CN = 12345678-01-000 |

- S/MIME Certificate

| Distinguished Name | Description | Example of DN Contents |
|---|---|---|
| 1.Country(C) | Indicates the country of the certificate issuer. | C = TW |
| 2. Organization(O) | Indicates the organization attribute of the CA. | O = TAIWAN-CA Inc. |
| 3. OrganizationUnit(OU) | Indicates the organization unit (issuing unit) attribute of the CA. | OU = TWCA SMIME User CA |
| 4. OrganizationUnit(OU) | Indicates the organization unit attribute (English name) of the RA. | OU = 12345678-RA-SMIME |
| 5. OrganizationUnit(OU) | Indicates the application or service attribute of the RA. | OU = SMIME |
| 6. Common Name (CN) | Indicates the common name of the certificate applicant; e.g. application type + the last 4 digits of the code + serial number or organization registration number + serial number. | CN = SMIME5678-00-00000(for individual) or<br><br>CN=12345678-00-00000(for organization) |
| Remark：The e-mail DN shall be indicated in the <SubjectAltName> column. | | |

- Code Signing Certificate

| Distinguished Name | Description | Example of DN Contents |
|---|---|---|
| 1.Country(C) | Indicates the country attribute of the certificate applicant. | C = TW |
| 2.PostalCode | Indicates the postal code attribute of the certificate applicant. | PostalCode=100 |

| | | |
|---|---|---|
| 3.State(S) | Indicates the state attribute of the certificate applicant. | S=Taiwan |
| 4.Locality(L) | Indicates the locality attribute of the certificate applicant. | L=Taipei |
| 5.STREET | Indicates the address attribute of the certificate applicant. | STREET= 10th Floor,85,Yen-Ping South Rd Taipei, Taiwan, R.O.C |
| 6. Organization(O) | Indicates the organization attribute (English name) of the certificate applicant. | O = TAIWAN-CA Inc. |
| 7. OrganizationUnit(OU) | Indicates the organization unit attribute of the certificate applicant. | OU = System |
| 8. Common Name (CN) | Indicates the common name attribute of the certificate applicant (same as the English organization common name of the certificate applicant). | CN = TAIWAN-CA Inc |
| Remark：The Postal Code and STREET can be omitted. | | |

- AATL Certificate

| Distinguished Name | Description | Example of DN Contents |
|---|---|---|
| 1.Country(C) | Indicates the country of the certificate issuer. | C = TW |
| 2.Organization(O) | Indicates the organizational policy of the CA. | O = TAIWAN-CA Inc. |
| 3.OrganizationUnit(OU) | Indicates the organization unit (issuing unit) attribute of the CA. | OU = TWCA InfoSec User CA |
| 4.OrganizationUnit(OU) | Indicates the organization unit attribute (English name) of the RA. | OU = 70759028-RA-InfoSec or 70759028-RA-AATL |
| 5.OrganizationUnit(OU) | Indicates the application or service attribute of the RA. | OU = Information Security |
| 6.CommonName(CN) | Indicates the common name of the subscriber. | CN = 70759028-AATL-TWCA |

(3) EC SECURITY Certificate

| Distinguished Name | Description | Example of DN Contents |
|---|---|---|
| 1.Country(C) | Indicates the country of the certificate issuer. | C = TW |
| 2. Organization(O) | Indicates the organization attribute (common DN) of the CA. | O = TaiCA Secure CA |
| 3. Organization(O) | Indicates the organization attribute (policy category name) of the CA. | O = Certificate Service Provider |
| 4. OrganizationUnit(OU) | Indicates the organization unit attribute (English name) of the RA. | OU = President Securities Corp. |

| | | |
|---|---|---|
| 5. OrganizationUnit(OU) | Indicates the organization unit attribute (branch or service category) of the RA. | OU = PSCNET |
| 6. Common Name (CN) | Indicates the common name of the certificate applicant (e.g. the citizen identity card number of an individual). | CN = TWA123456789-00 |

(4) Device Certificate

| Distinguished Name | Description | Example of DN Contents |
|---|---|---|
| 1.Country(C) | Indicates the country attribute of the device. | C = TW |
| 2.State(S) | Indicates the state attribute of the device. | S = TAIWAN |
| 3.Locality(L) | Indicates the locality attribute of the device. | L = TAIPEI |
| 4.Organization (O) | Indicates the organization name device owner. | O = TAIWAN-CA Inc. |
| 5.OrganizationUnit(OU) | Indicates the serial number of devices. | OU = TW120059-NAS |
| 6.CommonName(CN) | Device name. | CN = www.twca.com.tw |

(5) TSA Certificate

| Distinguished Name | Description | Example of DN Contents |
|---|---|---|
| 1.Country(C) | Indicates the country attribute of the device. | C = TW |
| 2.Organization (O) | Indicates the organization name device owner. | O = TAIWAN-CA Inc. |
| 3.CommonName(CN) | Indicates the common name of the TSA. | CN = 70759028-01-TSA |

2. The DN of this CA

(1) SSL UCA

| Distinguished Name | Description |
|---|---|
| 1.Country(C) | C=TW |
| 2. Organization(O) | O=TAIWAN-CA INC. |
| 3. OrganizationUnit(OU) | OU= SSL Security Services |
| 4. Common Name (CN) | CN=TWCA Secure Certification Authority |

Or

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

or

| Distinguished Name | Description |
|---|---|
| 1.Country(C) | C=TW |
| 2. Organization(O) | O=TAIWAN-CA |
| 3. OrganizationUnit(OU) | OU=Secure SSL Sub-CA |
| 4. Common Name (CN) | CN=TWCA Secure SSL Certification Authority |

(2) InfoSec UCA

| Distinguished Name | Description |
|---|---|
| 1.Country(C) | C=TW |
| 2. Organization(O) | O=TAIWAN-CA Inc. |
| 3. OrganizationUnit(OU) | OU=User CA |
| 4. Common Name (CN) | CN=TWCA InfoSec User CA |

(3) EC SECURITY UCA

| Distinguished Name | Description |
|---|---|
| 1.Country(C) | C=TW |
| 2. Organization(O) | O=TAIWAN-CA Inc. |
| 3. OrganizationUnit(OU) | OU=User CA |
| 4. Common Name (CN) | CN=TWCA ECSec User CA |

(4) Device Certificate UCA

| Distinguished Name | Description |
|---|---|
| 1.Country(C) | C=TW |
| 2. Organization(O) | O=TAIWAN-CA Inc. |
| 3. OrganizationUnit(OU) | OU= Secure SSL Sub-CA |
| 4. Common Name (CN) | CN=TWCA Secure SSL Certification Authority |

(5) TSA Certificate UCA

| Distinguished Name | Description |
|---|---|
| 1.Country(C) | C=TW |
| 2. Organization(O) | O=TAIWAN-CA Inc. |
| 3. OrganizationUnit(OU) | OU=Timestamping Sub-CA |
| 4. Common Name (CN) | CN=TWCA Timestamping 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 Individual, 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 and the organization name of subscribers.

### 3.1.6 Name Claim Dispute Resolution Procedures

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

### 3.2.2 Authentication of Organization Identity

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

The TLS/SSL certificate and device certificate must be subject to organization and domain(or IP address) validation to confirm whether the applicant is a legal entity and whether it has the ownership of the domain to be applied for. In addition, TWCA will check the CAA records to confirm whether the applicant allows TWCA to perform certificate issuance operations.

In the InfoSec Certificate, if the type of certificate application is S/MIME certificate, the organization and email validation must be performed to confirm whether the applicant is a legal organization, and to confirm that the applicant

has the ownership or control of mail boxes.

The following describes the validation methods of "Organizations validation", "Domain validation", "IP validation" and "Email validation" respectively:

(1) Organizations validation: Use the application documents submitted by the applicant to query the third-party public information or other certification information to confirm that the content of the application documents is consistent with the verified content.

(2) 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. 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.
2. Constructed Email to Domain Contact establishing the Applicant’s control over the FQDN by sending an email created by using ‘admin’, ‘administrator’, ‘webmaster’, ’hostmaster’ or ‘postmaster’ as the local part followed by the (“@”) sign, followed by an Authorization Domain name, including a Random Value in the email, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4.
3. Domain Name Service (DNS) Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7.
4. IP Address - by confirming the Applicant’s control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8.
5. Confirming the Applicant’s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a

DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 Section 3, performed in accordance with BR Section 3.2.2.4.13.

6. Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.14.
7. Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.15.
8. Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.16.
9. Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3, performed in accordance with BR Section 3.2.2.4.17.
10. Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file on the website. The HTTP status code of the response must be success (2xx). If it is a forwarding address, only the HTTP layer forwarding address (MUST be the result of a 301, 302, or

307 HTTP status code) is required. The URL to be forwarded must be an authorized Port using the HTTP/HTTPS protocol, performed in accordance with BR Section 3.2.2.4.18.

11. Confirming the Applicant’s control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555, performed in accordance with BR Section 3.2.2.4.19.

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

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

(4) IP Address validation: TWCA validates the Applicant's right to use or control each IP address that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the following procedures from section 3.2.2.5 of the Baseline Requirements:

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

confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5.

5. Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension", performed in accordance with BR Section 3.2.2.5.6.

(5) Email validation: TWCA uses at least one of the following validation methods to verify the right to use or ownership of the email address that the applicant wants to apply for in the certificate:

1. TWCA sends a random value to the designated recipient, where the recipient's email address is the email address specified in the Subject Alternative Name of the S/MIME certificate issued in the future, and TWCA verifies that random value.
2. TWCA uses the domain name to check and confirm the ownership of the email address. The domain name is defined as the email's local part followed by the ("@") sign. The verification method can be in 「(2) Domain validation」 Any of the defined validation methods.

## 3.2.3 Authentication of Individual Identity

If individual registers the level of assurance to Class 3, this individual may apply for registration in person and submit the relevant identity documents (an ID, passport or NHI Card) for the RA to verify or using the equivalent method to verify the identity of person. When the applicant is not the citizen of Taiwan, the verification should be conducted according to the relevant SOPs.

According to 「section 1.4 Certificate Usage」, TLS/SSL certificates and device certificates are not accepted by natural persons.

In the InfoSec Certificate, if the type of certificate is S/MIME certificate, the email validation must be performed to confirm whether the applicant is legal, and to confirm that the applicant has the ownership or control of mail box. The verification method is the same as 「section 3.2.2 Authentication of Organization Identity (5) Email validation」.

### 3.2.4 Non-verified Subscriber Information

This CA verifies all subscriber information.

### 3.2.5 Validation of Authority

The certifications or documents of identity of the 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 assure the key security.

When the validity of a subscriber key (certificate) is set to one year, this key must be rekeyed upon expiration in one year; i.e. the validity of the subscriber certificate is one year. Within the certificate rekey period (e.g. one month to expiration), the subscriber must re-generate a public and private key pair and apply to this CA and RA for issuing a new certificate. This process is known as the ‘rekey’ of certificate and private key.

The maximum validity of an InfoSec certificate, AATL certificate or EC SECURITY certificate is 39 months(The validity period of the private key is the same as the certificate validity period).

Prior to certificate expiration, subscribers of InfoSec certificate, AATL certificate and EC SECURITY certificate should sign the application for new public key certificate with the valid private key before delivering it to the RA to apply for issuing a new certificate.

When rekeying of the certificate and private key after the expiration of InfoSec certificate, AATL certificate and EC SECURITY certificate, subscribers must apply to the RA for certificate rekey over the counter, by mail or other methods that can effectively verify their identity. After obtaining the identity authentication data for certificate rekey from the RA, subscribers should use the certificate application and subscriber identity authentication data containing the new private key signature to apply for the issue of a new certificate to this CA or RA according to the RA's SOP. After receiving the certificate application from subscribers, apart from verifying the legitimacy of private key possession, the RA should verify the legitimacy and integrity the subscriber's certificate application.

TLS / SSL certificates and Device certificate have a validity period no greater than 398 days(The validity period of the private key is the same as the certificate validity period).

Subscribers should apply for a new certificate upon the expiration of their TLS / SSL certificates or Device certificate.

TSA certificate's private key have a validity period no greater than 15 months and the validity period of the certificate is no greater than 135 months.

Subscribers should apply for a new certificate upon the expiration of their TSA certificates.

### 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 or other forms of identity certification to this CA according to Section 3.2.

## 3.4 Identification and Authentication for Revocation Request

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

# 4. Certificate Life-Cycle Operational Requirements

## 4.1 Certificate Application

### 4.1.1 Who Can Submit a Certificate Application

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

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

### 4.1.2 Enrollment Process and Responsibilities

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

(1) RA must explain in detail to subscribers the representations and warranties specified in certification apply form and Subscriber Agreement, the operating procedure of the operation of relevant businesses and the provision of the user's guide and operation documents should be approved and confirmed by subscribers.
(2) Subscribers should correct and detailed information in the relevant application forms and submit the relevant supporting documents. After verifying the identity and supporting documents according to the SOP for identity authentication of different levels of assurance, RA should set the personal identification number (PIN) and protection password of subscribers to complete the subscriber registration.

# 4.2 Certificate Application Processing

## 4.2.1 Performing Identification and Authentication Functions

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

Prior to issuing a publicly-trusted TLS / SSL Certificate, TWCA checks 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 8659. TWCA 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 CAs within TWCA’s operational control are “twca.com.tw” and any domain containing those identifying domains as suffixes (e.g. example.twca.com.tw).

## 4.2.2 Approval and Rejection of Certificate Applications

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

## 4.2.3 Time to Process Certificate Applications

No stipulation.

# 4.3 Certificate Issuance

## 4.3.1 CA Actions for Certificate Issuance

1. TLS / SSL Certificates

(1) First-time applicants should prepare the ‘Company Change Registration Form’, ‘Domain Name Use Authorization’, ‘SSL Digital Certificate Application Form’, and the check or remittance receipt of the service fees; and send them to RA to make a certificate application. However, no ‘Company Change Registration Form’ and ‘Domain Name Use Authorization’ is required for an application for certificate renewal.
(2) When applying for TLS / SSL certificates from the TLS / SSL Certificate Application Website via the Internet, subscribers should first generate the subscriber certificate application file according to the registration requirements for TLS / SSL certificate application. Next, subscribers should fill in the information and password of the technical contact person, business contract person, and account contact person in accordance with setup information in the ‘SSL Digital Certificate Application Form’ to complete the certificate application procedure.
(3) After checking the application documents and certificate application information provided by subscribers, operating personnel will issue the subscriber certificate if no error is found and notify the subscriber by e-mail.

2. InfoSec Certificate, AATL certificate, TSA Certificate and EC SECURITY Certificate
(1) Subscribers must pass at least the PIN and password check and verification. After logging on to RA, subscribers should sign the certificate application information with the subscriber private key before delivering it to RA.
(2) After verifying the PIN and password of subscribers and checking the integrity of the certificate application information, RA should sign the certificate application information of subscribers with the RA private key if no error is found before delivering such information to this CA after encryption.
(3) After examining the certificate application information of subscribers received by RA and the legitimacy of the identity of both RA and subscribers and the integrity of information, this CA should issue the subscriber certificate and deliver it to RA if no error is found.
(4) After examining the legitimacy and integrity of the reply information of subscriber certificates from this CA, RA should deliver the subscriber certificate to the applicant if no error is found.
3. Device Certificate
(1) First-time applicants should prepare the ‘Company Change

Registration Form', 'Domain Name Use Authorization', 'Device Certificate Application Form'; and send them to RA to make a certificate application. However, no 'Company Change Registration Form' and 'Domain Name Use Authorization' is required for an application for certificate renewal.

(2) After proper identification and authentication of Subscriber, the digitally signed Certification Request Message is permitted to send to RA.

(3) RA verify the identification of the Subscriber and verify the Certification Request Message was signed by Subscriber's Private Key then send the Certificate Application Request via secured channel to this CA.

(4) This CA will verify the Certificate Application Request, RA identity and Subscriber identity. After verification without error, the Subscriber certificate will be issued by this CA then return it with Certificate Issued Response Message to RA.

(5) RA will verify the CA returned Certificate Issued Response Message then send the Certificate to Subscriber.

For security consideration, RA or this CA may deliver the certificate application and private key generation software to subscribers with reliable measures with security control. Also, the security of such software must be appropriately assessed and verified by RA or this CA.

### 4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

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

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

## 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) If the procedures are unfulfilled, this CA should immediately inform RA to revoke the certificate and re-initiate the certificate issuance procedure in Section 4.3.

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

If subscribers do not receive the issued certificates within seven days after issuance or have problems approved by this CA, they may request a re-issuance of certificates from RA or this CA.

## 4.4.2 Publication of the Certificate by the CA

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

## 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

# 4.5 Key Pair and Certificate Usage

## 4.5.1 Subscriber Private Key and Certificate Usage

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

Subscribers 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 the RA.

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

## 4.7.1 Circumstances for Certificate Re-key

Subject to Section 3.3.1.

## 4.7.2 Who May Request a New Public Re-key

Subscribers are entitled to re-key their certificates.

## 4.7.3 Processing Certificate Re-keying Requests

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

## 4.7.4 Notification of New Certificate Issuance to Subscriber

Subject to Section 4.3.2.

## 4.7.5 Conduct Constituting Acceptance of Re-keyed Certificate

Subject to Section 4.4.

## 4.7.6 Publication of the Re-keyed Certificate by the CA

Subject to Section 4.4.2.

### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Subject to Section 4.4.3.

## 4.8 Certificate Modification

Certificate modification refers to the issuance of a certificate after modifying the subscriber's 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 modify 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 Certificate 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 Modified Certificate

Not applicable.

### 4.8.6 Publication of the Modified 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

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

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

(1) Subscribers

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

lost, exposed or interpolated, or when there is a doubt of third-party theft.

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

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

(3) Responsible Units:

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

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.

## 4.9.2 Who can Request Revocation

RA or this CA related to subscribers, the competent authorities or a legally

authorized third party, and subscribers are entitled to request certificate revocation.

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

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

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

## 4.9.3 Procedure for Certificate Revocation

(1) Personal Revocation Requests:

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

(2) Online Revocation Requests:

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

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

The competent authorities, a court of law and an arbitration institution or other authorized parties should make an official certificate revocation request

to RA in writing.

## 4.9.4 Revocation Request Grace Period

When the circumstances for revocation are detected, subscribers 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.

This CA accepts requests of certificate revocation and reports of improper certificate use 24x7. The processing procedure after case acceptance is shown in Section 4.9.5.

## 4.9.5 Time Within Which CA Must Process the Revocation Request

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

## 4.9.8 Maximum Latency for CRLs

Not specified.

## 4.9.9 On-line Revocation/Status Checking Availability

This CA provides the online certificate status protocol (OCSP) service for TLS / SSL certificates. The service URL is indicated in the TLS / SSL certificates.

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

Prior to trusting the certificates issued by this CA, relying party must check the status of certificates. If relying party do not check the certificate status from the CRL issued by this CA, they should check the certificate status with OCSP according to 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 an "unknown" status.

## 4.9.11 Other Forms of Revocation Advertisements Available

Not specified.

## 4.9.12 Special Requirements for Key Compromise

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

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

When the 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) 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).
(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

1. TLS / SSL Certificate

Suspension of TLS / SSL certificate is currently unavailable.

2. InfoSec Certificate

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

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

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

(3) Responsible Units:
- The competent authorities or a court of law may request certification suspension according to the relevant SOP due to business needs.

3 EC SECURITY Certificate

Suspension of EC SECURITY certificate is currently unavailable.

4 Device Certificate

Suspension of Device certificate is currently unavailable.

5 AATL Certificate

Suspension of AATL certificate is currently unavailable.

6 TSA Certificate

Suspension of TSA certificate is currently unavailable.

## 4.9.14 Who Can Request Suspension

1. TLS / SSL Certificate

Suspension is Suspension is not applicable to TLS / SSL certificates.

2. InfoSec Certificate

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

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

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

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

3 EC SECURITY Certificate

Suspension is not applicable to EC SECURITY certificates.

4 Device Certificate

Suspension is not applicable to Device certificates.

5 AATL Certificate

Suspension is not applicable to AATL certificates.

6 TSA Certificate

Suspension of TSA certificate is currently unavailable.

## 4.9.15 Procedure for Suspension Request

1. TLS / SSL Certificate

Suspension is not applicable to TLS / SSL certificates.

2. InfoSec Certificate

(1) Personal Revocation Requests:

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

(2) Online Revocation Requests:

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

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

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

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

3. EC SECURITY Certificate

Suspension is not applicable to EC SECURITY certificates.

4 Device Certificate

Suspension of Device certificate is currently unavailable.

5 AATL Certificate

Suspension of AATL certificate is currently unavailable.

6 TSA Certificate

Suspension of TSA certificate is currently unavailable.

## 4.9.16 Limits on Suspension Period

1. TLS / SSL Certificate

Suspension is not applicable to TLS / SSL certificate.

2. InfoSec Certificate

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

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

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

3. EC SECURITY Certificate

Suspension is not applicable to EC SECURITY certificate.

4 Device Certificate

Suspension of Device certificate is currently unavailable.

5 AATL Certificate

Suspension of AATL certificate is currently unavailable.

6 TSA Certificate

Suspension of TSA certificate is currently unavailable.

# 4.10 Certificate Status Service

## 4.10.1 Operational Characteristics

Certificate status information is available via 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.

## 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** | **O** | **X** | **X** |
| **Administrator** | **X** | **O** | **X** |
| **Auditor** | **X** | **X** | **O** |

# 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 (not including keys for single use or one-time key)

(7) Certificate Registration/Signing

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

(8) Certificate Revocation

- The process of revocation request of certificates.

(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 every six months 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 are backed up at least once every six months and stored in the offsite backup location outside of this CA.

## 5.4.6 Audit Collection System

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

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

## 5.4.7 Notification to Event-Causing Subject

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

## 5.4.8 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 20 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 are 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/CRL 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/CRL 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 disclosure after generation.

Keys are generated in witness by the independent auditor. The independent auditor 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

Subscribers must use the certificates by this CA for electronic signature, encryption, and other purposes with reference to the level of assurance of certificates in accordance with the CPS and the specifications of business application systems. Also, subscribers must follow the instructions specified in the ‘Key Usage’ column in the standard extension of X.509 V3 certificates when using them in the relevant business systems.

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

# 6.2 Private Key Protection and Cryptographic Module Engineering Control

## 6.2.1 Cryptographic Module Standards and Controls

This CA protects private keys with the CNS 15135, ISO 19790 or FIPS 140-2 Class 3 hardware cryptographic modules equipped with multi-person control.

Private keys of AATL Certificate must be generated and stored on FIPS 140-2 Level 2 compliant cryptographic devices.

## 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 unauthorized use of the private key.

### 6.2.10 Method of Destroying Private Key

When a private key has expired, this CA will erase the memory of that private key in the HSM by means of zeroization, so as to destroy the old private key in HSM.

### 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 standard.

## 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.

(1) The key pairs of this CA are valid for a maximum term of 20 years.
(2) The InfoSec Certificate, AATL Certificate and EC SECURITY Certificate are valid for a maximum term of 39 months.
(3) The TLS / SSL Certificate and Device Certificate are valid for a maximum term of 398 days.
(4) The TSA Certificate is valid for a maximum term of 15 months.

# 6.4 Activation Data

## 6.4.1 Activation Data Generation and Installation

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

## 6.4.2 Activation Data Protection

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

## 6.4.3 Other Aspects of Activation Data

No stipulation.

# 6.5 Computer Security Controls

## 6.5.1 Specific Computer Security Technical Requirements

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

(1) System login with identification authentication.

(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 are 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-x962(10045)keyType(2)ecPublicKey(1)} |
| Signature | sha1WithRSAEncryption | {iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)5} |
| 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} |

This CA does not currently sign TLS / SSL Certificates (CP OID= 2.16.158.3.1.8.5) and TSA Certificates using sha1WithRSAEncryption algorithm.

### 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 OCSP specification as defined by RFC 6960 is supported.

## 7.3.2 OCSP Extensions

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

# 8. Compliance Audit and Other Assessments

## 8.1 Frequency and Circumstances of Assessment

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

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

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. The internal auditor will randomly select sample of the greater of one certificate or at least three percent of the TLS / SSL 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) CPS is complied 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.

## 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's personal information 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) To establish, publish and manage the CPS and CP for certificate issuance and the SOPs related to certification.
(2) To confirm the representations and warranties between this CA and RA, and RA should practice in accordance with this CPS, the CP, and related SOPs.
(3) To confirm the selection of certification system personnel (including independent contractors) and ensure that system operation conforms to the CPS.
(4) Operators should take good care of the registration and certificate data and related information of subscribers to prevent leakage, marauding, interpolation and/or unintended use of such data and information.
(5) To accept the request of certificate, certificate rekey, certificate suspension, certificate revocation, and certificate status check made by subscribers (RA) and the related information of registration request; to confirm the accuracy and integrity of the related transaction information delivered to this CA by RA and subscribers; to issue certificates; and to accurately and securely deliver related replies to subscribers in accordance with the CPS.
(6) To accurately and securely deliver TWCA certificates and CRLs to the repository in accordance with the CPS.
(7) To explain the detailed operating procedure of the request of certificate, certificate rekey, certificate suspension, certificate revocation, certificate registration and use, and the related representations and warranties in the contract or related documents for subscribers.
(8) The private key of this CA can only be used to issue and revoke subscriber certificates. If information encryption or another signing task is required, this CA must use a different and independent private key.

This CA Warranties the following:

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

- Identity of Applicant: as described in section 3.2.2 and 3.2.3.

## 9.6.2 RA Representations and Warranties

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

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

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

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

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

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

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

(8) When there are doubts regarding the marauding, exposure and/or loss of the corresponding private key of RA and certificates; or when there is

a change in the related RA information in the certificate, RA must immediately report to this CA issuing that certificate for handling in accordance with the related SOPs.

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

## 9.6.3 Subscriber Representations and Warranties

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

(2) When registering to RA, subscribers must understand and agree to the representations and warranties in the application form and contract, and the contents of the SOPs relating to the request of certificate, certificate rekey, certificate suspension, certificate revocation, certificate registration and use; and accept such prior to signing in the related documents.

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

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

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

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

## 9.6.4 Relying Party Representations and Warranties

(1) When using certificates, relying parties must understand and agree to

the CPS and the representations and warranties specified in the SOP of related business systems. Relying parties also use certificates in related business systems according to the business category specified in the certificate and this CPS without breaking the law and infringing the rights of a third party.

(2) When using certificates, relying parties must verify the accuracy and validity of certificates from the certificate chain in accordance with the CPS, the SOP of application business systems, and X.509 certificate standards. When there is a CRL security mechanism, relying parties should also check if the certificates are revoked or suspended.

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

### 9.6.5 Representations and Warranties of Other Participants

No stipulation.

## 9.7 Disclaimers of Warranties

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

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

(3) This CA is liable to indemnify the damages arising from or in connection with the damage caused to a third party from the leakage, marauding, interpolation or unintended use of the registration and/or certificate data of

subscribers as a result of the failure to keep such data in custody with due faith and due care of this CA.

(4) After receiving a request of certificate revocation or suspension, this CA should revoke or suspend the requested certificates no later than one workday. This CA should also issue the CRL and publish it in the repository within one day from certificate revocation or suspension. Prior to CRL publication, subscribers should take actions appropriate to minimize the impact on trustees and assume all liabilities resulting from the related certificates.

# 9.8 Limitation of Liability

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

# 9.9 Indemnities

Subject to Section 9.2.1.

# 9.10 Term and Termination

## 9.10.1 Term

This CPS 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) “Taiwan-CA Inc.” is the responsible unit of this CPS. Taiwan-CA Inc. 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) Should there be suggestions for updating this CPS, please deliver them to the contact person specified in Section 1.5.2 by mail or e-mail to forward them to the PMA of TWCA.
(2) After being reviewed and approved by the competent authorities, amendments of this CPS will be published in the repository for download.
(3) Unless otherwise specified, this CA will contact subscribers according to the methods specified in Section 9.11.

### 9.12.3 Circumstances Under Which OID Must Be Changed

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

## 9.13 Dispute Resolution Provisions

Subscribers 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.

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.

# 9.16 Miscellaneous Provisions

## 9.16.1 Entire Agreement

No stipulation.

## 9.16.2 Assignment

No stipulation.

## 9.16.3 Severability

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

This CPS is amended according to Section 9.12.

## 9.16.4 Enforcement

No stipulation.

### 9.16.5 Force Majeure

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

## 9.17 Other Provisions

No stipulation.

# Appendix 1 Glossary

(1).Internet

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

(2). (Electronic) Message

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

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

(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 |